



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
CARRERA DE INGENIERÍA EN ELECTRÓNICA TELECOMUNICACIONES
Y REDES

**“EVALUACIÓN DEL RENDIMIENTO DE LAS TÉCNICAS DE
VPNS MPLS CAPA 3 PARA STREAMING DE AUDIO Y VIDEO
CON IPV4 E IPV6”**

Trabajo de Titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

AUTOR: ALEX LEONEL YAUTIBUG CORO

DIRECTOR: Ing. ALBERTO ARELLANO AUCANCELA, Mg.

Riobamba - Ecuador

2020

©2020, Alex Leonel Yautibug Coro

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

Yo, Alex Leonel Yautibug Coro, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo 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 de la misma pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 10 de Marzo del 2020



Alex Leonel Yautibug Coro

060366639-7

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES

El tribunal del trabajo de titulación certifica que: El trabajo de titulación “**EVALUACIÓN DEL RENDIMIENTO DE LAS TÉCNICAS DE VPNS MPLS CAPA 3 PARA STREAMING DE AUDIO Y VIDEO CON IPV4 E IPV6**”, de responsabilidad de Alex Leonel Yautibug Coro, ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación quedando autorizada su presentación.

NOMBRE	FIRMA	FECHA
Ing. Marco Vinicio Ramos Valencia, Msc. PRESIDENTE DEL TRIBUNAL		<u>10/03/2020</u>
Ing. Alberto Arellano Aucancela, Mg. DIRECTOR DEL TRABAJO DE TITULACIÓN		<u>10/03/2020</u>
Ing. Jonny Israel Guaiña Yungan, Mg. MIEMBRO DE TRIBUNAL DEL TRABAJO DE TITULACIÓN		<u>10/03/2020</u>

DEDICATORIA

Dedico este trabajo a Dios, a mis padres, a mi esposa e hijo. A Dios quien me ha dado salud, fortaleza, entendimiento para culminar este camino, a mis padres por ser el pilar fundamental en toda mi educación, tanto académica, como en la vida, a mi esposa por su apoyo incondicional en todo momento, además a mi hijo que es mi mayor motivación para cruzar barreras que se ponen en mi camino y a todas las personas que de una u otra forma colaboraron en la realización del presente trabajo de titulación.

Todo este trabajo ha sido posible gracias a ellos.

Alex

AGRADECIMIENTO

A Dios por darme la vida y brindarme la oportunidad lograr una meta más en mi formación profesional.

Expresar mi agradecimiento y gratitud al director de tesis Ing. Alberto Arellano Aucancela, Mg. y al miembro del tribunal Ing. Jonny Guayña, por la confianza, apoyo, paciencia y sus sabios conocimientos compartidos para efectuar este trabajo.

Un profundo agradecimiento a mis padres Manuel y Madalena quienes han sido la base fundamental de este objetivo alcanzado, de igual forma a mi esposa Rocío, a mis suegros Manuel y Angelita por su apoyo contaste en el transcurso de este tiempo, a mi hijo Jhon Alexis quien es mi mayor inspiración para seguir luchando por la vida, A mi abuelito José Ramon quien ha sido parte importante en mi educación y a toda mi familia por estar pendiente y brindarme sus palabras de aliento.

Extiendo este agradecimiento a la Escuela Superior Politécnica de Chimborazo y a sus Autoridades y docentes quienes me permitieron alcanzar uno de mis objetivos personales, y finalmente mis amigos Fernando M, Cristian V, Ángel O, Franklin L, José P, Edison B, por haber convertido esta etapa estudiantil en una experiencia maravillosa.

Gracias a todos por confiar en mí.

Alex

TABLA DE CONTENIDO

INDICE DE TABLAS.....	xi
INDICE DE FIGURAS.....	xii
INDICE DE GRAFICOS.....	xvi
INDICE DE ANEXOS.....	xviii
RESUMEN.....	xix
ABSTRACT	xx
INTRODUCCIÓN	1

CAPÍTULO I

1 MARCO TEÓRICO

1.1 Multiprotocol Label Switching (MPLS)	8
1.1.1 Modos de funcionamiento	8
1.1.2 Modos Arquitectura de MPLS.....	9
1.1.3 Etiquetas de MPLS.....	10
1.1.4 Pila de etiquetas.....	11
1.1.5 Tipos Especiales de Etiquetas.....	12
1.1.6 Distribución de etiqueta.....	13
1.1.7 Distribución de etiquetas con LDP	13
1.2 MPLS con Redes Privadas Virtuales (MPLS - VPN).....	14
1.2.1 VPNs MPLS de capa 2	14
1.2.1 VPNs MPLS de capa 3	14
1.3 Técnicas de VPNs MPLS de capa 3.....	16
1.3.1 Técnica 6PE	16
1.3.1.2 Técnica 6VPE.....	18
1.4 Inter-AS MPLS L3VPN	20
1.4.1 Inter-AS MPLS VPN- Opción A.....	21
1.4.2 Inter-AS VPN-Opción B entre ASBRs.....	22
1.4.2.1 Método Next-hop-self	23
1.4.2.2 Método Redistribute connected.....	23
1.4.2.3 Método Multi-hop MP-eBGP.....	23
1.4.3 Inter-AS MPLS VPN-Opción C.....	24

1.4.4	<i>Inter-AS MPLS VPN-Opción AB</i>	25
1.4.5	<i>Inter-AS VPN IPv6</i>	26
1.5	Streaming de audio y video	26
1.5.1	<i>Uso de streaming</i>	27
1.5.2	<i>¿Qué necesito para hacer un streaming?</i>	27
1.5.3	<i>Software para el Servidor</i>	28
1.5.4	<i>Software para el cliente.</i>	28
1.5.5	<i>Códec de audio y video</i>	29
1.5.6	<i>Contenedores de Audio y Video</i>	29
1.6	Software de simulación	29
1.6.1	<i>Máquina virtual</i>	29
1.6.1.2	<i>Emulador VMware</i>	30
1.6.2	<i>Emulador GNS3</i>	30
1.6.3	<i>D-ITG</i>	31
1.6.3.1	<i>Arquitectura de D-ITG</i>	31
1.6.3.2	<i>Interfaz gráfica de usuario para D-ITG 2.7</i>	33
1.6.4	<i>Wireshark</i>	33
1.7	Parámetros para evaluar el rendimiento de una red	34
1.7.1	<i>Ancho de banda</i>	34
1.7.2	<i>Retardo o latencia</i>	35
1.7.3	<i>Variación de Retardo o Jitter</i>	35
1.7.4.	<i>Pérdida de Paquetes o Losst Rate</i>	36
1.7.5	<i>Rendimiento o Troughput</i>	36

CAPÍTULO II

2.	MARCO METODOLÓGICO	37
2.1	Diagrama de Bloques de la Metodología	37
2.2	Análisis de las técnicas VPNS MPLS capa 3	38
2.3	Virtualización del emulador GNS3	38
2.3.2	<i>Montar el Emulador GNS3 versión 2.1.21</i>	39

2.4	Escenario en Gns3 técnica 6PE	39
2.4.1	<i>Descripción del escenario de la técnica 6PE.....</i>	39
2.5	Escenario en Gns3 técnica 6VPE.	44
2.5.1	<i>Descripción del escenario de la técnica 6VPE.....</i>	44
2.6	Instalación del servidor Streaming VLC.	48
2.6.1	<i>Virtualización streaming de audio/ vídeo con el reproductor VLC media player</i>	48
2.6.2	<i>Configuración del servidor streaming VLC.</i>	49
2.6.3	<i>Configuración del receptor streaming VLC media Player</i>	51
2.7	Instalación software D-ITG.....	51
2.7.1	<i>Instalación de D-ITG para Windows 7.....</i>	51
2.7.2	<i>Instalación D-ITG y GUIDE en Ubuntu</i>	53
2.7.3	<i>Configuración de inyección de tráfico streaming con D-ITG en el emisor.....</i>	55
2.7.4	<i>Configuración de D-ITG en el receptor.....</i>	57

CAPÍTULO III

3.1	Técnica 6PE	59
3.1.1	<i>Pruebas de conectividad</i>	59
3.1.2	<i>Prueba de streaming con VLC.....</i>	63
3.1.2.1	<i>Pruebas de conexión de los Clientes con el Servidor.....</i>	65
3.1.3	<i>Evaluación de rendimiento con D-ITG.....</i>	68
3.1.3.1	<i>Parámetros configurados en el Emisor de D-ITG.</i>	68
3.1.3.2	<i>Resultados obtenidos en el receptor de D-ITG.</i>	69
3.2	Técnica 6VPE	77
3.2.1	<i>Pruebas de conectividad</i>	77
3.2.2	<i>Prueba de streaming.....</i>	83
3.2.2.1	<i>Transmisión del servidor streaming VLC media Player.....</i>	83
3.2.2.1	<i>Pruebas en el receptor VLC.....</i>	84
3.2.3	<i>Evaluación de rendimiento con D-ITG.....</i>	89
3.2.3.1	<i>Parámetros de configuración en el emisor D-ITG en el emisor</i>	89
3.2.3.2	<i>Resultados obtenidos en el receptor D-ITG.....</i>	89
3.3	Análisis de resultados evaluados entre las técnicas 6PE y 6VPE	97

CONCLUSIONES	113
RECOMENDACIONES.....	115
BIBLIOGRAFÍA	
ANEXOS	

ÍNDICE DE TABLAS

Tabla 1-1	Contiene los valores de etiquetas reservada.....	11
Tabla 2-1:	VPNs en capa 2 y capa 3.....	15
Tabla 3-1:	Técnicas de Transmisión y coexistencia IPv4-IPv6.....	18
Tabla 4-1:	Valoraciones de Retardo.....	35
Tabla 5-1:	Valoraciones de Jitter.....	36
Tabla 1-2:	Cuadro comparativo con características de las técnicas 6PE y 6VPE.....	38
Tabla 2-2:	Descripción general del escenario 6PE.....	40
Tabla 3-2:	Especificaciones de dispositivos utilizados en los escenario para 6PE y 6VPE.....	40
Tabla 4-2:	Direccionamiento de los clientes.....	42
Tabla 5-2:	Direccionamiento en Red Mpls e Inter-AS MPLS L3VPN.....	42
Tabla 6-2:	Direccionamiento del servidor.....	43
Tabla 7-2:	Descripción general del escenario 6VPE.....	44
Tabla 8-2:	Parámetro del flujo en el emisor o servidor.....	55
Tabla 1-3:	Parámetro del flujo en el emisor o servidor.....	68
Tabla 2-3:	Resumen de los resultados obtenidos por D-ITG en la técnica 6PE.....	76
Tabla 3-3:	Parámetro para el flujo en emisor o servidor.....	89
Tabla 4-3:	Resumen de los resultados obtenidos por D-ITG en la técnica 6VPE.....	96
Tabla 5-3:	Datos obtenido en porcentajes desde los diagramas de pastel.....	108

ÍNDICE DE FIGURAS

Figura 1-1:	Ubicación de MPLS en el Modelo OSI.....	8
Figura 2-1:	Funcionamiento Mpls.....	9
Figura 3-1:	Plano de control y de datos.....	9
Figura 4-1:	Estructura de una etiqueta MPLS.....	10
Figura 5-1:	Pila de etiqueta.....	12
Figura 6-1:	Etiqueta de un paquete IP en la red MPLS.....	14
Figura 7-1:	MPLS VPN con VRFs.....	15
Figura 8-1:	Túnel IPv6 sobre una nube MPLS con direccionamiento IPv4.....	16
Figura 9-1:	Prefijo IPv6 6PE o topología de método 6PE.....	17
Figura 10-1:	Enrutamiento 6PE.....	17
Figura 11-1:	Protocolos de enrutamiento con 6VPE.....	18
Figura 12-1:	Atributos de la técnica 6VPE	19
Figura 13-1:	Uso de RT para construir topologías VPN.....	20
Figura 14-1:	Plano de reenvío.....	20
Figura 15-1:	Opciones para implementar inter-AS Layer 3, como Opción A, B, C y D.....	21
Figura 16-1:	Back-to-Back VRF de Inter-AS-VPN Opción A.....	21
Figura 17-1:	Plano de control de Inter-AS-VPN Opción B.....	22
Figura 18-1:	Configuración en ASBR1 de Inter-AS-VPN Opción B.....	24
Figura 19-1:	VPNv4 entre los RR de Inter-AS-VPN Opción C.....	24
Figura 20-1:	Configuración de PE, RR y ASBR de Inter-AS-VPN Opción C.....	25
Figura 21-1:	MPLS VPN Inter-AS Option AB Topology.....	26
Figura 22-1:	Configuración Inter-AS IPv6 VPN.....	26
Figura 23-1:	Ilustración de una comunicación streaming.....	27
Figura 24-1:	Emulador de VMware Workstation 15 Pro.....	30
Figura 25-1:	VMware Player ejecutando la máquina virtual GNS3 VM.....	31
Figura 26-1:	Arquitectura D-ITG.....	32
Figura 27-1:	Interface gráfico D-ITG 2.7.....	33
Figura 28-1:	Captura de tráfico con Wireshark.....	34
Figura 1-2:	Escenario técnica 6PE.....	41
Figura 2-2:	Escenario técnica 6VPE.....	45
Figura 3-2:	Creación de VPNs/VRFs en los router de borde PE.....	46
Figura 4-2:	Inter-AS de proveedores en los routers ASBRS PE2-PE3.....	47
Figura 5-2:	Configuración en PE4 de Hub and Spoke.....	47
Figura 6-2:	Interface de VLC 3.0.8 en Windows 7.....	48
Figura 7-2:	Interface de VLC 3.0.8 en Ubuntu.....	48

Figura 8-2:	Ventana de VLC con la opción emitir.....	49
Figura 9-2:	Ventana de VLC opción añadir archivo de emisión	49
Figura 10-2:	Ventana de VLC configuración de protocolo, puerto y ruta	50
Figura 11-2:	Ventana de VLC configuración del parámetro ttl.....	50
Figura 12-2:	Funcionamiento Streaming.....	51
Figura 13-2:	Archivos descomprimidos DITG y la GUIDE en Windows 7.....	52
Figura 14-2:	Ejecución de GUIDE del Programa D-ITG con JAVA.....	52
Figura 15-2:	Interfaz del Programa D-ITG en Windows 7.....	53
Figura 16-2:	Terminal de Ubuntu con la instalación de los programas de apoyo.....	53
Figura 17-2:	Interfaz con la instalación de D-ITG.....	54
Figura 18-2:	Ejecución de la GUIDE del programa D-ITG en Ubuntu.....	54
Figura 19-2:	D-ITG definición del flujo en el servidor.	55
Figura 20-2:	D-ITG, Configuración en settings del emisor	56
Figura 21-2:	D-ITG, Configuración de Analyzer en emisor	56
Figura 22-2:	D-ITG, Configuración en el receptor	57
Figura 23-2:	D-ITG, Configuración de settings en receptor o cliente1.	57
Figura 24-2:	Archivos generados en Ubuntu en la recepción D-ITG	58
Figura 25-2:	Resultado de tráfico en el receptor.	58
Figura 1-3:	Prueba de conexión del cliente1 con cliente2, cliente3 y servidor.....	59
Figura 2-3:	Tráfico de ICMPv6 en Wireshark capturado entre CE1-PE1.....	60
Figura 3-3:	Prueba de conexión del cliente2 con cliente1, cliente3 y servidor.....	60
Figura 4-3:	Tráfico de ICMPv6 en Wireshark capturado entre PE2-CE2.....	61
Figura 5-3:	Dirección ipv6 en la maquina Ubuntu.....	61
Figura 6-3:	Prueba de conexión del cliente3 con Cliente1, Cliente2 y Servidor.....	61
Figura 7-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace CE3-PC3.....	62
Figura 8-3:	Prueba de conexión del cliente2 con cliente1, cliente3 y servidor.....	62
Figura 9-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace CE4-Servidor.....	63
Figura 10-3:	Ventana del programa SMPlayer con la dirección IPv6 del servidor.....	64
Figura 11-3:	Reproducción de video en SMPlayer.....	64
Figura 12-3:	Ventana configuración de parámetros de recepción.....	65
Figura 13-3:	Reproducción de video en Cliente1.....	65
Figura 14-3:	Tráfico de streaming en Wireshark capturado entre el enlace CE1-PE1.....	66
Figura 15-3:	Reproducción de video en Cliente3.....	66
Figura 16-3:	Tráfico de streaming en Wireshark capturado entre el enlace PE2-CE2.....	67
Figura 17-3:	Reproducción de video en Cliente3.....	67
Figura 18-3:	Tráfico de streaming en Wireshark capturado entre el enlace CE3-PCCliente3..	68
Figura 19-3:	D-ITG, Configuración en el receptor cliente 1 con 30s.....	69

Figura 20-3:	Resultado de tráfico en el cliente 1 con tiempo de recepción 30 segundos.....	69
Figura 21-3:	Resultado de tráfico en el cliente 1 con tiempo de recepción 45 segundos.....	70
Figura 22-3:	Resultado de tráfico en el cliente 1 con tiempo de recepción 60 segundos.....	70
Figura 23-3:	Tráfico de streaming en Wireshark capturado entre el enlace CE1-CLIENTE1.....	71
Figura 24-3:	Resultado de tráfico en el cliente 2 con tiempo de recepción 30 segundos.....	71
Figura 25-3:	Resultado de tráfico en el cliente 2 con tiempo de recepción 45 segundos.....	72
Figura 26-3:	Resultado de tráfico en el cliente 2 con tiempo de recepción 60 segundos.....	72
Figura 27-3:	Tráfico de streaming en Wireshark capturado entre el enlace PE2-CE2.....	73
Figura 28-3:	Resultado de tráfico en el cliente 3 con tiempo de recepción 30 segundos.....	73
Figura 29-3:	Resultado de tráfico en el cliente 3 con tiempo de recepción 45 segundos.....	74
Figura 30-3:	Resultado de D-ITG con protocolo UDP, cliente3 – servidor tiempo de 60 s.....	74
Figura 31-3:	Tráfico de streaming en Wireshark capturado en CE3-CLIENTE3.....	75
Figura 32-3:	Prueba de conexión del cliente1 con el servidor.....	77
Figura 33-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace CE1-Servidor.....	77
Figura 34-3:	Traceroute del CE1-Servidor.....	78
Figura 35-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE4-CE4.....	78
Figura 36-3:	Prueba de conexión del cliente2 con el servidor.....	79
Figura 37-3:	Traceroute del CE2-Servidor.....	79
Figura 38-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE4-CE4.....	80
Figura 39-3:	Prueba de conexión del cliente3 con el servidor.....	80
Figura 40-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE3-CE3.....	81
Figura 41-3:	Traceroute del CE3-Servidor.....	81
Figura 42-3:	Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE4-CE4.....	82
Figura 43-3:	Prueba de conexión del servidor al Cliente1, Cliente2 y Cliente3.....	82
Figura 44-3:	Traceroute del Servidor con Cliente1, cliente2 y Cliente3.....	83
Figura 45-3:	Transmisión correcta del Streaming en el servidor.....	83
Figura 46-3:	Reproducción de video en SMPlayer.....	84
Figura 47-3:	Reproducción de video con Reproductor VLC en Cliente1.....	84
Figura 48-3:	Tráfico de streaming en Wireshark capturado entre el enlace CE1-PE1.....	85
Figura 49-3:	Reproducción de video con Reproductor VLC en Cliente2.....	85
Figura 50-3:	Tráfico de streaming en Wireshark capturado entre el enlace PE2-CE2.....	86
Figura 51-3:	Tráfico de streaming capturado entre enlace PE4-CE4 método HUB and SPOKE.....	86
Figura 52-3:	Ventana configuración parámetros de recepción en VLC.....	87
Figura 53-3:	Reproducción de video con Reproductor VLC en Cliente3.....	87
Figura 54-3:	Tráfico de streaming en Wireshark capturado entre el enlace PE3-CE3.....	88

Figura 55-3:	Tráfico de streaming capturado entre enlace PE4-CE4 método HUB and SPOKE.....	88
Figura 56-3:	D-ITG, Configuración en el receptor cliente 1 con 30s.	89
Figura 57-3:	Resultado de tráfico en el cliente 1 con tiempo de recepción 30 segundos... ..	90
Figura 58-3:	Resultado de tráfico en el cliente 1 con tiempo de recepción 45 segundos.....	90
Figura 59-3:	Resultado de tráfico en el cliente 1 con tiempo de recepción 60 segundos.....	91
Figura 60-3:	Tráfico de streaming en Wireshark capturado entre el enlace CE1-CLIENTE1.....	91
Figura 61-3:	Resultado de tráfico en el cliente 2 con tiempo de recepción 30 segundos.....	92
Figura 62-3:	Resultado de tráfico en el cliente 2 con tiempo de recepción 45 segundos.....	92
Figura 63-3:	Resultado de tráfico en el cliente 2 con tiempo de recepción 60 segundos.....	93
Figura 64-3:	Resultado de tráfico en el cliente 3 con tiempo de recepción 30 segundos.....	93
Figura 65-3:	Resultado de tráfico en el cliente 3 con tiempo de recepción 45 segundos.....	94
Figura 66-3:	Resultado de D-ITG con protocolo UDP, cliente3 – servidor tiempo de 60 s....	94
Figura 67-3:	Tráfico de streaming en Wireshark capturado entre el enlace CE3-CLIENTE3.....	95

ÍNDICE DE GRÁFICOS

Gráfico 1-3:	Diagramas de barras Comparativas de Máximo delay entre las técnicas 6PE y 6VPE	97
Gráfico 2-3:	Diagramas de Barras de la sumatoria total comparativa de Máximo Delay.....	98
Gráfico 3-3:	Diagrama de pastel sumatoria total comparativa de Máximo Delay.....	98
Gráfico 4-3:	Diagrama de barras de promedio Delay de la tabla comparativa 6PE y 6VPE..	99
Gráfico 5-3:	Diagramas de Barras de la sumatoria total del parámetro promedio delay de las tablas comparativas 6PE y 6VPE.....	99
Gráfico 6-3:	Diagrama de pastel de la sumatoria comparativa del parámetro promedio de delay entre la técnica 6PE y 6VPE.....	100
Gráfico 7-3:	Diagramas de barras comparativas del parámetro Jitter entre la técnica 6PE y 6VPE.....	100
Gráfico 8-3:	Diagramas de barras comparativa de Jitter entre las técnicas 6PE Y 6VPE	101
Gráfico 9-3:	Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro total promedio de jitter.	101
Gráfico 10-3:	Diagramas de barras comparativa del parámetro desviación estándar de delay entre la técnica 6PE y 6VPE.	102
Gráfico 11-3:	Diagramas de barras comparativas del parámetro de desviación estándar de delay entre las técnicas 6PE Y 6VPE.....	102
Gráfico 12-3:	Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro desviación estándar de delay.....	103
Gráfico 13-3:	Diagrama de barras comparativas del parámetro velocidad promedio de bits entre la técnica 6PE y 6VPE.	103
Gráfico 14-3:	Diagramas de Barras de la sumatoria total comparativa del parámetro velocidad promedio de bits entre 6PE y 6VPE.....	104
Gráfico 15-3:	Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro velocidad promedio de bits.....	104
Gráfico 16-3:	Diagrama de barras comparativas del parámetro velocidad promedio de paquetes entre la técnica 6PE y 6VPE.....	105
Gráfico 17-3:	Diagramas de Barras de la sumatoria total comparativa del parámetro velocidad promedio de paquetes entre 6PE y 6VPE.....	105
Gráfico 18-3:	Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro velocidad promedio de paquetes.....	106
Gráfico 19-3:	Diagrama de barras comparativas del parámetro paquetes dropeados entre la técnica 6PE y 6VPE.....	107

Gráfico 20-3:	Diagramas de Barras de la sumatoria total comparativa del parámetro paquetes dropeados entre 6PE y 6VPE.....	107
Gráfico 21-3:	Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro paquetes Dropeados.....	108

ÍNDICE DE ANEXOS

ANEXO A: INSTALACIÓN DE GNS3

ANEXO B: VIRTUALIZANDO GNS3 Y ASIGNANDO RECURSOS A LA MÁQUINA VIRTUAL.

ANEXO C: CONFIGURACIÓN EN EL ESCENARIO DE TÉCNICA 6PE

ANEXO D: CONFIGURACIÓN DE LA TÉCNICA 6PVE

ANEXO E: INSTALACIÓN DE VLC EN APLIANCE UBUNTU 19.04

ANEXO F: PASOS PARA GRAFICAR EN UBUNTU.

RESUMEN

El objetivo del presente trabajo fue Evaluar el rendimiento de las técnicas de VPNs MPLS capa 3 para streaming Audio y Video con Ipv4 e Ipv6, se llevó a cabo un estudio minucioso de las VPNs MPLS capa 3 en específico de las técnicas 6PE y 6VPE, ambas técnicas tienen características similares, son utilizados por los proveedores de internet para transportar el flujo de una red de clientes con IPv6 sobre una red MPLS con IPv4, se realizaron dos escenarios de pruebas emulados en GNS3, en el primer escenario se realizó la emulación de la técnica 6PE con sus respectivas configuraciones y pruebas de streaming con VLC, en el segundo escenario se emuló la técnica 6VPE con sus respectivas configuraciones y diferencias: creación de VRFs para cada cliente en los routers PE, en los routers de ASBRs las VPNv6, en la red de servidor el método Hub and Spoke, finalmente se realizaron pruebas de streaming con VLC, para la evaluación de rendimiento se utilizó el software DITG mediante la inyección de tráfico streaming Servidor–Clientes, se obtuvo datos de calidad de servicio desde los clientes, para posterior análisis con diagrama de barras comparativas entre las técnicas 6PE y 6VPE, se concluye que, con la información obtenida de los escenarios propuestos y los tiempos determinados, la técnica 6PE es mejor para la transmisión y recepción de streaming con IPv4 e IPv6, la técnica 6PE obtuvo los siguientes resultados porcentuales de los diagramas de pastel: 18% menos en Máximo delay, 10% menos en Promedio de Delay, 4% menos en Jitter, 20% menos en la Desviación Estándar, 2% más en la Velocidad promedio de Bits, 2% más en la velocidad promedio de paquetes recibidos, en comparación con la técnica 6VPE, en la relación de paquetes dropeados se obtuvo un porcentaje igual por la utilización del protocolo UDP.

PALABRAS CLAVE: <TECNOLOGÍAS Y CIENCIAS DE LA INGENIERÍA>, <TELECOMUNICACIONES>, <MULTIPROTOCOLO POR CONMUTACIÓN DE ETIQUETAS (MPLS)>, <REDES PRIVADAS VIRTUALES CAPA 3 (VPNv3)>, <D-ITG GENERADOR DE TRÁFICO DISTRIBUIDO DE INTERNET (SOFTWARE)>, <GNS3 (SOFTWARE)>.



ABSTRACT

The objective of the present work was to evaluate the performance of the MPLS VPNs layer 3 techniques for Audio and Video streaming with IPv4 and IPv6, a detailed study of the VPNs MPLS layer 3 was carried out specifically of the 6PE and 6VPE techniques, both techniques have similar characteristics, are used by internet providers to transport the flow of a client network with IPv6 over a MPLS network with IPv4, two test scenarios were performed emulating GNS3, in the first scenario the 6PE technique was emulated with its respective configurations and streaming tests with VLC, in the second scenario the 6VPE technique was emulated with its respective configurations and differences: creation of VRFs for each client in the PE routers, in ASBR routers the VPNv6, in the server network the Hub and Spoke method, finally streaming tests were carried out with VLC, for the performance evaluation the DITG software was used by injecting streaming traffic Server-Clients, service quality data was obtained from the clients, for further analysis with comparative bar chart between 6PE and 6VPE techniques, it is concluded that, with the information obtained from the proposed scenarios and the determined times, 6PE technique is better for the transmission and reception of streaming with IPv4 and IPv6, 6PE technique obtained the Following percentage result of the pie charts: 18 % less in Maximum Delay, 10% less in Average Delay, 4% less in Average Jitter, 20% less in standard Deviation, 2% more in Average Bit Rate, 2% more in Average Received Packet Rate, compared to 6VPE technique, in Dropped Packet Rate an equal percentage was obtained by using UDP protocol.

KEY WORDS: <TECHNOLOGIES AND ENGINEERING SCIENCES>, <TELECOMMUNICATIONS>, <MULTIPROTOCOL LABEL SWITCHING (MPLS)>, <VIRTUAL PRIVATE NETWORKS LAYER 3 (VPN L3)>, <D-ITG DISTRIBUTED INTERNET TRAFFIC GENERATOR (SOFTWARE)>, <GNS3 (SOFTWARE)>.



INTRODUCCIÓN

Los proveedores de voz, video y datos distribuyen a los usuarios y clientes sus servicios utilizando diferente infraestructura. Con la evolución de las tecnologías estas redes existentes deben adaptarse a los nuevos requerimientos de los usuarios, basados en el mejoramiento de las prestaciones y costos, que permitan el uso de una sola infraestructura de red. Es inminente para la competitividad de las empresas de Telecomunicaciones la necesidad de migrar sus redes a nuevas tecnologías de convergencia. El modelo de red propuesto por la UIT para cumplir con estas características se denomina NGN o Redes de Próxima Generación.

Para mejorar el sistema de transmisión de datos es muy importante e imprescindible contar con un sistema que sea eficiente y sobre todo confiable incorporando los servicios que permitan una agilidad en el rendimiento de la corporación, como son voz, video y datos. Donde la transferencia de información llegue a su destino sin problema alguno y los servicios prestados por el mismo sean lo óptimo posible. Es por ello que se han desarrollado herramientas eficaces que permiten realizar la evaluación del rendimiento de la calidad de servicios aplicando protocolos y técnicas como lo es VPN con MPLS.

En el Ecuador en los últimos años se han introducido comunicaciones corporativas como estrategia para ofrecer mejores servicios y captar la mayor cantidad de usuarios, para esto se han implementado servicios que incorporan voz, datos y video permitiendo conectar instalaciones separadas por grandes distancias mediante red de datos aumentando el beneficio y garantizando la confiabilidad de su información transmitida. Es así como Instituciones telefónicas (Claro, Movistar, CNT, entre otras) se han visto en la necesidad de incorporar tecnología sofisticada que garantice la confiabilidad de su información compartida, que mejore su productividad y competitividad. Lo que se ha plasmado en la implementación de redes privadas virtuales con la aplicación de protocolos (L2TP, MPLS, IPSEC, entre otros) que permiten mantener la interconexión de todas las sedes de una empresa manteniendo la integridad de estas. (Roberto Usca, febrero 2018)

Telconet S.A. es otra de las empresas dedicada a ofrecer servicios de acceso a Internet y transmisión de datos, con tecnología Multi-Protocol Label Switching (MPLS) y en el backbone de Telconet S.A. en Quito es una red diseñada bajo el modelo jerárquico de tres capas (core, distribución y acceso), constituida por un conjunto de equipos de conmutación y enrutamiento marca Cisco. (Luisana Nieto, & Pablo Hidalgo, noviembre 2010)

La empresa de Movistar ofrece el Servicio VPN IP MPLS, que permite agregar todas las ventajas de las comunicaciones corporativas integradas a los negocios, asegurando su permanente evolución. VPN MPLS permite la creación de redes privadas virtuales que interconectan todas las sedes de su empresa y los recursos productivos desplegados en cada una de ellas, asegurando las capacidades necesarias para todos los tipos de comunicaciones. Este servicio de interconexión de redes utiliza como base la red MPLS de Movistar la cual ofrece calidad de servicio en la transmisión de voz, datos y video, mediante un servicio: Seguro: sus comunicaciones tienen características de seguridad insuperables. Convergente: transporte de comunicaciones de voz, datos y video en la misma Red Privada Virtual. Versátil: permite definir Clases de Servicio, asignando capacidades y priorizaciones de acuerdo con la necesidad específica de cada tipo de tráfico. Eficiente: asigna la capacidad disponible a las aplicaciones que la requieran automáticamente y con control de prioridades. Flexible: facilita la expansión de su negocio de forma ágil y simple, ya sea por el crecimiento de capacidad o por ampliación de cobertura geográfica.

FORMULACIÓN DEL PROBLEMA

La Evaluación de los mecanismos de interoperabilidad de Ipv4 e Ipv6 con VPNs Capa 3 en redes MPLS permitirá determinar la técnica con mejor rendimiento para el streaming de audio y video

SISTEMATIZACIÓN DEL PROBLEMA

- ¿Cuáles son las técnicas usadas en redes MPLS para garantizar interoperabilidad y confidencialidad Ipv4 e Ipv6?
- ¿Cuál es el valor máximo de retardo que se soporta, en la transmisión de audio y video en redes MPLS para garantizar interoperabilidad y confidencialidad?
- ¿Cuál es el formato de audio y video adecuado para garantizar la fidelidad en redes MPLS interoperables?

JUSTIFICACIÓN TEÓRICA

La presente investigación se realiza con el propósito es aportar al conocimiento sobre el uso de: MPLS, VPN-MPLS capa 3, los parámetros de rendimiento de una red y Streaming de Audio, Video.

En la actualidad las empresas y los proveedores de servicios buscan la necesidad de crear redes seguras para enviar y recibir datos (voz, video). Para resolver esta necesidad la tecnología VPN

MPLS es una buena opción, una conexión MPLS VPN permite a un proveedor de servicios crear una conexión de línea dedicada entre dos puntos, el tráfico es dirigido rápidamente a lo largo de la ruta de A - B, garantizando confidencialidad, integridad y seguridad, mediante la utilización de ingeniería de Tráfico permite garantizar calidad de servicio mediante el control de los flujos de datos que viajan por la red, permitiendo evitar la congestión, calculando las rutas más cortas, rutas que se encuentren libres y el ancho de banda disponible.

Las ventajas importantes de este protocolo son:

Ahorros de costes. Dependiendo de la combinación específica de aplicaciones y de la configuración de red de una empresa, los servicios basados en MPLS pueden reducir los costes entre un 10 y un 25% frente a otros servicios de datos comparables (como Frame Relay y ATM). Y, a medida que se vayan añadiendo a las infraestructuras de networking el tráfico de vídeo y voz, los ahorros de costes empiezan a dispararse alcanzando niveles de hasta un 40%.

Soporte de QoS. Uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio (QoS) mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y vídeo en las redes de datos.

MPLS VPNs

Una de las principales demandas de los usuarios que utilizan VPNs, es que cuenten con Calidad de Servicio (QoS).

Todo tráfico que va a entrar por las fronteras de la VPN MPLS es clasificado y etiquetado dependiendo de las políticas definidas por los suscriptores que fueron puestas en ejecución por el proveedor. Posteriormente el tráfico ya etiquetado es transportado a través del núcleo del proveedor, es así como el tráfico que viene entrando y el que está dentro del núcleo del proveedor puede ser clasificado en diversas clases.

Las VPN pueden ser creadas en redes de Capa 2 y de Capa 3. En la Figura 3 se puede observar la jerarquía de las variantes para construir ambos tipos de redes.

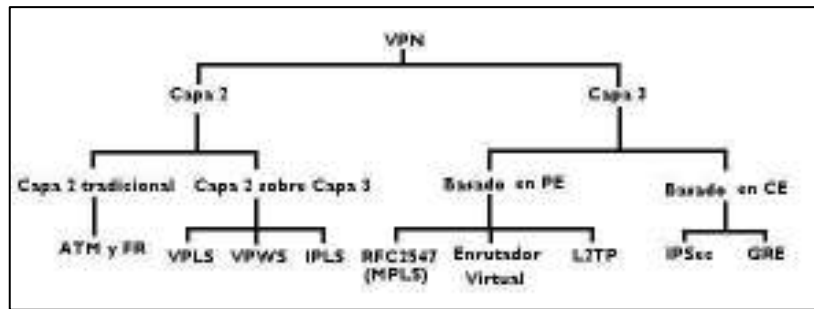


Figura1. Jerarquía VPN.
Fuente: MPLS VPNs

Técnicas de coexistencia de los protocolos IP entre IPv4 e IPv6 son Softwires, 6RD (6to4), 6PE (IPv6 en Provider Edge), 6VPE (IPv6 VPN Provider Edge), DS-lite, NAT64, etc.

En el presente trabajo se trabajará con las técnicas de 6PE (IPv6 en Provider Edge), 6VPE (IPv6 VPN Provider Edge) por que soportan: ingeniería de tráfico, calidad de servicio QoS y VPNs de capa 3.

Ingeniería de Tráfico (TE)

La ingeniería de Tráfico es una de las principales aplicaciones ofrecidas por MPLS debido a que permite mejorar el performance de las redes mediante el control de tráfico y la optimización del uso de los recursos; brindar servicios diferenciados, evitar la congestión y ahorrar costos. (Aguirre Sánchez, 2013).

Parámetros de Calidad de Servicio

Los 4 parámetros que definen la calidad de servicio los cuales son: ancho de banda, retardo, el jitter y la pérdida de paquetes.

Streaming .- se refiere a todo contenido de internet transmitido en tiempo real al momento de los hechos tal como lo hace la televisión digital, esta tecnología es pensado para emisiones de radio online y televisión online en directo o bajo demanda a través de internet, se envía la señal de audio y video a los servidores de streaming VLC y los que va a escuchar ver deben conectarse al servidor VLC a través de internet donde va escuchar a señal de audio y video en directo, el medio por el cual sus oyentes pueden conectarse a una radio puede ser una página web en la cual se incluye el reproductor de audio o también pueden escucharlo directamente a través de Windows media player

Formatos de Streaming de audio y video.

1.- MP4, MPEG-TS, MKV, MOV etc.

Según la investigación de Cisco : Global Mobile Data Traffic Forecast, 2016–2021 estima una pronóstico de tráfico de datos móviles.

Tabla 1-1: proyecciones de uso de aplicaciones de 2016 – 2021

Aplicaciones	2016	2021	CAGR 2016–2021
Web, data, and VoIP	2,153,676	6,434,681	24%
Video streaming	4,375,000	38,148,326	54%
Audio streaming	559,999	2,674,183	37%

Fuente: Global Mobile Data Traffic Forecast

Realizado por: Alex.Y, 2018.

GNS3

GNS3 es un emulador gráfico de red y software gratis que te permite diseñar topologías de red complejas y poner en marcha simulaciones interoperables con diferentes tipos de marcas como Huawei, Alcatel, cisco, juniper, etc.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarias imágenes IOS de Cisco Systems.
- Dynagen, un front-end basado en texto para Dynamips
- Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco o las personas que quieren pasar sus CCNA, CCNP, CCIE DAC o certificaciones.

JUSTIFICACIÓN APLICATIVA

En este proyecto de investigación se busca determinar la técnica más adecuada entre 6PE y 6VPE para la transmisión de audio y video en redes MPLS VPNS capa 3 confiables e interoperables para lo cual se utilizará el emulador de GNS3 que es un software libre que permite la

interoperabilidad de diferentes marcas que existen en el mercado como son Huawei, Alcatel, cisco, juniper, etc., con Qemu, IOS de routers y Switches.

A continuación, el escenario tentativo para las pruebas.

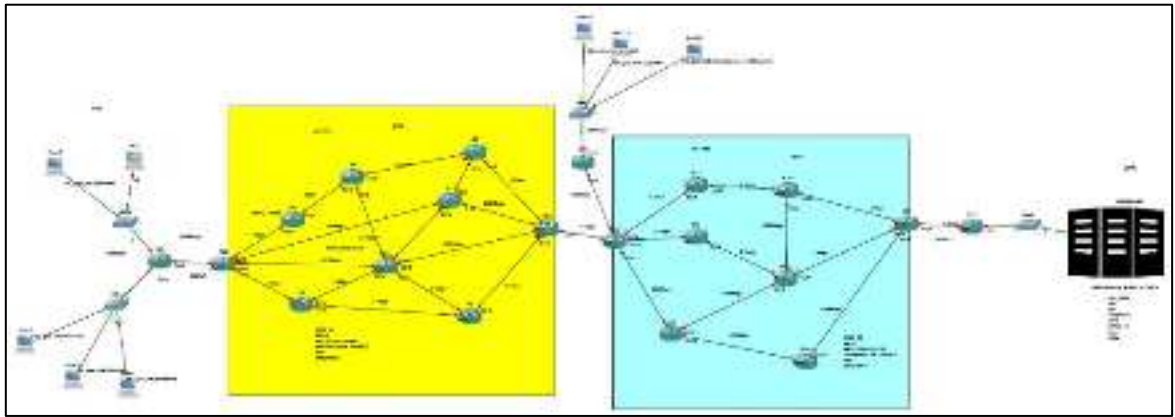


Figura 2. Escenario tentativo.

Fuente: Alex Y, 2018.

Se diseñará 2 escenarios de prueba en GNS3 para comprobar la interoperabilidad de los protocolos ipv4 e ipv6, (Clientes-núcleo MPLS- Servidor VLC), Escenario (ipv6-ipv4-ipv6)

Se simulará redes de clientes que accedan a servidor de streaming de audio y video VLC con diferente formatos y calidad de video atravesando diferentes sistemas autónomos, Cores de MPLS, protocolos de enrutamiento, VPNS-MPLS capa 3 con diferentes técnicas de entunelamiento 6PE/6VPE, se medirá los parámetros de jitter, retardos, y tasa de pérdidas.

Se realizará una evaluación de rendimientos con D-ITG y es un programa para inyectar tráfico y analizar los parámetros de calidad de servicio como delay, jitter y packet loss.

Para concluir este trabajo se dará como resultado que tipo de técnica es mejor (6PE o 6VPE), para streaming de audio y video.

OBJETIVOS

OBJETIVO GENERAL

Evaluar el rendimiento de las técnicas de VPNs MPLS capa 3 para streaming Audio y Video con Ipv4 e Ipv6.

OBJETIVOS ESPECIFICOS

- Estudiar las técnicas de VPNs MPLS capa3 6PE y 6VPE para streaming Audio y Video con Ipv4 e Ipv6.
- Diseñar los escenarios de pruebas en una plataforma de emulación para la verificación de tecnología VPNs MPLS.
- Evaluar mediante D-ITG los parámetros de calidad de servicio como delay, jitter y pérdida de paquetes.
- Determinar la técnica de VPN MPLS capa 3 con mejores características para la transmisión de streaming de audio y video.

CAPÍTULO I

1 MARCO TEÓRICO

En el presente capítulo, se da a conocer las principales técnicas, softwares y elementos necesarios para el análisis del rendimiento de las técnicas de VPNs MPLS capa 3 para streaming Audio y Video con Ipv4 e Ipv6.

1.1 Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) es una técnica creada para el reenvío de paquetes de alto rendimiento. El uso más desarrollado de MPLS en la actualidad es la habilitación de redes privadas virtuales (VPNs). Con la introducción de VPN habilitadas para MPLS, los diseñadores de red pueden escalar sus redes mejor que con los métodos disponibles en el pasado. (Ivan Penelnjack, 2002 pág. 2), en la siguiente **Figura 1-1**, se observa que MPLS está ubicada entre la capa 2 de Enlace de Datos y la Capa 3 la de Red.



Figura 1-1: Ubicación de MPLS en el Modelo OSI.

Fuente: <https://www.seacna.com/wp-content/uploads/2015/12/Capas-ISO-1.png>

1.1.1 Modos de funcionamiento

El reenvío de paquetes IP tradicional analiza la dirección IP de destino contenida en el encabezado de la capa de red de cada paquete a medida que el paquete viaja desde su origen hasta su destino final. Un enrutador analiza la dirección IP de destino de forma independiente en cada salto en la red. Los protocolos de enrutamiento dinámico o la configuración estática crean la base de datos

necesaria para analizar la dirección IP de destino (la tabla de enrutamiento). El proceso de implementación del enrutamiento de IP tradicional también se denomina destino salto por salto enrutamiento unicast. (Ivan Peneljack, 2002 pág. 11)

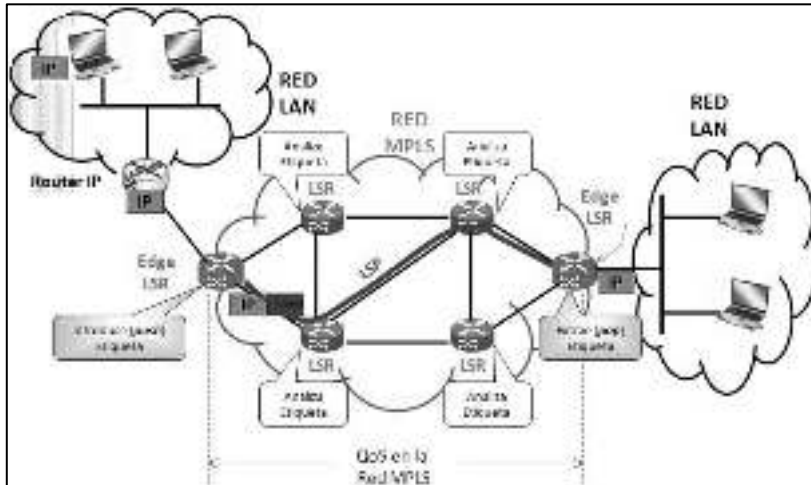


Figura 2-1: Funcionamiento Mpls.

Fuente: Gonzales (2012, p.26).

1.1.2 Modos Arquitectura de MPLS

MPLS se describe un modelo de arquitectura basado en dos planos:

- Plano de control (control plane): utilizado por los protocolos de routing IP y los protocolos de gestión de MPLS.
- Plano de datos (data plane): en este plano donde se realiza la conmutación de los paquetes.

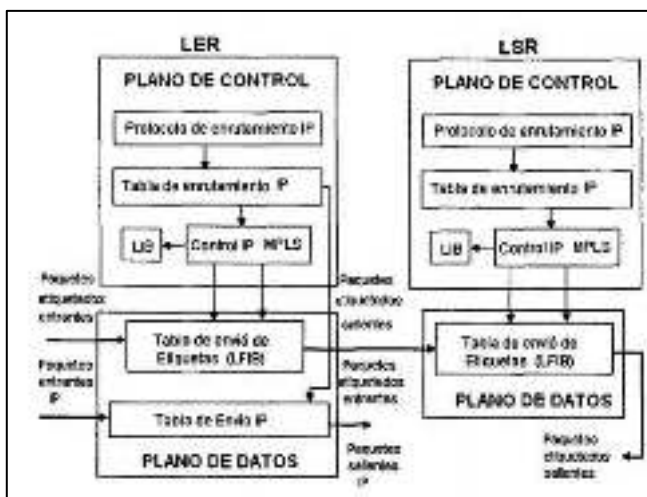


Figura 3-1: Plano de control y de datos.

Fuente: Gonzales (2012, p.27).

El plano de control se encarga de entender las complejidades del enrutamiento éste incluye los protocolos de enrutamiento OSPF, EIGRP IS-IS, BGP, además, existen protocolos de distribución

de etiquetas como TDP (Tag Distribution Protocol) y LDP (Label Distribution Protocol). TDP fue creado por Cisco. Una vez que este protocolo comenzó a dar los resultados esperados solventando los problemas de tráfico con etiquetas, se creó un estándar como el LDP (Santamaría, y otros, 2016 pág. 26).

El plano de datos lleva a cabo tareas relacionadas con el forwarding o envío de paquetes. Estos paquetes pueden ser ya sea paquetes IP o paquetes IP etiquetados. La información en el plano de datos, tal como el valor que llevan las etiquetas, se obtienen del plano de control, los procesos y funciones de cada plano, originan o generar tablas que mencionaremos a continuación:

- **RIB (Tabla de Ruteo IP).**- Contiene información originada por el protocolo de enrutamiento (IGP), está situada en el plano de control y muestra información IP-IP. (Santamaría, y otros, 2016 pág. 27)
- **LIB (Base de Información de Etiquetas).** - Esta situada en el plano de control y es originada por el protocolo de distribución de Etiquetas (LDP), contiene información del siguiente salto, como la etiqueta de salida de acuerdo a una dirección IP destino. (Santamaría, y otros, 2016 pág. 27)
- **FIB (Base de Información de Envío).**- Esta situada en el plano de datos, y es una Imagen de la tabla RIB, mapea las redes destinos y los ruteadores adyacentes. (Santamaría, y otros, 2016 pág. 27)
- **LFIB (Base de Información de Envío de Etiquetas).**- Está situada en el plano de datos, utiliza información de la tabla FIB y LIB para generar una tabla de etiquetas entrantes y salientes. (Santamaría, y otros, 2016 pág. 27)

1.1.3 Etiquetas de MPLS

Las funciones de las etiquetas MPLS son separar las operaciones de envío desde los destinos de capa 3 contenidos en la cabecera de los paquetes asociando una etiqueta con una FEC (Forwarding Equivalence Class). Siendo éste un mecanismo altamente eficiente para el envío de información. La etiqueta MPLS está conformada por 32 bits, divididos en cuatro campos que son los siguientes. Ver **Figura 4-1** (Santamaría, y otros, 2016 pág. 28)

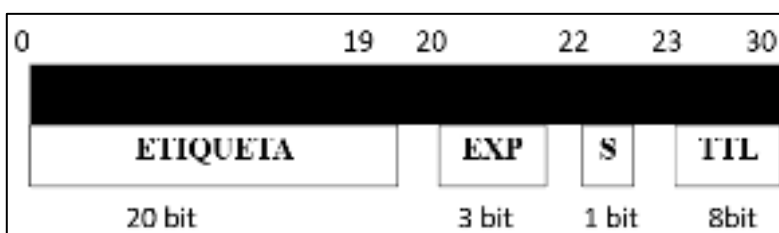


Figura 4-1: Estructura de una etiqueta MPLS.

Fuente: Gonzales (2014, p.29).

Etiqueta tiene un campo de 20 bits campo, este campo contiene el valor de la etiqueta y proporciona la información sobre el protocolo de nivel de red, así como información adicional necesaria para reenviar el paquete. **La tabla 1-1**, contiene los valores de etiquetas reservadas. (Santamaría, y otros, 2016 pág. 28)

La tabla 1-1 Contiene los valores de etiquetas reservada.

Etiqueta	Descripción
0	El paquete proviene de una red IPV4
1	Etiqueta alerta del enrutador.
2	El paquete proviene de una red IPV6
3	Etiqueta nula implícita
4 al 15	Reservados para usos por la agencia de Asignación de números de internet.

Fuente: Estudio de los diferentes modelos de inter-as mpls-vpns.

Elaborado por: Alex Y., 2019

Experimental CoS, tiene un campo de 3 bits, es el campo reservado para uso experimental, indica la clase de servicio (CoS).

Bottom of Stack Indicator (S), campo de 1 bit, es el campo de posición de la pila. Si tiene el valor de “1” indica que es la última etiqueta añadida al paquete IP, si es un “0” indica que hay más etiquetas añadidas al paquete.

Time To Live (TTL), consta con un campo de 8 bits, es un identificador similar a IP, su valor es reducido en cada nodo LSR, puede ser equivalente al del paquete IP, si su valor es “0” y el paquete aún no alcanza su destino el paquete será descartado. (Santamaría, y otros, 2016 pág. 28)

1.1.4 Pila de etiquetas

Es un conjunto ordenado de etiquetas donde cada uno tiene una función específica y es utilizada en varias aplicaciones como:

VPNs de Capa3 donde la segunda etiqueta de la pila indica la etiqueta VPN, Ingeniería de Tráfico (MPLS TE) donde el tope de la pila indica el punto final del túnel y la segunda etiqueta identifica el destino y L2 MPLS VPN donde el tope de la pila indica la cabecera del túnel y la segunda etiqueta el Circuito Virtual. en **figura 5-1** contiene los campos de las pilas de etiquetas. (Santamaría, y otros, 2016 pág. 29)

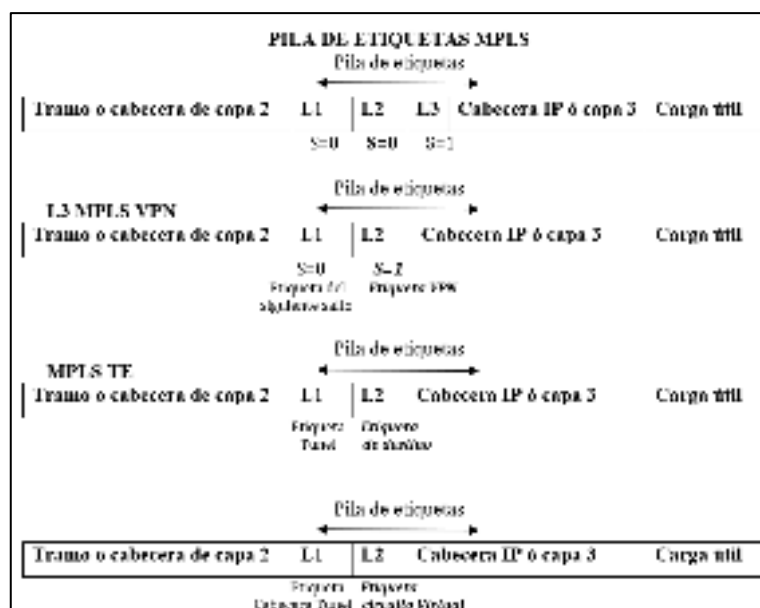


Figura 5-1: Pila de etiqueta.
Fuente: Chica & Samaniego (2008, p.30).

1.1.5 Tipos Especiales de Etiquetas

Existen diferentes tipos de etiquetas dependiendo de su localización en el dominio MPLS de las cuales mencionamos: Sin etiqueta (Untagged).- Es usada en MPLS VPN para enviar un paquete del dominio MPLS a un dominio de destino diferente. (Santamaría, y otros, 2016 pág. 30)

Etiqueta Nula implícita (Implicit-null) Esta etiqueta es asignada y distribuida por un LSR, para indicarle al siguiente salto que la etiqueta debe ser removida de la pila, resultando un paquete sin MPLS, el valor para esta etiqueta es 3 y es usada en las redes MPLS en el Penúltimo Salto (PHP). (Santamaría, y otros, 2016 pág. 30)

Etiqueta Nula Explícita (Explicit-null Label) Es una etiqueta ubicada en el fondo de la pila de etiquetas que nos indica que la operación a realizar es eliminar la etiqueta de la pila y remitir el paquete para que posiblemente sea procesado en base a la cabecera IPv4 o IPv6, su valor puede ser 0 (IPv4) o 2 (IPv6). La etiqueta es cambiada con un valor de 0 o 2 y enviado como un paquete MPLS al próximo salto, esta etiqueta es utilizada en la implementación de QoS con MPLS. (Santamaría, y otros, 2016 pág. 30)

Etiqueta de Agregación (Aggregate) Esta etiqueta permite identificar en una tabla la interfaz de salida cuando un paquete MPLS entrante es convertido a un paquete IP, esta etiqueta es usada en las aplicaciones MPLSVPN. (Santamaría, y otros, 2016 pág. 30)

1.1.6 Distribución de etiqueta

La primera etiqueta la pone el LSR de ingreso y pertenece a un LSP. El camino del paquete a través de la red MPLS está definido por el LSP. El LSR de ingreso o inicio pone las etiquetas, los LSR del intermedio cambian la etiqueta MPLS de entrada por otra y transmiten el paquete por el enlace de salida que corresponda. El LSR de salida quita todas las etiquetas y reenvía el paquete a los routers fuera de la nube MPLS. (Santamaría, y otros, 2016 pág. 31)

La distribución de etiquetas se puede hacer de dos formas:

- Distribución de etiquetas junto con la información de routing
- Utilización del protocolo de routing específico para la distribución de etiquetas

1.1.7 Distribución de etiquetas con LDP

Para cada prefijo IGP en la tabla de rutas, el nodo crea una asociación local, es decir, asocia cada prefijo con una etiqueta. Entonces el router distribuye esta asociación a todos sus nodos vecinos y se denominan asociaciones remotas. Los vecinos entonces almacenan tanto las asociaciones remotas como las asociaciones locales en una tabla especial, la Label Information Base (LIB). Cada nodo tiene una sola asociación local por cada prefijo, y varias asociaciones remotas ya que lo lógico es tener varios vecinos. (Santamaría, y otros, 2016 pág. 33)

Independientemente de las asociaciones remotas que reciba, el router debe seleccionar una sola etiqueta de salida para cada prefijo IP y decidir por enlace reenvía el tráfico. La tabla de rutas determina cual es el siguiente salto para cada prefijo IP.

En la siguiente **Figura 6-1** se observa un paquete IP entrando en la red MPLS por el router PE, donde se le pone la etiqueta 49 dado el prefijo IP destino y es enviado al siguiente nodo, en segundo router intercambia la etiqueta de entrada (49) por la de salida (5) y envía el paquete hacia el tercer router y este vuelve hacer el proceso de intercambiar la etiqueta de entrada (5) por la de salida (201) y reenvía de nuevo el paquete, este proceso se repite en los router que están dentro de la nube MPLS hasta que sale de la red MPLS, al final un router PE saca toda las etiquetas de MPLS y envía a un router CE solo con la dirección IP de destino. Lo vemos gráficamente en la siguiente figura 8.

(Santamaría, y otros, 2016 pág. 34)

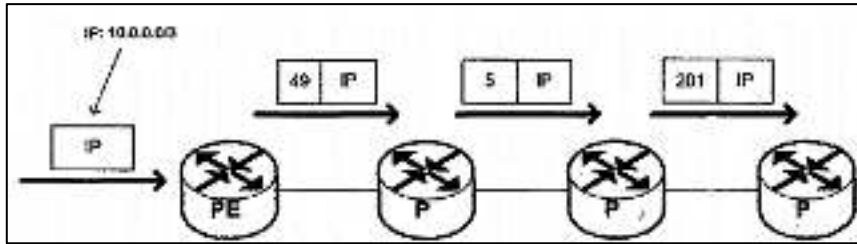


Figura 6-1: Etiqueta de un paquete IP en la red MPLS.

Fuente: Gonzales Carrasco (2011, p.34).

1.2 MPLS con Redes Privadas Virtuales (MPLS - VPN)

Las VPN más son las más utilizadas actualmente en las aplicaciones de la tecnología MPLS, ya que ofrecen escalabilidad, son sencillas de administrar y permiten dividir la red del proveedor, en redes más pequeñas con tablas de enrutamiento separadas. Se definen dos tipos de conexiones VPN: VPN de MPLS de capa 2 y VPN de MPLS de capa 3. (López Lario, 2017)

1.2.1 VPNs MPLS de capa 2

Existen VPNs de capa 2 sobre MPLS que utilizan VPLS, que es un tipo de red privada virtual de capa 2, point-to-multipoint, basada en Ethernet. Un cliente cuyos sitios pertenecieran a la misma LAN. En VPLS, cuando un paquete llega a un dispositivo PE del proveedor desde uno CE del cliente, éste es etiquetado con MPLS y enviado a través de la red del proveedor por una ruta conocida por su nombre en inglés como MPLS Label Switched Path (LSP), las rutas MPLS LSP que transportan tráfico VPLS entre los routers PE son llamadas pseudowires y son configurados de manera estática o distribuidas con BGP o LDP. (López Lario, 2017 pág. 7)

1.2.1 VPNs MPLS de capa 3

En VPNs capa 3, los Routers del proveedor participan en el esquema de ruteo del cliente. En el mismo se incluyen a los equipos de frontera del proveedor (Router Provider Edge, PE), en los cuales se generan tablas de ruteo especiales para separar las rutas privadas de los clientes de las rutas del proveedor. El proveedor asume la responsabilidad de manejar tablas de ruteo específicas para cada VPN, y distribuir esas rutas a los sitios remotos de la VPN. El Router PE del proveedor mantiene una tabla separada para cada VPN que tenga configurada, y estas tablas se completan con la información de prefijos que reciben desde los Routers Customer Edge (CE) conectados. (Cisco Systems, Inc, 2006)

Los Routers PE anuncian estas rutas específicas utilizando sesiones Multiprotocol BGP (MP-BGP) a otros PE en donde la VPN tenga presencia. MP-BGP se utiliza para distribuir

información de las VPNs, distribuir las rutas específicas de cada VPN, y negociar una etiqueta para la VPN. El PE recibe estos anuncios y coloca las rutas en la tabla específica de la VPN correspondiente, identificándola, utilizando los atributos de comunidades extendidas BGP de cada anuncio. En lo que respecta al forwarding, se utilizan LSPs MPLS para enviar el tráfico de la VPN, que pueden ser señalizados con protocolos tales como LDP o RSVP. (Cisco Systems, Inc, 2006)

Para configurar VPNs de capa 3 sobre MPLS se utiliza el concepto de “Virtual Routing and Forwarding” (VRFs), que son tablas de enrutamiento IP virtuales, una por cada VPN, que mantiene el router PE separadas de su tabla de enrutamiento global, En la siguiente **Figura 7-1** se puede mirar la función de VRFs donde el proveedor logra la privacidad que requieren las VPN al mantener separada la información de cada cliente o data , del enrutamiento MPLS con etiquetas.

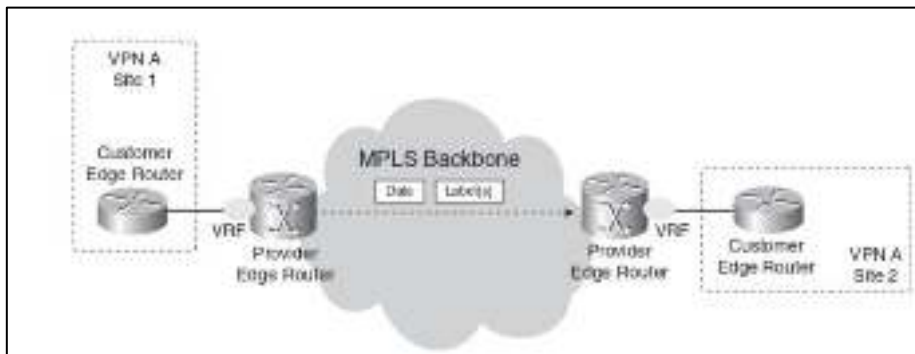


Figura 7-1: MPLS VPN con VRFs.

Fuente: Pruebas de escala de VPNs capa 2 y 3 para la implementación legada basada en MPLS.

Las VRF contienen el mismo tipo de información que las tablas de enrutamiento IP comunes, la diferencia es que son accedidas solamente en caso de que los paquetes sean originados por clientes que pertenezcan a la VPN asociada a la VRF. Cuando un paquete llega a un router PE del proveedor desde un router CE de un cliente que pertenezca a una VPN, es ruteado utilizando la VRF asociada a esa VPN. Con se observa en la **Tabla 2-1**. Existen VPN creadas en redes de Capa 2 y de Capa 3.

Tabla 2-1: VPNs en capa 2 y capa 3

Redes Privadas Virtuales (VPNs)			
CAPA 2	Capa 2 Tradicional	ATM	Modo de transferencia Asíncronico.
		FR	Frame Relay
	Capa 2 sobre capa 3 (L2oL3)	VPLS	Servicio Privado Virtual por Red: servicio punto a multipunto
		VPWS	Servicio Privado Virtual por Cable: servicio punto a punto

CAPA 3	Basado en PE	IPLS	Servicio de Red Exclusivo IP: es un servicio VPN de tipo VPLS
		L2TP	Layer Two Tunneling Protocol: encapsula y envía tramas independientes del protocolo TCP/UDP.
	Basado en CE	VPN MPLS	Es una tecnología incluida en routers de borde PE.
		ENRUTADOR VIRTUAL	La VPN utiliza enlaces punto a punto entre instancias de enrutadores virtuales que se ejecutan los enrutadores físicos.
Basado en CE	IPSEC	Internet Protocol security: comunicación sobre protocolo de internet IP.	
	GRE	Generic Routing Encapsulation: es un protocolo para el establecimiento de túneles a través de Internet.	

Fuente: Funcionamiento de una red MPLS VPN

Elaborado por: Alex Y., 2020

1.3 Técnicas de VPNs MPLS de capa 3.

En la actualidad se necesita de mecanismos que permitan utilizar infraestructuras IPv4 para llevar información de una red IPv6 y viceversa, una de las soluciones es la utilización de Túneles IPv6 en IPv4 estos túneles actúan como enlaces punto a punto y permiten trasportar tráfico IPv6 sobre una red MPLS con direccionamiento IPv4, los routers que están ubicados en los extremos finales son los encargados de realizar esta encapsulación en el origen y la desencapsulación en el destino.

La figura 8-1, muestra el concepto de tunneling.

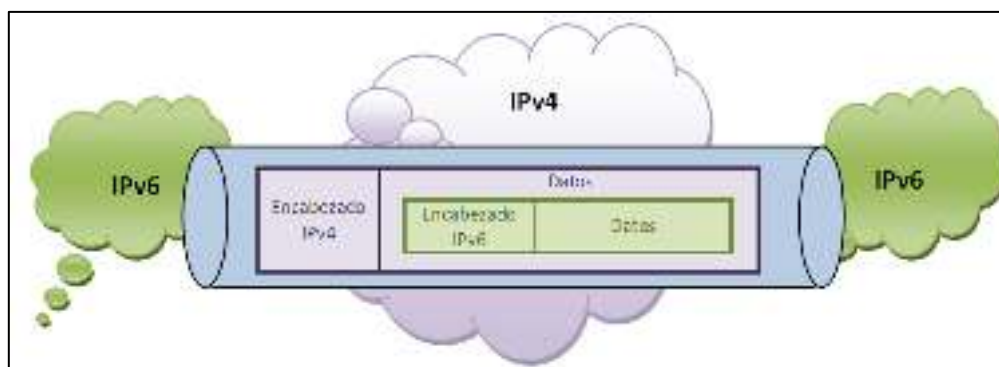


Figura 8-1: Túnel IPv6 sobre una nube MPLS con direccionamiento IPv4.

Fuente: Seguridad de redes implementadas sobre ipv6.

1.3.1 Técnica 6PE

Esta técnica permite transportar IPv6 a través de la red MPLS IPv4 utilizando el protocolo BGP. Cuando BGP soporta IPv4 e IPv6 se lo conoce como (Multiprotocol – Border Gateway Protocol) o (MP-BGP), los routers de borde del proveedor PE deben soportar IPv4 e IPv6 (Dual Stack). En

esta solución los equipos de borde del proveedor PE de ingreso tiene una jerarquía de etiquetas para que el tráfico IPv6 sea transparente para los routers de Core. (Palacios, y otros, 2019), en la **Figura 9-1**, se observa la topología de método 6PE, este método se encuentra en el RFC 4798

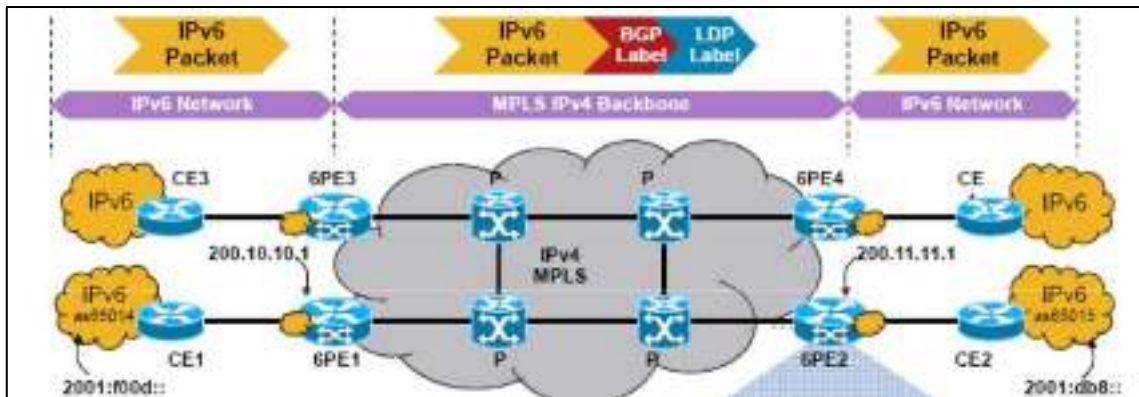


Figura 9-1: Topología de método 6PE.
Fuente: Cisco System.

Los LSP habilitados para IPv4 se pueden establecer utilizando LDP o RSVP-TE, cuando los paquetes IPv6 se tunelizan a través de la red central IPv4, el enrutador de entrada 6PE realiza directamente la imposición de etiquetas en el encabezado IPv6 usando MP-BGP, esta etiqueta indica al router de salida 6PE que el paquete es IPv6, también el router de entrada 6PE impone una etiqueta externa que corresponde a LSP con señal IPv4 que comienza en el enrutador de entrada 6PE y termina en el enrutador de salida 6PE. En la siguiente **Figura 10-1**, se observa el funcionamiento de la técnica 6PE.

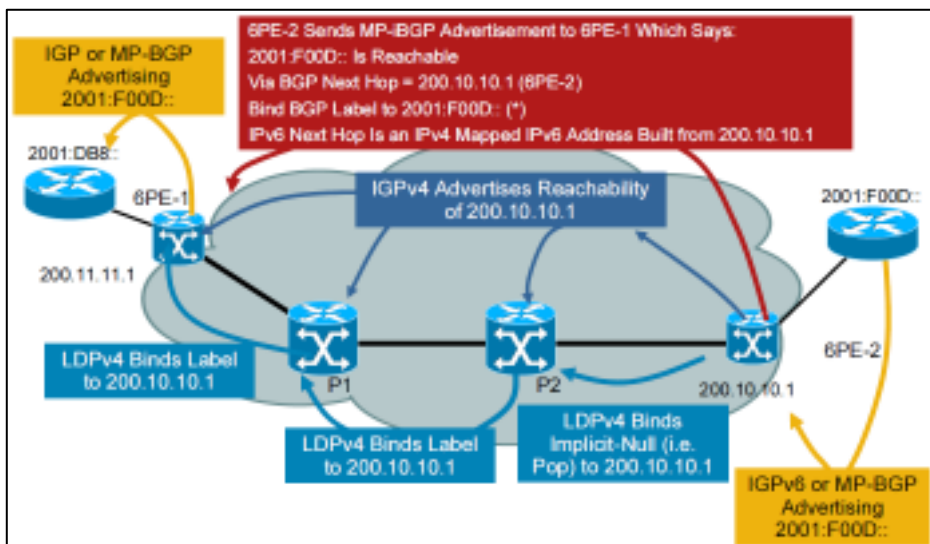


Figura 10-1: Enrutamiento 6PE.
Fuente: Multiprotocol Label Switching.

Paso para el Envío y recepción de paquetes 6PE

1.- envió los paquetes IPv6 desde los router de los clientes CE o Customer Edge .

2.- El router PE recibe un paquete Ipv6, busca el IP destino en el FIB para saber que etiquetas colocar.

3.- los routers P envían el paquete hasta la salida de la red MPLS cambiando las etiquetas que recibe en la entra y poniendo otra a la salida de enlace.

4.- Los PE salida, saca la última etiqueta para envía solos los paquetes IPV6 al router CE (Society, 2012)

Tabla 3-1: Conexión y enrutamiento de la técnica 6PE

Redes	Enrutamiento
Red de clientes	Reenvío: IPv6 Enrutamiento: IGPv6 (IS-IS, OSPF), estático
PE-CE	Reenvío: IPv6 Enrutamiento: eBGP, IGPv6 (IS-IS, OSPF), estático
PE-PE	Reenvío: MPLS Enrutamiento: MP-BGP, IGP Distribución de etiquetas: MP-BGP (V6), LDP (V4)
P-P	Reenvío: MPLS Enrutamiento, IGPv4 (IS-IS, OSPF) Distribución de etiquetas: LDP (V4)

Fuente: Multiprotocol Label Switching.

Elaborado por: Alex Y., 2020

1.3.1.2 Técnica 6VPE

6VPE agrega el soporte de IPv6 a la funcionalidad ya existente de MPLS VPN en IPv4, donde el cliente final mantiene el mismo servicio de VPN con las mismas funcionalidades (calidad de servicio, topologías full mesh o hub and spoke, acceso a internet, etc.), mientras que en el backbone MPLS se mantiene la misma modalidad de configuración para la provisión y operación, tanto para una VPNv4 como una VPNv6, se debe adaptar la capa de Edge MPLS “PE” que provisionará los servicios al cliente. Esta función posibilita brindar conectividad en VPN para IPv4, IPv4+IPv6, o IPv6 hacia el CE. Solo los routers PE deberán ser adaptados, minimizando el impacto, en la **Figura 11-1** se observa el funcionamiento de la técnica 6VPE. (Castro, 2010)

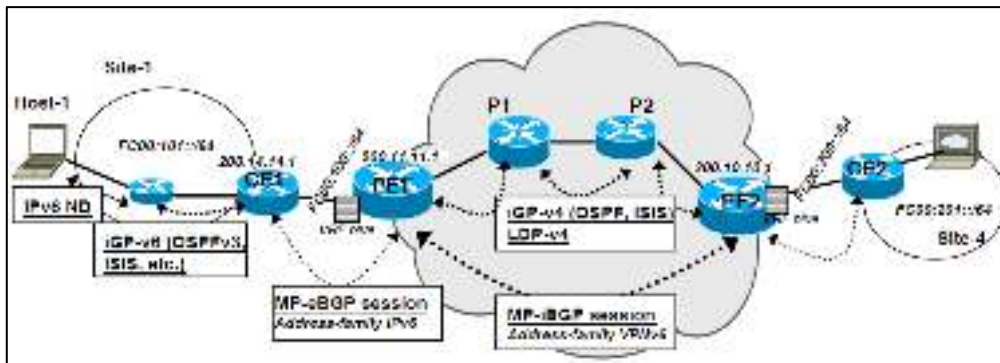


Figura 11-1: Protocolos de enrutamiento con 6VPE.

Fuente: Multiprotocol Label Switching.

La principal diferencia de este método es la creación de VRF en la routers de borde PE. El método de túnel 6VPE, se caracteriza en los enrutadores de borde PE se configura las direcciones IPv6 a las interfaces que van en dirección de CE, y en estas se crea las VRFs de los clientes, los router PE debe soporte los dos protocolos IPv4 / IPv6 simultáneamente. Otro de las cosa que se debe tener en consideración en los enrutadores PE es que distribuyen rutas VPN entre sí a través de MP-BGP y estos personaliza el enrutamiento de cliente VPN según la información VRF configurada localmente (Palacios, y otros, 2019).

Atributos de la técnica 6VPE son :

- Route Distinguisher (RD)
- Route Target (RT)
- VPN Label o Etiqueta de VPN

En la siguiente **Figura 12-1**, se observa los atributos de la técnica 6VPE.

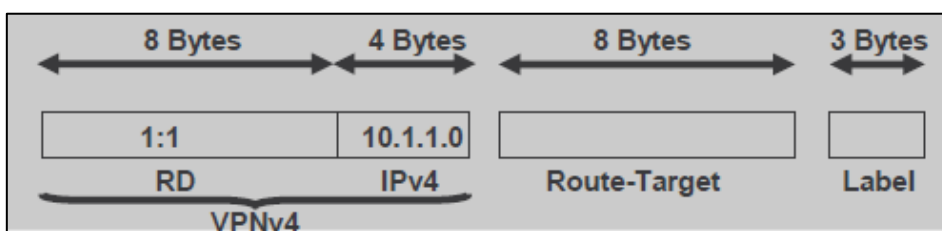


Figura 12-1: Atributos de la técnica 6VPE.

Fuente: Multiprotocol Label Switching.

RD. Tiene un campo de 8 bytes prefijado a la dirección IPv4 del cliente y hace que la dirección IPv4 del cliente sea única dentro de la red MPLS.

Route Targets: determinan qué VRF recibirá y qué rutas, contiene atributos de BGP extended community que se utiliza para controlar las rutas de VPN, existen tipos de RT: Export RT, Import RT y route-target both.

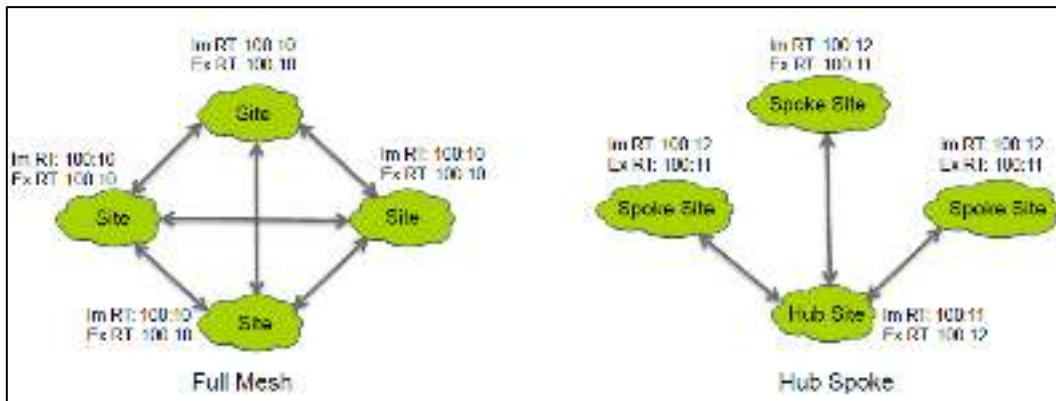


Figura 13-1: Uso de RT para construir topologías VPN.

Fuente: Multiprotocol Label Switching.

En la **Figura anterior** se observa los diferentes tipo de configuración de **RT** en una VPN con son: **full-mesh**, cada sitio de la VPN puede comunicarse con cualquier otro sitio y **Hub-and-Spoke**, la VPNs puede comunicarse solo con el Hub y con diferentes Spoke que están en la misma red y no pueden comunicarse entre redes Spoke

Label. Es un campo donde se coloca una etiqueta para llegar a la salida PE o al destino de Provider Edge la nube Mpls como se observa el siguiente **Figura 14-1**.

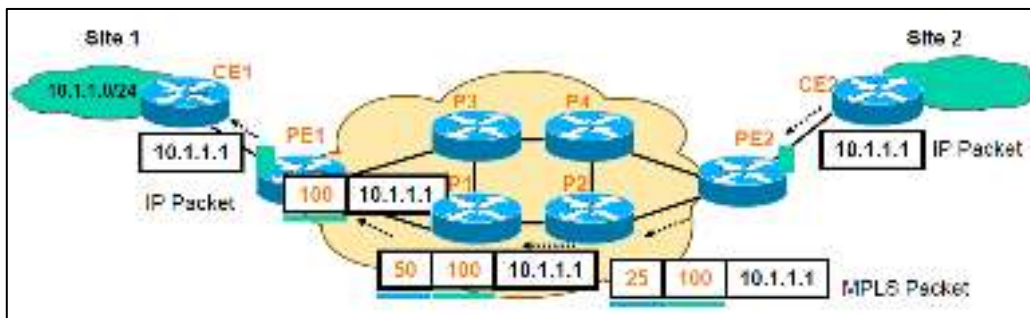


Figura 14-1: Plano de reenvío.

Fuente: Multiprotocol Label Switching.

1.4 Inter-AS MPLS L3VPN

MPLS se implementa en los ISP (proveedores de servicios de Internet), MPLS Layer 3 VPNS principalmente extiende los límites de enrutamiento de un cliente de una ubicación geográfica a otra, las rutas específicas del cliente se reciben en el router CE (Customer Edge) desde PE (Provider Edge/ISP), VPNS Inter-As MPLS layer 3 se puede implementar de 4 maneras diferentes, denominadas como Opción A, Opción B, Opción C y opción AB como se observa en la **Figura 15-1**. (CISCO, 2016)

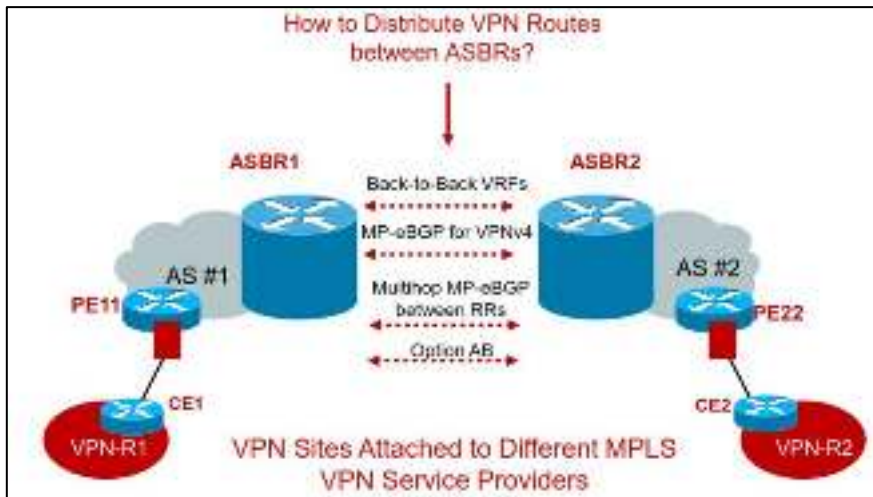


Figura 15-1: Opciones para implementar inter-AS Layer 3, como Opción A, B,C y D.
Fuente: I-AS MPLS Solutions.

1.4.1 Inter-AS MPLS VPN- Opción A

Este modelo llamado VRF-to-VRF (documentación RFC 4364) o back-to-back VRF (nombrado por Cisco) es el modelo es simple para permitir Inter-AS MPLS VPN entre diferentes proveedores.

Los routers que interconectan los AS de los proveedores funcionan como routers de borde llamados (ASBRs), y se encuentran interconectados a través de un único enlace que consiste en subinterfaces lógicas o por medio de múltiples enlaces físicos, en cada ASBR se configuran las VRFs para recoger las rutas VPN del cliente, y cada subinterfaz o interfaz conectada entre los ASBRs se asocia a una sola VRF del cliente. Los paquetes se envían como paquetes IP puros entre los ASBRs, y cualquier protocolo de enrutamiento PE-CE se pueden utilizar con el fin de anunciar el uno al otro la dirección involucrada en la VPN. (OVIEDO CALLE , y otros, 2016)

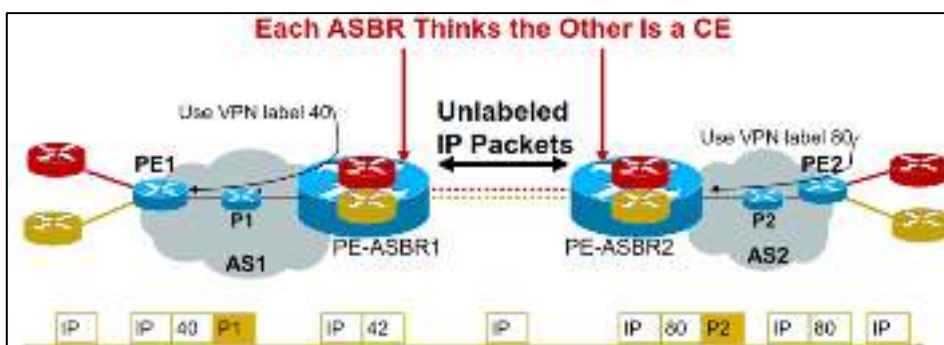


Figura 16-1: Back-to-Back VRF de Inter-AS-VPN Opción A.
Fuente: I-AS MPLS Solutions.

En la **Figura anterior** se puede ver A cada router ASBR trata el router vecino ASBR como una CE, y e intercambian las rutas IPv4 por VRF de la misma manera que lo hacen un PE y un CE, Esta opción es la solución más fácil de implementar una VPN Inter-AS MPLS, la desventaja es

que no es escalable porque hay que configurar todos los VRFs en los ASBRs. Y una ventaja es muy seguro para los proveedores de Internet, ya que no necesitan ninguna IGP, LDP o interacción MP-BGP entre sí. Sólo tienen que conectarse con una interfaz física y hacer tantas sub-interfaces como VPNs que desean conectarse, y luego utilizar un protocolo de enrutamiento PE-CE (podría ser hasta rutas estáticas) con el fin de intercambiar información de enrutamiento VPN. (OVIEDO CALLE , y otros, 2016 pág. 56)

1.4.2 Inter-AS VPN-Opción B entre ASBRs

En esta opción no hay necesidad de tener que configurar las VRFs por cada cliente entre los ASBRs como es en el caso en la opción A, en este método se intercambian prefijos VPNv4 o VPNv6 para diferenciar los clientes VPN, los ASBRs utilizan MP-eBGP entre sí para transportar las rutas VPNv4 o VPNv6 entre los sistemas autónomos, y los paquetes VPN se transportan como paquetes etiquetados entre los ASBRs. (OVIEDO CALLE , y otros, 2016 pág. 57), cómo se observa en la siguiente **Figura 17-1**.

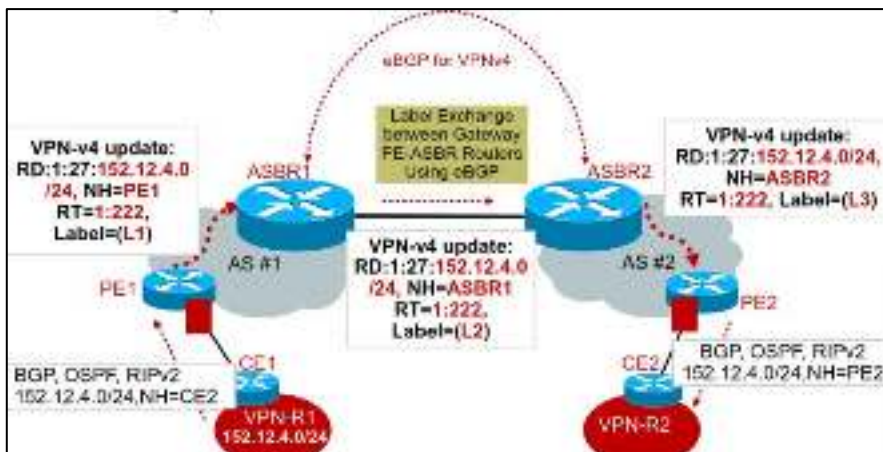


Figura 17-1: Plano de control de Inter-AS-VPN Opción B.
Fuente: I-AS MPLS Solutions.

El principal desventajas de esta opción B se en la calidad de servicio (QoS) y la garantía de entrega de extremo a extremo concretamente entre las ASBRs ya que el tráfico de todos los clientes es transportado por un único enlace como paquetes etiquetados, y muy probablemente este enlace tenga limitada capacidad de ancho de banda.

Este modelo tiene sub-opciones: a.- *Next-hop-self*, b.- *Redistribute connected* y c.- *Multi-hop MP-eBGP*, que difieren principalmente en la forma como se establece la sesión MP-eBGP entre los ASBRs. Las sub-opciones *Next-hop-self* y *Redistribute connected* utilizan las interfaces físicas conectadas directamente, mientras que la subopción *Multi-hop MP-eBGP* establece la sesión MP-eBGP mediante interfaces Loopback. (OVIEDO CALLE , y otros, 2016 pág. 58)

1.4.2.1 Método *Next-hop-self*

La sesión MP-eBGP se establece entre las interfaces físicas directamente conectadas, con *Next-hop-self*, cada ASBR debe anunciarse a sí mismo como el siguiente salto de la ruta MP-eBGP recibida por el ASBRs vecino cuando publica la ruta dentro de su propio sistema autónomo (AS) a través de MP-iBGP. Cada vez que el siguiente salto cambia, una nueva etiqueta se anuncia para el prefijo BGP. (OVIEDO CALLE , y otros, 2016 pág. 58)

1.4.2.2 Método *Redistribute connected*

La etiqueta MPLS VPN cambia solamente una vez en el ASBR local, cuando publica las rutas VPNv4 al ASBR remoto, y cuya etiqueta no será modificada por el ASBR remoto. Cada ASBR debe hacer que la dirección del siguiente salto del ASBR vecino sea alcanzable para su propio sistema autónomo y así ya no sea necesario que se anuncie a sí mismo como el siguiente salto de la ruta.

Es decir , el ASBR acepta la ruta sin cambiar el siguiente salto ni la etiqueta, que continúan siendo los del ASBR remoto. Lo que se hace en su lugar es redistribuirlas redes directamente conectadas dentro del IGP para anunciar el siguiente salto de las rutas recibidas desde el ASBR remoto. En el caso de los subopciones Método *Next-hop-self* y *Redistribute connected*, no hay necesidad de habilitar TDP/LDP o algún IGP entre los ASBRs. La sesión MP-eBGP que se establece en su lugar permite a las interfaces involucradas transmitan paquetes etiquetados, pues ambos ASBRs conocen las etiquetas VPN. (OVIEDO CALLE , y otros, 2016 pág. 59)

1.4.2.3 Método *Multi-hop MP-eBGP*

En este método, la sesión MP-eBGP entre los ASBRs se utiliza las IPs loopback de los routers en lugar de las interfaces físicas, utilizando para ello MP-eBGP Multisalto. Lo primero que se hace es configurar las direcciones IPs loopback como el siguiente salto en cada ASBR. Se puede también usar tanto el método *next-hop-self* como *redistribute connected*, debido a que el siguiente salto en el AS vecino es una ruta estática de la loopback.

Este método es utiliza principalmente cuando existen múltiples enlaces entre los ASBRs, con la finalidad de balancear carga para incrementar el ancho de banda disponible. A diferencia de las sub-opciones anteriores, aquí si se tiene que habilitar LDP entre los ASBRs debido a que ahora los vecinos MP-eBGP no se encuentran directamente conectados. La desventaja de esta opción está en la forma como los LSRs generan e insertan etiquetas para rutas estáticas. Además, esto varía significativamente si las interfaces que conectan los ASBRs son multiacceso o punto-punto. En la **Figura 18-1** se observa las configuraciones del Inter-AS-VPN opción B (OVIEDO CALLE , y otros, 2016 pág. 59)

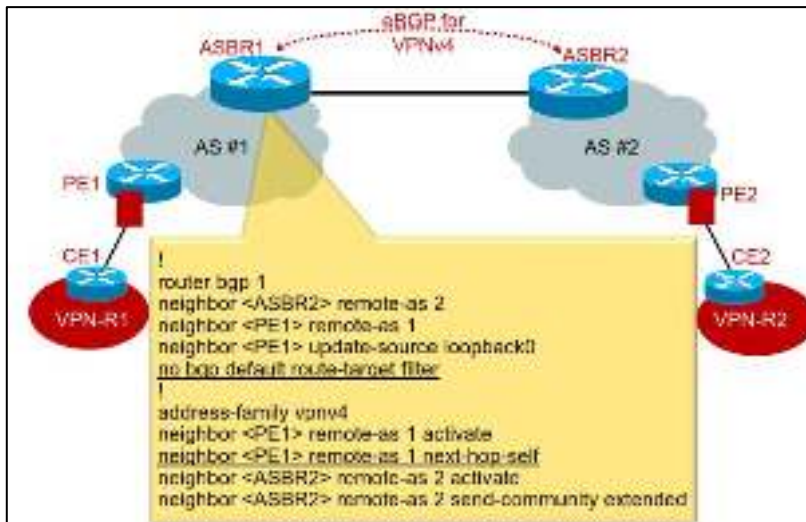


Figura 18-1: Configuración en ASBR1 de Inter-AS-VPN Opción B.
Fuente: I-AS MPLS Solutions

1.4.3 Inter-AS MPLS VPN-Opción C

Esta opción se considera que es la más escalable, ya que en comparación con la opción B, los ASBRs no necesitan aprender todos los prefijos VPNv4, debido a que ahora la sesión MP-eBGP se establece entre los routers Route Reflector (RRs), y no en los ASBRs. Los ASBRs serán los responsables únicamente de intercambiar las direcciones del siguiente salto IPv4 juntos con sus etiquetas a través de eBGP, completándose así la creación de un LSP desde el PE de ingreso local hasta el PE de egreso remoto. Ver en la siguiente **Figura 19-1**.

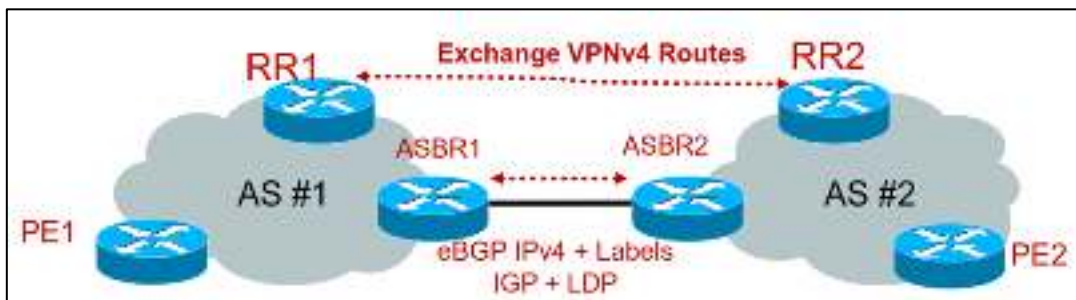


Figura 19-1: VPNv4 entre los RR de Inter-AS-VPN Opción C.
Fuente: I-AS MPLS Solutions

Multihop MP-eBGP entre Route-Reflectors (RRs). En cada ASBR se debe habilitar la sesión eBGP para permitir el intercambio de etiquetas MPLS junto con las rutas IPv4. Para la sesión MP-eBGP entre los Route Reflector (RRs), se debe hacer que el siguiente salto no sea modificado cuando las rutas VPNv4 se intercambien entre los RRs, y los prefijos VPNv4 tampoco deben modificarse. Este es el único caso en el que el LSP no es dividido y la etiqueta MPLS VPN original es usada en todo el tramo, pues el siguiente salto en la ruta VPNv4 nunca cambia.

Debido a que cada AS puede alcanzar los siguientes saltos internos del AS vecino, la seguridad hace que ésta sea una alternativa viable cuando los AS se encuentran bajo una misma autoridad, como es el caso de un proveedor con AS en diferentes regiones del mundo. Sin embargo, se puede incrementar la seguridad utilizando métodos de encriptación para que el tráfico esté cifrado, en la siguiente **Figura 20-1** se observa las configuraciones de Inter-AS-VPN Opción C. (OVIEDO CALLE , y otros, 2016 pág. 60)

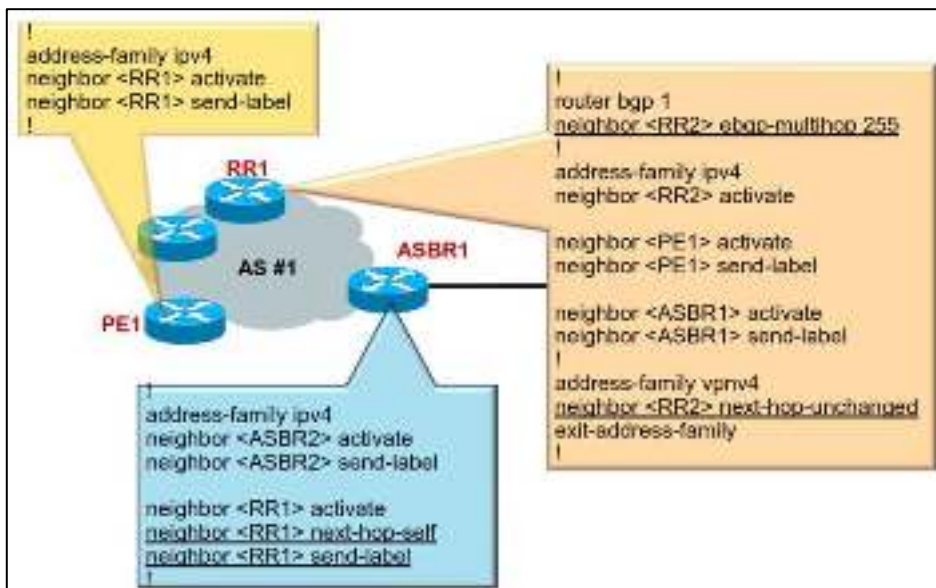


Figura 20-1: Configuración de RR en los ASBR Inter-AS Opción C.

Fuente: I-AS MPLS Solutions

1.4.4 Inter-AS MPLS VPN-Opción AB

Esta opción combina los mejores aspectos de las opciones A y B. Recordemos que la desventaja de la primera opción es que se necesita una sesión BGP para cada subinterfaz (una subinterfaz para cada VPN), que causa problemas de escalabilidad, ya que la red crece. En la segunda opción la desventaja es que, debido a que el tráfico es MPLS, no se puede aplicar mecanismos de calidad de servicio QoS para el tráfico IP y las VRFs no pueden aislarse.

La opción AB permite que los diferentes sistemas autónomos se puedan interconectar mediante el uso de una sola sesión MP-BGP en la tabla de enrutamiento global para transportar tráfico del plano de control. Esta sesión MP-eBGP señala los prefijos VPN entre los dos ASBRs para cada enrutamiento virtual y reenvío VRF. El tráfico de plano de datos está en una interfaz VRF. Este tráfico puede ser o bien IP o MPLS. En la **Figura 21-1** se muestra las opciones que ofrece este método. (OVIEDO CALLE , y otros, 2016 pág. 61)

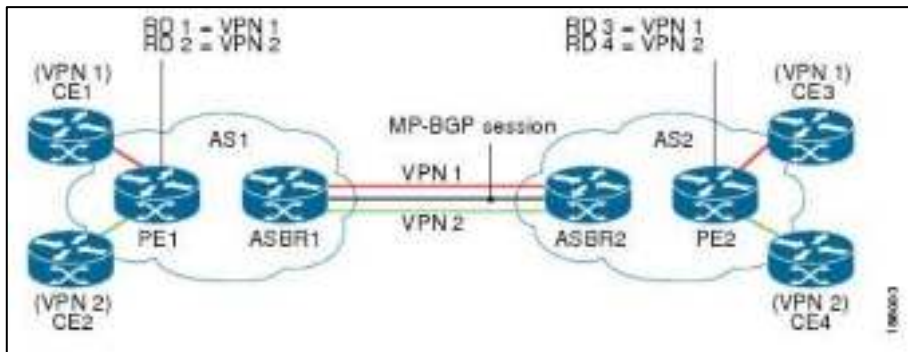


Figura 21-1: MPLS VPN Inter-AS Option AB Topology.
Fuente: MPLS VPN--Inter-AS Option AB

1.4.5 Inter-AS VPN IPv6

Las cuatro opciones de conectividad-ASBR-A ASBR estudiados en la sección anterior son compatibles con P6 Provider Edge Router - 6PE - modelo (IPv6) y VPN IPv6 Provider Edge- 6VPE - modelo (utiliza la opción A, B, C) (Live, 2010)

Como se ve en la siguiente **Figura 22-1**, se utiliza la dirección IPv4 dentro de la nube MPLS, es decir entre el router PE-ASBR1 mientras que entre ASBR1-ASBR2 puede ser IPv4 o IPv6 y entre ASBR2-PE2 utiliza la dirección IPv4 porque es la Área de MPLS.

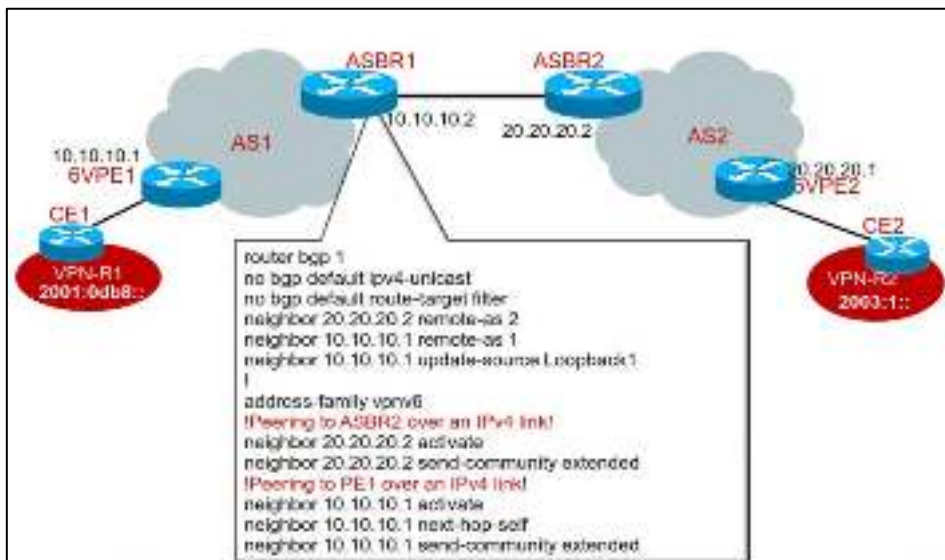


Figura 22-1: Configuración Inter-AS IPv6 VPN
Fuente: I-AS MPLS Solutions.

1.5 Streaming de audio y video

Streaming es una comunicación online mediante un proveedor de internet como, una emisora online que se presentan contenido en vivo y en directo y realizan programas y entrevistas para transmitir en tiempo real, no tienen frecuencia en AM o FM. Es solo por Internet o puede ser una

canal de Tv en vivo para usuarios de todo el mundo vean su emisión de vídeo sin límites geográficos, en vivo y en directo y en tiempo real. En otras palabras, el Streaming es el comúnmente llamado Radio online, TV online o WebTV. (CeHis LTDA., 2016)

El streaming simplemente es la tecnología que nos permite ver un archivo de audio o video directamente desde internet en una página o aplicación móvil sin descargarlo previamente a nuestro dispositivo, con el auge de plataformas de transmisión de contenidos como Netflix, Spotify, Dezeer, Hulu, iTunes entre otras, el termino streaming entra a nuestro vocabulario con más fuerza cada día. Y es que desde que aparecieron estos jugadores en el mapa, ver un video, escuchar música, películas, eventos en vivo, programas de TV, por internet, es pan de cada día, en la **Figura 23-1** se ve la ilustración de una comunicación streaming. (CeHis LTDA., 2016)



Figura 23-1: Ilustración de una comunicación streaming.

Fuente: <http://streaming.com.co/blog/2015/05/18/que-es-y-para-que-sirve-el-streaming/>

1.5.1 Uso de streaming

En los últimos años con la evolución de comunicación digital se puede hacer comunicación en tiempo real por ejemplo los miembros de una compañía vean, un seminario, una conferencia o la feria y/o exposición a la que no todos tus clientes podrán asistir, esa fiesta que quieres que todo el mundo vea, es decir que streaming permite transmitir por internet toda esta serie de eventos o contenidos a través de un sitio web o móvil.

1.5.2 ¿Qué necesito para hacer un streaming?

Un proveedor de Servicios de Streaming. Puede ser un proveedor gratuito o uno de pago. Te recomiendo por supuesto para proyectos serios o empresariales contratar los servicios de un profesional,

Elementos y equipos de Transmisión. Debes contar con equipos (Hardware) que te permitan capturar una señal de audio y video de una cámara, por ejemplo, y enviarla a tu proveedor de streaming para que se pueda visualizar desde internet. También se necesita algún software que

codifique la señal de audio y video y establezca la conexión con el servidor de Video. (CeHis LTDA., 2016)

Un computador Para comenzar a transmitir es necesario contar con un equipo PC o Mac con ciertas características, Conexión a internet: Tal vez el factor más importante que define la calidad de la imagen o audio que experimentara el visitante. Se requiere una conexión de Internet en el punto donde se originará la señal. Dicha conexión debe cumplir unos requerimientos mínimos, se sugiere que para una transmisión de audio se cuente con una conexión no inferior a 1Mbps de subida (UPLOAD). En vídeo se recomienda 2Mbps de UPLOAD para una buena calidad de imagen. (CeHis LTDA., 2016)

1.5.3 Software para el Servidor

Existe software libre y gratuito para comenzar la emisión de audio. VLC es el más popular en cuanto al vídeo, lo que hacen es realizar la codificación de los datos de tal forma de que sean lo suficientemente “livianos” para transmitirse rápidamente sin perder calidad, Códecs como AAC plus, mp3 para el Audio y H264 o VP6 en video son los más comunes, técnicamente cualquier PC podría ser servidor de streaming, sin embargo, dado que son estos equipos quienes procesan todos los datos de audio y video requieren gran capacidad de procesamiento.

Generalmente son servidores XEON QuadCore con hasta 8 núcleos. Por otra parte, también son los encargados de la distribución hacia todo Internet. por tanto, deben tener un gran ancho de banda y transferencia para poder recibir cientos o miles de solicitudes simultaneas. Son equipos ubicados en datacenter con conexiones redundantes de 100Mbps o hasta de 1Gbps o más Gbps, si pusiéramos un servicio de estos en nuestro hogar, no lograríamos transmitir nuestra señal a más de 5 personas al mismo tiempo. (CeHis LTDA., 2016)

En cuanto a servidores se refiere, hay cientos de empresas proveedores de servicio de streaming, al igual que con el hosting existen otras tantas que ofrecen este servicio gratuitamente bajo algunas condiciones de uso (Publicidad y uso de marca). Es decisión de cada usuario cual es el servicio que más le conviene (De pago o gratis) según el uso o requerimiento que tenga para su empresa o compañía. (CeHis LTDA., 2016)

1.5.4 Software para el cliente.

Es quien se encarga de recibir la señal desde el emisor, decodificarla según sea el caso, y redistribuir dichos datos a tantos usuarios como se soliciten desde la página web del usuario

1.5.5 *Códec de audio y video*

Códec viene de codificador-decodificador. Básicamente, un códec es una pieza de software capaz de transformar un flujo de datos o señal la mayoría de los códecs realizan una compresión de la información, en muchos casos con pérdida. A mayor pérdida menor calidad. Un códec codifica un flujo de datos o señal para su almacenaje o transmisión y lo decodifica para su reproducción. (Yáñez Izquierdo, 2011 pág. 3)

Códecs de audio: Algunos códecs usuales de audio son: PCM (Pulse Code Modulation), Flac (Free Lossless Audio Códec), Mp3 (Mpeg layer 3), Wma (Windows media audio), Aac (advanced audio códec), Amr (adaptive multi rate) (usado en telefonía móvil) y los códecs de video: ZMBV (zip motion block video, AVS (audio video standard), H.264 (usado en blue-ray), mpeg-2 (usado en DVDs)

1.5.6 *Contenedores de Audio y Video*

Un contenedor es un formato de archivo que indica como los distintos tipos de datos que contiene un archivo coexisten dentro del archivo, los formatos contenedores se suelen utilizar en archivos multimedia, en donde en un archivo pueden coexistir datos de vídeo, de audio y/o otro tipo de información (información de sincronización, subtítulos. (Yáñez Izquierdo, 2011 pág. 6)

Contenedores exclusivos de audio: AIFF, WAV, XMF, algunos contenedores de videos: avi (.avi), matroska (.mkv), quicktime (.mov), realmedia (.rm), mp4 (.mp4), mpeg-ts (.ts).

1.6 *Software de simulación*

1.6.1 *Máquina virtual*

Una máquina virtual es un equipo con software que, al igual que un equipo físico, ejecuta un sistema operativo y aplicaciones. La máquina virtual está compuesta por un conjunto de archivos de configuración y especificaciones. Además, cuenta con el respaldo de los recursos físicos de un host. Todas las máquinas virtuales tienen dispositivos virtuales que ofrecen la misma funcionalidad que un hardware físico, son más portátiles, más seguras y fáciles de administrar. (VMware, Inc., 2017 pág. 11)

Para usar una máquina virtual lo primero que necesitas es instalar una aplicación en tu PC capaz de crearla o al menos reproducirla. Hay varias aplicaciones muy conocidas capaz de hacer esto, aunque las más famosas son VMware, VirtualBox, QEMU y Parallels.

1.6.1.2 Emulador VMware

VMware Workstation es un producto de software de la empresa VMware Inc., que consiste de una máquina virtual para computadoras x86 y 64, este software permite a los usuarios armar múltiples computadoras virtuales x86 y 64 y usar una o más de esas computadoras virtuales simultáneamente con el sistema operativo anfitrión. Cada instancia de máquina virtual puede ejecutar su propio sistema operativo huésped como Windows, Linux, etc. En la siguiente **Figura 24-1** se observa la ventana principal de VMware Workstation 15 Pro. (Alegsa, 2016)

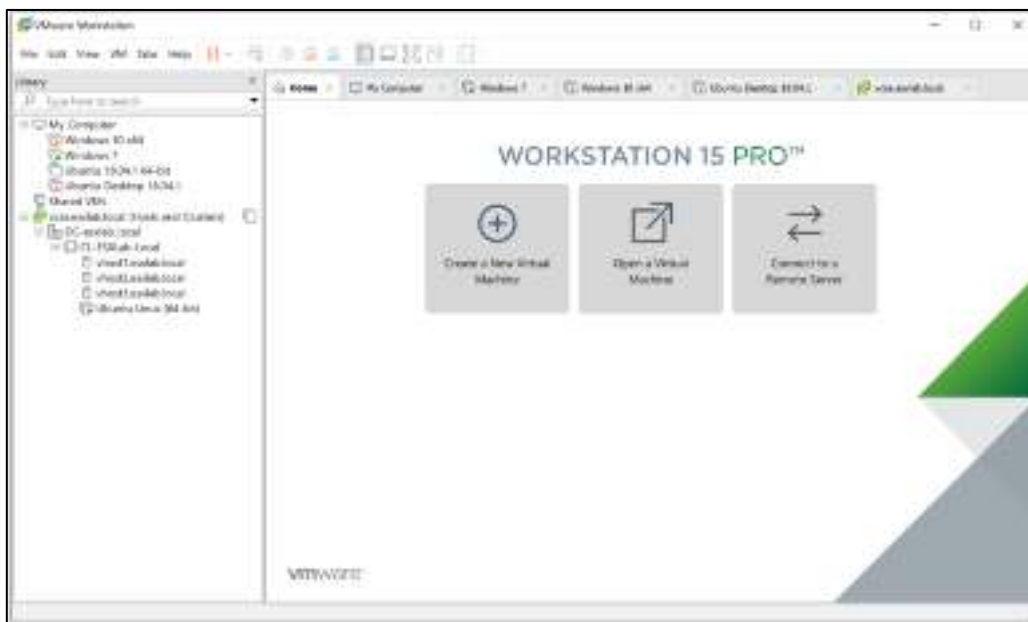


Figura 24-1: Emulador de VMware Workstation 15 Pro.

Fuente: <https://www.artistapirata.com/linux-vmware-workstation-15-pro-32-y-64-bits/>

1.6.2 Emulador GNS3

GNS3 es una aplicación realizada en Python que usa las librerías de Dynagen para crear la interfaz gráfica. Sus principales funciones son editar el archivo de texto .net y realizar las operaciones de interfaz por línea de comandos (CLI) de Dynagen y Dynamips. Este software es un emulador de dispositivos. Es posible copiar el IOS Cisco desde un router Cisco físico real y correr este en un virtual emulado en GNS3, también simula las características y funcionalidades de dispositivos tales como un switch, GNS3 puede ser considerado como un lugar de reunión para una variedad de emuladores de sistemas operativos. Estos emuladores son Dynamips, Qemu, Pemu, Virtual Box y VMware. En la **Figura 25-1** Se observa VMware Player ejecutando la máquina virtual GNS3 VM. (GOMÉZ CARMONA, 2017)

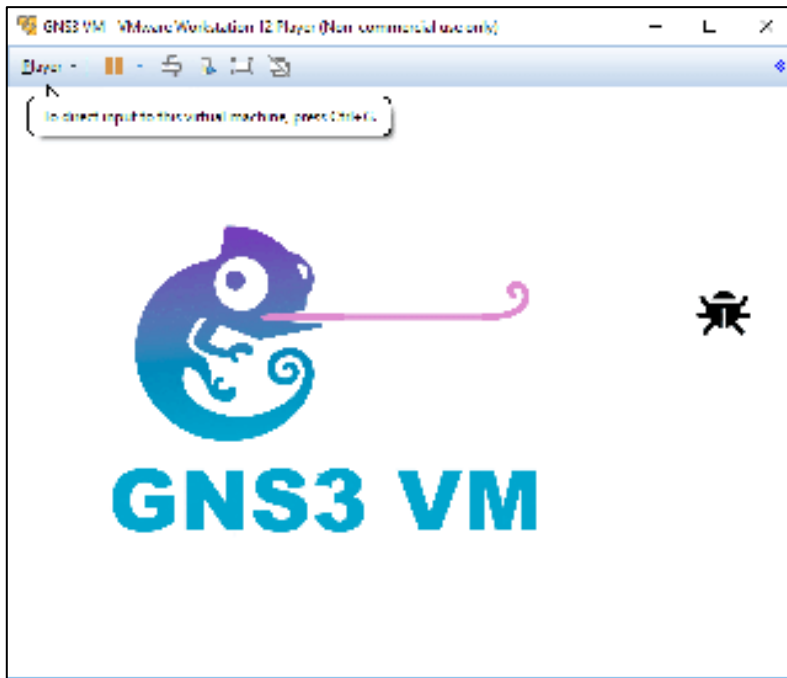


Figura 25-1: VMware Player ejecutando la máquina virtual GNS3 VM.

Fuente: <https://i2.wp.com/telectronika.com/wp-content/uploads/2018/06/GNS3-VM-inicio.png?ssl=1>

1.6.3 D-ITG

Distributed Internet Traffic Generator (D-ITG), es una plataforma de código abierto capaz de producir tráfico con paquetes de tamaño determinado, replicando procesos estocásticos apropiados para el tamaño de paquetes (PS - PACKET Size) y para el tiempo interno de salida entre paquetes (IDT - Inter Departure Time between pACKets), soporta protocolos IPv4 e IPv6, tráfico UDP y TCP, que pueden ser generados en las capas de red, transporte y aplicación, trabaja sobre Linux, OSX y Windows.

El programa puede calcular el retardo de ida (OWD - One Way Delay) y el de ida y vuelta (RTT - Round Trip Time); entrega también la evaluación de paquetes perdidos y la medida del throughput por lo que está concebido para ser usada como una herramienta distribuida de medición de rendimiento. (CANO, y otros, 2012 pág. 74)

1.6.3.1 Arquitectura de D-ITG

La plataforma D-ITG sigue el modelo cliente-servidor y muestra una arquitectura distribuida multicomponente. La **Figura 26-1** muestra la relación entre los principales bloques del programa que son ITGSend, ITGRecv, ITGLog, e ITGDec, la comunicación entre el transmisor y el receptor se realiza usando un canal de señalización separado de los datos bajo un protocolo de configuración. (Traffic Specification Protocol - TSP). (CANO, y otros, 2012 pág. 75)

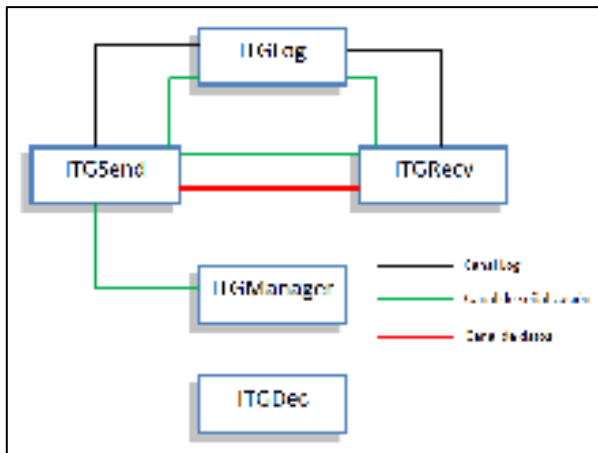


Figura 26-1: Arquitectura D-ITG.

Fuente: Análisis del desempeño de una red con tecnología wi-fi

ITGSend. - Es el componente destinado a la transmisión, opera en 3 modos diferentes:

a) Modo de flujo único. Un solo canal es responsable por la generación de un solo flujo y del manejo de la señal a través del protocolo TSP.

b) Modo de flujo múltiple. Se genera un conjunto de flujos, que opera como una aplicación multiproceso, un canal implementa el protocolo TSP y guía el proceso mientras que el otro genera el flujo de tráfico.

c) Modo Daemon. El componente de transmisión es controlado remotamente por el ITGManager. Para recoger estadísticas, durante el proceso ITGSend registra la información acerca de los flujos generados.

ITGRecv.- Trabaja siempre como una herramienta daemon, escuchando permanentemente si hay nuevas conexiones TSP. Cuando una nueva conexión requiere entrar, éste genera un nuevo segmento por cada flujo, responsable por el manejo de la comunicación con el transmisor.

ITGLog.- Es un servidor de registro, corre en un distinto alojamiento que el ITGSend y el ITGRecv, se encarga de recibir y almacenar la múltiple información del transmisor y receptor. Para esta actividad de registro se usa un protocolo de señalización que permite la entrada y salida al servidor. La información puede ser enviada mediante un canal confiable (TCP) o por un canal no tan confiable (UDP).

ITGDec.- Es una utilidad que permite decodificar toda la información generada en el “log” de ITGSend y en el “log” de ITGRecv para analizar los resultados.

D-ITG permite almacenar información en el transmisor y en el receptor, y es posible recuperar información desde donde se generó, adicionalmente permite al transmisor y al receptor conectarse con un servidor remoto mediante una operación de Log o registro, lo que es útil cuando el transmisor o el receptor tienen limitada capacidad de almacenamiento como en el caso de PDAs, o celulares. (CANO, y otros, 2012 pág. 76)

1.6.3.2 Interfaz gráfica de usuario para D-ITG 2.7

Esta GUI está escrita en Java y debe admitir cualquier plataforma en la que D-ITG sea y será portado. Básicamente es un contenedor para las herramientas de línea de comandos incluidas en el software D-ITG, su licencia, actualmente es gratis, puede usarlo y distribuirlo libremente, en la **Figura 27-1** se observa la Interface gráfico D-ITG 2.7.

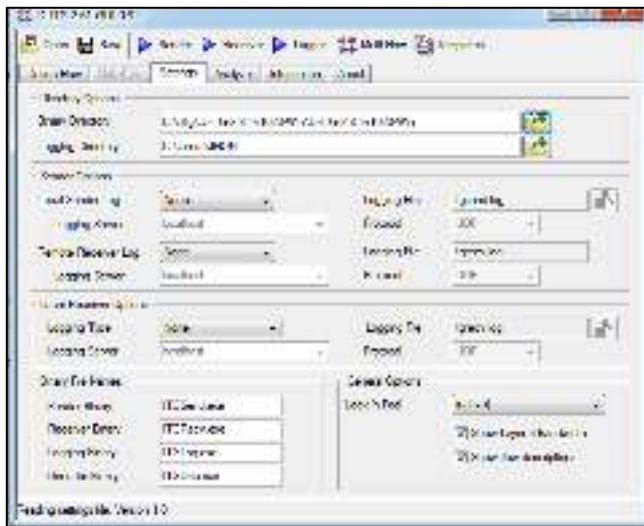


Figura 27-1: Interface gráfico D-ITG 2.7.

Fuente: <http://www.semken.com/projekte/index.html>

1.6.4 Wireshark

Wireshark es un analizador de protocolos open-source actualmente está disponible para plataformas Windows y Unix, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red. Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente (versión 3.0.7); y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados.

Gracias a que Wireshark “entiende” la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar

ciertas tareas en el análisis de tráfico. En la **Figura 28-1** se observa la ventana de Wireshark. (INTECO, 2011)

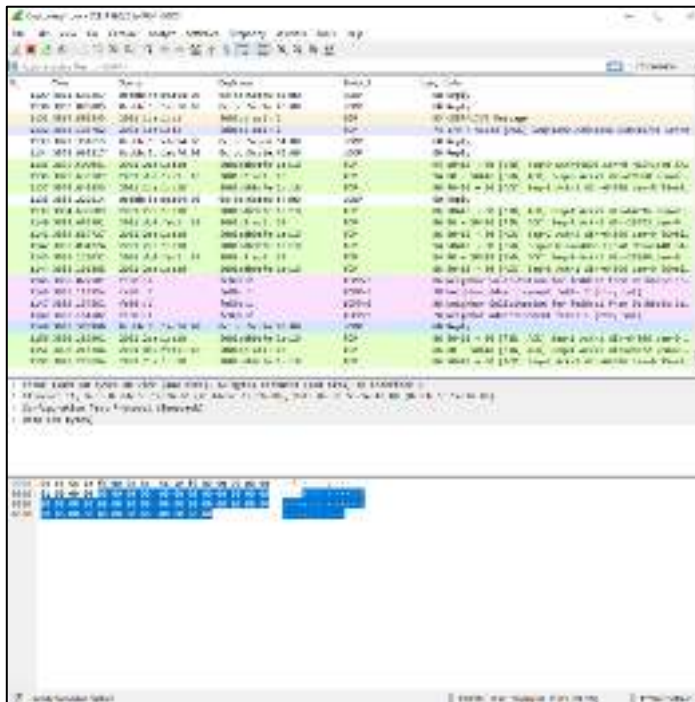


Figura 28-1: Captura de tráfico con Wireshark.

Fuente: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html

1.7 Parámetros para evaluar el rendimiento de una red

1.7.1 Ancho de banda

Según Filippis, (2012) el ancho de banda es la cantidad de información que puede transmitir de una sola vez, en un paquete desde el punto de origen hacia el destino y se mide en Kbps, Mbps y Gbps. Considerada como la medida de datos y recursos de comunicación que van a hacer disponibles o consumidas en una red establecida, expresados en Bits o múltiplos de ella. En que la velocidad de transmisión máxima que esta transmite la información depende de la misma. (Usca, 2018 pág. 37)

Es por ello que se debe considerar esta variable ya que de esta depende que se pueda llevar la suficiente información como para sostener la transmisión de voz, datos y video de una manera eficiente y estable, para ello se debe considerar generalmente la sucesión de conexiones que están presentes en la red como también dando el suficiente ancho de banda para cada una de ellas ya que si una de estas conexiones es más lenta que las otras y se encontrara en el punto de mayor operación , actuara como un cuello de botella causando lentitud en la comunicación. (Usca, 2018 pág. 37)

1.7.2 Retardo o latencia

En (Filippis, 2012), se menciona que latencia “Es el tiempo que demora un paquete de datos en llegar desde el origen al destino. Esto está limitado por leyes físicas de los medios de transmisión (cables de fibra, cables de cobre, enlaces satelitales, etc.) y adicionalmente por los dispositivos intermedios de transmisión de datos (routers, switches, gateways y firewalls)”, por lo que se debe hacer referencia al ancho de banda y también a la latencia presente en la comunicación de la red y todo esto se logra gracias a la optimización de una correcta infraestructura con el uso de tecnología adecuada, de modo que estas redes de datos sean lo más veloces y eficientes posibles. (Usca, 2018 pág. 37)

La latencia o retardo entre el punto de inicio y fin de la comunicación se recomienda que debiera ser inferior a 150 ms. El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta. (Usca, 2018 pág. 37)

La tabla de los umbrales máximos de retardo según las recomendaciones UIT-T, G.1010, Y.1541 y la IEEE 802.1p

Tabla 4-1: Valoraciones de Retardo.

Tráfico	Excelente	Muy Bueno	No adecuado
Streaming	≤ 100 ms	> 100 ms y ≤ 250 ms	> 250 ms

Realizado por: Alex Y., 2020.

1.7.3 Variación de Retardo o Jitter

(APOGEE, 2014), comenta que “Es la desviación no deseada de una señal periódica del momento ideal” (p.1), que es asumida como periódica por lo que esta se convierte en un factor importante y no deseado en el interior del diseño y desempeño de las redes de comunicación. Por lo tanto, es la variación en un determinado tiempo de arribo al receptor de la información, el mismo parámetro se tiene en cuenta en el proyecto de investigación. (Usca, 2018 pág. 38)

(Brognara, 2016), menciona que el jitter entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado. (Usca, 2018 pág. 38)

La tabla de los umbrales máximos de Jitter según las recomendaciones UIT-T, G.1010, Y.1541 y la IEEE 802.1p

Tabla 5-1: Valoraciones de Jitter.

Tráfico	Excelente	Muy Bueno	No adecuado
Streaming	≤ 35 ms	> 35 ms y ≤ 65 ms	> 65 ms

Realizado por: Alex Y., 2020.

1.7.4. Pérdida de Paquetes o Losst Rate

Se refiere al descarte de información o paquetes en la red debido a las fallas de los dispositivos de red, exceso de tráfico, mala administración de los nodos, la pérdida de paquetes también depende del protocolo de capa de transporte que se esté utilizando los cuales pueden ser TCP o UDP, donde TCP asegura que los paquetes lleguen a su destino sin importar el tiempo de transmisión, este protocolo es más utilizado para la transferencia de datos; en cambio el protocolo UDP asegura que los datos lleguen en un buen tiempo pero no toma en cuenta si los paquetes llegan completos, este tipo de protocolo es empleado para el servicio de Streaming y mide en %". (Pincay, y otros, 2015)

1.7.5 Rendimiento o Troughput

“El Troughput técnicamente es la capacidad de información que un elemento de red puede mover en un periodo de tiempo, es la velocidad real de transporte de datos a través de una red, se mide en bps”. (AGUIRRE ROJAS, 2017 pág. 40)

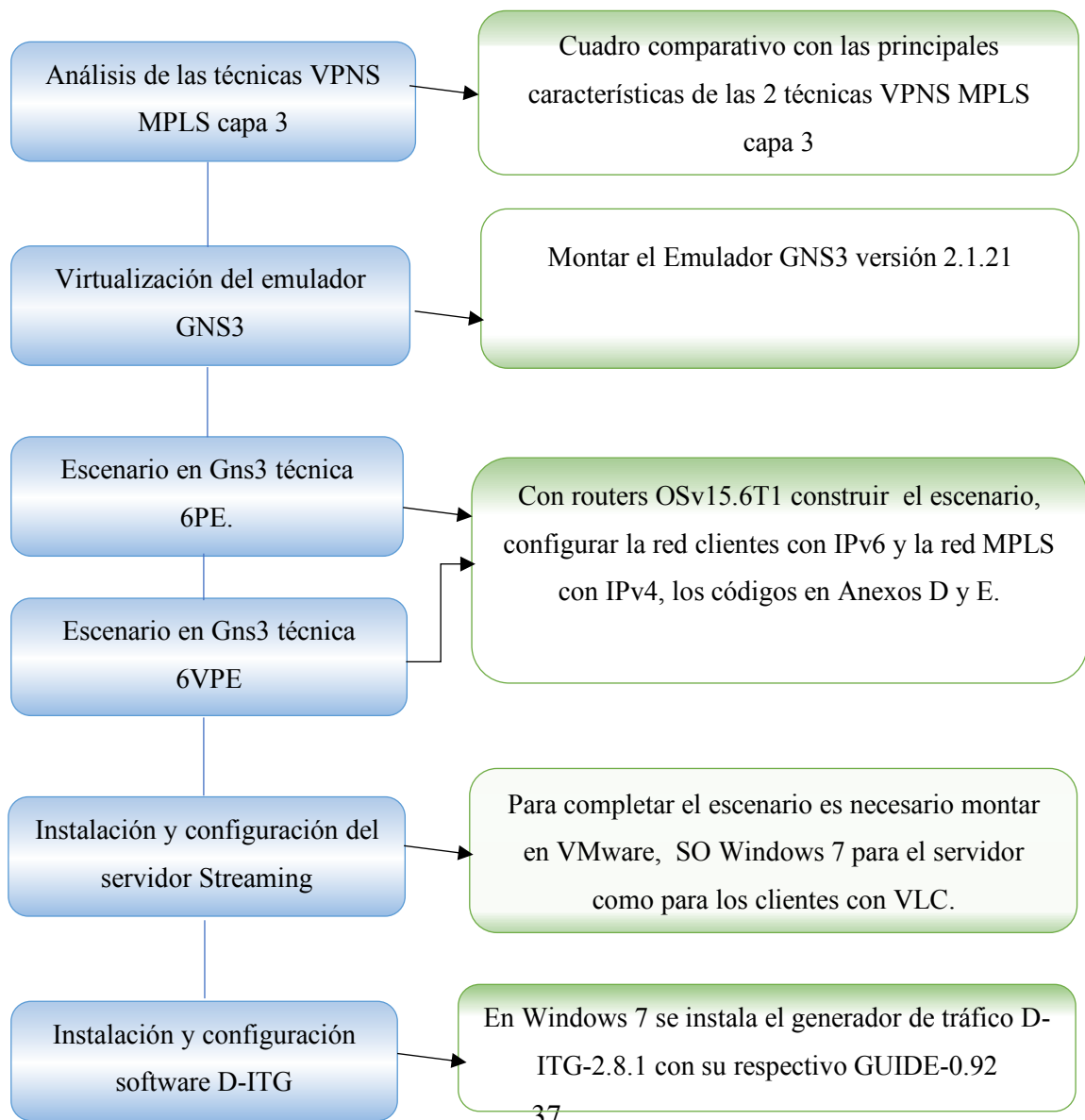
CAPITULO II

2. MARCO METODOLÓGICO

En este capítulo se detalla todos los procesos realizados para la Evaluación del rendimiento de las técnicas de VPNS MPLS capa 3 para streaming de audio y video con ipv4 e ipv6, se tuvo en consideración muchos aspectos, las mejores técnicas VPN MPLS , el software de emulación y equipo tecnológico adecuado para obtener un funcionamiento eficaz.

2.1 Diagrama de Bloques de la Metodología

A continuación se plantea un diagrama de bloques, en el cual se describe la metodología usada para desarrollar la Evaluación del rendimiento de las técnicas de VPNS MPLS capa 3 para streaming de audio y video con ipv4 e ipv6.



2.2 Análisis de las técnicas VPNS MPLS capa 3

Partiendo desde el punto de vista técnico se ha podido observar las principales características de las técnicas VPNS MPLS capa 3 y su función específica, lo cual nos lleva a realizar un análisis y ver la técnica con mejores características.

Tabla 1-2: Cuadro comparativo con características de las técnicas 6PE y 6VPE.

Técnicas	Características principales
6PE	<ul style="list-style-type: none"> • Estandarizado en RFC 4798. • Transporta el flujo IPv6 en una red MPLS basada en IPv4 • Los prefijos IPv6 se anuncian mediante BGP interna (i-BGP). • Los routers de borde del proveedor PE deben soportar IPv4 e IPv6 (Dual Stack) • Los ASBR del proveedor soportan Inter-AS Opción A, B, C o AB • Interacciones de enrutamiento en 6PE es: red de clientes IPv6 Enrutamiento: IGPv6 (IS-IS, OSPF), estático, PE-CE es IPv6 Enrutamiento eBGP, IGPv6 (IS-IS, OSPF), estático y PE-PE MPLS Enrutamiento: MP-BGP, IGP Distribución de etiquetas: MP-BGP (V6), LDP (V4) • En 6PE solamente se mantiene una tabla de enrutamiento.
6VPE	<ul style="list-style-type: none"> • Estandarizado en RFC 4659. • La comunicación se logra utilizando LSP (Label Switch Path) a través del núcleo MPLS. • Utilizan MP-BGP (Multiprotocol BGP) sobre IPv4 para intercambiar rutas IPv6. • Los routers PE deben ser doble pila. • Los routers del núcleo MPLS transporta paquetes IPv6, dado que solo consideran los encabezados MPLS. • En los Routers PE se crea VPNS y Obviamente las VRF. • Los ASBR del proveedor soportan Inter-AS Opción A, B, C o AB con VPNv6 o VPNv4 • La técnica 6VPE tiene los Atributos que son :Route Distinguisher (RD), Route Target (RT) full Mesh o Hub and Spoke y VPN Label o Etiqueta de VPN • 6VPE maneja diferentes tablas de enrutamiento independientes, separadas lógicamente. • Ampliamente utilizadas por los principales ISPs ya que brinda mayor seguridad de la información. •

Realizado por: Alex Y.,2020.

2.3 Virtualización del emulador GNS3

La virtualización permite realizar pruebas software y hardware antes de implementar un programa, un sistema operativo o alguna aplicación que influya directamente en la actividad diaria de una empresa obteniendo resultados que pueden ser satisfactorios o también adversos que afecta a toda la infraestructura.

Para iniciar con la virtualización de Del Emulador se ha tomado en consideración una máquina física con características avanzadas, procesador Core i7-770HQ de 2.80Ghz, memoria RAM de 16 GB para tener ningún problema al realizar la emulación en GNS3 virtualizado, cabe señalar que se simula el servidor de streaming VLC en Windows 7 y los clientes trabajan con Windows 7 y Ubuntu .

2.3.2 Montar el Emulador GNS3 versión 2.1.21

Gns3 es un Emulador que ofrece una manera fácil de diseñar y construir redes de cualquier tamaño y es gratuito, se realiza la descarga desde la página oficial disponible en www.gns3.com/software/download una vez descargado se realiza la instalación de GNS3 versión 2.1.21 para Windows, se puede observar en el apartado del **ANEXO A**.

Una vez instalado VMware y GNS3 se debe virtualizar con el siguientes proceso, abrir VMware e importar todo el emulador GNS3 virtualizado en Ubuntu con sus respectivos IOS, Dynamips, Qemu, asignar recursos a la nueva máquina virtual como cantidad de memoria RAM para este proyecto se asignó 10 GB, el tamaño del disco duro, adaptadores de red etc. Ver el **ANEXO B**.

2.4 Escenario en Gns3 técnica 6PE

Para cumplir con el objetivo propuesto, se trabaja con la técnica 6PE el cual permiten ejecutar IPv6 sobre una red MPLS solo IPv4 donde utiliza enrutadores PE de doble pila, los enrutadores PE, ejecutan MP-BGP para intercambiar prefijos IPv6 y el LSP (Label Switched Path) basada en IPv4 por ende permite a los proveedores de servicios ofrecer IPv6 a sus clientes sin realizar cambios importantes en el núcleo de su red MPLS, 6PE utiliza la tabla de enrutamiento global IPv6 en los enrutadores PE.

2.4.1 Descripción del escenario de la técnica 6PE

Una vez analizada y estudiada de forma técnica, se plantea el escenario de la **Figura 1-2**, para realizar las pruebas correspondientes de streaming de audio y video para posteriormente realizar la evaluación del rendimiento con DITG de la técnica 6PE con ipv4 e ipv6”

Máquina virtual de Gns3 está listo para trabajar, se debe empezar configurando e instalando los IOS de router, para el proyecto propuesto se utiliza routers Cisco OSv15.6T1.

Mediante la **Figura 1-2** y la **Tabla 2-2** se realiza una breve descripción, Los clientes utilizan direccionamiento IPv6, el router CE1 – PE1 utiliza para intercambio de paquetes BGP(MP-BGP), PE1 es doble pila para el soporte de la técnica de Transmisión y coexistencia IPv6-IPv4 6PE donde la este utiliza únicamente la tabla de enrutamiento para el intercambio de paquete con red Mpls, dentro de la nube Mpls P1-P2 los router intercambian etiquetas, entre los router ASBR PE2-PE3 se utiliza MP-BGP INTER AS Opción B para el intercambio de paquetes entre el sistema autónomo 400 y 500, se realiza el mismo proceso anterior hasta llegar al servidor.

Tabla 2-2: Descripción general del escenario 6PE

Clientes PCs-CE1	CE1-PE1	PE1-PE2	P1-P2	ASBR PE2-PE3	Servidor CE4-Servidor
Ipv6 Nativo	-Ipv6 Native -Link local -MP-BGP	.-Reenvío: MPLS IPv6+etiqueta -Enrutamiento: MP- BGP, OSPF 10 área 0 -Distribución de etiquetas: MP-BGP (V6), LDP (V4) -IPV4	-IPv4 -OSPF 10 área 0 -Etiqueta forwarding (LSP)	-IPv6 MP-BGP INTER AS Opción B	Ipv6 Nativo

Realizado por: Alex Y.,2020.

En el escenario de la **Figura 1-2** y **Figura 2-2** se trabaja con las dispositivos de router y maquinas virtualizadas en VMware con se especifica en la siguiente **Tabla 3.2**.

Tabla 3-2: Especificaciones de dispositivos utilizados en los escenario para 6PE y 6VPE.

Router	Maquinas Clientes 1 y 2	Maquina Cliente 3
21 Routers Cisco IOSv15.6(2)T-1 Memoria RAM 512 MB Utilización de memoria RAM 10752 MB	Máquina virtual (VMware) SO. Windows 7 Professional X64 RAM 1 GB Disco duro 30 GB	Appliance Ubuntu Guest 19.04 Nombre de usuario: osboxes Contraseña: osboxes.org RAM 1 GB

Realizado por: Alex Y.,2020.

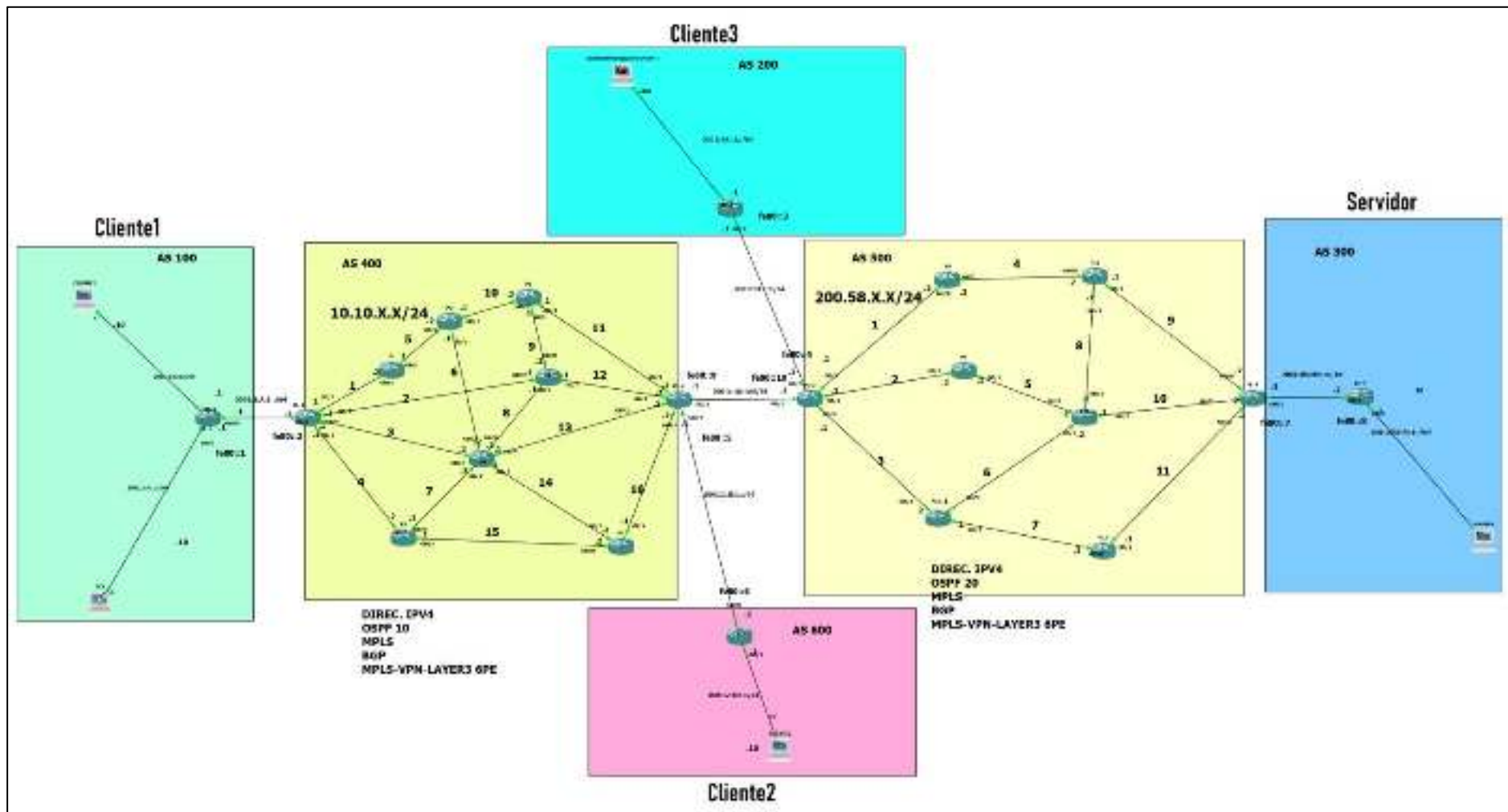


Figura 1-2: Escenario técnica 6PE.
 Realizado por: Yautibug, A. 2020.

Clientes: las configuraciones se basan en las direcciones y parámetros expuestas a continuación en la **tabla 4-2**.

Tabla 4-2: Direccionamiento de los clientes.

	Equipo	Interfaz	Dirección IP	Link Local	AS	PC
Cliente1	CE1	G0/0 G0/2 G0/1	2001:1:A:1::1/64 2001:2:A:1::1/64 2001:3:A:1::1/64	fe80::1	100	Máquina virtual (VMware) SO. Windows 7 Professional X64 RAM 1 GB Disco duro 30 GB Dirección IP 2001:2:a:1::10/64
Cliente2	CE2	G0/0 G0/1	2001:1:B:1::2/64 2001:2:B:1::1/64	fe80::6	600	Máquina virtual (VMware) SO. Windows 7 Professional X64 RAM 1 GB Disco duro 30 GB Dirección IP 2001:2:a:1::10/64
Cliente3	CE3	G0/0 G0/1	2001:1:C:1::1/64 2001:2:C:1::1/64	fe80::3	200	Appliance Ubuntu Guest 19.04 Nombre de usuario: osboxes Contraseña: osboxes.org RAM 1 GB Dirección IP 2001:2:a:1::10/64

Realizado por: Alex y.,2020.

Red Mpls e Inter-AS MPLS L3VPN

Tabla 5-2: Direccionamiento en Red Mpls e Inter-AS MPLS L3VPN

Equipo	Interfaz	Dirección IP	Link Local	SA	OSPF	Área	Etiqueta MPLS
PE1	G0/0 G0/1 G 0/2 G 0/3 G 0/4 lo0	2001:1:A:1::2/64 10.10.1.1/24 10.10.4.1/24 10.10.2.1/24 10.10.3.1/24 17.17.17.17/30	fe80::2 - - - - -	400	- 10 10 10 10 10	- 0 0 0 0 0	Range 1700 1780
P1	G0/0 G0/1 Lo0	10.10.1.2/24 10.10.5.1/24 1.1.1.1 /30	- - -	- - -	10 10 10	0 0 0	Range 100 180
P2	G0/0 G0/1 G0/2 Lo0	10.10.5.2/24 10.10.10.1/24 10.10.6.1/24 2.2.2.2/30	- - - -	-	10 10 10 10	0 0 0 0	Range 200 280
P3	G0/0 G0/1 G0/2 Lo0	10.10.7.1/24 10.10.4.2/24 10.10.15.1/24 3.3.3.3/30	- - - -	-	10 10 10 10	0 0 0 0	Range 300 380
P4	G0/0 G0/1 G0/2 G0/3 G0/4 G0/5 Lo0	10.10.8.2/24 10.10.7.2/24 10.10.3.2/24 10.10.3.2/24 10.10.13.1/24 10.10.14.1/24 4.4.4.4/30	- - - - - - -	-	10 10 10 10 10 10 10	0 0 0 0 0 0 0	Range 400 480
P5	G0/0 G0/1 G0/2 Lo0	10.10.10.2/24 10.10.9.1/24 10.10.11.1/24 5.5.5.5/30	- - - -	-	10 10 10 10	0	Range 500 580
P6	G0/0 G0/1	10.10.9.2/24 10.10.8.1/24	- -	-	10 10	0	Range 600 680

	G0/2 G0/3 Lo0	10.10.2.2/24 10.10.12.1/24 6.6.6.6/30	- - -		10 10 10		
P7	G0/0 G0/1 G0/2 Lo0	10.10.15.2/24 10.10.14.2/24 10.10.16.1/24 7.7.7.7/30	- - - -	-	10	0	Range 700 780
PE2	G0/0 G0/1 G 0/2 G 0/3 G 0/4 G 0/5 lo0	10.10.11.2/24 10.10.12.2/24 10.10.13.2/24 10.10.16.2/24 2001:1:B:1::1/64 2001:1:D:1::1/64 18.18.18.18/30	- - - - fe80::5 fe80::9 -	400	10 10 10 10 - - 10	0 0 0 0 - - 0	Range 1800 1880
PE3	G0/0 G0/1 G 0/2 G 0/4 G 0/5 lo0	2001:1:D:1::2/64 200.58.1.1/24 200.58.2.1/24 200.58.3.1/24 2001:1:C:1::2/64 19.19.19.19/30	fe80::9 - - - fe80::4 -	500	- 20 20 20 - 20	- 0 0 0 - 0	Range 1900 1980
P8	G0/0 G0/1 lo0	200.58.1.2/24 200.58.4.1/24 8.8.8.8/30	- - -	-	20 20 20	0 0 0	Range 800 880
P9	G0/0 G0/1 lo0	200.58.2.2/24 200.58.5.1/24 9.9.9.9/30	- - -	-	20 20 20	0 0 0	Range 900 980
P10	G0/0 G0/1 G0/2 lo0	200.58.3.2/24 200.58.6.1/24 200.58.7.1/24 10.10.10.10/30	- - - -	-	20 20 20 20	0 0 0 0	Range 1000 1080
P11	G0/0 G0/1 G0/2 lo0	200.58.4.2/24 200.58.9.1/24 200.58.8.1/24 11.11.11.11/30	- - - -	-	20 20 20 20	0 0 0 0	Range 1100 1180
P12	G0/0 G0/1 G0/2 G0/3 lo0	200.58.5.2/24 200.58.10.1/24 200.58.6.2/24 200.58.8.2/24 12.12.12.12/30	- - - - -	-	20 20 20 20 20	0 0 0 0 0	Range 1200 1280
P13	G0/0 G0/1 lo0	200.58.7.2/24 200.58.11.1/24 13.13.13.13/30	- - -	-	20 20 20	0 0 0	Range 1300 1380
PE4	G0/0 G0/1 G 0/2 G 0/3 lo0	200.58.9.2/24 200.58.10.2/24 200.58.11.2/24 2001:db6:fe:1::1/64 12.12.12.12/30	- - - fe80::2 -	500	- 20 20 20 20	- 0 0 0 0	Range 1700 1780

Realizado por: Alex y.,2020.

Servidor

Tabla 6-2: Direccionamiento del servidor.

	Equipo	Interfaz	Dirección IP	Link Local	SA	PC
SERVIDOR	CE4	G0/0 G0/1	2001:db6:fe:1::2/64 2001:db7:fe:1::1/64	fe80::8	300	Máquina virtual (VMware) SO. Windows 7 Professional X64 RAM 1 GB Disco duro 30 GB Dirección 2001:db7:fe:1::10/64 IP

Realizado por: Alex y.,2020.

Para ver la configuración de la técnica 6PE ver el **ANEXO C**.

2.5 Escenario en Gns3 técnica 6VPE.

IPv6 sobre MPLS/VPN en los equipos de borde (6VPE) la principal característica soporta redes VPN e instancias de enrutamiento VRF conmutando tráfico IPv6 correspondiente a VPN/VRF en los routers de borde y encapsulando los paquetes con MPLS de Core IPv4 así permitiendo entregar tráfico IPv6 nativo al CE.

2.5.1 Descripción del escenario de la técnica 6VPE

Esta técnica proporciona un servicio dedicado al cliente mediante la creación de VPN y la tabla de VRF para enrutamiento en los router de borde Provider Edge (PE) haciendo un breve descripción de la **Figura 2-2**, es: clientes utilizan direccionamiento IPv6, el router CE1 – PE1 utiliza para intercambio de paquetes BGP(MP-BGP), en PE1 se crea las VPNs y la tabla de enrutamiento VRF para el intercambio de paquete, dentro de la nube Mpls P1-P2 los router intercambian etiquetas, entre los routers ASBR PE2-PE3 se utiliza VPNv6 y MP-BGP INTER AS Opción B para el intercambio de paquetes entre el sistema autónomo 400 y 500, se realiza el mismo proceso anterior entre P8-P9, en PE4 – CE4 se realiza el método de Hub and Spoke, en el servidor se comunica con IPv6 nativo.

Tabla 7-2: Descripción general del escenario 6VPE

Cientes PCs-CE1	CE1-PE1	PE1-PE4	P1-P2	ASBR PE2-PE3	PE4-CE4	Servidor CE4-Servidor
Ipv6 Nativo	-Ipv6 Native -Link local -MP-BGP	-Crea VPN y VRF -Reenvío: MPLS IPv6+etiqueta -Enrutamiento: MP-BGP, OSPF 10 área 0 -Distribución de etiquetas: MP-BGP (V6), LDP (V4) -IPV4	-IPv4 -OSPF 10 área 0 -Etiqueta forwarding (LSP)	-IPv6 --MP-BGP INTER AS Opción B con VPNv6	- Crea VPN y VRF -Método HUB and Spoke -Ipv6 Native -Link local -MP-BGP	Ipv6 Nativo

Realizado por: Alex y.,2020.

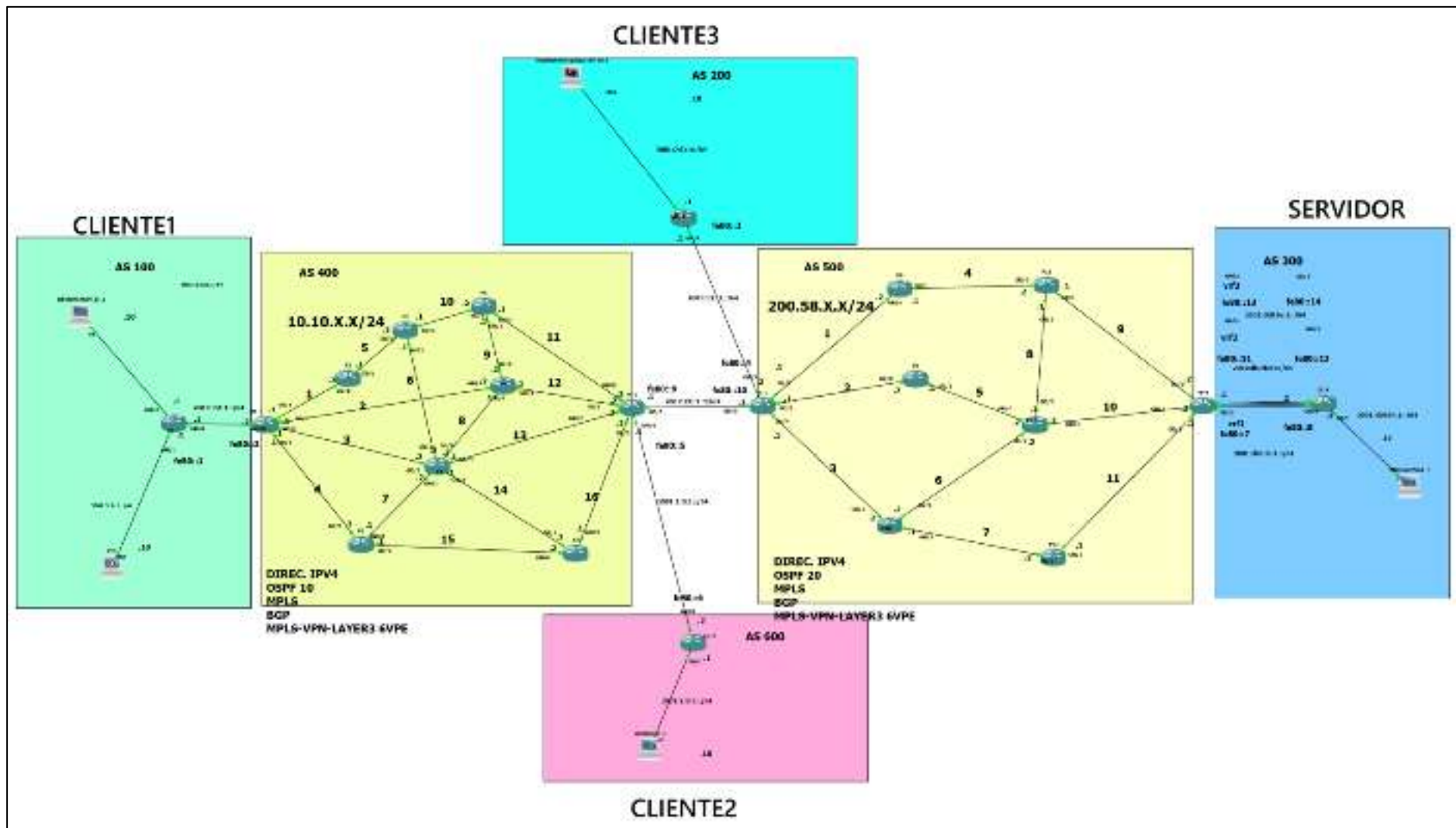


Figura 2-2: Escenario técnica 6VPE.
 Realizado por: Yautibug, A. 2020.

El direccionamiento y enrutamiento observar en la **Tabla 4-2**, **Tabla 5-2** y **Tabla 6-2**, 6VPE a diferencia de la técnica 6PE visto anteriormente radica en la creación de VPNs/VRFs en los router de borde PE como se muestra a continuación en el **Figura 3-2**, la interconexión de diferentes proveedores en los routers de borde llamados ASBRS *PE2-PE3* donde se crea una VPNv6 dentro de la protocolo MP-BGP para el intercambio de paquetes ver en el **Figura 4-2**, y en PE4 se configura el método de Hub and Spoke con atributos de RT route-target both para la comunicación con el servidor mirar el **Figura 5-2**.

```

hostname PE-1
!
boot-start-marker
boot-end-marker
!
vrf definition Cliente1
 rd 1:1
!
 address-family ipv6
  route-target export 1:1
  route-target import 1:1
  exit-address-family
!
interface GigabitEthernet0/0
 vrf forwarding Cliente1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address FE80::2 link-local
 ipv6 address 2001::A::1::2/64
 ipA fa
 no cdp enable
!
router bgp 400
 bgp router-id 17.17.17.17
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 18.18.18.18 remote-as 400
 neighbor 18.18.18.18 update-source loopback0
!
 address-family vpnv6
  neighbor 18.18.18.18 activate
  neighbor 18.18.18.18 send-community extended
  exit-address-family
!
 address-family ipv6 vrf Cliente1
  redistribute connected
  neighbor 2001::A::1::1 remote-as 101
  neighbor 2001::A::1::1 activate
  exit-address-family
!

hostname PE-2
!
boot-start-marker
boot-end-marker
!
vrf definition Cliente2
 rd 2:2
!
 address-family ipv6
  route-target export 2:2
  route-target import 2:2
  exit-address-family
!
interface GigabitEthernet0/0
 vrf forwarding Cliente2
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address FE80::3 link-local
 ipv6 address FE80::3 link-local
 ipv6 address 2001::B::1::3/64
 ipA fa
 no cdp enable
!

hostname PE-3
!
boot-start-marker
boot-end-marker
!
vrf definition Cliente3
 rd 3:3
!
 address-family ipv6
  route-target export 3:3
  route-target import 3:3
  exit-address-family
!
interface GigabitEthernet0/0
 vrf forwarding Cliente3
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address FE80::4 link-local
 ipv6 address 2001::C::1::3/64
 ipA fa
 no cdp enable
!

vrf definition Cliente4
 rd 1:1
!
 address-family ipv6
  route-target export 1:1
  route-target import 1:1
  exit-address-family
!
vrf definition Cliente5
 rd 2:2
!
 address-family ipv6
  route-target export 2:2
  route-target import 2:2
  exit-address-family
!
vrf definition Cliente6
 rd 3:3
!
 address-family ipv6
  route-target export 3:3
  route-target import 3:3
  exit-address-family
!
interface GigabitEthernet0/0
 vrf forwarding Cliente4
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address FE80::5 link-local
 ipv6 address 2001::D::1::4/64
 ipA fa
 no cdp enable
!
interface GigabitEthernet0/1
 vrf forwarding Cliente5
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address FE80::11 link-local
 ipv6 address 2001::D::1::4/64
 ipA fa
 no cdp enable
!
interface GigabitEthernet0/5
 vrf forwarding Cliente6
 no ip address
 duplex auto
 speed auto
 media-type rj45
 ipv6 address FE80::22 link-local
 ipv6 address 2001::D::1::4/64
 ipA fa
 no cdp enable
!

```

Figura 3-2: Creación de VPNs/VRFs en los router de borde PE.
Realizado por: Yautibug, A. 2020.

2.6 Instalación del servidor Streaming VLC.

En la Figura 1-2: Escenario técnica 6PE y Figura 2-2: Escenario técnica 6VPE los clientes y el servidor se debe virtualizar con VLC para realizar el streaming de Audio y video para lo cual es necesario montar en VMware, los sistemas operativos Windows 7 para el servidor como los clientes.

2.6.1 Virtualización streaming de audio/ video con el reproductor VLC media player

VLC media player es un reproductor multiplataforma gratuito y de código abierto que reproduce la mayoría de archivos multimedia, este software permite hacer streaming y a los usuarios a acceder en tiempo real a películas, documentales o música, ahorrando tanto espacio en disco y tiempo, para el presente trabajo se instala *VLC 3.0.8 para Windows 64 bits* en las máquinas virtualizadas anteriormente con Windows 7 con en Appliance Ubuntu. Para Windows 7 se puede descargar desde la página oficial de VLC <https://www.videolan.org/vlc/index.es.html> una vez terminado la descarga, hacer la instalación.



Figura 6-2: Interface de VLC 3.0.8 en Windows 7

Realizado por: Yautibug, A. 2020.

Para Appliance Ubuntu la instalación es diferente se debe realizar por línea de comando se puede guiar en el link web <https://linuxconfig.org/how-to-install-java-on-ubuntu-19-10-eoan-ermine-linux>. Ver ANEXO E el proceso de instalación.



Figura 7-2: Interface de VLC 3.0.8 en Ubuntu

Realizado por: Yautibug, A. 2020.

2.6.2 Configuración del servidor streaming VLC.

1. Abrir VLC, escoger la opción *Medio* y luego *Emitir*

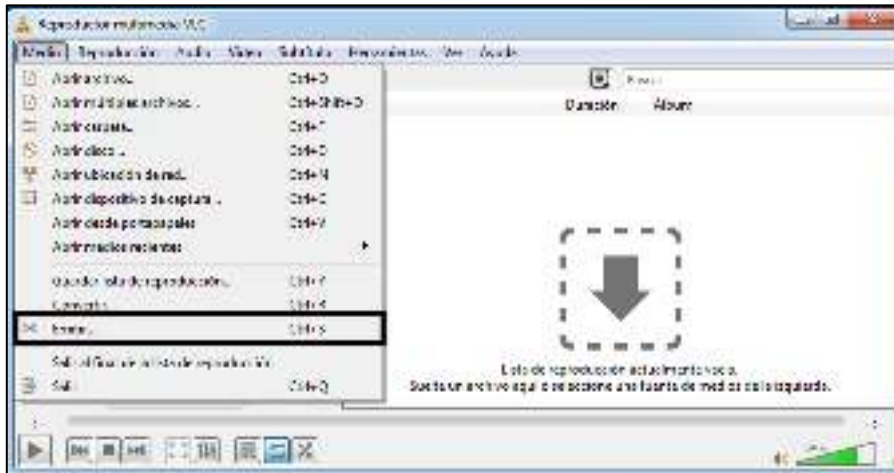


Figura 8-2: Ventana de VLC con la opción emitir.

Realizado por: Yautibug, A. 2020.

2. Luego *Añadir* el archivo a transmitir y continuar haciendo click en *Emitir*

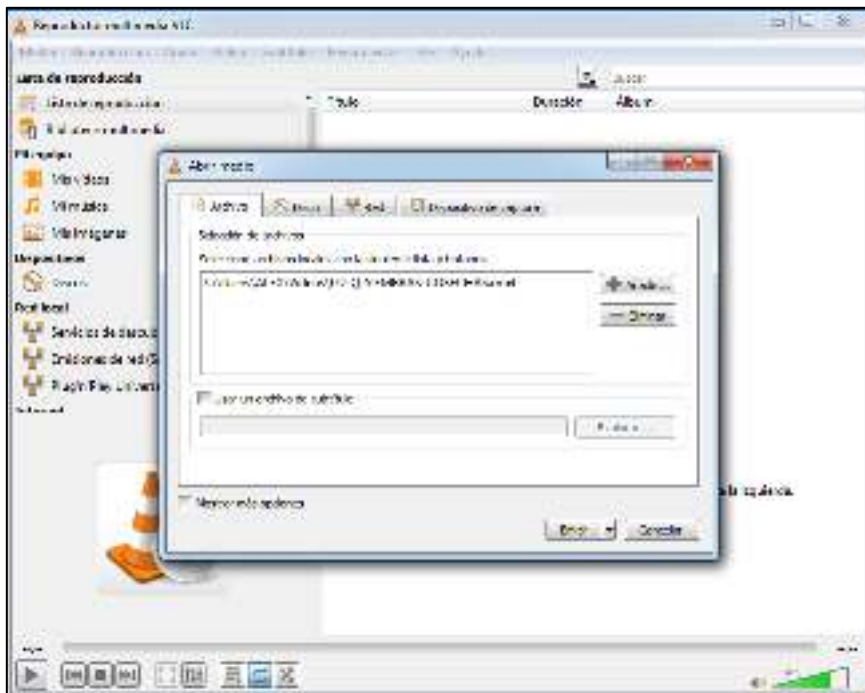


Figura 9-2: Ventana de VLC opción añadir archivo de emisión .

Realizado por: Yautibug, A. 2020.

3. En la siguiente ventana escoger la opción *Mostrar en local* para ver el video que se está transmitiendo, también escoger el *protocolo* a transmitir donde se encuentra los protocolos más utilizados para la transmisión multimedia como son: HTTP , RTP, RTSP, Icecast y UDP para este proyecto se trabaja con el protocolo HTTP, luego en la opción añadir se debe configurar el puerto y ruta para este caso el puerto 8080 y la ruta /leonel

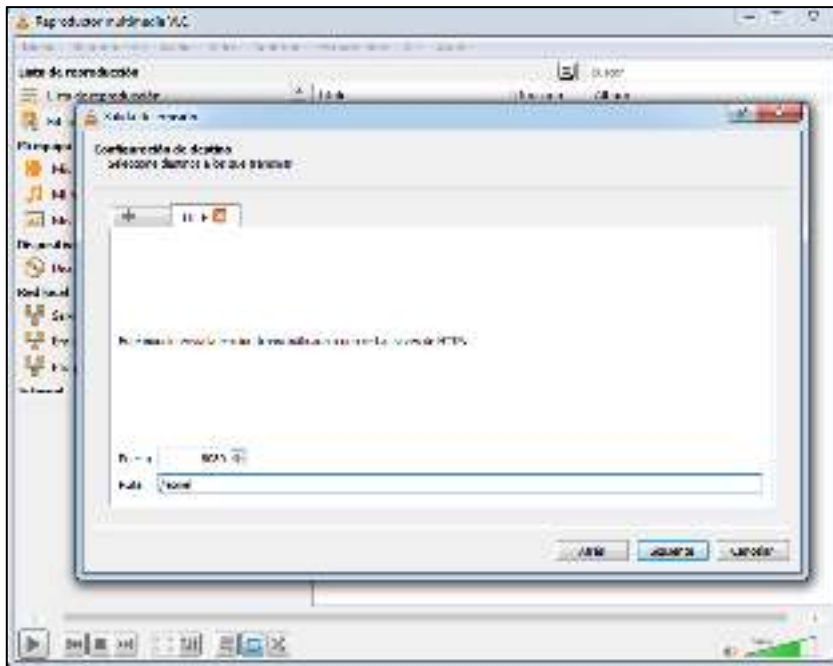


Figura 10-2: Ventana de VLC configuración de protocolo, puerto y ruta .
Realizado por: Yautibug, A. 2020.

4. Para terminar, en la ventana de *configuración de preferencias* se debe modificar un parámetro muy importante el tiempo de vida de los paquetes a enviar ya que se va a transmitir a otra red LANs para este caso se configuró $ttl=20$ luego hacer click en *Emitir* y empezara la transmisión el servidor VLC.

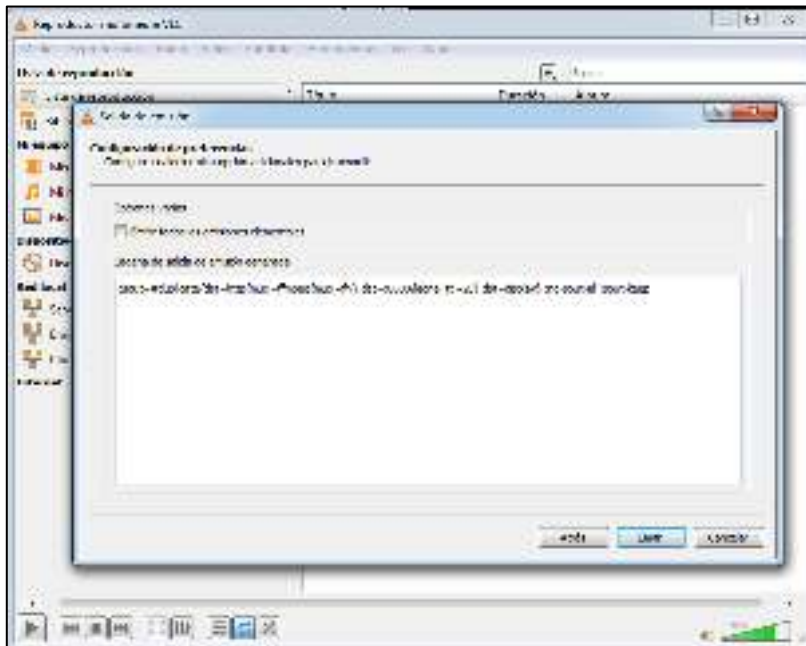


Figura 11-2: Ventana de VLC configuración del parámetro ttl.
Realizado por: Yautibug, A. 2020.

5. Como se escogió anteriormente la opción *Mostrar en local* entonces se visualiza el video que se está transmitiendo.



Figura 12-2: Funcionamiento Streaming.
Realizado por: Yautibug, A. 2020.

2.6.3 Configuración del receptor streaming VLC media Player

El cliente con sistema operativo (Windows y Ubuntu) ya tiene instalado en su equipo virtualizado el reproductor VLC, ahora se configura el receptor.

Abrir el reproductor VLC en el receptor, una vez que está ejecutando escoger la opción *medio* y luego se da clic *abrir ubicación de red* y se desplegara la ventana de configuración de los parámetro a conectarse con servidor streaming como son: el protocolo, dirección IPv6 del servidor, el puerto por el que está trasmitiendo el servidor y la ruta, para este trabajo es `http://[200:1:db7:fe:1::10]:8080/leonel`

2.7 Instalación software D-ITG

2.7.1 Instalación de D-ITG para Windows 7

La descarga se realiza desde la página web oficial Distributed Internet Traffic Generator(D-ITG) <http://www.grid.unina.it/software/ITG/download.php> una vez descargados los programas *D-ITG-2.8.1-r1023-src.zip* y la interfaz Gráfica de la página de Graphical User Interface

(<http://www.semken.com/projekte/index.html>) D-ITG GUI 0.92 beta, se procede a instalar tanto el inyector de tráfico como la interfaz gráfica.

Descomprimir los archivos y guardar en una carpeta root, es decir en una nueva carpeta en el disco los 2 archivos el DITG y la GUIDE .



Figura 13-2: Archivos descomprimidos DITG y la GUIDE en Windows 7
Realizado por: Yautibug, A. 2020.

Instalar Java de 64 bits para Windows desde <https://www.java.com/es/download/>. Una vez instalado java se debe ir a la carpeta de ITGGUI al archivo (.jar) abrir con java y comenzara a correr DITG GUIDE en Windows 7.

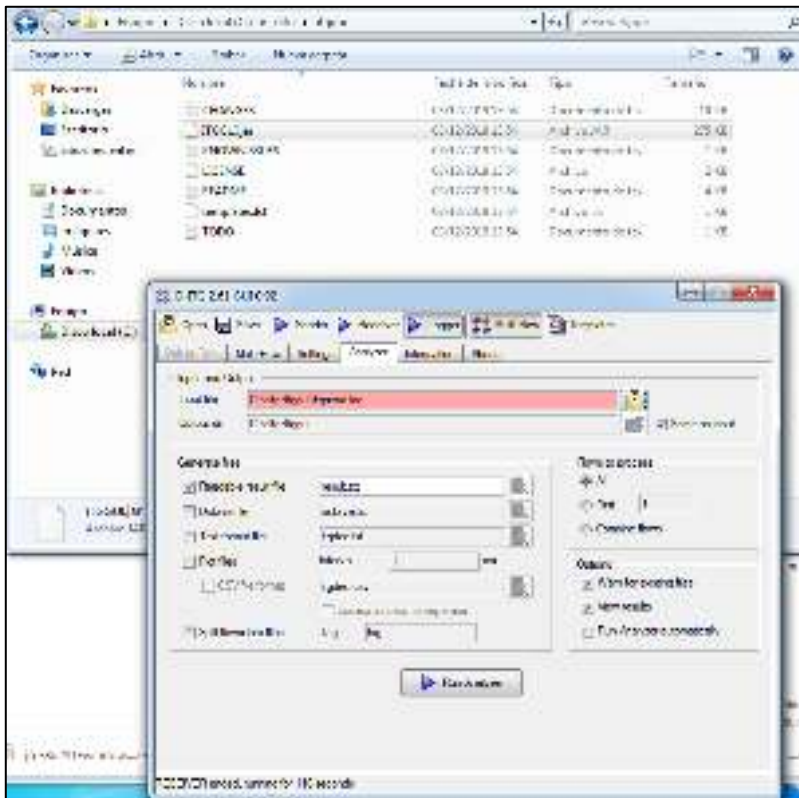


Figura 14-2: Ejecución de GUIDE del Programa D-ITG con JAVA.
Realizado por: Yautibug, A. 2020.

Por último, configurar DITG en la opción *settings*, y en *Binary Directory* redirigir a la carpeta que esta el programa general D-ITG en este caso la carpeta *C:/ditg/ D-ITG-2.8.1-r1023-win* y *Logging Directory* en donde está la carpeta *C:/ditg/ D-ITG-2.8.1-r1023-win/logs* donde se almacenara los datos para graficar con la opción *Analyzer*.



Figura 15-2: Interfaz del Programa D-ITG en Windows 7.
Realizado por: Yautibug, A. 2020.

2.7.2 Instalación D-ITG y GUIDE en Ubuntu

El primer paso consiste en descargar el inyector y la interfaz gráfica de usuario para DITG, Inyector D-ITG: <http://www.grid.unina.it/software/ITG/download.php> y la Interfaz gráfica en : <http://www.semken.com/projekte/index.html> es necesario también descargar los programas de apoyo para la respectiva instalación y funcionamiento adecuado del inyector de tráfico, como son Sun-java6-jre, g++ y octave.

Pasos para instalar los programas de apoyo se debe ejecutar los siguientes comando en la terminal de Ubuntu, la maquina debe tener conexión a internet.

- Sudo apt-get install g++
- Sudo apt-get update
- Sudo apt-get install octave



Figura 16-2: Terminal de Ubuntu con la instalación de los programas de apoyo.
Realizado por: Yautibug, A. 2020.

Una vez descargado el programa para descomprimir crear una carpeta root y descomprimir los 2 archivos *D-ITG-2.8.1-r1023-win* y *D-ITG GUI 0.92* para la posterior instalación ejecutando los comandos.

- cd root
- ls
- cd D-ITG-2.8.1-r1023-src.
- Ls
- cd D-ITG-2.8.1-r1023
- cd src
- ls
- make

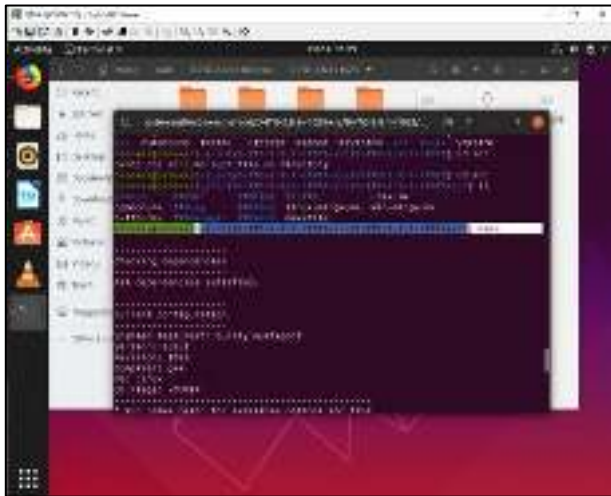


Figura 17-2: Interfaz con la instalación de D-ITG.
Realizado por: Yautibug, A. 2020.

Para ejecutar la interfaz gráfica para el usuario ejecutar los siguientes comandos.

- *Cd root*
- *Ls*
- *Cd itggui-092*
- *Ls*
- *Java -jar ITGGUI.jar*



Figura 18-2: Ejecución de la GUIDE del programa D-ITG en Ubuntu.
Realizado por: Yautibug, A. 2020.

Para culminar se configura en la opción *settings* en la opción *Binary Directory C:/root/ D-ITG-2.8.1-r1023-scr/bin* y *Logging Directory* para este es recomendable crear una carpeta logs para guardar los archivos para en un futuro realizar análisis, *C:/root/ D-ITG-2.8.1-r1023-scr/logs*.

2.7.3 Configuración de inyección de tráfico streaming con D-ITG en el emisor

Para la inyección de tráfico streaming con el programa D-ITG (Distributed Internet Traffic Generator) en el emisor o servidor se realiza las siguientes configuraciones primeramente se debe definir el flujo de datos como se puede observar en la **Figura 19-2**, con los parámetros resumidos en la **Tabla 7-2**, se envió en 3 tiempos con 30, 45, y 60, segundos

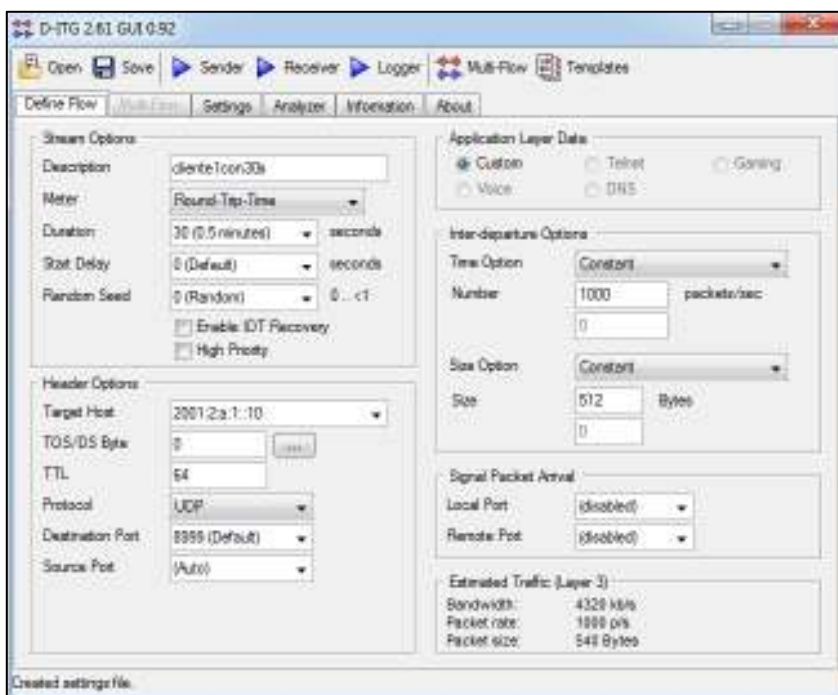


Figura 19-2: D-ITG definición del flujo en el servidor.
Realizado por: Yautibug, A. 2020.

Tabla 8-2: Parámetro para el flujo en emisor o servidor.

Parámetro	Valor
Direcciones de Destinos	2001:2:a:1::10 2001:2:b:1::10 2001:2:c:1::10
Tiempos de transmisión	30s, 45s y 60s
Meter	Round-Trip-time
TTL	64
Protocolo	UDP
Numero de paquete por segundo	1000 Paquetes/sec
Tamaño del paquete	512 Bytes

Realizado por: Yautibug, A. 2020.

La configuración del emisor se indica en la **Figura 20-2**, en la misma se especifica la *directorio binario* y del *log* en donde se encuentran los archivos, el fichero de registro a enviar se denomina *itgsend.log* y se renombra el archivo de salida que se alojará en el receptor.

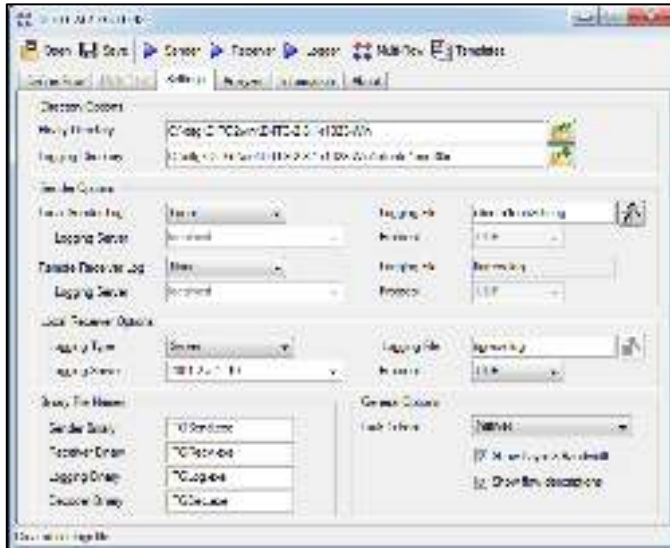


Figura 20-2: D-ITG, Configuración en settings del emisor .
Realizado por: Yautibug, A. 2020.

En la pestaña Analyzer, como se muestra en la **Figura 21-2**, se determina las direcciones del archivo de entrada y de salida, además se señalan los ficheros que se desean generar, en este caso se obtuvieron archivos .txt que resume los resultados del flujo de streaming enviado.



Figura 21-2: D-ITG, Configuración de Analyzer en emisor .
Realizado por: Yautibug, A. 2020.

2.7.4 Configuración de D-ITG en el receptor

La configuración en el receptor se asemeja a la del inyector en el emisor, con la única diferencia que el host objetivo es local, como se muestra en la **Figura 22-2**.

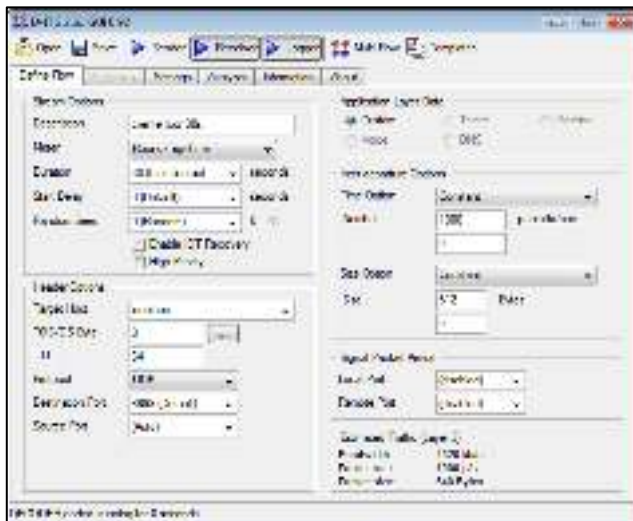


Figura 22-2: D-ITG, Configuración en el receptor .
Realizado por: Yautibug, A. 2020.

En la pestaña de Settings se definen las direcciones del archivo log y el archivo binario, además se configuran en *local receiver* configurar con la opción *local* y en *Logging file* configurar el nombre del archivo log, como la **Figura 23-2**, Una vez terminado la configuración en el emisor y el receptor, en el receptor se activa el botón *Logger y Receiver* para recibir, almacenar y capturar el tráfico y luego en el receptor activar el *Logger y Sender* para comenzar la inyección del tráfico.

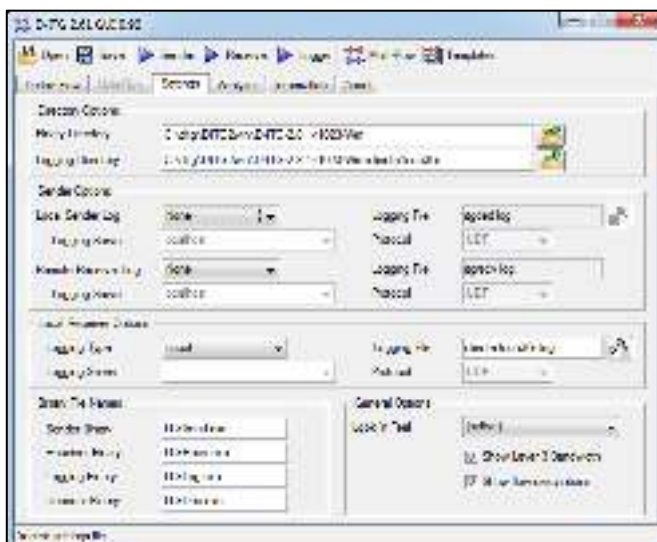


Figura 23-2: D-ITG, Configuración de settings en receptor o cliente1.
Realizado por: Yautibug, A. 2020.

En la pestaña Analyzer del receptor, se determina las direcciones del archivo de entrada y de salida, además se señalan los ficheros que se desean generar, en este caso se obtuvieron archivos

.txt de los resultados de recepción, y en Ubuntu los archivos .dat que posteriormente servirán para obtener las gráficas de delay, jitter, y packet loss con la herramienta ITGplot para graficar en Ubuntu Ver ANEXO F



Figura 24-2: Archivos generados en Ubuntu en la recepción D-ITG .
Realizado por:Yautibug, A. 2020.

Para observar los resultados de debe pilzar en boton analyzer

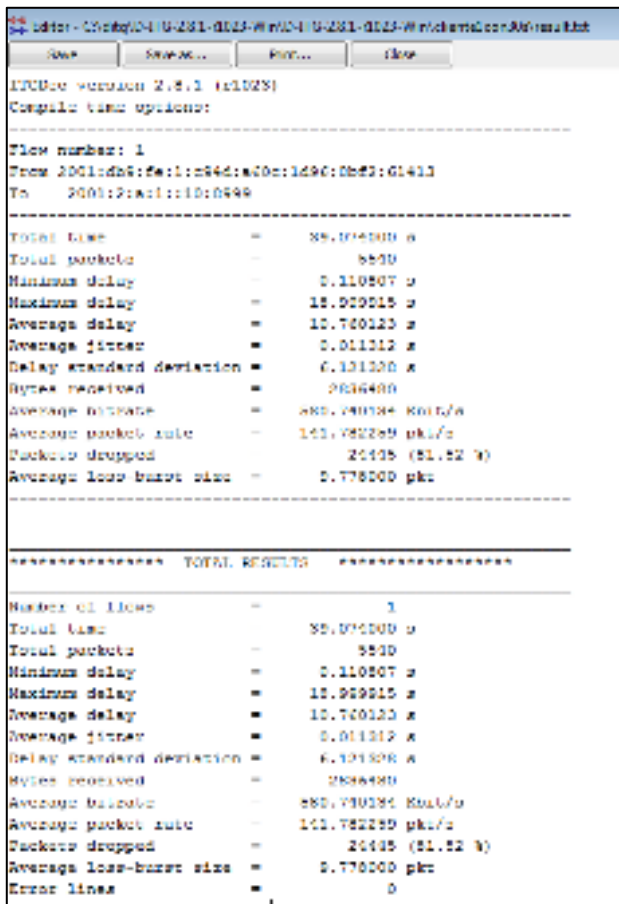


Figura 25-2: Resultado de tráfico en el receptor.
Realizado por:Yautibug, A. 2020.

CAPITULO III

3 MARCO DE RESULTADOS

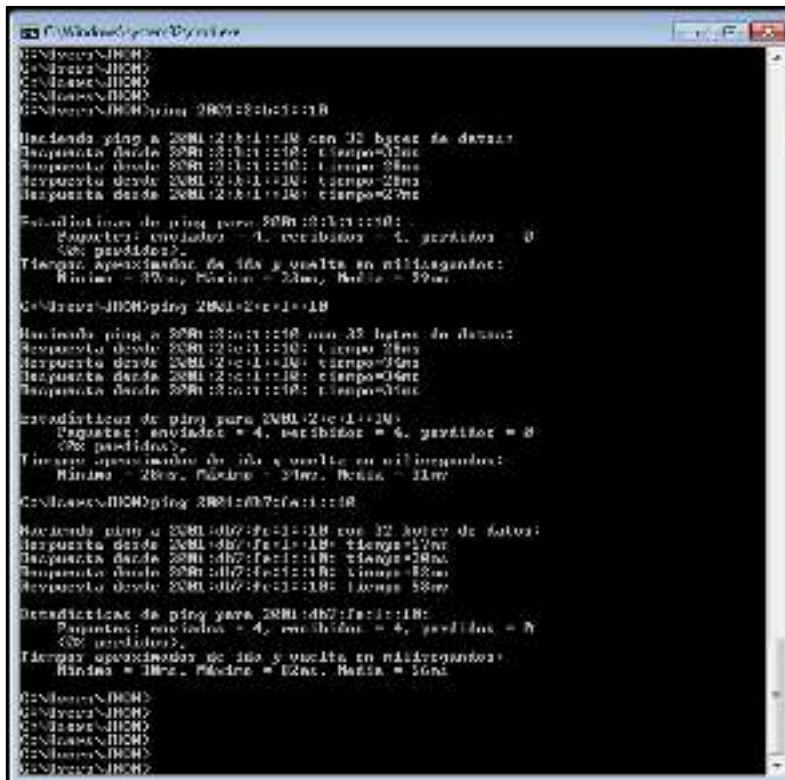
En este capítulo se analiza los resultados obtenidos de las diversas pruebas realizadas en los escenarios de las técnicas 6PE y 6VPE, estas pruebas se basan en la transmisión de streaming mediante un servidor VLC y evaluación de rendimiento a través de programa D-ITG.

3.1 Técnica 6PE

3.1.1 Pruebas de conectividad

Del escenario del capítulo anterior **Figura 1-2**. Se realizó las pruebas de conexión entre cliente1-cliente2, cliente1-cliente3, cliente1-servidor, cliente2-cliente1, cliente2-cliente3, cliente2-servidor, cliente3-cliente1, cliente3-cliente2 y cliente3-servidor

Desde el CLIENTE1 dirección ipv6 2001:2:a:1::10 se realizó las pruebas de conexión al CLIENTE2 ipv6 2001:2:b:1::10, CLIENTE3 ipv6 2001:2:c:1::10 y SERVIDOR 2001:db7:fe:1::10.



```
C:\Windows\system32\cmd.exe
C:\Users\JHC&gt;
C:\Users\JHC&gt;
C:\Users\JHC&gt;
C:\Users\JHC&gt;
C:\Users\JHC&gt;ping 2001:2:b:1::10

Haciendo ping a 2001:2:b:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:b:1::10: tiempo=11ms
Respuesta desde 2001:2:b:1::10: tiempo=28ms
Respuesta desde 2001:2:b:1::10: tiempo=28ms
Respuesta desde 2001:2:b:1::10: tiempo=27ms

Estadísticas de ping para 2001:2:b:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempo aproximado de ida y vuelta en milisegundos:
        Mínimo = 11ms, Máximo = 28ms, Prom. = 23ms

C:\Users\JHC&gt;ping 2001:2:c:1::10

Haciendo ping a 2001:2:c:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:c:1::10: tiempo=34ms
Respuesta desde 2001:2:c:1::10: tiempo=34ms
Respuesta desde 2001:2:c:1::10: tiempo=34ms
Respuesta desde 2001:2:c:1::10: tiempo=34ms

Estadísticas de ping para 2001:2:c:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempo aproximado de ida y vuelta en milisegundos:
        Mínimo = 28ms, Máximo = 34ms, Prom. = 31ms

C:\Users\JHC&gt;ping 2001:db7:fe:1::10

Haciendo ping a 2001:db7:fe:1::10 con 32 bytes de datos:
Respuesta desde 2001:db7:fe:1::10: tiempo=17ms
Respuesta desde 2001:db7:fe:1::10: tiempo=28ms
Respuesta desde 2001:db7:fe:1::10: tiempo=28ms
Respuesta desde 2001:db7:fe:1::10: tiempo=28ms

Estadísticas de ping para 2001:db7:fe:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempo aproximado de ida y vuelta en milisegundos:
        Mínimo = 17ms, Máximo = 28ms, Prom. = 26ms

C:\Users\JHC&gt;
C:\Users\JHC&gt;
C:\Users\JHC&gt;
C:\Users\JHC&gt;
C:\Users\JHC&gt;
```

Figura 1-3: Prueba de conexión del cliente1 con cliente2, cliente3 y servidor. Realizado por: Yautibug, A. 2020.

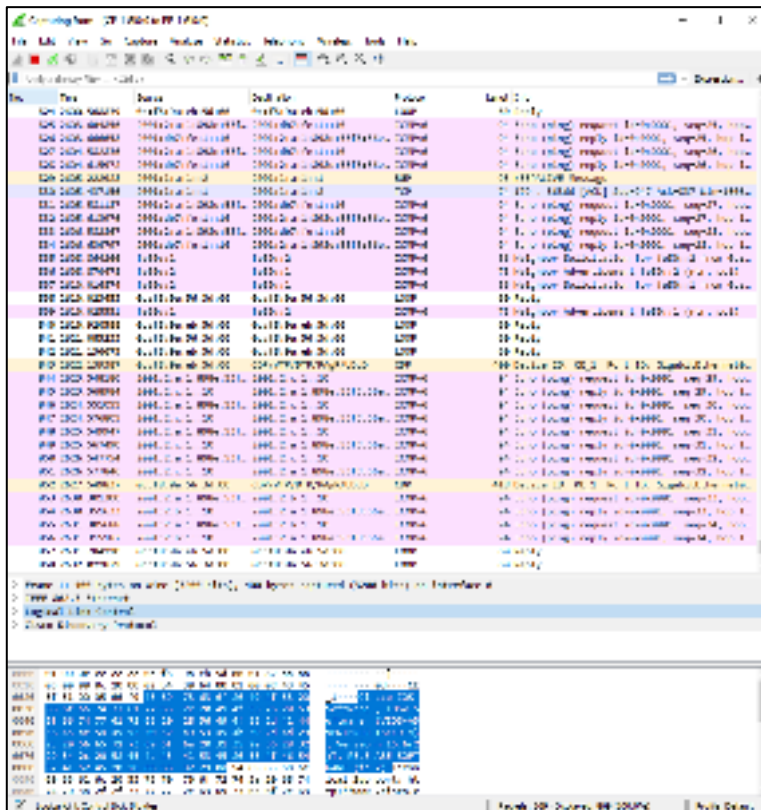


Figura 2-3: : Tráfico de ICMPv6 en Wireshark capturado entre CE1-PE1.
Realizado por:Yautibug, A. 2020.

Prueba de conexión desde el cliente 2 con dirección ipv6 2001:2:b:1::10 con los cliente1, cliente3 y servidor

```

C:\Users\LEOMEL>ping 2001:2:a:1::10

Realizando ping a 2001:2:a:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:a:1::10: tiempo=42ms
Respuesta desde 2001:2:a:1::10: tiempo=23ms
Respuesta desde 2001:2:a:1::10: tiempo=31ms
Respuesta desde 2001:2:a:1::10: tiempo=22ms

Estadísticas de ping para 2001:2:a:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdido),
    Tiempo aproximado de ida y vuelta en milisegundos:
        Mínimo = 22ms, Máximo = 42ms, Media = 29ms

C:\Users\LEOMEL>ping 2001:2:c:1::10

Realizando ping a 2001:2:c:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:c:1::10: tiempo=8ms
Respuesta desde 2001:2:c:1::10: tiempo=8ms
Respuesta desde 2001:2:c:1::10: tiempo=78ms
Respuesta desde 2001:2:c:1::10: tiempo=18ms

Estadísticas de ping para 2001:2:c:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdido),
    Tiempo aproximado de ida y vuelta en milisegundos:
        Mínimo = 8ms, Máximo = 78ms, Media = 32ms

C:\Users\LEOMEL>ping 2001:db7:fe:1::10

Realizando ping a 2001:db7:fe:1::10 con 32 bytes de datos:
Respuesta desde 2001:db7:fe:1::10: tiempo=36ms
Respuesta desde 2001:db7:fe:1::10: tiempo=29ms
Respuesta desde 2001:db7:fe:1::10: tiempo=38ms
Respuesta desde 2001:db7:fe:1::10: tiempo=32ms

Estadísticas de ping para 2001:db7:fe:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdido),
    Tiempo aproximado de ida y vuelta en milisegundos:
        Mínimo = 29ms, Máximo = 38ms, Media = 31ms
  
```

Figura 3-3: Prueba de conexión del cliente2 con cliente1, cliente3 y servidor.
Realizado por:Yautibug, A. 2020.

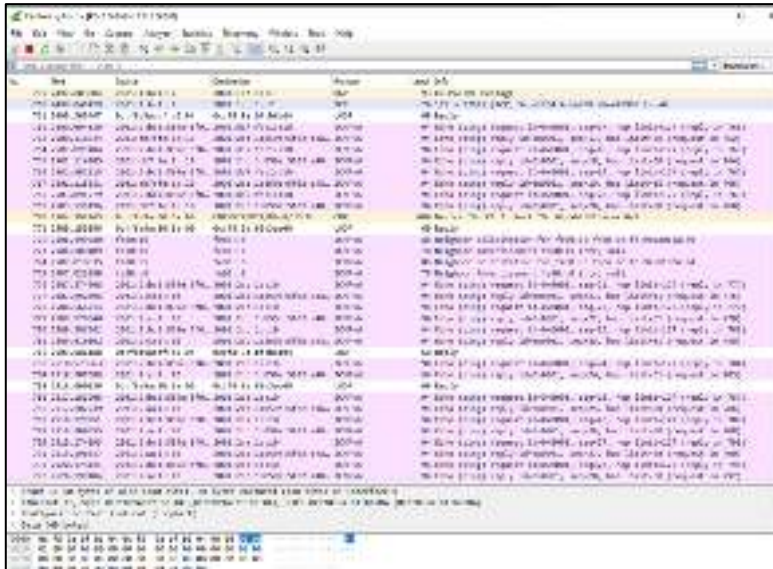


Figura 4-3: Tráfico de ICMPv6 en Wireshark capturado entre PE2-CE2.
Realizado por: Yautibug, A. 2020.

Prueba de conexión desde cliente3 es una máquina Ubuntu con ipv6 2001:2:c:1::10 con los cliente1, cliente2 y servidor.

```
osboxes@osboxes:~$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 2001:2:c:1::10 prefixlen 64 scopeid 0x0<global>
```

Figura 5-3: Dirección ipv6 en la maquina Ubuntu.
Realizado por: Yautibug, A. 2020.

```
osboxes@osboxes:~$ ping 2001:2:a:1::10
PING 2001:2:a:1::10(2001:2:a:1::10) 56 data bytes:
64 bytes from 2001:2:a:1::10: icmp_seq=1 ttl=64 time=10.10 ms
64 bytes from 2001:2:a:1::10: icmp_seq=2 ttl=64 time=28.6 ms
64 bytes from 2001:2:a:1::10: icmp_seq=3 ttl=64 time=26.3 ms
64 bytes from 2001:2:a:1::10: icmp_seq=4 ttl=64 time=40.8 ms
64 bytes from 2001:2:a:1::10: icmp_seq=5 ttl=64 time=25.4 ms
^C
--- 2001:2:a:1::10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 10.588/16.889/70.417/18.368 ms
osboxes@osboxes:~$ ping 2001:2:b:1::10
PING 2001:2:b:1::10(2001:2:b:1::10) 56 data bytes:
64 bytes from 2001:2:b:1::10: icmp_seq=1 ttl=64 time=14.8 ms
64 bytes from 2001:2:b:1::10: icmp_seq=2 ttl=64 time=16.5 ms
64 bytes from 2001:2:b:1::10: icmp_seq=3 ttl=64 time=16.2 ms
64 bytes from 2001:2:b:1::10: icmp_seq=4 ttl=64 time=17.3 ms
64 bytes from 2001:2:b:1::10: icmp_seq=5 ttl=64 time=11.4 ms
^C
--- 2001:2:b:1::10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 15.418/19.501/34.825/7.828 ms
osboxes@osboxes:~$ ping 2001:db7:fe:1::10
PING 2001:db7:fe:1::10(2001:db7:fe:1::10) 56 data bytes:
64 bytes from 2001:db7:fe:1::10: icmp_seq=1 ttl=64 time=29.8 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=2 ttl=64 time=15.7 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=3 ttl=64 time=21.16 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=4 ttl=64 time=29.9 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=5 ttl=64 time=23.2 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=6 ttl=64 time=18.2 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=7 ttl=64 time=26.1 ms
64 bytes from 2001:db7:fe:1::10: icmp_seq=8 ttl=64 time=43.9 ms
^C
--- 2001:db7:fe:1::10 ping statistics ---
9 packets transmitted, 8 received, 11.111% packet loss, time 28ms
rtt min/avg/max/mdev = 15.658/27.182/53.408/18.938 ms
osboxes@osboxes:~$
```

Figura 6-3: Prueba de conexión del cliente3 con Cliente1, Cliente2 y Servidor.
Realizado por: Yautibug, A. 2020.

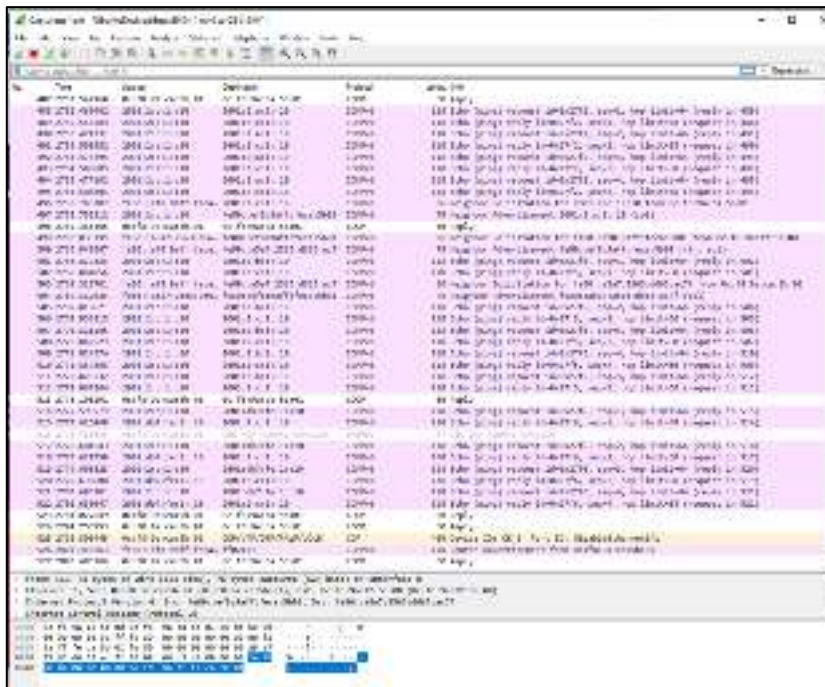


Figura 7-3: Tráfico de ICMPv6 en Wireshark capturado entre el enlace CE3-PC3.
Realizado por: Yautibug, A. 2020.

Prueba de conexión desde el servidor con ipv6 2001:db7:fe:1::10 a Cliente1, Cliente2 y Cliente3.

```

C:\Users\ALEX>ping 2001:2:a:1::10

Haciendo ping a 2001:2:a:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:a:1::10: tiempo=56ms
Respuesta desde 2001:2:a:1::10: tiempo=57ms
Respuesta desde 2001:2:a:1::10: tiempo=50ms
Respuesta desde 2001:2:a:1::10: tiempo=46ms

Estadísticas de ping para 2001:2:a:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 46ms, Máximo = 57ms, Media = 54ms

C:\Users\ALEX>ping 2001:2:b:1::10

Haciendo ping a 2001:2:b:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:b:1::10: tiempo=79ms
Respuesta desde 2001:2:b:1::10: tiempo=32ms
Respuesta desde 2001:2:b:1::10: tiempo=26ms
Respuesta desde 2001:2:b:1::10: tiempo=68ms

Estadísticas de ping para 2001:2:b:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 26ms, Máximo = 79ms, Media = 51ms

C:\Users\ALEX>ping 2001:2:c:1::10

Haciendo ping a 2001:2:c:1::10 con 32 bytes de datos:
Respuesta desde 2001:2:c:1::10: tiempo=17ms
Respuesta desde 2001:2:c:1::10: tiempo=16ms
Respuesta desde 2001:2:c:1::10: tiempo=12ms
Respuesta desde 2001:2:c:1::10: tiempo=17ms

Estadísticas de ping para 2001:2:c:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 12ms, Máximo = 17ms, Media = 15ms
  
```

Figura 8-3: Prueba de conexión del cliente2 con cliente1, cliente3 y servidor.
Realizado por: Yautibug, A. 2020.

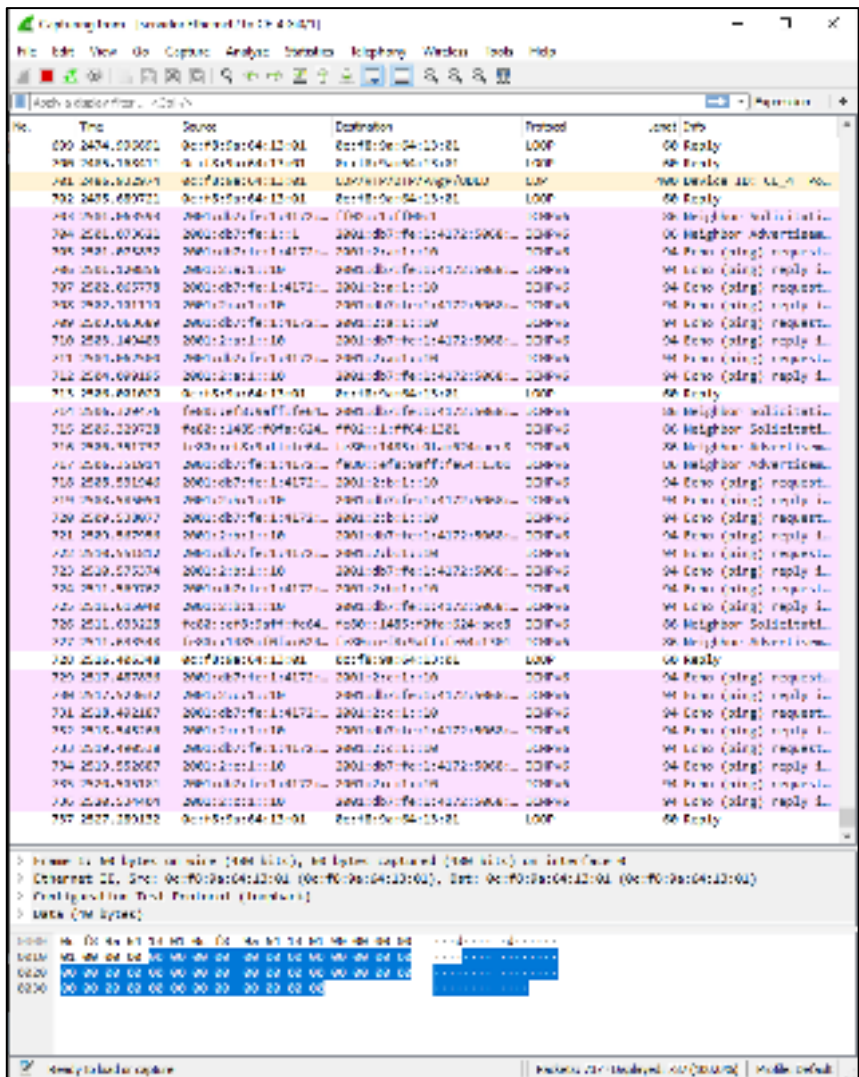


Figura 9-3: Tráfico de ICMPv6 en Wireshark capturado entre el enlace CE4-Servidor. Realizado por: Yautibug, A. 2020.

3.1.2 Prueba de streaming con VLC

Para esta prueba primero se realizó la configuración del servidor streaming con el software VLC ver la configuración en el **Capítulo II sección 2.6.2**

Configuración del servidor VLC: protocolo *http* para trasmision, con la dirección IPv6 *200:1:db7:fe:1::10*, puerto *:8080*, nombre de Transmisión: *leonel* al final queda configurado de la siguiente forma. *http://[200:1:db9:fe:1::10]:8080/leonel*

Para hacer la comprobación en el mismo servidor que está realizando el streaming, se configura otro software SMPlayer con la dirección del servidor.

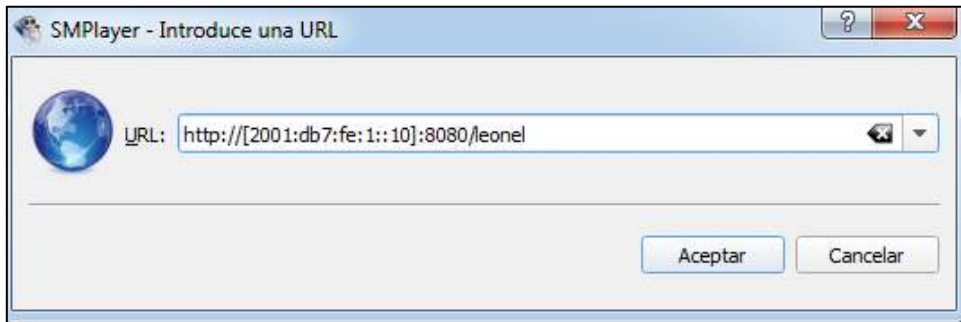


Figura 10-3: Ventana del programa SMPlayer con la dirección IPv6 del servidor.
Realizado por: Yautibug, A. 2020.

Como se observa en la siguiente **Figura 11-3** se comprobó que la transmisión de streaming esta correcta en el servidor.

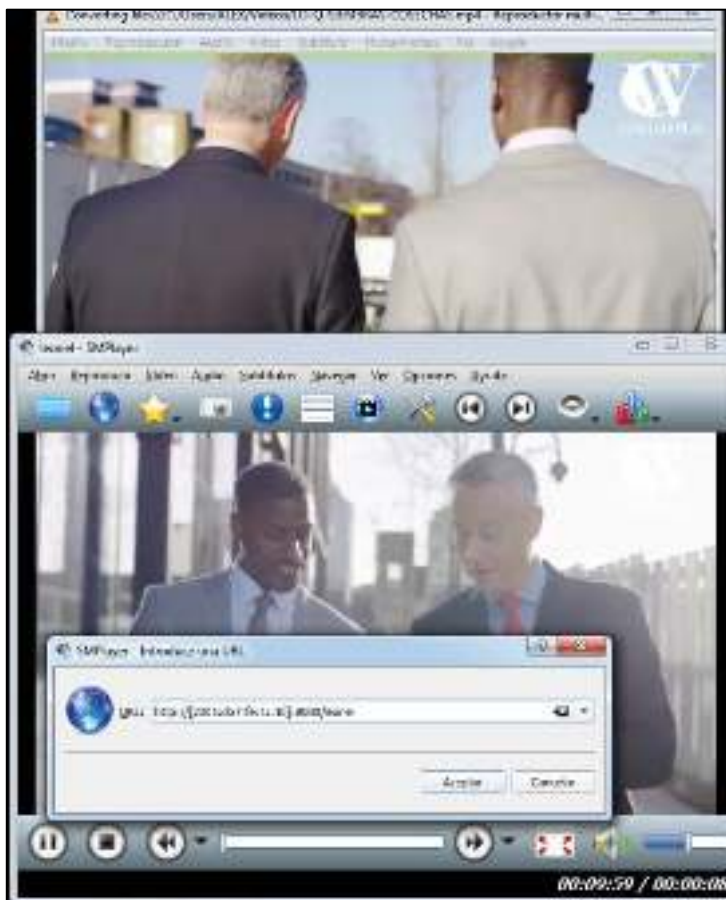


Figura 11-3: Reproducción de video en el servidor con multimedia SMPlayer.
Realizado por: Yautibug, A. 2020.

3.1.2.1 Pruebas de conexión de los Clientes con el Servidor

Abrir el reproductor VLC en el receptor, escoger la opción *medio* y luego se da clic *abrir ubicación de red* y se desplegara la ventana de configuración de los parámetro a conectarse con servidor streaming como son: el protocolo, dirección IPv6 del servidor, el puerto por el que está trasmitiendo el servidor y la ruta, para este trabajo es `http://[200:1:db7:fe:1::10]:8080/leonel`

Recepto1 o Cliente1 Abrir el reproductor VLC y configurar los parámetros de recepción.

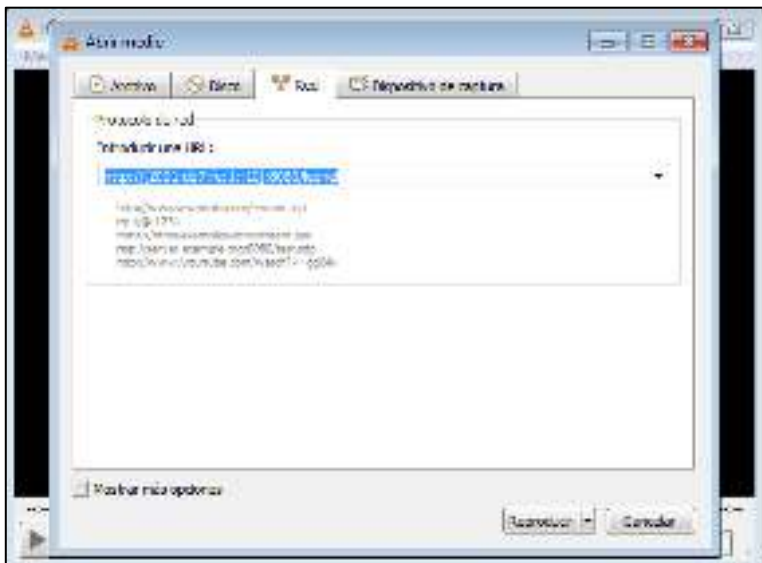


Figura 12-3: Ventana configuración de parámetros de recepción.
Realizado por: Yautibug, A. 2020.

Al hacer click inició la reproducción del contenido multimedia que este emitiendo el servidor.



Figura 13-3: Reproducción de video en Cliente1.
Realizado por: Yautibug, A. 2020.

Mediante la herramienta Wireshark se capturo los paquete de recepción a nivel de transporte por el protocolo TCP.

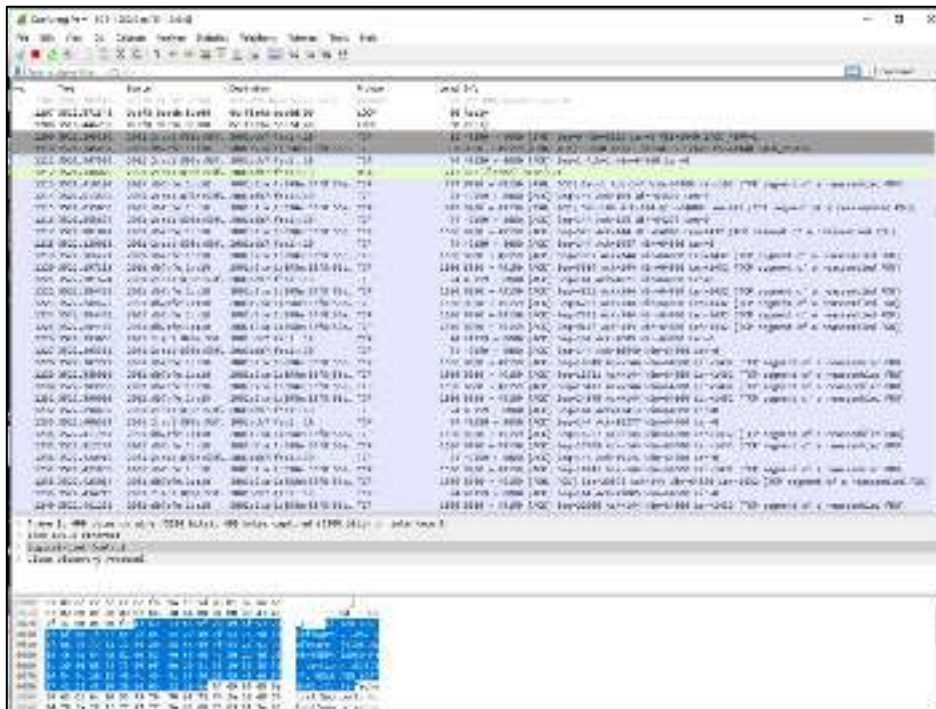


Figura 14-3 Tráfico de streaming en Wireshark capturado entre el enlace CE1-PE1.
Realizado por: Yautibug, A. 2020.

Prueba de conexión Cliente2 con el servidor Streaming.



Figura 15-3: Reproducción de video en Cliente3.
Realizado por: Yautibug, A. 2020.

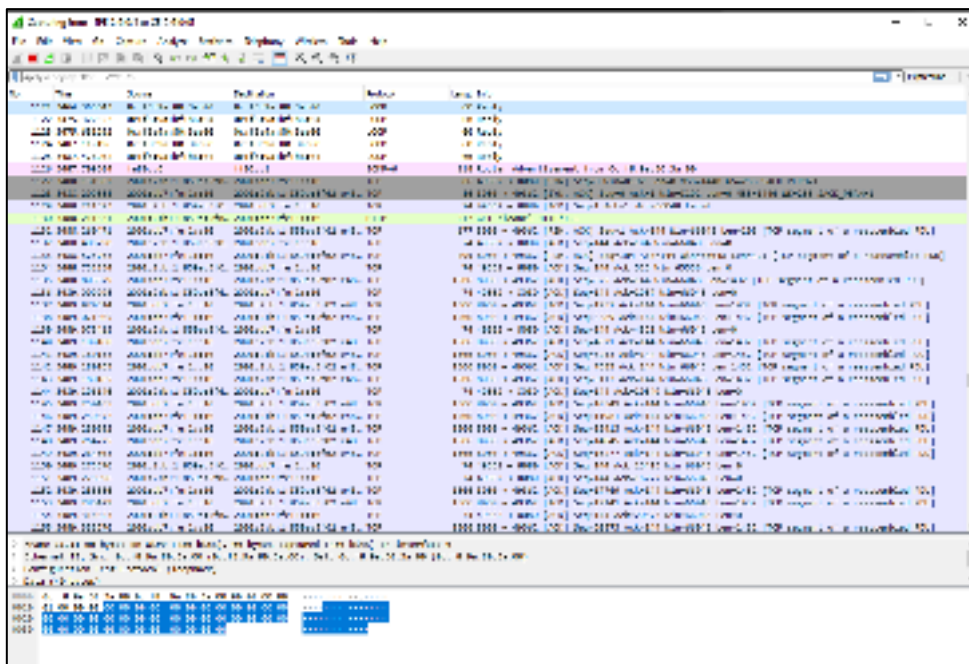


Figura 16-3 Tráfico de streaming en Wireshark capturado entre el enlace PE2-CE2.
 Realizado por: Yautibug, A. 2020.

Prueba de conexión máquina Ubuntu Cliente3 con el servidor streaming VLC.

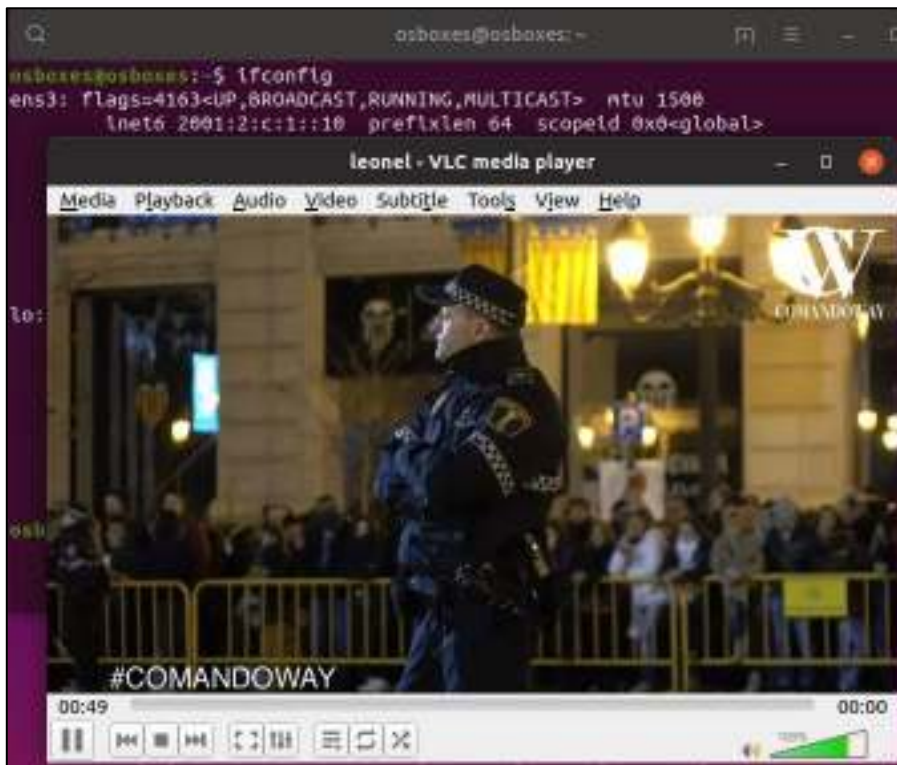


Figura 17-3: Reproducción de video en Cliente3.
 Realizado por: Yautibug, A. 2020.

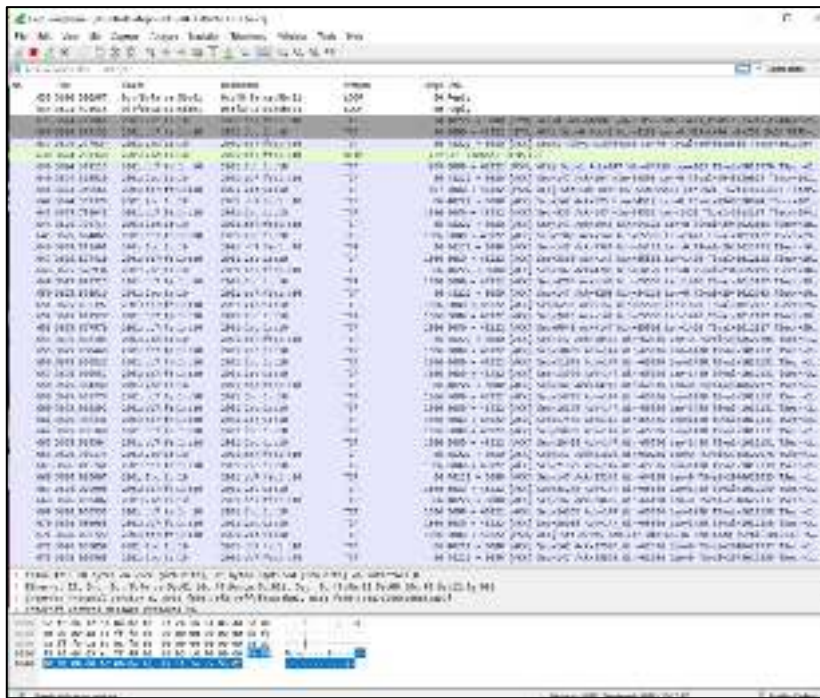


Figura 18-3: Tráfico de streaming capturado entre el enlace CE3-PC Cliente3 con Wireshark. Realizado por: Yautibug, A. 2020.

3.1.3 Evaluación de rendimiento con D-ITG

Una vez realizado las pruebas de conexión y streaming con VLC, se empleó la herramienta de software D-ITG (Distributed Internet Traffic Generator) para inyección de tráfico streaming, la configuración del emisor como el receptor ver en el **capítulo II** la sección 2.7.3, las pruebas realizadas tuvieron distintos tiempos de duración de: 30, 45 y 60 segundos y se determinó en cada tiempo el valor de todo los parámetros que da D-ITG en especial delay, jitter y packet loss, al final de las pruebas se capturó el tráfico UDP con Wireshark.

3.1.3.1 Parámetros configurados en el Emisor de D-ITG.

En el emisor o servidor se realizó las siguientes configuraciones con los parámetros resumidos en la **Tabla 1-3**, se envió paquetes en 3 diferentes tiempos 30, 45, y 60, segundos

Tabla 1-3: Parámetro para el flujo en emisor o servidor del Software D-ITG.

Parámetro	Valor
Direcciones de Destinos	2001:2:a:1::10 2001:2:b:1::10 2001:2:c:1::10
Tiempos de transmisión	30s, 45s y 60s
Meter	Round-Trip-time
TTL	64
Protocolo	UDP
Numero de paquete por segundo	1000 Paquetes /seg
Tamaño del paquete	512 Bytes

Realizado por: Yautibug, A. 2020.

3.1.3.2 Resultados obtenidos en el receptor de D-ITG.

Resultados obtenidos en el programa D-ITG luego de la recepción del tráfico en el cliente1 con tiempo de recepción de 30 segundos con se muestra en la **Figura 19-3**.

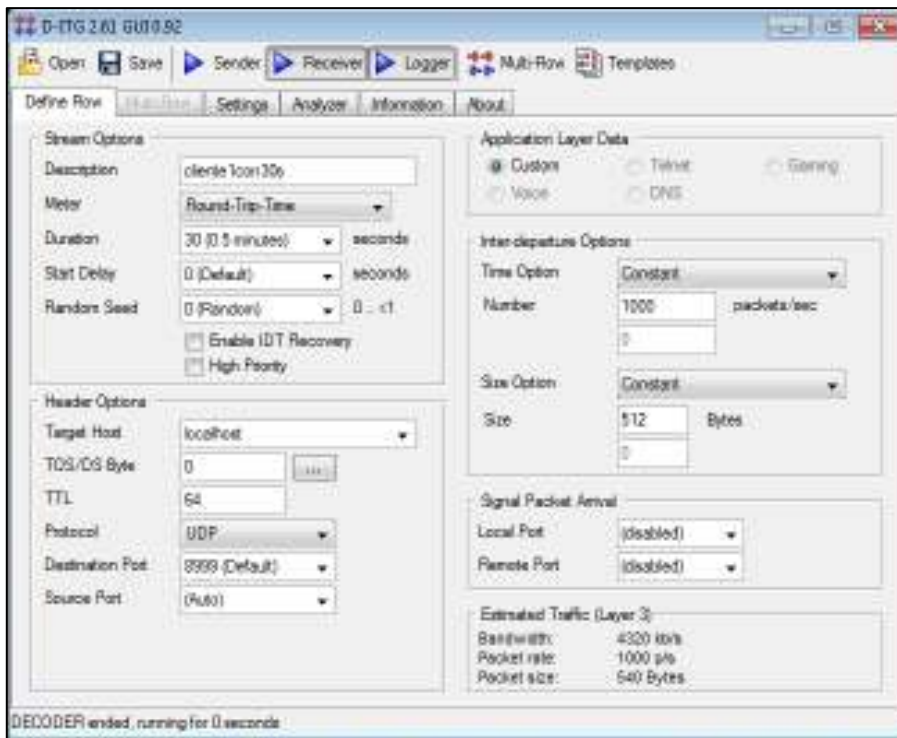


Figura 19-3: D-ITG, Configuración en el receptor cliente 1 con 30s.

Realizado por: Yautibug, A. 2020.

Resultado en el receptor cliente 1 con tiempo de recepción 30 segundos

```
Flow number: 1
From 2001:db7:fe:1:a81e:855b:3d20:641d:60989
To 2001:2:a:1::10:8999
-----
Total time = 38.398000 s
Total packets = 5402
Minimum delay = -0.432497 s
Maximum delay = 16.277803 s
Average delay = 10.654983 s
Average jitter = 0.009968 s
Delay standard deviation = 3.974502 s
Bytes received = 2765824
Average bitrate = 576.243346 Kbit/s
Average packet rate = 140.684411 pkt/s
Packets dropped = 24558 (81.97 %)
Average loss-burst size = 11.699857 pkt
```

Figura 20-3: Resultado de tráfico en el cliente 1 con tiempo de recepción 30 segundos.

Realizado por: Yautibug, A. 2020.

Resultado en el receptor cliente 1 con tiempo de recepción 45 segundos

***** TOTAL RESULTS *****		
Number of flows	=	1
Total time	=	54.044000 s
Total packets	=	7650
Minimum delay	=	-0.052079 s
Maximum delay	=	14.183950 s
Average delay	=	10.270906 s
Average jitter	=	0.011041 s
Delay standard deviation	=	3.626508 s
Bytes received	=	3916800
Average bitrate	=	579.794242 Kbit/s
Average packet rate	=	141.551329 pkt/s
Packets dropped	=	33624 (81.47 %)
Average loss-burst size	=	9.986338 pkt
Error lines	=	0

Figura 21-3: Resultado de tráfico en el cliente 1 con tiempo de recepción 45 segundos.

Realizado por: Yautibug, A. 2020.

Resultado en el receptor cliente 1 con tiempo de recepción 60 segundos

ITGDec version 2.8.1 (r1023)		
Compile-time options:		

Flow number: 1		
From 2001:db7:fe:1:85be:b32d:4cfe:ce10:49818		
To 2001:2:a:1::10:8999		

Total time	=	76.377000 s
Total packets	=	11237
Minimum delay	=	-0.073098 s
Maximum delay	=	16.813967 s
Average delay	=	10.905075 s
Average jitter	=	0.011251 s
Delay standard deviation	=	4.395857 s
Bytes received	=	5753344
Average bitrate	=	602.625817 Kbit/s
Average packet rate	=	147.125444 pkt/s
Packets dropped	=	48663 (81.24 %)
Average loss-burst size	=	12.990657 pkt

Figura 22-3: Resultado de tráfico en el cliente 1 con tiempo de recepción 60 segundos.

Realizado por: Yautibug, A. 2020.

En la siguiente **Figura 43-3** se visualiza la captura de paquetes streaming con el protocolo UDP a nivel de transporte con Wireshark.

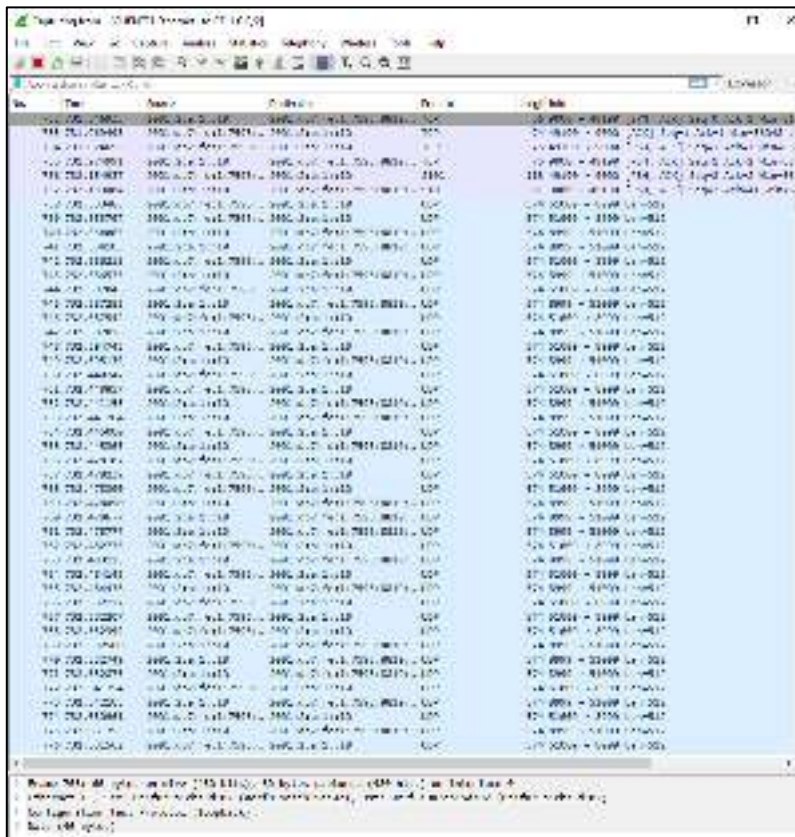


Figura 23-3: Tráfico de streaming en Wireshark capturado entre el enlace CE1-CLIENTE1. Realizado por: Yautibug, A. 2020.

Receptor cliente 2 con 30 segundos

```
ITGDec version 2.0.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db7:fe:1:41aa:d3d2:a553:7ddd:59873
To 2001:2:b:1::10:8999
-----
Total time = 34.282000 s
Total packets = 6178
Minimum delay = 0.529998 s
Maximum delay = 5.654098 s
Average delay = 3.535291 s
Average jitter = 0.006474 s
Delay standard deviation = 1.494793 s
Bytes received = 3163136
Average bitrate = 738.145032 Kbit/s
Average packet rate = 180.211190 pkt/s
Packets dropped = 23805 (79.39 %)
Average loss-burst size = 4.653049 pkt
```

Figura 24-3: Resultado de tráfico en el cliente 2 con tiempo de recepción 30 segundos. Realizado por: Yautibug, A. 2020.

Receptor cliente 2 con tiempo de recepción 45 segundos

```
ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db7:fe:1:41aa:d3d2:a553:7ddd:64534
To 2001:2:b:1::10:8999
-----
Total time           = 47.575000 s
Total packets        = 8622
Minimum delay        = 0.495997 s
Maximum delay        = 5.003261 s
Average delay        = 3.604459 s
Average jitter       = 0.006828 s
Delay standard deviation = 0.923361 s
Bytes received       = 4414464
Average bitrate      = 742.316595 Kbit/s
Average packet rate  = 181.229637 pkt/s
Packets dropped      = 36372 (80.84 %)
Average loss-burst size = 5.162811 pkt
```

Figura 25-3: Resultado de tráfico en el cliente 2 con tiempo de recepción 45 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 1 con tiempo de recepción 45 segundos

```
ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db7:fe:1:b91d:170c:13d:48eb:52314
To 2001:2:b:1::10:8999
-----
Total time           = 69.688000 s
Total packets        = 11267
Minimum delay        = 0.928557 s
Maximum delay        = 11.463963 s
Average delay        = 8.612269 s
Average jitter       = 0.009533 s
Delay standard deviation = 2.866317 s
Bytes received       = 5768704
Average bitrate      = 662.232120 Kbit/s
Average packet rate  = 161.677764 pkt/s
Packets dropped      = 48727 (81.22 %)
Average loss-burst size = 7.065980 pkt
```

Figura 26-3: Resultado de tráfico en el cliente 2 con tiempo de recepción 60 segundos.

Realizado por: Yautibug, A. 2020.

En la siguiente **Figura 27-3** se visualiza la captura de paquetes streaming con el protocolo UDP a nivel de transporte con Wireshark.

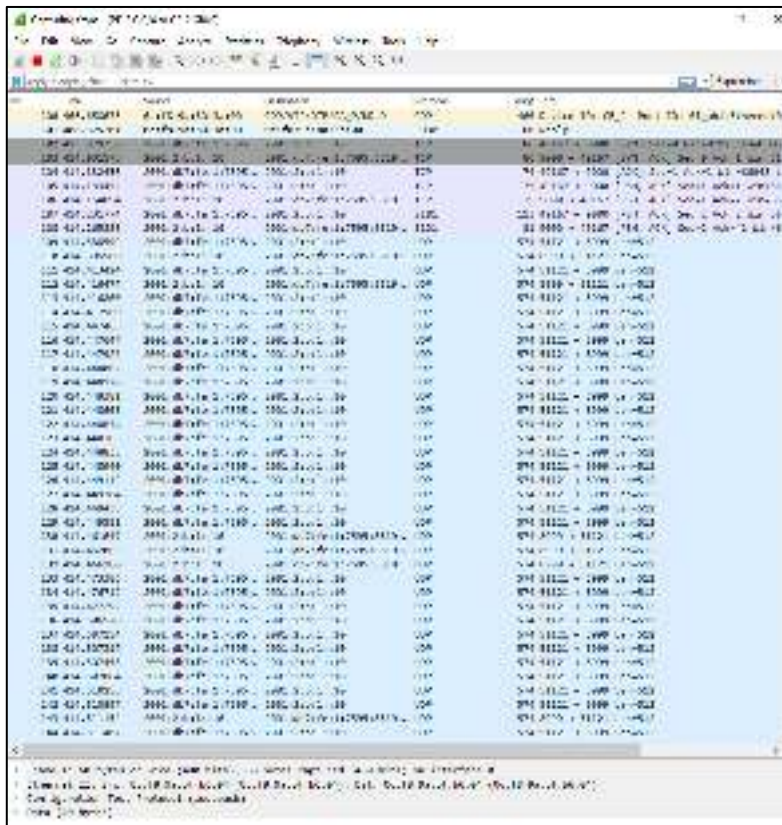


Figura 27-3: Tráfico de streaming en Wireshark capturado entre el enlace PE2-CE2.
Realizado por: Yautibug, A. 2020.

Receptor cliente 3 es una máquina Ubuntu con tiempo de recepción 30 segundos

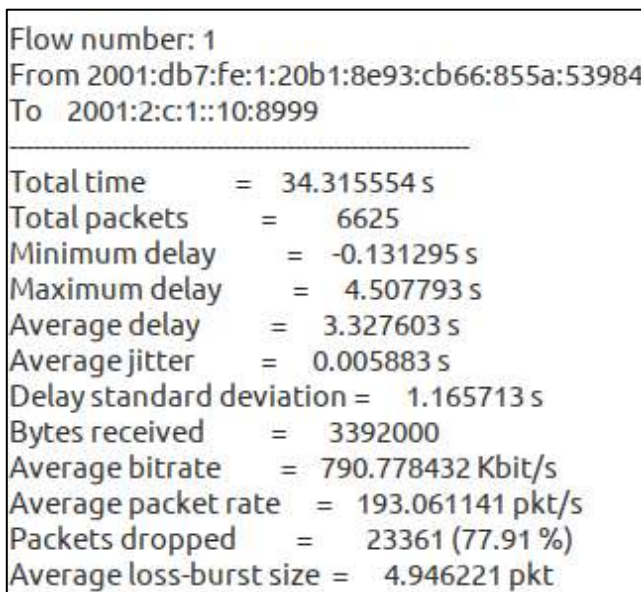


Figura 28-3: Resultado de tráfico en el cliente 3 con tiempo de recepción 30 segundos.
Realizado por: Yautibug, A. 2020.

Receptor cliente 3 con tiempo de recepción 45 segundos

Flow number: 1	
From 2001:db7:fe:1:744d:5c99:a228:3274:54707	
To 2001:2:c:1::10:8999	
<hr/>	
Total time	= 47.496434 s
Total packets	= 8774
Minimum delay	= -0.204412 s
Maximum delay	= 3.941655 s
Average delay	= 2.320023 s
Average jitter	= 0.006410 s
Delay standard deviation	= 1.054231 s
Bytes received	= 4492288
Average bitrate	= 756.652678 Kbit/s
Average packet rate	= 184.729658 pkt/s
Packets dropped	= 36217 (80.50 %)
Average loss-burst size	= 4.965314 pkt

Figura 29-3: Resultado de tráfico en el cliente 3 con tiempo de recepción 45 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 3 con tiempo de recepción 60 segundos

Flow number: 1	
From 2001:db7:fe:1:744d:5c99:a228:3274:49773	
To 2001:2:c:1::10:8999	
<hr/>	
Total time	= 64.070050 s
Total packets	= 10774
Minimum delay	= 0.418194 s
Maximum delay	= 5.515812 s
Average delay	= 3.532340 s
Average jitter	= 0.007319 s
Delay standard deviation	= 1.483416 s
Bytes received	= 5516288
Average bitrate	= 688.782106 Kbit/s
Average packet rate	= 168.159694 pkt/s
Packets dropped	= 49225 (82.04 %)
Average loss-burst size	= 5.065343 pkt

Figura 30-3: Resultado de D-ITG con protocolo UDP, cliente3 – servidor con tiempo de 60 s.

Realizado por: Yautibug, A. 2020.

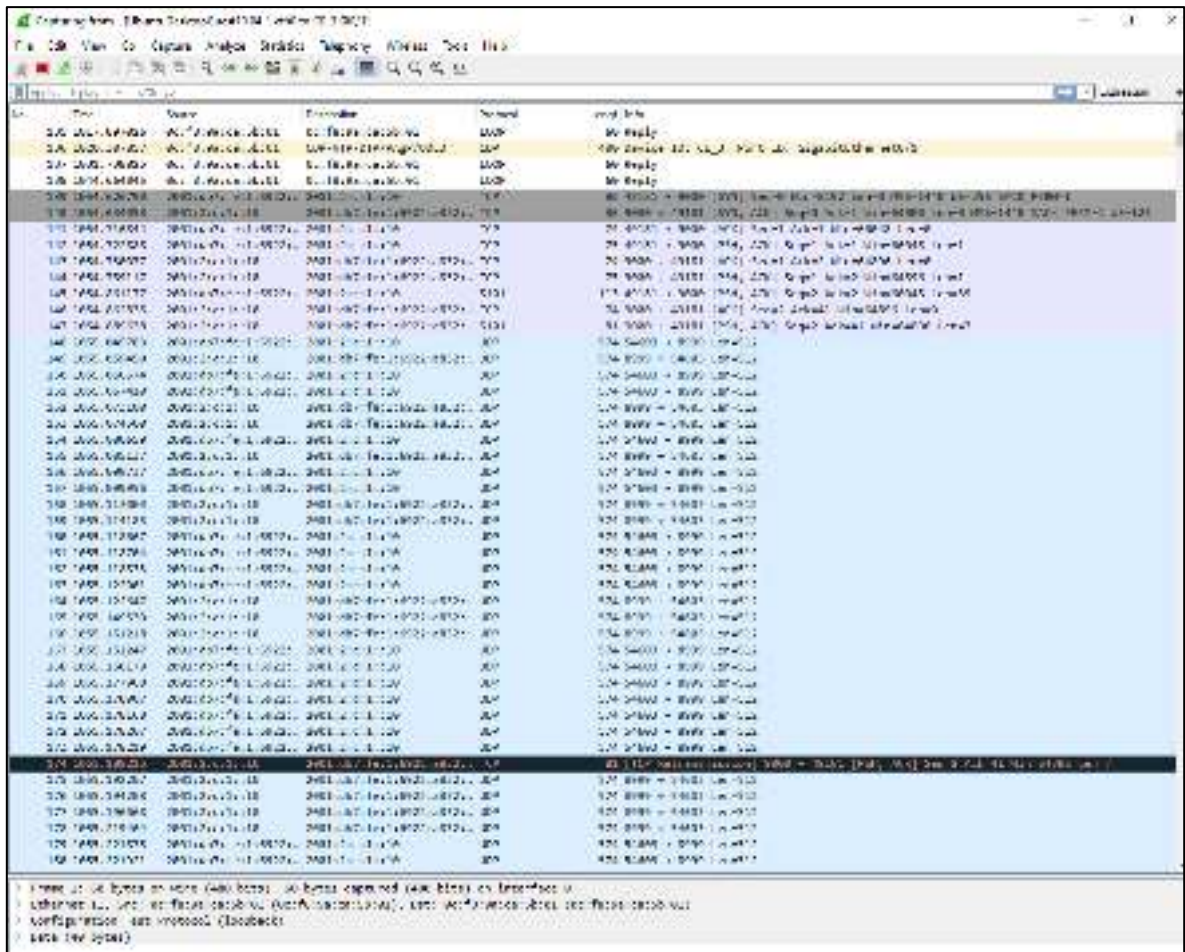


Figura 31-3: Tráfico de streaming en Wireshark capturado entre el enlace CE3-CLIENTE3.
 Realizado por: Yautibug, A. 2020.

Se efectuó 9 pruebas con D-ITG con la finalidad de medir los parámetros de calidad contenidos en la **Tabla 2-3**, primero se realizó una inyección de tráfico streaming desde el servidor a cliente1, clientes2 y cliente 3 visualizar en la **Tabla 1-3**, con los siguientes parámetro constantes de emisión: Número de paquete por segundo 1000 [paquet/sec], protocolo UDP, Tamaño del paquete 512 [Bytes], Meter con la opción Round-Trip-time [ida y vuelta] y la variación de Tiempos de recepción 30 , 45 y 60 [segundos] y en los 3 clientes se recibió este tráfico de streaming para luego comparar con la técnica 6VPE y saber cuál es la mejor técnica para transmisión y recepción de audio y video.

Tabla 2-3: Resumen de los resultados obtenidos por D-ITG en la técnica 6PE

Parámetro	Servidor – Cliente1			Servidor – Cliente2			Servidor – Cliente3			Suma
Tiempo de emisión [s]	30	45	60	30	45	60	30	45	60	
Tiempo[s]	38,398	54,044	76,377	34,282	47,575	69,688	34,316	47,496	64,07	466,246
Total de paquetes [Unid]	5402	7650	11237	6178	8354	11261	6625	8774	10774	76255
Mínimo delay [s]	-0,432	-0,052	-0,073	0,529	0,495	0,928	-0,131	-0,204	0,418	1,479
Máximo delay [s]	16,277	14,183	16,813967	5,654	5,003	11,463	4,507	3,941	5,515	83,356
Promedio de delay o latencia [s]	10,654	10,270	10,905	3,53	3,604	8,612	3,327	2,320	3,532	56,759
Promedio Jitter [ms]	9,968	11,041	11,251	6,474	6,828	9,533	5,883	6,41	7,379	74,767
Desviación Estándar del delay [s]	3,974	3,626	4,395	1,494	0,923	2,866	1,165	1,054	1,483	20,980
Bytes recibidos [Unid]	2765824	3916800	5753344	3163136	4414464	5768704	3392000	4492288	5516288	39182848
Velocid. Promedio de Bits [kbits/s]	576,243	579,794	602,625	738,145	742,316	662,232	790,778	756,652	688,782	6137,570
Velocid. Promedio de paquetes [pkt/s]	140,684	141,551	147,125	180,211	181,229	161,677	193,061	184,729	168,159	1498,426
Paquetes Dropeados [unid.]	24558(81,97)	33624(81,47)	48663(81,24)	23805(79,39)	36372(80,84)	48727(81,22)	23361(77,91)	36217(80,5)	49225(82,04)	324552(80,73)
Tamaño promedio loss-burst [pkt]	11,699	9,986	12,990	4,653	5,162	7,065	4,946	4,965	5,065	66,535
Líneas de Error	0	0	0	0	0	0	0	0	0	0

Realizado por: Yautibug, A. 2020.

3.2 Técnica 6VPE

Del escenario del capítulo anterior **Figura 2-2**. Se realizó las pruebas de conectividad capa 3 entre VPNs/VRFs de los clientes con el servidor VLC como son: cliente1-servidor, cliente2-servidor, y cliente3-servidor

3.2.1 Pruebas de conectividad

Desde el CLIENTE1 dirección ipv6 2001:2:a:1::10 se realizó las pruebas de conexión al SERVIDOR 2001:db9:fe:1::10.

```
C:\Users\JHON>
C:\Users\JHON>
C:\Users\JHON>ping 2001:db9:fe:1::10

Haciendo ping a 2001:db9:fe:1::10 con 32 bytes de datos:
Respuesta desde 2001:db9:fe:1::10: tiempo=88ms
Respuesta desde 2001:db9:fe:1::10: tiempo=71ms
Respuesta desde 2001:db9:fe:1::10: tiempo=38ms
Respuesta desde 2001:db9:fe:1::10: tiempo=31ms

Estadísticas de ping para 2001:db9:fe:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 31ms, Máximo = 88ms, Media = 57ms
```

Figura 32-3: Prueba de conexión del cliente1 con el servidor.
Realizado por:Yautibug, A. 2020.

En el enlace CE1-PE1 se capturo de paquetes ICMPv6 al momento de hacer las prueba de conexión del cliente uno con el servidor VLC.

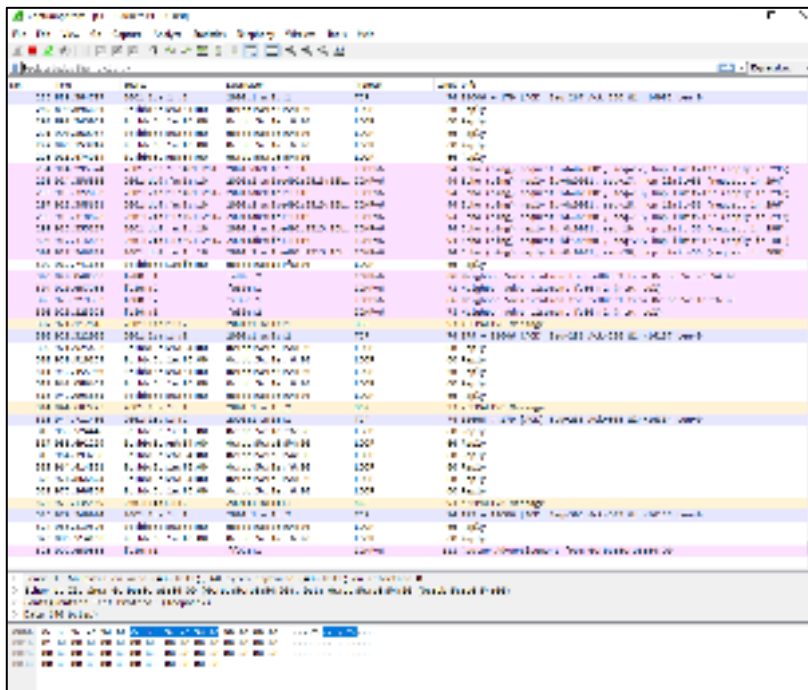


Figura 33-3: Tráfico de ICMPv6 en Wireshark capturado entre el enlace CE1-Servidor.
Realizado por:Yautibug, A. 2020.

Prueba de conexión desde el Cliente2 dirección ipv6 2001:2:a:1::10 al servidor VLC 2001:db9:fe:1::10

```
C:\Users\LEONEL>ping 2001:db9:fe:1::10

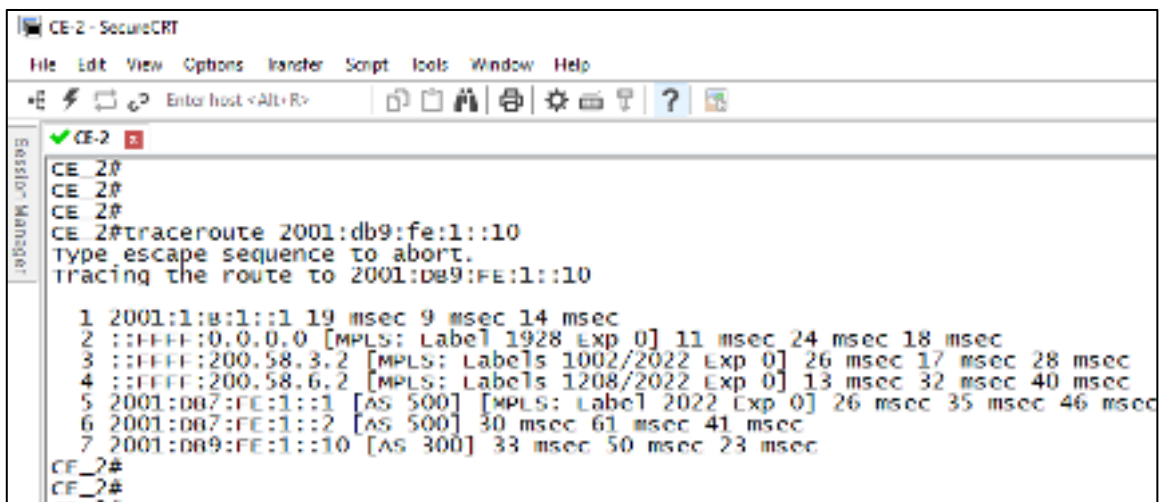
Haciendo ping a 2001:db9:fe:1::10 con 32 bytes de datos:
Respuesta desde 2001:db9:fe:1::10: tiempo=50ms
Respuesta desde 2001:db9:fe:1::10: tiempo=45ms
Respuesta desde 2001:db9:fe:1::10: tiempo=26ms
Respuesta desde 2001:db9:fe:1::10: tiempo=46ms

Estadísticas de ping para 2001:db9:fe:1::10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 26ms, Máximo = 50ms, Media = 41ms
```

Figura 36-3: Prueba de conexión del cliente2 con el servidor.

Realizado por: Yautibug, A. 2020.

Con se observa en la siguiente **Figura 37-3** se realizó un traceroute desde el CE-2 al servidor para visualizar la ruta que toma los paquetes. Dirección de los hosts por los que va pasando, y el tiempo que toma en cada salto hasta su llegada al destino.



```
CE-2 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt>R
CE-2
CE_2#
CE_2#
CE_2#tracert 2001:db9:fe:1::10
Type escape sequence to abort.
Tracing the route to 2001:DB9:FE:1::10

 0  2001:1:b:1::1 19 msec 9 msec 14 msec
 1  ::ffff:0.0.0.0 [MPLS: Label 1928 Exp 0] 11 msec 24 msec 18 msec
 2  ::ffff:200.58.3.2 [MPLS: Labels 1002/2022 Exp 0] 26 msec 17 msec 28 msec
 3  ::ffff:200.58.6.2 [MPLS: Labels 1208/2022 Exp 0] 13 msec 32 msec 40 msec
 4  2001:db7:fe:1::1 [AS 500] [MPLS: Label 2022 Exp 0] 26 msec 35 msec 46 msec
 5  2001:db7:fe:1::2 [AS 500] 30 msec 61 msec 41 msec
 6  2001:db9:fe:1::10 [AS 300] 33 msec 50 msec 23 msec
CE_2#
CE_2#
```

Figura 37-3: Traceroute del CE2-Servidor.

Realizado por: Yautibug, A. 2020.

En la técnica 6VPE se crea VRFs en los router PE, se aplica el método HUB and SPOKE en el enlace del servidor PE4-CE4 creando un enlace dedicado para el cliente2 con dirección IPv6 2001:db7:fe:1::/64

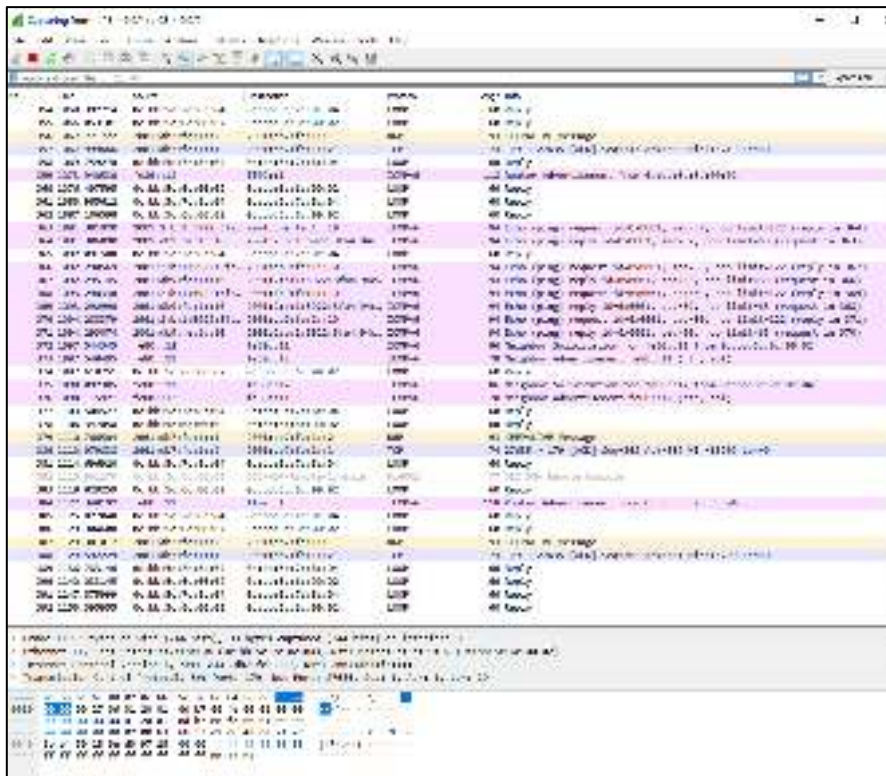


Figura 38-3: Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE4-CE4. Realizado por: Yautibug, A. 2020.

Prueba de conectividad capa 3 desde la máquina Ubuntu cliente3 con dirección IPv6 2001:2:c:1::10 con el servidor VLC.

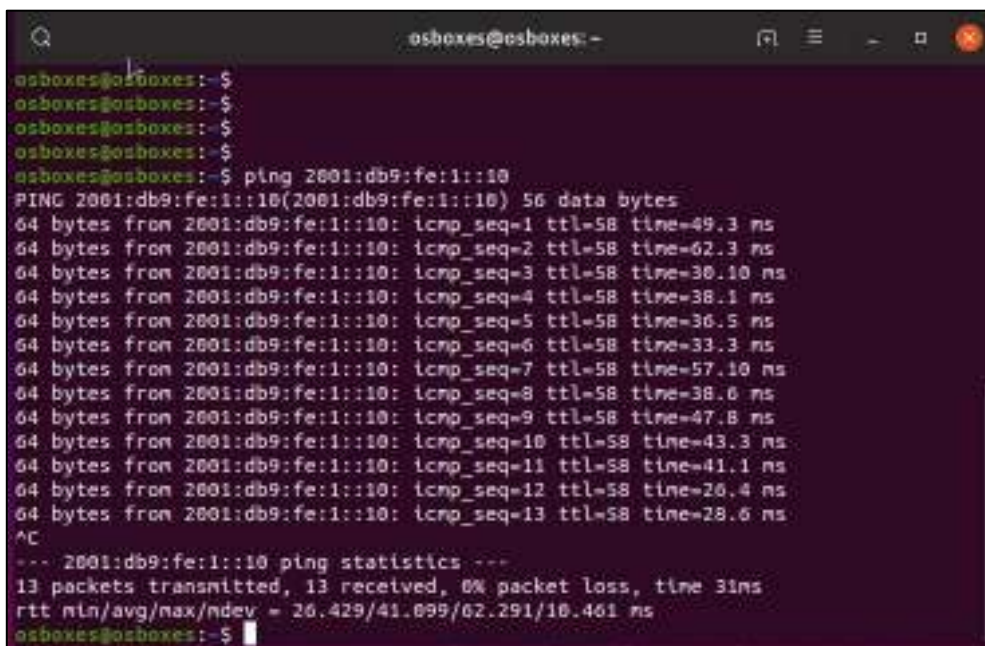


Figura 39-3: Prueba de conexión del cliente3 con el servidor. Realizado por: Yautibug, A. 2020.

En el enlace CE3-PE3 se capturó con wireshark los paquetes ICMPv6 al momento de hacer la prueba de conexión del Cliente3 - servidor VLC.

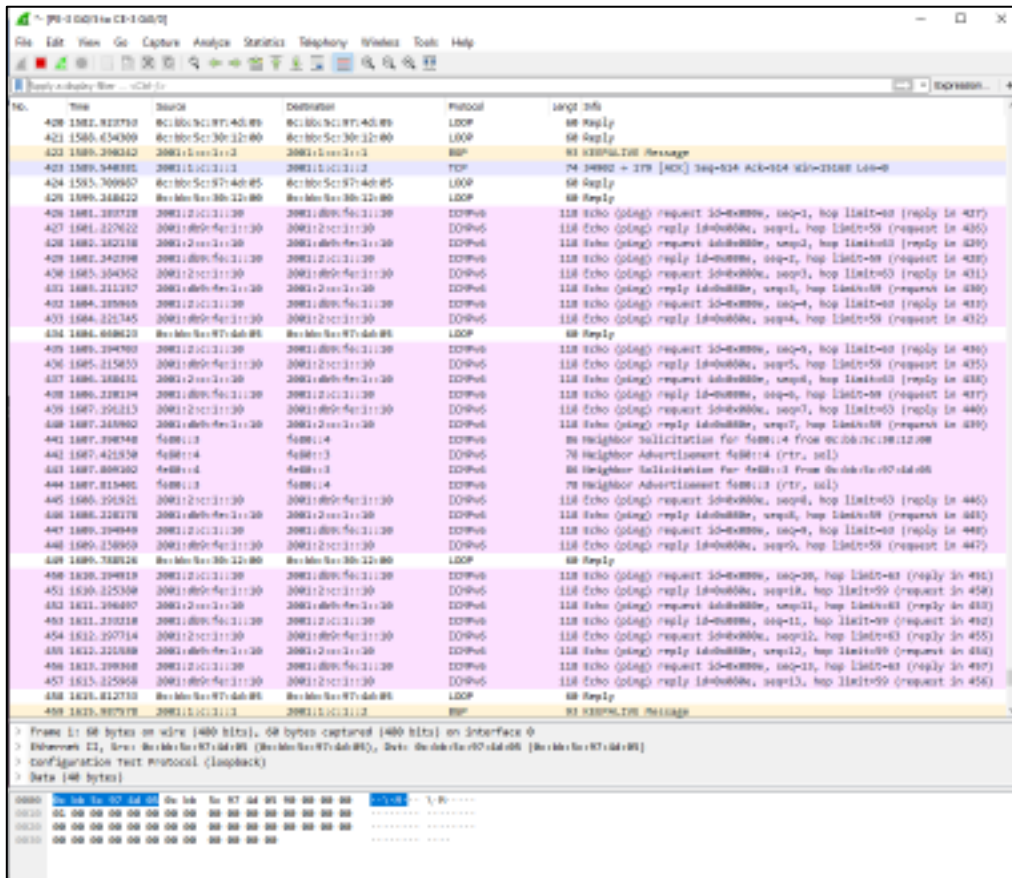


Figura 40-3: Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE3-CE3.
Realizado por: Yautibug, A. 2020

se realizó un traceroute desde el CE-3 al servidor para visualizar la ruta que toma los paquetes hasta llegar al destino.

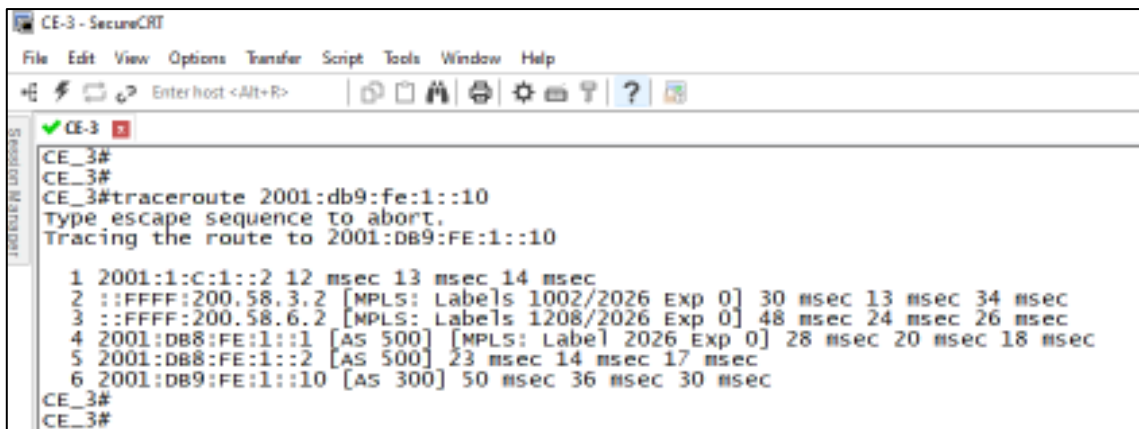


Figura 41-3: Traceroute del CE3-Servidor.
Realizado por: Yautibug, A. 2020.

En PE4-CE4 se aplica un método HUB and SPOKE para crear un enlace dedicado, para el cliente3 con dirección IPv6 2001:db8:fe:1::/64

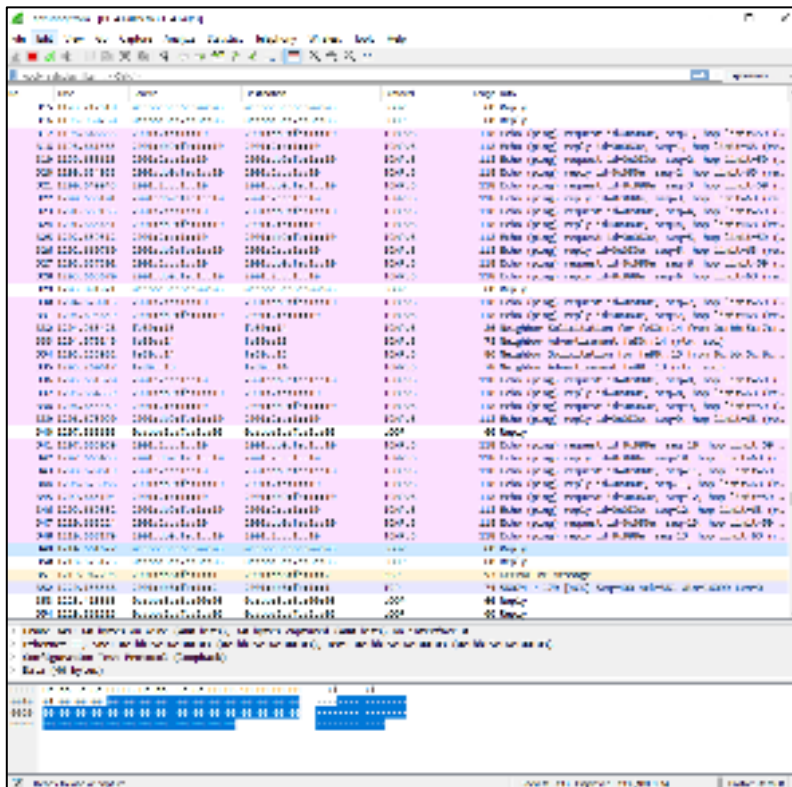


Figura 42-3: Tráfico de ICMPv6 en Wireshark capturado entre el enlace PE4-CE4. Realizado por: Yautibug, A. 2020

Pruebas de conectividad desde el servidor al Cliente1, Cliente2 y Cliente3.

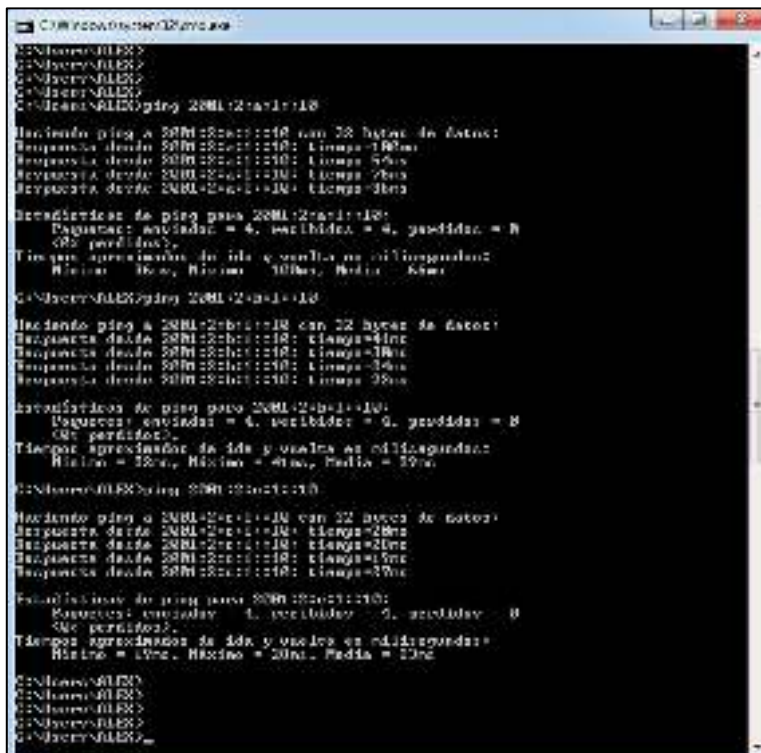


Figura 43-3: Prueba de conexión del servidor al Cliente1, Cliente2 y Cliente3. Realizado por: Yautibug, A. 2020.

Se realizó un traceroute desde el servidor al Cliente1 Cliente2 y Cliente3 para visualizar la ruta y tiempo que toma los paquetes hasta llegar al destino.

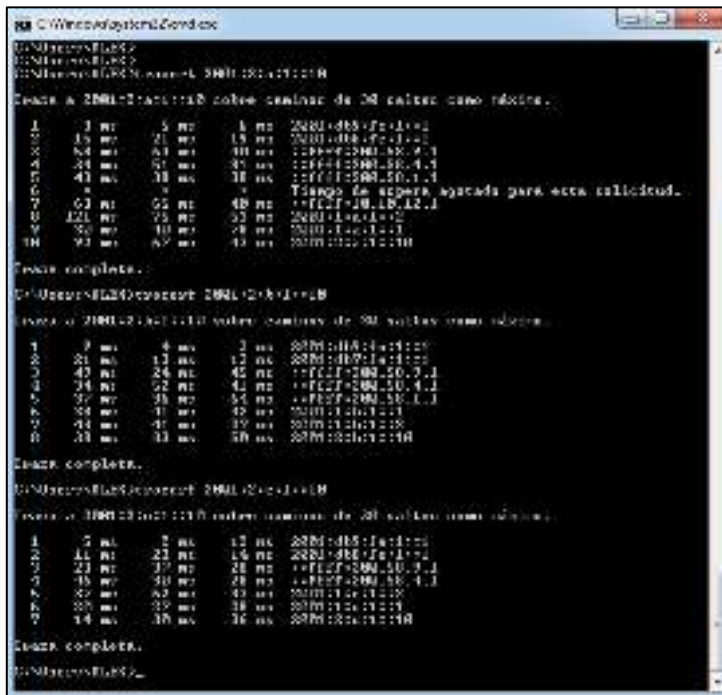


Figura 44-3: traceroute del Servidor con Cliente1, cliente2 y Cliente3.
Realizado por: Yautibug, A. 2020.

3.2.2 Prueba de streaming

3.2.2.1 Transmisión del servidor streaming VLC media Player

Servidor.- **Capítulo II** sección 2.6.2 se configuro el servidor se debe seguir los mismo pasos hasta llegar a emitir y empieza a transmitir el streaming con VLC Media Player.



Figura 45-3: Transmisión correcta del Streaming en el servidor.
Realizado por: Yautibug, A. 2020.

En la misma máquina del servidor se comprobó que la transmisión de streaming es correcta con la ayuda de otro reproductor SMPlayer.



Figura 46-3: Reproducción de video en SMPlayer.
Realizado por: Yautibug, A. 2020.

3.2.2.1 Pruebas en el receptor VLC

Abrir el reproductor VLC en el receptor, una vez que está ejecutando escoger la opción *medio* y luego se da clic *abrir ubicación de red* y se desplegara la ventana de configuración de los parámetro a conectarse con servidor streaming: el protocolo, dirección IPv6 del servidor, el puerto por el que está trasmitiendo el servidor y la ruta, para este trabajo es `http://[200:1:db9:fe:1::10]:8080/leonel`

Prueba de conectividad streaming desde el Cliente1 al Servidor.



Figura 47-3: Reproducción de video con Reproductor VLC en Cliente1.
Realizado por: Yautibug, A. 2020.

En la siguiente **Figura 48-3** se visualiza la captura en Wireshark de paquetes streaming con el protocolo TCP a nivel de transporte.

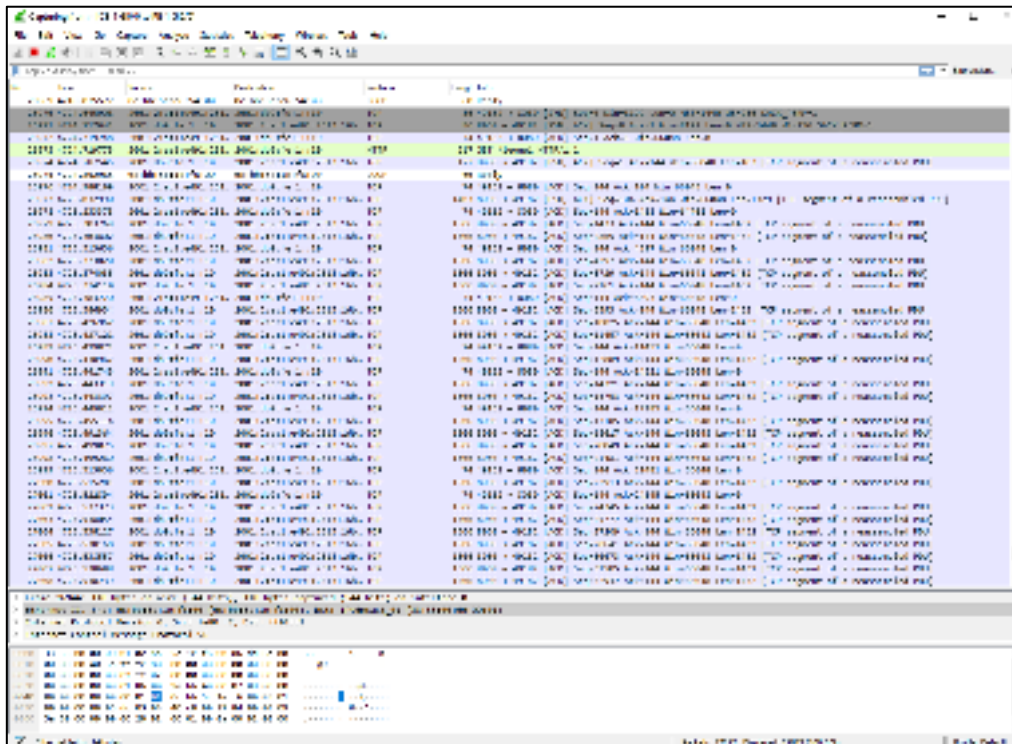


Figura 48-3 Tráfico de streaming en Wireshark capturado entre el enlace CE1-PE1. Realizado por: Yautibug, A. 2020.

Prueba de conectividad streaming desde el Cliente2 al Servidor.

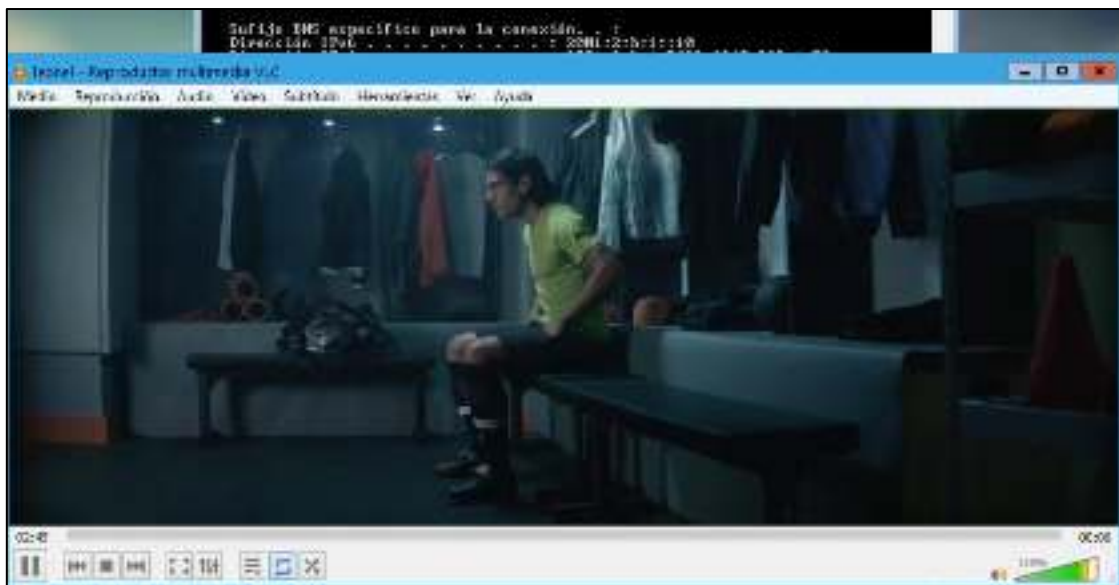


Figura 49-3: Reproducción de video con Reproductor VLC en Cliente2. Realizado por: Yautibug, A. 2020.

Se visualiza la captura en Wireshark de paquetes streaming con el protocolo TCP a nivel de transporte en el enlace PE2-CE2 del escenario **Figura 2-2**.

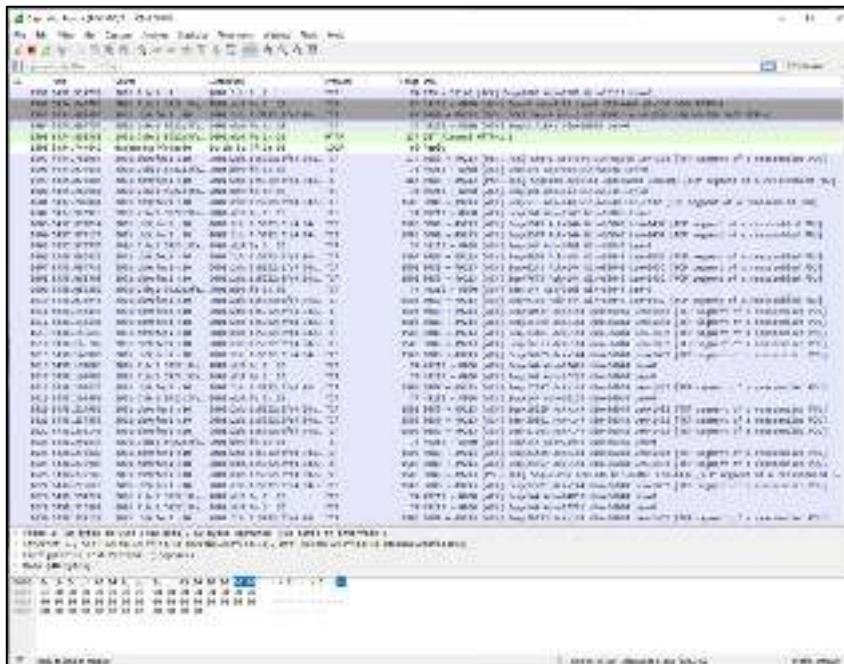


Figura 50-3 Tráfico de streaming en Wireshark capturado entre el enlace PE2-CE2.
Realizado por: Yautibug, A. 2020.

En el enlace PE4-CE4 se aplica el método HUB and SPOKE para crear un enlace dedicado para el cliente2 con dirección IPv6 2001:db7:fe:1::/64

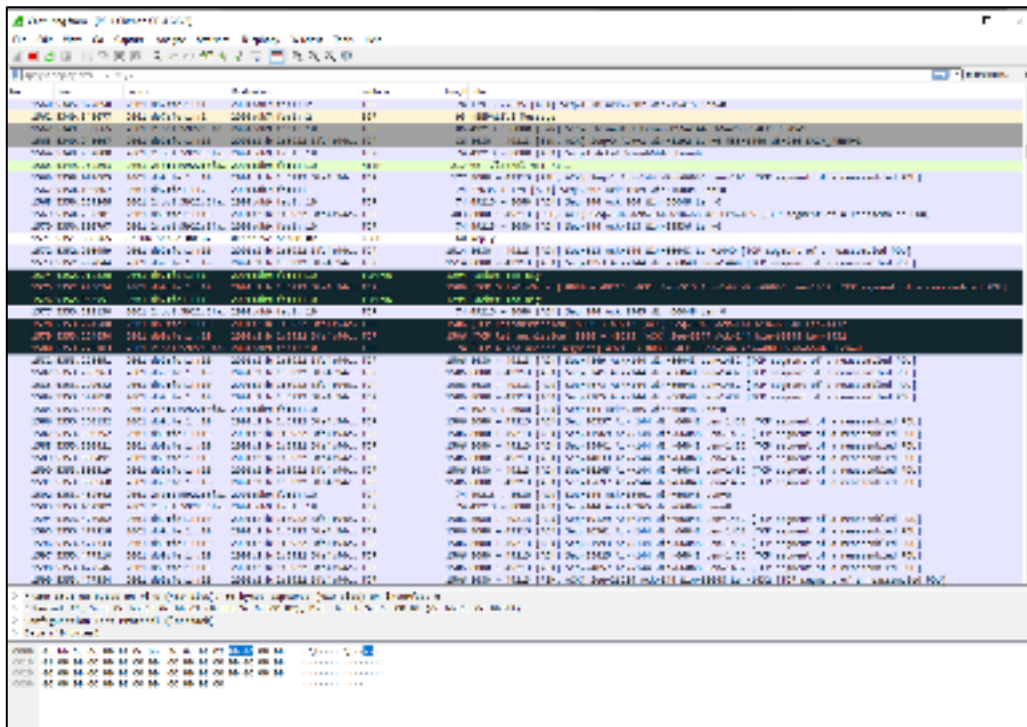


Figura 51-3: Tráfico de streaming capturado entre el enlace PE4-CE4 método HUB and SPOKE
Realizado por: Yautibug, A. 2020.

Prueba de conectividad streaming desde máquina Ubuntu Cliente3 al Servidor VLC.

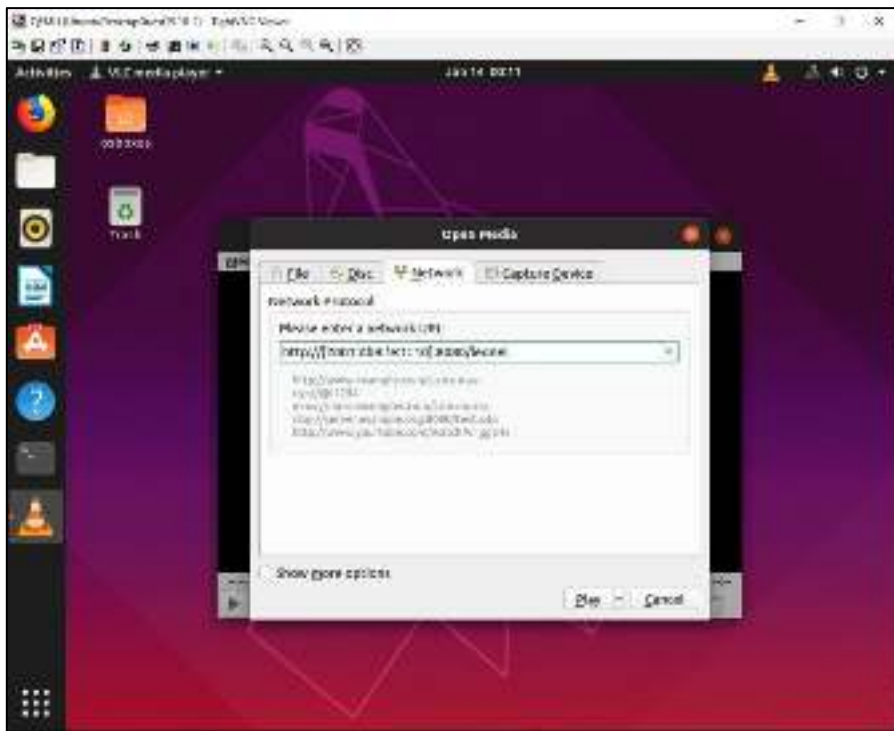


Figura 52-3: Ventana configuración parámetros de recepción en VLC.
Realizado por: Yautibug, A. 2020.

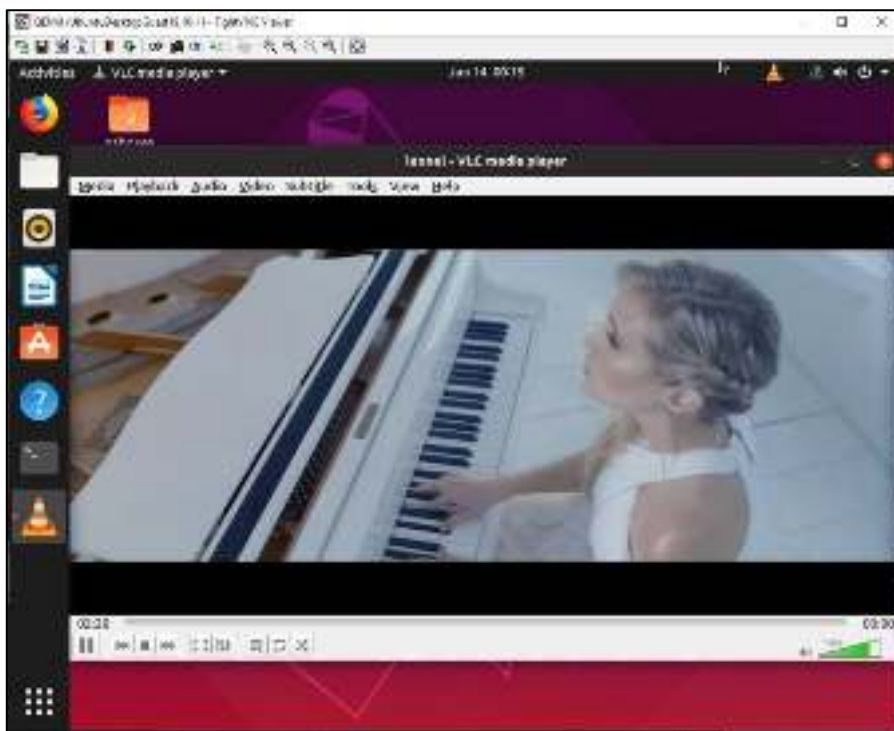


Figura 53-3: Reproducción de video con Reproductor VLC en Cliente3.
Realizado por: Yautibug, A. 2020.

Se visualiza la captura en Wireshark de paquetes streaming con el protocolo TCP a nivel de transporte en el enlace PE3-CE3 del escenario **Figura 2-2**.

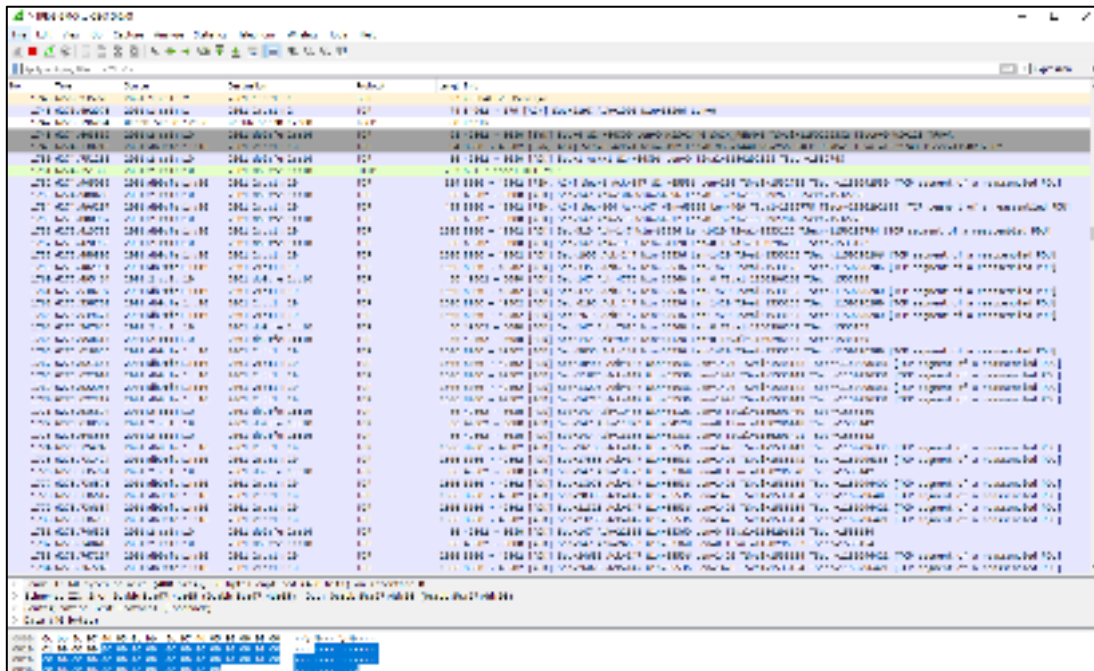


Figura 54-3: Tráfico de streaming en Wireshark capturado entre el enlace PE3-CE3.
Realizado por: Yautibug, A. 2020.

En el enlace PE4-CE4 se aplica el método HUB and SPOKE para crear un enlace dedicado para el cliente3 con dirección IPv6 2001:db8:fe:1::/64

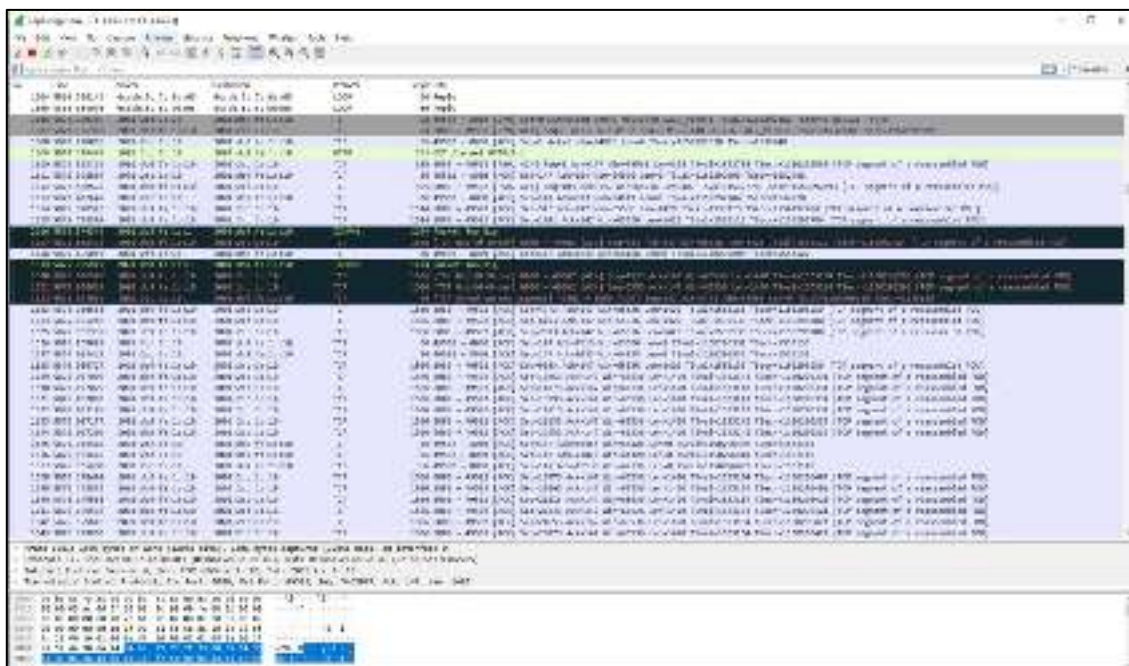


Figura 55-3: Tráfico de streaming capturado entre el enlace PE4-CE4 método HUB and SPOKE.
Realizado por: Yautibug, A. 2020.

3.2.3 Evaluación de rendimiento con D-ITG

Mediante D-ITG se realizó la evaluación de rendimiento de esta técnica 6VPE, con los parámetros de Latencia Jitter, Perdida de paquetes, Mínimo delay ,Máximo delay, Promedio delay o latencia. Desviación Estándar del delay, Bytes recibidos, Velocid. Promedio de Bits, Velocidad promedio de paquetes, Paquetes y Tamaño Promedio de loss-burst.

3.2.3.1 Parámetros de configuración en el emisor D-ITG en el emisor

En el servidor se realizó las configuraciones con los parámetros resumidos en la **Tabla 3-3**, para ver las configuración del emisor o servidor D-ITG observar en el **Capítulo II** la sección **2.7.3**.

Tabla 3-3: Parámetro del flujo en el emisor o servidor del Software D-ITG.

Parámetro	Valor
Direcciones de Destinos	2001:2:a:1::10 2001:2:b:1::10 2001:2:c:1::10
Tiempos de transmisión	30s, 45s y 60s
Meter	Round-Trip-time
TTL	64
Protocolo	UDP
Numero de paquete por segundo	1000 paquetes/seg
Tamaño del paquete	512 Bytes

Realizado por: Yautibug, A. 2020.

3.2.3.2 Resultados obtenidos en el receptor D-ITG

Los Resultados obtenidos por el programa D-ITG luego de la recepción del streaming en el cliente con tiempo de recepción de 30 segundos con se muestra en la **Figura 56-3**.

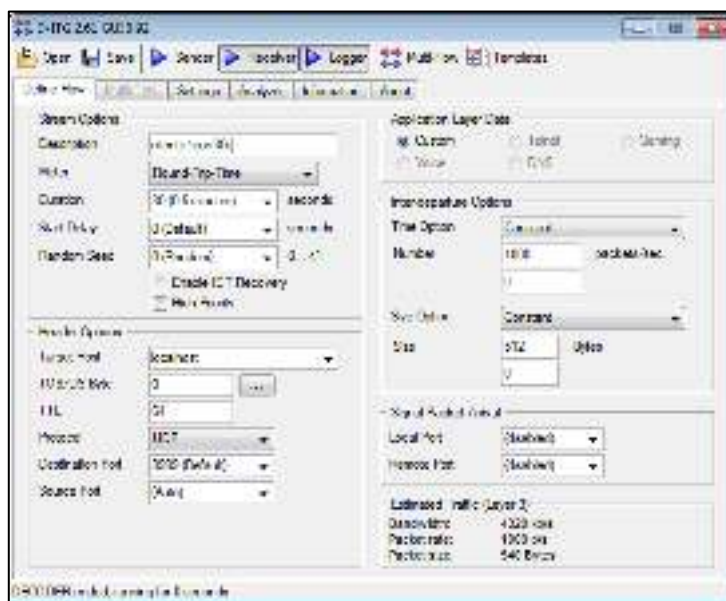


Figura 56-3: D-ITG, Configuración en el receptor cliente 1 con 30s.

Realizado por: Yautibug, A. 2020.

```

ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db9:fe:1:c94d:a60c:1d96:8bf2:61413
To 2001:2:a:1::10:8999
-----
Total time           = 39.074000 s
Total packets        = 5540
Minimum delay        = 0.110807 s
Maximum delay        = 18.999915 s
Average delay        = 10.760123 s
Average jitter        = 0.011312 s
Delay standard deviation = 6.121328 s
Bytes received       = 2836480
Average bitrate      = 580.740134 Kbit/s
Average packet rate  = 141.782259 pkt/s
Packets dropped      = 24445 (81.52 %)
Average loss-burst size = 9.778000 pkt

```

Figura 57-3: Resultado de tráfico en el cliente 1 con tiempo de recepción 30 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 1 con tiempo de recepción 45 segundos

```

ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db9:fe:1:5950:cd7b:d17b:f949:62214
To 2001:2:a:1::10:8999
-----
Total time           = 59.813000 s
Total packets        = 7689
Minimum delay        = -0.026345 s
Maximum delay        = 21.078933 s
Average delay        = 8.688463 s
Average jitter        = 0.011487 s
Delay standard deviation = 5.403356 s
Bytes received       = 3936768
Average bitrate      = 526.543460 Kbit/s
Average packet rate  = 128.550650 pkt/s
Packets dropped      = 37294 (82.91 %)
Average loss-burst size = 14.305332 pkt

```

Figura 58-3: Resultado de tráfico en el cliente 1 con tiempo de recepción 45 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 1 con tiempo de recepción 60 segundos

```
ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db9:fe:1:5950:cd7b:d17b:f949:55247
To 2001:2:a:1::10:8999
-----
Total time = 74.791000 s
Total packets = 9785
Minimum delay = -0.017887 s
Maximum delay = 18.165698 s
Average delay = 10.779940 s
Average jitter = 0.010905 s
Delay standard deviation = 3.511278 s
Bytes received = 5009920
Average bitrate = 535.884799 Kbit/s
Average packet rate = 130.831250 pkt/s
Packets dropped = 50180 (83.68 %)
Average loss-burst size = 13.669300 pkt
```

Figura 59-3: Resultado de tráfico en el cliente 1 con tiempo de recepción 60 segundos. Realizado por: Yautibug, A. 2020.

En la siguiente **Figura 60-3** se visualiza la captura en Wireshark de paquetes streaming con el protocolo UDP a nivel de transporte.

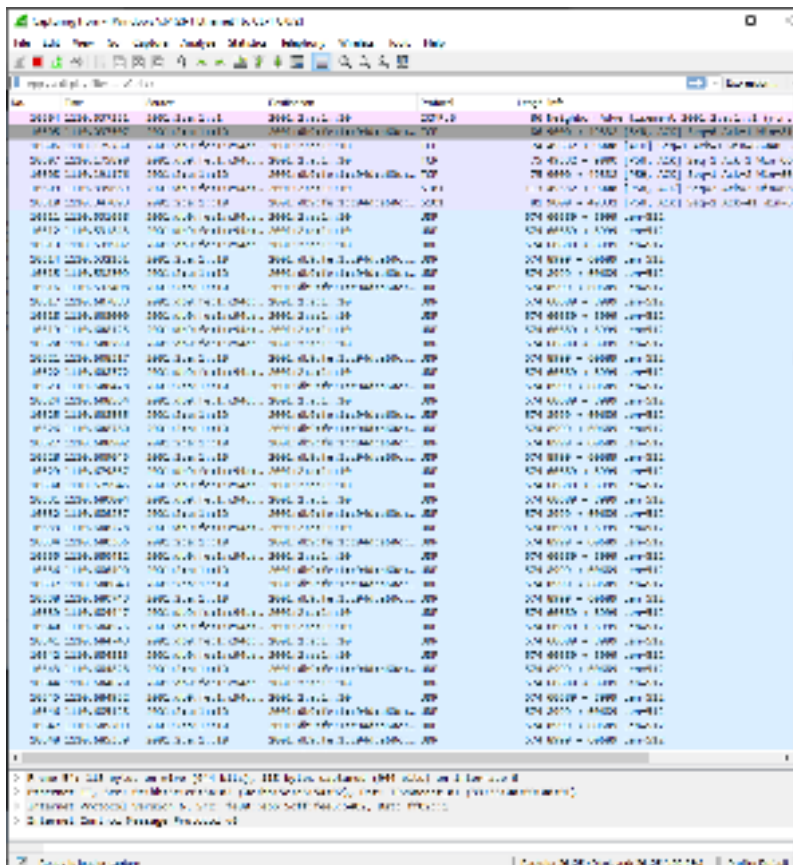


Figura 60-3: Tráfico de streaming en Wireshark capturado entre el enlace CE1-CLIENTE1. Realizado por: Yautibug, A. 2020.

Receptor cliente 2 con tiempo de recepción 30 segundos

```
ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db9:fe:1:c94d:a60c:1d96:8bf2:51073
To 2001:2:b:1::10:8999|
-----
Total time           = 38.393000 s
Total packets        = 6679
Minimum delay        = 1.362997 s
Maximum delay        = 11.695405 s
Average delay        = 9.104033 s
Average jitter       = 0.008164 s
Delay standard deviation = 2.424706 s
Bytes received       = 3419648
Average bitrate      = 712.556560 Kbit/s
Average packet rate  = 173.964004 pkt/s
Packets dropped      = 23302 (77.72 %)
Average loss-burst size = 6.351049 pkt
```

Figura 61-3: Resultado de tráfico en el cliente 2 con tiempo de recepción 30 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 2 con tiempo de recepción 45 segundos

```
ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db9:fe:1:c94d:a60c:1d96:8bf2:60908
To 2001:2:b:1::10:8999
-----
Total time           = 58.093000 s
Total packets        = 9591
Minimum delay        = 1.344998 s
Maximum delay        = 14.668028 s
Average delay        = 8.673474 s
Average jitter       = 0.009010 s
Delay standard deviation = 4.402710 s
Bytes received       = 4910592
Average bitrate      = 676.238721 Kbit/s
Average packet rate  = 165.097344 pkt/s
Packets dropped      = 35392 (78.68 %)
Average loss-burst size = 8.623782 pkt
```

Figura 62-3: Resultado de tráfico en el cliente 2 con tiempo de recepción 45 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 1 con tiempo de recepción 45 segundos

```
ITGDec version 2.8.1 (r1023)
Compile-time options:
-----
Flow number: 1
From 2001:db9:fe:1:c94d:a60c:1d96:8bf2:57320
To 2001:2:b:1::10:8999
-----
Total time           = 70.896000 s
Total packets        = 10431
Minimum delay        = 1.354366 s
Maximum delay        = 12.485875 s
Average delay        = 8.555290 s
Average jitter       = 0.008320 s
Delay standard deviation = 2.873809 s
Bytes received       = 5340672
Average bitrate      = 602.648612 Kbit/s
Average packet rate  = 147.131009 pkt/s
Packets dropped      = 49551 (82.61 %)
Average loss-burst size = 7.800850 pkt
```

Figura 63-3: Resultado de tráfico en el cliente 2 con tiempo de recepción 60 segundos.

Realizado por: Yautibug, A. 2020.

Receptor máquina Ubuntu cliente 3 con tiempo de recepción 30 segundos

```
Flow number: 1
From 2001:db9:fe:1:f4bc:a004:265b:5a85:61127
To 2001:2:c:1::10:8999
-----
Total time           = 37.568611 s
Total packets        = 6995
Minimum delay        = -0.491354 s
Maximum delay        = 8.373659 s
Average delay        = 4.511395 s
Average jitter       = 0.007624 s
Delay standard deviation = 2.887560 s
Bytes received       = 3581440
Average bitrate      = 762.645177 Kbit/s
Average packet rate  = 186.192670 pkt/s
Packets dropped      = 22994 (76.67 %)
Average loss-burst size = 5.926289 pkt
```

Figura 64-3: Resultado de tráfico en el cliente 3 con tiempo de recepción 30 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 3 con tiempo de recepción 45 segundos

Flow number: 1	I
From 2001:db9:fe:1:d0c6:c983:74c8:cdf3:57578	
To 2001:2:c:1::10:8999	
<hr/>	
Total time	= 49.890271 s
Total packets	= 9376
Minimum delay	= -0.898630 s
Maximum delay	= 8.372551 s
Average delay	= 3.732060 s
Average jitter	= 0.007678 s
Delay standard deviation	= 2.520263 s
Bytes received	= 4800512
Average bitrate	= 769.771245 Kbit/s
Average packet rate	= 187.932433 pkt/s
Packets dropped	= 35619 (79.16 %)
Average loss-burst size	= 5.397636 pkt

Figura 65-3: Resultado de tráfico en el cliente 3 con tiempo de recepción 45 segundos.

Realizado por: Yautibug, A. 2020.

Receptor cliente 3 con tiempo de recepción 60 segundos

Flow number: 1	
From 2001:db9:fe:1:c94d:a60c:1d96:8bf2:64518	
To 2001:2:c:1::10:8999	
<hr/>	
Total time	= 66.032413 s
Total packets	= 12154
Minimum delay	= -0.433988 s
Maximum delay	= 6.457468 s
Average delay	= 4.312969 s
Average jitter	= 0.007628 s
Delay standard deviation	= 1.652835 s
Bytes received	= 6222848
Average bitrate	= 753.914354 Kbit/s
Average packet rate	= 184.061122 pkt/s
Packets dropped	= 47833 (79.74 %)
Average loss-burst size	= 4.861571 pkt

Figura 66-3: Resultado de D-ITG con protocolo UDP, cliente3 – servidor con tiempo de 60 s.

Realizado por: Yautibug, A. 2020.

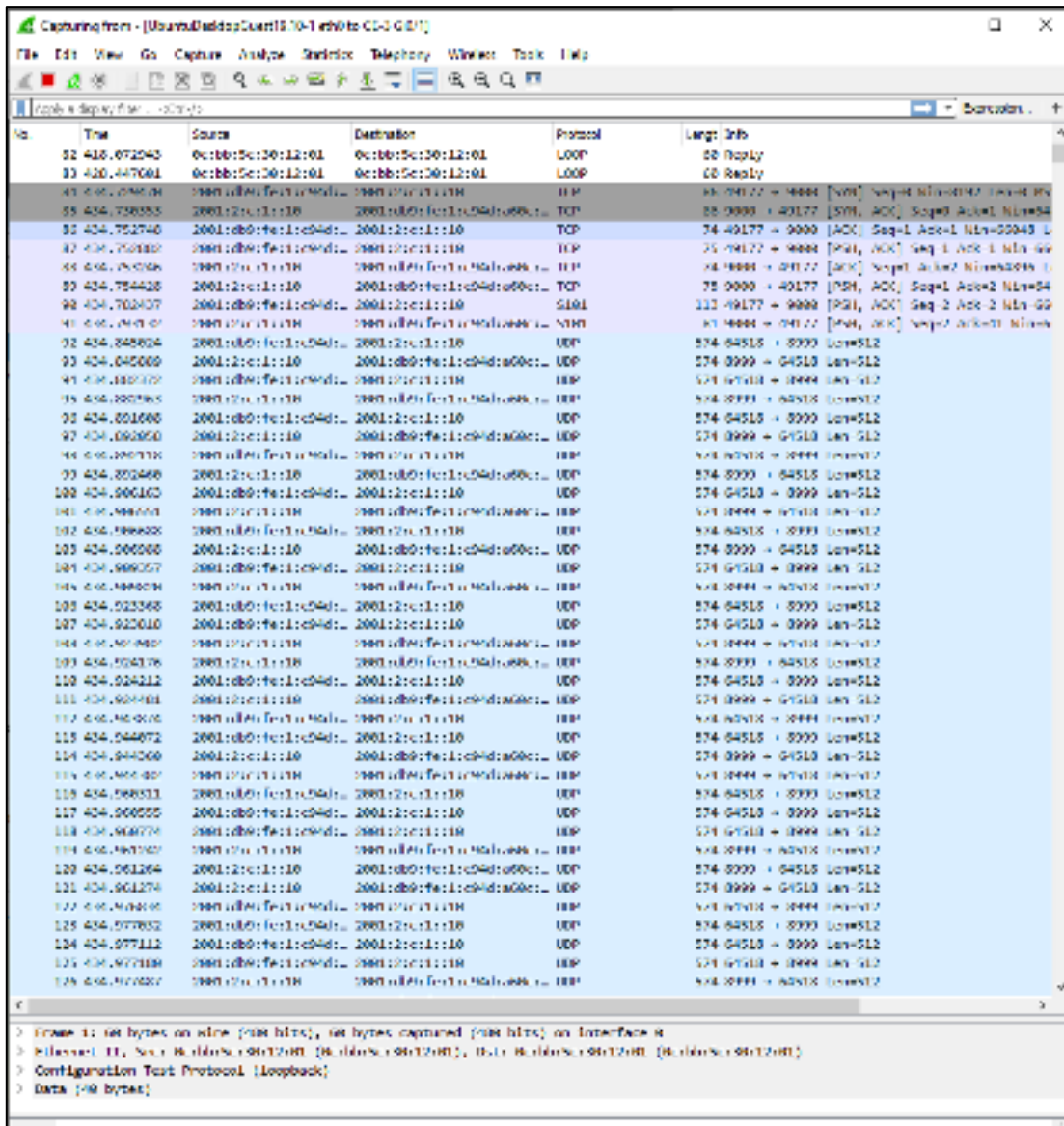


Figura 67-3: Tráfico de streaming en Wireshark capturado entre el enlace CE3-CLIENTE3. Realizado por: Yautibug, A. 2020.

Se ejecutó 9 pruebas con D-ITG con la finalidad de medir Jitter, Latencia y Perdida de paquetes, Mínimo delay ,Máximo delay, Promedio delay o latencia. Desviación Estándar del delay, Bytes recibidos, Velocid. Promedio de Bits, Velocidad promedio de paquetes, Paquetes y Tamaño Promedio de loss-burst, se realizó una inyección de tráfico streaming desde el servidor a cliente1, clientes2 y cliente 3, con los siguientes parámetro constantes de emisión ver en la **Tabla 3-3:** Número de paquete por segundo 1000 [paquet/sec], protocolo UDP, Tamaño del paquete 512 [Bytes], Meter con la opción Round-Trip-time [ida y vuelta] y la variación de Tiempos de recepción 30 , 45 y 60 [segundos], en los 3 clientes se recibió tráfico de streaming para luego comparar con la técnica **6PE** y saber cuál es la mejor técnica para transmisión y recepción de audio y video.

Tabla 4-3: Resumen de los resultados obtenidos por D-ITG en la técnica 6VPE

Parámetro	Servidor – Cliente1			Servidor – Cliente2			Servidor – Cliente3			Suma
Tiempo de emisión [s]	30	45	60	30	45	60	30	45	60	
Tiempo recepción [s]	39,074	59,813	74,791	38,393	58,093	70,896	37,569	49,89	66,032	494,551
Paquetes recibidos [Unid]	5540	7689	9785	6679	9591	10431	6995	9376	12154	78240
Mínimo delay [s]	0,110	-0,263	-0,017	1,362	1,344	1,354	-0,491	-0,898	-0,433	2,067
Máximo delay [s]	18,999	21,078	18,165	11,695	14,668	12,485	8,373	8,372551	6,457	120,292
Promedio delay o latencia [s]	10,760	8,688	10,779	9,104	8,673	8,555	4,511	3,732	4,312	69,114
Promedio Jitter [ms]	11,312	11,487	10,905	8,164	9,01	8,32	7,624	7,678	7,628	82,128
Desviación Estándar del delay [s]	6,121	5,403	3,511	2,424	4,402	2,873	2,887	2,520	1,652	31,793
Bytes recibidos [Unid]	2836480	3936768	5009920	3419648	4910592	5340672	3581440	4800512	6222848	40058880
Velocid. Promedio de Bits [kbits/s]	580,740	526,543	535,884	712,556	676,238721	602,648612	762,645	769,771	753,914	5920,939
Velocidad promedio de paquetes [pkt/s]	141,782	128,550	130,831	173,964	165,097	147,131	186,192	187,932	184,061	1445,540
Paquetes dropeados [%]	24445(81,52)	37294(82,91)	50180(83,67)	23302(77,72)	35392(78,68)	49551(82,61)	22994(76,67)	35619(79,16)	47833(79,74)	326610(80,30)
Tamaño Promedio de loss-burst [pkt]	9,778	14,305	13,669	6,351	8,623	7,800	5,926	5,397	4,861	76,7138
Líneas de Error	0	0	0	0	0	0	0	0	0	0

Realizado por: Yautibug, A. 2020

3.3 Análisis de resultados evaluados entre las técnicas 6PE y 6VPE

Para el análisis final entre las 2 técnicas, se utilizó la **Tabla 2-3** de la técnica 6PE y la **Tabla 4-3** de la técnica 6VPE con la cual se realizó una comparativa entre estas 2 técnicas en los siguientes parámetros evaluados con el software D-IGT: Máximo delay [s], Promedio delay o latencia [s], Promedio Jitter [s], Desviación Estándar del delay [s], Velocid. Promedio de Bits [kbits/s], Velocidad promedios de paquetes [pkt/s], y Paquetes dropeados [%] con estos parámetros se procedió a graficar la comparativa con diagrama de barras, luego las gráficas de la suma total de los parámetros evaluados y por último se realizó las gráficas en diagrama de pastel con porcentajes de diferencias entre la técnica 6PE y 6VPE.

Se observa en la siguiente **Gráfico 1-3**, los diagramas de barras Comparativa del parámetro Máximo delay entre las técnicas 6PE y 6VPE. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 16,277 [s] mientras que la técnica 6VPE 18,999 [s], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 14,183 [s] mientras que la técnica 6VPE 21.078 [s], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 16,813 [s] mientras que la técnica 6VPE 18,165 [s]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 2,654 [s] mientras que la técnica 6VPE 11,695 [s], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 5,003 [s] mientras que la técnica 6VPE 14,668 [s], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 11,463 [s] mientras que la técnica 6VPE 12,485 [s]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 4,507 [s] mientras que la técnica 6VPE 8,373 [s], Cliente 3 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 3,941 [s] mientras que la técnica 6VPE 8,372 [s], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Máximo delay de 5,515 [s] mientras que la técnica 6VPE 6,457 [s]

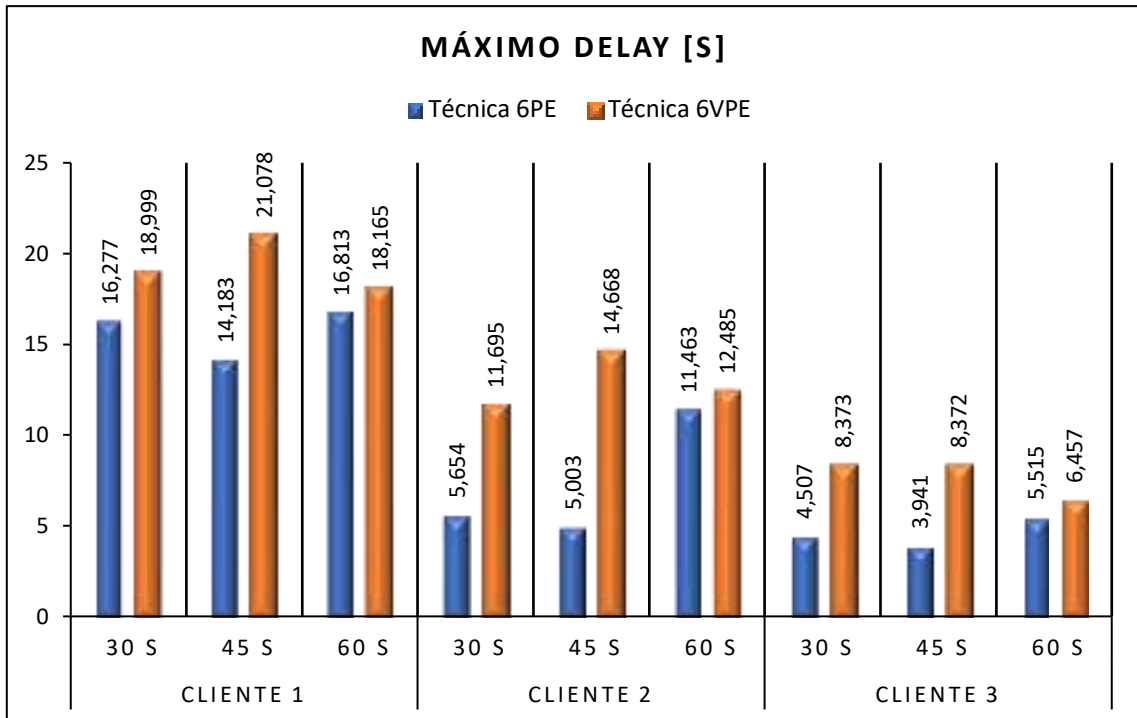


Gráfico 1-3: Diagramas de barras Comparativas de Máximo delay entre las técnicas 6PE y 6VPE
 Realizado por: Yautibug, A. 2020.

De la **Tabla 2-3** técnica 6PE y **Tabla 4-3** técnica 6VPE se realizó la sumatoria total del parámetro Máximo Delay, luego se graficó el diagrama de barras comparativas de la suma total como se muestra en el **Gráfico 2-3**, la técnica 6PE tiene un valor total de Máximo Delay de 83,356 [s] mientras que la técnica 6VPE tiene 120,292 [s]

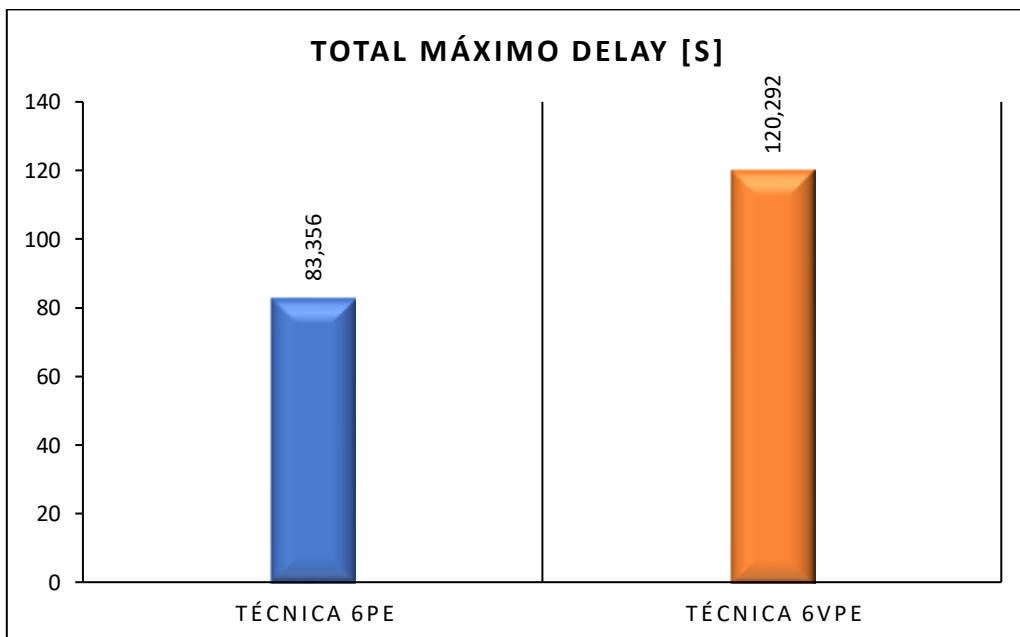


Gráfico 2-3: Diagramas de Barras de la sumatoria total comparativa de Máximo Delay.
 Realizado por: Yautibug, A. 2020.

En la **Gráfica 3-3**, se observa el diagrama de pastel de la sumatoria total comparativa de Máximo Delay de la **Tabla 2-3** y **Tabla 4-3**, expresado en porcentajes para visualizar que, la técnica 6PE tiene un porcentaje de 41% mientras que la técnica 6VPE tiene un valor porcentual de 59%, entonces la técnica 6PE es mejor ya que tiene un 18 % menos de retardo con respecto a 6VPE.

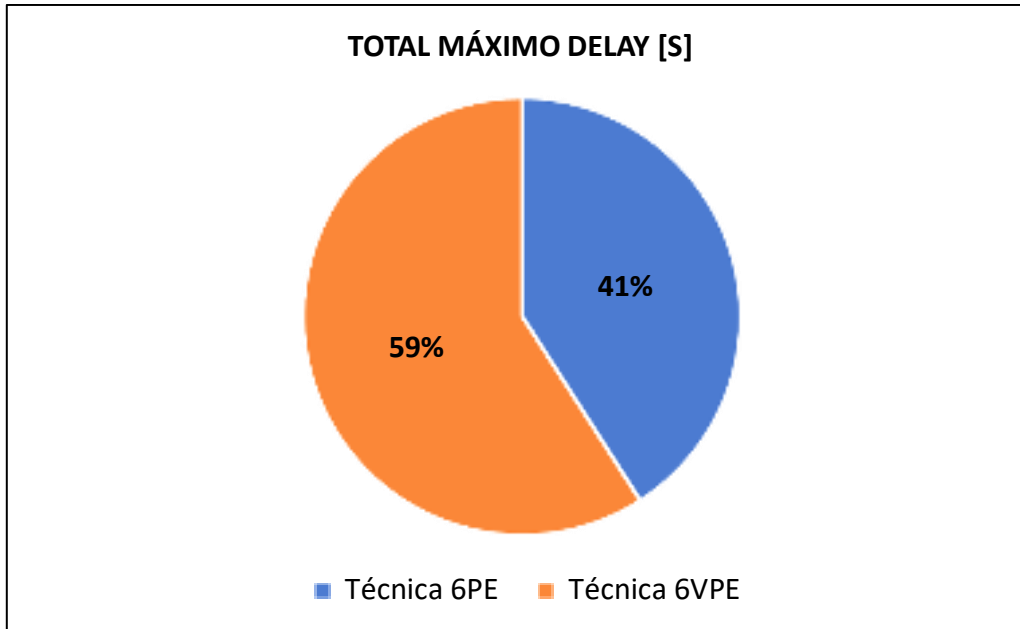


Gráfico 3-3: Diagrama de pastel sumatoria total comparativa de Máximo Delay.
Realizado por: Yautibug, A. 2020.

En la **Gráfico 4-3**, se visualiza el diagrama de barra de la Media Aritmética (Promedio o Media) de parámetro Delay o latencia de la tabla comparativa **Tabla 2-3** y **Tabla 4-3**. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 10,654 [s] mientras que la técnica 6VPE tiene 10,760 [s], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 10,270 [s] mientras que la técnica 6VPE 8,688 [s], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 10,905 [s] mientras que la técnica 6VPE 10,779 [s]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 3,535 [s] mientras que la técnica 6VPE 9,104 [s], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 3,604 [s] mientras que la técnica 6VPE 8,673 [s], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 8,612 [s] mientras que la técnica 6VPE 8,555 [s]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 3,327 [s] mientras que la técnica 6VPE 4,511 [s], Cliente 3 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 2,320 [s] mientras que el la técnica 6VPE 3,732 [s], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Promedio de Delay de 3,532 [s] mientras que el la técnica 6VPE 4,312 [s]

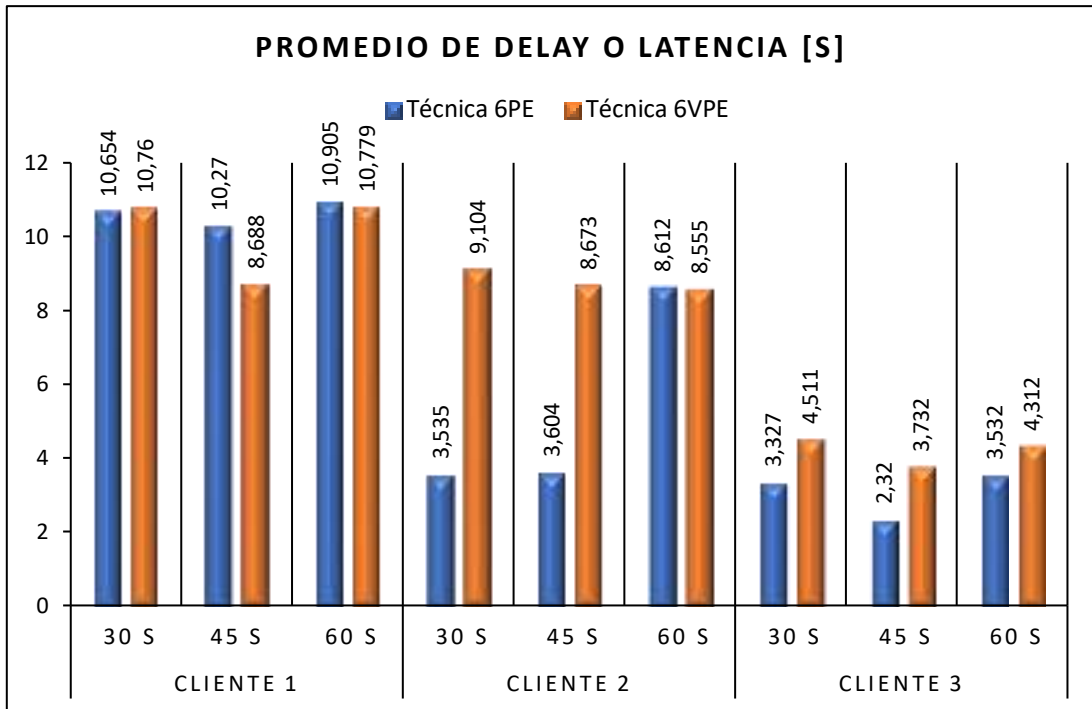


Gráfico 4-3: Diagramas de barras del promedio Delay de la tabla comparativa 6PE y 6VPE
 Realizado por: Yautibug, A. 2020.

En la siguiente **Gráfico 5-3** se observa el diagrama de barra, de la sumatoria total de la Media Aritmética o Promedio de Delay obtenidos de la tabla comparativa 6PE y 6VPE, la técnica 6PE tiene valor total de Promedio de Delay de 56,759 [s] mientras que la técnica 6VPE tiene 69,114 [s]

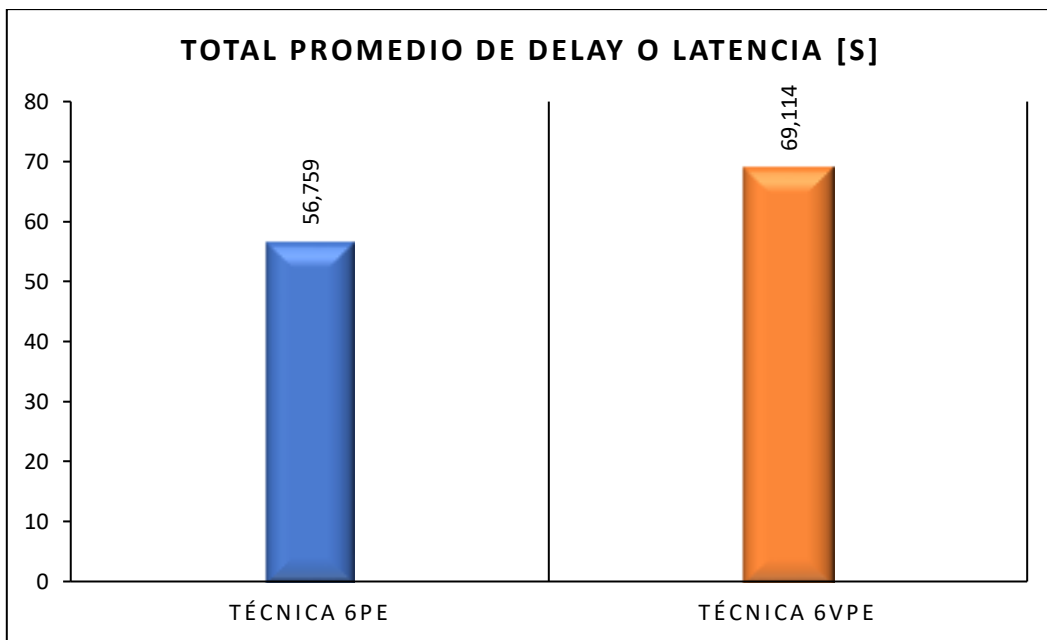


Gráfico 5-3: Diagramas de Barras de la sumatoria total del parámetro promedio delay de las tablas comparativas 6PE y 6VPE.
 Realizado por: Yautibug, A. 2020.

Grafico 6-3, se se realizo el diagrama de pastel, con los datos obtenidos de la sumatoria total de la tablas **Tabla 2-3** y **Tabla 4-3** del parámetro Promedio de Delay , la técnica 6PE tiene un porcentaje de 45% mientras que la técnica 6VPE tiene un valor porcentual de 55%, entonces la técnica 6PE es mejor en un 10 % menos, en promedio de latencia en relación con la técnica 6VPE.

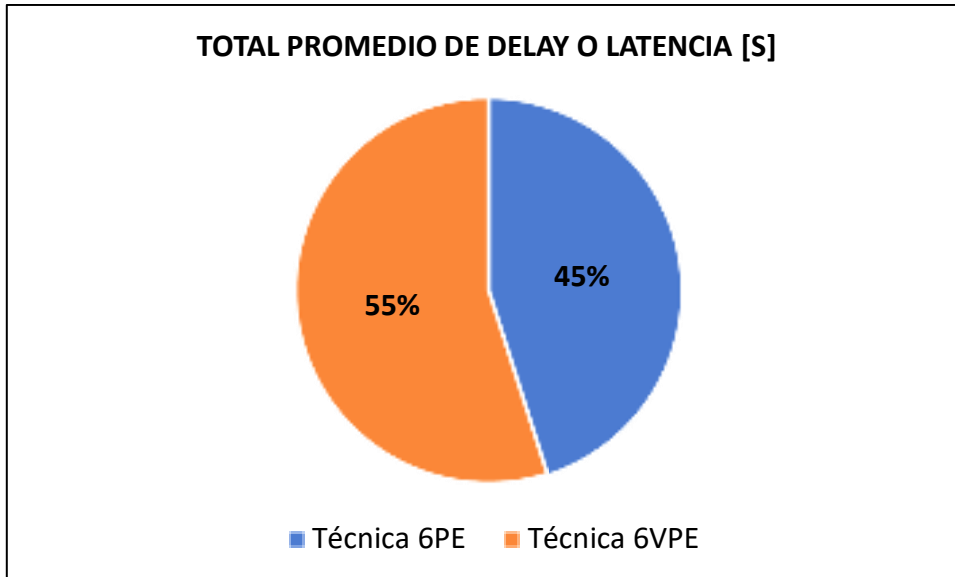


Gráfico 6-3: Diagrama de pastel de la sumatoria comparativa del parámetro promedio de delay entre la técnica 6PE y 6VPE.

Realizado por: Yautibug, A. 2020.

En el **Gráfico 7-3** se observa diagrama de barra comparativa del parámetro Jitter con los datos obtenidos del software D-ITG entre la técnica 6PE y 6VPE. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 9,968 [ms] mientras que la técnica 6VPE tiene 11,312 [ms], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 11,041 [ms] mientras que la técnica 6VPE 11,487 m[s], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 11,251 [ms] mientras que la técnica 6VPE 10,779 [ms]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 6,474 [ms] mientras que la técnica 6VPE 8.164 [ms], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 6.828 [ms] mientras que la técnica 6VPE 9,010 [ms], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 9,553 [ms] mientras que la técnica 6VPE 8,320 [ms]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 5,883 [ms] mientras que la técnica 6VPE 7,624 [ms], Cliente 3 con recepción de 45 segundos se observa que la técnica 6PE tiene una valor Promedio de Jitter de 6,410 [ms] mientras que el la técnica 6VPE 7,678 [ms], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Promedio de Jitter de 7,379 [ms] mientras que el la técnica 6VPE 7,628 [ms]

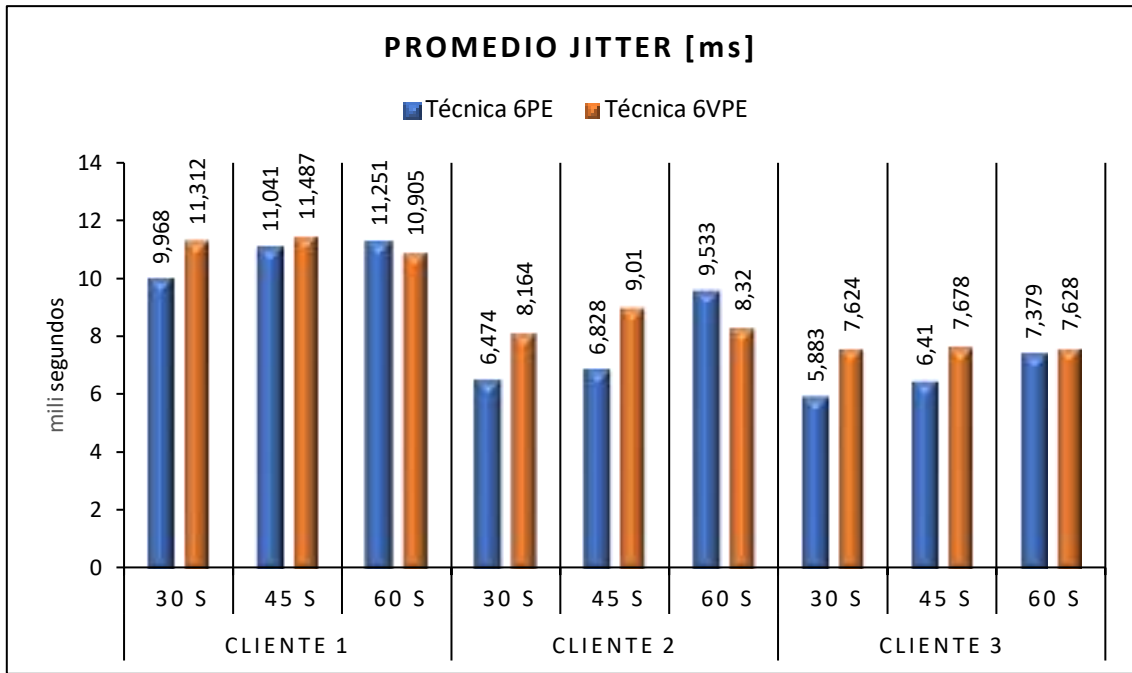


Gráfico 7-3: Diagramas de barras comparativas del parámetro Jitter entre la técnica 6PE y 6VPE.
Realizado por: Yautibug, A. 2020.

Se realizó pruebas con tres clientes en 3 diferentes tiempos de 30 seg, 45 seg y 60 seg, luego se graficó la sumatoria total del parámetro Promedio de Jitter entre las 2 técnicas en estudio, ver la **Gráfico 8-3**, donde la técnica 6PE tiene valor total de Promedio de Jitter de 74,767 [ms] mientras que la técnica 6VPE tiene 82,128 [ms]

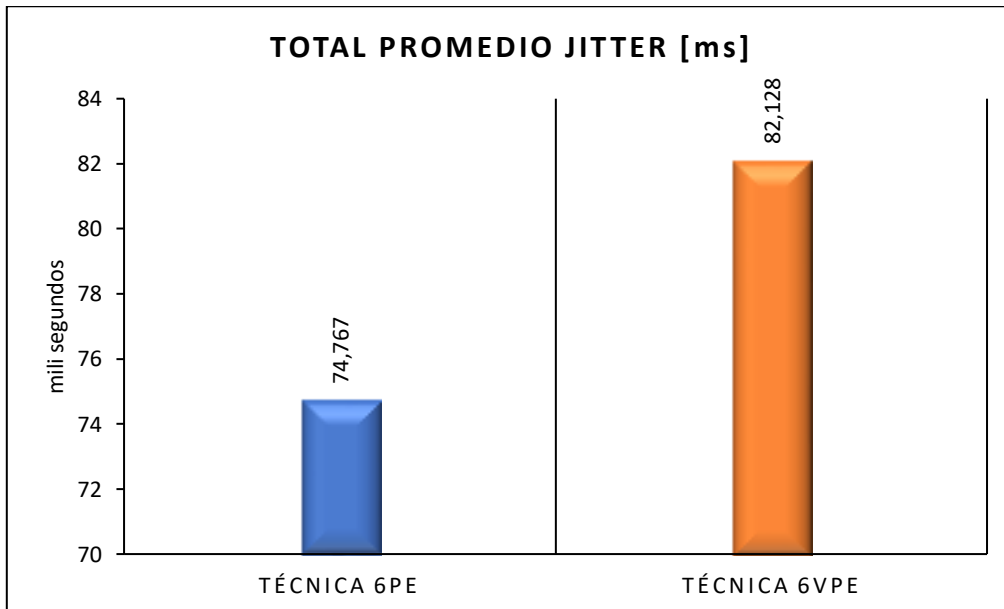


Gráfico 8-3: Diagramas de barras comparativa de Jitter entre las técnicas 6PE Y 6VPE
Realizado por: Yautibug, A. 2020.

Gráfico 9-3. Diagrama de pastel de la sumatoria total de datos obtenidos de la simulación de streaming con el software D-ITG del parámetro Promedio de Jitter, la técnica 6PE tiene un porcentaje de 48% mientras que la técnica 6VPE tiene un valor porcentual de 52%, entonces la técnica 6PE es mejor en un 4 % menos, en promedio de Jitter en relación con la técnica 6VPE.

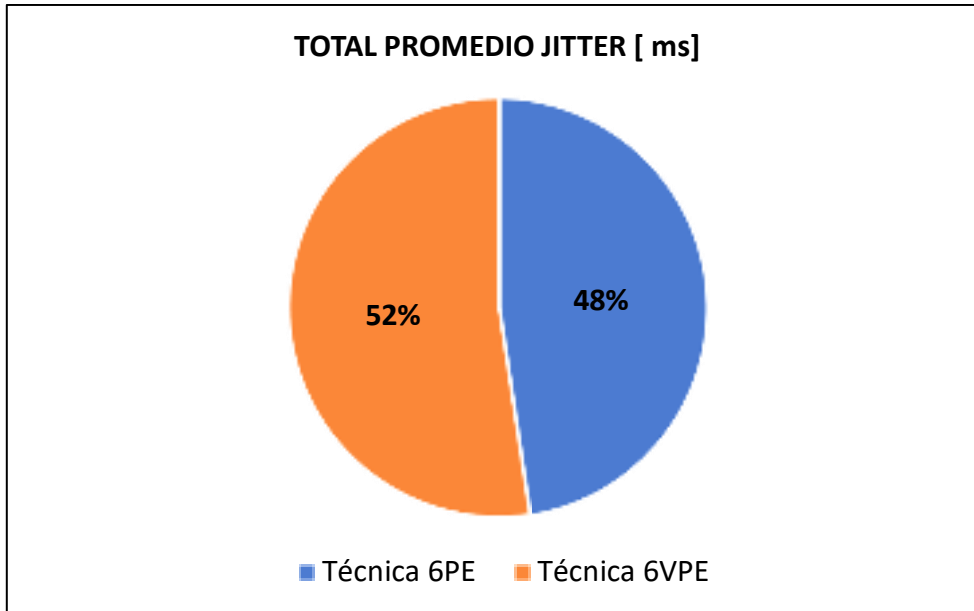


Gráfico 9-3: Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro total promedio de jitter.

Realizado por: Yautibug, A. 2020.

EL parametro de la desviación estándar de delay evalúa la dispersión o separación de datos recibidos en 3 clientes, ver el siguiente **Gráfico 10-3** el Diagrama de barra comparativa del parámetro Desviación Estándar de Delay con los datos obtenidos del software D-ITG entre la técnica 6PE y 6VPE. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 3,974 [s] mientras que la técnica 6VPE tiene 6,121 [s], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 3,626 [s] mientras que la técnica 6VPE 5,403 [s], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 4,395 [s] mientras que la técnica 6VPE 3,511[s]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 1,494 [s] mientras que la técnica 6VPE 2,424 [s], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 0,923 [s] mientras que la técnica 6VPE 4,402 [s], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 2,886 [s] mientras que la técnica 6VPE 2,873 [s]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 1,165 [s] mientras que la técnica 6VPE 2,887 [s], Cliente 3 con recepción de 45 segundos se

observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 1,054 [s] mientras que el la técnica 6VPE 2,520 [s], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Desviación Estándar de Delay de 1,483 [s] mientras que el la técnica 6VPE 1,652 [s]

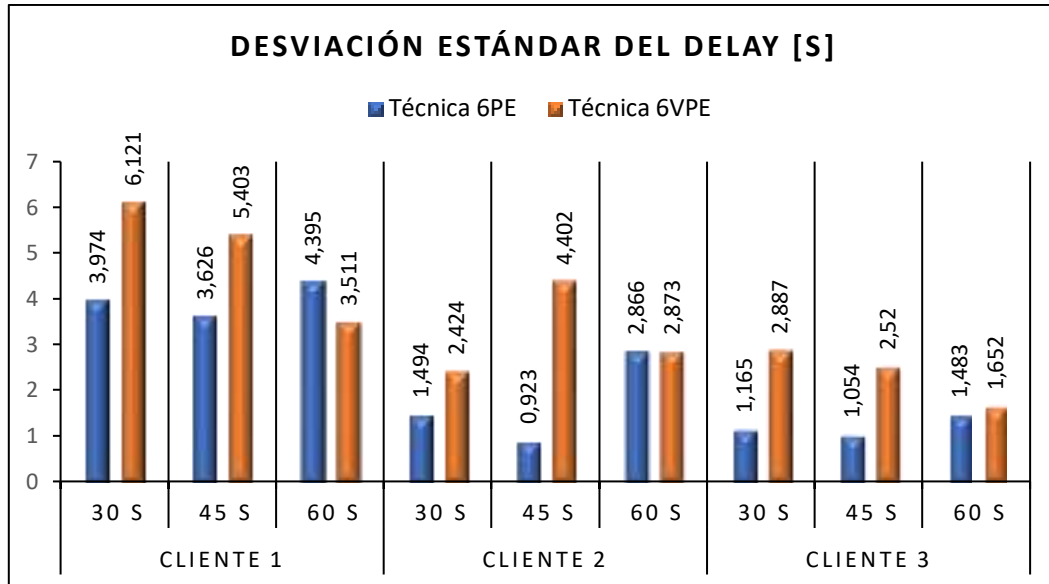


Gráfico 10-3: Diagramas de barras comparativa del parámetro Desviación Estándar de Delay entre la técnica 6PE y 6VPE.

Realizado por: Yautibug, A. 2020.

Gráfico 11-3, se observa los Diagramas de Barras de la sumatoria total del parámetro Desviación Estándar de Delay entre la técnica 6PE y 6VPE, la técnica 6PE tiene valor total de Desviación Estándar de Delay de 20,980 [s] mientras que la técnica 6VPE tiene 31,793 [s]

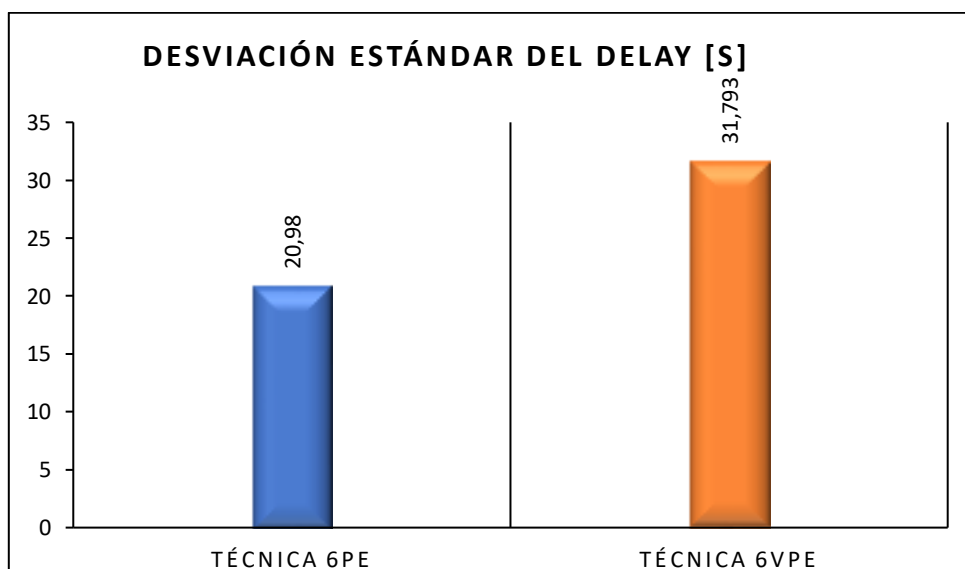


Gráfico 11-3: Diagramas de barras comparativas del parámetro de desviación estándar de delay entre las técnicas 6PE Y 6VPE.

Realizado por: Yautibug, A. 2020.

Gráfico 12-3. Diagrama de pastel de la sumatoria de los datos obtenido de la simulación de streaming con el software D-ITG, del parámetro Promedio Desviación Estándar de Delay, la técnica 6PE tiene un porcentaje de 40% mientras que la técnica 6VPE tiene un valor porcentual de 60%, entonces la técnica 6PE es mejor en un 20 % menos, en la dispersión o separación de datos recibidos en relación con la técnica 6VPE.

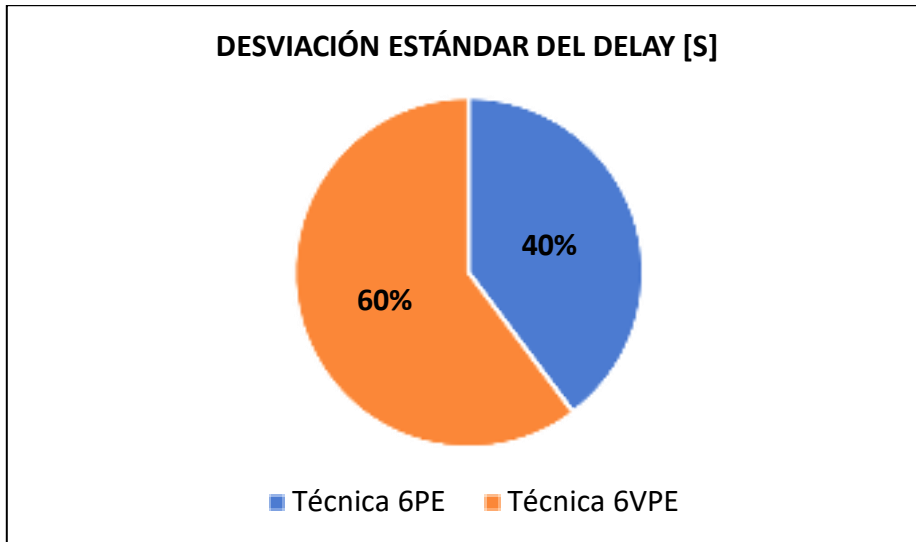


Gráfico 12-3: Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro desviación estándar de delay.

Realizado por: Yautibug, A. 2020.

El parametro velocidad promedio de bit (*average Bitrate*) evalúa el número de bits recibido o procesado por unidad de tiempo, ver el siguiente **Gráfico 13-3** el Diagrama de barra comparativa del parámetro Velocidad Promedio de Bits con los datos obtenidos del software D-ITG entre la técnica 6PE y 6VPE. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 576,243 [Kbits/s] mientras que la técnica 6VPE tiene 580,740 [Kbits/s], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 579,794 [Kbits/s] mientras que la técnica 6VPE 526,543 [Kbits/s], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 602,625 [Kbits/s] mientras que la técnica 6VPE 535,884 [Kbits/s]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 738,145 [Kbits/s] mientras que la técnica 6VPE 712,556 [Kbits/s], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 742,316 [Kbits/s] mientras que la técnica 6VPE 676,238 [Kbits/s], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 662,232 [Kbits/s] mientras que la técnica 6VPE 602,648 [Kbits/s]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 790,778 [Kbits/s] mientras que la técnica 6VPE 762,645 [Kbits/s], Cliente 3 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 756,652

[Kbits/s] mientras que el la técnica 6VPE 769,771 [Kbits/s], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Bits de 688,782 [Kbits/s] mientras que el la técnica 6VPE 735,914 [Kbits/s]

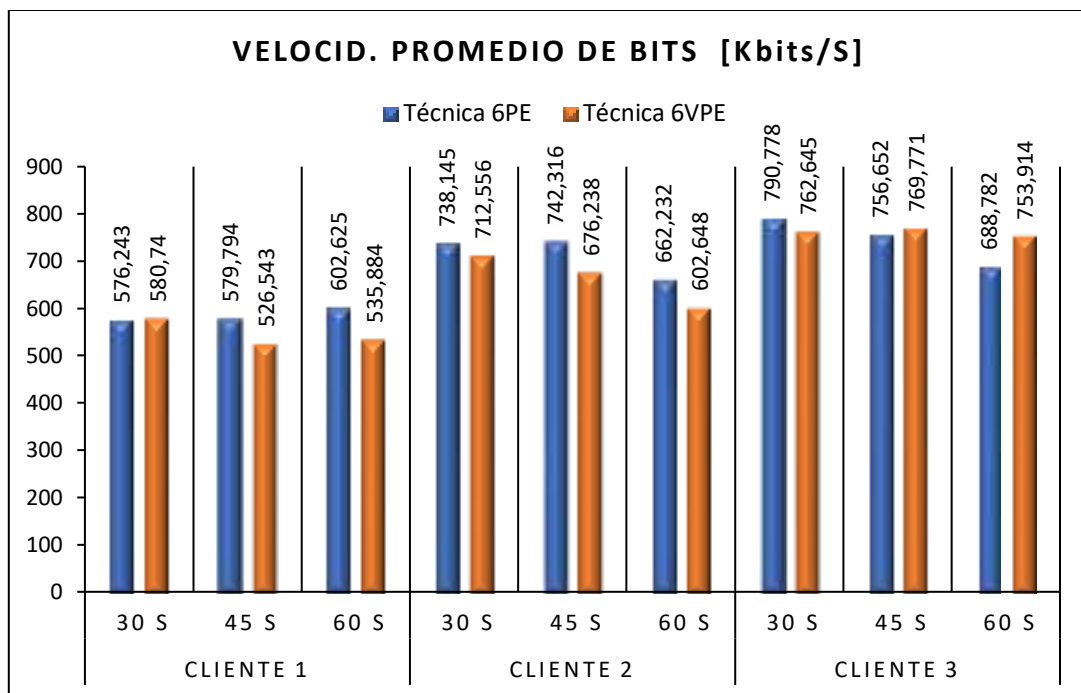


Gráfico 13-3: Diagrama de barras comparativas del parámetro Velocidad Promedio de Bits entre la técnica 6PE y 6VPE.
Realizado por: Yautibug, A. 2020.

En el **Gráfico 14-3**, se observa el diagrama de Barras de la sumatoria total de la velocidad promedio de bits con los datos de la **Tabla 2-3** y **Tabla 4-3**, la técnica 6PE tiene valor total de Velocidad Promedio de Bits de 613,756 [Kbits/s] mientras que la técnica 6VPE tiene 5920,939 [Kbits/s].

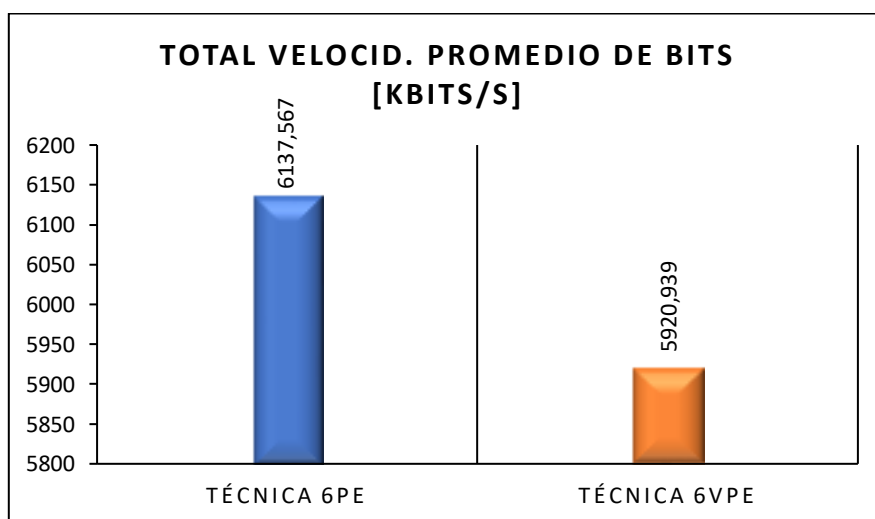


Gráfico 14-3: Diagramas de Barras de la sumatoria total comparativa del parámetro velocidad promedio de bits entre 6PE y 6VPE.
Realizado por: Yautibug, A. 2020.

Gráfico 15-3. Diagrama de pastel de la sumatoria de los datos obtenido de la simulación de streaming con el software D-ITG, del parámetro de Velocidad Promedio de Bits , la técnica 6PE tiene un porcentaje de 51% mientras que la técnica 6VPE tiene un valor porcentual de 49%, entonces la técnica 6PE es mejor en un 2% más, en relación con la técnica 6VPE.

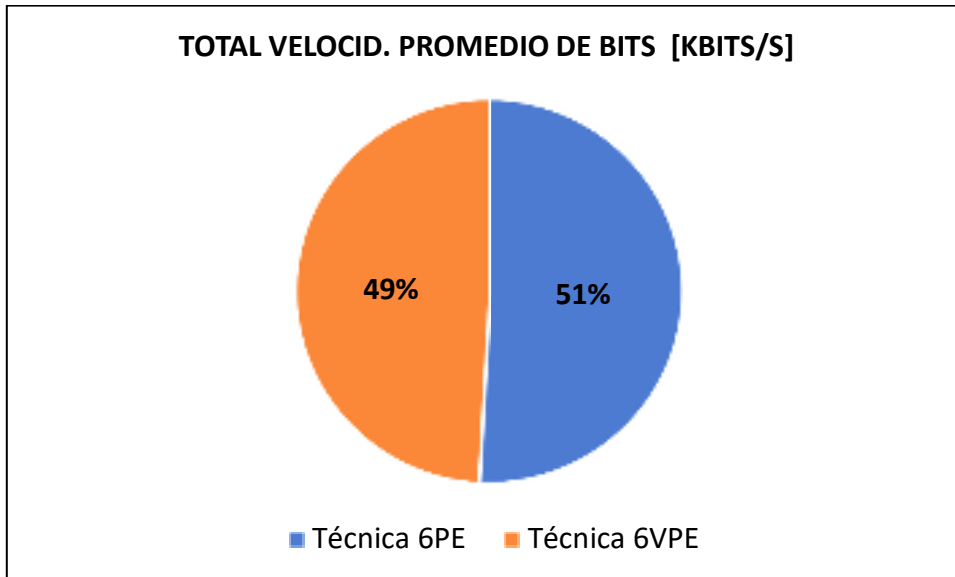


Gráfico 15-3: Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro velocidad promedio de bits.

Realizado por: Yautibug, A. 2020.

El parámetro velocidad promedio de paquete (average packet rate) se evalúa el número de paquetes recibido por unidad de tiempo, ver el siguiente **Gráfico 16-3**. Diagrama de barra comparativa del parámetro velocidad promedio de paquete con los datos obtenidos del software D-ITG entre la técnica 6PE y 6VPE. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Paquetes de 140,684 [Pkt/s] mientras que la técnica 6VPE tiene 141,782 [Pkt/s], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Paquetes de 141,551 [Pkt/s] mientras que la técnica 6VPE 128,550 [Pkt/s], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor Velocidad Promedio de Paquetes de 147,125 [Pkt/s] mientras que la técnica 6VPE 130,831 [Pkt/s]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor Velocidad Promedio de Paquetes de 180,211 [Pkt/s] mientras que la técnica 6VPE 173,964 [Pkt/s], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Paquetes de 181,229 [Pkt/s] mientras que la técnica 6VPE 165,097 [Pkt/s], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Paquetes de 161,677 [Pkt/s] mientras que la técnica 6VPE 147,131 [Pkt/s]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Paquetes de 193,061 [Pkt/s] mientras que la técnica 6VPE 186,192 [Pkt/s], Cliente 3 con recepción de 45 segundos se observa que la técnica 6PE tiene un

valor de Velocidad Promedio de Paquetes de 184,729 [Pkt/s] mientras que el la técnica 6VPE 187,932 [Pkt/s], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Velocidad Promedio de Paquetes de 168,159 [Pkt/s] mientras que el la técnica 6VPE 184,061 [Pkt/s]

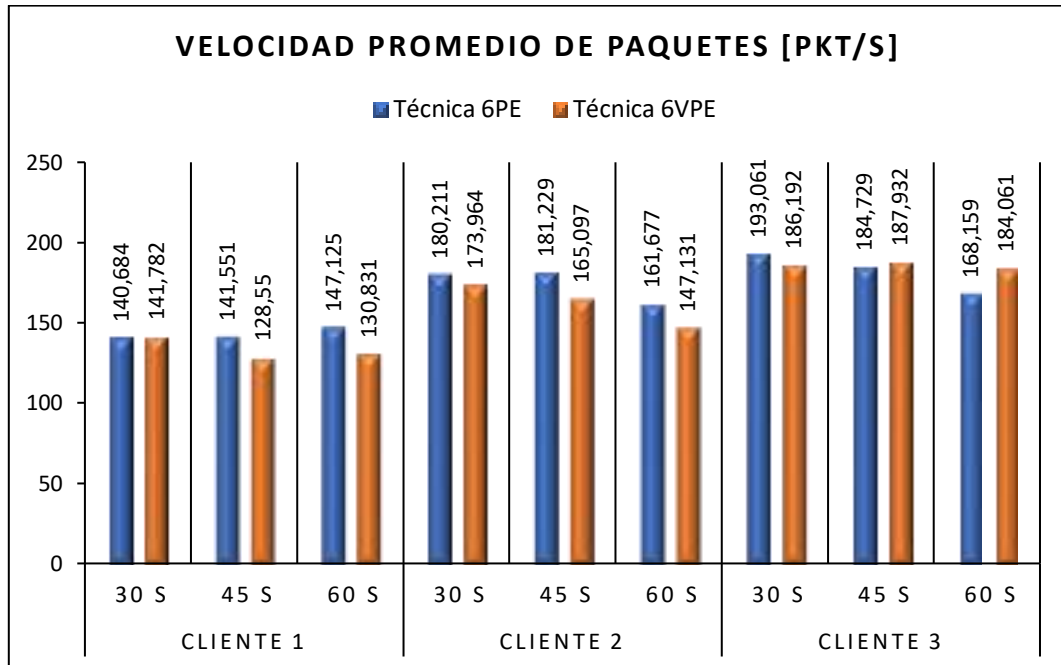


Gráfico 16-3: Diagrama de barras comparativas del parámetro Velocidad Promedio de Paquetes entre la técnica 6PE y 6VPE.

Realizado por: Yautibug, A. 2020.

Gráfico 17-3, se observa el diagrama de Barras de la sumatoria total del parámetro Velocidad Promedio de Paquetes con los datos de la **Tabla 2-3** y **Tabla 4-3**, la técnica 6PE tiene valor total de Velocidad Promedio de Paquetes de 1498,426 [Pkt/s] mientras que la técnica 6VPE tiene 1445,540 [Kbits/s].

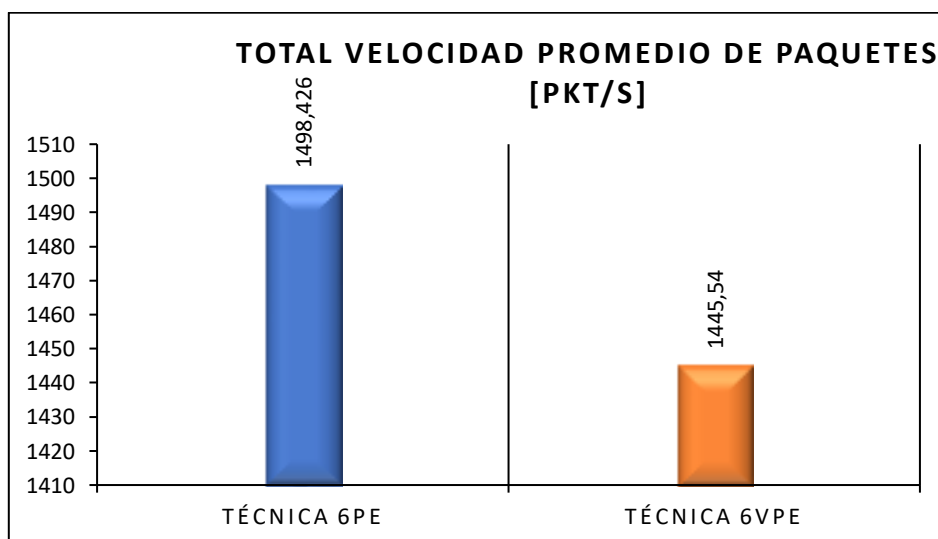


Gráfico 17-3: Diagramas de Barras de la sumatoria total comparativa del parámetro velocidad promedio de paquetes entre 6PE y 6VPE.

Realizado por: Yautibug, A. 2020.

Gráfico 18-3. Diagrama de pastel de la sumatoria de los datos obtenido de la simulación de streaming con el software D-ITG, del parámetro de Velocidad Promedio de Paquetes, la técnica 6PE tiene un porcentaje de 51% mientras que la técnica 6VPE tiene un valor porcentual de 49%, entonces la técnica 6PE es mejor en un 2% más, en relación con la técnica 6VPE.

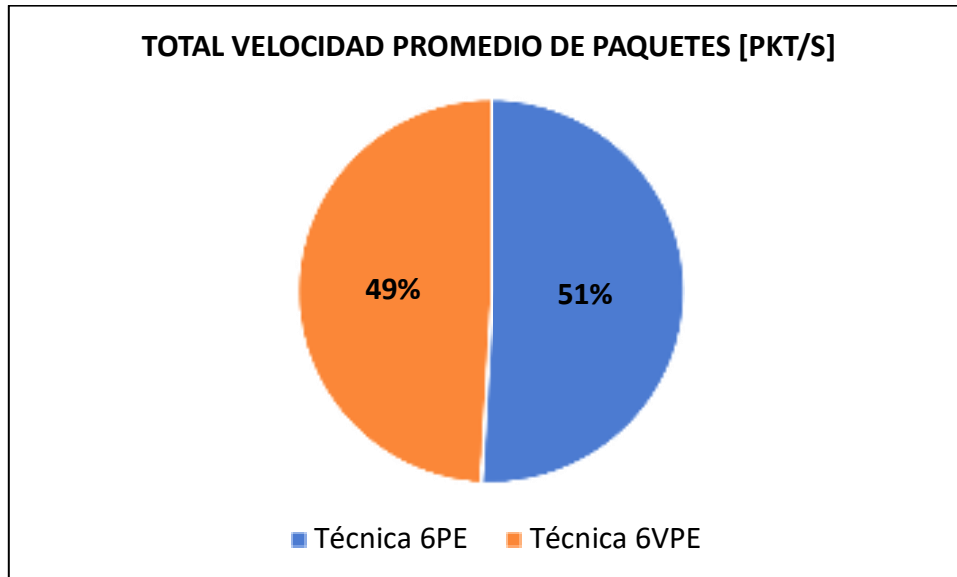


Gráfico 18-3: Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro Velocidad Promedio de Paquetes.

Realizado por: Yautibug, A. 2020.

Para este parámetro se recibió desde el Servidor paquetes de tráfico UDP protocolo en tiempo real, lo cual no es necesario que lleguen todos los paquetes enviados mientras la información se mantenga legible, con UDP el porcentaje de paquetes perdidos se incrementa de forma directamente proporcional a la velocidad de transmisión de recepción, ver la **Gráfico 19-** de paquetes perdidos o dropeados en diagramas de barras comparativas entre las 2 técnicas 6PE y 6VPE, el porcentaje y las unidades de los paquetes dropeados son considerable se debe a la distancia del que existe entre el enlace del servidor- clientes y en los recursos de hardware y software de la maquina física. ver el **Gráfico 16-3.** Diagrama de barra comparativa del parámetro paquetes dropeados con los datos obtenidos del software D-ITG entre la técnica 6PE y 6VPE. Cliente 1 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 24558 [Unida.] mientras que la técnica 6VPE tiene 24445 [Unida.], Cliente 1 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 33624 [Unida.] mientras que la técnica 6VPE 37294 [Unida.], Cliente 1 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 48663 [Unida.] mientras que la técnica 6VPE 50180 [Unida.]. Cliente 2 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 23803 [Unida.] mientras que la técnica 6VPE 23302 [Unida.], Cliente 2 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 36372 [Unida.] mientras que la técnica 6VPE 35392

[Unida.], Cliente 2 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 48727 [Unida.] mientras que la técnica 6VPE 49551 [Unida.]. Cliente 3 con recepción de 30 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 23361 [Unida.] mientras que la técnica 6VPE 22994 [Unida.], Cliente 3 con recepción de 45 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 36217 [Unida.] mientras que el la técnica 6VPE 35619 [Unida.], Cliente 3 con recepción de 60 segundos se observa que la técnica 6PE tiene un valor de Paquetes Dropeados de 49225 [Unida.] mientras que el la técnica 6VPE 47833 [Unida.]

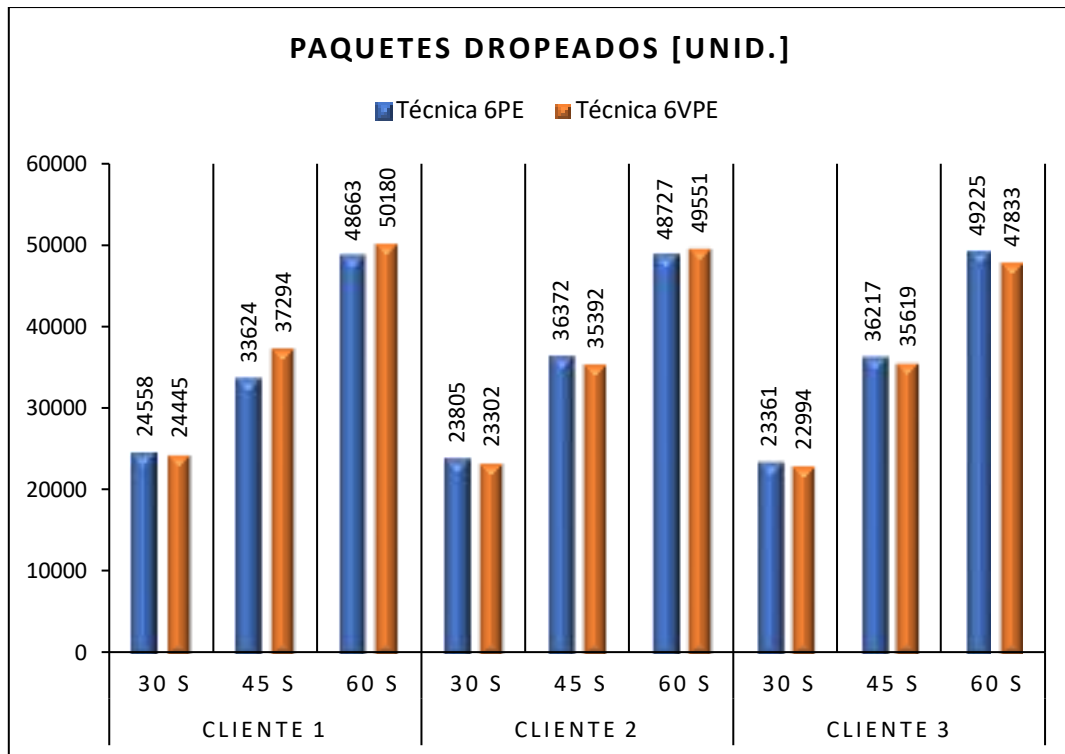


Gráfico 19-3: Diagrama de barras comparativas del parámetro Paquetes Dropeados entre la técnica 6PE y 6VPE.

Realizado por: Yautibug, A. 2020.

Gráfico 20-3, se observa el diagrama de Barras de la sumatoria total del parámetro paquetes dropeados con los datos de la **Tabla 2-3** y **Tabla 4-3**, la técnica 6PE tiene valor total de Paquetes Dropeados de 324552 [Unida.] mientras que la técnica 6VPE tiene 326610 [Unida.].

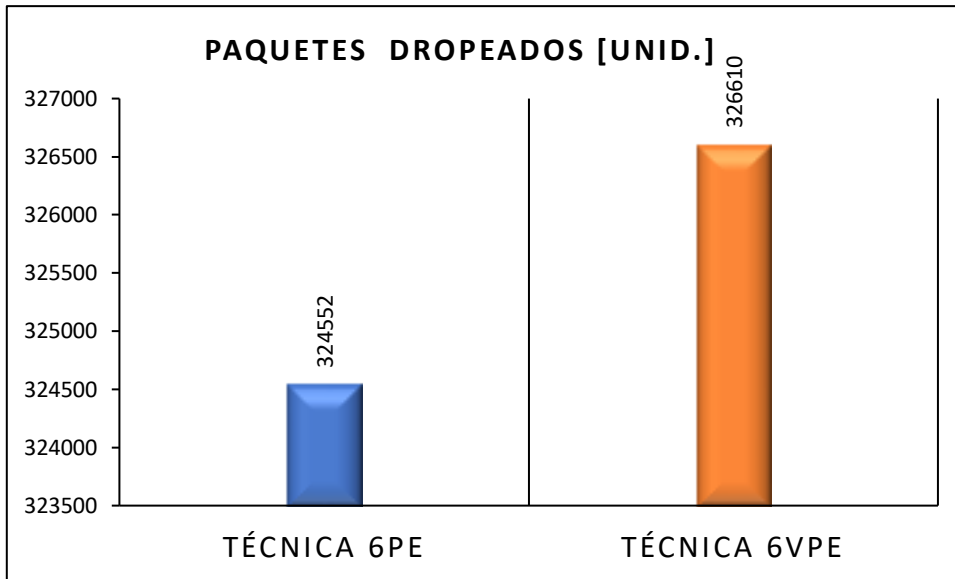


Gráfico 20-3: Diagramas de Barras de la sumatoria total comparativa del parámetro Paquetes Dropeados entre 6PE y 6VPE.
Realizado por: Yautibug, A. 2020.

Gráfico 21-3. Diagrama de pastel de la sumatoria paquetes dropeados con los datos obtenido de la simulación de streaming con el software D-ITG, del parámetro de Paquetes Dropeados, la técnica 6PE tiene un porcentaje de 50% mientras que la técnica 6VPE tiene un valor porcentual de 50%, las 2 técnicas utilizaron el protocolo de transporte UDP por ende, ahí la igual de porcentajes de paquetes dropeados es decir 50% para cada uno.

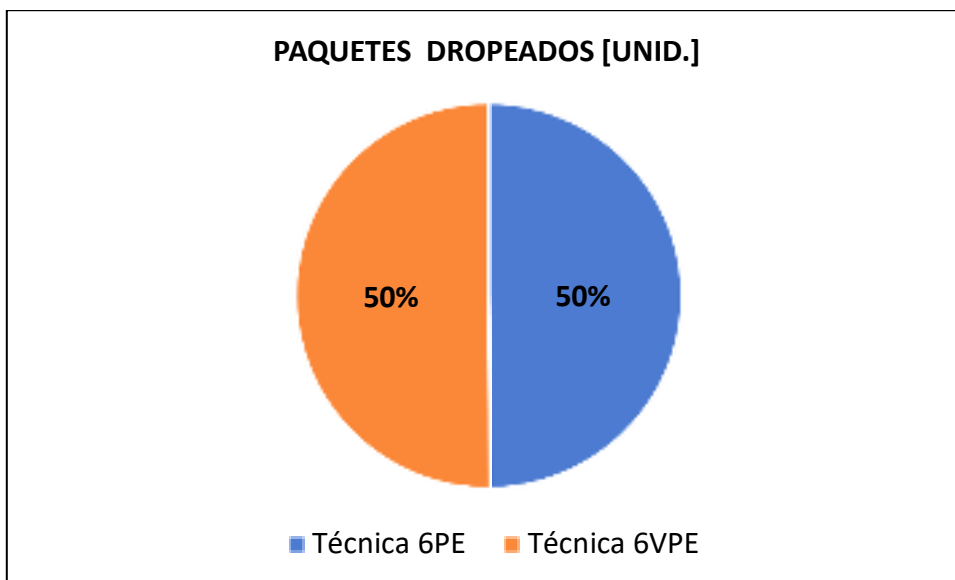


Gráfico 21-3: Diagrama de pastel comparativo entre la técnica 6PE y 6VPE del parámetro Paquetes Dropeados.
Realizado por: Yautibug, A. 2020.

En la siguiente **Tabla5-3** se visualiza los datos obtenido en porcentajes desde los diagramas de pastel de los parámetros evaluados, mediante esos datos se puede observar que la técnica 6PE es mejor para trasmisión de audio y video con IPv6 e IPv4.

Tabla 5-3: Datos obtenido en porcentajes desde los diagramas de pastel.

Parámetros	Técnica 6PE %	Técnica 6VPE %
Máximo delay [s]	41	59
Promedio delay o latencia [s]	45	55
Promedio Jitter [ms]	48	52
Desviación Estándar del delay [s]	40	60
Velocid. Promedio de Bits [kbits/s]	51	49
Velocidad promedio de paquetes [pkt/s]	51	49
Paquetes dropeados [%]	50	50

Realizado por: Yautibug, A. 2020

CONCLUSIONES

Se realizó un estudio técnico y minucioso de las VPNs MPLS capa3 en específico de las técnicas 6PE y 6VPE para streaming Audio y Video con Ipv4 e Ipv6, estas técnicas tienen características similares son utilizados por los proveedores de internet o ISP para transporta el flujo de una red de clientes con IPv6 sobre una red MPLS con IPv4, los routers de borde PE (Provider Edge) soportan dual stack es decir IPv6 e IPv4, para la comunicación ipv6 e ipv4 utiliza MP-BGP, en la interconexión entre diferentes sistemas autónomos se utiliza Inter-AS MPLS con las diferentes opciones A, B,C o AB, la principal diferencia entre estas 2 técnicas radica en que la técnica 6VPE crea una VRF por VPN para cada clientes en los router de borde PE y otra diferencia está en los router ASBRs crea VPNv4 o VPNv6 para el intercambio de paquetes entre sistemas autónomos diferentes.

Para el presente proyecto se realizaron 2 escenarios de prueba en el emulador GNS3, el primer escenario se realizó la emulación la técnica 6PE con sus respectivas configuraciones y luego las pruebas de conectividad de capa 3, finalmente las pruebas de transmisión y recepción de streaming desde el servidor a diferentes clientes con el programa VLC. En el segundo escenario la técnica 6VPE se configuro de igual manera todo el escenario, con la diferencia de la creación de VRFs correspondientes para cada cliente en los router de borde PE, en los routers de ASBRs se creó VPNv6, en la red del servidor se aplicó método Hub and Spoke, al igual que en la técnica anterior se realizó la pruebas de conectividad de capa 3 y luego la transmisión de streaming con VLC se realizó la comprobación de la transmisión streaming con el software Wireshark.

Con la herramienta D-ITG se inyectó tráfico de streaming desde el servidor-clientes con diferentes tiempos de recepción: 30 seg., 45 seg. y 60 seg., luego se graficó el diagrama de barras para comparar las 2 técnicas 6PE Y 6VPE de los parámetros de calidad: Máximo delay , promedio delay, promedio Jitter, desviación Estándar delay, velocidad Promedio de Bits, velocidad promedio de paquetes y paquetes dropeados, finalmente se graficó los diagramas de Pasteles para saber los porcentajes de los parámetros evaluados.

La técnica 6PE trabaja con la tabla de routing y la 6VPE trabaja con las tablas de routing y la tabla de VRFs esto afecta en la transmisión de streaming ya que la técnica 6VPE tiene mayor seguridad, mayor campos de control , mayor procesamiento de datos por ende tiene mayor valor delay y jitter afectando en la calidad del video.

se concluye que, con la información obtenida de los escenarios propuestos y los tiempos determinados, la técnica 6PE es mejor para la transmisión y recepción de streaming con IPv4 e IPv6, la técnica 6PE obtuvo los siguientes resultados porcentuales de los diagramas de pastel: 18% menos en Máximo delay, 10% menos en Promedio de Delay, 4% menos en Jitter, 20% menos en la Desviación Estándar, 2% más en la Velocidad promedio de Bits, 2% más en la velocidad promedio de paquetes recibidos, en comparación con la técnica 6VPE, en la relación de paquetes dropeados se obtuvo un porcentaje igual por la utilización del protocolo UDP.

RECOMENDACIONES

Con la herramienta de D-ITG se recomienda configurar correctamente en el emisor los parámetros: protocolo, tiempo de inyección, la dirección de destino, tamaño del paquete, número de paquetes a enviar por segundo, ya que debido a esas configuraciones se receptorá en el cliente para evaluar los parámetro deseados.

Se recomienda que en escenario los routers de borde PE debe ser dual stack para procesar IPV6 e IPV4 por ende esos router debe ser de mayor capacidad de procesamiento.

Se recomienda la configuración de inter-AS Layer 3 Opción B en los Routers ASBRs porque son los más utilizados por los ISPs ya que ofrece características: calidad de servicio (QoS), VPNv6 para el intercambio de paquetes entre sistemas Autónomos mediante MP-eBGP y fácil configuración.

En la máquinas físicas como virtuales se recomienda desactivar los Firewall y antivirus.

BIBLIOGRAFÍA

AGUIRRE ROJAS, Mirian Mercedes. Diseño de una red lan y wlan que brinde calidad de servicio, caso de estudio. unidad educativa San Rafael [En línea] (Trabajo de titulación).(Maestría) Pontificia Universidad Católica del Ecuador, Quito, Ecuador. 2017. pp. 40 Disponible en : <http://repositorio.puce.edu.ec/bitstream/handle/22000/14121/Caso%20de%20Estudio%20M%20Aguirre_13Oct2017.pdf?sequence=1&isAllowed=y>

ALEGSA, Leandro. *Definición de VMware Workstation* [blog]. España 2016.[consulta: 5 de Diciembre 2016]. Disponible en : <http://www.alegsa.com.ar/Dic/vmware_workstation.php >

GÓMEZ CARMONA, Joaquín. Propuesta de manual de prácticas de laboratorio de redes utilizando el emulador GNS3. [En línea] (Trabajo de diplomado).(Maestría) Universidad Central “Marta Abreu” de Las Villas, Santa Clara, Cuba 2017. pp. 22. Disponible en : <<http://dspace.uclv.edu.cu/bitstream/handle/123456789/7888/Joaqu%c3%adn%20G%c3%b3mez.pdf?sequence=1&isAllowed=y>>

CASTRO, Gabriel N. *Introducción de ipv6 en telecom Argentina* [blog]. Argentina, 2010 [consulta: 30 Octubre 2019]. Disponible en : <<https://dokumen.tips/documents/introduccion-de-ipv6-en-telecom-introduccion-de-ipv6-en-telecom-argentina.html>>

CeHis LTDA. *Qué es y para que sirve el Streaming* [blog]. Argentina, Avila Fabian, 2016 [consulta: 02 de Febrero de 2020]. Disponible en : <<https://cehis.net/sitio/ayuda-video-streaming/asistencia-y-soporte/base-de-conocimiento-faq/ayuda-video-streaming/que-es-y-para-que-sirve-el-streaming?fbclid=IwAR35WZalTN6Qw2PhqAqw1CuuIy0j9D9IiUwEo8YFgXO-Pz0awiCJUzqDaW4> >

CISCO. *Configuración y verificación de la opción 3 de la capa 3 MPLS VPN INTER-AS con IOS e IOS-XR.*[blog]. Mexico,2016. [consulta: 1 de Enero de 2020] . Disponible en : <<https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/200557-Configuration-and-Verification-of-Layer.html> >

Cisco Systems, Inc. *BGP MPLS IP Redes privadas virtuales (VPN)* [blog]. España, 2006. [consulta: 2 Febrero de 2020]. Disponible en : <<https://tools.ietf.org/html/rfc4364> >

CANO, Isabel, & ALEMIDA, Fernanda. Análisis del desempeño de una red con tecnología wi-fi para largas distancias en la región costa de Ecuador [En línea] (Trabajo de titulación).(Pregrado). Escuela Politécnica del Ejército, Sangolquí, Ecuador. 2012. pp. 74-76. Disponible en : <<http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/5710/T-ESPE-034113.pdf?sequence=1&isAllowed=y>>

INTECO. *Análisis de tráfico con wireshark* [En línea]. España: Manuel Belda, 2011. [consulta: 20 de diciembre 2019] Disponible en: <https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf>

PENELNJACK ,I. *MPLS and VPN Architectures volumen II.* [En línea]. Estados unidos 2003.pp. 142, [consulta: 2 de diciembre 2019]. Disponible en: <<http://www.ciscopress.com/store/mpls-and-vpn-architectures-volume-ii-9781587051128>>

CISCO LIVE. *I-AS MPLS Solutions*[En línea].Mexico: afiliados, 2010. [consulta: 7 de diciembre 2019] Disponible en: < http://uruhu.su/doc/Cisco_I-AS-MPLS.pdf>

LÓPEZ LARIO, Gustavo Gabriel. Pruebas de escala de VPNs capa 2 y 3 para la implementación legada basada en MPLS [En línea] (Trabajo de titulación).(Pregrado). Universidad de la República, Uruguay : 2017. pp. 4-7. Disponible en: <<https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/19034/1/2603.pdf>>

Palacios, L. & Mantilla, C. “Propuesta método de migración y coexistencia de IPv6 sobre red IP/MPLS para proveedor de servicios” *Revistas Espacios* [En línea], 2019 Mexico. pp. 14 [consultado 16 de Diciembre 2019]. Disponible en: <<http://www.revistaespacios.com/a19v40n11/a19v40n11p18.pdf>>

PINCAY ESPINOZA, Edison Geovanny, & TARCO QUITO, Dionicio. Análisis comparativo de la calidad de servicio entre las redes actuales y las redes de próxima generació. (Trabajo de titulación).(Pregrado). Escuela Superior Politécnica de CHimborazo, Riobamba, Ecuador. 2015. pp. 36.

OVIEDO CALLE, Iván Eduard , & SANTAMARIA SILUPU, Jorge Luis. Estudio de los diferentes modelos de inter-as mpls-vpns para brindar una propuesta técnica que permita la comunicación entre múltiples proveedores de servicios [En línea] (Trabajo de titulación).(Pregrado) Universidad Nacional de Piura, Piura, Peru. 2016. pp. 55-61. Disponible en: <<http://repositorio.unp.edu.pe/bitstream/handle/UNP/826/IET-SAN-SIL-16.pdf?sequence=1&isAllowed=y>>

SOCIETY INTERNET. *IPv6 en redes MPLS* [En línea]. Estados Unidos: Filiales, 2012. [consulta: 20 de diciembre 2019]. Disponible en: <http://www.6deploy.eu/workshops2/20121015_panama_panama/3%20-%20Introduccion%20a%20MPLS%20+%206PE.pdf>

USCA VELOZ, Roberto Bernardo. Evaluación del protocolo mpls con la aplicación de vpn para mejorar el rendimiento del sistema de transmisión de datos de la Corporación Nacional de Electricidad Regional Bolívar (Trabajo de titulación).(Pregrado). Escuela Superior Politecnica de Chimborazo, Riobamba, Ecuador. 2018. pp. 37-39.

VMWARE INC. Administrar máquinas virtuales de vSphere [En línea].España,filiales, [consultado 16 de dicimembre 2019]. disponible en: < https://docs.vmware.com/es/VMware-vSphere/6.0/vsphere-esxi-vcenter-server-601-virtual-machine-admin-guide.pdf?fbclid=IwAR0aAfH18dLSz_zTKEXVeiiYagz-p3yOClIKrnlPw9Im8RLMPlr6sJSMBc. >

Yáñez Izquierdo, Antonio. 2011. *Formatos de audio y vídeo: códecs* [En línea]. Ecuador, 2011. [consultado 16 de dicimembre 2019]. disponible en : <<http://www.edu.xunta.gal/centros/cfrcoruna/aulavirtual2/file.php/110/FormacionBasica9-Codecs.pdf>>

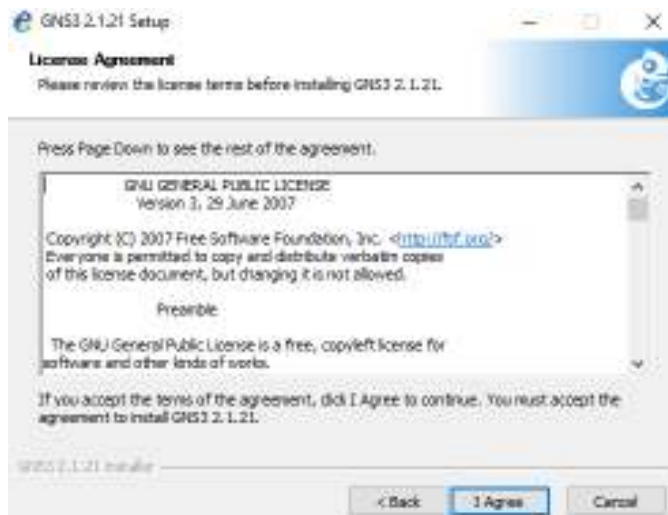


ANEXOS

ANEXO A: INSTALACIÓN DE GNS3

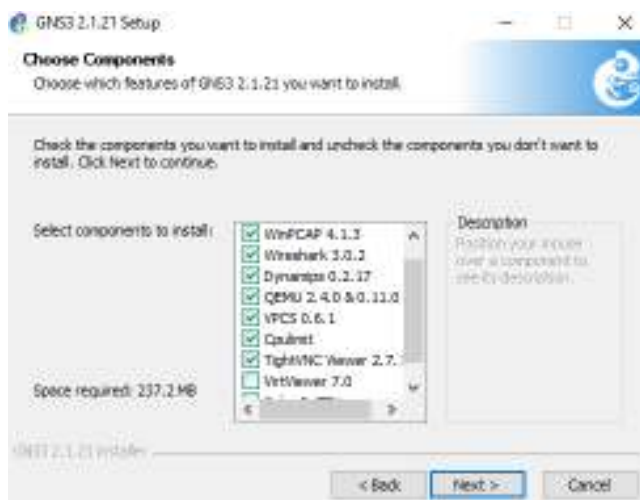
Una vez finalizada la descarga se debe ejecutar el archivo, luego les pedirá permisos de administrador, le dan Ok

1.- Aparecerá la referencia al acuerdo de licencia para poder ejecutar la instalación GNS3. Dar Click en “Agree”.



2.- Elige el Folder donde se instalará el acceso directo en el menú inicio se recomienda dejarlo por defecto.

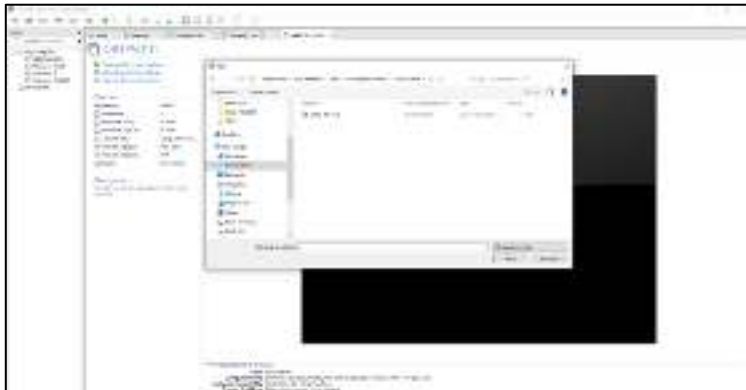
3 Seleccionar de componentes para la instalación GNS3: WinPCAP, WireShark, Dynamips, QEMU, VPCS, Cpulimit, TightVNC Viewer, Solar Winds Response y Npcap.



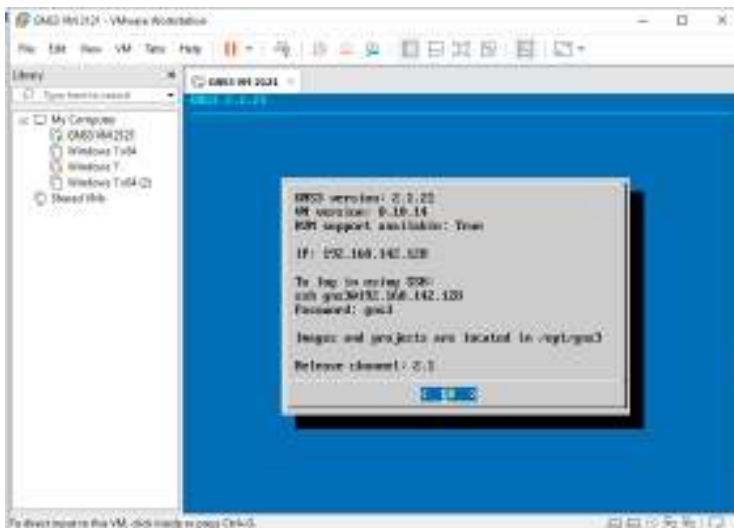
4.- En la ventana install dar Click y empezara la instalación de todo los programas elegidos anteriormente.

5.- Finalmente se concluye con la instalación GNS3. Seleccionar Start GNS3.

ANEXO B: EN VMWARE IMPORTANDO EL SOFTWARE VIRTUALIZADO EN UBUNTU DE GNS3 Y ASIGNANDO RECURSOS A LA MÁQUINA VIRTUAL.



Una vez ya Montado la máquina virtual en VMware .



Por último, la pantalla principal máquina virtual de GNS3 podrán ver en la parte izquierda los routers a disposición, para utilizarlo en una topología se debe arrastrar el router al centro de la pantalla en blanco.



Anexo C:- CONFIGURACIÓN EN EL ESCENARIO DE TECNICA 6PE

```
CE_1
HOSTname CE_1
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:1:A:1::1/64
ipv6 address fe80::1 link-local
no shutd
exit
interface gigabitEthernet 0/2
ipv6 enable
ipv6 address 2001:2:A:1::1/64
no shutd
exit
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:3:A:1::1/64
no shutd
exit
router bgp 100
bgp router-id 1.1.1.2
no bgp default ipv4-unicast
neighbor 2001:1:A:1::2 remote-as 400
address-family ipv6 unicast
neighbor 2001:1:A:1::2 activate
network 2001:2:A:1::/64
network 2001:1:A:1::/64
network 2001:3:A:1::/64
exit
exit

PE-1
HOSTname PE_1
ipv6 unicast-routing
ipv6 cef
mpls label range 1700 1780
mpls ldp router-id lo0 force
router ospf 10
router-id 17.17.17.17
mpls ldp autoconfig
exit
inter lo0
ip add 17.17.17.17 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
mpls ip
ipv6 enable
ipv6 address 2001:1:A:1::2/64
ipv6 address fe80::2 link-local
no shutd
exit
interface gigabitEthernet 0/1
mpls ip
ip add 10.10.1.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
mpls ip
ip add 10.10.2.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/4
mpls ip
ip add 10.10.3.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
mpls ip

P1
HOSTname P1
mpls label range 100 180
mpls ldp router-id lo0 force
router ospf 10
router-id 1.1.1.1
mpls ldp autoconfig
exit
interface lo0
ip add 1.1.1.1 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.5.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.1.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit

P2
HOSTname P2
mpls label range 200 280
mpls ldp router-id lo0 force
router ospf 10
router-id 2.2.2.2
mpls ldp autoconfig
exit
interface lo0
ip add 2.2.2.2 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.10.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.5.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.6.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit

P3
HOSTname P3
mpls ip
mpls label range 300 380
mpls ldp router-id lo0 force
router ospf 10
router-id 3.3.3.3

ip add 10.10.4.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
router bgp 400
no bgp default ipv4-unicast
neighbor 18.18.18.18 remote-as 400
neighbor 18.18.18.18 update-source loopback0
neighbor 2001:1:A:1::1 remote-as 100
address-family ipv6 unicast
neighbor 2001:1:A:1::1 activate
neighbor 18.18.18.18 activate
neighbor 18.18.18.18 send-label
exit
exit
```

```

mpls ldp autoconfig
exit
interface lo0
ip add 3.3.3.3 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.4.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.15.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.7.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
P4
HOSTname P4
mpls label range 400 480
mpls ldp router-id lo0 force
router ospf 10
router-id 4.4.4.4
mpls ldp autoconfig
exit
interface lo0
ip add 4.4.4.4 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/5
ip address 10.10.14.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.7.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
ip address 10.10.3.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.6.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.8.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/4
ip address 10.10.13.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
P5
HOSTname P5
mpls label range 500 580
mpls ldp router-id lo0 force
router ospf 10
router-id 5.5.5.5
mpls ldp autoconfig
exit
interface lo0
ip add 5.5.5.5 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.10.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.11.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.9.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
P6
HOSTname P6
mpls ip
mpls label range 600 680
mpls ldp router-id lo0 force
router ospf 10
router-id 6.6.6.6
mpls ldp autoconfig
exit
interface lo0
ip add 6.6.6.6 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.9.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.2.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.8.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
ip address 10.10.12.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
P7
HOSTname P7
mpls ip
mpls label range 700 780
mpls ldp router-id lo0 force
router ospf 10
router-id 7.7.7.7
mpls ldp autoconfig
exit
interface lo0
ip add 7.7.7.7 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.15.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.14.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.16.1 255.255.255.0
no shutd
ip ospf 10 area 0

```



```

exit
PE-2
HOSTname PE-2
ipv6 unicast-routing
ipv6 cef
mpls label range 1800 1880
mpls ldp router-id lo0 force
router ospf 10
router-id 18.18.18.18
mpls ldp autoconfig
exit
inter lo0
ip add 18.18.18.18 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
mpls ip
ip add 10.10.11.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.12.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.13.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
ip address 10.10.16.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/4
mpls ip
ipv6 enable
ipv6 address 2001:1:B:1::1/64
ipv6 address fe80::5 link-local
no shutd
exit
interface gigabitEthernet 0/5
ipv6 enable
ipv6 address 2001:1:D:1::1/64
ipv6 address fe80::9 link-local
no shutd
exit
router bgp 400
bgp router-id 18.18.18.18
no bgp default ipv4-unicast
neighbor 17.17.17.17 remote-as 400
neighbor 17.17.17.17 update-source loopback0
neighbor 2001:1:D:1::2 remote-as 500
neighbor 2001:1:B:1::2 remote-as 600
no synchronization
address-family ipv6 unicast
neighbor 2001:1:D:1::2 activate
neighbor 2001:1:B:1::2 activate
neighbor 17.17.17.17 activate
neighbor 17.17.17.17 send-label
redistribute connected
no synchronization
exit
exit
CE_2
HOSTname CE_2
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:1:B:1::2/64
ipv6 address fe80::6 link-local
no shutd
exit

interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:2:B:1::1/64
no shutd
exit
router bgp 600
bgp router-id 1.1.1.3
no bgp default ipv4-unicast
neighbor 2001:1:B:1::1 remote-as 400
address-family ipv6 unicast
neighbor 2001:1:B:1::1 activate
network 2001:2:B:1::/64
network 2001:1:B:1::/64
exit
exit
CE_3
HOSTname CE_3
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:1:C:1::1/64
ipv6 address fe80::3 link-local
no shutd
exit
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:2:C:1::1/64
no shutd
exit
router bgp 200
bgp router-id 1.1.1.4
no bgp default ipv4-unicast
neighbor 2001:1:C:1::2 remote-as 500
address-family ipv6 unicast
neighbor 2001:1:C:1::2 activate
network 2001:2:C:1::/64
network 2001:1:C:1::/64
exit
exit
PE-3
HOSTname PE_3
ipv6 unicast-routing
ipv6 cef
mpls label range 1900 1980
mpls ldp router-id lo0 force
router ospf 20
router-id 19.19.19.19
mpls ldp autoconfig
exit
inter lo0
ip add 19.19.19.19 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
mpls ip
ip add 200.58.1.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/2
mpls ip
ip add 200.58.2.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/4
mpls ip
ip add 200.58.3.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

interface gigabitEthernet 0/5
mpls ip

```

```

ipv6 enable
ipv6 address 2001:1:C:1::2/64
ipv6 address fe80::4 link-local
no shutd
exit
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:1:D:1::2/64
ipv6 address fe80::10 link-local
no shutd
exit
router bgp 500
bgp router-id 19.19.19.19
no bgp default ipv4-unicast
neighbor 20.20.20.20 remote-as 500
neighbor 20.20.20.20 update-source loopback0
neighbor 2001:1:D:1::1 remote-as 400
neighbor 2001:1:C:1::1 remote-as 200
no synchronization
address-family ipv6 unicast
neighbor 2001:1:D:1::1 activate
neighbor 2001:1:C:1::1 activate
neighbor 20.20.20.20 activate
neighbor 20.20.20.20 send-label
redistribute connected
no synchronization
exit
exit

P8
HOSTname P8
mpls label range 800 880
mpls ldp router-id lo0 force
router ospf 20
router-id 8.8.8.8
mpls ldp autoconfig
exit
interface lo0
ip add 8.8.8.8 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.1.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.4.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

P9
HOSTname P9
mpls label range 900 980
mpls ldp router-id lo0 force
router ospf 20
router-id 9.9.9.9
mpls ldp autoconfig
exit
interface lo0
ip add 9.9.9.9 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.2.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.5.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

P10
ip ospf 20 area 0

P11
HOSTname P11
mpls label range 1100 1180
mpls ldp router-id lo0 force
router ospf 20
router-id 11.11.11.11
mpls ldp autoconfig
exit
interface lo0
ip add 11.11.11.11 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.4.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.9.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/2
ip address 200.58.8.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

P12
HOSTname P12
mpls label range 1200 1280
mpls ldp router-id lo0 force
router ospf 20
router-id 12.12.12.12
mpls ldp autoconfig
exit
interface lo0
ip add 12.12.12.12 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.10.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.5.2 255.255.255.0
no shutd

exit

```

```

interface gigabitEthernet 0/2
ip address 200.58.6.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/3
ip address 200.58.8.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit

```

P13

```

HOSTname P13
mpls label range 1300 1380
mpls ldp router-id lo0 force
router ospf 20
router-id 13.13.13.13
mpls ldp autoconfig
exit
interface lo0
ip add 13.13.13.13 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.7.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.11.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

```

PE-4

```

HOSTname PE-4
ipv6 unicast-routing
mpls label range 2000 2280
mpls ldp router-id lo0 force
router ospf 20
router-id 20.20.20.20
mpls ldp autoconfig
exit
inter lo0
ip add 20.20.20.20 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
mpls ip
ip add 200.58.9.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.10.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/2
ip address 200.58.11.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/3
mpls ip
ipv6 enable
ipv6 address 2001:db6:fe:1::1/64
ipv6 address fe80::7 link-local
no shutd
exit
router bgp 500
no bgp default ipv4-unicast
neighbor 19.19.19.19 remote-as 500
neighbor 19.19.19.19 update-source loopback0
neighbor 2001:db6:fe:1::2 remote-as 300
address-family ipv6 unicast
neighbor 2001:db6:fe:1::2 activate

```

```

neighbor 19.19.19.19 activate
neighbor 19.19.19.19 send-label
exit
exit

```

CE_4

```

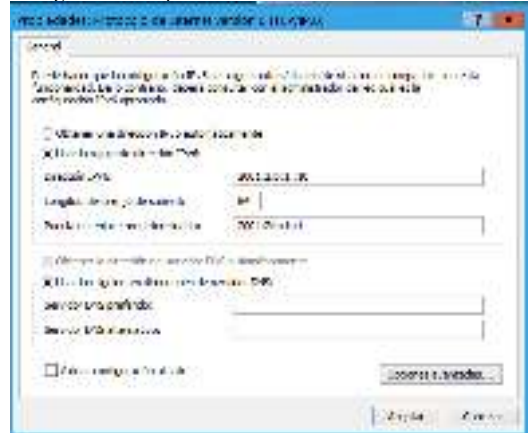
HOSTname CE_4
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:db6:fe:1::2/64
ipv6 address fe80::8 link-local
no shutd
exit
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:db7:fe:1::1/64
no shutd
exit
router bgp 300
bgp router-id 1.1.1.5
no bgp default ipv4-unicast
neighbor 2001:db6:fe:1::1 remote-as 500
address-family ipv6 unicast
neighbor 2001:db6:fe:1::1 activate
network 2001:db6:fe:1::/64
network 2001:db7:fe:1::/64
exit
exit

```

configuración de ip en el cliente 1.



configuración de ip en el Servidor.



ANEXO D:- CONFIGURACIÓN DE LA TÉCNICA 6PVE

```
CE_1
  HOStname CE_1
  ipv6 unicast-routing
  interface gigabitEthernet 0/0
  ipv6 enable
  ipv6 address 2001:1:A:1::1/64
  ipv6 address fe80::1 link-local
  no shutd
  exit
  interface gigabitEthernet 0/2
  ipv6 enable
  ipv6 address 2001:2:A:1::1/64
  no shutd
  exit
  interface gigabitEthernet 0/1
  ipv6 enable
  ipv6 address 2001:3:A:1::1/64
  no shutd
  exit
  router bgp 100
  bgp router-id 1.1.1.2
  no bgp default ipv4-unicast
  neighbor 2001:1:A:1::2 remote-as 400
  address-family ipv6
  neighbor 2001:1:A:1::2 activate
  network 2001:2:A:1::/64
  network 2001:1:A:1::/64
  network 2001:3:A:1::/64
  exit
  exit

PE-1
  HOStname PE_1
  ipv6 unicast-routing
  mpls label range 1700 1780
  mpls ldp router-id lo0 force
  vrf definition Cliente1
  rd 1:1
  address-family ipv6
  route-target both 1:1
  exit
  exit
  router ospf 10
  router-id 17.17.17.17
  mpls ldp autoconfig
  exit
  inter lo0
  ip add 17.17.17.17 255.255.255.255
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/0
  mpls ip
  ipv6 enable
  vrf forwarding Cliente1
  ipv6 address 2001:1:A:1::2/64
  ipv6 address fe80::2 link-local
  no shutd
  exit
  interface gigabitEthernet 0/1
  mpls ip
  ip add 10.10.1.1 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/3
  mpls ip
  ip add 10.10.2.1 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/4
  mpls ip
  ip add 10.10.3.1 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/2
  mpls ip
  ip add 10.10.4.1 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
  router bgp 400
  bgp router-id 17.17.17.17
  no bgp default ipv4-unicast
  neighbor 18.18.18.18 remote-as 400
  neighbor 18.18.18.18 update-source loopback0
  address-family vpnv6
  neighbor 18.18.18.18 activate
  neighbor 18.18.18.18 send-community extended
  redistribute connected
  no synchronization
  address-family ipv6 unicast vrf Cliente1
  redistribute connected
  neighbor 2001:1:A:1::1 remote-as 100
  neighbor 2001:1:A:1::1 activate
  exit
  exit

P1
  HOStname P1
  mpls ip
  ip cef
  mpls label range 100 180
  mpls ldp router-id lo0 force
  router ospf 10
  router-id 1.1.1.1
  mpls ldp autoconfig
  exit
  interface lo0
  ip add 1.1.1.1 255.255.255.255
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/1
  ip address 10.10.5.1 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/0
  ip address 10.10.1.2 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit

P2
  HOStname P2
  mpls ip
  ip cef
  mpls label range 200 280
  mpls ldp router-id lo0 force
  router ospf 10
  router-id 2.2.2.2
  mpls ldp autoconfig
  exit
  interface lo0
  ip add 2.2.2.2 255.255.255.255
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/1
  ip address 10.10.10.1 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
  interface gigabitEthernet 0/0
  ip address 10.10.5.2 255.255.255.0
  no shutd
  ip ospf 10 area 0
  exit
```

P3

```

interface gigabitEthernet 0/2
ip address 10.10.6.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit

HOSTname P3
mpls ip
ip cef
mpls label range 300 380
mpls ldp router-id lo0 force
router ospf 10
router-id 3.3.3.3
mpls ldp autoconfig
exit
interface lo0
ip add 3.3.3.3 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.4.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.15.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.7.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit

P4

HOSTname P4
mpls ip
ip cef
mpls label range 400 480
mpls ldp router-id lo0 force
router ospf 10
router-id 4.4.4.4
mpls ldp autoconfig
exit
interface lo0
ip add 4.4.4.4 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/5
ip address 10.10.14.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.7.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
ip address 10.10.3.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.6.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.8.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/4
ip address 10.10.13.1 255.255.255.0
no shutd

```

P5

```

ip ospf 10 area 0
exit

HOSTname P5
mpls ip
ip cef
mpls label range 500 580
mpls ldp router-id lo0 force
router ospf 10
router-id 5.5.5.5
mpls ldp autoconfig
exit
interface lo0
ip add 5.5.5.5 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.10.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.11.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.9.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit

P6

HOSTname P6
mpls ip
ip cef
mpls label range 600 680
mpls ldp router-id lo0 force
router ospf 10
router-id 6.6.6.6
mpls ldp autoconfig
exit
interface lo0
ip add 6.6.6.6 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.9.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.2.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.8.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
ip address 10.10.12.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit

P7

HOSTname P7
mpls ip
ip cef
mpls label range 700 780
mpls ldp router-id lo0 force
router ospf 10
router-id 7.7.7.7
mpls ldp autoconfig
exit

```

```

interface lo0
ip add 7.7.7.7 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
ip address 10.10.15.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.14.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.16.1 255.255.255.0
no shutd
ip ospf 10 area 0
exit
PE-2
HOSTname PE-2
mpls ip
ip cef
ipv6 unicast-routing
mpls label range 1800 1880
mpls ldp router-id lo0 force
router ospf 10
router-id 18.18.18.18
mpls ldp autoconfig
redistribute connected
exit
inter lo0
ip add 18.18.18.18 255.255.255.255
ip ospf 10 area 0
exit
interface gigabitEthernet 0/0
mpls ip
ip add 10.10.11.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/1
ip address 10.10.12.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/2
ip address 10.10.13.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/3
ip address 10.10.16.2 255.255.255.0
no shutd
ip ospf 10 area 0
exit
interface gigabitEthernet 0/5
ipv6 enable
mpls bgp forwarding
ipv6 address 2001:1:D:1::1/64
ipv6 address fe80::9 link-local
no shutd
mpls bgp forwarding
exit
vrf definition Cliente2
rd 2:2
address-family ipv6
route-target both 2:2
exit
exit
interface gigabitEthernet 0/4
mpls ip
ipv6 enable
vrf forwarding Cliente2
ipv6 address 2001:1:B:1::1/64
ipv6 address fe80::5 link-local
no shutd
exit
router bgp 400
bgp router-id 18.18.18.18
bgp log-neighbor-changes
no bgp default route-target filter
no bgp default ipv4-unicast
neighbor 17.17.17.17 remote-as 400
neighbor 17.17.17.17 update-source loopback0
neighbor 2001:1:D:1::2 remote-as 500
no synchronization
address-family vpnv6
neighbor 17.17.17.17 activate
neighbor 17.17.17.17 send-community extended
neighbor 17.17.17.17 next-hop-self
neighbor 2001:1:D:1::2 remote-as 500
neighbor 2001:1:D:1::2 activate
neighbor 2001:1:D:1::2 send-community
extended
redistribute connected
no synchronization
address-family ipv6 unicast vrf Cliente2
redistribute connected
neighbor 2001:1:B:1::2 remote-as 600
neighbor 2001:1:B:1::2 activate
exit
exit
CE_2
HOSTname CE_2
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:1:B:1::2/64
ipv6 address fe80::6 link-local
no shutd
exit
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:2:B:1::1/64
no shutd
exit
router bgp 600
bgp router-id 1.1.1.3
no bgp default ipv4-unicast
neighbor 2001:1:B:1::1 remote-as 400
address-family ipv6
neighbor 2001:1:B:1::1 activate
network 2001:2:B:1::/64
network 2001:1:B:1::/64
exit
CE_3
HOSTname CE_3
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:1:C:1::1/64
ipv6 address fe80::3 link-local
no shutd
exit
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:2:C:1::1/64
no shutd
exit
router bgp 200
bgp router-id 1.1.1.4
no bgp default ipv4-unicast
neighbor 2001:1:C:1::2 remote-as 500
address-family ipv6
neighbor 2001:1:C:1::2 activate
network 2001:2:C:1::/64
network 2001:1:C:1::/64
exit
exit
PE-3
HOSTname PE_3

```

```

ipv6 unicast-routing
mpls label range 1900 1980
mpls ldp router-id lo0 force
vrf definition Cliente3
rd 3:3
address-family ipv6
route-target both 3:3
exit
router ospf 20
router-id 19.19.19.19
mpls ldp autoconfig
redistribute connected
exit
inter lo0
ip add 19.19.19.19 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
mpls ip
ip add 200.58.1.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/2
mpls ip
ip add 200.58.2.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/4
mpls ip
ip add 200.58.3.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/5
mpls ip
ipv6 enable
vrf forwarding Cliente3
ipv6 address 2001:1:C:1::2/64
ipv6 address fe80::4 link-local
no shutd
exit
interface gigabitEthernet 0/0
ipv6 enable
mpls bgp forwarding
ipv6 address 2001:1:D:1::2/64
ipv6 address fe80::10 link-local
no shutd
mpls bgp forwarding
exit
router bgp 500
bgp router-id 19.19.19.19
bgp log-neighbor-changes
no bgp default route-target filter
no bgp default ipv4-unicast
neighbor 20.20.20.20 remote-as 500
neighbor 20.20.20.20 update-source loopback0
neighbor 2001:1:D:1::1 remote-as 400
address-family vpnv6
neighbor 20.20.20.20 activate
neighbor 20.20.20.20 send-community extended
neighbor 20.20.20.20 next-hop-self
neighbor 2001:1:D:1::1 remote-as 400
neighbor 2001:1:D:1::1 activate
neighbor 2001:1:D:1::1 send-community
extended
redistribute connected
no synchronization
address-family ipv6 unicast vrf Cliente3
neighbor 2001:1:C:1::1 remote-as 200
neighbor 2001:1:C:1::1 activate
exit
exit

```

P8

HOSTname P8

```

mpls ip
ip cef
mpls label range 800 880
mpls ldp router-id lo0 force
router ospf 20
router-id 8.8.8.8
mpls ldp autoconfig
exit
interface lo0
ip add 8.8.8.8 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.1.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.4.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

```

P9

```

HOSTname P9
mpls ip
ip cef
mpls label range 900 980
mpls ldp router-id lo0 force
router ospf 20
router-id 9.9.9.9
mpls ldp autoconfig
exit
interface lo0
ip add 9.9.9.9 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.2.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.5.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

```

P10

```

HOSTname P10
mpls ip
ip cef
mpls label range 1000 1080
mpls ldp router-id lo0 force
router ospf 20
router-id 10.10.10.10
mpls ldp autoconfig
exit
interface lo0
ip add 10.10.10.10 255.255.255.255
ip ospf 20 area 0
exit
interface gigabitEthernet 0/0
ip address 200.58.3.2 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/1
ip address 200.58.6.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit
interface gigabitEthernet 0/2
ip address 200.58.7.1 255.255.255.0
no shutd
ip ospf 20 area 0
exit

```

P11

	<pre> HOSTname P11 mpls ip ip cef mpls label range 1100 1180 mpls ldp router-id lo0 force router ospf 20 router-id 11.11.11.11 mpls ldp autoconfig exit interface lo0 ip add 11.11.11.11 255.255.255.255 ip ospf 20 area 0 exit interface gigabitEthernet 0/0 ip address 200.58.4.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/1 ip address 200.58.9.1 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/2 ip address 200.58.8.1 255.255.255.0 no shutd ip ospf 20 area 0 exit </pre>	
P12	<pre> HOSTname P12 mpls ip ip cef mpls label range 1200 1280 mpls ldp router-id lo0 force router ospf 20 router-id 12.12.12.12 mpls ldp autoconfig exit interface lo0 ip add 12.12.12.12 255.255.255.255 ip ospf 20 area 0 exit interface gigabitEthernet 0/1 ip address 200.58.10.1 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/0 ip address 200.58.5.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/2 ip address 200.58.6.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/3 ip address 200.58.8.2 255.255.255.0 no shutd ip ospf 20 area 0 exit </pre>	
P13	<pre> HOSTname P13 mpls ip ip cef mpls label range 1300 1380 mpls ldp router-id lo0 force router ospf 20 router-id 13.13.13.13 mpls ldp autoconfig exit interface lo0 ip add 13.13.13.13 255.255.255.255 ip ospf 20 area 0 exit </pre>	<pre> interface gigabitEthernet 0/0 ip address 200.58.7.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/1 ip address 200.58.11.1 255.255.255.0 no shutd ip ospf 20 area 0 exit PE-4 HOSTname PE-4 ipv6 unicast-routing mpls label range 2000 2280 mpls ldp router-id lo0 force vrf definition Cliente1 rd 1:1 address-family ipv6 route-target both 1:1 exit vrf definition Cliente2 rd 2:2 address-family ipv6 route-target both 2:2 exit vrf definition Cliente3 rd 3:3 address-family ipv6 route-target both 3:3 exit router ospf 20 router-id 20.20.20.20 mpls ldp autoconfig exit inter lo0 ip add 20.20.20.20 255.255.255.255 ip ospf 20 area 0 exit interface gigabitEthernet 0/0 mpls ip ip add 200.58.9.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/1 ip address 200.58.10.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/2 ip address 200.58.11.2 255.255.255.0 no shutd ip ospf 20 area 0 exit interface gigabitEthernet 0/3 mpls ip ipv6 enable vrf forwarding Cliente1 ipv6 address 2001:db6:fe:1::1/64 ipv6 address fe80::7 link-local no shutd exit interface gigabitEthernet 0/4 mpls ip ipv6 enable vrf forwarding Cliente2 ipv6 address 2001:db7:fe:1::1/64 ipv6 address fe80::11 link-local no shutd exit interface gigabitEthernet 0/5 mpls ip ipv6 enable vrf forwarding Cliente3 </pre>


```

ipv6 address 2001:db8:fe:1::1/64
ipv6 address fe80::13 link-local
no shutd
exit
router bgp 500
bgp router-id 20.20.20.20
no bgp default ipv4-unicast
neighbor 19.19.19.19 remote-as 500
neighbor 19.19.19.19 update-source loopback0
redistribute connected
address-family vpnv6
neighbor 19.19.19.19 activate
neighbor 19.19.19.19 send-community extended
no synchronization
address-family ipv6 unicast vrf Cliente1
neighbor 2001:db6:fe:1::2 remote-as 300
neighbor 2001:db6:fe:1::2 activate
neighbor 2001:db6:fe:1::2 as-override
redistribute connected
no synchronization
address-family ipv6 unicast vrf Cliente2
neighbor 2001:db7:fe:1::2 remote-as 300
neighbor 2001:db7:fe:1::2 activate
neighbor 2001:db7:fe:1::2 allowas-in
redistribute connected
no synchronization
address-family ipv6 unicast vrf Cliente3
neighbor 2001:db8:fe:1::2 remote-as 300
neighbor 2001:db8:fe:1::2 activate
redistribute connected
no synchronization
exit

```

CE_4

```

HOSTname CE_4
ipv6 unicast-routing
interface gigabitEthernet 0/0
ipv6 enable
ipv6 address 2001:db6:fe:1::2/64
ipv6 address fe80::8 link-local
no shutd
exit
interface gigabitEthernet 0/2
ipv6 enable
ipv6 address 2001:db7:fe:1::2/64
ipv6 address fe80::12 link-local
no shutd
exit
interface gigabitEthernet 0/3
ipv6 enable
ipv6 address 2001:db8:fe:1::2/64
ipv6 address fe80::14 link-local
no shutd
exit
interface gigabitEthernet 0/1
ipv6 enable
ipv6 address 2001:db9:fe:1::1/64
no shutd
exit
router bgp 300
bgp router-id 1.1.1.8
no bgp default ipv4-unicast
neighbor 2001:db6:fe:1::1 remote-as 500
neighbor 2001:db7:fe:1::1 remote-as 500
neighbor 2001:db8:fe:1::1 remote-as 500
address-family ipv6
neighbor 2001:db6:fe:1::1 activate
neighbor 2001:db7:fe:1::1 activate
neighbor 2001:db8:fe:1::1 activate
network 2001:db6:fe:1::/64
network 2001:db7:fe:1::/64
network 2001:db8:fe:1::/64
network 2001:db9:fe:1::/64
exit
exit

```

configuración de ip en el cliente 1.



configuración de ip en el Servidor.



Configuración de Appliance Ubuntu

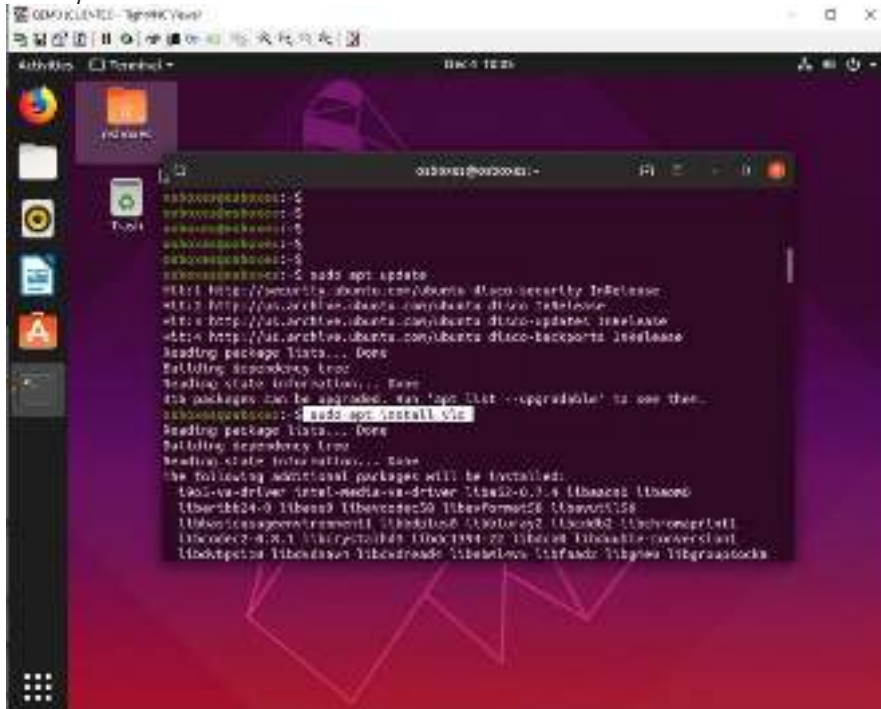


ANEXO E:- INSTALACIÓN DE VLC EN APLIANCE UBUNTU 19.04

Para instalar VLC se debe tener conexión a internet en la máquina de Ubuntu , abrir una terminal y ejecutar lo siguientes comandos:

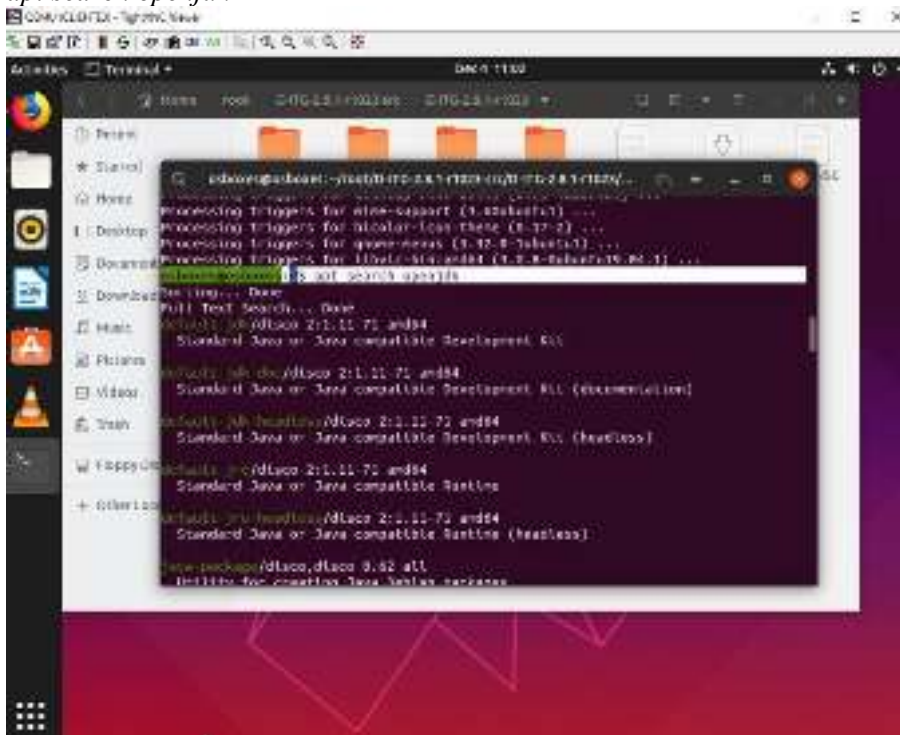
sudo apt Update

sudo apt install Vlc



Por defecto, Ubuntu 19.10 Linux ofrece múltiples versiones de Java OpenJDK 8,11,13 y 14 están disponibles en un repositorio estándar de Ubuntu.

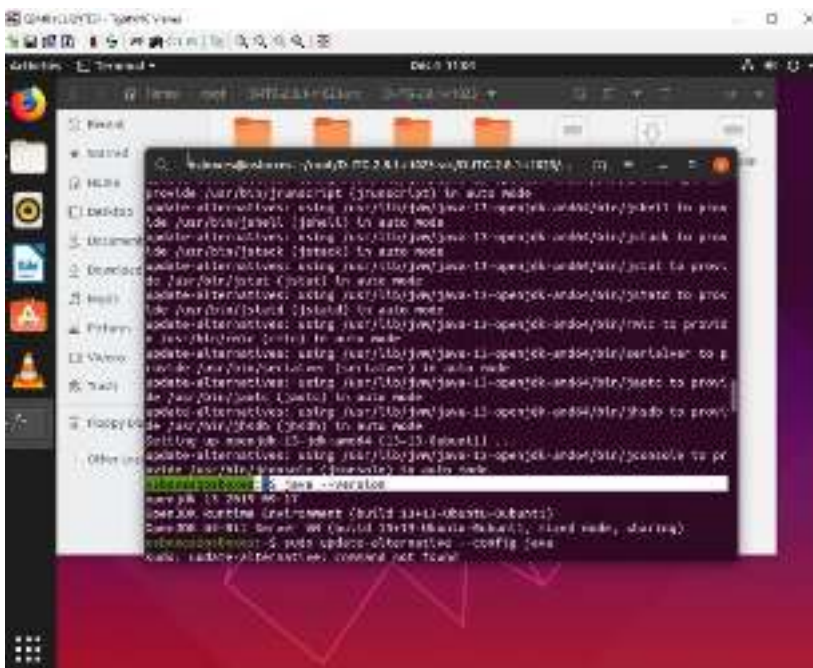
apt search openjdk



Una vez visualizado, instale cualquiera de las versiones Java de OpenJDK disponibles. Por ejemplo: *sudo apt install openjdk-13-jdk*



Para instalar en Ubuntu java, en esta etapa, el comando java debe estar disponible en su sistema y devolver su versión instalada: `java --versión`



Para ayudar puede guiarse en link web: <https://linuxconfig.org/how-to-install-java-on-ubuntu-19-10-eoan-ermine-linux>

ANEXO F:- PASOS PARA GRAFICAR EN UBUNTU.

En el terminal de Maquina Ubuntu se debe ejecutar los siguiente comandos.

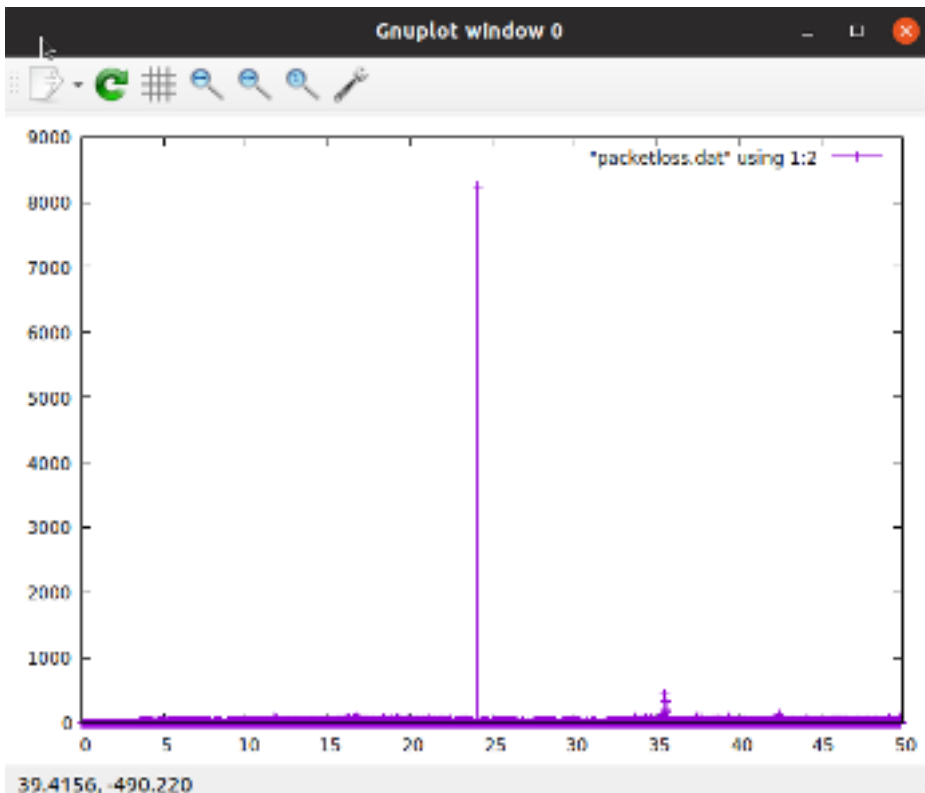
Gnuplot

Cd 'copiar el link de donde están ubicados los archivos a graficar'

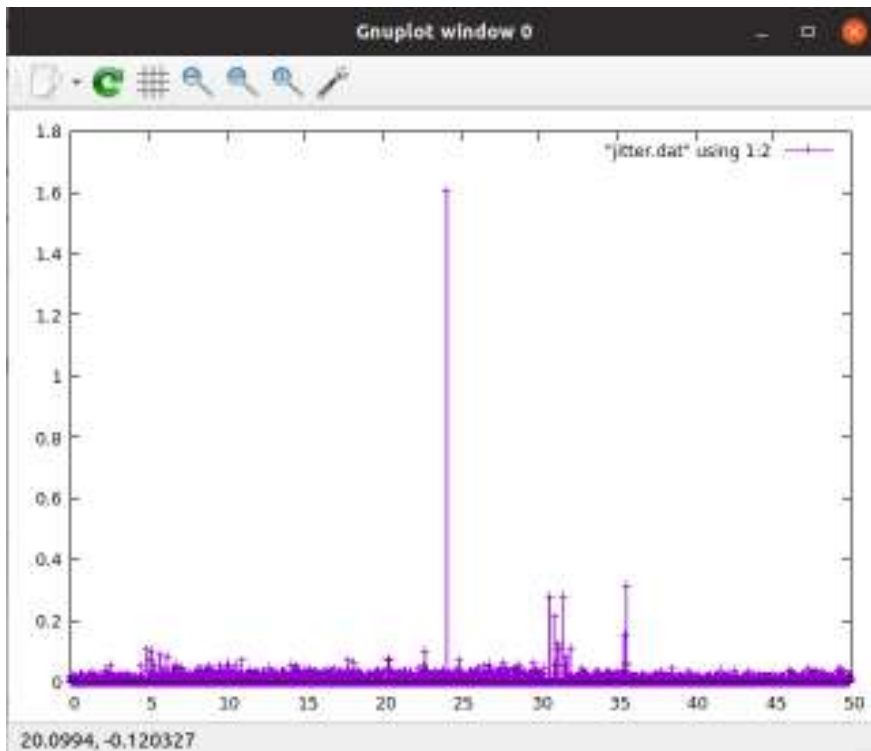
Plot "packetloss.dat" using 1:2 with linespoints

```
osboxes@osboxes: ~  
osboxes@osboxes:~$ gnuplot  
  
  G N U P L O T  
  Verston 5.2 patchlevel 6   Last modified 2019-01-01  
  
  Copyright (C) 1986-1993, 1998, 2004, 2007-2018  
  Thomas Williams, Colin Kelley and many others  
  
  gnuplot home:      http://www.gnuplot.info  
  faq, bugs, etc:   type "help FAQ"  
  immediate help:   type "help" (plot window: hit 'h')  
  
Terminal type is now 'qt'  
gnuplot> cd "/home/osboxes/root/0-ITG-2.0.1-r1823-src/0-ITG-2.0.1-r1823/lags/clientscan45s"  
gnuplot> plot "packetloss.dat" using 1:2 with linespoints  
gnuplot> plot "packetloss.dat" using 1:2 with linespoints  
gnuplot>
```

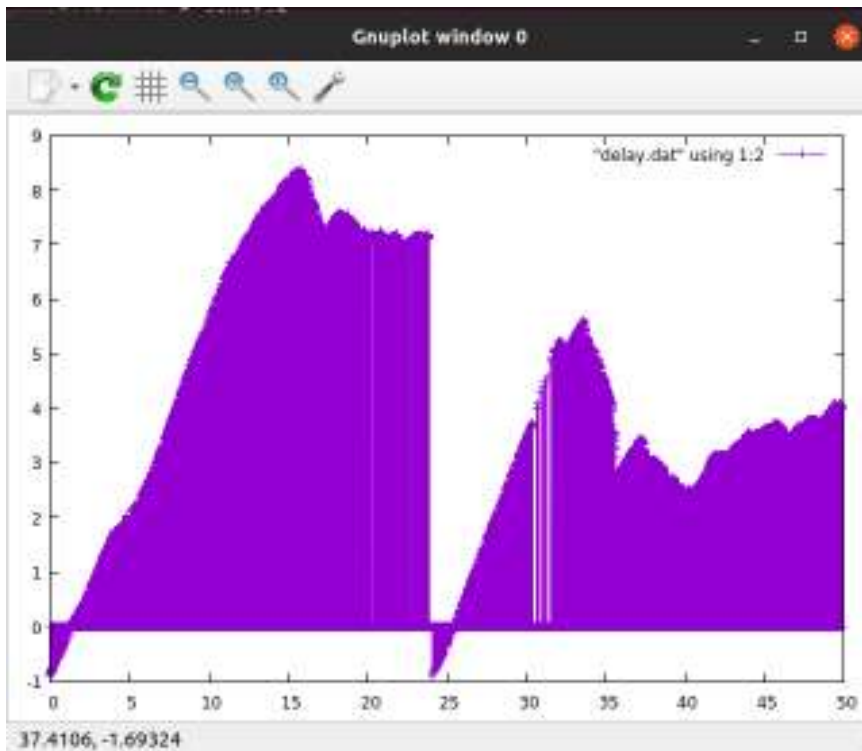
Grafica de packetloss en cliente 3 con recepción de 45 segundos



Grafica de jitter en cliente 3 con recepción de 45 segundos



Grafica de delay en cliente 3 con recepción de 45 segundos





ESCUELA SUPERIOR POLITÉCNICA DE
CHIMBORAZO



DIRECCIÓN DE BIBLIOTECAS Y RECURSOS
PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

UNIDAD DE PROCESOS TÉCNICOS
REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 10 / 03 / 2020

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: Alex Leonel Yautibug Coro
INFORMACIÓN INSTITUCIONAL
Facultad: Informática y Electrónica
Carrera: Ingeniería en Electrónica Telecomunicaciones y Redes
Título a optar: Ingeniero en Electrónica Telecomunicaciones y Redes
f. Analista de Biblioteca responsable: 