ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACIÓN DE UN PROTOTIPO DE RED IP/MPLS PARA EL ESTUDIO DE TRÁFICO MULTICAST, UTILIZANDO MULTICAST VPN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

BYRON FERNANDO ARIAS SARANGO
byr_1920@hotmail.com

DIRECTOR: ING. PABLO WILIAN HIDALGO LASCANO
phidalgo@ieee.org

CO-DIRECTOR: ING. LEONARDO SALAZAR ESTÉVEZ
lsenallo@hotmail.com

Quito, Febrero 2016

DECLARACIÓN

Yo, Byron Fernando Arias Sarango, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Byron Fernando Arias Sarango

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Byron Fernando Arias Sarango, bajo nuestra supervisión.

_____	_____
Ing. Pablo Hidalgo	**Ing. Leonardo Salazar**
DIRECTOR DE PROYECTO	**CO-DIRECTOR DE PROYECTO**

AGRADECIMIENTOS

A mi madre Lidia y a mis hermanos Ángel y Mirian, por fortalecerme día a día con sus oraciones y palabras de ánimo.

Al Ing. Pablo Hidalgo, por haber depositado su confianza en mí desde el primer instante en que empezamos este Proyecto.

Al Ing. Leonardo Salazar, por ser mi guía y un verdadero ejemplo a seguir como amigo y como profesional.

A los compañeros del Laboratorio de Informática de la FIEE, a cargo del Ing. José Estrada, por facilitarme las instalaciones y equipos, con total apertura y generosidad.

A mis amigos, Luis, Carlos y Santiago, por compartir las vicisitudes y alegrías de la vida. ¡Gracias amigos!

DEDICATORIA

A mi madre, Lidia, sabes que te amo con todo mi corazón.

A un gran amigo, Diego Carrillo Jiménez (†). Sé que nos volveremos a encontrar en el Reino de los Cielos…

CONTENIDO

DECLARACIÓN……i

CERTIFICACIÓN ii

AGRADECIMIENTOS iii

DEDICATORIA iv

CONTENIDO v

ÍNDICE DE FIGURAS xi

ÍNDICE DE TABLAS xiv

ÍNDICE DE ECUACIONES xviii

RESUMEN……xix

PRESENTACIÓN……xxi

CAPÍTULO 1

1. MARCO TEÓRICO 1

1.1 INTRODUCCIÓN 1

1.2 IP MULTICAST 1

1.2.1 DIRECCIONAMIENTO MULTICAST IPv4 2

1.2.1.1 Direccionamiento multicast a nivel de capa 3 2

1.2.1.1.1 Direcciones IP multicast bien conocidas 2

1.2.1.1.2 Rango de Direcciones IP multicast 2

1.2.1.2 Direccionamiento multicast a nivel de capa 2 3

1.2.2 DIRECCIONAMIENTO MULTICAST IPv6 4

1.2.2.1 Direccionamiento multicast a nivel de capa 3 4

1.2.2.2 Direccionamiento multicast a nivel de capa 2 5

1.2.3 TERMINOLOGÍA IP MULTICAST 5

1.2.3.1 Reverse Path Forwarding (RPF) 6

1.2.3.2 Shortest Path Tree (SPT) – Árbol de camino más corto 7

1.2.3.3 Terminología de rama y hoja en multicast 8
1.2.4 ÁRBOLES DE DISTRIBUCIÓN MULTICAST 9
1.2.4.1 Árboles de Fuente (Source Trees) 9
1.2.4.2 Árboles Compartidos (Shared Trees) 10
1.3 PROTOCOLOS DE INTERACCIÓN ENTRE MIEMBROS MULTICAST 11
1.3.1 INTERNET GROUP MANAGEMENT PROTOCOL (IGMP - IPV4) 11
1.3.1.1 IGMPv1 12
1.3.1.2 IGMPv2 12
1.3.1.3 IGMPv3 12
1.3.2 MULTICAST LISTENER DISCOVERY (MLD - IPv6) 13
1.4 ALGORITMOS DE REENVÍO MULTICAST 13
1.4.1 ALGORITMO DE INUNDACIÓN 13
1.4.2 ALGORITMO DE ÁRBOL DE EXPANSIÓN (SPANNING TREE) 14
1.4.3 ALGORITMO REVERSE PATH BROADCASTING (RPB) 14
1.4.4 ALGORITMO REVERSE PATH MULTICASTING (RPM) 15
1.5 PROTOCOLOS DE ENRUTAMIENTO MULTICAST 16
1.5.1 CORE BASED TREE (ÁRBOL BASADO EN EL NÚCLEO) – CBT 16
1.5.2 DISTANCE VECTOR MULTICAST ROUTING PROTOCOL (PROTOCOLO DE ENRUTAMIENTO MULTICAST POR VECTOR DISTANCIA) – DVMRP 16
1.5.3 MULTICAST OPEN SHORTEST PATH FIRST (OSPF MULTICAST) – MOSPF 16
1.5.4 PROTOCOL INDEPENDENT MULTICAST (PROTOCOLO INDEPENDIENTE MULTICAST) – PIM 17
1.5.4.1 Dense Mode (Modo denso) – PIM DM 17

1.5.4.2 Sparse Mode (Modo disperso) – PIM SM 18
1.5.4.3 PIM Bidirectional (PIM bidireccional) – PIM BiDir 19
1.5.4.4 Source Specific Multicast (PIM de Fuente Multicast Específica) – PIM SSM 20
1.5.4.5 Any Source Multicast (ASM) 20
1.5.5 PROTOCOLO INDEPENDENTE MULTICAST PARA IPV6 20
1.5.5.1 PIM SM para IPv6 multicast 21
1.5.5.2 PIM SSM para IPv6 multicast 21
1.6 REDES PRIVADAS VIRTUALES MULTICAST EN IP/MPLS 21
1.6.1 UNICAST VPN 21
1.6.1.1 Definición y Tipos de VPN basadas en MPLS 22
1.6.1.1.1 Redes Privadas Virtuales de capa 2 (L2VPN) 22
1.6.1.1.2 Redes Privadas Virtuales de capa 3 (L3VPN) 23
1.6.1.2 Componentes de la red 23
1.6.1.2.1 CE (Customer Edge) 23
1.6.1.2.2 PE (Provider Edge) 24
1.6.1.2.3 P (Provider) 24
1.6.1.3 Terminología en la Arquitectura MPLS VPN 24
1.6.1.3.1 Virtual Routing / Forwarding (VRF) 24
1.6.1.3.2 Route Distinguisher – RD 25
1.6.1.3.3 Route Target – RT 25
1.6.1.3.4 Propagación de rutas a través del Multiprotocolo BGP 26
1.6.1.3.5 Reenvío de paquetes etiquetados 26
1.7 MULTICAST VPN 28
1.7.1 NOCIONES DE MVPN 28
1.7.2 COMPONENTES DE UNA MVPN 28
1.7.2.1 Dominio multicast 28

1.7.2.2 Multicast Virtual Routing Forwarding – MVRF 29
1.7.2.3 Multicast Tunnel Interface (MTI) 30
1.7.2.4 Árboles de distribución multicast 30
1.7.3 ADYACENCIAS EN PIM 31
1.7.4 ÁRBOLES DE DISTRIBUCIÓN MULTICAST EN MVPN 31
1.7.4.1 MDT por defecto 32
1.7.4.2 MDT de datos 34
1.7.5 REVERSE PATH FORWARDING EN MVPN 35

CAPÍTULO 2

2. IMPLEMENTACIÓN DEL PROTOTIPO 37
2.1 ANÁLISIS Y COMPARACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO MULTICAST PARA IPV4 37
2.2 CONFIGURACIÓN DE LOS ROUTERS CISCO CON UNICAST Y MULTICAST VPN EN LA RED IP/MPLS 43
2.2.1 UNICAST VPN 44
2.2.1.1 Router PE1 (Provider Edge 1) 44
2.2.1.2 Router P (Provider) 46
2.2.1.3 Router CE1 (Customer Edge 1) 47
2.2.2 MULTICAST VPN 48
2.2.2.1 Router P (Provider) 48
2.2.2.2 Router PE1 (Provider Edge 1) 48
2.2.2.3 Router CE1 (Customer Edge 1) 49
2.2.2.4 Pruebas de validación 50
2.3 INSTALACIÓN Y CONFIGURACIÓN DEL GENERADOR DE TRÁFICO, SOFTWARE DE EMISIÓN DE VIDEO Y HERRAMIENTA DE MONITOREO DE VIDEO 55
2.3.1 JPERF 55

2.3.2 SOFTWARE DE EMISIÓN DE VIDEO VLC 57
2.3.2.1 Métodos de streaming 57
2.3.2.2 Opciones de transcodificación 59
2.3.2.3 Opciones de streaming 59
2.3.3 HERRAMIENTA DE MONITOREO DE VIDEO FAULTLINE 60

CAPÍTULO 3

3. ANÁLISIS DE RESULTADOS 63
3.1 BREVE INTRODUCCIÓN A LA TEORÍA DE COLAS 64
3.2 BATERÍA DE PRUEBAS 1 67
3.2.1 EXPERIMENTO 67
3.2.2 PRESENTACIÓN DE RESULTADOS 68
3.2.3 INFERENCIA DE RESULTADOS 74
3.3 BATERÍA DE PRUEBAS 2 75
3.3.1 EXPERIMENTO 75
3.3.2 PRESENTACIÓN DE RESULTADOS 75
3.3.3 INFERENCIA DE RESULTADOS 79
3.4 BATERÍA DE PRUEBAS 3 79
3.4.1 EXPERIMENTO 79
3.4.2 PRESENTACIÓN DE RESULTADOS 80
3.4.3 INFERENCIA DE RESULTADOS 83
3.5 BATERÍA DE PRUEBAS 4 84
3.5.1 EXPERIMENTO 84
3.5.2 PRESENTACIÓN DE RESULTADOS 84
3.5.3 INFERENCIA DE RESULTADOS 85
3.6 BATERÍA DE PRUEBAS 5 86
3.6.1 EXPERIMENTO 86
3.6.2 PRESENTACIÓN DE RESULTADOS 86

3.6.3 INFERENCIA DE RESULTADOS 91
3.7 BATERÍA DE PRUEBAS 6 92
3.7.1 EXPERIMENTO 92
3.7.2 PRESENTACIÓN DE RESULTADOS..... 92
3.7.3 INFERENCIA DE RESULTADOS 95
3.8 BATERÍA DE PRUEBAS 7 96
3.8.1 EXPERIMENTO 96
3.8.2 PRESENTACIÓN DE RESULTADOS..... 97
3.8.3 INFERENCIA DE RESULTADOS 100
3.9 BATERÍA DE PRUEBAS 8 100
3.9.1 EXPERIMENTO EMISIÓN DE VIDEO..... 100
3.9.2 PRESENTACIÓN DE RESULTADOS UNICAST Y MULTICAST..... 101
3.9.3 INFERENCIA DE RESULTADOS UNICAST Y MULTICAST 107
3.10 DISCERNIMIENTO DEL TRÁFICO MULTICAST EN IP/MPLS MVPN 108

CAPÍTULO 4

4. CONCLUSIONES Y RECOMENDACIONES 113
4.1 CONCLUSIONES 113
4.2 RECOMENDACIONES 114
REFERENCIAS BIBLIOGRÁFICAS..... 116
ANEXOS 120

ÍNDICE DE FIGURAS

CAPÍTULO 1

Figura 1.1 Modos de transmisión 1
Figura 1.2 Relación entre las direcciones multicast IP y MAC 4
Figura 1.3 Mapeo de las direcciones multicast IPv6 a Ethernet 5
Figura 1.4 Chequeo RPF fallido 7
Figura 1.5 Chequeo RPF satisfactorio 8
Figura 1.6 Ejemplo de un árbol de distribución fuente 10
Figura 1.7 Ejemplo de un árbol de distribución compartido 11
Figura 1.8 Representación de los árboles de expansión y RPB 14
Figura 1.9 Representación del árbol RPM 15
Figura 1.10 Funcionamiento de PIM – DM 17
Figura 1.11 Funcionamiento de PIM – SM 19
Figura 1.12 Jerarquía de las VPN 22
Figura 1.13 Routers participantes en una red BGP/MPLS VPN 23
Figura 1.14 VRF en un router PE 25
Figura 1.15 Propagación de rutas por medio del Multiprotocolo BGP 26
Figura 1.16 Reenvío de paquetes en una red MPLS VPN 27
Figura 1.17 Concepto de dominio multicast dentro de un SP 29
Figura 1.18 Adyacencias en PIM 32
Figura 1.19 Encapsulamiento del paquete-Cliente 33
Figura 1.20 Árboles de distribución multicast por defecto y de datos 34

CAPÍTULO 2

Figura 2.1 Esquema de la red con los protocolos de enrutamiento multicast 39
Figura 2.2 Diagrama detallado del prototipo de la red 42
Figura 2.3 Interconexión de los routers en el laboratorio 41
Figura 2.4 Tabla de enrutamiento multicast en CE1 51
Figura 2.5 Ejecución del comando mtrace desde CE1 51
Figura 2.6 Grupos IGMP asociados a la VRF REDES en CE1 52

Figura 2.7 Esquema del encapsulamiento en GRE desde PE1 52
Figura 2.8 Tabla de enrutamiento multicast global para PE1 53
Figura 2.9 Tabla de enrutamiento multicast mVRF en PE1 53
Figura 2.10 Tabla de enrutamiento multicast mVRF en PE2 54
Figura 2.11 Tabla de enrutamiento multicast mVRF en PE3 54
Figura 2.12 MDT establecido desde la loopback 0 de PE1 54
Figura 2.13 Adyacencias PIM en PE1 55
Figura 2.14 Ventana principal de la herramienta Jperf 56
Figura 2.15 Opciones de emisión y recepción en VLC 57
Figura 2.16 Métodos de streaming en VLC 58
Figura 2.17 Recepción de video utilizando el protocolo RTP 58
Figura 2.18 Opciones de transcodificación en VLC 59
Figura 2.19 Campo TTL para transmisiones con UDP 59
Figura 2.20 Ventana principal de la herramienta FaultLine 60
Figura 2.21 Medición de parámetros durante 60 segundos con FaultLine 61
Figura 2.22 Resultados de las mediciones del throughput con FaultLine 62
Figura 2.23 Resultados de las mediciones del jitter con FaultLine 62

CAPÍTULO 3

Figura 3.1 Sistema con m servidores 64
Figura 3.2 Esquema de análisis de los sistemas de encolamiento ‘Router PE1’ y ‘Router P’ 66
Figura 3.3 Tiempo de permanencia en el sistema vs el jitter del tráfico unicast UDP, a una tasa de 3 Mb/s 71
Figura 3.4 El jitter vs el porcentaje de pérdida de paquetes del tráfico unicast UDP a 4 Mb/s 77
Figura 3.5 El jitter vs el porcentaje de pérdida de paquetes del tráfico unicast UDP a 5 Mb/s 81
Figura 3.6 Tiempo de permanencia en el sistema vs el jitter del tráfico multicast @ 6 Mb/s 89
Figura 3.7 El jitter vs el porcentaje de pérdida de paquetes del tráfico multicast a 8 Mb/s 94

Figura 3.8 El jitter vs el porcentaje de pérdida de paquetes
del tráfico multicast a 10 Mb/s 98
Figura 3.9 Jitter presente en unicast vs jitter presente en multicast..... 105
Figura 3.10 Captura de tráfico multicast entre CE1 y PE1 108
Figura 3.11 Captura de tráfico multicast entre PE2 y CE2 109
Figura 3.12 Captura de tráfico multicast entre PE3 y CE3 109
Figura 3.13 Captura de tráfico multicast entre PE1 y P..... 110
Figura 3.14 Captura de tráfico multicast entre P y PE2..... 110
Figura 3.15 Captura de tráfico multicast entre P y PE3..... 111
Figura 3.16 Encapsulamiento de PIM en CEs 111
Figura 3.17 Encapsulamiento de PIM en los PEs y P 112

ÍNDICE DE TABLAS

CAPÍTULO 1

Tabla 1.1 Direcciones IP multicast clase D bien conocidas 3
Tabla 1.2 Direcciones IPv6 multicast bien conocidas..... 5

CAPÍTULO 2

Tabla 2.1 Comparación de los protocolos de enrutamiento multicast 40
Tabla 2.2 Direccionamiento IP de la red..... 43
Tabla 2.3 Características de los computadores fuente y receptor 43
Tabla 2.4 Significado de las banderas en Jperf..... 56

CAPÍTULO 3

Tabla 3.1 Resultados estadísticos de la generación de tráfico unicast UDP para 64 bytes @ 3 Mb/s 68
Tabla 3.2 Promedio de los resultados del experimento generación de tráfico unicast UDP @ 3 Mb/s para todos los tamaños de payload 69
Tabla 3.3 Intensidad de tráfico para el sistema PE1 y comprobación del porcentaje de pérdida de paquetes para todos los valores de payload unicast UDP @ 3 Mb/s..... 70
Tabla 3.4 Tiempos (retardos): de servicio, de espera en la cola, y de permanencia en el sistema PE1, para todos los valores de payload unicast UDP @ 3 Mb/s..... 71
Tabla 3.5 Correlación de Spearman entre el tiempo de permanencia en el sistema PE1 y el jitter para unicast UDP @ 3 Mb/s 73
Tabla 3.6 Resultados estadísticos de la generación de tráfico unicast UDP para 64 bytes @ 4 Mb/s 75
Tabla 3.7 Promedio de los resultados del experimento generación de tráfico unicast UDP @ 4 Mb/s para todos los tamaños de payload..... 76

Tabla 3.8 Intensidad de tráfico para el sistema Router PE1 y porcentaje de pérdida de paquetes para todos los valores de payload unicast UDP @ 4 Mb/s 76
Tabla 3.9 Correlación de Spearman entre la carga útil, el jitter y el porcentaje de pérdida de paquetes en el sistema PE1 para unicast UDP @ 4 Mb/s 78
Tabla 3.10 Resultados estadísticos de la generación de tráfico unicast UDP para 64 bytes @ 5 Mb/s 80
Tabla 3.11 Promedio de los resultados del experimento generación de tráfico unicast UDP @ 5 Mb/s para todos los tamaños de payload 80
Tabla 3.12 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de payload unicast UDP @ 5 Mb/s 81
Tabla 3.13 Correlación de Spearman entre la carga útil, el jitter y el porcentaje de pérdida de paquetes en el sistema PE1 para unicast UDP @ 5 Mb/s 82
Tabla 3.14 Promedio de los resultados de la generación de tráfico unicast TCP 84
Tabla 3.15 Factor de intensidad de tráfico para el sistema Router PE1 para todos los valores de payload en unicast TCP 85
Tabla 3.16 Retardos de servicio, de espera en la cola, y de permanencia en el sistema Router PE1 para todos los valores de payload en unicast TCP 85
Tabla 3.17 Resultados estadísticos de la generación de tráfico multicast para 64 bytes @ 6 Mb/s 86
Tabla 3.18 Promedio de los resultados del experimento generación de tráfico multicast @ 6 Mb/s para todos los tamaños de payload 87
Tabla 3.19 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de payload en multicast @ 6 Mb/s 88

Tabla 3.20 Retardos de servicio, de espera en la cola, y de permanencia en el sistema PE1 para todos los valores de payload en multicast @ 6 Mb/s 89
Tabla 3.21 Correlación de Spearman entre el tiempo de permanencia en el sistema PE1 y el jitter para multicast @ 6 Mb/s 90
Tabla 3.22 Resultados estadísticos de la generación de tráfico multicast para 64 bytes @ 8 Mb/s 92
Tabla 3.23 Promedio de los resultados del experimento generación de tráfico multicast @ 8 Mb/s para todos los tamaños de payload 93
Tabla 3.24 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de payload en multicast @ 8 Mb/s 93
Tabla 3.25 Correlación de Spearman entre la carga útil, el jitter y el porcentaje de pérdida de paquetes en el sistema PE1 para multicast @ 8 Mb/s 94
Tabla 3.26 Resultados estadísticos de la generación de tráfico multicast para 64 bytes @ 10 Mb/s 96
Tabla 3.27 Promedio de los resultados del experimento generación de tráfico multicast @ 10 Mb/s para todos los tamaños de payload 97
Tabla 3.28 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de payload en multicast @10 Mb/s 97
Tabla 3.29 Correlación de Spearman entre la carga útil, el jitter y el porcentaje de pérdida de paquetes en el sistema Router PE1 para multicast @ 10 Mb/s 99
Tabla 3.30 Características principales del video a transmitir 101
Tabla 3.31 Resultados estadísticos de la emisión de video unicast 101
Tabla 3.32 Resultados estadísticos de la emisión de video multicast 101
Tabla 3.33 Intensidad de tráfico y retardos en el sistema PE1 en unicast *y* multicast 104

Tabla 3.34 Recolección de muestras de jitter en las emisiones de video unicast *y* multicast 104
Tabla 3.35 Correlación de Spearman y Kendall entre el jitter unicast y el jitter multicast en la emisión del video 106
Tabla 3.36 Replanteamiento de la correlación de Spearman y Kendall entre el jitter unicast y el jitter multicast en la emisión del video 107

ÍNDICE DE ECUACIONES

CAPÍTULO 3

Ecuación 3.1 Intensidad de tráfico 64
Ecuación 3.2 Intensidad de tráfico en función de λ, L y R 65
Ecuación 3.3 Intensidad de tráfico en función de los tiempos de servicio y arribo 65
Ecuación 3.4 Tiempo de permanencia en el sistema 65
Ecuación 3.5 Tiempo promedio de espera en la cola 65
Ecuación 3.6 Tasa de pérdida de paquetes en función de las tasas de arribo de los paquetes a los sistemas PE1 y P 66
Ecuación 3.7 Tasa de arribo de paquetes al sistema en función del throughput y del tamaño del paquete 69

RESUMEN

El presente proyecto de titulación busca brindar un análisis de la tecnología denominada *multicast* de redes privadas virtuales, valiéndose para ello de la implementación de tráfico *multicast* sobre un prototipo de red IP/MPLS, empleando dicha tecnología en un ambiente de laboratorio.

En el primer capítulo se describe la tecnología IP *multicast*, su particular terminología, los árboles de distribución *multicast*, así como los algoritmos de reenvío *multicast*. Además, se aborda el estudio de los protocolos de enrutamiento *multicast* para IPv4 e IPv6, principalmente a PIM (Protocolo Independiente de Multidifusión). De manera introductoria, se hace un estudio de *unicast* VPN en IP/MPLS, para luego detallar el tema concerniente a *multicast* VPN (mVPN) en entornos IP/MPLS.

En el segundo capítulo se escoge el protocolo de enrutamiento *multicast*, previo a un análisis, para implementarlo en la red IP/MPLS mVPN. Se realizan las respectivas configuraciones en los *routers* Cisco para desplegar tanto la tecnología *unicast* VPN como mVPN. Se presenta el generador de tráfico Jperf, así como el emisor de video VLC. Se elaboran dos ambientes de análisis de pruebas: *unicast* y *multicast*.

En el tercer capítulo se describe la implementación del ambiente de pruebas como tal. Se inyecta tráfico *unicast* sobre la red *unicast* VPN IP/MPLS, así como tráfico *multicast* sobre la red *multicast* VPN IP/MPLS, con el propósito de medir los parámetros como *throughput*, *jitter* y la pérdida de paquetes. Adicionalmente se presentan argumentos que contribuyen al análisis del comportamiento de estos tipos de tráfico sobre dichas tecnologías.

En el cuarto capítulo se proporcionan las conclusiones que se obtuvo de la elaboración de este proyecto, así como las recomendaciones a tomar en cuenta y las posibles líneas de investigación a seguir.

En la parte de Anexos se encuentran, principalmente, los archivos de configuración de los *routers* y manuales de generación de tráfico. El Anexo A contiene los archivos de configuración de cada uno de los *routers* empleados en el prototipo *unicast* y

multicast. El Anexo B describe los pasos a seguir para la generación de tráfico *unicast* y *multicast,* utilizando la herramienta Jperf. El Anexo C contiene los pasos para la emisión de video en ambientes *unicast* y *multicast,* utilizando el *software* de video VLC. El Anexo D detalla los tabulados correspondientes a la generación de tráfico *unicast* y *multicast* con Jperf y VLC. Finalmente, el Anexo E muestra un manual de análisis de datos con el programa para Estadística SPSS *STATISTICS.*

PRESENTACIÓN

Los proveedores de servicios (SP) manejan grandes volúmenes de información a través de sus infraestructuras de red, como por ejemplo IP/MPLS, en donde cada vez más la información y contenido multimedia se transmite en tiempo real. Esto implica que se debe gestionar adecuadamente esta información con la menor cantidad de recursos, para lograr una optimización de éstos con la incorporación de nuevas tecnologías, protocolos y arquitecturas de red aptas para este propósito.

Con el fin de distribuir información *multicast,* tales como datos financieros, *e-learning*, IPTV, música en línea, entre otros, a varios lugares a la vez y al mismo tiempo, surge la idea de la tecnología *multicast* IP. Es por eso que, los SP deben tener la capacidad de brindar tecnologías, tales como *multicast* VPN, a través de su infraestructura IP/MPLS. Aunque este tema posee varios años desde su creación, muchos de los SP internacionales ya cuentan con esta infraestructura; sin embargo, la mayor parte de nuestro mercado local aún no la despliega.

Por esta razón, este proyecto de titulación busca brindar un aporte de este tema a aquellas empresas o SP que desean optimizar sus recursos tecnológicos y satisfacer a sus clientes con un buen servicio, al mismo tiempo y en diferentes localidades a la vez, con el único propósito de salvaguardar, siempre, el factor costo/beneficio, tanto para la entidad como para el usuario final.

1. MARCO TEÓRICO

1.1 INTRODUCCIÓN

La tecnología *multicast* presenta una característica popular utilizada principalmente por clientes empresariales en sus redes IP [1]. La característica que hace particular a *multicast* es aquella que permite una distribución eficiente de la información entre una sola fuente y múltiples receptores.

Este estudio está orientado a los Proveedores de Servicios (SP, por sus siglas en inglés), en cuya cartera está el brindar servicios *multicast* entre múltiples sitios de un cliente VPN (*Virtual Private Network*), que poseen una red *multicast* existente o tengan la intención de implementar esta característica dentro de su red. Aquella característica es conocida como *Multicast VPN* (MVPN, por sus siglas en inglés).

1.2 IP MULTICAST [1], [2]

IP *multicast* es una tecnología diseñada para reducir tráfico y a la vez entregar un solo *stream*[1] de información a cientos o miles de clientes corporativos o residenciales. Como se observa en la Figura 1.1, existen tres modos de comunicación: *unicast*, *broadcast* y *multicast*.

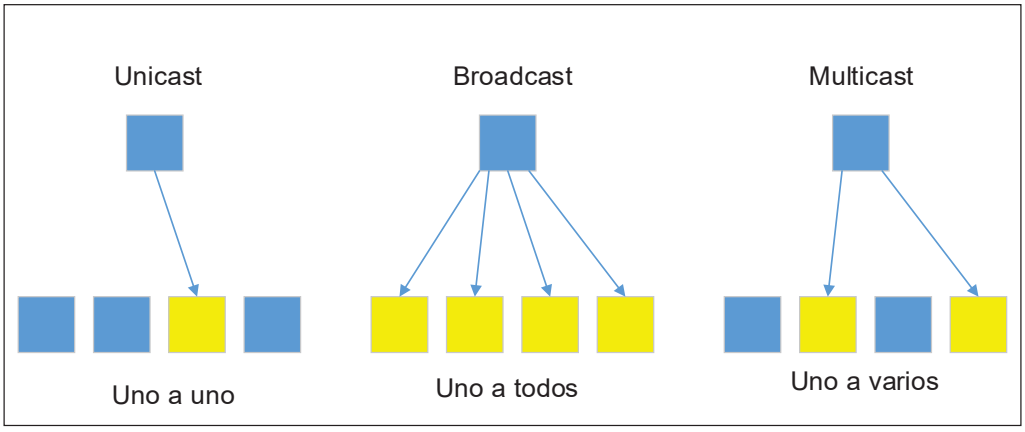

Figura 1.1 Modos de transmisión [2]

En comparación con IP *unicast*, IP *multicast* posee la capacidad de minimizar la carga de información en los *hosts,* tanto en el envío como en la recepción, además

[1] *Stream* es la transmisión o flujo de información.

de reducir el tráfico total de la red. Dentro de una red *multicast*, los *routers* son responsables de replicar y distribuir el contenido *multicast* a todos los *hosts* que pertenecen a un grupo *multicast* en particular.

Los *routers* usan protocolos de enrutamiento *multicast* tales como PIM (*Protocol Independent Multicast*) para construir árboles de distribución y transmitir contenido *multicast*. En cambio, a nivel de las aplicaciones *unicast* tradicionales se requiere que una fuente transmita una copia por cada receptor individual en el grupo.

IP *multicast* también se emplea en las siguientes tecnologías:

- Redes IPv4
- Redes IPv6
- MPLS VPN
- Redes móviles e inalámbricas

1.2.1 DIRECCIONAMIENTO MULTICAST IPv4

1.2.1.1 Direccionamiento multicast a nivel de capa 3 [3], [4]

1.2.1.1.1 Direcciones IP multicast bien conocidas

Los paquetes *multicast* tienen una dirección fuente *unicast* y una dirección de destino *multicast*; debido a esto, un grupo *multicast* IP está asociado a una única dirección IP *multicast*. En la Tabla 1.1 se describen las direcciones IP *multicast* bien conocidas pertenecientes a la clase D.

1.2.1.1.2 Rango de Direcciones IP multicast [5]

El rango de direcciones 224.0.0.0 a 239.255.255.255 representa el espacio de direcciones IPv4 *multicast* y está reservado para todo tipo de aplicaciones *multicast*. El rango de direcciones 224.0.0.0 a 224.0.0.255 es asignado por la IANA (*Internet Assigned Numbers Authority*, Autoridad de Números Asignados a Internet) a protocolos de red sobre segmentos locales.

El rango de direcciones 224.0.1.0 a la 224.0.1.255 es asignado también por la IANA a los protocolos que son reenviados a toda la red. Los *routers* reenvían los paquetes con las direcciones de destino utilizadas dentro de este intervalo. El intervalo de direcciones que va desde la dirección IP 232.0.0.0 hasta la 232.255.255.255 se

emplea para las aplicaciones SSM (*Source-Specific Multicast,* Multidifusión de Fuente Específica).

DIRECCIÓN	USO
224.0.0.1	Todos los *hosts multicast*
224.0.0.2	Todos los *routers multicast*
224.0.0.4	*Routers* DVMRP[2]
224.0.0.5	Todos los *routers* OSPF
224.0.0.6	*Routers* Designados OSPF[3]
224.0.0.9	*Routers* RIPv2
224.0.0.10	*Routers* EIGRP
224.0.0.13	*Routers* PIM
224.0.0.22	IGMPv3
224.0.0.25	RGMP[4]
224.0.1.39	Cisco-RP-Announce[5]
224.0.1.40	Cisco-RP-Discovery[6]

Tabla 1.1 Direcciones IP *multicast* clase D bien conocidas [5]

El rango de direcciones 233.0.0.0 hasta la 233.255.255.255 es denominado de direccionamiento GLOP y se utiliza para asignar, de forma automática, 256 direcciones IP *multicast* a cualquier empresa propietaria de una ASN (*Autonomous System*, Sistema Autónomo) registrado. El intervalo de direcciones 239.0.0.0 a la 239.255.255.255 se utiliza para dominios *multicast* privados y son llamadas direcciones *multicast* administrativas; estas direcciones no son enrutadas entre dominios, de tal manera que pueden ser reutilizadas. Las direcciones IP *multicast* restantes pertenecientes a la clase D, pueden ser empleadas por cualquier entidad para enrutar tráfico a cualquier organización en Internet y son asignadas de manera temporal; además, son significativas a nivel global.

1.2.1.2 Direccionamiento multicast a nivel de capa 2 [4], [5]

Los dispositivos de capa enlace reconocen tráfico *multicast*, debido a que cada dirección IP *multicast* está asociada a una dirección MAC. Los primeros 24 bits de

---

[2] *Distance Vector Multicast Routing Protocol,* Protocolo de enrutamiento *multicast* por vector distancia
[3] En OSPF, es el *router* con el valor de prioridad más alta, es decir, la dirección IP más alta de todas las interfaces *loopbacks* configuradas
[4] *Router-port Group Management Protocol,* Protocolo propietario de Cisco utilizado entre *routers multicast* y *switches*
[5] Mensaje de Anuncio *Rendezvous Point* de Cisco
[6] Mensaje de Descubrimiento *Rendezvous Point* de Cisco

la dirección MAC (que posee 48 bits) identifican al código del fabricante y corresponden al prefijo 01005E, y el bit número 25 es siempre 0. Los restantes 23 bits son copiados a partir de los 23 bits del extremo derecho de la dirección IP, como se observa en la Figura 1.2.

Lamentablemente, este método no asigna una dirección MAC *multicast* única por cada dirección IP *multicast*, debido a que los últimos 23 bits de la dirección IP son asignados a la dirección MAC. Como ejemplo, se menciona la dirección IP 238.10.24.5 que produce con claridad la misma dirección MAC 0100.5E0A.1805 que la dirección IP *multicast* 228.10.24.5.

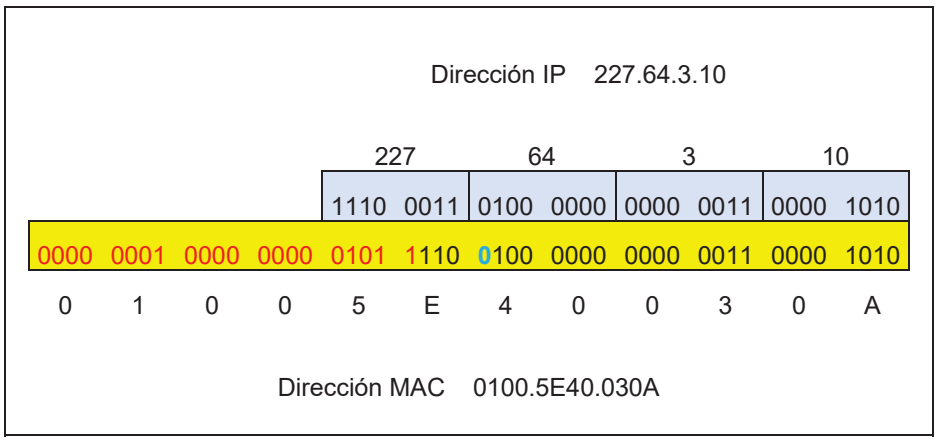

Figura 1.2 Relación entre las direcciones *multicast* IP y MAC [5]

Si accidentalmente esto sucediera, un paquete de una aplicación *multicast* IP distinta podría ser identificada como de capa 3, siendo descartada. Sin embargo, los administradores de red deberían ser cuidadosos cuando implementen aplicaciones *multicast*. De esta manera, ellos pueden prevenir direcciones IP que producen direcciones MAC idénticas.

1.2.2 DIRECCIONAMIENTO MULTICAST IPv6

1.2.2.1 Direccionamiento multicast a nivel de capa 3 [26]

Las direcciones IPv6 *multicast* tienen los primeros 8 bits fijados a 1111 1111, por ello, una dirección IPv6 *multicast* siempre inicia con el prefijo FF. La Tabla 1.2 detalla las direcciones IPv6 *multicast* bien conocidas. A continuación de los 8 primeros bits, la dirección *multicast* incluye una estructura adicional, que consta de los campos bandera (4 bits), alcance (4 bits) y el grupo multicast (112 bits).

DIRECCIÓN	DESCRIPCIÓN
FF02::1	Todos los nodos en un segmento de red local
FF02::2	Todos los *routers* en un segmento de red local
FF02::5	*Routers* OSPF v3
FF02::6	*Routers* designados OSPF v3
FF02::8	*Routers* IPv6 para IS-IS
FF02::9	*Routers* RIP
FF02::A	*Routers* EIGRP
FF02::D	*Router* PIM
FF02::16	Reportes MLD v2
FF02::1:2	Todos los servidores DHCP y transmisión de agentes en un segmento de red local
FF05::1:3	Todos los servidores DHCP en un sitio de red local

Tabla 1.2 Direcciones IPv6 *multicast* bien conocidas

1.2.2.2 Direccionamiento multicast a nivel de capa 2 [23]

IPv6 toma un enfoque similar al mapeo de las direcciones IPv4 *multicast* a las direcciones *multicast* de capa 2. El algoritmo de mapeo exacto depende del tipo de medio. En el caso de Ethernet, el método de mapeo de una dirección IPv6 *multicast* a una dirección *multicast* Ethernet es el de anteponer el valor 0x3333 a los últimos cuatro bytes de la dirección IPv6 *multicast* para formar una dirección *multicast* Ethernet de 48 bits. Como ejemplo se citan los servidores DHCPv6 asignados por la IANA, FF05::1:3, que es mapeada a la dirección MAC Ethernet 33-33-00-01-00-03 como se muestra en la Figura 1.3.

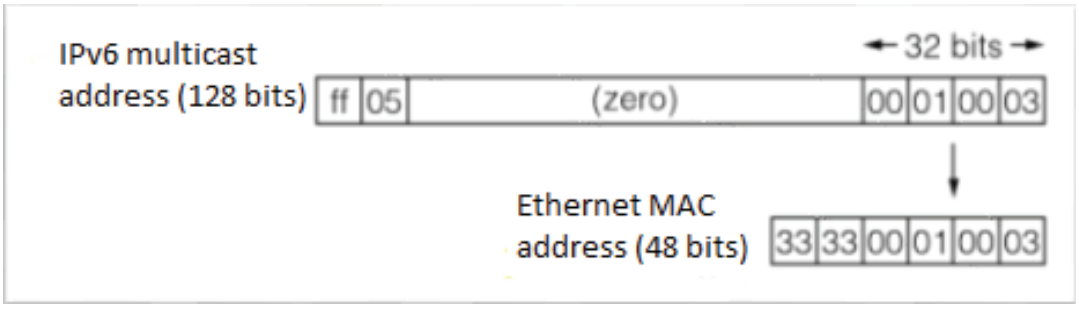

Figura 1.3 Mapeo de las direcciones *multicast* IPv6 a Ethernet [23]

1.2.3 TERMINOLOGÍA IP MULTICAST [14]

Multicast tiene su propio conjunto particular de términos y acrónimos que se aplican a redes y dispositivos de enrutamiento IP *multicast*. En una red *multicast*, el componente clave es el 'dispositivo de enrutamiento', el cual es capaz de replicar paquetes y, por lo tanto, capaz de replicar *multicast*.

Los dispositivos de enrutamiento en la red IP *multicast* tienen exactamente la misma topología que una red basada en *unicast*, al emplear un 'protocolo de enrutamiento *multicast*' para construir un 'árbol de distribución' que conecte los receptores a las 'fuentes'. En terminología *multicast*, el árbol de distribución está 'enraizado o arraigado (*rooted*)' a la fuente, ya que la raíz del árbol de distribución es la fuente.

La interfaz del dispositivo de enrutamiento que conduce hacia la fuente es la interfaz de 'subida (*upstream*)', aunque también se utiliza el término menos preciso 'interfaz entrante'. Asimismo, la interfaz del dispositivo de enrutamiento que conduce hacia los receptores es la 'interfaz de bajada' (*downstream*), aunque el término menos preciso 'interfaz saliente' también se emplea.

Una de las complejidades de los protocolos de enrutamiento *multicast* es la necesidad de prevenir lazos de enrutamiento, debido al riesgo de tener paquetes replicados en varias ocasiones. Para prevenir esto, existen algunas estrategias *multicast*: *Reverse Path Forwarding* (RPF) y *Shortest Path Tree* (SPT) que ayudan a prevenir lazos de enrutamiento mediante la definición de rutas de enrutamiento de diferentes maneras.

1.2.3.1 Reverse Path Forwarding (RPF) [9]

Cada paquete *multicast* recibido en una interfaz de un *router* está sujeto a un chequeo RPF. El chequeo RPF determina si el paquete es reenviado o descartado, lo que previene los lazos de paquetes en una red. RPF opera de la siguiente forma:

- Cuando un paquete *multicast* arriba a un *router*, la dirección fuente de ese paquete se chequea para asegurarse que la interfaz de entrada, en verdad, va hacia la fuente.
- Si el chequeo pasa, el paquete *multicast* se reenvía a las interfaces pertinentes (pero no a la interfaz RPF).
- Si el chequeo RPF falla, el paquete se descarta.

La interfaz que se utiliza para el chequeo RPF se denomina interfaz RPF. PIM usa la información que se encuentra en la tabla de enrutamiento *unicast* para determinar la interfaz RPF. La Figura 1.4 muestra el proceso de un chequeo RPF para un paquete que arriba a una interfaz equivocada. Un paquete *unicast* de la fuente

192.168.0.10 arriba a la interfaz Gi0/0. Un chequeo de la tabla de enrutamiento *multicast* muestra que la red 192.168.0.0 es accesible a la interfaz Gi1/1, no a la Gi0/0; por lo tanto el chequeo RPF falla y el paquete se descarta.

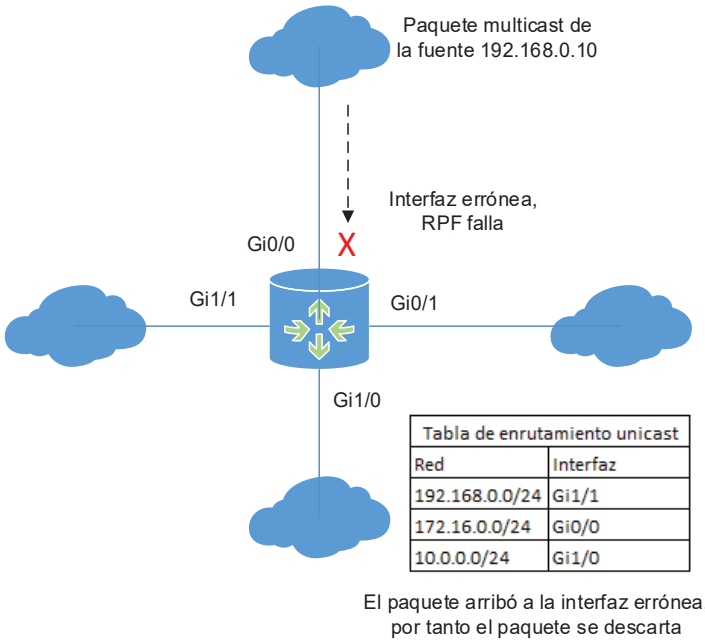

Figura 1.4 Chequeo RPF fallido

Mientras que la Figura 1.5 muestra el chequeo RPF para un paquete *multicast* que llega a la interfaz correcta. El paquete *multicast* arriba a la interfaz Gi1/1, el cual empareja la interfaz para esta red en la tabla de enrutamiento *unicast*. Por lo tanto, el chequeo RPF pasa y el paquete *multicast* se replica a aquellas interfaces salientes para el grupo *multicast*.

1.2.3.2 Shortest Path Tree (SPT) – Árbol de camino más corto [25]

El proceso de un enrutamiento óptimo eventualmente resulta en encontrar el árbol de camino más corto. El camino o trayecto desde la raíz a cada destino es el camino más corto. Sin embargo, el número de árboles y la formación de éstos en enrutamiento *unicast* y *multicast* son diferentes.

En el enrutamiento *unicast*, cada *router* en el dominio tiene una tabla que define un árbol de camino más corto a posibles destinos. Mientras que, en el enrutamiento *multicast*, cada *router* involucrado necesita construir un árbol de camino más corto para cada grupo.

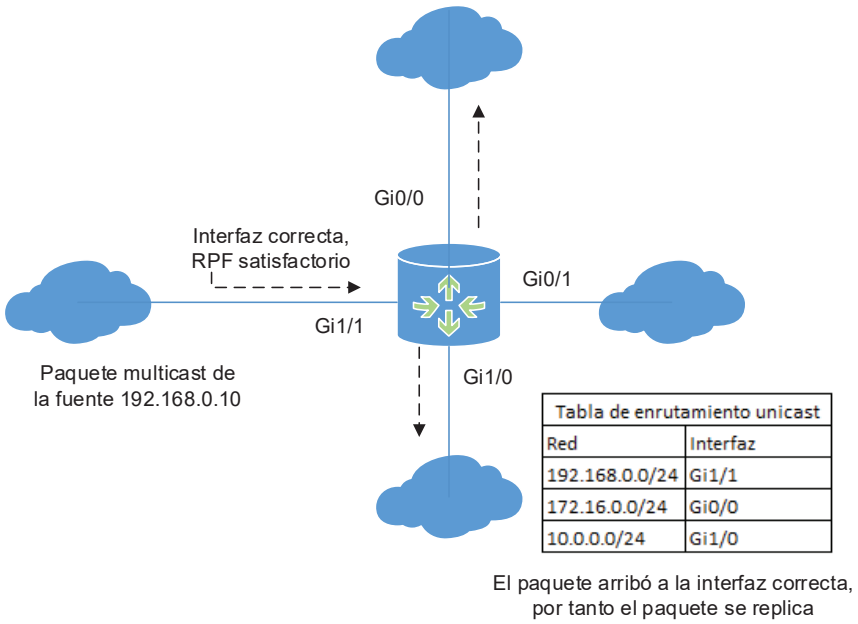

Figura 1.5 Chequeo RPF satisfactorio

Para el caso de los árboles basados en la fuente, cada *router* necesita tener un árbol de camino más corto para cada grupo. Por otro lado, para el caso de los árboles compartidos, solamente el *router* de *core*, el cual posee un árbol de camino más corto, está involucrado en *multicast*.

1.2.3.3 Terminología de rama y hoja en multicast [14]

Cada subred con *hosts* en un dispositivo de enrutamiento que posee, al menos, un receptor interesado es una 'hoja' en el árbol de distribución. Los dispositivos de enrutamiento pueden tener múltiples hojas en diferentes interfaces y deben enviar una copia del paquete IP *multicast* en cada interfaz con, al menos, una hoja.

Cuando una nueva hoja se añade al árbol (la interfaz de la subred con el *host* que previamente no ha recibido copias de paquetes *multicast*), una nueva 'rama' se construye, la hoja se junta o se conecta al árbol, y los paquetes replicados se envían fuera de la interfaz.

El número de hojas en una interfaz en particular no afecta al dispositivo de enrutamiento. Esta acción es la misma para una sola hoja o para muchas. Cuando una rama no contiene hojas debido a que no existen *hosts* interesados en la interfaz del dispositivo de enrutamiento que conduce a esa subred IP, entonces la rama es

'podada (*pruned*)' del árbol de distribución y aquellos paquetes que no son *multicast* se envían fuera de esa interfaz.

Los paquetes se replican y se envían por varias interfaces sólo cuando los árboles de distribución se ramifican en un dispositivo de enrutamiento. Todas las colecciones de *hosts* reciben el mismo *stream* de paquetes IP, usualmente de la misma fuente *multicast*, y son llamados 'grupos'.

En las redes IP *multicast*, el tráfico se entrega a los grupos *multicast* basados en una dirección IP *multicast*, o 'grupo *multicast*'. Los grupos determinan la ubicación de las hojas, y las hojas determinan las ramas de la red *multicast*.

1.2.4 ÁRBOLES DE DISTRIBUCIÓN MULTICAST [9]

Los paquetes *multicast* se envían a través de la red usando árboles de distribución *multicast*. La red es responsable de replicar el mismo paquete a cada punto de bifurcación en el árbol; esto significa que, solamente una copia del paquete viaja sobre un enlace particular de la red, lo que hace que los árboles *multicast* sean extremadamente eficientes para distribuir la misma información a muchos receptores.

1.2.4.1 Árboles de Fuente (Source Trees)

El *host* origen (fuente) del tráfico *multicast* está localizado en la raíz del árbol, y los receptores están ubicados en las terminaciones de las ramas. Este tipo de árbol posee una tabla de envío *multicast* que consiste de una serie de entradas de estado *multicast* que se almacenan en la caché del *router*. Las entradas de estado para un árbol fuente emplean la notación (S, G), en donde la letra S representa la dirección IP del origen o fuente, y la G representa la dirección IP del grupo.

Un árbol fuente implica que la ruta o camino entre la fuente *multicast* y los receptores debe ser la ruta disponible más corta; por consiguiente, los árboles fuente son también denominados como árboles de camino más corto.

Existe un árbol fuente independiente por cada fuente que se encuentre transmitiendo paquetes *multicast*, si y solo si aquellas fuentes están transmitiendo datos al mismo grupo; es decir que habrá una entrada de estado de envío (S, G) por cada fuente activa en la red.

Un ejemplo de este tipo de árbol, se visualiza en la Figura 1.6, en donde la fuente 196.7.25.12 de la raíz del árbol está transmitiendo paquetes *multicast* al grupo destino 239.194.0.5, de los cuales hay dos receptores interesados. La entrada de envío para el *stream multicast* es (196.7.25.12, 239.194.0.5).

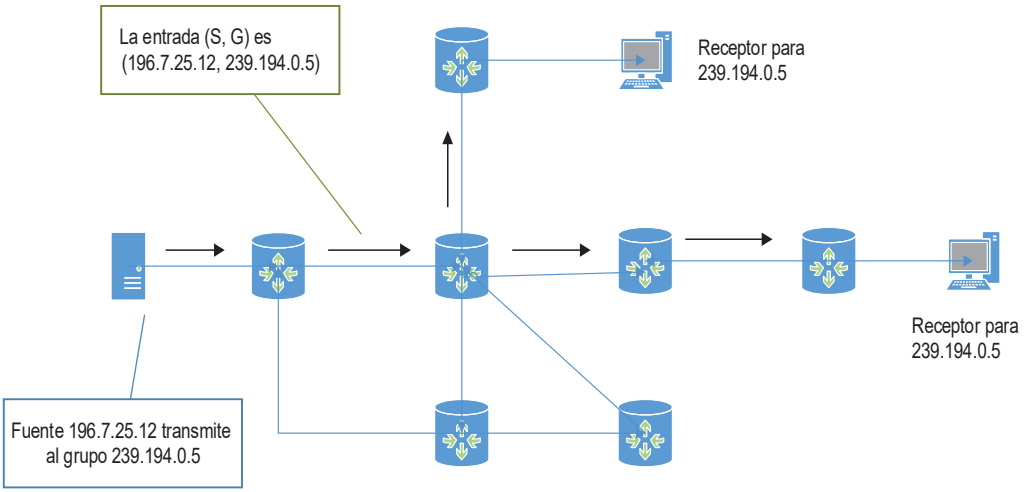

Figura 1.6 Ejemplo de un árbol de distribución fuente [9]

Un punto importante acerca de los árboles fuente es que un extremo receptor sólo puede unirse a este árbol si tiene conocimiento de la dirección IP de la fuente que está transmitiendo al grupo en el que está interesado; es decir que, para unirse a un árbol fuente, una juntura (S, G) se debe emitir desde ese extremo receptor.

1.2.4.2 Árboles Compartidos (Shared Trees)

Los árboles compartidos difieren de los de fuente en que la raíz del árbol es un punto común de encuentro en algún lugar de la red. Este punto común se denomina *Rendezvous Point* (RP, por sus siglas en inglés) y es el punto en el cual los receptores se juntan para aprender de las fuentes activas; por ende, las fuentes *multicast* deben transmitir su tráfico hacia el RP.

Cuando los receptores se unen a un grupo *multicast* en un árbol compartido, la raíz del árbol será siempre el RP y el tráfico *multicast* será transmitido desde el RP a los receptores. En tal virtud, el papel del RP es el de ser un intermediario entre las fuentes y los receptores. Además, un RP puede ser la raíz de todos los grupos *multicast* en la red o, a su vez, diferentes rangos de grupos *multicast* pueden ser asociados con diferentes RP.

La notación que usan los árboles compartidos en sus entradas de envío *multicast* es (*, G), debido a que todas las fuentes de un grupo particular comparten el mismo árbol, y el símbolo * o *wildcard* representa todas esas fuentes, como lo muestra la Figura 1.7. En este ejemplo, el tráfico *multicast* de los *hosts* origen (fuentes) 196.7.25.18 y 196.7.25.12, que no necesariamente pertenecen a la misma red de origen, viajan hacia el RP y a continuación se dirigen a los dos receptores. Existen dos entradas de enrutamiento, una por cada grupo *multicast* que comparte el árbol y que son las (*, 239.194.0.5) y (*, 239.194.0.7).

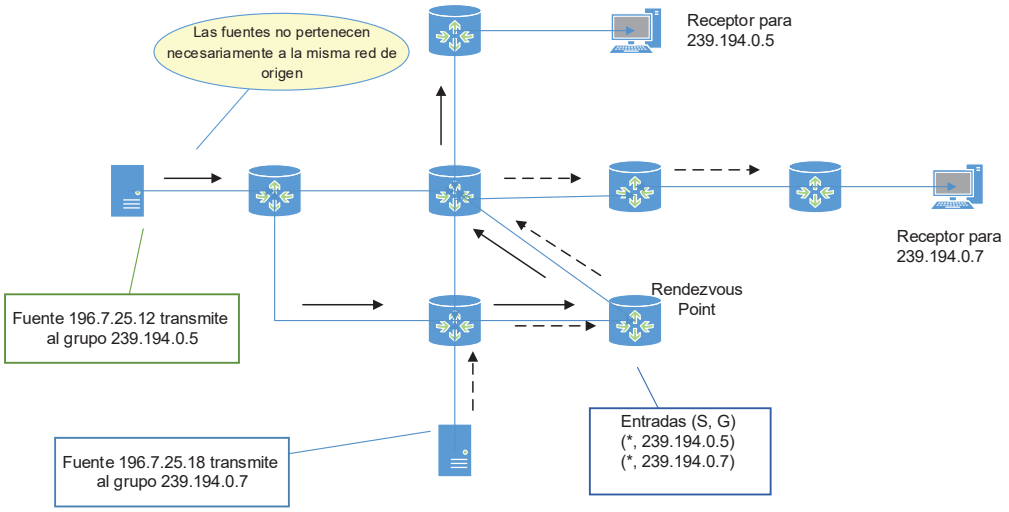

Figura 1.7 Ejemplo de un árbol de distribución compartido [9]

Los árboles compartidos permiten al extremo receptor, obtener los datos de un grupo *multicast* sin tener la necesidad de conocer la dirección IP de la fuente, ya que la única dirección IP que debe conocer es la del RP. Este punto se puede configurar de forma estática o dinámica en los *routers* a través de mecanismos tales como Auto-RP[7] (*Auto Rendezvous Point*) o *Bootstrap Router* (BSR, por sus siglas en inglés).

1.3 PROTOCOLOS DE INTERACCIÓN ENTRE MIEMBROS MULTICAST

1.3.1 INTERNET GROUP MANAGEMENT PROTOCOL (IGMP - IPV4) [2], [3]

IGMP, por sus siglas en inglés, es el protocolo utilizado por los receptores finales o *hosts* para unirse o dejar un grupo de *hosts multicast*. La información de los

[7] Estos mecanismos se citan únicamente como referencia. No forman parte del estudio.

miembros del grupo es intercambiada entre un *host* específico y el *router multicast* más cercano; sin embargo, un receptor puede pertenecer a uno o a muchos grupos *multicast*.

Un mensaje de los miembros del grupo IGMP expresa el deseo de recibir tráfico destinado a un grupo *multicast*. Para ello, IGMP posee dos fases [6]:

- Fase 1: Cuando se forma un nuevo grupo *multicast*, un *host* envía un mensaje IGMP a la dirección *multicast* del grupo declarando su pertenencia. Seguidamente, los *routers multicast* locales reciben el mensaje y establecen el enrutamiento necesario para propagar la información de pertenencia del grupo a otros *routers multicast* a través de la red.
- Fase 2: Debido a que esta pertenencia es dinámica, los *routers multicast* locales, de forma periódica, sondean a los *hosts* en la red local para determinar si alguno de los *hosts* aún siguen siendo miembro de cada grupo. Si algún *host* responde para un grupo dado, el *router* mantiene el grupo activo; si ninguno de los *hosts* reporta su pertenencia en un grupo luego de varios sondeos, el *router multicast* asume que ninguno de los *hosts* de la red permanecen en el grupo y suspende los anuncios de las pertenencias de grupos a otros *routers multicast*.

1.3.1.1 IGMPv1

Proporciona a los *hosts* mecanismos para unirse a grupos y reportar los miembros del grupo, así como un mecanismo enrutador con el fin de consultar la participación del grupo. Muchas de las aplicaciones ya no usan esta versión.

1.3.1.2 IGMPv2

Esta versión es la más utilizada y desarrollada; provee todos los mecanismos de IGMPv1, así como un mecanismo para los *hosts* de abandonar un grupo *multicast*, y un mecanismo de enrutador para el envío de consultas a los miembros de un grupo específico.

1.3.1.3 IGMPv3

Es el estándar para la gestión de pertenencia a grupos *multicast*, e incluye la compatibilidad con SSM (*Source Specific Multicast*) que permite a los *hosts* unirse

a *streams multicast* en función de cada fuente. Esta versión maneja consultas, reportes y abandonos en fuentes específicas.

1.3.2 MULTICAST LISTENER DISCOVERY (MLD - IPv6) [7], [8]

El protocolo de Descubrimiento de Oyentes *Multicast* (MLD, por sus siglas en inglés) es equivalente al protocolo IGMP, pero en IPv6. La versión actual del protocolo es MLDv2 y es interoperable con su antecesor MLDv1. MLD es utilizado por *hosts* y *routers* IPv6 para transmitir información sobre los miembros de un grupo.

Una vez que el *host* anuncia su pertenencia, tal como lo fue en IGMP, un *router* de la red utiliza MLDv2 para sondear al *host* de forma periódica, para determinar si ese *host* es aún miembro del o de los grupos. Un conjunto de *routers multicast* en una red dada cooperan para elegir un '*router* consultor' que, periódicamente, envía consultas; sin embargo, si el '*router* consultor' actual llega a fallar, otro *router multicast* de la red se hace cargo de aquella responsabilidad.

En MLDv2, se definen tres tipos de mensajes de consulta que los *routers* envían: consultas generales (*general queries*), consultas específicas de direcciones *multicast* (*multicast address specific queries*) y consultas de dirección *multicast* y de fuente específica (*multicast address and source specific queries*) [6]. Al igual que IGMP, un *router multicast* envía consultas generales a los *hosts* para que respondan a qué grupos *multicast* se encuentran asociados.

1.4 ALGORITMOS DE REENVÍO MULTICAST [10], [11], [24]

Para proveer el servicio de entrega de paquetes *multicast* es necesario definir los protocolos de enrutamiento *multicast*, los cuales serán los responsables de la construcción de los árboles *multicast* y de realizar el reenvío de paquetes *multicast*. Para tal propósito, se abordarán una serie de algoritmos que pueden ser utilizados en este tipo de protocolos.

1.4.1 ALGORITMO DE INUNDACIÓN

Este algoritmo consiste en que, cuando un *router* recibe un paquete *multicast*, verifica si lo ha recibido con anterioridad o si es la primera vez que lo recibe. Si se trata de la primera vez, el *router* redirigirá el paquete *multicast* a todas las interfaces

excepto por aquella que la recibió; si es todo lo contrario, el paquete será descartado y de esta forma, se asegura que todos los *routers* de la red reciban una copia del paquete, aunque no estén suscritos a un grupo.

1.4.2 ALGORITMO DE ÁRBOL DE EXPANSIÓN (SPANNING TREE)

Este algoritmo selecciona un subconjunto de enlaces para definir una estructura de árbol, de tal manera que exista un único camino activo entre dos *routers*, lo que permite obtener una topología libre de lazos. Debido a que este árbol se expande hacia todos los nodos de una red, se lo denomina árbol de expansión. Cuando un *router* recibe un paquete *multicast*, lo reenvía por todos los enlaces que forman parte del árbol de expansión, excepto por el enlace que recibió el paquete *multicast*.

En la Figura 1.8 se aprecia una pequeña red de prueba constituida por siete nodos y nueve enlaces, luego se presenta la misma red aplicada con el algoritmo de árbol de expansión, cuya fuente es el *router* S.

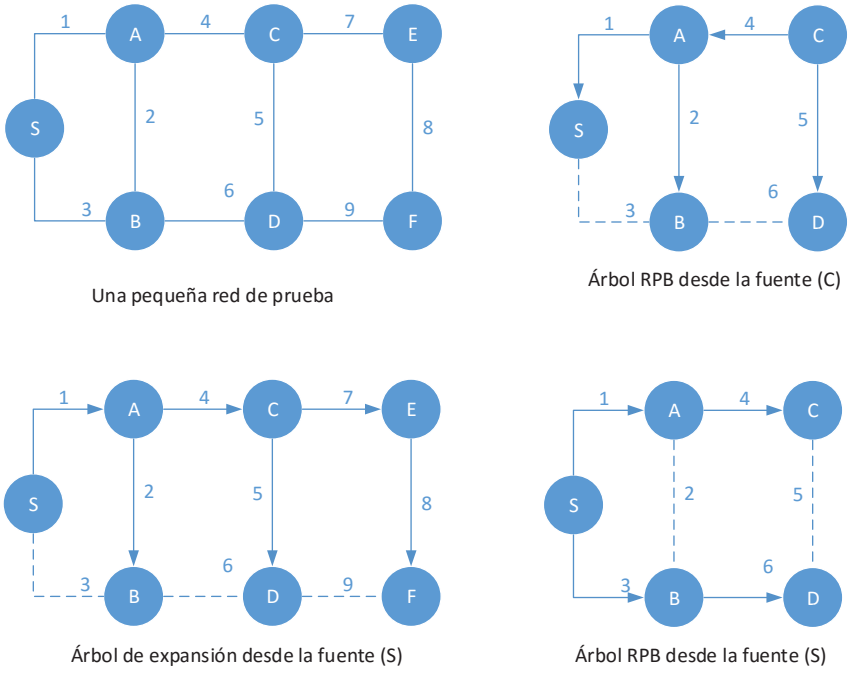

Figura 1.8 Representación de los árboles de expansión y RPB

1.4.3 ALGORITMO REVERSE PATH BROADCASTING (RPB)

Este algoritmo construye un árbol implícito por cada fuente existente en la red, en comparación de construir un árbol de expansión para toda la red. Es por ello que,

si existen muchas fuentes para un mismo grupo, se procede a construir un árbol de expansión para cada par de unión (S, G).

En la Figura 1.8 se muestra un ejemplo de árbol RPB: la red está compuesta por cinco nodos, seis enlaces y dos fuentes, C y S. Tanto para la fuente C como para S se construyen sendos árboles de expansión, en tal virtud, existirán dos pares de unión que serán (S, G) y (C, G).

1.4.4 ALGORITMO REVERSE PATH MULTICASTING (RPM)

Este algoritmo construye un árbol de expansión cuando existen *routers* que tienen subredes que, a su vez, poseen miembros de un grupo. Los *routers* que están en el borde de la red y no tienen *routers* intermedios en el árbol son llamados '*routers* hoja', tal como se ilustra en la Figura 1.9.

Si las subredes conectadas al *router* hoja no tienen miembros grupales, el *router* puede transmitir un mensaje de poda a su 'enlace padre', informando al '*router* de *upstream*' que no debe enviar paquetes para un par (S, G) en particular, en la interfaz hija que recibe el mensaje de poda. Los mensajes de poda son enviados un solo salto hacia atrás.

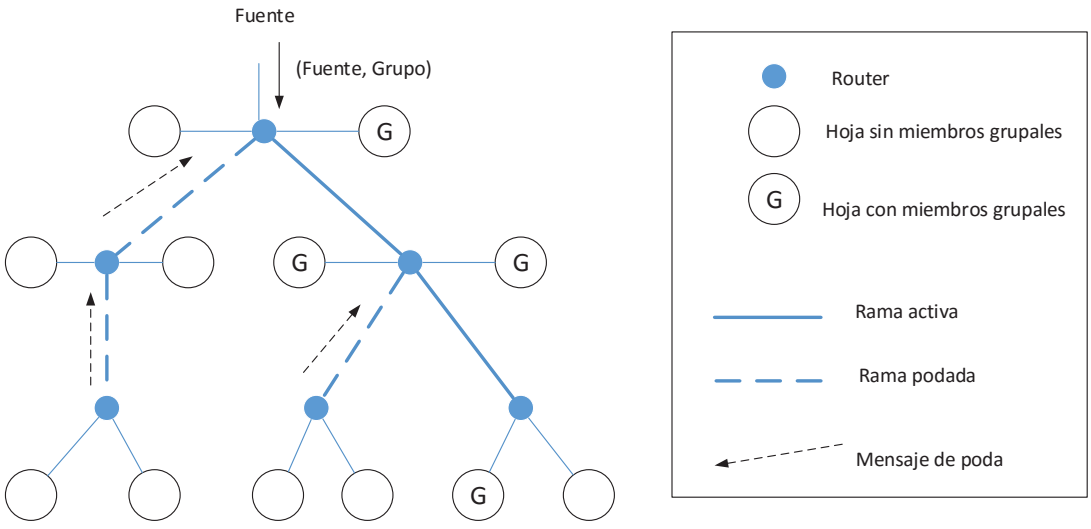

Figura 1.9 Representación del árbol RPM

La sucesión de mensajes de poda crea un árbol de reenvío *multicast* que contiene solamente ramas 'vivas o activas', es decir, las ramas que conectan a los miembros de un grupo activo.

1.5 PROTOCOLOS DE ENRUTAMIENTO MULTICAST

1.5.1 CORE BASED TREE (ÁRBOL BASADO EN EL NÚCLEO) – CBT [12]

CBT construye el árbol de distribución basándose en un *core*, que representa el centro del grupo *multicast*. En el instante en que un nuevo miembro envía un mensaje para unirse al grupo, éste va por medio del camino más corto hasta el centro, actualizando la información en los *routers* a lo largo del trayecto.

CBT usa las tablas de cualquier protocolo *unicast*, a diferencia de DVMRP (*Distance Vector Multicast Routing Protocol*) y MOSPF (*Multicast Open Shortest Path First*) que usan RIP y OSPF respectivamente. El problema con el protocolo de enrutamiento *multicast* CBT es la concentración de tráfico que generan las fuentes y cuyos flujos se colocan únicamente sobre los enlaces del árbol de distribución *multicast*.

1.5.2 DISTANCE VECTOR MULTICAST ROUTING PROTOCOL (PROTOCOLO DE ENRUTAMIENTO MULTICAST POR VECTOR DISTANCIA) – DVMRP [10], [13]

DVMRP es uno de los protocolos de enrutamiento *multicast* más antiguos y es un protocolo de vector distancia diseñado para soportar el envío de paquetes *multicast* a través de una red. Un fundamento clave introducido por DVMRP ha sido el de emplear distintos árboles de reenvío para cada uno de los grupos *multicast*.

DVMRP construye árboles *multicast* basados en la fuente usando algunas variantes del algoritmo RPB y cuya especificación original se derivó del protocolo RIP. La mayor diferencia entre RIP y DVMRP se da en que RIP, se preocupa en calcular el siguiente salto hacia un destino, mientras que DVMRP calcula el siguiente salto hacia la fuente.

1.5.3 MULTICAST OPEN SHORTEST PATH FIRST (OSPF MULTICAST) – MOSPF [12]

MOSPF es una extensión del protocolo *unicast* OSPF. OSPF posee una tabla de datos que es elaborada por cinco tipos de anuncios denominados LSAs (*Link State Advertisements*) y en el que, para MOSPF, se agrega un nuevo LSA que descubre la membresía del grupo a partir de IGMP.

Cuando un paquete arriba a un *router*, éste construye un árbol de camino más corto SPT, mediante el algoritmo Dijkstra, y reenvía el paquete *multicast* a través del SPT hasta los receptores. Los árboles en cada *router* son construidos bajo demanda; sin embargo, esta característica es poco escalable cuando existe mucha interactividad entre los grupos *multicast* y muchas fuentes.

1.5.4 PROTOCOL INDEPENDENT MULTICAST (PROTOCOLO INDEPENDIENTE MULTICAST) – PIM [9]

El protocolo *multicast* más ampliamente desarrollado es PIM. Usa la tabla de enrutamiento *unicast* para descubrir si el paquete *multicast* ha llegado a la interfaz correcta. Se han creado y están disponibles muchas variantes de PIM.

1.5.4.1 Dense Mode (Modo denso) – PIM DM [14]

En este modo de PIM, la suposición es que casi todas las subredes posibles tienen, al menos, un receptor esperando recibir el tráfico *multicast* desde la fuente; entonces, la red es inundada con el tráfico en todas las posibles ramas, luego éstas son podadas cuando las ramas no expresan un interés en recibir los paquetes, ya sea de manera explícita (por mensaje) o implícita (tiempo de espera agotado). Esta forma de operación del modo denso en *multicast* se puede apreciar en la Figura 1.10.

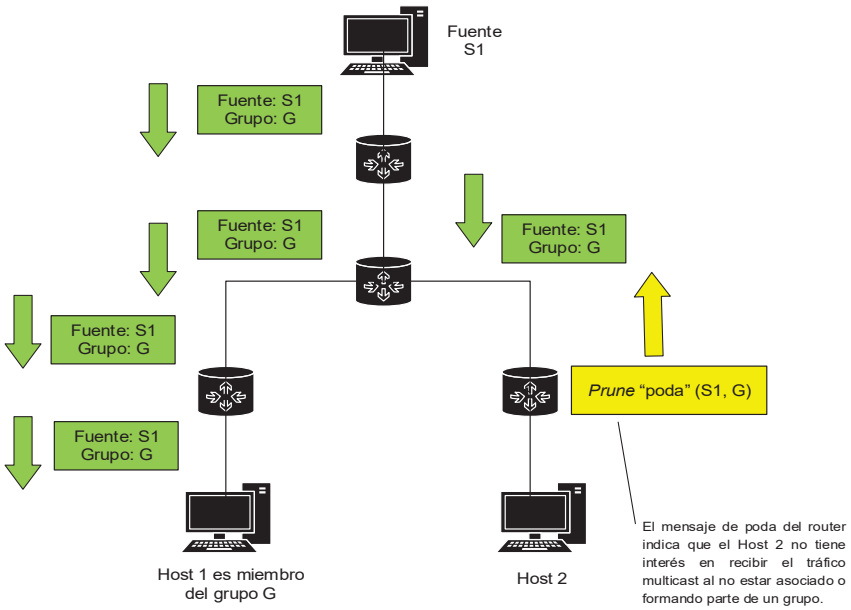

Figura 1.10 Funcionamiento de PIM – DM [2]

PIM DM permite a un dispositivo de enrutamiento usar cualquier protocolo de enrutamiento *unicast* y llevar a cabo chequeos RPF empleando la tabla de enrutamiento *unicast*. PIM DM tiene un mensaje de unión o juntura implícito, cuyos dispositivos de enrutamiento usan el método de 'inundación/poda' (*flooding and prune*) para entregar el tráfico a todas partes, y determinar los lugares en los cuales los receptores están desinteresados en recibir ese tráfico.

PIM DM usa los árboles de distribución basados en la fuente en la forma (S, G) al igual que todos los protocolos en modo denso. Las LAN son las redes apropiadas para ejecutar modo denso. Algunos protocolos *multicast*, especialmente los más antiguos, soportan únicamente el modo denso, lo cual los hace inapropiados para usarlos en el Internet. Soporta únicamente IPv4 [15].

1.5.4.2 Sparse Mode (Modo disperso) – PIM SM [2], [14]

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

Este protocolo *multicast* permite a un dispositivo de enrutamiento usar cualquier protocolo de enrutamiento *unicast* y llevar a cabo la comprobación RPF usando la tabla de enrutamiento *unicast*. PIM SM tiene un mensaje de unión o juntura explícito, de manera que los dispositivos de enrutamiento determinan en dónde se encuentran los receptores interesados y envían mensajes de unión *upstream* a sus vecinos, construyendo árboles desde los receptores hasta el RP, como se aprecia en la Figura 1.11.

PIM SM usa un dispositivo de enrutamiento RP como la fuente inicial de tráfico del grupo *multicast* y luego construye árboles de distribución en la forma (*, G) al igual que todos los protocolos en modo disperso. Las WAN son las redes apropiadas para implementar SM y, en efecto, una guía práctica *multicast* es el de no ejecutar modo denso en una WAN bajo ninguna circunstancia. Soporta tanto IPv4 como IPv6 [15].

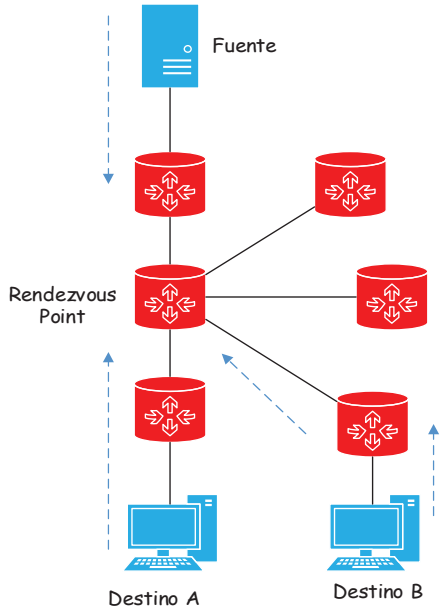

Figura 1.11 Funcionamiento de PIM – SM [5]

1.5.4.3 PIM Bidirectional (PIM bidireccional) – PIM BiDir [14]

Es una variación de PIM. PIM BiDir construye árboles compartidos bidireccionales que están enraizados en una dirección RP. El tráfico bidireccional no conmuta a árboles de camino más corto como PIM SM y es, por tanto, óptimo para el tamaño de los estados de enrutamiento en lugar de la longitud del camino. Esto significa que la latencia extremo a extremo podría ser mayor, comparada con PIM SM.

Las rutas PIM bidireccionales son siempre rutas (*, G), por tanto, este protocolo elimina la necesidad de rutas (S, G). Los árboles de grupos bidireccionales (*, G) llevan el tráfico en ambos sentidos: *upstream*, desde las fuentes hacia el RP y *downstream*, desde el RP hacia los receptores.

En consecuencia, las reglas estrictas basadas en la comprobación RPF presentes en otros modos PIM, no aplican a PIM bidireccional. En su lugar, las rutas PIM bidireccionales (*, G) reenvían el tráfico desde todas las fuentes y desde el RP.

Los dispositivos de enrutamiento PIM bidireccional deben tener la habilidad de aceptar tráfico en muchas interfaces entrantes. PIM Bidir es escalable, debido a que no necesita el estado de fuente específica (S, G). PIM Bidir está recomendado en ambientes con muchas fuentes y receptores dispersos. Soporta tanto IPv4 como IPv6 [15].

1.5.4.4 Source Specific Multicast (PIM de Fuente Multicast Específica) – PIM SSM [14], [9]

Es una forma mejorada de PIM que permite a un cliente recibir tráfico *multicast* directamente de la fuente, sin la ayuda de un RP. SSM construye siempre un árbol fuente entre los receptores y la fuente. Debido a que la fuente es conocida, una unión o juntura (S, G) se puede emitir hacia la fuente del árbol, lo que elimina la necesidad de construir árboles compartidos y RP. Se emplea comúnmente con IGMPv3 para crear un árbol de camino más corto entre el receptor y la fuente. Soporta tanto IPv4 como IPv6 [15].

1.5.4.5 Any Source Multicast (ASM) [16]

ASM es la forma más tradicional de *multicast* en donde se pueden tener múltiples fuentes en el mismo grupo, en contraste con SSM, donde se especifica una sola fuente en particular. ASM permite que un *host* mapee las direcciones IP y luego las envíe a un número de grupos *multicast* vía direcciones IP.

Este método de enrutamiento *multicast* permite a los *hosts* transmitir desde los grupos sin ninguna restricción en los lugares donde se encuentren los usuarios finales. Soporta tanto IPv4 como IPv6 [15].

1.5.5 PROTOCOLO INDEPENDENTE MULTICAST PARA IPV6 [22]

Esta implementación de PIM soporta PIM SM y PIM SSM para IPv6 *multicast*. Cuando múltiples *routers* se conectan a una red multiacceso, un *router* se asigna con el rol de *route*r designado. El *router* designado recibe datos de la fuente en la interfaz entrante y reenvía estos datos, vía multidifusión, a sus vecinos en las interfaces salientes. En la tabla de enrutamiento del *router* designado se lista la fuente como la dirección IP de la fuente y el grupo como la dirección IP del grupo *multicast*.

Los vecinos intercambian mensajes de *"hello"* periódicamente para determinar el *router* designado. El *router* con la dirección de red más alta se convertirá en el *router* designado. Si el *router* designado recibe subsecuentemente un mensaje de *"hello"* de un vecino con una dirección de red mayor, aquel vecino será el nuevo *router* designado.

1.5.5.1 PIM SM para IPv6 multicast

Un *router* designado de un *host* envía mensajes de unión al RP cuando aquel *host* desea unirse al grupo. Cuando un *host* quiere dejar un grupo, se comunica con su *router* designado a través de MLD. Cuando el *router* designado ya no tiene *hosts* pertenecientes a un determinado grupo, éste envía un mensaje de "poda" al RP.

PIM SM usa temporizadores para mantener a los árboles de la red. Si un *router* PIM SM no recibe información de un vecino o *host* dentro de un tiempo establecido, conocido como tiempo de espera, éste remueve la información asociada de su tabla de enrutamiento.

1.5.5.2 PIM SSM para IPv6 multicast

PIM SSM *multicast* es una extensión del protocolo PIM. Al usar SSM, un cliente puede recibir tráfico *multicast* directamente de la fuente. PIM SSM utiliza la funcionalidad de PIM SM para crear un árbol de camino más corto (SPT) entre el cliente y la fuente, pero construye el SPT sin usar un RP.

Las ventajas que la red configurada con SSM posee sobre una red tradicionalmente configurada con PIM SM son: no necesitan de árboles compartidos o RP y la administración es simplificada, es decir se necesita únicamente configurar PIM SM en las interfaces de todos los *routers*, y emitir los comandos necesarios SSM (incluyendo MLD en el receptor de la LAN).

1.6 REDES PRIVADAS VIRTUALES MULTICAST EN IP/MPLS

Antes de entrar al tema de redes privadas virtuales *multicast*, se debe realizar un análisis previo de lo que significan las VPN basadas en *unicast* dentro de la infraestructura IP/MPLS, ya que permitirá obtener una visión más detallada de cómo se interrelacionan estas tecnologías.

1.6.1 UNICAST VPN [2]

El RFC 2547bis[8] y su sucesor el RFC 4364[9] definen mecanismos que permiten a los proveedores de servicios usar su *backbone* IP/MPLS para brindar servicios de

[8] El RFC 2547bis (BGP/MPLS IP VPN) es comúnmente denominado “El Borrador de Rosen” (Draft-Rosen), debido a su autor Eric Rosen.
[9] El RFC 4364 aborda el tema central “BGP/MPLS IP Virtual Private Networks (VPN)”, cuya autoría se debe al mismo Eric Rosen.

VPN a sus clientes. Son también conocidos como BGP/MPLS VPN, BGP/MPLS IP VPN o simplemente L3VPN, ya que BGP es el protocolo que se emplea para distribuir la información de enrutamiento VPN a través del *backbone* del proveedor y MPLS se utiliza para enviar el tráfico VPN desde un sitio VPN a otro.

1.6.1.1 Definición y Tipos de VPN basadas en MPLS [17]

Una *Virtual Private Network* es una red que emula una red privada sobre una infraestructura común y provee comunicación a nivel de las capas 2 o 3 del modelo de referencia ISO/OSI[10]. El mínimo requerimiento para conectar las VPN es que todos los sitios de los clientes de la red privada sean capaces de interconectarse y estén completamente separados de otras VPN.

1.6.1.1.1 Redes Privadas Virtuales de capa 2 (L2VPN) [18]

Este tipo de VPN ofrece independencia entre la red del cliente y la red del SP (*Service Provider*), ya que brinda la factibilidad de transportar servicios emulados de un sitio hacia otro; es decir, se lo realiza de unas formas transparentes para los CE (*Customer Edge*, Equipo de borde del cliente) ubicadas en la red del cliente.

A nivel de capa 2 del modelo ISO/OSI, las VPN abordan dos tipos de conectividad, que son conexión punto – punto y punto – multipunto. Algunos ejemplos de L2VPN se muestran en la Figura 1.12, en donde priman las tecnologías ATM, *Frame Relay*, Servicio Privado Virtual por Cable (VPWS) Servicio Privado Virtual LAN (VPLS) y Servicio de Red Exclusivo IP (IPLS).

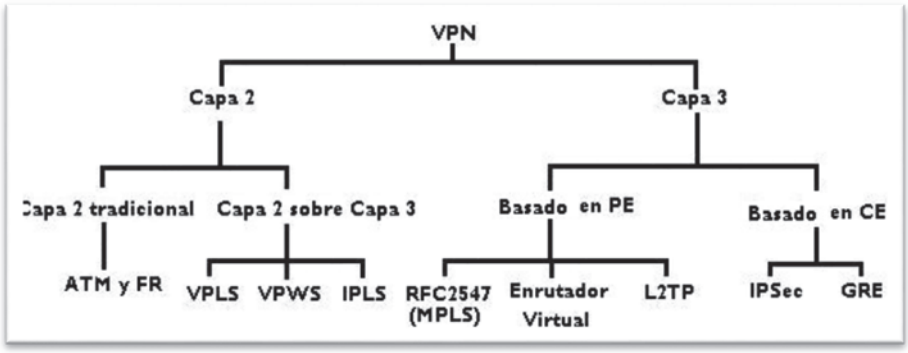

Figura 1.12 Jerarquía de las VPN [19]

[10] Hace referencia al modelo de la Organización Internacional de Estandarización, ISO por sus siglas en inglés; y Modelo de Interconexión de Sistemas Abiertos, OSI por sus siglas en inglés.

1.6.1.1.2 Redes Privadas Virtuales de capa 3 (L3VPN) [20]

L3VPN es un conjunto de sitios que comparten información de enrutamiento común y cuya conectividad es gestionada por un conjunto de políticas; es por ello, que los sitios que componen una L3VPN están conectados a través del *backbone* del proveedor de servicios. Los RFC 2547bis y 4364 hacen referencia a este tipo de VPN en IP/MPLS.

La Figura 1.12, de la misma manera que en L2VPN, muestra algunos ejemplos de VPN en capa 3, como son el RFC 2547bis, enrutador virtual y L2TP (*Layer 2 Tunneling Protocol*) todos éstos basados sobre PE; IPsec y GRE (*Generic Encapsulation Routing*), basados sobre CE.

1.6.1.2 Componentes de la red [3], [2]

Los *routers* en BGP/MPLS VPN presentan tres roles diferentes que desempeñan en esta arquitectura. La Figura 1.13 muestra a los *routers* que participan en una red BGP/MPLS VPN.

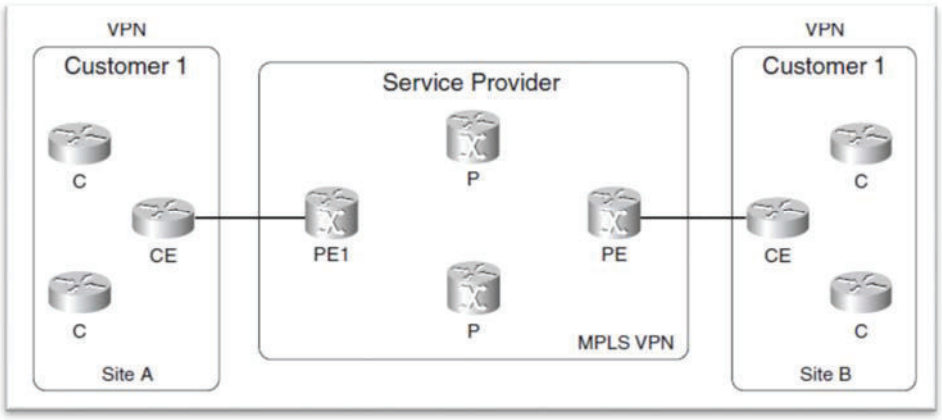

Figura 1.13 *Routers* participantes en una red BGP/MPLS VPN [17]

1.6.1.2.1 CE (Customer Edge)

Es aquel dispositivo (*router* o *host*) que provee al cliente el acceso a la red del proveedor de servicios sobre un enlace de datos hacia uno o más *routers* PE y que es administrado por el SP o por el cliente. El CE no necesita tener visibilidad hacia el *core* del SP. Típicamente, el CE intercambia rutas del cliente con el PE o PEs conectados a éste, empleando protocolos IP tales como RIP, OSPF o a través de enrutamiento estático.

1.6.1.2.2 PE (Provider Edge)

Es aquel o aquellos *routers* administrados por el SP y conectados a un conjunto de CE. Aunque un PE mantiene información de enrutamiento VPN, sólo requiere mantener las rutas VPN para aquellas VPN que están directamente conectadas. Después de haber aprendido las rutas VPN de los *routers* CE, un *router* PE intercambia información de enrutamiento con otros *routers* PE usando IBGP (*Internal Border Gateway Protocol*).

1.6.1.2.3 P (Provider) [3]

Es aquel *router* (o *routers*) gestionado por el SP, cuyos enlaces están dentro del *backbone* del SP y que provee la infraestructura de enrutamiento para interconectar los *routers* PE entre sí, de tal forma que actúan como puntos transitorios de los túneles de transporte y que además, no mantienen ningún estado de enrutamiento con los CE.

Asimismo, en MPLS VPN sucede que:

- Un *router* P mantiene la información de enrutamiento y etiquetas para la tabla de enrutamiento global, únicamente. Éste no tiene enrutamiento o información de los estados para las VPN cliente.
- Un *router* CE mantiene una adyacencia de enrutamiento con su *router* PE vecino, únicamente. Los *routers* CE no se 'miran' con otros *routers* CE, pero aún tienen la habilidad de acceder a otros *routers* CE en sus VPN a través de la ruta óptima que lo proporciona la 'red P' (red de *core*).

1.6.1.3 Terminología en la Arquitectura MPLS VPN [2], [17]

1.6.1.3.1 Virtual Routing / Forwarding (VRF)

Una VRF es una instancia del reenvío y del enrutamiento de una VPN. Un *router* PE posee una instancia VRF por cada VPN conectado a éste; por consiguiente, un PE contiene la tabla de enrutamiento global y, a su vez, contiene una tabla de enrutamiento VRF por cada VPN conectada al PE, como se visualiza en la Figura 1.14.

La tabla de enrutamiento VRF por cliente tiene prefijos que están poblados por protocolos de enrutamiento dinámico y estático, al igual que la tabla de

enrutamiento global. El concepto de métrica, distancia, siguiente salto no cambia. Dado que la instancia VRF se asocia con interfaces, solamente los paquetes IP que ingresan al *router* PE a través de esas instancias VRF se reenvían acorde a la tabla VRF.

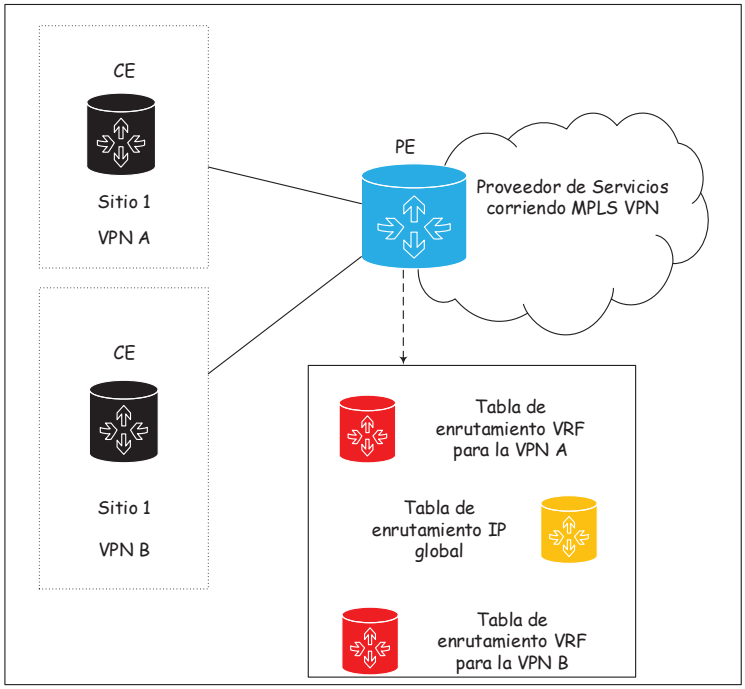

Figura 1.14 VRF en un *router* PE [17]

1.6.1.3.2 Route Distinguisher – RD

Un RD es un campo de 64 bits utilizado para hacer prefijos VRF únicos cuando el Multiprotocolo BGP[11] los transporta. La función del RD no es la de un identificador VPN, ya que escenarios VPN más complejos podrían requerir más que un RD por VPN. Simplemente se usa para identificar de manera única las rutas VPN.

1.6.1.3.3 Route Target – RT

Importar una RT significa que la ruta VPNv4 recibida del Multiprotocolo BGP es comprobada para una comunidad, que es el RT. Si el resultado es una igualdad, el prefijo es puesto en la tabla de enrutamiento VRF como una ruta IPv4. Si la igualdad no ocurre, el prefijo es rechazado.

[11] Multiprotocolo BGP está descrito en el RFC 4760. Son extensiones multiprotocolo con BGP, que permite a BGP transportar información de enrutamiento para múltiples protocolos de la capa de red [24].

1.6.1.3.4 Propagación de rutas a través del Multiprotocolo BGP

BGP es un protocolo de enrutamiento probado y estable para transportar muchas rutas y, sobre todo, la tabla de enrutamiento de Internet. Debido a que las rutas VPN del cliente son únicas, cuando se coloca el RD para cada ruta IPv4, los convierte en rutas VPNv4; de esta manera, todas las rutas de los clientes pueden ser transportadas a través de la red MPLS VPN de manera segura.

La Figura 1.15 muestra los pasos de la propagación de la ruta desde el *router* CE del sitio A hasta el *router* CE del sitio B por la red MPLS VPN. El *router* PE recibe las rutas IPv4 del *router* CE a través de algún protocolo IGP[12] (*Interior Gateway Protocol*) o eBGP (BGP externo). Estas rutas IPv4 se colocan en la tabla de enrutamiento VRF. Dichas rutas se anexan con el RD que se asigna a cada VRF; por consiguiente, se convierten en rutas VPNv4 que son puestas en el Multiprotocolo BGP.

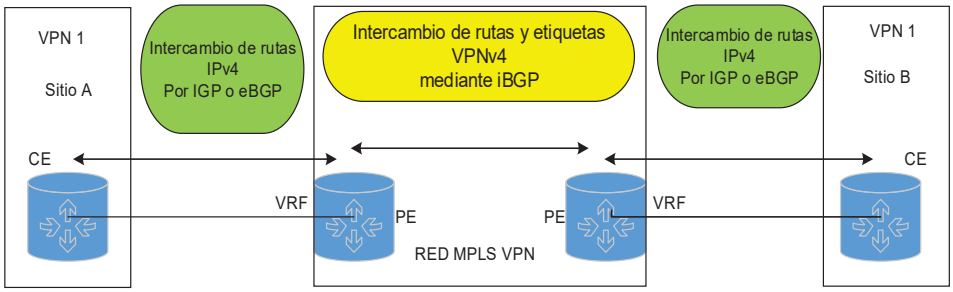

Figura 1.15 Propagación de rutas por medio del Multiprotocolo BGP [17]

BGP se encarga de la distribución de estas rutas VPNv4 a todos los *routers* PE de la red MPLS VPN. En los *routers* PE, las rutas VPNv4 son removidas de los RD y puestas en la tabla de enrutamiento VRF como rutas IPv4. Estas rutas IPv4 se anuncian al *router* CE a través de IGP o eBGP que se ejecuta entre los *routers* CE y PE.

1.6.1.3.5 Reenvío de paquetes etiquetados

Los paquetes no pueden ser reenviados como paquetes IP puros entre los sitios. Los *routers* P no pueden reenviarlos debido a que ellos no tienen la información

[12] IGP es una descripción genérica que se refiere a cualquier protocolo, como OSPF o IS-IS, que utilizan los *routers* interiores cuando intercambian información de enrutamiento.

VRF de cada sitio. MPLS puede resolver este problema etiquetando los paquetes. Para ello, los *routers* P deben tener solamente la información de reenvío correcto de las etiquetas para reenviar los paquetes.

La forma más común es configurar el Protocolo de Distribución de Etiquetas (*Label Distribution Protocol*, LDP por siglas en inglés) en todos los *routers* P y PE, de tal manera que todo el tráfico IP sea de etiquetas conmutadas. Luego, los paquetes IP son etiquetados y reenviados con una etiqueta del *router* PE de entrada hacia el *router* PE de salida. Un *router* P nunca realiza la búsqueda de la dirección IP de destino.

Por lo tanto, el tráfico VRF a VRF tiene dos etiquetas en la red MPLS VPN. La etiqueta superior es la etiqueta IGP y es distribuida por LDP entre los *routers* P y PE, salto por salto. La etiqueta inferior es la etiqueta VPN que es anunciada por el Multiprotocolo BGP desde un PE a otro PE. Los *routers* P usan la etiqueta IGP para reenviar el paquete hacia el *router* PE de salida correcto. El *router* PE de salida usa la etiqueta VPN para reenviar el paquete IP hacia el *router* CE correcto.

La Figura 1.16 muestra el paquete reenviado en una red MPLS VPN. El paquete ingresa al *router* PE en la interfaz VRF como un paquete IPv4. Éste es reenviado a través de la red MPLS VPN con dos etiquetas. Los *routers* P reenvían el paquete utilizando la etiqueta superior. La etiqueta superior es intercambiada en cada *router* P. Las etiquetas son removidas en el *router* PE de salida y el paquete es reenviado como un paquete IPv4 sobre la interfaz VRF hacia el *router* CE. El *router* CE correcto se encuentra buscándolo en la etiqueta VPN.

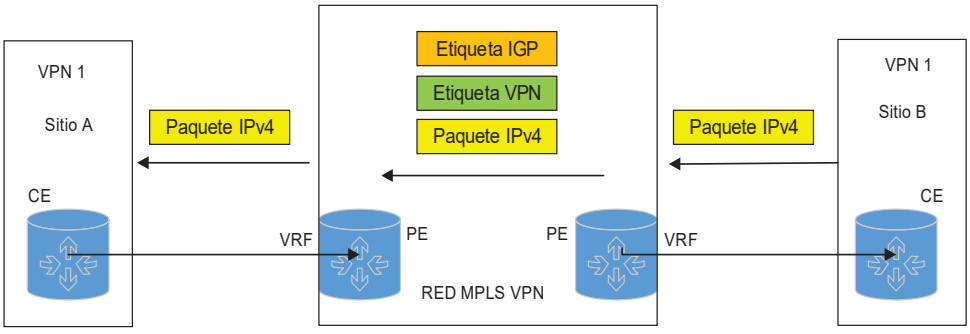

Figura 1.16 Reenvío de paquetes en una red MPLS VPN [17]

1.7 MULTICAST VPN [9], [21]

1.7.1 NOCIONES DE MVPN

Multicast VPN es una solución para el apoyo a IP *multicast* en un cliente IP VPN aprovisionado a través de la infraestructura MPLS VPN de un proveedor.

1.7.2 COMPONENTES DE UNA MVPN

1.7.2.1 Dominio multicast

Un dominio *multicast* es un conjunto de instancias de enrutamiento y reenvío virtual (VRF) habilitadas para *multicast* que pueden enviar tráfico *multicast* a otra VRF. Estas VRF *multicast* se denotan como MVRF. Los dominios *multicast* 'mapean' todos los grupos *multicast* de un cliente que existe en una VPN particular a un único grupo *multicast* global en la red del proveedor. Esto se consigue encapsulando los paquetes *multicast* originales del cliente dentro de un paquete proveedor usando GRE.

Cada *router* PE que está soportando un cliente MVPN es parte del dominio *multicast* para aquel cliente. Muchos clientes finales pueden unirse a un *router* PE particular, lo que significa que el *router* PE puede ser un miembro de muchos dominios *multicast*, uno por cada cliente MVPN que esté conectado a éste.

La red del proveedor construye un árbol de distribución *multicast* por defecto (MDT por defecto) entre los *routers* PE por cada dominio *multicast* usando una única dirección de grupo *multicast* asignado por el SP. Estos grupos *multicast* únicos se denominan grupos-MDT. Cada MVRF pertenece a un MDT por defecto.

La Figura 1.17 ilustra el concepto de dominios *multicast* en una red de un SP. Las VPN A y B pertenecen a dominios *multicast* por separado. El *core* del SP crea un MDT por defecto para cada uno de estos dominios *multicast* usando las direcciones del grupo-MDT 224.10.10.10 para A y 224.20.20.20 para B. Los *routers* PE1 y PE2 se unen a los MDT por defecto como si estuvieran conectados a los sitios A y B. El *router* PE3 solo necesita conectarse al MDT por defecto de la VPN B.

Los paquetes de A o B que viajen por aquellos MDT por defecto, son encapsulados usando GRE. La dirección IP de la fuente del paquete externo corresponde a la

dirección BGP del *router* PE transmisor y el destino es la dirección del grupo MDT respectivo. En esencia, GRE oculta el paquete *multicast* del cliente en la red del proveedor y permite mapear muchos grupos *multicast* en una VPN a un solo grupo *multicast* proveedor. Los *routers* P del SP solo ven la fuente y el destino de la cabecera IP externa que asignó el SP.

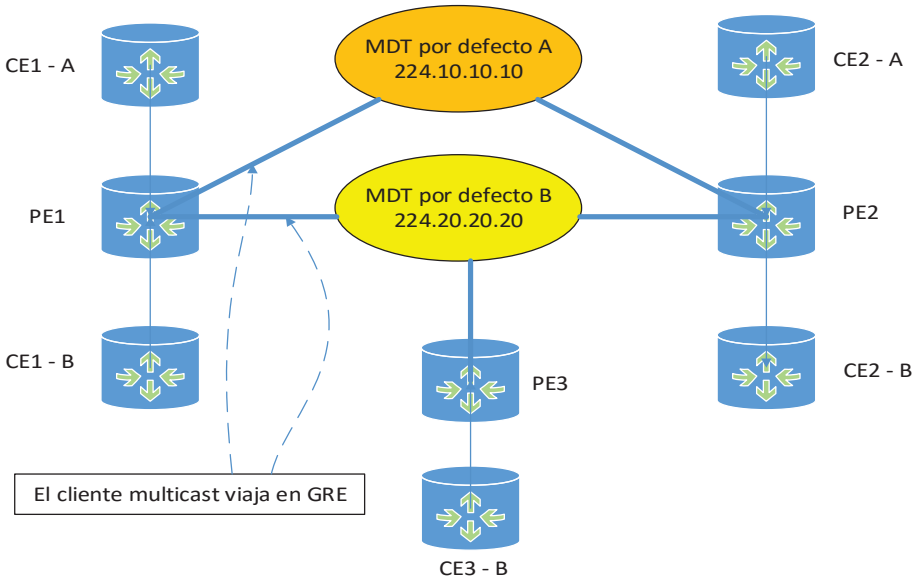

Figura 1.17 Concepto de dominio *multicast* dentro de un SP [1]

Esta fuente y destino aparecen como una entrada de estado (S, G) en la tabla *multicast* global del SP. Un *router* P está solamente informado de las direcciones fuente del *router* PE y de las direcciones del grupo-MDT que forman los MDT.

El tráfico del *router* CE que viaja por un MDT es reenviado en un paquete encapsulado GRE (paquete-Proveedor) usando la dirección de grupo MDT como su destino. El paquete-Proveedor GRE emplea únicamente IP y ningunas de las cabeceras de la etiqueta MPLS son aplicadas al tráfico MDT. Únicamente existe en el *core* IP *multicast* puro.

1.7.2.2 Multicast Virtual Routing Forwarding – MVRF

En un *router* PE, cada VRF puede tener una tabla de enrutamiento y reenvío *multicast*, denominada *multicast* VRF (MVRF). Esta MVRF es vista desde el *router* PE hacia la red *multicast* VPN del cliente. La MVRF contiene toda la información de enrutamiento *multicast* para aquella VPN. Cuando un *router* recibe datos *multicast*

o paquetes de control de la interfaz de un *router* CE en una VRF, el chequeo RPF así como el reenvío, se los realizará en su respectiva MVRF.

1.7.2.3 Multicast Tunnel Interface (MTI)

El MTI es la representación del acceso al dominio *multicast*. MTI aparece en la MVRF como una interfaz llamada Túnel x (*Tunnel x*), donde x es el número del túnel. Para cada dominio *multicast* en el que una MVRF participa, hay una correspondiente MTI. Una MTI es esencialmente un *gateway* que conecta el ambiente del cliente (MVRF) al ambiente global del SP (MDT).

Los paquetes-Cliente enviados al MTI son encapsulados dentro de un paquete-Proveedor (usando GRE) y reenviado a lo largo del MDT. Cuando el *router* PE envía el tráfico al MTI, éste se convierte en la raíz de aquel árbol; luego, el *router* PE que recibe el tráfico de un MTI, se convierte en una hoja de aquel MDT.

Es necesario, solamente, un único MTI para acceder a un dominio *multicast*. El mismo MTI se usa para reenviar el tráfico independientemente de si éste va hacia el MDT por defecto o a múltiples MDTs de datos asociados con aquel dominio *multicast*. El MTI se crea de forma dinámica tras la configuración del MDT por defecto y no puede ser configurado de manera explícita.

1.7.2.4 Árboles de distribución multicast

Son utilizados para transportar tráfico *multicast* del cliente entre *routers* PE en un dominio *multicast* común. Algunos de estos aspectos importantes de la operación del dominio *multicast* dentro del contexto de una VPN *multicast* se detallan a continuación.

- Una MVPN es asignada a un dominio *multicast*.
- Una dirección de grupo del proveedor es definida por un dominio *multicast* y esta dirección debe ser única.
- Los paquetes del cliente son encapsulados en los *routers* PE conectados a los sitios del cliente y enviados sobre el MDT como paquetes del proveedor. Esto asegura que la red de transporte no necesite conocimiento alguno de la información de enrutamiento *multicast* del cliente.
    - ✓ La dirección fuente de los paquetes del proveedor es siempre la dirección de la fuente MP-BGP.

- ✓ La dirección de destino es la dirección de grupo del proveedor. Esta dirección es asignada durante la configuración de la MVPN y es también conocida como la Dirección de Grupo VPN.
- ✓ La encapsulación es típicamente GRE.

1.7.3 ADYACENCIAS EN PIM

Cada VRF que ha permitido el enrutamiento *multicast* tiene una única instancia PIM creada en el *router* PE. Esta instancia en una VRF específica forma una adyacencia PIM con cada *router* CE (con PIM habilitado) en aquella MVRF. Las entradas de enrutamiento *multicast* del cliente que crea cada instancia PIM son específicas a su correspondiente MVRF.

Adicional a la adyacencia PIM del *router* CE, el *router* PE forma otros dos tipos de adyacencias PIM. El primero es la adyacencia PIM con otros *routers* PE que tienen MVRF en el mismo dominio *multicast*. Esta adyacencia PIM del *router* PE es accesible a través de la MTI y se usa para transportar información *multicast* entre MVRF (por un MDT) recorriendo el *backbone*. Las adyacencias PIM del *router* PE se mantienen usando la misma instancia PIM que se emplea entre los *routers* PE y CE por la MVRF asociada.

El segundo tipo de adyacencia PIM es creado por la instancia PIM global. El *router* PE mantiene las adyacencias PIM con cada uno de sus vecinos IGP, que son los *routers* P, o los *routers* PE directamente conectados. La instancia global PIM se usa para crear los árboles de distribución *multicast* (MDT) que conectan las MVRF. Los *routers* CE no forman adyacencias PIM entre sí, ni tampoco forman una adyacencia los *routers* CE y PE mediante la instancia PIM global.

La Figura 1.18 muestra los diferentes tipos de adyacencias PIM en la red de un SP para una VPN A. Una adyacencia PIM existe entre el *router* CE1 y el *router* PE1, así como entre el *router* CE2 y el PE2. Debido a que las MVRF A son parte del mismo dominio *multicast*, una adyacencia PIM está activa entre los *routers* PE1 y PE2. Ambos *routers* tienen una adyacencia PIM en la tabla global hacia el *router* P.

1.7.4 ÁRBOLES DE DISTRIBUCIÓN MULTICAST EN MVPN

Un árbol de distribución *multicast* (MDT) se usa para transportar el tráfico *multicast* del cliente de distintas maneras, sobre una infraestructura de transporte

compartida. En términos simples, un MDT es un árbol *multicast* único que se crea por MVPN. Los MDT consisten de tres componentes: MDT por defecto, MDT de datos y la MTI.

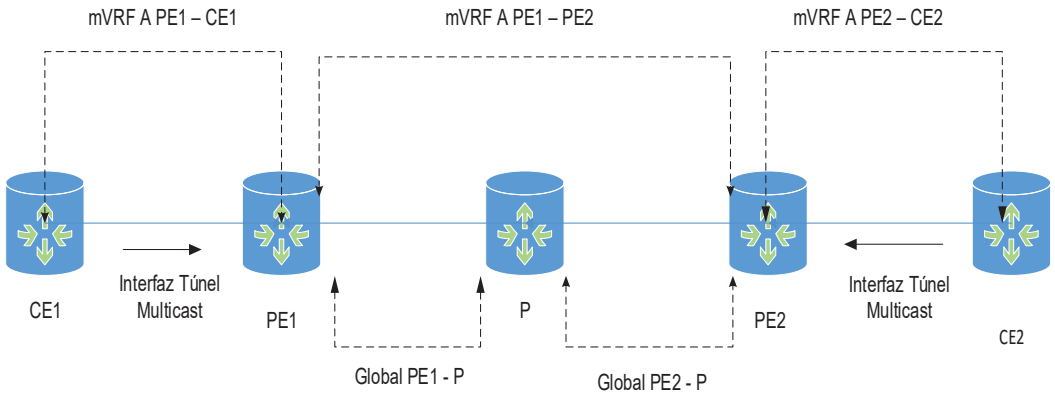

Figura 1.18 Adyacencias en PIM [1]

1.7.4.1 MDT por defecto

Una MVPN usa este MDT para enviar tráfico *multicast* de bajo ancho de banda o aquel tráfico que es destinado a ser distribuido a un amplio conjunto de receptores. Siempre se usa para enviar tráfico de control *multicast* entre los *routers* PE en un dominio *multicast* y se crea por cada MVPN en un *router* PE.

Cuando un *router* PE se une a un MDT, éste llega a ser la raíz del árbol y sus pares PE remotos llegan a ser las hojas del árbol. Por el contrario, el *router* PE local llega a ser una hoja del mismo árbol, lo que permite que el *router* PE participe en un dominio *multicast* como ambos, es decir, una fuente y receptor a la vez.

Cuando un *router* PE reenvía un paquete *multicast* del cliente sobre un MDT, éste es encapsulado con GRE. Esto es que, el grupo *multicast* de una VPN particular pueda ser mapeada a un único grupo-MDT en la red del proveedor. La dirección de fuente de la cabecera IP del paquete externo es la dirección de emparejamiento local del Multiprotocolo BGP del PE.

La dirección de destino es la dirección de grupo-MDT asignado al dominio *multicast*. Por tanto, la red del proveedor está solamente interesada en las direcciones IP y la cabecera de GRE (alojada por el mismo SP), y no en el direccionamiento específico del cliente.

Luego, los paquetes son reenviados en la red del proveedor usando la dirección *multicast* del grupo-MDT al igual que cualquier otro paquete *multicast* con el chequeo RPF normal, siendo realizado en la dirección fuente (el cual, en este caso, es el PE origen). Cuando el paquete arriba al *router* PE desde un MDT, el encapsulamiento se remueve y el paquete *multicast* original del cliente se reenvía a su correspondiente MVRF.

El MVRF 'target' proviene de la dirección del grupo-MDT en el campo destino de la cabecera encapsulada. Por tanto, usando este proceso, los paquetes *multicast* del cliente son enviados por el túnel a través de la red del proveedor a las hojas MDT asignadas. Cada MDT es una red o malla de túneles *multicast* formando el dominio *multicast*. La Figura 1.19 ilustra el proceso de encapsulamiento del paquete del cliente a través de un MDT.

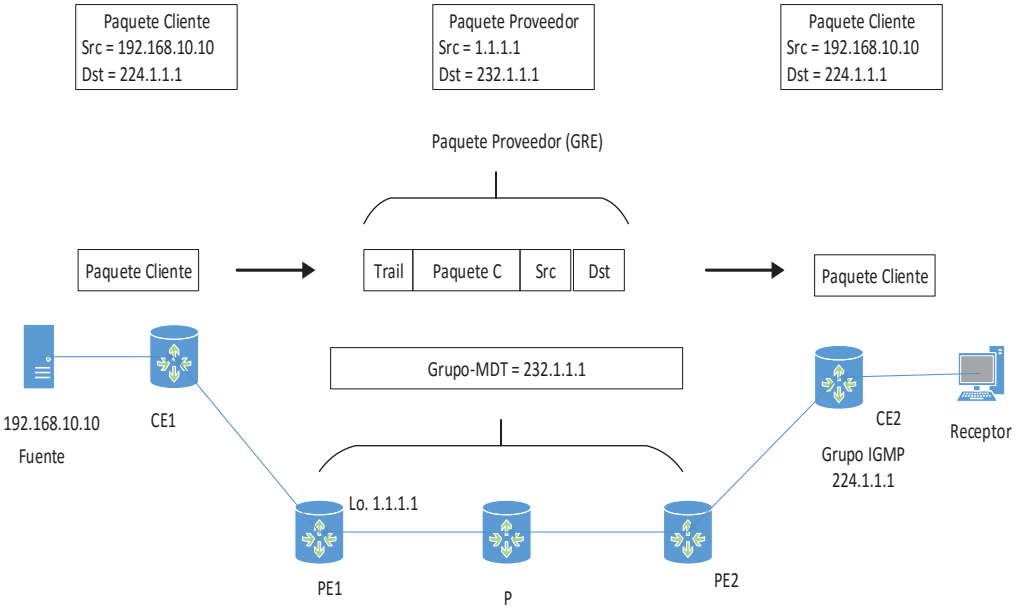

Figura 1.19 Encapsulamiento del paquete-Cliente [1]

En este ejemplo, una fuente situada en CE1 envía tráfico a un receptor situado en CE2 usando el grupo (*, 224.1.1.1). El MDT por defecto para este dominio *multicast* ha sido definido por la dirección 232.1.1.1, y este valor se configura en cada una de las VRF. El *router* PE1 encapsula el tráfico *multicast* destinado al grupo 224.1.1.1 de la fuente 192.168.10.10, en el lugar de CE1, dentro de un paquete-Proveedor usando encapsulamiento GRE.

El campo ToS de la cabecera IP (*Type of Service,* 1 byte) del paquete-Cliente es también copiado al paquete-Proveedor. La dirección fuente del paquete-Proveedor es la dirección de emparejamiento BGP del *router* PE1 (1.1.1.1), y la dirección destino es el grupo-MDT (232.1.1.1). Cuando el paquete-Proveedor arriba al *router* PE2, el encapsulamiento es retirado y el paquete-Cliente original es reenviado hacia el receptor.

1.7.4.2 MDT de datos

Este tipo de MDT se utiliza para enviar, dentro de un túnel, el tráfico de la fuente que tenga gran ancho de banda a través de la red del proveedor a aquellos *routers* PE interesados. Evitan inundaciones innecesarias de tráfico *multicast* del cliente a todos los *routers* PE en un dominio *multicast*.

La Figura 1.20 muestra los dos tipos de árboles *multicast* definidos para MVPN. La línea entrecortada conecta todos los *routers* PE, ya que tanto fuentes como receptores de paquetes *multicast* constituyen el MDT por defecto. Mientras que la línea continua está enraizada en el PE1 y se ramifica hacia los *routers* PE2 y PE3, y representa al MDT de datos, el cual se encarga de enviar el *stream* de datos de gran ancho de banda. El MDT de datos no se extiende a PE4 debido a que CE4 no tiene un expreso interés en recibir el *stream multicast* de gran ancho de banda.

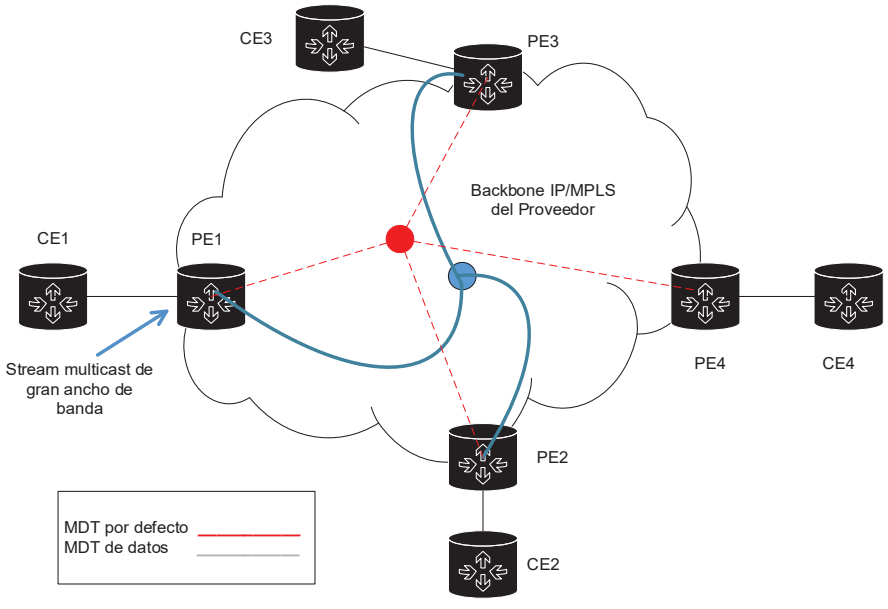

Figura 1.20 Árboles de distribución *multicast* por defecto y de datos [21]

Para aplicaciones de gran ancho de banda que tienen receptores distribuidos muy escasos, se podría presentar el problema latente de inundaciones innecesarias en los *routers* PE. Para superar este problema, se puede crear un grupo MDT de datos para minimizar la inundación, enviando datos únicamente a aquellos *routers* PE que poseen receptores VPN activos.

El MDT de datos se crea dinámicamente si un *stream multicast* particular excede un umbral de ancho de banda. Cada VRF puede tener un '*pool*' de grupos MDT de datos alojados en éste. Cuando un *router* PE crea un MDT de datos, el tráfico fuente *multicast* se encapsula de la misma manera como lo fue en el MDT por defecto, pero el grupo de destino es tomado del *pool* de MDT de datos.

1.7.5 REVERSE PATH FORWARDING EN MVPN

En un ambiente MVPN, el chequeo RPF puede ser categorizado en tres tipos de paquetes *multicast*:

- Paquetes-Cliente recibidos de una interfaz cliente a un *router* PE en la MVRF.
- Paquetes-Proveedor recibidos de un *router* PE o de la interfaz del *router* P en la tabla de enrutamiento global.
- Paquetes-Cliente recibidos de una interfaz túnel *multicast* en la MVRF.

El chequeo RPF para las primeras dos categorías está realizado como un legado de los procedimientos RPF en IP *multicast*. La información de la interfaz es recogida de la tabla de enrutamiento y guardada en un estado. Para los paquetes-Cliente, la búsqueda de la fuente-Cliente en la tabla de enrutamiento *unicast* VRF devuelve una interfaz del *router* PE asociado con aquella VRF.

Para los paquetes-Proveedor, la búsqueda de la fuente-Proveedor en la tabla de enrutamiento global devuelve una interfaz conectada a otro *router* P o a otro *router* PE. Los resultados de estas búsquedas se usan como interfaces RPF.

En la tercera categoría, los paquetes-Cliente son originados desde los *routers* PE remotos en la red y han viajado a través de la red del proveedor por el MDT. Por lo tanto, desde la perspectiva de la MVRF, estos paquetes-Cliente deben haber sido recibidos en el MTI. Sin embargo, debido a que el MTI no participa en el enrutamiento *unicast*, una búsqueda de la fuente-Cliente en la VRF no devolverá una interfaz túnel.

En su lugar, la ruta hacia la fuente-Cliente tendrá que ser distribuida por el Multiprotocolo BGP como un prefijo VPNv4 del *router* PE remoto. Esto implica que la interfaz receptora está actualmente en la red del proveedor. En este caso, el procedimiento RPF ha sido modificado de manera que si el Multiprotocolo BGP ha aprendido un prefijo que contiene la dirección fuente-Cliente, la interfaz RPF es fijada al MTI que está asociada con aquella MVRF.

El vecino RPF se selecciona de acuerdo a dos criterios. Primero, el vecino RPF debe ser el siguiente salto BGP hacia la fuente-Cliente, que aparece en la tabla de enrutamiento para aquella VRF. Segundo, la misma dirección del siguiente salto BGP debe aparecer como un vecino PIM en la tabla de adyacencias para la MVRF. Esta es la razón para que PIM deba usar la dirección de emparejamiento BGP cuando envía los paquetes '*hello*' a través del MDT.

2. IMPLEMENTACIÓN DEL PROTOTIPO

2.1 ANÁLISIS Y COMPARACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO MULTICAST PARA IPV4 [27], [14], [10]

Dentro de los protocolos de enrutamiento *multicast* existen criterios que los hacen similares unos con otros. Es así que los árboles de distribución basados en la fuente trabajan en modo denso, mientras que los árboles de distribución compartidos emplean el modo disperso. Por otra parte, estos protocolos determinan su unión a los grupos *multicast*, ya sea de manera explícita (por mensajes) o de manera implícita (inundación/poda).

Los árboles compartidos en relación a los árboles fuente ofrecen una mayor escalabilidad, en cuanto se refiere a la 'cantidad de receptores existentes en un grupo *multicast'*. Se puede afirmar que: *"… esta característica se refiere a la memoria necesaria en los routers para el almacenamiento de las tablas y a la carga producida en los vínculos, debido al mantenimiento de una mayor cantidad de árboles de distribución."* [27]

DVMRP es un protocolo de modo denso, y emplea un método implícito de unión o de inundación/poda (característico de este modo) para entregar el tráfico *multicast* a todos, y luego determina los lugares en donde los receptores no se encuentran con algún interés. Además, este protocolo de enrutamiento *multicast* utiliza los árboles de distribución basados en la fuente para construir sus tablas de enrutamiento *multicast*. DVMRP se deriva del protocolo de enrutamiento *unicast* RIP. Funciona a través del algoritmo RPM.

MOSPF es un protocolo de modo denso, sin embargo, emplea un mensaje de unión explícito; de esta manera, los *routers* no necesitan inundar toda la red con tráfico *multicast*. MOSPF emplea los árboles de distribución basados en la fuente. MOSPF utiliza el protocolo de enrutamiento *unicast* OSPF para su funcionamiento en un dominio, o si está compuesta por una o varias áreas OSPF. Utiliza el algoritmo RPM y SPT.

CBT es un protocolo de modo disperso, está basado en árboles compartidos y para pertenecer a un grupo, emplea mecanismos de forma explícita de solicitud. Puede

trabajar con cualquier protocolo de enrutamiento *unicast*. Al ser un protocolo de modo disperso ofrece mayor escalabilidad en redes WAN. Su RP está localizado en el *core* de la red. Usa el algoritmo ST y SPT.

PIM recibe su nombre (Protocolo Independiente *Multicast*) ya que no depende de los mecanismos propuestos por algún protocolo de enrutamiento *unicast*. Sin embargo, PIM necesita la presencia de cualquier protocolo de enrutamiento *unicast*, con el fin de proveer información a la tabla de enrutamiento para adaptar los cambios a su topología.

PIM DM es un protocolo de modo denso y se basa en árboles de fuente para su constitución. Cuando una red es inundada con tráfico *multicast*, enseguida son podadas aquellas ramas que no expresan un interés en recibir los paquetes *multicast*, de manera implícita. Emplea el algoritmo RPM.

PIM SM comparte las mismas características de CBT, tales como modo disperso, unión explícita y se basa en los árboles compartidos. Este tipo de protocolo es el más común dentro de las redes de área extendida. Los *routers* que están directamente conectados o miembros *downstream* son requeridos para unirse a los árboles de distribución SM para transmitir mensajes de manera explícita. Si un *router* no llega a ser parte de este árbol de distribución, éste no recibirá el tráfico *multicast* direccionado a ese grupo. Si la acción inmediata de un protocolo en DM es reenviar el tráfico, la acción por defecto que utiliza SM es bloquear el tráfico, a menos que sea requerido explícitamente. Selecciona un router RP para constituir su nueva fuente.

PIM Bidir es una variación de PIM que construye árboles compartidos bidireccionales que son enraizados en el punto RP. Por ende, se clasifica como un protocolo de enrutamiento *multicast* disperso. BiDir escala muy bien debido a que no necesita estados como los pares (S, G). Además es recomendado en ambientes que tienen fuentes dispersas, así como muchos receptores dispersos. Emplea mensajes de unión explícita para unirse a los árboles de distribución.

PIM SSM es una mejora del protocolo de enrutamiento *multicast* PIM SM; sin embargo no necesita un RP para comunicarse entre la fuente y los receptores, lo que supone que construye árboles basados en la fuente, pero conserva el modo

disperso que tiene PIM SM. Envía mensajes de forma explícita para unirse a un árbol de distribución.

Luego de analizar los protocolos de enrutamiento *multicast*, se establecerá una comparación entre éstos, y para ello, se considerarán algunos parámetros citados en el análisis, como los tipos de árboles *multicast*, los modos de operación denso y disperso y nuevos criterios como la escalabilidad (ver Tabla 2.1).

Luego de esta comparación, se decidió escoger a los protocolos PIM-SM (Protocolo Independiente *Multicast*, modo disperso) y PIM-SSM (PIM, *Source Specific Multicast*) para la implementación en el prototipo de MVPN IP/MPLS, tal como se observa en la Figura 2.1, por los siguientes aspectos:

- Escalabilidad
- Por ser utilizados en redes de área extendida gestionados por grandes SP (Proveedores de Servicios de Internet)
- Su configuración se basa, amplia y efectivamente, en la bibliografía de este proyecto [28]
- PIM-SSM (*Source Specific Multicast*), al igual que ASM (*Any Source Multicast*) y BiDir (bidireccional), son protocolos que se emplean para la construcción del árbol de distribución *multicast* MDT en el *core* de la red IP/MPLS

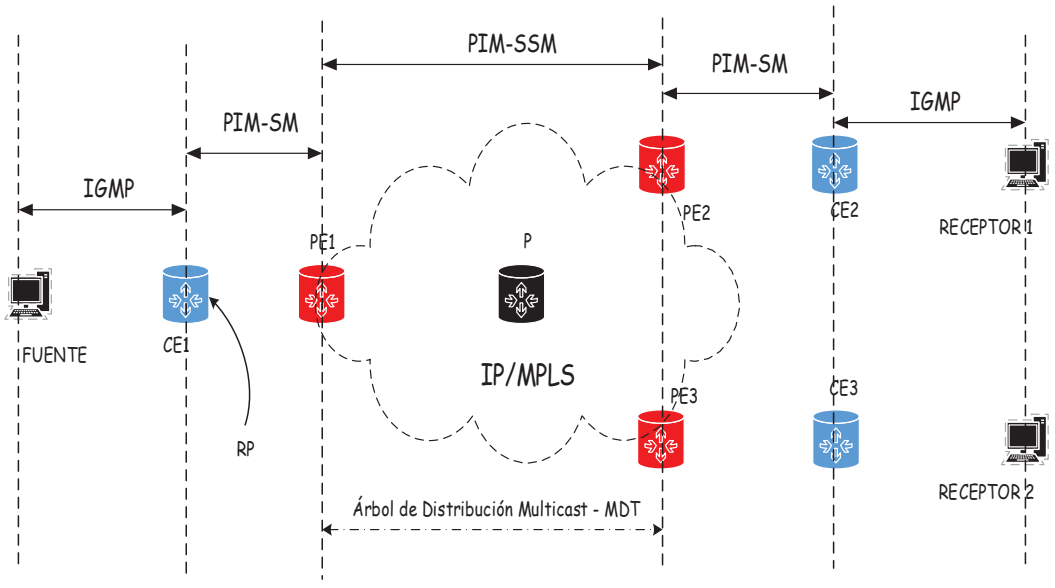

Figura 2.1 Esquema de la red con los protocolos de enrutamiento *multicast*

Protocolo de Enrutamiento Multicast	Escalabilidad	Punto de encuentro	Árbol compartido (*, G)	Árbol fuente (S, G)	Protocolo de enrutamiento unicast que depende	Unión explícita	Unión implícita	Modo disperso	Modo denso
DVMRP	No	No	No	Sí	RIP	No	Sí	No	Sí
MOSPF	No	No	No	Sí	OSPF	Sí	No	No	Sí
CBT	Sí	Sí (*core*)	Sí	No	independiente	Sí	No	Sí	No
PIM DM	No	No	No	Sí	independiente	No	Sí	No	Sí
PIM SM	Sí	Sí (RP)	Sí	No	independiente	Sí	No	Sí	No
PIM BiDir	Sí	Sí (RP)	Sí	No	independiente	Sí	No	No	No
PIM SSM	Sí	No	No	Sí	independiente	Sí	No	Sí	No

Tabla 2.1 Comparación de los protocolos de enrutamiento *multicast* [14]

Posterior al análisis efectuado anteriormente, se pasa a la etapa de montaje de la red en el laboratorio de la FIEE, con la disposición de los equipos como se ilustra en la Figura 2.2.

Se configurarán los *routers* de marca Cisco 1941 que posee actualmente el laboratorio de Informática de la FIEE, y que poseen las características de levantar MPLS y PIM-SM en sus interfaces, PIM-SSM a nivel global y MVPN sobre IP/MPLS.

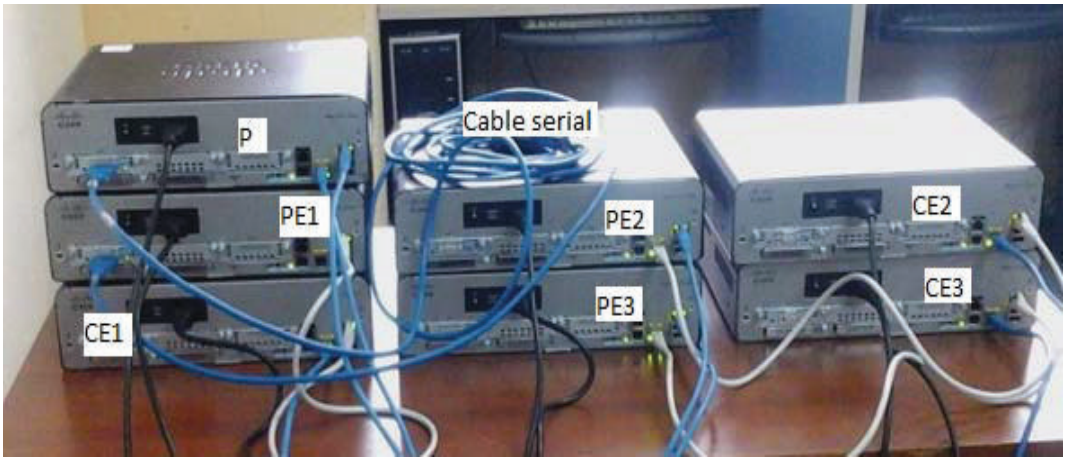

Figura 2.2 Interconexión de los *routers* en el laboratorio

Por la falta de otra interfaz *Gigabit Ethernet* en el *router* P, que serviría para conectar los *routers* PE1 y P, se tuvo que usar una interfaz serial (cuyo ancho de banda máximo es de 8 Mb/s), lo que ocasionó una limitante para cruzar el tráfico con un mayor ancho de banda, formándose un “cuello de botella”. En la Figura 2.3 se aprecia el empleo de la interfaz serial en la interconexión de los equipos en el laboratorio.

Las características principales que presentaron los *routers* Cisco 1941 del laboratorio fueron: IOS 15.1(4)M4, dos interfaces *Gigabit Ethernet*, dos interfaces seriales (síncrono/asíncrono), un módulo *Virtual Private Network* (VPN), una memoria no volátil de 255 Kbytes y una memoria Flash ATA (lectura/escritura) de 250 Mbytes.

La Tabla 2.2 describe el direccionamiento IP de la red: (a) Direccionamiento IP de los *routers*; (b) Direccionamiento IP de la fuente y receptores; (c) Direccionamiento IP del árbol de distribución *multicast*, y del grupo *multicast* IGMP.

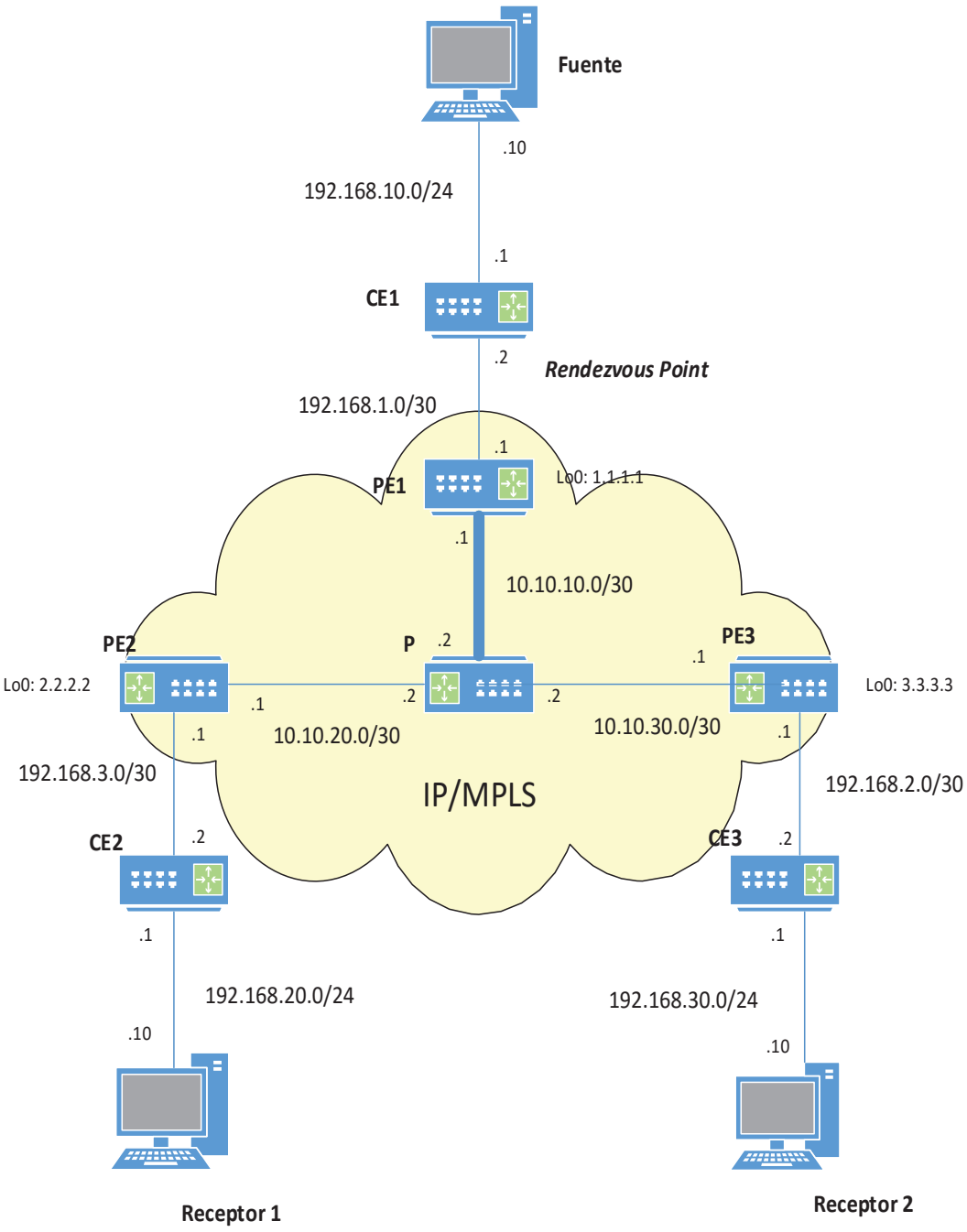

Figura 2.3 Diagrama detallado del prototipo de la red

Para la implementación del prototipo se usaron tres computadoras, una que es la fuente, transmisor o emisor, y las dos restantes, que funcionaron como receptores o destinos. Como se trata de un prototipo de laboratorio, se contó con las computadoras del laboratorio de la FIEE, cuyas características principales se muestran en la Tabla 2.3.

ROUTER	INTERFAZ	DIRECCIÓN IP	MÁSCARA
PE1	*Loopback0*	1.1.1.1	255.255.255.255
	GigabitEthernet	192.168.1.1	255.255.255.252
	Serial	10.10.10.1	255.255.255.252
PE2	*Loopback0*	2.2.2.2	255.255.255.255
	GigabitEthernet	10.10.20.1	255.255.255.252
	GigabitEthernet	192.168.2.1	255.255.255.252
PE3	*Loopback0*	3.3.3.3	255.255.255.255
	GigabitEthernet	10.10.30.1	255.255.255.252
	GigabitEthernet	192.168.3.1	255.255.255.252
P	*Serial*	10.10.10.2	255.255.255.252
	GigabitEthernet	10.10.20.2	255.255.255.252
	GigabitEthernet	10.10.30.2	255.255.255.252
CE1	*GigabitEthernet*	192.168.1.2	255.255.255.252
	GigabitEthernet	192.168.10.1	255.255.255.0
CE2	*GigabitEthernet*	192.168.2.2	255.255.255.252
	GigabitEthernet	192.168.20.1	255.255.255.0
CE3	*GigabitEthernet*	192.168.3.2	255.255.255.252
	GigabitEthernet	192.168.30.1	255.255.255.0

(a)

COMPUTADOR	DIRECCIÓN IP	MÁSCARA	GATEWAY
Fuente	192.168.10.10	255.255.255.0	192.168.10.1
Receptor1	192.168.20.20	255.255.255.0	192.168.20.1
Receptor2	192.168.30.30	255.255.255.0	192.168.30.1

(b)

	DIRECCIÓN IP	WILDCARD
Grupo IGMP	228.0.0.0	0.255.255.255
MDT por defecto	232.1.1.1	

(c)

Tabla 2.2 Direccionamiento IP de la red

	FUENTE	RECEPTOR
Procesador	Core i7 @ 3,4 GHz	Core i7 @ 2,93 GHz
Memoria	6 GB	4 GB
Sistema operativo	Windows 7 / 64 bits	Windows 7 / 64 bits

Tabla 2.3 Características de los computadores fuente y receptor

2.2 CONFIGURACIÓN DE LOS ROUTERS CISCO CON UNICAST Y MULTICAST VPN EN LA RED IP/MPLS

De modo general, se presentan los comandos de configuración con sus principales características, tanto para *unicast* como para *multicast*. Los archivos de configuración de todos los *routers* se los puede apreciar en el Anexo A.

2.2.1 UNICAST VPN [30]

Se configura las interfaces de todos los *routers* del prototipo con las direcciones IP descritas en la Tabla 2.2, tanto en las interfaces *Gigabit Ethernet* y serial, así como en las interfaces *loopback*. Para la interfaz serial se fijará a su máximo valor de ancho de banda, que es de 8 Mbps. Posteriormente, en los *routers* de la nube del proveedor, se configura un protocolo IGP, que para este caso es OSPF. Sobre esta infraestructura, se configura MPLS en la nube del proveedor, utilizando LDP para la distribución de etiquetas.

En los *routers* de borde de la red MPLS se implementa una VPN L3, llamada REDES, utilizando el protocolo MP-BGP para el intercambio de prefijos VPNv4. Seguidamente, del lado del cliente, se crea la VPN L3 (REDES) y se configura el enrutamiento dentro de la VPN L3 del cliente, empleando el protocolo RIP.

2.2.1.1 Router PE1 (Provider Edge 1)

- Configuración de un protocolo de enrutamiento *Interior Gateway Protocol*, que en este caso es OSPF.

```
PE1(config)#router ospf 200

PE1(config-router)#network 1.1.1.1 0.0.0.0 area 0

PE1(config-router)#network 10.10.10.0 0.0.0.3 area 0
```

- Habilitación de MPLS en la interfaz de cara al *core*.

```
PE1(config)#interface x/y

PE1(config-if)#mpls ip
```

- Configuración de la instancia VRF.

```
PE1(config)#ip vrf REDES
```

- Configuración del *Route Distinguisher*.

```
PE1(config-vrf)#rd 200:200
```

- Definición de la política importar/exportar de la ruta.

```
PE1(config-vrf)#route-target export 200:200
```

```
PE1(config-vrf)#route-target import 200:200
```

- Asociación de la VRF a la interfaz.

```
PE1(config)#interface x/y

PE1(config-if)#ip vrf forwarding REDES
```

- Configuración del proceso BGP.

```
PE1(config)#router bgp 200
```

- Configuración de los vecinos BGP VPNv4.

```
PE1(config-router)#neighbor 2.2.2.2 remote-as 200

PE1(config-router)#neighbor 2.2.2.2 update-source Loopback0

PE1(config-router)#neighbor 3.3.3.3 remote-as 200

PE1(config-router)#neighbor 3.3.3.3 update-source Loopback0
```

- Configuración del *address-family* IPv4 de BGP.

```
PE1(config-router)#address-family ipv4

PE1(config-router-af)#neighbor 2.2.2.2 activate

PE1(config-router-af)#neighbor 3.3.3.3 activate
```

- Configuración del *address-family* VPNv4 de BGP.

```
PE1(config-router)#address-family vpnv4

PE1(config-router-af)#neighbor 2.2.2.2 activate

PE1(config-router-af)#neighbor 2.2.2.2 send-community extended

PE1(config-router-af)#neighbor 3.3.3.3 activate

PE1(config-router-af)#neighbor 3.3.3.3 send-community extended

PE1(config-router-af)#exit-address-family
```

- Configuración del protocolo de enrutamiento RIP para la VRF.

```
PE1(config)#router rip
```

```
PE1(config-router)#version 2
```

- Redistribución de los prefijos VPNv4 del protocolo MP-BGP (*MultiProtocol - BGP*) en RIP, mediante un *address-family*.

```
PE1(config-router)#address-family ipv4 vrf REDES
PE1(config-router-af)#redistribute bgp 200 metric 10
PE1(config-router-af)#network 192.168.1.0
PE1(config-router-af)#no auto-summary
PE1(config-router-af)#version 2
PE1(config-router-af)#exit-address-family
PE1(config-router-af)#no auto-summary
PE1(config-router-af)#exit-address-family
```

- Redistribución de las rutas RIP para la VRF en el protocolo MP-BGP.

```
PE1(config-router)#address-family ipv4 vrf REDES
PE1(config-router-af)#redistribute rip metric 50
PE1(config-router-af)#exit-address-family
```

- Configuración de SNMPv1 con su respectiva comunidad y en modo sólo lectura, para su posterior monitoreo.

```
PE1(config)#snmp-server community publicPE1 RO
```

2.2.1.2 Router P (Provider)

- Configuración de un protocolo de enrutamiento *Interior Gateway Protocol*, que en este caso es OSPF.

```
P(config)#router ospf 200
P(config-router)#network 10.10.10.0 0.0.0.3 area 0
P(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

- Configuración de MPLS en todas las interfaces.

```
P(config)#interface x/y

P(config-if)#mpls ip
```

- Configuración de SNMPv1 con su respectiva comunidad y en modo sólo lectura, para su posterior monitoreo.

```
P(config)#snmp-server community publicP RO
```

2.2.1.3 Router CE1 (Customer Edge 1)

- Configuración de la instancia VRF.

```
CE1(config)#ip vrf REDES
```

- Configuración del *Route Distinguisher*.

```
CE1(config-vrf)#rd 200:200
```

- Asociación de la VRF a la interfaz.

```
CE1(config)#interface x/y

CE1(config-if)#ip vrf forwarding REDES
```

- Configuración del protocolo de enrutamiento RIP para la VRF.

```
CE1(config)#router rip

CE1(config-router)#version 2

CE1(config-router)#address-family ipv4 vrf REDES

CE1(config-router-af)#network 192.168.1.0

CE1(config-router-af)#network 192.168.10.0

CE1(config-router-af)#no auto-summary

CE1(config-router-af)# version 2

CE1(config-router-af)#exit-address-family
```

- Configuración de SNMPv1 con su respectiva comunidad y en modo sólo lectura, para su posterior monitoreo.

```
CE(config)#snmp-server community publicCE1 RO
```

2.2.2 MULTICAST VPN [28], [29]

Una vez establecida la infraestructura *unicast* VPN, se habilita el enrutamiento *multicast* en los *routers* del proveedor y del cliente; de la misma forma, se configura el enrutamiento *multicast* para la VPN L3 en los *routers* de borde pertenecientes a la nube del proveedor. A continuación se habilita el protocolo de enrutamiento *multicast* PIM SM en cada interfaz de todos los *routers*; así como el protocolo de enrutamiento *multicast* PIM SSM en los *routers* que pertenecen al proveedor, es decir en los *routers* PE y P.

Para cumplir con el criterio del protocolo PIM SM, se configura el *Rendezvous Point* en los *routers* de borde del proveedor y del cliente. Por otro lado se crea una lista de control de acceso ACL para la unión de los *hosts* o receptores al grupo *multicast*, a través de IGMP. Dicha ACL se 'vincula' al comando '*ip pim rp-address 192.168.1.2*'.

Luego se configura el árbol de distribución *multicast* por defecto MDT dentro de la VPN L3 en los *routers* de borde del proveedor. Dentro del proceso BGP de cada *router* de borde del proveedor, se crea una familia de direcciones para el árbol de distribución *multicast,* con el fin de intercambiar información y actualización del MDT entre cada uno de los vecinos PE de la nube del proveedor.

2.2.2.1 Router P (Provider)

- Habilitación del enrutamiento *multicast*.

```
P(config)#ip multicast-routing
```

- Habilitación de PIM SM en las interfaces.

```
P(config)#interface x/y

P(config-if)#ip pim sparse-mode
```

- Habilitación de PIM SSM a nivel global.

```
P(config)#ip pim ssm default
```

2.2.2.2 Router PE1 (Provider Edge 1)

- Habilitación del enrutamiento *multicast*.

```
PE1(config)#ip multicast-routing
```

- Habilitación del enrutamiento *multicast* para la VRF.

```
PE1(config)#ip multicast-routing vrf REDES
```

- Habilitación de PIM SM en las interfaces.

```
PE1(config)#interface x/y

PE1(config-if)#ip pim sparse-mode
```

- Habilitación de PIM SSM a nivel global.

```
PE1(config)#ip pim ssm default
```

- Configuración de IGMP, por medio de una lista de control de acceso.

```
PE1(config)#access-list 50 permit 228.0.0.0 0.255.255.255
```

- Configuración del RP para la VRF.

```
PE1(config)#ip pim vrf REDES rp-address 192.168.1.2 50
```

- Configuración de la dirección del grupo MDT en la VRF.

```
PE1(config)#ip vrf REDES

PE1(config-vrf)#mdt default 232.1.1.1
```

- Configuración del *address-family* MDT en BGP.

```
PE1(config)#router bgp 200

PE1(config-router)#address-family ipv4 mdt

PE1(config-router-af)#neighbor 2.2.2.2 activate

PE1(config-router-af)#neighbor 2.2.2.2 send-community extended

PE1(config-router-af)#neighbor 3.3.3.3 activate

PE1(config-router-af)#neighbor 3.3.3.3 send-community extended
```

2.2.2.3 Router CE1 (Customer Edge 1)

- Habilitación del enrutamiento *multicast*.

```
CE1(config)#ip multicast-routing
```

- Habilitación de PIM SM en las interfaces.

```
CE1(config)#interface x/y

CE1(config-if)#ip pim sparse-mode
```

- Configuración del *Rendezvous Point*.

```
CE1(config)#ip pim rp-address 192.168.1.2
```

- Configuración de IGMP, por medio de una lista de control de acceso.

```
PE1(config)#access-list 50 permit 228.0.0.0 0.255.255.255
```

2.2.2.4 Pruebas de validación [29], [31]

La fuente está localizada detrás del *router* CE1, mientras que los receptores se encuentran detrás de CE2 y CE3. Cuando la fuente inicia el envío de tráfico *multicast* para la dirección de grupo 228.1.1.1, el *router* CE1 recibe los paquetes, chequea su tabla de enrutamiento *multicast* para el grupo 228.1.1.1, y crea una entrada (*, G), que para este caso es (*, 228.1.1.1), en su tabla de enrutamiento *multicast*.

Además, se crea un mensaje '*Register*' encapsulando el paquete *multicast* con la dirección del RP que es la 192.168.1.2 y lo reenvía al *router* PE1 como se aprecia en la Figura 2.4. Asimismo, el RP crea una entrada (S, G), que para este caso es (192.168.10.10, 228.1.1.1), conmuta sobre el árbol SPT (árbol de camino más corto) y envía un mensaje '*Register-stop*' al *router* CE1. El RP envía mensajes periódicos '*Join/Prune*' (Unión/Poda) a las interfaces *upstream* de los *routers* para unirse al árbol SPT.

Adicionalmente en la Figura 2.4, se visualiza para la entrada (*, 228.1.1.1) las banderas **SJC**, en donde **S** indica que está configurada en el modo PIM SM; **J**, unión al árbol SPT; y **C**, estado conectado.

En la Figura 2.5 se aprecia la ejecución del comando **mtrace**. Este comando es análogo al comando **tracert** en Windows o **traceroute** en Linux, y señala los distintos saltos que debe alcanzar un origen (192.168.10.10) hasta su destino (192.168.20.20).

```
CE1#sh ip mroute vrf REDES 228.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

*, 228.1.1.1), 03:06:18/00:02:52, RP 192.168.1.2, flags: SJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 01:24:19/00:02:43
    GigabitEthernet0/0, Forward/Sparse, 03:05:44/00:02:52

192.168.10.10, 228.1.1.1), 01:24:21/00:03:02, flags: T
  Incoming interface: GigabitEthernet0/1, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0, Forward/Sparse, 01:24:21/00:02:56
```

Figura 2.4 Tabla de enrutamiento *multicast* en CE1

```
CE1#mtrace
VRF name: REDES
Source address or name: 192.168.10.10
Destination address or name: 192.168.20.20
Group address or name: 228.1.1.1
Multicast request TTL [64]:
Response address for mtrace:
Type escape sequence to abort.
Mtrace from 192.168.10.10 to 192.168.20.20 via group 228.1.1.1 in VRF REDES
From source (?) to destination (?)
Querying full reverse path...
 0  192.168.20.20
-1  192.168.2.2 None  [192.168.10.0/24]
-2  0.0.0.0 None Admin. Prohibited !RPF!192.168.2.1 [default]
-3  0.0.0.0 None  [192.168.10.0/24]
-4  192.168.1.2 PIM Reached RP/Core [192.168.10.0/24]
CE1#
```

Figura 2.5 Ejecución del comando **mtrace** desde CE1

Este comando tiene la particularidad de que, en lugar de iniciar su ejecución desde el origen, lo hace desde el destino y termina en el origen; esto se debe, principalmente, a que IP *multicast* emplea toda comprobación, como en el caso de RPF, de la manera de 'camino inverso' o 'camino reverso'.

La Figura 2.6 ilustra los grupos de vecinos IGMP que están asociados a la VRF REDES. Se debe tomar en cuenta que el único grupo IGMP con el que se trabaja es el que posee la dirección IP 228.1.1.1; sin embargo, por defecto, aparecen otras direcciones de clase D cuando se configura IP *multicast*.

```
CE1#sh ip igmp vrf REDES group
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter   Gr
oup Accounted
239.192.152.143  GigabitEthernet0/1       01:42:40  00:02:22  192.168.10.10
239.255.255.250  GigabitEthernet0/1       04:10:20  00:02:23  192.168.10.10
228.1.1.1        GigabitEthernet0/1       01:42:40  00:02:23  192.168.10.10
224.0.1.40       GigabitEthernet0/0       04:57:06  00:02:17  192.168.1.2
CE1#
```

Figura 2.6 Grupos IGMP asociados a la VRF REDES en CE1

Luego que el *router* PE1 recibe los paquetes *multicast* sobre la VRF REDES, encapsula los paquetes *multicast* en GRE y los reenvía al grupo MDT por defecto 232.1.1.1 vía el Túnel MTI 1, como se muestra en la Figura 2.7. De esta manera, los *routers* PE2 y PE3 reciben esos paquetes GRE. Ambos *routers* desencapsulan los paquetes GRE y recuperan los paquetes *multicast*.

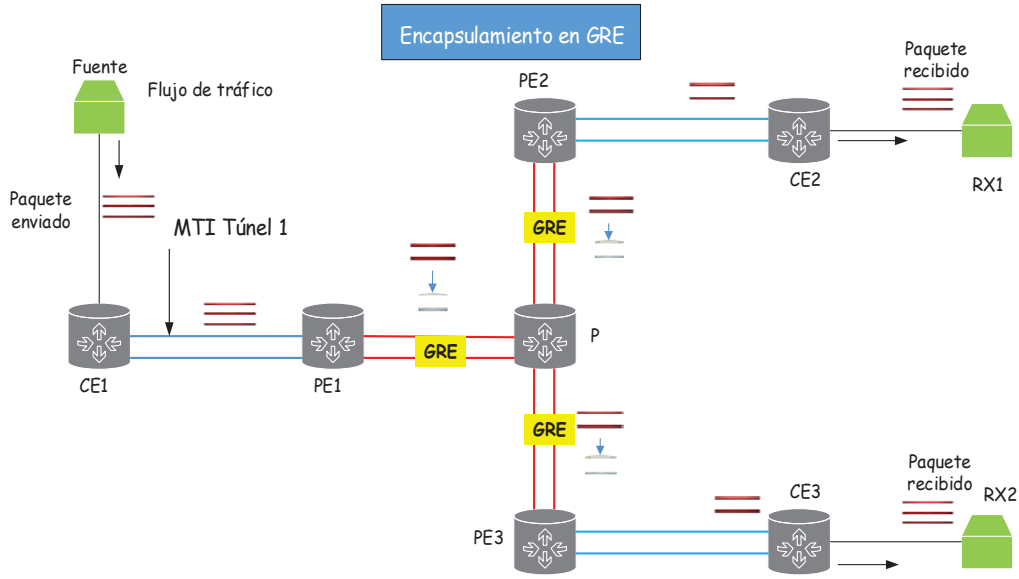

Figura 2.7 Esquema del encapsulamiento en GRE desde PE1

Hipotéticamente, si el *router* PE3 no tuviese algún receptor interesado en recibir el tráfico *multicast*, descartaría aquellos paquetes. Por otra parte, el *router* PE2 chequea su tabla de enrutamiento *multicast* y reenvía al *router* CE2; por consiguiente, éste reenviará esos paquetes sobre la interfaz VRF al *router* CE2. El *router* CE2 chequea su tabla de enrutamiento *multicast* y reenvía los paquetes a su receptor.

La Figura 2.8 muestra la tabla de enrutamiento *multicast* global en PE1, mediante la ejecución del comando *'show ip mroute'*. Los demás *routers* PE que se

encuentran en el mismo dominio *multicast*, tendrán la misma tabla de enrutamiento *multicast*.

La bandera **Z** indica que los paquetes *multicast* son enviados en la interfaz túnel *multicast* MTI, mientras que la bandera **s** indica que está configurado dentro de un grupo de Fuente Específica (SSM).

Las entradas de enrutamiento de la mVRF en PE1, observadas a través de la ejecución de la sentencia *'show ip mroute vrf REDES'* en las Figuras 2.9, 2.10 y 2.11, indican que la interfaz entrante es la *Gigabit Ethernet* 0/0 (la interfaz VRF hacia el *router* CE1), mientras que la interfaz saliente es la interfaz Túnel 1. En los *routers* PE2 y PE3, la interfaz entrante es el Túnel 1 y la interfaces salientes hacia el *router* CE2 y CE3 son las interfaces *Gigabit Ethernet* 0/1.

```
(2.2.2.2, 232.1.1.1), 03:20:29/stopped, flags: sTIZ
  Incoming interface: GigabitEthernet0/1, RPF nbr 10.10.10.2
  Outgoing interface list:
    MVRF REDES, Forward/Sparse, 03:20:29/00:00:30

(1.1.1.1, 232.1.1.1), 03:22:01/00:03:05, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 03:22:01/00:03:05

(3.3.3.3, 232.1.1.1), 03:22:01/stopped, flags: sTIZ
  Incoming interface: GigabitEthernet0/1, RPF nbr 10.10.10.2
  Outgoing interface list:
    MVRF REDES, Forward/Sparse, 03:22:01/00:01:58

(*, 224.0.1.40), 04:40:44/00:02:45, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Loopback0, Forward/Sparse, 04:40:42/00:02:45
```

Figura 2.8 Tabla de enrutamiento *multicast* global para PE1

```
(*, 228.1.1.1), 03:08:29/00:02:31, RP 192.168.1.2, flags: S
  Incoming interface: GigabitEthernet0/0, RPF nbr 192.168.1.2
  Outgoing interface list:
    Tunnel1, Forward/Sparse, 03:08:29/00:02:31

(192.168.10.10, 228.1.1.1), 01:27:01/00:02:20, flags: T
  Incoming interface: GigabitEthernet0/0, RPF nbr 192.168.1.2
  Outgoing interface list:
    Tunnel1, Forward/Sparse, 01:27:01/00:03:23

(*, 224.0.1.40), 04:41:30/00:02:56, RP 0.0.0.0, flags: DPL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

Figura 2.9 Tabla de enrutamiento *multicast* mVRF en PE1

```
(*, 228.1.1.1), 03:14:41/00:02:35, RP 192.168.1.2, flags: S
  Incoming interface: Tunnel1, RPF nbr 1.1.1.1
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 03:14:41/00:02:35

(192.168.10.10, 228.1.1.1), 01:33:40/00:01:38, flags: T
  Incoming interface: Tunnel1, RPF nbr 1.1.1.1
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 01:33:40/00:03:13

(*, 224.0.1.40), 04:44:38/00:02:07, RP 0.0.0.0, flags: DPL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

Figura 2.10 Tabla de enrutamiento *multicast* mVRF en PE2

```
(*, 228.1.1.1), 03:17:27/00:02:44, RP 192.168.1.2, flags: S
  Incoming interface: Tunnel1, RPF nbr 1.1.1.1
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 03:17:27/00:02:44

(192.168.10.10, 228.1.1.1), 01:35:59/00:03:20, flags: T
  Incoming interface: Tunnel1, RPF nbr 1.1.1.1
  Outgoing interface list:
    GigabitEthernet0/1, Forward/Sparse, 01:35:59/00:02:56

(*, 224.0.1.40), 04:45:06/00:02:31, RP 0.0.0.0, flags: DPL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null
```

Figura 2.11 Tabla de enrutamiento *multicast* mVRF en PE3

Cuando un *router* PE crea un árbol MDT por defecto, éste actualiza a sus otros pares usando MP-BGP. La Figura 2.12 muestra la dirección de aquel MDT. Por otro lado, 'la nueva fuente', dentro del *core* IP/MPLS, es la *loopback* 0 de PE1 (1.1.1.1/32) y el 'nuevo grupo' es la dirección del MDT, ya que GRE encapsula los paquetes *multicast* del cliente y los envía a través del Túnel 1.

```
PE1#sh ip pim mdt
  * implies mdt is the default MDT
  MDT Group/Num   Interface   Source                VRF
* 232.1.1.1       Tunnel1     Loopback0             REDES
PE1#
```

Figura 2.12 MDT establecido desde la *loopback* 0 de PE1

En la Figura 2.13 se observan las adyacencias PIM que PE1 mantiene con CE1 hacia la dirección 192.168.1.2 de CE1, por medio de la VRF. Mientras que, con PE2 y PE3, la adyacencia se forma vía la interfaz Túnel MTI 1 para la VRF.

```
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.1.2       GigabitEthernet0/0       04:43:08/00:01:20 v2    1 / DR S P G
2.2.2.2           Tunnel1                  03:22:53/00:01:37 v2    1 / S P G
3.3.3.3           Tunnel1                  03:24:21/00:01:42 v2    1 / DR S P G
PE1#
```

Figura 2.13 Adyacencias PIM en PE1

2.3 INSTALACIÓN Y CONFIGURACIÓN DEL GENERADOR DE TRÁFICO, SOFTWARE DE EMISIÓN DE VIDEO Y HERRAMIENTA DE MONITOREO DE VIDEO

2.3.1 JPERF [33], [34]

Ésta es una herramienta de libre distribución que posee una interfaz gráfica de usuario, desarrollada en Java, y basada en Iperf, que permite generar tráfico TCP o UDP, *unicast* y/o *multicast*, con el fin de obtener estadísticas del *throughput* y el *jitter* de una red, ya sea en una LAN o WAN; además, tiene la capacidad de "correr" sobre plataformas Linux y Windows con las mismas funcionalidades.

Jperf permite al usuario ver el comportamiento del *throughput* y el *jitter* en tiempo real, tanto de forma gráfica como de texto, según se observa en los recuadros 1 y 2 de la Figura 2.14, respectivamente. Se pueden almacenar los resultados finales como el *throughput*, cantidad de datos enviados/recibidos, *jitter* y pérdida de paquetes a un archivo que puede ser leído por cualquier editor de texto.

Este *software* de generación de tráfico se compone del cliente (fuente) y del servidor (receptor), como se aprecia en el recuadro 3 de la misma figura. Del lado del cliente, se añade la dirección IP del servidor y se conecta a través del puerto 5001. Asimismo, se pueden ejecutar varios *streams* al mismo tiempo. Del lado del servidor, se coloca el mismo puerto 5001 en modo de escucha y si el usuario lo desea, puede agregar un sinnúmero de conexiones simultáneas.

Como se observa en el recuadro 4, dentro de las opciones de TCP, es posible variar el tamaño del búfer, el tamaño de la ventana TCP, el tamaño máximo del segmento y el seleccionar la no generación de retardo TCP. Mientras que para UDP, permite variar el *throughput*, el tamaño del búfer y el tamaño del paquete UDP. Para transmisiones *multicast*, permite adherirse a algún grupo agregando su dirección IP.

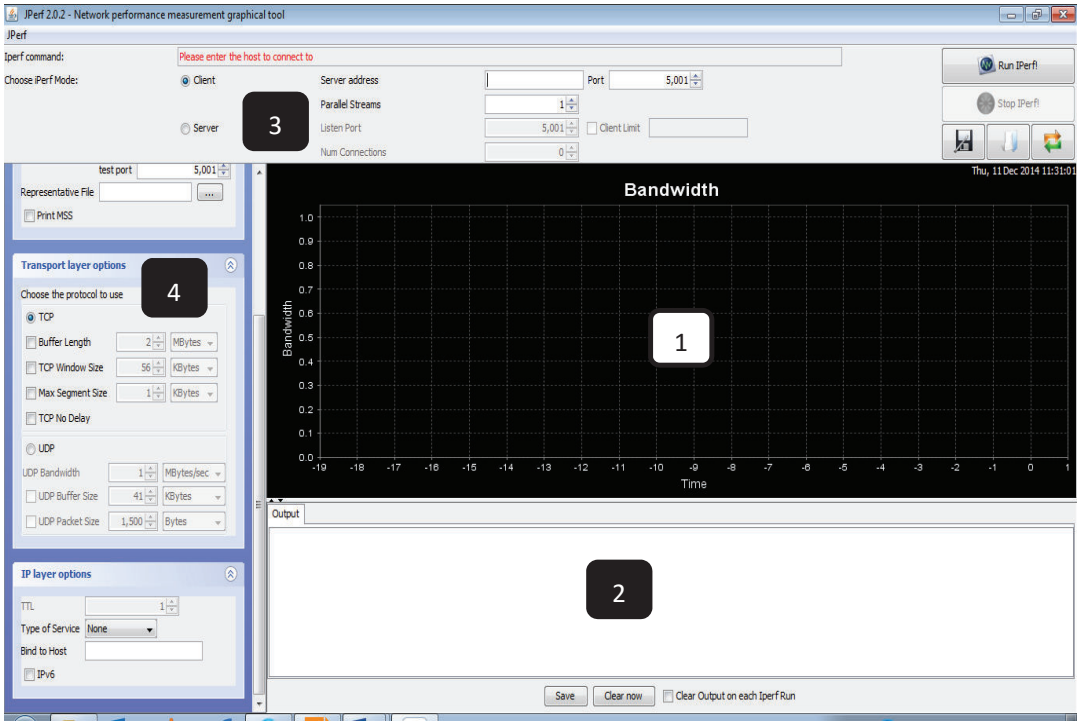

Figura 2.14 Ventana principal de la herramienta Jperf

La Tabla 2.4 describe las 'banderas' de Jperf, que no son más que los parámetros a escoger para la generación/recepción de tráfico, ya que Jperf se basa en Iperf y esta herramienta funciona a través de la línea de comandos de un *shell* de mandatos.

BANDERA	SIGNIFICADO	EJEMPLO
-c	Dirección IP *unicast* o *multicast*	192.168.20.20
-u	UDP	---
-P	*Streams* paralelos	1
-i	Intervalo de tiempo	1 segundo
-p	Número de puerto	5004
-l	longitud del PDU	1000,0 Bytes
-f	Desplegar resultados en bits	Kbits
-b	*Throughput*	125,0 Kbps
-t	Tiempo de muestreo	900 segundos
-T	Valor del TTL	10
-s	Servidor	---
-B	Asociar a un grupo *multicast*	228.1.1.1

Tabla 2.4 Significado de las banderas en Jperf

Sin embargo, un estudio realizado acerca del comportamiento de algunos generadores de tráfico, entre ellos Jperf, indica que el desempeño y los resultados de varias pruebas a que fueron sometidos, mostraron un desempeño 'distinto' entre ellos, sin mencionar cuál era el 'mejor generador de tráfico'. [33]

2.3.2 SOFTWARE DE EMISIÓN DE VIDEO VLC [35], [36]

VLC es un *software* de libre distribución desarrollado por VideoLAN. VLC puede ser utilizado como servidor y como cliente para realizar y recibir *streaming unicast* o *multicast* en una red. Esta herramienta es capaz de realizar *streams* de medios sobre redes de computadoras y transcodificar archivos multimedia.

La Figura 2.15 muestra las principales opciones de VLC para realizar una transmisión de audio/video, como son el 'Emitir' (transmisión) y el 'Abrir volcado de red' (recepción).

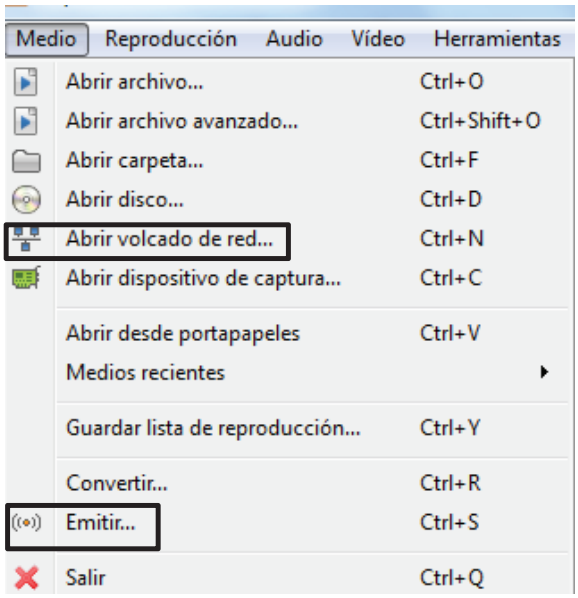

Figura 2. 15 Opciones de emisión y recepción en VLC

2.3.2.1 Métodos de streaming

VLC soporta varios métodos de compresión de audio y video y formatos de archivos, y de manera particular, protocolos de *streaming*. La Figura 2.16 ilustra todos los métodos posibles con los que puede trabajar esta herramienta, como es a través de HTTP (Protocolo de Transferencia de Hipertexto), RTP (Protocolo de Transporte en Tiempo Real) / MPEG *Transport Stream*, UDP (*legacy*) (Protocolo de

Datagrama de Usuario), etc. y *Icecast* que es un servidor de video *streaming* del sistema operativo Linux al que puede conectarse el reproductor multimedia VLC.

- RTP/UDP *unicast*: Se realiza el *stream* a una sola computadora. Para ello se debe ingresar la dirección IP del cliente (rango de 0.0.0.0 a la 223.255.255.255).
- RTP/UDP *multicast*: Se realiza el *stream* a múltiples computadoras usando *multicast*. Se debe ingresar la dirección IP del grupo *multicast* (rango de 224.0.0.0 a 239.255.255.255). La Figura 2.17 ilustra la recepción de un video usando este método.

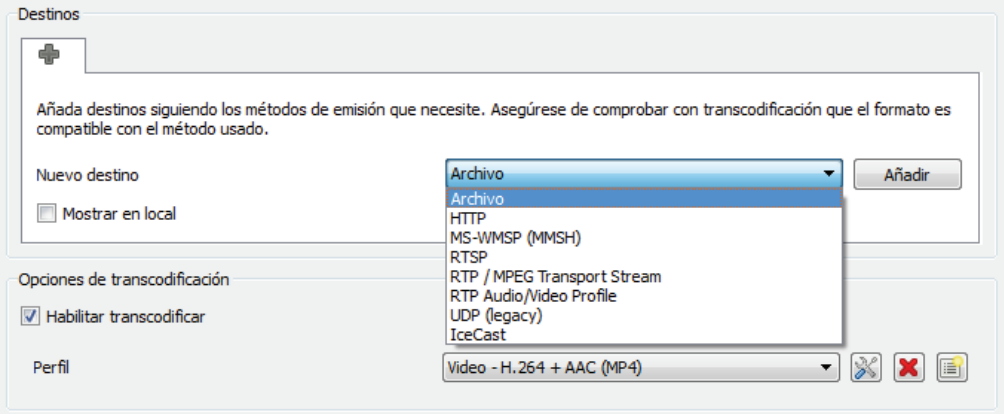

Figura 2.16 Métodos de *streaming* en VLC

- HTTP: El *stream* se lo realiza usando el protocolo HTTP. VLC escuchará en todas las interfaces de la red del servidor en el puerto 8080.

Figura 2.17 Recepción de video utilizando el protocolo RTP

2.3.2.2 Opciones de transcodificación [37]

Si se escoge la opción 'Transcodificar' se puede especificar el nuevo códec de audio y video que se desea ingresar para transcodificarlo, con el propósito de que todos los clientes puedan reproducir el contenido. Existen varios formatos comprimidos (MP3, OGG, etc.), así como también sin comprimir, como se observa en la Figura 2.18. Se puede no utilizar transcodificación; pero si se utiliza, se debe observar cuál es el formato óptimo con que se va a trabajar.

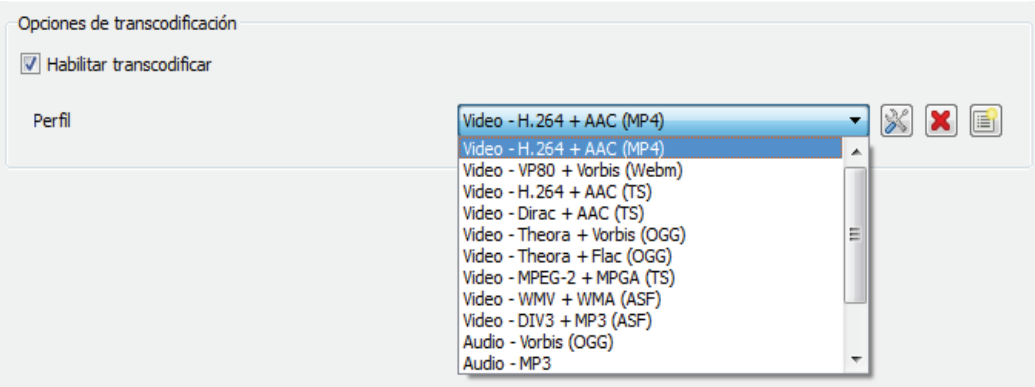

Figura 2.18 Opciones de transcodificación en VLC

2.3.2.3 Opciones de streaming

Para realizar un *streaming* de audio/video es muy importante conocer el campo *Time To Live* (TTL) que muestra el número de *routers* por los cuales el *stream* debe pasar, esto es para los métodos de acceso *unicast* TCP y *unicast* UDP. Si se desconoce este parámetro se debe dejar el valor por defecto. Por defecto, el valor de TTL es 1, lo que significa que el *stream* no pasará por ningún *router*.

Se deberá incrementar este valor para trabajar en ambientes *multicast*. Para este proyecto se escogió la versión VLC 1.1.8 ya que permite modificar el valor de TTL y alcanzar el destino, a diferencia de las últimas versiones que no permiten modificar este campo. En la Figura 2.19 se observa el campo TTL a ser modificado.

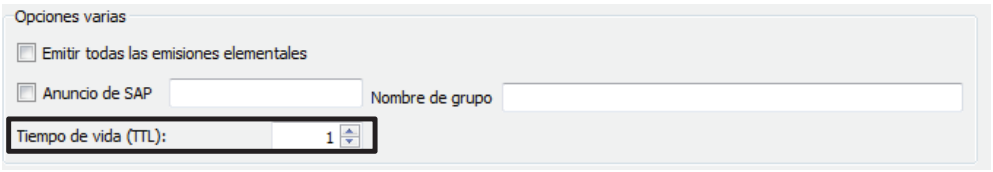

Figura 2.19 Campo TTL para transmisiones con UDP

2.3.3 HERRAMIENTA DE MONITOREO DE VIDEO FAULTLINE [32]

FaultLine, de la empresa Certus Digital, es una aplicación para el monitoreo de video, que trabaja sobre la plataforma Windows, tal como se aprecia en la Figura 2.20.

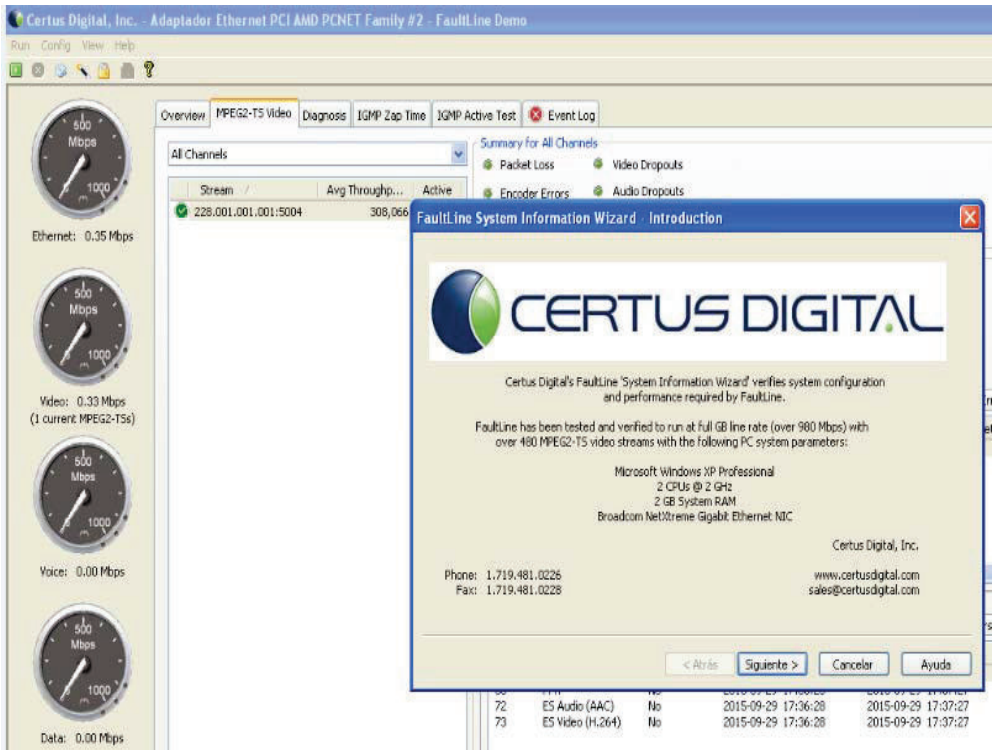

Figura 2.20 Ventana principal de la herramienta *FaultLine*

Esta aplicación analiza el desempeño de video sobre IP proporcionando la búsqueda de paquetes de video o de IPTV sospechosos para identificar sus problemas en cuanto se refiere a su contenido, codificación, o situaciones anómalas de la red; presenta al usuario final un detalle de las estadísticas, alarmas y alertas de dicho comportamiento a lo largo del tiempo.

Además, *FaultLine* provee un análisis de la transmisión de *streams* de varios formatos de video (MPEG-1, MPEG-2[13], H.264, MPEG-4), métricas de los principales parámetros de calidad de servicio y calidad de experiencia como la pérdida de paquetes y *jitter,* el *throughput* por *stream* tanto para *streams unicast* y

[13] MPEG-2 *Transport Stream* (MPEG-2 TS) es un formato de contenedor para la transmisión de *streams* elementales (video, audio y datos), mientras que MPEG-2 y MPEG-4/H.264 son estándares para la compresión de audio y video.

multicast de video sobre IP e IPTV, hasta un número máximo de 1024 *streams* de video simultáneos. Como se observa en la Figura 2.21, la versión de prueba permite una recolección de datos de hasta 60 segundos.

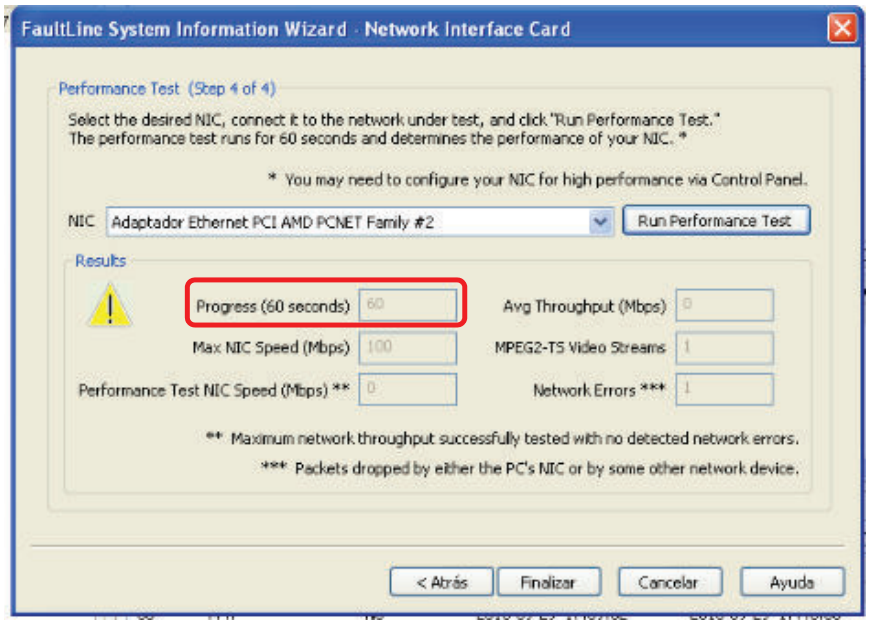

Figura 2.21 Medición de parámetros durante 60 segundos con *FaultLine*

FaultLine "corre" sobre máquinas basadas en Windows (puede estar activa durante las 24 horas del día todos los días) preferiblemente sobre las versiones XP, 7 y Server 2003. Los datos registrados pueden ser guardados en un archivo de texto para su posterior análisis.

Para un correcto funcionamiento se debe disponer de una tarjeta de red cuyo valor dependerá de cuánta carga de video se desee analizar, ya que esta herramienta proporciona mediciones de hasta 1 Gb/s. Asimismo, los mínimos requerimientos que el *hardware* del computador debe poseer son el disponer un procesador de 2 GHz *Dual Core* y una memoria RAM de 2 GB.

Para iniciar un *test* de video sólo basta con ingresar la dirección IP del host *unicast* o grupo *multicast* a ser analizado En las Figuras 2.22 y 2.23 se aprecian los resultados de las mediciones del *throughput*, así como también de las mediciones del *jitter,* respectivamente, una vez finalizado el período de análisis.

Este *software* emplea dos formas para conectarse a la red y monitorear el video: pasiva y activa. En la forma pasiva, *FaultLine* debe conectarse a un divisor (*splitter*)

eléctrico u óptico. En la forma activa, *FaultLine* se conecta a un puerto no usado de un *switch*, previamente configurado con la característica de '*mirror*' o espejo.

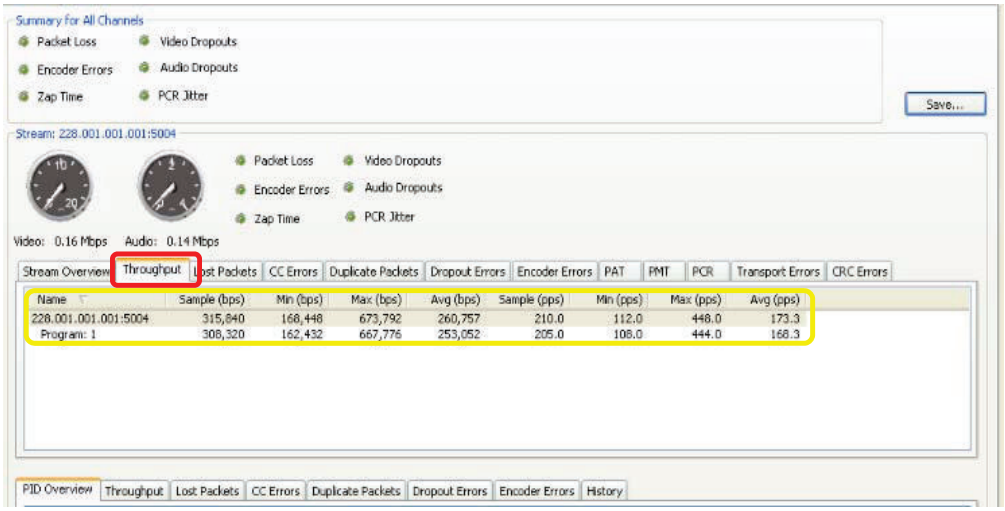

Figura 2.22 Resultados de las mediciones del *throughput* con *FaultLine*

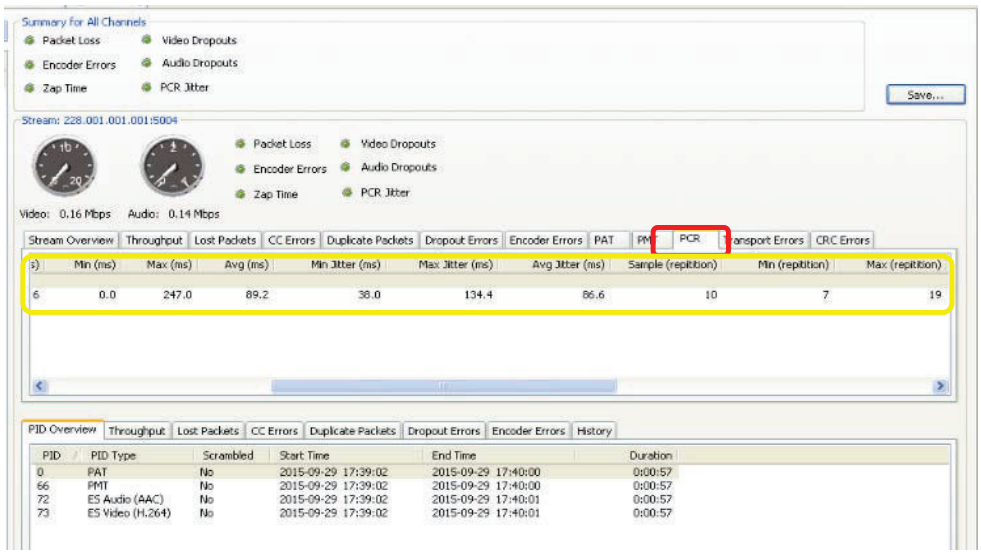

Figura 2.23 Resultados de las mediciones del *jitter* con *FaultLine*

3. ANÁLISIS DE RESULTADOS

Durante esta fase se elaboraron distintos escenarios de pruebas que comprendieron la generación de tráfico y la emisión de video *unicast* y *multicast* sobre los prototipos de red IP/MPLS *unicast* VPN y *multicast* VPN. Además se midieron algunos parámetros de calidad de servicio para su posterior análisis.

Luego de la generación de tráfico y la emisión de video en ambos escenarios (*unicast* y *multicast*) se obtuvieron datos propios en cada receptor y que podían ser abiertos desde cualquier editor de texto. Estos tabulados contienen los valores de los parámetros medidos durante el período de ejecución de cada prueba.

Para el caso de Jperf se generaron datos cada segundo, lo que conllevó a almacenar gran cantidad de información. Es por ello que se optó por recoger una muestra de 30 observaciones de una población de 100 por cada receptor. Luego se decidió juntar las mediciones de ambos receptores con el fin de obtener un factor común de mediciones para su mejor comprensión y análisis.

Un caso distinto se presentó para *FaultLine*. Esta herramienta generó reportes de sus mediciones luego de haber transcurrido 60 segundos de la reproducción del video. Es así que se midieron 20 observaciones con el propósito de cubrir la mayor parte de la difusión del video.

De la misma forma, como sucedió con Jperf, se decidió juntar las mediciones de ambos receptores (video) con la finalidad de obtener un factor común de mediciones para su mejor comprensión y análisis.

Para estudiar los datos medidos de un fenómeno experimental que ocurrió en laboratorio, es necesario contar con ‘medidas estadísticas’ que contribuyan a reunir todos estos datos de mejor manera para entender y analizar sus resultados.

Para cada parámetro se tomó en cuenta los valores máximo y mínimo como referentes; la media (promedio) como medida principal; la mediana, para comparar en cuánto difiere o se asemeja a la media; y la desviación estándar, que al ser matemáticamente la raíz cuadrada de la varianza, brinda información de qué tan agrupados o dispersos se encuentran los datos medidos respecto a su media.

3.1 BREVE INTRODUCCIÓN A LA TEORÍA DE COLAS [38], [39], [40]

La limitante que se presentó en el prototipo fue el ancho de banda del enlace comprendido entre los *routers* PE1 y P, cuyo valor máximo es de 8 Mb/s y que genera un "cuello de botella" al tráfico que cursa por ese trayecto de la red. Debido a este factor, se estudió el tema de teoría de colas para entender de mejor manera el comportamiento de los parámetros de calidad de servicio de la red, recogidos durante el muestreo.

Un sistema de encolamiento como se presenta en la Figura 3.1, consiste de una cola de tamaño finito o infinito y uno o más servidores idénticos. Un servidor sólo puede servir a un paquete a la vez, ya sea que se encuentre ocupado o no.

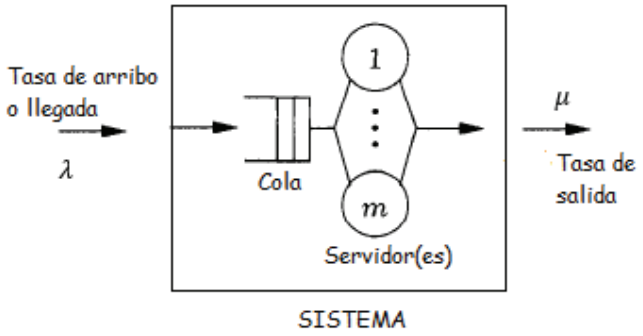

Figura 3.1 Sistema con m servidores [38]

La intensidad de tráfico *ρ* (adimensional), se define como la razón entre la tasa de arribo al sistema *λ*, y la tasa máxima de salida *μ* que suministra el servidor, tal como lo muestra la Ecuación 3.1.

$$\rho = \frac{tasa\ de\ arribo\ o\ llegada}{tasa\ de\ salida} = \frac{\lambda}{\mu}$$

Ecuación 3.1 Intensidad de tráfico [39]

Por otra parte, si se denota al ancho de banda del enlace de salida a la cual los bits son puestos fuera de la cola como *R*, y a *L* como el tamaño del paquete, la intensidad de tráfico se define como la relación del producto de la tasa de arribo de los paquetes por su respectivo tamaño dividido para el ancho de banda del enlace de salida, como lo muestra la Ecuación 3.2.

$$Si\ \mu = \frac{R}{L} \rightarrow \rho = \frac{\lambda . L}{R}$$

Ecuación 3.2 Intensidad de tráfico en función de λ, L y R [40]

De la misma forma, se puede interpretar a la intensidad de tráfico como la razón entre el tiempo de servicio y el tiempo de arribo, tal como se expresa en la Ecuación 3.3.

$$\rho = \frac{tiempo\ \ de\ servicio}{tiempo\ de\ arribo} = \frac{1/\mu}{1/\lambda}$$

Ecuación 3.3 Intensidad de tráfico en función de los tiempos de servicio y arribo [39]

En conclusión, para que un sistema tenga una solución, es necesario que $\rho < 1$. Si por el contrario, $\rho \geq 1$, se tendrá que la tasa de llegada o arribo al sistema es mayor que la tasa de salida; o dicho en otras palabras, el tiempo que asigna el servidor en 'atender' a un paquete es mayor que el tiempo de arribo.

Asimismo se puede interpretar el tiempo promedio de permanencia en el sistema, denotado como *T*, a la razón entre el tiempo de servicio y el complemento de la intensidad de tráfico. La Ecuación 3.4 determina el tiempo de permanencia en el sistema.

$$T = \frac{\frac{1}{\mu}}{1 - \rho}$$

Ecuación 3.4 Tiempo de permanencia en el sistema [39]

La diferencia entre los tiempos de permanencia en el sistema y el tiempo de servicio, como se observa en la Ecuación 3.5, se denomina tiempo promedio de espera en la cola, denotado como *W*.

$$W = T - t_s$$

Ecuación 3.5 Tiempo promedio de espera en la cola [39]

La Figura 3.2 muestra un esquema de análisis de los sistemas de encolamiento '*Router* PE1' y '*Router* P' interconectados por el enlace de "cuello de botella" y que pertenecen a la red IP/MPLS, cuya inferencia sirve para los escenarios *unicast* y *multicast*.

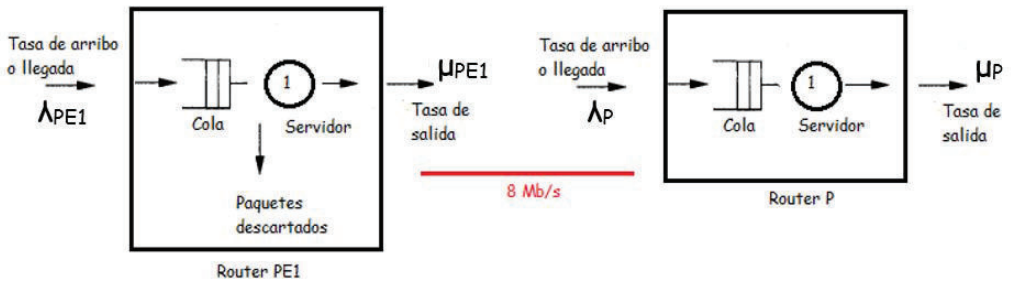

Figura 3.2 Esquema de análisis de los sistemas de encolamiento '*Router* PE1' y '*Router* P'

En el sistema denominado '*Router* PE1' existe una tasa de arribo λ_{PE1} a la cual llegan los paquetes e ingresan a la cola de tipo FIFO (Primero en Ingresar, Primero en Salir) y que luego son atendidos por el servidor, y finalmente son puestos en el canal (enlace de 8 Mb/s) a una tasa de salida de paquetes μ_{PE1}.

En el sistema '*Router* P' se visualiza una tasa de arribo λ_P a la cual llegan los paquetes e ingresan a la cola de tipo FIFO; posteriormente, los paquetes son atendidos por el servidor, y finalmente son puestos en el canal (de 1 Gb/s) a una tasa de salida de paquetes μ_P.

Cuando un paquete arriba a un *router* o a un nodo, podría encontrarse con una cola totalmente llena; si no existe lugar alguno para almacenar un paquete, el *router* descartará ese paquete, lo que significa que el paquete se perderá. La sumatoria de la tasa de paquetes recibidos con éxito más la tasa de paquetes perdidos dan como resultado la tasa total de paquetes. La tasa de pérdida de paquetes se encuentra en función de la tasa de arribo de paquetes para el sistema *Router* P y de la tasa de arribo de paquetes para el sistema *Router* PE1, y está dada por la Ecuación 3.6.

$$Tasa\ pérdida\ de\ paquetes = 1 - \frac{\lambda_P}{\lambda_{PE1}}$$

Ecuación 3.6 Tasa de pérdida de paquetes en función de las tasas de arribo de los paquetes a los sistemas PE1 y P

Si bien λ_{PE1} y λ_P representan las tasas de arribo de paquetes a los sistemas *Router* PE1 y *Router* P respectivamente, así como μ_{PE1} y μ_P denotan las tasas de salida de los paquetes de los sistemas *Router* PE1 y *Router* P, no se debe relacionar λ y μ

como variables que presentan un mismo comportamiento, solo por el hecho de que llevan la misma unidad (paquete/segundo).

Como quedó definido, λ constituye el número de paquetes promedio por unidad de tiempo que llegan a un sistema de encolamiento y precisamente, aunque parezca obvio, está en función del número de paquetes y de la unidad de tiempo; en otras palabras, λ representa el *throughput* promedio de entrada a un sistema.

Por lógica, se supondría el mismo raciocinio para μ, pero no lo es, ya que la tasa promedio de salida de paquetes de un sistema de encolamiento se encuentra en función del valor del ancho de banda del enlace de salida del sistema y del tamaño del paquete (carga útil), lo que no constituye un '*throughput*', aunque posea la misma unidad que la tasa de arribo de paquetes a un sistema.

Sin embargo, se puede decir que el valor máximo al cual se pueden colocar los paquetes fuera del sistema, no debe ser mayor que el valor de μ. Esto quiere decir que el valor de aquel *throughput* no debe exceder la capacidad del enlace o ancho de banda por el que viajarán los paquetes. Esto corrobora la definición misma de la tasa de salida de paquetes (μ) de un sistema de encolamiento.

Por el razonamiento antes expuesto, se toma en cuenta a los '*throughputs*' de ambos sistemas para relacionarlos tanto a λ_P como el *throughput* de salida del sistema *Router* PE1, y a λ_{PE1} como el *throughput* de entrada a dicho sistema, con el propósito de obtener un valor: el porcentaje de paquetes recibidos con éxito.

Si la relación entre las tasas λ_P y λ_{PE1} es pequeña, la razón de pérdida de paquetes será grande, ya que λ_P es mucho menor que λ_{PE1}; por el contrario, si aquella relación es grande, la tasa de pérdida de paquetes será pequeña, debido a que λ_P se aproxima a λ_{PE1}. Por lo tanto, existen escenarios en donde se presentan mayores pérdidas de paquetes que en otros.

3.2 BATERÍA DE PRUEBAS 1

3.2.1 EXPERIMENTO

Generación de tráfico *unicast* UDP en la red IP/MPLS *unicast* VPN con tamaños de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes, utilizando Jperf. El *throughput* nominal de la fuente es de 6 Mb/s (3 Mb/s por cada

receptor). Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente, el número de paquetes recibidos y el porcentaje de pérdida de paquetes. La Tabla 3.1 muestra los resultados estadísticos de la generación de tráfico *unicast* UDP para un tamaño de carga útil de 64 bytes a un *throughput* nominal de 3 Mb/s.[14]

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2275	0,014	943	5858	16,1
Máximo	2524	0,389	1535	5978	25,7
Media	2398,9	0,14	1201	5886	20,4
Mediana	2397	0,084	1188	5875	20,2
Desv. Est.	63,3	0,13	135,8	34,7	2,3

Tabla 3.1 Resultados estadísticos de la generación de tráfico *unicast* UDP para 64 bytes @ 3 Mb/s

3.2.2 PRESENTACIÓN DE RESULTADOS

La Tabla 3.2 detalla los valores promedio de los parámetros de calidad de servicio registrados para cada tipo de *payload,* como son el *throughput*, el *jitter*, los paquetes generados por la fuente, los paquetes recibidos en los receptores y el porcentaje de pérdida de paquetes que existieron luego de la generación de tráfico *unicast* UDP a 3 Mb/s.

Para una mejor explicación, se tomó en cuenta los datos de la carga útil de 64 bytes. Desde el punto de vista de la fuente *unicast*, ésta genera dos emisiones, por lo cual se multiplica por 2 al *throughput,* medido en unidades de paquetes/s, que arriban al *router* PE1 y que constituye el valor de $\lambda_{PE1.}$

$$\lambda_{PE1} = 2\ x\ 5886\ \left[\frac{paquete}{s}\right] \Rightarrow \lambda_{PE1} = 11772\ \left[\frac{paquete}{s}\right]$$

Luego se obtiene el valor de μ_{PE1} (tasa de salida de paquetes del sistema de encolamiento *Router* PE1) a partir de la Ecuación 3.2, sabiendo que el enlace de salida corresponde al "cuello de botella" (entre los routers *PE1* y *P*) de valor 8 Mb/s.

[14] En el Anexo D "Tabulados correspondientes a la Generación de Tráfico *Unicast* y *Multicast* con Jperf y VLC" se encuentran los resultados estadísticos con todos los tamaños de carga útil y *throughputs* nominales de la fase de experimentación.

Payload [B]	*Throughput* [Kb/s]	*Jitter* [ms]	Paquetes generados [p/s]	Paquetes recibidos [p/s]	Tasa de pérdidas [%]
64	2398,9	0,14	5886	4685	20,4
128	2990,7	0,356	2934	2921	0,5
256	2994,5	0,945	1466	1462	0,3
512	2993,9	2,657	733	731	0,2
1024	2998,1	5,199	366	366	0,1
1400	3002	6,826	268	268	0,0

Tabla 3.2 Promedio de los resultados del experimento generación de tráfico *unicast* UDP @ 3 Mb/s para todos los tamaños de *payload*

$$\mu_{PE1} = \frac{R}{L} = \frac{8\left[\frac{Mbits}{s}\right] x \frac{10^6\ [bits]}{1\ [Mbit]}}{64\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow \mu_{PE1} = 15625\ \left[\frac{paquete}{s}\right]$$

Para conseguir la intensidad de tráfico del sistema PE1, es necesario dividir ambos resultados anteriores. Además si ρ_{PE1} es menor a 1, se pueden calcular las variables de tiempo *T,* t_s y *W* para el sistema PE1.

$$\rho_{PE1} = \frac{\lambda_{PE1}}{\mu_{PE1}} = \frac{11772\left[\frac{paquete}{s}\right]}{15625\left[\frac{paquete}{s}\right]} \Rightarrow \rho_{PE1} = 0{,}75$$

Después de haber atravesado “el cuello de botella”, el *throughput* nominal del paquete que fue enviado desde la fuente, disminuyó de 3000 Kb/s a 2398,9 Kb/s para este caso en estudio. Por ello, otra forma de calcular la tasa de arribo a un sistema está en función del *throughput* de llegada al *router* (bits/s) y el tamaño del paquete. La Ecuación 3.7 muestra dicha relación.

$$\lambda = \frac{throughput}{L}$$

Ecuación 3.7 Tasa de arribo de paquetes al sistema en función del *throughput* y del tamaño del paquete

Así como sucedió con λ_{PE1}, se multiplica por 2 al *throughput* de la tasa de arribo de paquetes al sistema P (λ_P), ya que la fuente *unicast* genera dos emisiones. Mediante la Ecuación 3.7, se halla la variable λ_P.

$$\lambda_P = \frac{2\ x\ throughput}{L} = \frac{2\ x\ 2398{,}87\left[\frac{Kb}{s}\right]\ x\ \frac{1000\ [bits]}{1\ [Kb]}}{64\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow \lambda_P = 9371\ \left[\frac{paquete}{s}\right]$$

De la misma forma se encuentra el valor de μ_P a través de la Ecuación 3.2.

$$\mu_P = \frac{R}{L} = \frac{1\left[\frac{Gbit}{s}\right] x \frac{10^9\,[bits]}{1\,[Gbit]}}{64\,[B]\; x\; \frac{8\,[bits]}{1\,[B]}} \Rightarrow\; \mu_P = 1953125\left[\frac{paquete}{s}\right]$$

Finalmente se calcula el valor de ρ_P.

$$\rho_P = \frac{\lambda_P}{\mu_P} = \frac{9371\left[\frac{paquete}{s}\right]}{1953125\left[\frac{paquete}{s}\right]} \Rightarrow\; \rho_P = 0{,}0048$$

La Tabla 3.3 muestra las tasas de arribo y de salida de los sistemas PE1 y P, así como la comprobación del porcentaje de pérdidas de paquetes frente a los datos obtenidos en la generación de tráfico *unicast* UDP para todos los tamaños de carga útil vistos. Se observa en este tabulado que el factor de intensidad de tráfico para cualquier valor de *payload* en el sistema PE1 es constante e igual a 0,75.

$$Relación\ pérdida\ de\ paquetes = 1 - \frac{\lambda_P}{\lambda_{PE1}} = 0{,}204 = 20{,}4\%$$

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	λ_P [p/s]	Pérdidas [%]
64	11772	15625	0,75	9371	20,4
128	5868	7812,5	0,75	5841	0,5
256	2932	3906,3	0,75	2924	0,3
512	1465	1953,1	0,75	1462	0,2
1024	733	976,6	0,75	732	0,1
1400	536	714,3	0,75	536	0,0

Tabla 3.3 Intensidad de tráfico para el sistema PE1 y comprobación del porcentaje de pérdida de paquetes para todos los valores de *payload unicast* UDP @ 3 Mb/s

A partir del factor de intensidad de tráfico de PE1 se calculan los valores del tiempo de servicio ts_{PE1}, el tiempo de permanencia en el sistema T_{PE1}, y el tiempo promedio de espera en la cola W_{PE1}. Estos datos se muestran en detalle en la Tabla 3.4.

$$ts_{PE1} = \frac{1}{\mu_{PE1}} = \frac{1}{15625\left[\frac{paquete}{s}\right]} \Rightarrow\; ts_{PE1} = 64\,[us]$$

$$T_{PE1} = \frac{\frac{1}{\mu_{PE1}}}{1 - \rho_{PE1}} = \frac{\frac{1}{15625\left[\frac{paquete}{s}\right]}}{1 - 0{,}75} \Rightarrow\; T_{PE1} = 256\,[us]$$

$$W_{PE1} = T_{PE1} - ts_{PE1} = 256\ [us] - 64\ [us] \Rightarrow W_{PE1} = 196\ [us]$$

Payload [B]	ts_{PE1} [us]	W_{PE1} [us]	T_{PE1} [us]
64	64	192	256
128	128	384	512
256	256	768	1024
512	512	1536	2048
1024	1024	3072	4096
1400	1400	4200	5600

Tabla 3.4 Tiempos (retardos): de servicio, de espera en la cola, y de permanencia en el sistema PE1, para todos los valores de *payload unicast* UDP @ 3 Mb/s

Debido a que T_{PE1} es un 'retardo' considerable en relación al resto de 'sistemas *Routers*' de la red por el "cuello de botella" existente, se trató de determinar si el tiempo promedio que un paquete permanece en el sistema PE1 (Tabla 3.4) incide, mantiene o posee correlación alguna con el *jitter* (Tabla 3.2), para todos los tamaños de carga útil.

La Figura 3.3 muestra un gráfico de dispersión de datos entre estas variables, para todos los tamaños de *payload.* Nótese que la línea de tendencia central tiene una pendiente positiva, lo que presume que el tiempo de permanencia en el sistema PE1 y el *jitter* son directamente proporcionales.

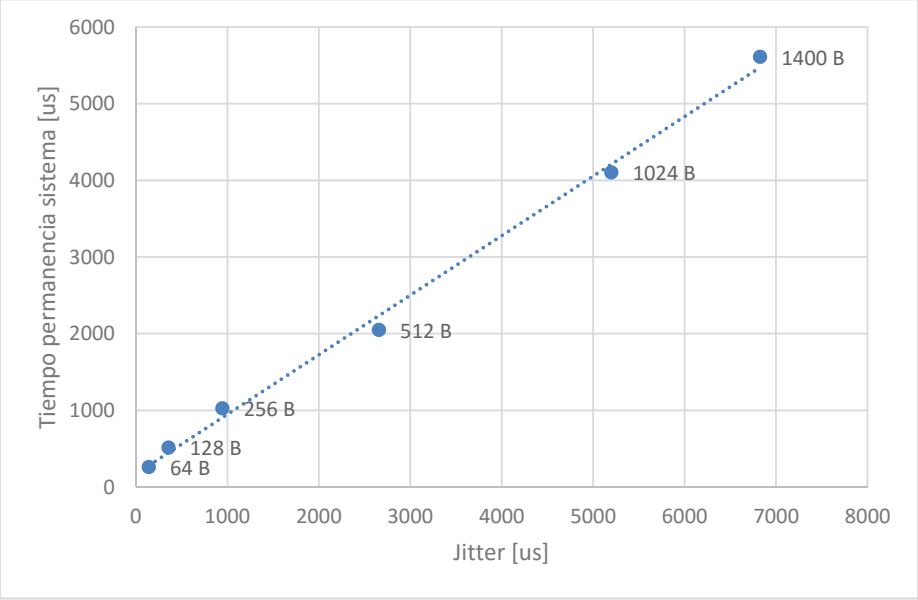

Figura 3.3 Tiempo de permanencia en el sistema vs el *jitter* del tráfico *unicast* UDP, a una tasa de 3 Mb/s

Por la razón antes expuesta se planteó una prueba de hipótesis estadística entre estas dos variables. Existen dos clases de pruebas estadísticas: paramétricas y no paramétricas. Las pruebas paramétricas poseen una gran capacidad para detectar una relación real o verdadera entre dos variables, si existiese.

Para abordar el estudio de una prueba paramétrica se toman en cuenta tres factores. El primer factor es disponer una población numérica con una muestra mínima de 30 observaciones; el segundo factor obedece a que, esta población o poblaciones a ser analizadas, sigan una distribución normal; y el tercer factor exige que las varianzas de las variables de estudio sean homogéneas.

Para este caso de estudio se tiene un muestreo muy bajo (seis, correspondientes a los distintos tamaños de *payload*); la población, tanto del *jitter* como del tiempo de permanencia en el sistema, no siguen una distribución normal, y sus varianzas no son homogéneas. Por lo tanto, no se puede realizar una prueba estadística paramétrica.

El coeficiente de correlación de Spearman es un tipo de estudio estadístico no paramétrico que no necesita conocer previamente la distribución de una población y permite trabajar con cualquier tamaño de muestra.

Spearman es una medida de la relación que existe entre los rangos de dos variables y puede variar desde -1,00 a +1,00. El valor -1,00 indica una relación negativa perfecta y el valor +1,00 señala una relación positiva perfecta. El valor cero indica que no existe relación alguna entre las variables. [41]

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1 [15]: se plantea una hipótesis alterna bidireccional.

H_0: No existe una correlación entre el tiempo de permanencia en el sistema PE1 y el *jitter*, en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 3 Mb/s para distintos tamaños de carga útil sobre la red *unicast* VPN IP/MPLS.

H_1: Existe una correlación entre el tiempo de permanencia en el sistema PE1 y el *jitter*, en la generación/recepción de tráfico *unicast* UDP con un *throughput*

[15] Las hipótesis son direccionales o bidireccionales (no direccionales). Las direccionales señalan la dirección de la diferencia, mientras que las bidireccionales no lo hacen. Por ejemplo el valor promedio del *jitter* es mayor al de la permanencia (hay una tendencia hacia qué variable se inclina la prueba de hipótesis).

nominal de 3 Mb/s para distintos tamaños de carga útil sobre la red *unicast* VPN IP/MPLS.

b.) Establecimiento del nivel de significancia: el nivel de significancia será del 5% = 0,05

c.) Generación de los resultados estadísticos: para ello se cuenta con el programa de estadística *SPSS Statistics* [16]. Los resultados se aprecian en la Tabla 3.5.

			CARGA_ÚTIL	JITTER	PERMANENCIA
Rho de Spearman	CARGA_ÚTIL	Coeficiente de correlación	1,000	1,000**	1,000**
		Sig. (bilateral)	.	.	.
		N	6	6	6
	JITTER	Coeficiente de correlación	1,000**	1,000	1,000**
		Sig. (bilateral)	.	.	.
		N	6	6	6
	PERMANENCIA	Coeficiente de correlación	1,000**	1,000**	1,000
		Sig. (bilateral)	.	.	.
		N	6	6	6

El punto "." indica un valor de *p* = 0,0

Tabla 3.5 Correlación de Spearman entre el tiempo de permanencia en el sistema PE1 y el *jitter* para *unicast* UDP a 3 Mb/s

d.) Valoración de *Rho* calculado entre la carga útil y el *jitter* = 1,000

Valor de *p* entre la carga útil y el *jitter* = 0,0

Valoración de *Rho* calculado entre la carga útil y el tiempo de permanencia en el sistema PE1 = 1,000

Valor de *p* entre la carga útil y el tiempo de permanencia en el sistema PE1 = 0,0

e.) Interpretación (dar como respuesta una de las hipótesis):

Ya que los valores de probabilidad *p* son menores que el nivel de significancia, en ambos casos, se rechaza la hipótesis nula y se acepta la alterna.

Por lo tanto, existe una correlación entre el tiempo de permanencia en el sistema PE1 y el *jitter*, en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 3 Mb/s para distintos tamaños de carga útil sobre la red *unicast* VPN IP/MPLS.

[16] Para mayor información ver el Anexo E "Manual de Análisis de Datos con SPSS STATISTICS".

f.) Interpretación del valor de *Rho* entre la carga útil y el *jitter*

1) 0,00 No existe correlación
2) De 0,01 a 0,19 Muy baja correlación positiva
3) De 0,20 a 0,39 Baja correlación positiva
4) De 0,40 a 0,59 Moderada correlación positiva
5) De 0,60 a 0,79 Buena correlación positiva
6) De 0,80 a 0,99 Muy buena correlación positiva
7) 1,00 Correlación perfecta positiva

g.) Interpretación del valor de *Rho* entre la carga útil y el tiempo de permanencia en el sistema PE1

1) 0,00 No existe correlación
2) De 0,01 a 0,19 Muy baja correlación positiva
3) De 0,20 a 0,39 Baja correlación positiva
4) De 0,40 a 0,59 Moderada correlación positiva
5) De 0,60 a 0,79 Buena correlación positiva
6) De 0,80 a 0,99 Muy buena correlación positiva
7) 1,00 Correlación perfecta positiva

h.) Conclusión:

Al obtener un valor de *Rho* de +1,00 entre la carga útil, el *jitter* y el tiempo de permanencia de un paquete en el sistema PE1 se concluye que existe una correlación positiva perfecta entre estas tres variables en el sistema *Router* PE1. En decir, si un paquete con mayor carga útil se transmite por la red *unicast* VPN IP/MPLS con un *throughput* nominal de 6 Mb/s (3 Mb/s por receptor), el tiempo de permanencia de un paquete en el sistema *Router* PE1 tenderá a incrementarse, así como también la variación del retardo.

3.2.3 INFERENCIA DE RESULTADOS

- La intensidad de tráfico permanece constante e igual a 0,75 para cualquier tamaño de carga útil experimental, si y solo si se transmite un paquete al mismo *throughput* nominal, es decir a 3 Mb/s por receptor.
- Mientras mayor es el número de paquetes con menor carga útil por unidad de tiempo, que arriban al sistema PE1 desde la fuente, dicho sistema empezará a descartar paquetes, ya que posee una capacidad finita de almacenamiento.

Esto genera un incremento en el porcentaje de la pérdida de paquetes (0% al 20,4%), aunque disminuya el tiempo de permanencia en el sistema PE1 (de 5611 us a 260 us).

- El tamaño de carga útil (64 B a 1400 B) se correlaciona directamente con la variación del retardo (140 us a 6826 us) y con el tiempo que un paquete permanece en el sistema PE1 (256 us a 5600 us), si y solo si el *throughput* nominal al que se transmite dicho paquete está por debajo del valor del enlace de "cuello de botella" (PE1 - P), es decir a 3 Mb/s por receptor, o el factor de intensidad de tráfico sea inferior a 1.

3.3 BATERÍA DE PRUEBAS 2

3.3.1 EXPERIMENTO

Generación de tráfico *unicast* UDP en la red IP/MPLS *unicast* VPN con un tamaño de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes, utilizando Jperf. El *throughput* nominal de la fuente es de 8 Mb/s (4 Mb/s por cada receptor). Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente, el número de paquetes recibidos y el porcentaje de pérdida de paquetes. La Tabla 3.6 indica los resultados estadísticos de la generación de tráfico *unicast* UDP para un tamaño de carga útil de 64 bytes a un *throughput* nominal de 4 Mb/s.

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2111	0,018	2945	7659	38,0
Máximo	2523	0,128	3535	7937	46,0
Media	2358,4	0,043	3198	7804,5	41,0
Mediana	2352	0,04	3212	7803	41,0
Desv. Est.	82,3	0,02	139,3	62,6	1,9

Tabla 3.6 Resultados estadísticos de la generación de tráfico *unicast* UDP para 64 bytes @ 4 Mb/s

3.3.2 PRESENTACIÓN DE RESULTADOS

La Tabla 3.7 describe los valores promedio de los parámetros de calidad de servicio para cada tipo de *payload: throughput*, *jitter*, paquetes generados por la fuente,

paquetes recibidos en los receptores y el porcentaje de pérdida de paquetes que existieron luego de la generación de tráfico *unicast* UDP a 4 Mb/s.

Payload [B]	*Throughput* [Kb/s]	*Jitter* [ms]	Paquetes generados [p/s]	Paquetes recibidos [p/s]	Tasa de pérdidas [%]
64	2358,4	0,043	7805	4606	41,0
128	2990,8	0,175	3906	2921	25,2
256	3445,8	0,564	1955	1680	14,1
512	3727,2	2,004	979	910	7,1
1024	3875,8	3,452	488	473	3,1
1400	3947,3	4,293	359	352	1,9

Tabla 3.7 Promedio de los resultados del experimento generación de tráfico *unicast* UDP @ 4 Mb/s para todos los tamaños de *payload*

Al calcular la intensidad de tráfico, se observó que ρ_{PE1} es igual a 1; por consiguiente, no se puede calcular las variables de tiempo *T* y *W* para el sistema PE1, ya que en teoría *T* tendería al infinito. La Tabla 3.8 muestra las tasas de arribo y salida, la intensidad de tráfico para PE1 y la comprobación del porcentaje de pérdida de paquetes para el tráfico *unicast* UDP a 4 Mb/s.

Por otro lado se planteó una prueba de hipótesis con el fin de saber si el tamaño de carga útil se relaciona con el incremento del *jitter* y con la disminución del porcentaje de pérdida de paquetes, como se observó en la Tabla 3.7. Este planteamiento no asevera que uno de los factores sea el causal del otro, ya que la correlación estadística no implica causalidad, sino el grado de unión y de dirección que hay entre las variables a indagar.

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	λ_P [p/s]	Pérdidas [%]
64	15609	15625	1,0	9212	41,0
128	7813	7813	1,0	5841	25,2
256	3910	3906	1,0	3365	13,9
512	1959	1953	1,0	1820	7,1
1024	977	977	1,0	946	3,1
1400	719	714	1,0	705	1,9

Tabla 3.8 Intensidad de tráfico para el sistema *Router* PE1 y porcentaje de pérdida de paquetes para todos los valores de *payload unicast* UDP @ 4 Mb/s

La Figura 3.4 muestra un gráfico de dispersión de datos entre las dos variables para todos los tamaños de carga útil. Nótese que la línea de tendencia central tiene una

pendiente negativa, lo que supone que el porcentaje de pérdida de paquetes y el *jitter* son inversamente proporcionales.

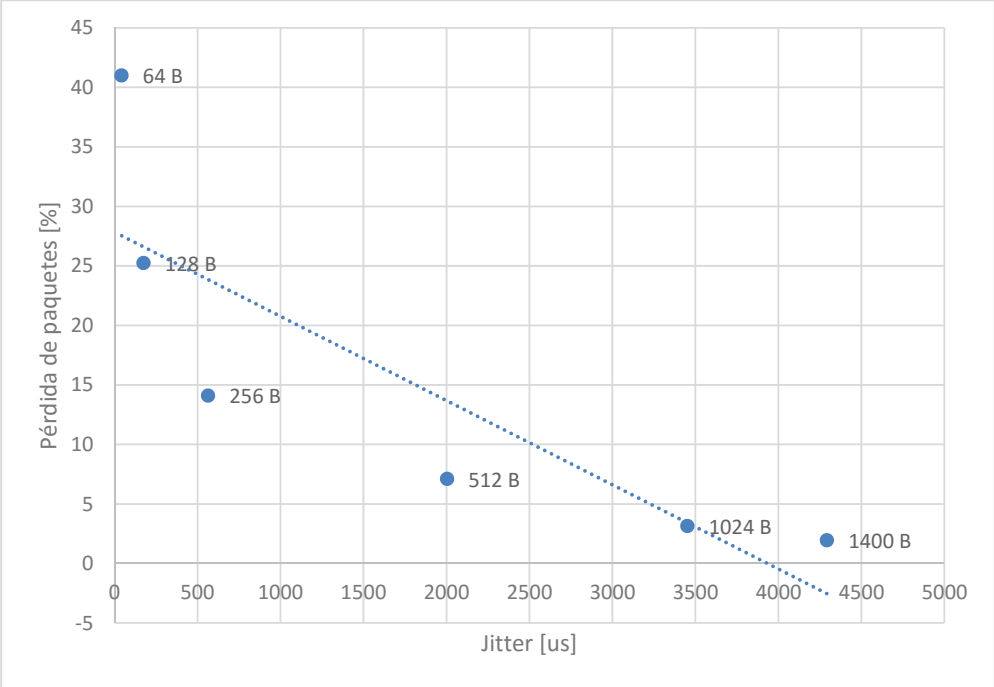

Figura 3.4 El *jitter* vs el porcentaje de pérdida de paquetes del tráfico *unicast* UDP @ 4 Mb/s

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1: se plantea una hipótesis alterna bidireccional

H_0: No existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 8 Mb/s (4 Mb/s por receptor) sobre la red *unicast* VPN IP/MPLS.

H_1: Existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 8 Mb/s (4 Mb/s por receptor) sobre la red *unicast* VPN IP/MPLS.

b.) Establecimiento del nivel de significancia: el nivel de significancia será del 5% = 0,05

c.) Generación de los resultados estadísticos: para ello se cuenta con el *software* de estadística *SPSS Statistics*. Los resultados se describen en la Tabla 3.9.

			CARGA_ÚTIL	JITTER	PÉRDIDA
Rho de Spearman	CARGA_ÚTIL	Coeficiente de correlación	1,000	1,000**	-1,000**
		Sig. (bilateral)	.	.	.
		N	6	6	6
	JITTER	Coeficiente de correlación	1,000**	1,000	-1,000**
		Sig. (bilateral)	.	.	.
		N	6	6	6
	PÉRDIDA	Coeficiente de correlación	-1,000**	-1,000**	1,000
		Sig. (bilateral)	.	.	.
		N	6	6	6

Tabla 3.9 Correlación de Spearman entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en el sistema PE1 para *unicast* UDP @ 4 Mb/s

d.) Valoración de *Rho* calculado entre la carga útil y el *jitter* = 1,000

Valor de *p* entre la carga útil y el *jitter* = 0,0.

Valoración de *Rho* calculado entre la carga útil y el porcentaje de pérdida de paquetes = -1,000

Valor de *p* entre la carga útil y el porcentaje de pérdida de paquetes = 0,0.

e.) Interpretación (dar como respuesta una de las hipótesis):

Como el valor de probabilidad *p* es menor que el nivel de significancia, en ambas situaciones, se rechaza la hipótesis nula y se acepta la alterna. Consecuentemente, existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 8 Mb/s (4 Mb/s por receptor) sobre la red *unicast* VPN IP/MPLS.

f.) Interpretación del valor de *Rho* entre la carga útil y el *jitter:* +1,00 Correlación perfecta positiva.

g.) Interpretación del valor de *Rho* entre la carga útil y el porcentaje de pérdida de paquetes: -1,00 Correlación perfecta negativa.

h.) Conclusión:

Al obtener un valor de *Rho* de +1,00 entre la carga útil y el *jitter* se concluye que existe una correlación positiva perfecta entre estas dos variables en el sistema PE1. Es decir, si se transmiten paquetes con cargas cada vez mayores por la

red *unicast* VPN IP/MPLS con un *throughput* nominal de 8 Mb/s (4 Mb/s por receptor), de la misma forma variará la variación del retardo.

Mientras que, al obtener un valor de *Rho* de -1,00 entre la carga útil y el porcentaje de pérdida de paquetes se concluye que existe una correlación negativa perfecta entre estas dos variables en el sistema PE1. Si se envían paquetes con cargas cada vez más grandes por la red *unicast* VPN IP/MPLS con un *throughput* nominal de 4 Mb/s por receptor, el porcentaje de pérdida de paquetes disminuirá.

3.3.3 INFERENCIA DE RESULTADOS

- La intensidad de tráfico permanece constante e igual a 1 para cualquier tamaño de carga útil experimental, si y solo si se transmite un paquete al mismo *throughput* nominal, es decir a 4 Mb/s por receptor. Esto produce que la intensidad de tráfico llegue a su valor máximo, es decir, la tasa de arribo y salida del sistema PE1 sean aproximadamente iguales.
- Mientras mayor es el número de paquetes con menor carga útil por unidad de tiempo, que arriban al sistema PE1, dicho sistema empezará a descartar paquetes debido a que posee una capacidad finita de almacenamiento, y generará un incremento en el porcentaje de pérdida de paquetes (1,9% a 41%).
- No se logró obtener el valor del tiempo de permanencia en el sistema PE1, debido a que la intensidad de tráfico fue igual a 1; por tanto se realizaron pruebas de hipótesis estadística con el fin de correlacionar el tamaño del *payload* con la variación del retardo y el porcentaje de pérdida de paquetes. Se determinó que existe un alto grado de correlación directa entre la variación del retardo (43 us a 4293 us) y el tamaño de carga útil (64 B a 1400 B); y de la misma manera, existe un alto grado de correlación inversa entre el porcentaje de pérdida de paquetes (41% a 1,9%) y el tamaño de carga útil (64 B a 1400 B).

3.4 BATERÍA DE PRUEBAS 3

3.4.1 EXPERIMENTO

Generación de tráfico *unicast* UDP, en la red IP/MPLS *unicast* VPN con un tamaño de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes,

utilizando Jperf. El *throughput* nominal de la fuente es de 10 Mb/s (5 Mb/s por cada receptor). Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente, el número de paquetes recibidos y el porcentaje de pérdida de paquetes. En la Tabla 3.10 se aprecian los resultados estadísticos de la generación de tráfico *unicast* UDP para un tamaño de carga útil de 64 bytes a un *throughput* nominal de 5 Mb/s.

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2268	0,03	4718	9639	48,0
Máximo	2597	1,046	5346	9974	55,0
Media	2403,9	0,241	5110	9804,7	52,1
Mediana	2391,5	0,109	5131	9791	52,5
Desv. Est.	76,3	0,26	154,9	64,4	1,6

Tabla 3.10 Resultados estadísticos de la generación de tráfico *unicast* UDP para 64 bytes @ 5 Mb/s

3.4.2 PRESENTACIÓN DE RESULTADOS

Se detalla en la Tabla 3.11, los valores promedio de los parámetros de calidad de servicio para cada tipo de *payload: throughput*, *jitter*, paquetes generados por la fuente, paquetes recibidos en los receptores y el porcentaje de pérdida de paquetes que existieron luego de la generación de tráfico *unicast* UDP a 5 Mb/s.

Al obtener ρ_{PE1}, se observó que el factor de intensidad de tráfico es mayor a 1; por ende, no se pueden calcular las variables de tiempo T, t_s y W para el sistema PE1. La Tabla 3.12 describe las tasas de arribo y salida, la intensidad de tráfico para PE1 y el porcentaje de pérdida de paquetes para el tráfico *unicast* UDP a 5 Mb/s.

Payload [B]	*Throughput* [Kb/s]	*Jitter* [ms]	Paquetes generados [p/s]	Paquetes recibidos [p/s]	Tasa de pérdidas [%]
64	2403,9	0,241	9805	4695	52,1
128	3008,3	0,59	4904	2942	40,1
256	3391,3	0,504	2445	1656	32,2
512	3723,7	1,775	1225	909	25,8
1024	3873,1	3,733	614	473	23,0
1400	3957,7	5,302	450	353	21,5

Tabla 3.11 Promedio de los resultados del experimento generación de tráfico *unicast* UDP @ 5 Mb/s para todos los tamaños de *Payload*

Se consideró plantear una prueba de hipótesis con el objetivo de conocer si el tamaño de carga útil se relaciona con un incremento en el *jitter* y una disminución en el porcentaje de pérdida de paquetes como se observó en la Tabla 3.11.

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	λ_P [p/s]	Pérdidas [%]
64	19609	15625	1,26	9390	52,1
128	9809	7813	1,26	5876	40,1
256	4890	3906	1,25	3312	32,3
512	2451	1953	1,25	1818	25,8
1024	1229	977	1,26	946	23,0
1400	900	714	1,26	707	21,5

Tabla 3.12 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de *payload unicast* UDP @ 5 Mb/s

La Figura 3.5 representa un gráfico de dispersión de datos entre estas tres variables a examinar para todos los tamaños de carga útil. Nótese que la línea de tendencia central tiene una pendiente negativa, lo que supone que el porcentaje de pérdida de paquetes y el *jitter* son inversamente proporcionales.

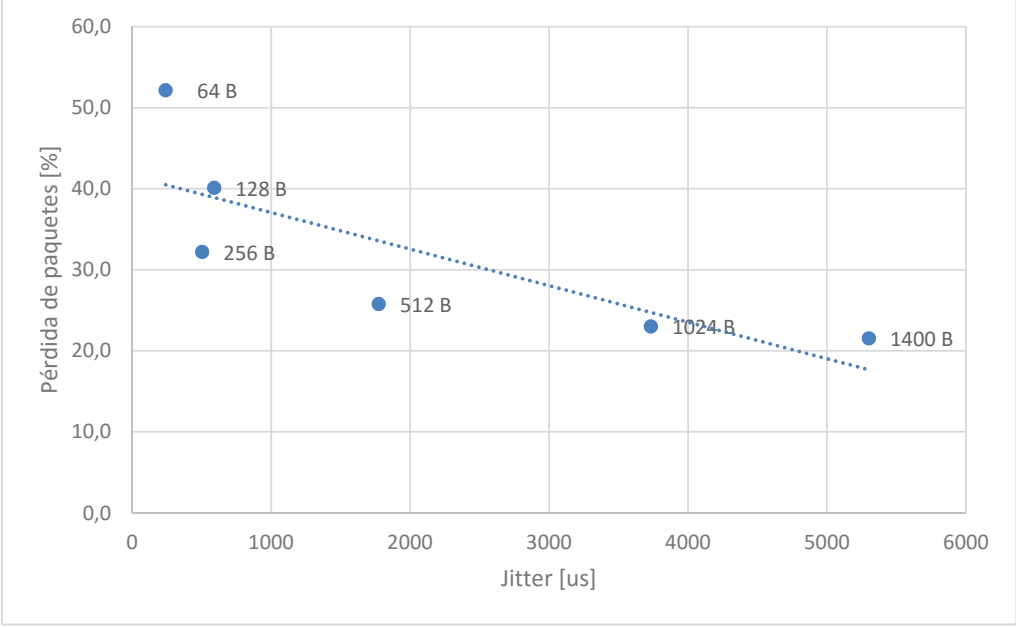

Figura 3.5 El *jitter* vs el porcentaje de pérdida de paquetes del tráfico *unicast* UDP @ 5 Mb/s

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1: se plantea una hipótesis alterna bidireccional

H_0: No existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 10 Mb/s (5 Mb/s por receptor) sobre la red *unicast* VPN IP/MPLS.

H_1: Existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 10 Mb/s (5 Mb/s por receptor) sobre la red *unicast* VPN IP/MPLS.

b.) Establecimiento del nivel de significancia: el nivel de significancia será del 5% = 0,05

c.) Generación de los resultados estadísticos: para ello se cuenta con el *software* de estadística *SPSS Statistics*. Los resultados se visualizan en la Tabla 3.13.

Correlaciones

			CARGA_ÚTIL	JITTER	PÉRDIDA
Rho de Spearman	CARGA_ÚTIL	Coeficiente de correlación	1,000	,943**	-1,000**
		Sig. (bilateral)	.	,005	.
		N	6	6	6
	JITTER	Coeficiente de correlación	,943**	1,000	-,943**
		Sig. (bilateral)	,005	.	,005
		N	6	6	6
	PÉRDIDA	Coeficiente de correlación	-1,000**	-,943**	1,000
		Sig. (bilateral)	.	,005	.
		N	6	6	6

Tabla 3.13 Correlación de Spearman entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en el sistema PE1 para *unicast* UDP @ 5 Mb/s

d.) Valoración de *Rho* calculado entre la carga útil y el *jitter* = 0,943

Valor de *p* entre la carga útil y el *jitter* = 0,005

Valoración de *Rho* calculado entre la carga útil y el porcentaje de pérdida de paquetes = -1,000

Valor de *p* entre la carga útil y el porcentaje de pérdida de paquetes = 0,0

e.) Interpretación (dar como respuesta una de las hipótesis):

Ya que el valor de probabilidad *p* es menor que el nivel de significancia, en ambos casos, se rechaza la hipótesis nula y se acepta la alterna.

Existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *unicast* UDP con un *throughput* nominal de 10 Mb/s (5 Mb/s por receptor) sobre la red *unicast* VPN IP/MPLS.

f.) Interpretación del valor de *Rho* entre la carga útil y el *jitter:* de 0,80 a 0,99 Muy buena correlación positiva.

g.) Interpretación del valor de *Rho* entre la carga útil y el porcentaje de pérdida de paquetes: -1,00 Correlación perfecta negativa.

h.) Conclusión:

Al obtener un valor de *Rho* de +0,943 entre la carga útil y el *jitter* se concluye que existe una muy buena correlación positiva entre estas dos variables en el sistema PE1. En otras palabras, si un paquete con mayor carga útil se transmite por la red *unicast* VPN IP/MPLS con un *throughput* nominal de 5 Mb/s por receptor, asimismo se incrementará la variación del retardo.

Mientras que, al obtener un valor de *Rho* de -1,00 entre la carga útil y el porcentaje de pérdida de paquetes se concluye que existe una correlación negativa perfecta entre estas dos variables en el sistema PE1. Si un paquete con mayor carga útil se envía por la red *unicast* VPN IP/MPLS con un *throughput* nominal de 5 Mb/s por receptor, el porcentaje de pérdida de paquetes disminuirá.

3.4.3 INFERENCIA DE RESULTADOS

- La intensidad de tráfico permanece cerca al 1,26 para cualquier tamaño de carga útil experimental, si y solo si se transmite un paquete al mismo *throughput* nominal, es decir a 5 Mb/s por receptor. Esto significa que la intensidad de tráfico sobrepasa su valor máximo, es decir, la tasa de arribo es mayor a la de salida del sistema PE1.

- Mientras mayor es el número de paquetes con menor carga útil por unidad de tiempo, que arriban al sistema PE1, dicho sistema empezará a descartar paquetes debido a que posee una capacidad finita de almacenamiento, y generará un incremento en el porcentaje de pérdida de paquetes (21,5% a 52,1%).

- No se logró obtener el valor del tiempo de permanencia en el sistema PE1, debido a que la intensidad de tráfico fue mayor a 1; por tanto se realizaron pruebas de hipótesis estadística con el fin de correlacionar el tamaño del *payload* con la variación del retardo y el porcentaje de pérdida de paquetes. Se determinó que existe un alto grado de correlación directa entre la variación del retardo (241 us a 5302 us) y el tamaño de carga útil (64 B a 1400 B); y de la misma manera, existe un alto grado de correlación inversa entre el porcentaje de pérdida de paquetes (52,1% a 21,5%) y el tamaño de carga útil (64 B a 1400 B).

3.5 BATERÍA DE PRUEBAS 4

3.5.1 EXPERIMENTO

Generación de tráfico *unicast* TCP en la red IP/MPLS *unicast* VPN con un tamaño de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes, utilizando Jperf.

El *throughput* nominal lo determina automáticamente el *software*. Los parámetros a medir en cada receptor son el *throughput*, el número de paquetes generados por la fuente y el número de paquetes recibidos.

La Tabla 3.14 ilustra el promedio de los resultados de la generación de tráfico *unicast* TCP para todos los tamaños de carga útil.

Payload	Tamaño [KB]	*Throughput* [Kb/s]	Paquetes generados	Paquetes recibidos
64 bytes	48634	3984	779	760
128 bytes	49727	4000	398	389
256 bytes	48600	3981	195	190
512 bytes	49820	4000	100	94
1024 bytes	48408	3965	49	48
1400 bytes	48088	3939	36	35

Tabla 3.14 Promedio de los resultados de la generación de tráfico *unicast* TCP

3.5.2 PRESENTACIÓN DE RESULTADOS

La Tabla 3.15 muestra las tasas de arribo, salida y la intensidad de tráfico para PE1 correspondiente al tráfico *unicast* TCP. Luego del cálculo del factor de intensidad

de tráfico, se apreció que ρ_{PE1} es menor a 1; por lo tanto, se pueden calcular las variables de tiempo *T,* t_s y *W* para el sistema PE1. La Tabla 3.16 detalla dichos tiempos.

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}
64	1558	15625	0,1
128	796	7813	0,1
256	390	3906	0,1
512	200	1953	0,1
1024	98	977	0,1
1400	72	714	0,1

Tabla 3.15 Factor de intensidad de tráfico para el sistema *Router* PE1 para todos los valores de *payload* en *unicast* TCP

Payload [B]	ts_{PE1} [us]	W_{PE1} [us]	T_{PE1} [us]
64	64	7	71
128	128	14	142
256	256	28	284
512	512	57	569
1024	1024	114	1138
1400	1400	156	1556

Tabla 3.16 Retardos de servicio, de espera en la cola, y de permanencia en el sistema *Router* PE1 para todos los valores de *payload* en *unicast* TCP

3.5.3 INFERENCIA DE RESULTADOS

- El control de flujo, característico de TCP, evitó que la fuente transmita o envíe datos, de una manera más rápida, de la que el receptor o *host* puede recibirlos y procesarlos [42]. Por ello el *throughput* nominal se mantuvo cercano a los 4 Mb/s, a pesar de utilizar distintos tamaños de carga útil.

- Asimismo, el control de congestión es un mecanismo utilizado por la red para limitar la congestión, que en este caso, es ocasionada por el "cuello de botella" formado entre los *routers* PE1 y P. Esto conllevó a que la intensidad de tráfico tienda a 0,1 en el punto más crítico de la red IP /MPLS que es el sistema PE1.

- A mayor número de paquetes con menor carga útil por unidad de tiempo que arriban al sistema, disminuye el tiempo de permanencia en el sistema PE1 (1556 us a 71 us).

3.6 BATERÍA DE PRUEBAS 5

3.6.1 EXPERIMENTO

Generación de tráfico *multicast* en la red IP/MPLS *multicast* VPN con un tamaño de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes, utilizando Jperf. El *throughput* nominal es de 6 Mb/s. Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente, el número de paquetes recibidos y el porcentaje de pérdida de paquetes. La Tabla 3.17 muestra los resultados estadísticos de la generación de tráfico *multicast* para un tamaño de carga útil de 64 bytes y un *throughput* nominal de 6 Mb/s.

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	4151	0,042	3617	11743	31,0
Máximo	4226	0,252	3683	11930	31,0
Media	4166,9	0,09	3632	11770,7	31,0
Mediana	4158,5	0,05	3627	11746	31,0
Desv. Est.	22,97	0,07	19,7	63,4	0,0

Tabla 3.17 Resultados estadísticos de la generación de tráfico *multicast* para 64 bytes @ 6 Mb/s

3.6.2 PRESENTACIÓN DE RESULTADOS

La Tabla 3.18 proporciona los valores promedio de los parámetros de calidad de servicio para cada tipo de *payload,* como son el *throughput*, el *jitter*, los paquetes generados por la fuente, los paquetes recibidos en los receptores y el porcentaje de pérdida de paquetes que existieron luego de la generación de tráfico *multicast* a 6 Mb/s.

Se consideran los datos de la carga útil de 64 bytes para efectuar el análisis. Desde el punto de vista de la fuente *multicast*, ésta genera una sola emisión, es decir, los *hosts* pertenecientes al grupo *multicast* recibirán el mismo contenido, por lo cual no se multiplica por 2 al *throughput* (paquetes/s) que arriban al sistema PE1 y que constituye el valor de $\lambda_{PE1.}$

$$\lambda_{PE1} = 11771 \left[\frac{paquete}{s}\right]$$

Payload [B]	*Throughput* [Kb/s]	*Jitter* [ms]	Paquetes generados [p/s]	Paquetes recibidos [p/s]	Tasa de pérdidas [%]
64	4166,9	0,09	11771	8139	31,0
128	5491,8	0,827	5885	5363	8,9
256	6009	0,235	2934	2934	0,0
512	6000	0,809	1467	1465	0,2
1024	5966,8	1,896	733	728	0,6
1400	5973,7	3,177	536	533	0,6

Tabla 3.18 Promedio de los resultados del experimento generación de tráfico *multicast* @ 6 Mb/s para todos los tamaños de *payload*

Luego se obtiene el valor de μ_{PE1} a partir de la Ecuación 3.2, sabiendo que el enlace de salida corresponde al "cuello de botella" de valor 8 Mb/s (comprendido entre los *routers* PE1 y P).

$$\mu_{PE1} = \frac{R}{L} = \frac{8\left[\frac{Mbits}{s}\right] x \frac{10^6\ [bits]}{1\ [Mbit]}}{64\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow \mu_{PE1} = 15625\ \left[\frac{paquete}{s}\right]$$

Para hallar la intensidad de tráfico del sistema PE1, es necesario dividir ambos resultados anteriores. Si ρ_{PE1} es menor que 1, se pueden calcular las variables de tiempo *T,* t_s y *W* para el sistema PE1.

$$\rho_{PE1} = \frac{\lambda_{PE1}}{\mu_{PE1}} = \frac{11771\left[\frac{paquete}{s}\right]}{15625\left[\frac{paquete}{s}\right]} \Rightarrow \rho_{PE1} = 0{,}75$$

Después de haber atravesado el "cuello de botella", el *throughput* nominal del paquete que fue enviado desde la fuente, decrementó de 6000 Kb/s a 4166,9 Kb/s. Así como sucedió con λ_{PE1}, no se multiplica por 2 al *throughput* de la tasa de arribo de paquetes al sistema P (λ_P), ya que la fuente *multicast* genera una única emisión. Mediante la Ecuación 3.7 se halla la variable λ_P.

$$\lambda_P = \frac{throughput}{L} = \frac{4166{,}9\left[\frac{Kb}{s}\right]\ x\ \frac{1000\ [bits]}{1\ [Kb]}}{64\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow \lambda_P = 8138{,}5\ \left[\frac{paquete}{s}\right]$$

De la misma forma se encuentra el valor de μ_P a través de la Ecuación 3.2.

$$\mu_P = \frac{R}{L} = \frac{1\left[\frac{Gbit}{s}\right] x \frac{10^9\ [bits]}{1\ [Gbit]}}{64\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow \mu_P = 1953125\ \left[\frac{paquete}{s}\right]$$

Finalmente se calcula el valor de ρ_P.

$$\rho_P = \frac{\lambda_P}{\mu_P} = \frac{8138{,}5\left[\frac{paquete}{s}\right]}{1953125\left[\frac{paquete}{s}\right]} \Rightarrow \rho_P = 0{,}0042$$

La Tabla 3.19 muestra las tasas de arribo y de salida de los sistemas PE1 y P, así como la comprobación del porcentaje de pérdidas de paquetes frente a los datos obtenidos en la generación de tráfico *multicast* para todos los tamaños de carga útil vistos.

Se observa en este tabulado 3.19 que la intensidad de tráfico para cualquier valor de *payload* en el sistema PE1 es constante e igual a 0,75, como sucedió en *unicast* UDP @ 3 Mb/s.

$$Relación\ pérdida\ de\ paquetes = 1 - \frac{\lambda_P}{\lambda_{PE1}} = 0{,}309 = 30{,}9\%$$

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	λ_P [p/s]	Pérdidas [%]
64	11771	15625	0,75	8138,5	30,9
128	5885	7812,5	0,75	5363,1	8,9
256	2934	3906,3	0,75	2934,1	0,0
512	1467	1953,1	0,75	1464,8	0,1
1024	733	976,6	0,75	728,4	0,6
1400	536	714,3	0,75	533,4	0,6

Tabla 3.19 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de *payload* en *multicast* @ 6 Mb/s

A partir de la intensidad de tráfico de PE1 se calculan los valores del tiempo de servicio ts_{PE1}, el tiempo de permanencia en el sistema T_{PE1}, y el tiempo promedio de espera en la cola W_{PE1}. Estos datos se muestran en detalle en la Tabla 3.20.

$$ts_{PE1} = \frac{1}{\mu_{PE1}} = \frac{1}{15625\left[\frac{paquete}{s}\right]} \Rightarrow ts_{PE1} = 64\ [us]$$

$$T_{PE1} = \frac{\frac{1}{\mu_{PE1}}}{1 - \rho_{PE1}} = \frac{\frac{1}{15625\left[\frac{paquete}{s}\right]}}{1 - 0{,}75} \Rightarrow T_{PE1} = 256\ [us]$$

$$W_{PE1} = T_{PE1} - ts_{PE1} = 256\ [us] - 64\ [us] \Rightarrow W_{PE1} = 192\ [us]$$

Ya que T_{PE1} es un retardo importante por ser una consecuencia del "cuello de botella", en relación al resto de 'sistemas *Routers*' de la red, se optó por comprobar si el tiempo promedio que un paquete permanece en el sistema PE1 (Tabla 3.20) incide o mantiene una correlación estadística con el *jitter* (Tabla 3.18), para todos los tamaños de *payload,* mediante una prueba de hipótesis.

Payload [B]	ts_{PE1} [us]	W_{PE1} [us]	T_{PE1} [us]
64	64	192	256
128	128	384	512
256	256	768	1024
512	512	1536	2048
1024	1024	3072	4096
1400	1400	4200	5600

Tabla 3.20 Retardos de servicio, de espera en la cola, y de permanencia en el sistema PE1 para todos los valores de *payload* en *multicast* @ 6 Mb/s

La Figura 3.6 muestra un gráfico de dispersión de datos entre estas dos variables a examinar para todos los tamaños de carga útil. Nótese que la línea de tendencia central tiene una pendiente positiva, lo que supone que el tiempo de permanencia en el sistema PE1 y el *jitter* son directamente proporcionales.

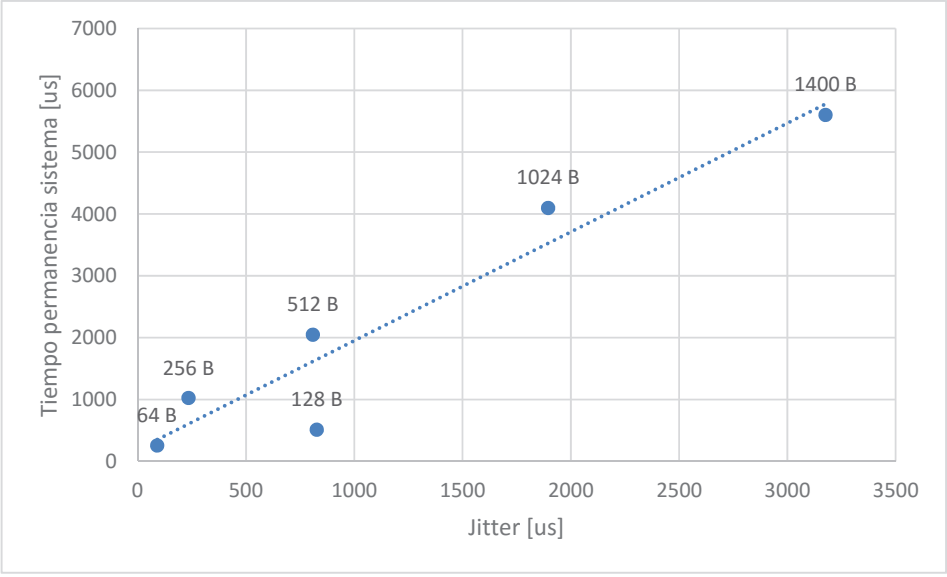

Figura 3.6 Tiempo de permanencia en el sistema vs el *jitter* del tráfico *multicast* @ 6 Mb/s

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1: se plantea una hipótesis alterna bidireccional

H_0: No existe una correlación entre el tiempo de permanencia en el sistema PE1 y el *jitter*, en la generación/recepción de tráfico *multicast,* con un *throughput* nominal de 6 Mb/s para distintos tamaños de carga útil sobre la red MVPN IP/MPLS.

H_1: Existe una correlación entre el tiempo de permanencia en el sistema PE1 y el *jitter*, en la generación/recepción de tráfico *multicast,* con un *throughput* nominal de 6 Mb/s para distintos tamaños de carga útil sobre la red MVPN IP/MPLS.

b.) Establecimiento del nivel de significancia: el nivel de significancia será del 5% = 0,05

c.) Generación de los resultados estadísticos: para ello se cuenta con el programa de estadística *SPSS Statistics*. Los resultados se aprecian en la Tabla 3.21.

d.) Valoración de *Rho* calculado entre la carga útil y el *jitter* = 0,829

Valor de *p* entre la carga útil y el *jitter* = 0,042

Valoración de *Rho* calculado entre la carga útil y el tiempo de permanencia en el sistema PE1 = 1,000

Valor de *p* entre la carga útil y el tiempo de permanencia en el sistema PE1= 0,0

Correlaciones

			CARGA_ÚTIL	JITTER	PERMANENCIA
Rho de Spearman	CARGA_ÚTIL	Coeficiente de correlación	1,000	,829*	1,000**
		Sig. (bilateral)	.	,042	.
		N	6	6	6
	JITTER	Coeficiente de correlación	,829*	1,000	,829*
		Sig. (bilateral)	,042	.	,042
		N	6	6	6
	PERMANENCIA	Coeficiente de correlación	1,000**	,829*	1,000
		Sig. (bilateral)	.	,042	.
		N	6	6	6

Tabla 3.21 Correlación de Spearman entre el tiempo de permanencia en el sistema PE1 y el *jitter* para *multicast* @ 6 Mb/s

d.) Interpretación (dar como respuesta una de las hipótesis):

Ya que los valores de probabilidad *p* son menores que el nivel de significancia, en ambos casos, se rechaza la hipótesis nula y se acepta la alterna.

Por lo tanto, existe una correlación entre el tiempo de permanencia en el sistema PE1 y el *jitter*, en la generación/recepción de tráfico *multicast,* con un *throughput* nominal de 6 Mb/s para distintos tamaños de carga útil sobre la red *M*VPN IP/MPLS.

e.) Interpretación del valor de *Rho* entre la carga útil y el *jitter:* De 0,80 a 0,99 Muy buena correlación positiva

f.) Interpretación del valor de *Rho* entre la carga útil y el tiempo de permanencia en el sistema PE1: 1,00 Correlación perfecta positiva

g.) Conclusión:

Por un lado, al obtener un valor de *Rho* de +0,829 entre la carga útil y el *jitter* se concluye que existe una muy buena correlación positiva entre estas dos variables en el sistema PE1. Es decir, si un paquete con mayor carga útil se transmite por la red MVPN IP/MPLS con un *throughput* nominal de 6 Mb/s, habrá una mayor variación del retardo.

Por otro lado, al obtener un valor de *Rho* de +1,00 entre la carga útil y el tiempo de permanencia de un paquete en el sistema PE1 se concluye que existe una correlación positiva perfecta entre estas dos variables en el sistema PE1. Si un paquete con mayor carga útil se envía por la red MVPN IP/MPLS con un *throughput* nominal de 6 Mb/s, el tiempo de permanencia de un paquete en el sistema PE1 se incrementará.

3.6.3 INFERENCIA DE RESULTADOS

- La intensidad de tráfico permanece constante e igual a 0,75 para cualquier tamaño de carga útil experimental, si y solo si se transmite un paquete al mismo *throughput* nominal, es decir a 6 Mb/s.
- Mientras mayor es el número de paquetes con menor carga útil por unidad de tiempo, que llegan al sistema PE1 desde la fuente, dicho sistema empezará a descartar paquetes, ya que posee una capacidad finita de almacenamiento. Esto genera un incremento en el porcentaje de pérdida de paquetes (0,6% al

31%), aunque sí disminuya el tiempo de permanencia en el sistema PE1 (de 5600 us a 256 us).

- El tamaño de carga útil (64 B a 1400 B) se correlaciona directamente con la variación del retardo (90 us a 3177 us) y el tiempo que un paquete permanece en el sistema PE1 (256 us a 5600 us), si y solo si el *throughput* nominal al que se transmite dicho paquete está por debajo del valor del enlace de "cuello de botella" (PE1 - P), es decir a 6 Mb/s, o el factor de intensidad de tráfico sea inferior a 1.

3.7 BATERÍA DE PRUEBAS 6

3.7.1 EXPERIMENTO

Generación de tráfico *multicast* en la red IP/MPLS *multicast* VPN con un tamaño de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes, utilizando Jperf. El *throughput* nominal es de 8 Mb/s. Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente, el número de paquetes recibidos y el porcentaje de pérdida de paquetes. La Tabla 3.22 ilustra los resultados estadísticos de la generación de tráfico *multicast* para un tamaño de carga útil de 64 bytes y un *throughput* nominal de 8 Mb/s.

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	4036	0,002	7479	15595	48,00
Máximo	4222	0,019	7720	15845	49,00
Media	4160	0,008	7507,7	15633	48,03
Mediana	4156	0,005	7483	15601	48,00
Desv. Est.	31,04	0,01	61,6	84,3	0,18

Tabla 3.22 Resultados estadísticos de la generación de tráfico *multicast* para 64 bytes @ 8 Mb/s

3.7.2 PRESENTACIÓN DE RESULTADOS

La Tabla 3.23 describe los valores promedio de los parámetros de calidad de servicio para cada tipo de *payload: throughput*, *jitter*, paquetes generados por la fuente, paquetes recibidos en los receptores y el porcentaje de pérdida de paquetes que existieron luego de la generación de tráfico *multicast* a 8 Mb/s.

Payload [B]	*Throughput* [Kb/s]	*Jitter* [ms]	Paquetes generados [p/s]	Paquetes recibidos [p/s]	Tasa de pérdidas [%]
64	4159,8	0,008	15633	8125	48,1
128	5479,9	0,272	7816	5351	31,3
256	6532,1	0,804	3908	3190	18,1
512	7210,1	0,674	1954	1760	9,9
1024	7622,1	2,010	977	930	4,8
1400	7735,6	2,613	715	691	3,4

Tabla 3.23 Promedio de los resultados del experimento generación de tráfico *multicast* @ 8 Mb/s para todos los tamaños de *payload*

Al calcular la intensidad de tráfico, se observó que ρ_{PE1} es igual a 1; por tanto, no se pueden calcular las variables de tiempo T, t_s y W para el sistema PE1, ya que en teoría T tendería al infinito. La Tabla 3.24 muestra las tasas de arribo y salida, el factor de intensidad de tráfico para PE1 y la comprobación del porcentaje de pérdida de paquetes para el tráfico *multicast* a 8 Mb/s.

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	λ_P [p/s]	Pérdidas [%]
64	15633	15625	1,00	8124,7	48,0
128	7816	7812,5	1,00	5351,4	31,5
256	3908	3906,3	1,00	3189,5	18,4
512	1954	1953,1	1,00	1760,3	9,9
1024	977	976,6	1,00	930,4	4,8
1400	715	714,3	1,00	690,7	3,3

Tabla 3.24 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de *payload* en *multicast* @ 8 Mb/s

Por otro lado se planteó una prueba de hipótesis con el fin de saber si el tamaño de carga útil se relaciona con un incremento en el *jitter* y una disminución en el porcentaje de pérdida de paquetes, como se observó en la Tabla 3.23.

La Figura 3.7 muestra un gráfico de dispersión de datos entre estas las dos variables a examinar para todos los tamaños de carga útil. Nótese que la línea de tendencia central tiene una pendiente negativa, lo que presume que el porcentaje de pérdida de paquetes y el *jitter* son inversamente proporcionales.

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1: se plantea una hipótesis alterna bidireccional

H_0: No existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *multicast* con un *throughput* nominal de 8 Mb/s sobre la red MVPN IP/MPLS.

H_1: Existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *multicast* con un *throughput* nominal de 8 Mb/s sobre la red MVPN IP/MPLS.

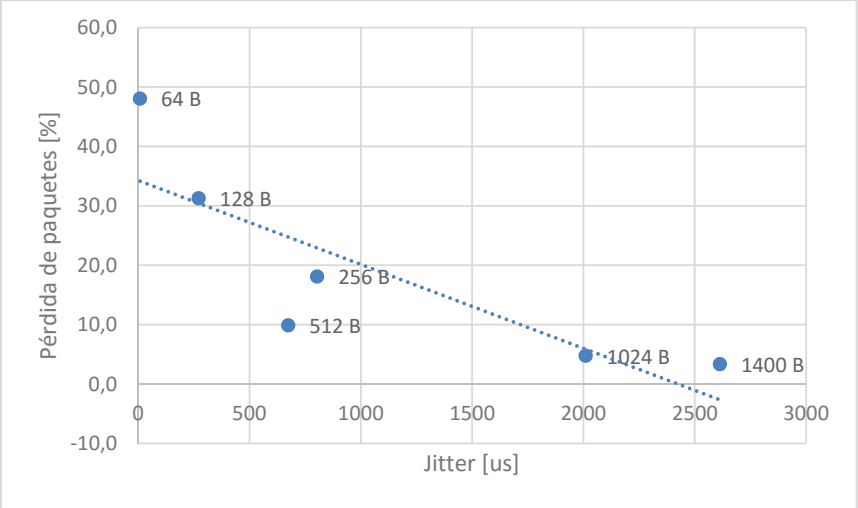

Figura 3.7 El *jitter* vs el porcentaje de pérdida de paquetes del tráfico *multicast* @ 8 Mb/s

b.) Establecimiento del nivel de significancia: el nivel de significancia será del 5% = 0,05

c.) Generación de los resultados estadísticos: para ello se cuenta con el *software* de estadística *SPSS Statistics*. Los resultados se describen en la Tabla 3.25.

			CARGA_ÚTIL	JITTER	PÉRDIDA
Rho de Spearman	CARGA_ÚTIL	Coeficiente de correlación	1,000	,943**	-1,000**
		Sig. (bilateral)	.	,005	.
		N	6	6	6
	JITTER	Coeficiente de correlación	,943**	1,000	-,943**
		Sig. (bilateral)	,005	.	,005
		N	6	6	6
	PÉRDIDA	Coeficiente de correlación	-1,000**	-,943**	1,000
		Sig. (bilateral)	.	,005	.
		N	6	6	6

Tabla 3.25 Correlación de Spearman entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en el sistema PE1 para *multicast* @ 8 Mb/s

d.) Valoración de *Rho* calculado entre la carga útil y el *jitter* = 0,943

Valor de *p* entre la carga útil y el *jitter* = 0,005

Valoración de *Rho* calculado entre la carga útil y el porcentaje de pérdida de paquetes = -1,000

Valor de *p* entre la carga útil y el porcentaje de pérdida de paquetes = 0,0.

e.) Interpretación (dar como respuesta una de las hipótesis):

Como el valor de probabilidad *p* es menor que el nivel de significancia, en ambas situaciones, se rechaza la hipótesis nula y se acepta la alterna. En consecuencia, existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *multicast* con un *throughput* nominal de 8 Mb/s sobre la red MVPN IP/MPLS.

f.) Interpretación del valor de *Rho* entre la carga útil y el *jitter:* de 0,80 a 0,99 Muy buena correlación positiva

g.) Interpretación del valor de *Rho* entre la carga útil y el porcentaje de pérdida de paquetes: -1,00 Correlación perfecta negativa

h.) Conclusión:

Al obtener un valor de *Rho* de +0,943 entre la carga útil y el *jitter* se concluye que existe una muy buena correlación positiva entre estas dos variables en el sistema PE1. Es decir, si se transmiten paquetes con cargas cada vez mayores por la red MVPN IP/MPLS con un *throughput* nominal de 8 Mb/s, también aumentará, en la misma proporción, la variación del retardo.

Mientras que, al obtener un valor de *Rho* de -1,00 entre la carga útil y el porcentaje de pérdida de paquetes se concluye que existe una correlación negativa perfecta entre estas dos variables en el sistema *Router* PE1. Si un paquete con mayor carga útil se transmite por la red MVPN IP/MPLS con un *throughput* nominal de 8 Mb/s, el porcentaje de pérdida de paquetes disminuirá.

3.7.3 INFERENCIA DE RESULTADOS

- La intensidad de tráfico permanece constante e igual a 1 para cualquier tamaño de carga útil experimental, si y solo si se transmite un paquete al mismo *throughput* nominal, es decir a 8 Mb/s. Esto produce que la intensidad de tráfico

llegue a su valor máximo, es decir, la tasa de arribo y salida del sistema PE1 son aproximadamente iguales.

- Mientras mayor es el número de paquetes con menor carga útil por unidad de tiempo, que arriban al sistema PE1, dicho sistema empezará a descartar paquetes debido a que posee una capacidad finita de almacenamiento, y generará un incremento en el porcentaje de pérdida de paquetes (3,3% a 48,0%).
- No se logró obtener el valor del tiempo de permanencia en el sistema PE1, debido a que la intensidad de tráfico fue igual a 1; por tanto se realizaron pruebas de hipótesis estadística con el fin de correlacionar el tamaño del *payload* con la variación del retardo y el porcentaje de pérdida de paquetes. Se determinó que existe un alto grado de correlación directa entre la variación del retardo (8 us a 2613 us) y el tamaño de carga útil (64 B a 1400 B); y de la misma manera, existe un alto grado de correlación inversa entre el porcentaje de pérdida de paquetes (48,0% a 3,3%) y el tamaño de carga útil (64 B a 1400 B).

3.8 BATERÍA DE PRUEBAS 7

3.8.1 EXPERIMENTO

Generación de tráfico *multicast* en la red IP/MPLS *multicast* VPN con un tamaño de carga útil de 64 bytes, 128 bytes, 256 bytes, 512 bytes, 1024 bytes y 1400 bytes, utilizando Jperf. El *throughput* nominal es de 10 Mb/s. Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente, el número de paquetes recibidos y el porcentaje de pérdida de paquetes. La Tabla 3.26 muestra los resultados estadísticos de la generación de tráfico *multicast* para un tamaño de carga útil de 64 bytes a un *throughput* nominal de 10 Mb/s.

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	4157	0	11445	19567	58,0
Máximo	4227	0,007	11635	19891	59,0
Media	4169	0,003	11476,6	19618	58,5
Mediana	4160	0,003	11454	19577	58,0
Desv. Est.	23,2	0,002	61,8	106,7	0,51

Tabla 3.26 Resultados estadísticos de la generación de tráfico *multicast* para 64 bytes @ 10 Mb/s

3.8.2 PRESENTACIÓN DE RESULTADOS

Se detalla en la Tabla 3.27, los valores promedio de los parámetros de calidad de servicio para cada tipo de *payload: throughput*, *jitter*, paquetes generados por la fuente, paquetes recibidos en los receptores y el porcentaje de pérdida de paquetes que existieron luego de la generación de tráfico *multicast* a 10 Mb/s.

Al obtener ρ_{PE1}, se observó que la intensidad de tráfico es mayor a 1; por ende, no se pueden calcular las variables de tiempo T, t_s y W para el sistema PE. La Tabla 3.28 describe las tasas de arribo y salida, la intensidad de tráfico para PE1 y la verificación del porcentaje de pérdida de paquetes para el tráfico *multicast* a 10 Mb/s.

Payload [B]	*Throughput* [Kb/s]	*Jitter* [ms]	Paquetes generados [p/s]	Paquetes recibidos [p/s]	Tasa de pérdidas [%]
64	4168,6	0,003	19620	8142	58,5
128	5490,2	0,013	9816	5364	45,1
256	6494,1	0,232	4904	3171	35,4
512	7206,6	0,658	2446	1759	28,1
1024	7534,4	2,070	1221	920	24,7
1400	7684,8	2,522	893	686	23,4

Tabla 3.27 Promedio de los resultados del experimento generación de tráfico *multicast* @ 10 Mb/s para todos los tamaños de *payload*

Payload [B]	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	λ_P [p/s]	Pérdidas [%]
64	19620	15625	1,26	8141,8	58,5
128	9816	7812,5	1,26	5361,6	45,4
256	4904	3906,3	1,26	3170,9	35,3
512	2446	1953,1	1,25	1759,4	28,1
1024	1221	976,6	1,25	919,7	24,7
1400	893	714,3	1,25	686,1	23,2

Tabla 3.28 Intensidad de tráfico para el sistema PE1 y porcentaje de pérdida de paquetes para todos los valores de *payload* en *multicast* a 10 Mb/s

Se consideró plantear una prueba de hipótesis con el objetivo de conocer si el tamaño de carga útil se relaciona con un incremento en el *jitter* y una disminución en el porcentaje de pérdida de paquetes como se observó en la Tabla 3.27.

La Figura 3.8 representa un gráfico de dispersión de datos entre estas tres variables a examinar para todos los tamaños de carga útil. Nótese que la línea de tendencia

central tiene una pendiente negativa, lo que presume que el porcentaje de pérdida de paquetes y el *jitter* son inversamente proporcionales.

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1: se plantea una hipótesis alterna bidireccional

H_0: No existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *multicast* con un *throughput* nominal de 10 Mb/s sobre la red MVPN IP/MPLS.

H_1: Existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *multicast* con un *throughput* nominal de 10 Mb/s sobre la red MVPN IP/MPLS.

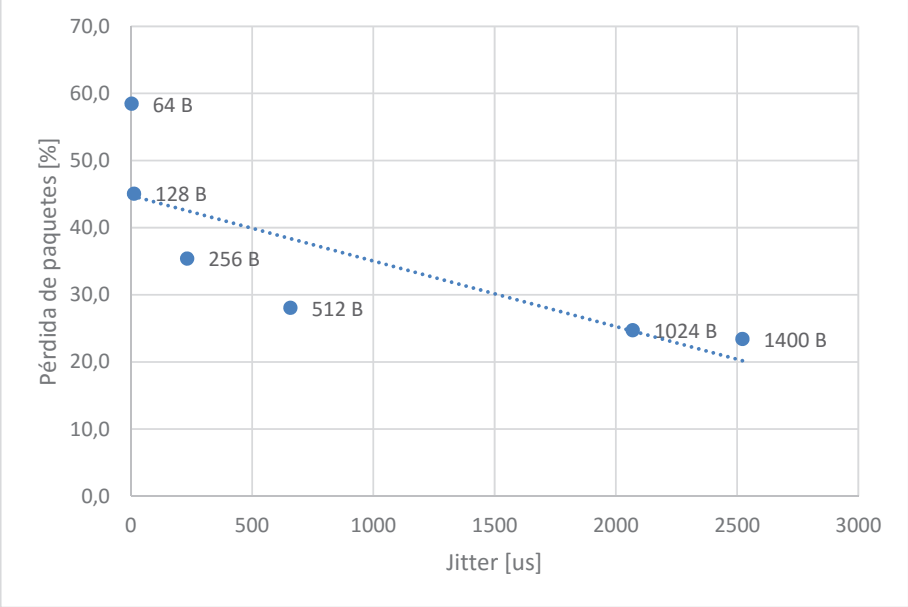

Figura 3.8 El *jitter* vs el porcentaje de pérdida de paquetes del tráfico *multicast* @ 10 Mb/s

b.) Establecimiento del nivel de significancia: el nivel de significancia será del 5% = 0,05

c.) Generación de los resultados estadísticos: para ello se cuenta con el *software* de estadística *SPSS Statistics*. Los resultados se visualizan en la Tabla 3.29.

d.) Valoración de *Rho* calculado entre la carga útil y el *jitter* = 1,000

Valor de *p* entre la carga útil y el *jitter* = 0,0

Valoración de *Rho* calculado entre la carga útil y el porcentaje de pérdida de paquetes = -1,000

Valor de *p* entre la carga útil y el porcentaje de pérdida de paquetes = 0,0.

e.) Interpretación (dar como respuesta una de las hipótesis):

Como el valor de probabilidad *p* es menor que el nivel de significancia, en ambas situaciones, se rechaza la hipótesis nula y se acepta la alterna. Por tanto, existe una correlación entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en la generación/recepción de tráfico *multicast* con un *throughput* nominal de 10 Mb/s sobre la red MVPN IP/MPLS.

f.) Interpretación del valor de *Rho* entre la carga útil y el *jitter:* 1,00 Correlación perfecta positiva

g.) Interpretación del valor de *Rho* entre la carga útil y el porcentaje de pérdida de paquetes: -1,00 Correlación perfecta negativa

Correlaciones

			CARGA_ÚTIL	JITTER	PÉRDIDA
Rho de Spearman	CARGA_ÚTIL	Coeficiente de correlación	1,000	1,000**	-1,000**
		Sig. (bilateral)	.	.	.
		N	6	6	6
	JITTER	Coeficiente de correlación	1,000**	1,000	-1,000**
		Sig. (bilateral)	.	.	.
		N	6	6	6
	PÉRDIDA	Coeficiente de correlación	-1,000**	-1,000**	1,000
		Sig. (bilateral)	.	.	.
		N	6	6	6

Tabla 3.29 Correlación de Spearman entre la carga útil, el *jitter* y el porcentaje de pérdida de paquetes en el sistema *Router* PE1 para *multicast* @ 10 Mb/s

h.) Conclusión:

Al obtener un valor de *Rho* de +1,00 entre la carga útil y el *jitter* se concluye que existe una correlación perfecta positiva entre estas dos variables en el sistema PE1. Se concluye que, si un paquete con mayor carga útil se envía por la red MVPN IP/MPLS con un *throughput* nominal de 10 Mb/s, aumentará en la misma proporción su variación del retardo.

Asimismo, al obtener un valor de *Rho* de -1,00 entre la carga útil y el porcentaje de pérdida de paquetes, se concluye que existe una correlación negativa

perfecta entre estas dos variables en el sistema PE1. Si un paquete con mayor carga útil se transmite por la red MVPN IP/MPLS con un *throughput* nominal de 10 Mb/s, el porcentaje de pérdida de paquetes decrementará.

3.8.3 INFERENCIA DE RESULTADOS

- La intensidad de tráfico permanece cerca al 1,26 para cualquier tamaño de carga útil experimental, si y solo si se transmite un paquete al mismo *throughput* nominal, es decir a 10 Mb/s. Esto significa que la intensidad de tráfico sobrepasa su valor máximo, es decir, la tasa de arribo es mayor a la de salida del sistema PE1.

- Mientras mayor es el número de paquetes con menor carga útil por unidad de tiempo, que arriban al sistema PE1, dicho sistema empezará a descartar paquetes debido a que posee una capacidad finita de almacenamiento, y generará un incremento en el porcentaje de la pérdida de paquetes (23,2% a 58,5%).

- No se logró obtener el valor del tiempo de permanencia en el sistema PE1, debido a que la intensidad de tráfico fue mayor a 1; por tanto se realizaron pruebas de hipótesis estadística con el fin de correlacionar el tamaño del *payload* con la variación del retardo y el porcentaje de pérdida de paquetes. Se determinó que existe un alto grado de correlación directa entre la variación del retardo (3 us a 2522 us) y el tamaño de carga útil (64 B a 1400 B); y de la misma manera, existe un alto grado de correlación inversa entre el porcentaje de pérdida de paquetes (58,5% a 23,2%) y el tamaño de carga útil (64 B a 1400 B).

3.9 BATERÍA DE PRUEBAS 8

3.9.1 EXPERIMENTO EMISIÓN DE VIDEO

Transmisión de video *unicast* sobre la red IP/MPLS *unicast* VPN y emisión de video *multicast* sobre la red IP/MPLS MVPN, utilizando VLC. Los parámetros a medir en cada receptor son el *throughput*, el *jitter*, el número de paquetes transmitidos por la fuente y el número de paquetes recibidos. En la Tabla 3.30 se aprecian las características principales del video a transmitir.

3.9.2 PRESENTACIÓN DE RESULTADOS UNICAST Y MULTICAST

La Tabla 3.31 muestra los resultados estadísticos de la emisión de video *unicast*, así como en la Tabla 3.32 se aprecian los resultados para la transmisión de video *multicast,* cuyo paquete de video posee un tamaño de carga útil de 188 bytes.

Nombre	Medir ancho de banda con Jperf.mp4
Tamaño	18,8 MB
Resolución	576 x 360
Duración	8 minutos
Frecuencia de muestreo del sonido	44 KHz

Tabla 3.30 Características principales del video a transmitir

Unicast:

Cálculo de la tasa de arribo al sistema PE1, a partir del *throughput* promedio (en pps) de la Tabla 3.31.

$$\lambda_{PE1} = 2\ x\ 158{,}8\ \left[\frac{paquete}{s}\right] \Rightarrow \lambda_{PE1} = 317{,}6\ \left[\frac{paquete}{s}\right]$$

	Payload	*Throughput* [b/s]	Paquetes generados [p/s]	Paquetes perdidos [p/s]	*Jitter* [us]
Mínimo	188	210580	115,4	0	4
Máximo	188	282310	187,7	0	12
Promedio	188	246308	158,8	0	6,6
Mediana	188	239986	158,2	0	5,9
Desv. Est.	0	17830,6	18,4	0	2,5

Tabla 3.31 Resultados estadísticos de la emisión de video *unicast*

	Payload	*Throughput* [b/s]	Paquetes generados [p/s]	Paquetes perdidos [p/s]	*Jitter* [us]
Mínimo	188	211312	140,5	0	7,8
Máximo	188	308066	204,6	0	14,8
Promedio	188	248017	164,9	0	10,8
Mediana	188	245944	163,5	0	10,6
Desv. Est.	0	23388,5	15,5	0	1,7

Tabla 3.32 Resultados estadísticos de la emisión de video *multicast*

Cálculo de la tasa de salida del sistema *Router* PE1, sabiendo que la carga útil es de 188 bytes.

$$\mu_{PE1} = \frac{R}{L} = \frac{8\left[\frac{Mbits}{s}\right] x \frac{10^6\ [bits]}{1\ [Mbit]}}{188\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow\ \mu_{PE1} = 5319{,}2\ \left[\frac{paquete}{s}\right]$$

Cálculo de la intensidad de tráfico del sistema PE1.

$$\rho_{PE1} = \frac{\lambda_{PE1}}{\mu_{PE1}} = \frac{317{,}6\ \left[\frac{paquete}{s}\right]}{5319{,}2\ \left[\frac{paquete}{s}\right]} \Rightarrow\ \rho_{PE1} = 0{,}06$$

Como ρ_{PE1} es menor que 1, se puede calcular las variables de tiempo *T,* t_s y *W* para el sistema PE1.

$$ts_{PE1} = \frac{1}{\mu_{PE1}} = \frac{1}{5319{,}2\ \left[\frac{paquete}{s}\right]} \Rightarrow\ ts_{PE1} = 188\ [us]$$

$$T_{PE1} = \frac{\frac{1}{\mu_{PE1}}}{1 - \rho_{PE1}} = \frac{\frac{1}{5319{,}2\ \left[\frac{paquete}{s}\right]}}{1 - 0{,}06} \Rightarrow\ T_{PE1} = 200\ [us]$$

$$W_{PE1} = T_{PE1} - ts_{PE1} = 200\ [us] - 188\ [us] \Rightarrow W_{PE1} = 12\ [us]$$

La tasa de arribo al sistema P está dado por el valor de la mediana del *throughput* (en b/s) y el tamaño de carga útil del paquete del video, que es de 188 bytes:

$$\lambda_P = 2\ x\ 239986\ \left[\frac{bit}{s}\right] x\ \frac{1\ B}{8\ bits}\ x\ \frac{1\ paquete}{188\ B} \Rightarrow \lambda_P = 2\ x\ 159{,}6\ \left[\frac{paquete}{s}\right]$$

El porcentaje de paquetes que pasaron con éxito por el router PE1 (K_{PE1}) está dado por la tasa de arribo de paquetes al sistema P ($\boldsymbol{\lambda_P}$) y la tasa de llegada al sistema PE1 (λ_{PE1}), como sigue:

$$K_{PE1} = \frac{\lambda_P}{\lambda_{PE1}}\ x\ 100\% = \frac{2\ x\ 159{,}6\ pps}{2\ x\ 158{,}2\ pps}\ x\ 100\% \approx\ 100\ \%$$

Por consiguiente, el porcentaje de pérdida de paquetes es nulo. La Tabla 3.33 resume los resultados obtenidos, principalmente de la intensidad de tráfico como

también de los retardos de servicio, de espera en la cola y el retardo de permanencia en el sistema PE1.

Multicast:

Cálculo de la tasa de salida del sistema *Router* PE1 sabiendo que la carga útil es de 188 bytes.

$$\mu_{PE1} = \frac{R}{L} = \frac{8\left[\frac{Mbits}{s}\right] x \frac{10^6\ [bits]}{1\ [Mbit]}}{188\ [B]\ x\ \frac{8\ [bits]}{1\ [B]}} \Rightarrow\ \mu_{PE1} = 5319{,}2\ \left[\frac{paquete}{s}\right]$$

Cálculo de la intensidad de tráfico del sistema PE1, conociendo que la tasa de arribo es de 164,9 p/s (Tabla 3.32).

$$\rho_{PE1} = \frac{\lambda_{PE1}}{\mu_{PE1}} = \frac{164{,}9\ \left[\frac{paquete}{s}\right]}{5319{,}2\ \left[\frac{paquete}{s}\right]} \Rightarrow\ \rho_{PE1} = 0{,}03$$

Como ρ_{PE1} es menor que 1, se puede calcular las variables de tiempo *T,* t_s y *W* para el sistema PE1.

$$ts_{PE1} = \frac{1}{\mu_{PE1}} = \frac{1}{5319{,}2\ \left[\frac{paquete}{s}\right]} \Rightarrow\ ts_{PE1} = 188\ [us]$$

$$T_{PE1} = \frac{\frac{1}{\mu_{PE1}}}{1 - \rho_{PE1}} = \frac{\frac{1}{5319{,}2\ \left[\frac{paquete}{s}\right]}}{1 - 0{,}03} \Rightarrow\ T_{PE1} = 194\ [us]$$

$$W_{PE1} = T_{PE1} - ts_{PE1} = 194\ [us] - 188\ [us] \Rightarrow W_{PE1} = 6\ [us]$$

La tasa de arribo al sistema P está dado por el valor de la mediana del *throughput* (en b/s) y el tamaño de carga útil del paquete del video, que es de 188 bytes:

$$\lambda_P = 245944\ \left[\frac{bit}{s}\right] x\ \frac{1\ B}{8\ bits}\ x\ \frac{1\ paquete}{188\ B} \Rightarrow \lambda_P =\ 163{,}5\ \left[\frac{paquete}{s}\right]$$

El porcentaje de paquetes que pasaron con éxito por el router PE1 (K_{PE1}) está dado por la tasa de arribo de paquetes al sistema P ($\boldsymbol{\lambda_P}$) y la tasa de llegada al sistema PE1 (λ_{PE1}), como sigue:

$$K_{PE1} = \frac{\lambda_P}{\lambda_{PE1}}\ x\ 100\% = \frac{163{,}5\ pps}{163{,}5\ pps}\ x\ 100\% =\ 100\ \%$$

Por tanto, el porcentaje de pérdida de paquetes es cero. En la Tabla 3.33 se aprecia los resultados obtenidos, principalmente, de la intensidad de tráfico así como de los retardos de servicio, de espera en la cola y el retardo de permanencia en el sistema *Router* PE1.

	λ_{PE1} [p/s]	μ_{PE1} [p/s]	ρ_{PE1}	ts_{PE1} [us]	W_{PE1} [us]	T_{PE1} [us]
UCAST	158,2	5319,1	0,06	188	12	200
MCAST	163,5	5319,1	0,03	188	6	194

Tabla 3.33 Intensidad de tráfico y retardos en el sistema PE1 en *unicast* y *multicast*

En ambos escenarios de emisiones de video se recolectaron sendas cantidades de *jitter*, como se ilustra en la Tabla 3.34. Para la emisión de video *unicast* se obtuvo un valor medio de *jitter* de 6,6 us con una desviación estándar de 2,5 us; mientras que para la trasmisión de video *multicast* se logró un *jitter* promedio de 10,8 us con una desviación estándar de 1,7 us. *A priori,* se podría afirmar que la presencia del factor *jitter* en la emisión *unicast* es menor que en la transmisión *multicast*.

Jitter unicast [us]				*Jitter multicast* [us]			
5,8	8,1	7,7	8,3	8,8	7,9	10,8	10,6
5,3	4,5	7,1	5,7	11,3	10,8	11,9	7,8
7,8	11,8	3,8	4,6	8,7	10,7	10,2	9,5
4,3	9,6	12	4,1	12,1	14,7	10,4	8,7
3,8	4,1	8,1	6,1	10,6	12,2	9,3	10,4

Tabla 3.34 Recolección de muestras de *jitter* en las emisiones de video *unicast y multicast*

Si se observa la Figura 3.9, los datos se hallan muy dispersos y la línea recta de tendencia central no presenta una pendiente positiva o negativa como para dilucidar si ambos factores son directa o indirectamente proporcionales.

Por lo tanto, se planteó una prueba de hipótesis para conocer la relación entre el *jitter* presente en el video *unicast* frente al *jitter* medido en el video *multicast.* Para ello se utilizará la correlación de Spearman y otro factor estadístico similar, el *tau-b* de Kendall[17], para corroborar el resultado.

[17] El *Tau-b* de Kendall es una medida de correlación que presenta muchas similitudes con el coeficiente de Spearman. Es empleado también en estudios estadísticos no paramétricos.

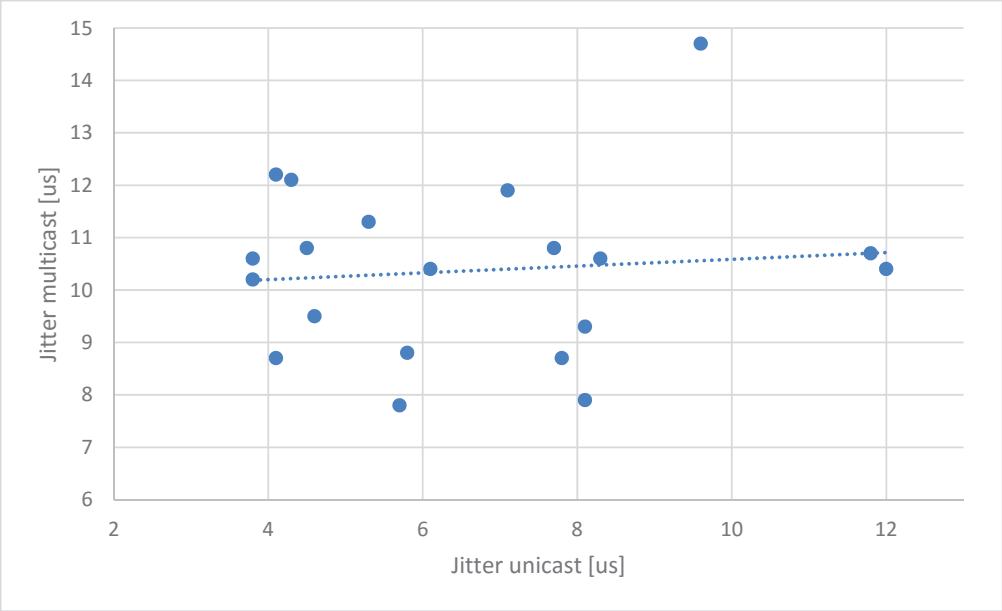

Figura 3.9 *Jitter* presente en *unicast* vs *jitter* presente en *multicast*

a.) Planteamiento de las hipótesis nula H_0 y alterna H_1: se formula una hipótesis alterna bidireccional.

H_0: Los valores promedio del parámetro *jitter* en *unicast* y *multicast,* durante la emisión de video, no son iguales.

H_1: Los valores promedio del parámetro *jitter* en *unicast* y *multicast,* durante la emisión de video, son iguales.

b.) Establecimiento del nivel de significancia: nivel de significancia 5% = 0,05

c.) Generación de los resultados estadísticos en el programa *SPSS Statistics.* Los resultados se detallan en la Tabla 3.35.

d.) Valoración de *Rho* de Spearman calculado = -0,032

Valor de *p* = 0,892

Valoración de *Tau-b* de Kendall calculado = -0,038

Valor de *p* = 0,820

e.) Interpretar (dar como respuesta una de las hipótesis):

El valor de ambas probabilidades es mayor que el nivel de significancia del 5%; esto quiere decir que no se rechaza la hipótesis nula.

Por lo tanto, los valores promedio del parámetro *jitter* en *unicast* y *multicast,* durante la emisión de video, no son iguales.

Correlaciones

			JITTER_UCAST_V	JITTER_MCAST_V
tau_b de Kendall	JITTER_UCAST_V	Coeficiente de correlación	1,000	-,038
		Sig. (bilateral)	.	,820
		N	20	20
	JITTER_MCAST_V	Coeficiente de correlación	-,038	1,000
		Sig. (bilateral)	,820	.
		N	20	20
Rho de Spearman	JITTER_UCAST_V	Coeficiente de correlación	1,000	-,032
		Sig. (bilateral)	.	,892
		N	20	20
	JITTER_MCAST_V	Coeficiente de correlación	-,032	1,000
		Sig. (bilateral)	,892	.
		N	20	20

Tabla 3.35 Correlación de Spearman y Kendall entre el *jitter unicast* y el *jitter multicast* en la emisión del video

f.) Replanteamiento de las hipótesis nula H_0 y alternativa H_1: se formula una hipótesis alterna direccional, con el fin de saber si uno de los dos *jitter* es menor.

H_0: El valor promedio del parámetro *jitter* en *unicast* no es menor que el valor promedio del *jitter* en *multicast,* durante la emisión de video.

H_1: El valor promedio del parámetro *jitter* en *unicast* es menor que el valor promedio del *jitter* en *multicast,* durante la emisión de video.

g.) Establecimiento del nivel de significancia: nivel de significancia 5% = 0,05

h.) Generación de los resultados estadísticos en el programa *SPSS Statistics.* Los resultados se describen en la Tabla 3.36.

i.) Valoración de *Rho* de Spearman calculado = -0,032

Valor de *p* = 0,446

Valoración de *Tau-b* de Kendall calculado = -0,038

Valor de *p* = 0,410

j.) Interpretar (dar como respuesta una de las hipótesis):

El valor de ambas probabilidades es mayor que el nivel de significancia del 5%; esto quiere decir que no se rechaza la hipótesis nula. Por lo tanto, el valor promedio del parámetro *jitter* en *unicast* no es menor que el valor promedio del *jitter* en *multicast,* durante la emisión de video.

Correlaciones

			JITTER_UCAST_V	JITTER_MCAST_V
tau_b de Kendall	JITTER_UCAST_V	Coeficiente de correlación	1,000	-,038
		Sig. (unilateral)	.	,410
		N	20	20
	JITTER_MCAST_V	Coeficiente de correlación	-,038	1,000
		Sig. (unilateral)	,410	.
		N	20	20
Rho de Spearman	JITTER_UCAST_V	Coeficiente de correlación	1,000	-,032
		Sig. (unilateral)	.	,446
		N	20	20
	JITTER_MCAST_V	Coeficiente de correlación	-,032	1,000
		Sig. (unilateral)	,446	.
		N	20	20

Tabla 3.36 Replanteamiento de la correlación de Spearman y Kendall entre el *jitter unicast* y el *jitter multicast* en la emisión del video

k.) Interpretación del valor de *Rho* y *Tau-b*: De 0,00 a -0,19 Muy baja correlación negativa

Al obtener un valor de *Rho* de -0,032 y *Tau-b* de -0,038, se manifiesta que existe una muy baja correlación negativa entre el *jitter unicast* y el *jitter multicast,* es decir casi no existe correlación entre sus valores promedios. Se concluye que otros factores internos o externos a la emisión de video influyen, de forma significativa, en la variación del retardo en ambos ambientes.

3.9.3 INFERENCIA DE RESULTADOS UNICAST Y MULTICAST

- No hubo pérdida de paquetes durante la emisión de video *unicast* y *multicast* ya que no se reflejaron 'anomalías' en las imágenes ni cortes en el audio. Eso se corroboró tanto de parte del medidor de tráfico de video (*FaultLine*) como de la relación entre las tasas de arribo a los sistemas P y PE1. En otras palabras, todos los paquetes que ingresaron al sistema PE1 fueron 'atendidos' con éxito.

- A través de los coeficientes de correlación de Spearman y Kendall, se comprobó que el valor promedio del *jitter unicast* no posee relación alguna con el valor promedio del *jitter multicast* en la emisión de video, ya sea de carácter *unicast* o *multicast.* Éstos son índices que, muy probablemente, obedecen a variaciones del retardo de permanencia en el sistema PE1.

- La intensidad de tráfico en la transmisión de video es el mismo para *unicast* y *multicast*, así como el tiempo de servicio y el tiempo de espera en la cola. En este ambiente de prueba con 'condiciones normales', el tiempo que atiende el servidor del sistema a un paquete es mayor al tiempo que le toma a la cola en despachar a dicho paquete, ya que la intensidad del tráfico es casi nula.

3.10 DISCERNIMIENTO DEL TRÁFICO MULTICAST EN IP/MPLS MVPN

Para este análisis se emplea el generador de tráfico Jperf, para transmitir tráfico *multicast* con un tamaño de datos de 1000 bytes, a un ancho de banda de 125 Kb/s. La fuente posee la dirección IP 192.168.10.10 y forma parte del grupo *multicast* IP 228.1.1.1, con la ayuda de IGMP. La fuente tiene la labor de enviar tráfico *multicast* a los receptores que son miembros del mismo grupo *multicast*.

La Figura 3.10 muestra que el *payload* o carga útil, que llega procedente de la fuente, es encapsulado en UDP, que agrega 8 bytes de cabecera; luego, baja a IP, en donde es encapsulado y añadido 20 bytes de cabecera. A continuación es encapsulado en Ethernet II, donde éste coloca 18 bytes de cabecera y cola.

El campo CRC de Ethernet II no se muestra en la captura, sin embargo, sí se lo considera como parte de la cola. Toda la trama da un total de 1046 bytes y no de 1042 bytes, como se aprecia en la figura. Además se aprecia la dirección física destino *multicast*, ya que ésta inicia con el valor hexadecimal 01005E.

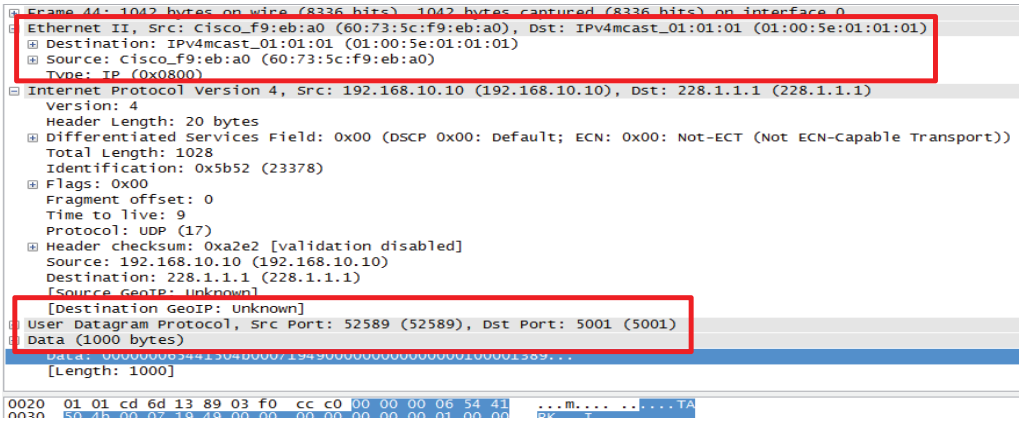

Figura 3.10 Captura de tráfico *multicast* entre CE1 y PE1

El mismo procedimiento ocurre cuando el paquete *multicast* es entregado a CE2 por parte de PE2 (Figura 3.11) y a CE3 por parte de PE3 (Figura 3.12). UDP

encapsula el *payload* y agrega 8 bytes correspondientes a su cabecera; IP, 20 bytes de cabecera; Ethernet II, 18 bytes de cabecera y cola.

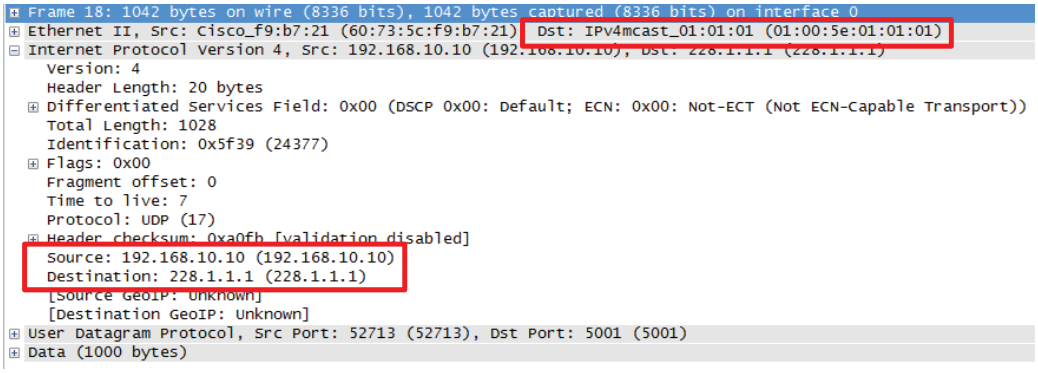

Figura 3.11 Captura de tráfico *multicast* entre PE2 y CE2

Una vez que el paquete *multicast* arriba a PE1, éste lo desencapsula y recupera el dato original. Enseguida, el protocolo UDP vuelve a añadir 8 bytes de cabecera. Luego desciende hasta IP, en donde lo encapsula y coloca 20 bytes de cabecera. Como dirección fuente coloca a la 192.168.10.10 y a la dirección de grupo, la 228.1.1.1.

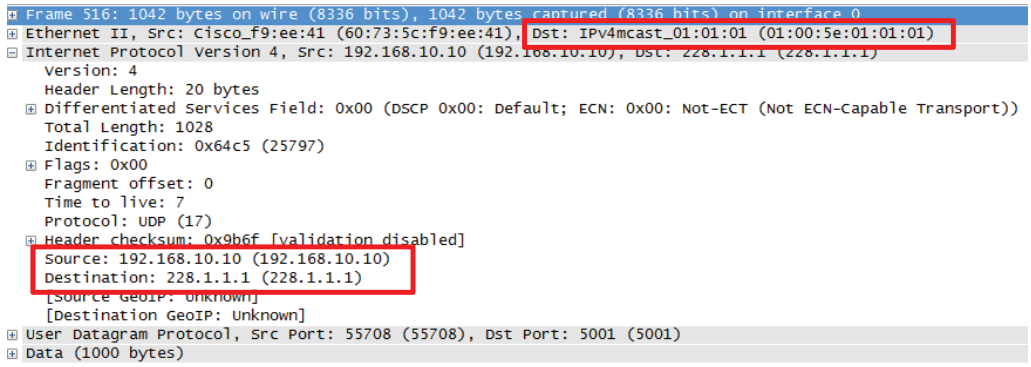

Figura 3.12 Captura de tráfico *multicast* entre PE3 y CE3

Ahora, para enviar a través de la nube IP/MPLS MVPN, todo este *payload* es encapsulado en GRE (4 bytes), y vuelve a descender hasta IP, en donde es encapsulado y agregado 20 bytes de cabecera. [43]

En este punto, de cara al *core*, se añade una nueva fuente, 1.1.1.1/32, que viene a ser la dirección *loopback* de PE1, acompañada de la dirección de destino 232.1.1.1 correspondiente a la dirección IP del árbol de distribución *multicast* por defecto, y que desde ese instante, se convierte en la nueva dirección *multicast* de destino, como se ilustra en la Figura 3.13. La longitud total de la trama es de 1070 bytes

correspondiente a 1000 bytes de *payload*, 8 bytes de UDP, 20 bytes de IP, 4 bytes de GRE, otros 20 bytes de IP y 18 bytes de Ethernet II.

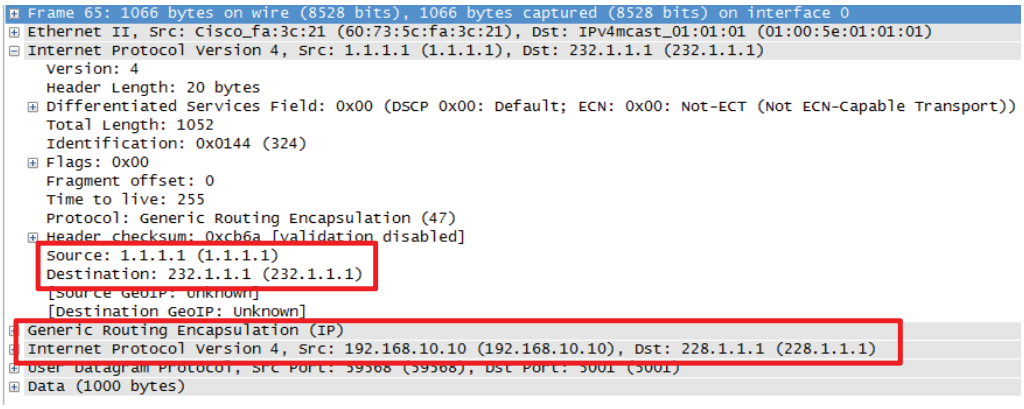

Figura 3.13 Captura de tráfico *multicast* entre PE1 y P

De la misma manera ocurre cuando el paquete *multicast* es entregado a PE2 y PE3 por parte de P (Figuras 3.14 y 3.15). UDP encapsula el *payload* y agrega 8 bytes correspondientes a su cabecera; GRE, 4 bytes; IP, 20 bytes de cabecera; Ethernet II, 18 bytes de cabecera y cola.

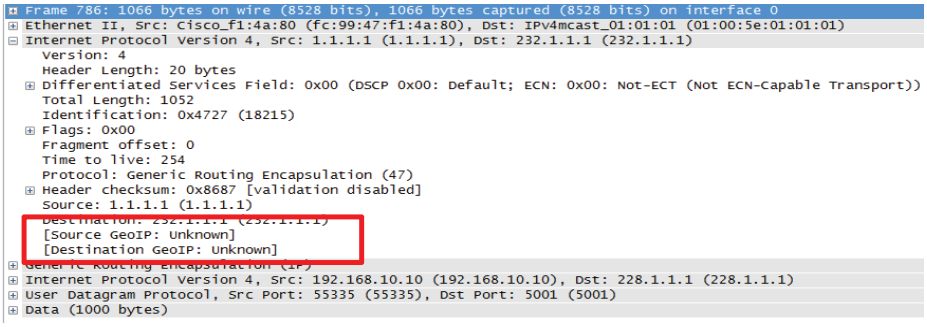

Figura 3.14 Captura de tráfico *multicast* entre P y PE2

Por otra parte y de manera singular, todos los *routers* que fueron configurados con, al menos, un protocolo de enrutamiento *unicast* o *multicast*, generaron en su tabla de enrutamiento *multicast*, automáticamente, una dirección IP *multicast*. Es decir, todos los *routers* habilitados con PIM generaron la dirección IP 224.0.0.13 correspondiente a 'todos los *routers* PIM'.

El mismo hecho ocurrió con aquellos *routers* que manejan enrutamiento con el protocolo RIP (224.0.0.9); aquellos que manejan enrutamiento con el protocolo OSPF (224.0.0.5) y a los *routers* que anuncian, por medio de IGMPv2, el descubrimiento de un RP Cisco, mediante la dirección IP *multicast* 228.0.1.40.

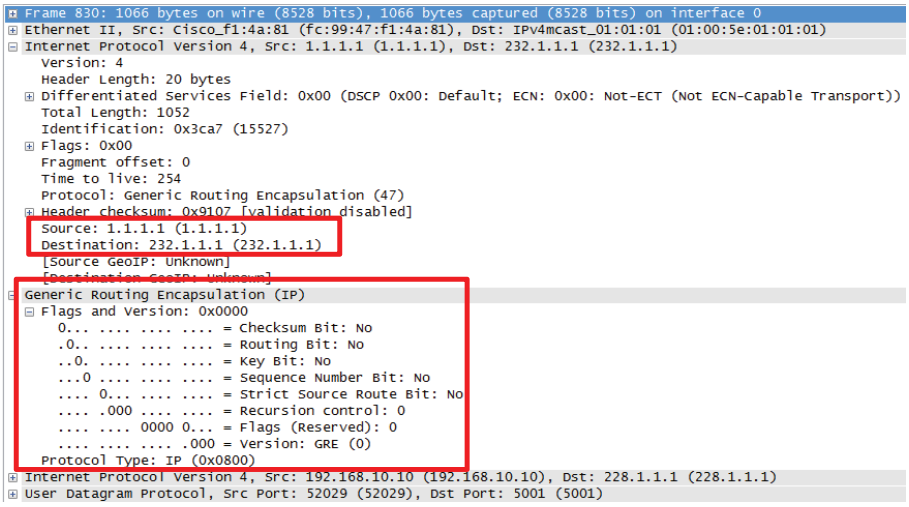

Figura 3.15 Captura de tráfico *multicast* entre P y PE3

Por su parte, el protocolo de enrutamiento *multicast* PIM no transporta ningún paquete *multicast* o *payload*. En efecto, PIM actúa en la parte de control de establecimiento de la sesión *multicast*. Todos los *routers* PIM llevan información de la dirección de grupo *multicast* 228.1.1.1 y la dirección IP del RP 192.168.1.2.

En los *routers* de borde del cliente (CEs), IP agrega a su fuente la dirección 192.168.1.2 que corresponde a la raíz del árbol *multicast*, es decir el RP, ya que se configuró con PIM SM, el cual construye árboles de grupo compartido. Como dirección de destino coloca la 224.0.0.2, que es la dirección *multicast* de 'todos los *routers* ubicados en un mismo segmento de red', como se muestra en la Figura 3.16.

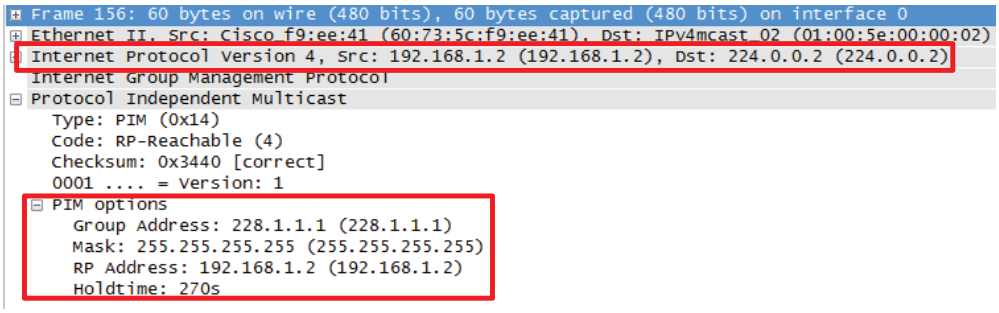

Figura 3.16 Encapsulamiento de PIM en CEs

Asimismo, en los *routers* del proveedor (PEs y P), esta información es encapsulada en GRE, pero la nueva raíz del árbol viene a ser la dirección 1.1.1.1 con dirección de grupo *multicast* 232.1.1.1 correspondiente a la MDT por defecto, como se aprecia en la Figura 3.17.

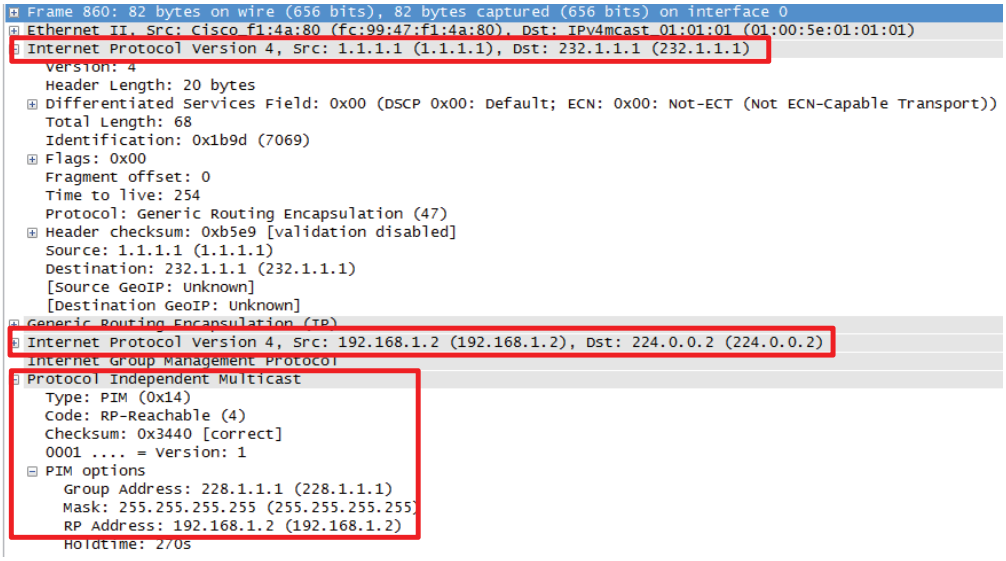

Figura 3.17 Encapsulamiento de PIM en los PEs y P

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Se estudió que *Multicast* VPN es una tecnología que se superpone a la infraestructura *unicast* VPN en redes IP/MPLS, en donde los *routers* emplean protocolos de enrutamiento *multicast* para construir árboles de distribución y transmitir cualquier tipo de contenido *multicast* hasta los receptores, logrando de esta manera, una optimización del ancho de banda.

- Se determinó que si la fuente emite un número cada vez mayor de paquetes con menos carga útil por unidad de tiempo, a través de la red IP/MPLS *unicast* VPN o MVPN, el sistema de encolamiento PE1 descartará más paquetes, ya que la capacidad de almacenamiento de la cola es superada por el volumen de tráfico que cursa por aquel sistema; por ende, se generará un incremento en el porcentaje de pérdida de paquetes.

- En los escenarios donde la intensidad de tráfico fue menor a 1, el *throughput* de los paquetes recibidos (con éxito) con menos carga útil, fue directamente proporcional a la variación del retardo y de la misma forma al tiempo de permanencia en el sistema PE1. Mediante el planteamiento de hipótesis y de la prueba estadística no paramétrica de Spearman se confirmó que el tiempo de permanencia en el sistema PE1 se relacionaba positiva e íntimamente con la variación del retardo.

- En aquellos escenarios donde la intensidad de tráfico fue igual o mayor a 1, el *throughput* de los paquetes recibidos (con éxito) con menos carga útil, fue directamente proporcional a la variación del retardo, e inversamente proporcional al porcentaje de pérdida de paquetes. Es así que con el planteamiento de hipótesis y el empleo de la prueba estadística no paramétrica de Spearman se corroboró que la variación del retardo se relacionaba negativa y fuertemente con el porcentaje de pérdida de paquetes.

- En la emisión de video *unicast* y *multicast* se tomaron muestras del *jitter* y se observó que el valor promedio de este parámetro era menor en *unicast* frente a

multicast. A través de los estadísticos de prueba de Kendall y Spearman se planteó una prueba de hipótesis, logrando establecer que la variación del retardo *unicast* no era mayor a *multicast*, y de la misma manera, ambas variaciones del retardo tampoco eran iguales. Al suscitarse esta emisión de video bajo condiciones normales (sin sobrecargar a la red), la asimetría entre los promedios de *jitter* obedece, fundamentalmente, al retardo o tiempo que se tome el sistema de encolamiento PE1 en tratar a los distintos *streams* de video *unicast* y *multicast*.

- Se observó que GRE es un protocolo que encapsula los paquetes que contienen datos *multicast*, con el objetivo de transportarlos sobre otro tipo de protocolo de capa Red, en este caso IP, para atravesar la red IP/MPLS MVPN, a través del árbol de distribución *multicast* por defecto. Esto implica que, MVPN usa una combinación de PIM y encapsulamiento GRE para el plano de control y de datos, respectivamente. MPLS como tal, no interviene en este tipo de tecnología.

4.2 RECOMENDACIONES

- Simular o emular, dentro del ambiente de la red IP/MPLS MVPN, otros protocolos de enrutamiento *multicast*, como PIM-DM y PIM-SM/DM, con el fin de comparar sus desempeños frente a PIM-SM. PIM SM/DM es un modo híbrido de PIM que presenta Cisco y que conjuga los modos de operación disperso y denso. Cuando existe un grupo *multicast* vinculado a la dirección de un RP, PIM SM/DM trabajará en modo disperso. Si aquel grupo no está vinculado a ningún RP, trabajará en modo denso.

- Incorporar algún protocolo de seguridad en los datos *multicast*, como es el caso de IPsec, ya que la seguridad es un factor primordial al momento de proteger los datos. De la misma manera se recomienda establecer políticas de seguridad, encriptación y acceso exclusivo a determinadas aplicaciones y puntos vulnerables en la red IP/MPLS MVPN, como son el RP y la fuente, ya que son los encargados de distribuir el tráfico *multicast*.

- Implementar el árbol MDT de datos, aparte del árbol MDT por defecto, cuando existan varios receptores o hosts dispersos en los sitios del ciente en la red IP/MPLS MVPN y expresen su interés en recibir un determinado tráfico *multicast*, y que a su vez este tráfico *multicast* tenga un gran ancho de banda. Esto se debe a que en teoría, el MDT por defecto, fue concebido para transportar información *multicast* tanto de control como de datos, de bajo ancho de banda. Si el umbral de ancho de banda configurado para el árbol MDT por defecto esté por saturarse, debido al tráfico *multicast*, automáticamente se 'disparará' el árbol MDT de datos, para transportar únicamente los datos *multicast*.

- Emplear un protocolo de enrutamiento *multicast* dentro de una red IP/MPLS MVPN, como PIM BiDir, cuando se presenten lugares de un cliente en donde existan muchas fuentes y muchos receptores, que deseen transmitir tráfico *multicast* en ambos sentidos; ya que PIM BiDir es capaz de construir árboles de distribución compartidos para reenviar datos *multicast* en ambas direcciones.

- Implementar calidad de servicio a través de la reserva de recursos, mediante la extensión de los protocolos de señalización CR-LDP y RSVP-TE, para *multicast*, cuando se requiera transmitir aplicaciones *multicast* tales como video *streaming*, videoconferencia o telepresencia, que son sensibles al retardo o a su variación.

REFERENCIAS BIBLIOGRÁFICAS

[1] GUICHARD, Jim; PEPELNJAK, Ivan; APCAR, Jeff. “MPLS and VPN Architectures” Volume II. Cisco Press 2003, EEUU.

[2] JOSEPH, Vinod; MULUGU, Srinivas. “Deploying Next Generation *Multicast*-Enabled Applications”. Elsevier 2011, EEUU.

[3] SÁNCHEZ MONGE, Antonio. “This week: Deploying BGP *Multicast* VPNs” 2nd Edition. Juniper 2012.

[4] ODOM, Wendell; HEALY, Rus; DONOHUE, Denise. “CCIE Routing and Switching. Certification Guide” 4th Edition. Cisco Press 2010.

[5] ARIGANELO, Ernesto; BARRIENTOS SEVILLA, Enrique. “Redes Cisco CCNP a fondo”. Editorial Ra-Ma, España 2010.

[6] COMER, Douglas. Internetworking with TCP/IP Vol. I: Principles, Protocols and Architectures, 6th Edition. Pearson 2014, EEUU.

[7] CISCO LIVE 365. “IPv6 *Multicast* Deployment” BRKRST – 3301. Cisco Systems 2011.

[8] KIVINIEMI, Teemu. “Implementation of an IPv4 to IPv6 Translator” Master’s Thesis. Helsinky University of Technology 2009.

[9] WILLIAMSON, Beau. “Developing IP *Multicast* Networks”. Cisco Systems 2005.

[10] SEMERIA, Chuck; MAUFER, Tom. “Introduction to IP *Multicast* Routing”. Disponible en: http://www.stanford.edu/class/ee384a/files/Introduction_to_IP_*Multicast*_Routing.pdf, al 29 de marzo del 2014.

[11] INGTELECO. “Transparencias de redes de ordenadores, Tema 12 IP *Multicast*”. Disponible en: http://ingteleco.webcindario.com/Redes/Transparencias/Tema%2012%20-%20IP%20*Multicast*.pdf, al 31 de marzo del 2014.

[12] GACITÚA DECAR, Verónica Andrea; Tesis “Evaluación de algoritmos de rutemiento multipunto en redes de computadores”. Disponible en: http://www.computing.dcu.ie/~vgacitua/files/Master_Tesis.pdf, al 31 de marzo del 2014.

[13] TREJO, Natalia Bibiana. Tesis “Aplicación de *Multicast* IPv6 Seguro

a Servicios de Información en Entornos Grid". Madrid, 2008.

[14] JUNIPER NETWORKS. "Junos OS, *Multicast* Protocols Feature Guide for Routing Devices". Juniper Networks 2014.

[15] SHEPHERD, Greg. "Introduction to IP *Multicast*" BRKIPM – 1261. Cisco Live 365, Cisco Systems 2011.

[16] WIKIPEDIA. "*Any-source multicast*". Disponible en: http://en.wikipedia.org/wiki/Any-source_*multicast*, al 02 de abril de 2014.

[17] DE GHEIN, Luc. "MPLS Fundamentals". Cisco Systems 2007.

[18] FALCONÍ NORIEGA, Marco Fabricio; RODRÍGUEZ GARCÍA, Lucía Silveria. Tesis EPN "Análisis de Riesgos de la Red IP/MPLS de la Corporación Nacional de Telecomunicaciones, basado en la Norma ISO/IEC 27005 y Propuesta de Mejoramiento del Control de Acceso a la Administración de sus dispositivos". Quito, enero 2012.

[19] ANÓNIMO. "MPLS VPNs". Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo3.pdf, al 23 de septiembre del 2013.

[20] ANÓNIMO. "Understanding using MPLS-based Layer 2 and Layer 3 VPNs on EX Series *Switches*". Disponible en: http://www.juniper.net/techpubs/en_US/junos13.2/topics/concept/mpls-ex-series-vpn-layer2-layer3.html, al 24 de abril del 2014.

[21] METZ, Chris. "Multiprotocol Label Switching and IP, Part 2" *Multicast* Virtual Private Networks. Cisco Systems 2006.

[22] JUNIPER NETWORKS. "Understanding PIM for IPv6 *Multicast*". Disponible en: http://www.juniper.net/techpubs/en_US/junose15.1/topics/concept/pim-ipv6-understanding.html, al 19 de octubre del 2015

[23] LI, Qing; TATUYA, Jinmei; SHIMA, Keiichi. "IPv6 Advanced Protocols Implementation". Morgan Kaufmann, 2010.

[24] BARRIGA, Miguel; VISCAÍNO, Juan. "Estudio de los protocolos de enrutamiento multicast sobre MPLS aplicado a la provisión del servicio de IPTV en la CNT Riobamba", Tesis de Grado. Riobamba, 2013.

[25] FOROUZAN, Behrouz, "TCP/IP Protocol Suite", Fourth edition. McGraw-Hill, EEUU 2010.

[26] DAVIES, Joseph. "Understanding IPv6" Second edition. Microsoft Corporation, 2008.

[27] RIGOTTI, Guillermo. Tesis de Maestría “Implementación y Análisis de CBTv2 en el medioambiente Ns”. Universidad Nacional de La Plata - Argentina, 1998. Disponible en: http://sedici.unlp.edu.ar/bit*stream*/handle/10915/2209/2_ _Perspectiva_de_los_protocolos_de_ruteo_*multicast*.pdf?sequence=5, al 10 de septiembre de 2014.

[28] White paper “Multi-VRF and IP *Multicast*”. Cisco Systems, 2005. Disponible en: http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd8012033f.pdf, al 10 de abril de 2014.

[29] ANDIORIO, Jeff. “MPLS *Multicast* Routing IOS”. Disponible en: http://networking-notes.blogspot.com/2013/01/*multicast*-vpn.html, al 19 de abril del 2014.

[30] LOBO, Lancy; LAKSHMAN, Umesh. “MPLS Configuration on Cisco IOS Software”. Cisco Press 2005.

[31] ANÓNIMO. “mVPN – Knowledge Base”. Disponible en: https://sites.google.com/site/amitsciscozone/mvpn, al 5 de agosto de 2014.

[32] CERTUS DIGITAL - FaultLine. “FaultLine Literature”. Disponible en: http://www.certusdigital.com/downloads/Literature/FaultLine%20FAQ.pdf, al 20 de octubre de 2015.

[33] KOLAHI, Samad; NARAYAN, Shaneel; NGUYEN, Du. SUNARTO, Yonathan. “Performance Monitoring of Various Network Traffic Generators”. Nueva Zelanda, IEEE 2011.

[34] ANÓNIMO. “Troubleshooting client speed and traffic shapping using Jperf”. Disponible en: https://kb.meraki.com/knowledge_base/troubleshooting-client-speed-and-traffic-shapping-using-jperf, al 17 de diciembre de 2014.

[35] ANÓNIMO. “VLC’s Homepage”. Disponible en: https://wiki.videolan.org/VLC_media_player/, al 28 de diciembre de 2014.

[36] ANÓNIMO. “VLC media player”. Disponible en: http://en.wikipedia.org/wiki/VLC_media_player, al 28 de diciembre de 2014.

[37] USUARIO DEBIAN. Servidor de *streaming* de video. Disponible en: http://usuariodebian.blogspot.com/2015/02/vlc-servidor-de-streaming-de-

video.html, al 26 de mayo de 2015.

[38] GUNTER, Bolch; GREINER, Stefan; DE MEER, Hermann; TRIVEDI, Kishor. “Queueing Networks and Markov Chains”. EEUU, 1998.

[39] SERRANO YÁNEZ-MINGOT, Pablo; HERNÁNDEZ GUTIÉRREZ, José Alberto. “Una introducción amable a la teoría de colas”. Universidad Carlos III de Madrid, España, 2015. Disponible en: http://www.it.uc3m.es/pablo/teoria-colas/introduccion-teoria-colas.pdf, al 24/09/2015.

[40] KUROSE, James; ROSS, Keith. “Computer Networking: A Top Down Approach”. EEUU, 2013.

[41] LIND, Douglas; MARCHAL, William; MASON, Robert. “Estadística para Administración y Economía”. Colombia, 2004.

[42] MODIANO, Eytan. “Control de congestión y flujo”. Disponible en: http://mit.ocw.universia.net/6-263JData-Communication NetworksFall2002/NR/rdonlyres/Electrical-Engineering-and-Computer-Science/6-263JData-Communication-NetworksFall2002/1ADB752D-6B6B-4AB7-B123-B03D4726C2CA/0/Lectures22_23.pdf, al 3 de junio de 2015.

[43] WIKIPEDIA. “Generic Routing Encapsulation”. Disponible en http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation, al 1 de febrero de 2015.

ANEXOS

Anexo A: ARCHIVOS DE CONFIGURACIÓN DE LOS *ROUTERS* UTILIZADOS EN LA IMPLEMENTACIÓN DE *UNICAST* Y *MULTICAST* VPN……..……..…..A-1

Anexo B: MANUAL DE GENERACIÓN DE TRÁFICO UTILIZANDO JPERF……..……..B-1

Anexo C: MANUAL DE EMISIÓN DE VIDEO UTILIZANDO VLC.....C-1

Anexo D: TABULADOS CORRESPONDIENTES A LA GENERACIÓN DE TRÁFICO *UNICAST* Y *MULTICAST* CON JPERF Y VLC……..…….....D-1

Anexo E: MANUAL DE ANÁLISIS DE DATOS CON SPSS STATISTICS……..E-1

ANEXO A

ARCHIVOS DE CONFIGURACIÓN DE LOS ROUTERS UTILIZADOS EN LA IMPLEMENTACIÓN DE *UNICAST* Y *MULTICAST* VPN

A.1 *UNICAST*…….....…….....A-1

A.2 *MULTICAST*….……...……..... A-9

A.1 *UNICAST*

A.1.1 *Router* CE1

```
!
hostname CE1
!
ip cef
!
!
ip vrf REDES
 rd 200:200
!
!
no ip domain lookup
no ipv6 cef
!
!
interface gigabitEthernet0/0
 description CE1 - PE1
 ip vrf forwarding REDES
 ip address 192.168.1.2 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface gigabitEthernet0/1
 description CE1 - LAN1
 ip vrf forwarding REDES
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 no shutdown
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  network 192.168.1.0
  network 192.168.10.0
  no auto-summary
  version 2
 exit-address-family
!
```

```
!
snmp-server community publicCE1 RO
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.1.2 *Router* PE1

```
!
hostname PE1
!
ip cef
!
!
ip vrf REDES
 rd 200:200
 route-target export 200:200
 route-target import 200:200
!
!
no ip domain lookup
no ipv6 cef
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
!
interface gigabitEthernet0/0
 description PE1 - CE1
 ip vrf forwarding REDES
 ip address 192.168.1.1 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface gigabitEthernet0/1
 description PE1 - P
 ip address 10.10.10.1 255.255.255.252
 duplex auto
 speed auto
 mpls ip
 no cdp enable
 no shutdown
!
router ospf 200
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 10.10.10.0 0.0.0.3 area 0
!
router rip
 version 2
```

```
 !
 address-family ipv4 vrf REDES
  redistribute bgp 200 metric 10
  network 192.168.1.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 200
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf REDES
  redistribute rip metric 50
  no synchronization
 exit-address-family
!
!
snmp-server community publicPE1 RO
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.1.3 *Router* P

```
!
hostname P
!
ip cef
!
!
no ip domain lookup
no ipv6 cef
!
!
```

```
interface gigabitEthernet0/0
 description P - PE2
 ip address 10.10.20.2 255.255.255.252
 duplex auto
 speed auto
 mpls ip
 no cdp enable
 no shutdown
!
interface gigabitEthernet0/1
 description P - PE3
 ip address 10.10.30.2 255.255.255.252
 duplex auto
 speed auto
 mpls ip
 no cdp enable
 no shutdown
!
interface serial0/1/0
 description P - PE1
 ip address 10.10.10.2 255.255.255.252
 clock rate 8000000
 duplex auto
 speed auto
 mpls ip
 no cdp enable
 no shutdown
!
!
router ospf 200
 log-adjacency-changes
 network 10.10.20.0 0.0.0.3 area 0
 network 10.10.30.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.3 area 0
!
!
snmp-server community publicP RO
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.1.4 *Router* PE2

```
!
hostname PE2
!
ip cef
!
!
ip vrf REDES
 rd 200:200
 route-target export 200:200
```

```
 route-target import 200:200
!
!
no ip domain lookup
no ipv6 cef
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
!
interface gigabitEthernet0/0
 description PE2 - P
 ip address 10.10.20.1 255.255.255.252
 duplex auto
 speed auto
 mpls ip
 no cdp enable
 no shutdown
!
interface gigabitEthernet0/1
 description PE2 - CE2
 ip vrf forwarding REDES
 ip address 192.168.2.1 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
router ospf 200
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.20.0 0.0.0.3 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  redistribute bgp 200 metric 10
  network 192.168.2.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 200
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 3.3.3.3 remote-as 200
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
```

```
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf REDES
  redistribute rip metric 50
  no synchronization
 exit-address-family
!
!
snmp-server community publicPE2 RO
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.1.5 *Router* PE3

```
!
hostname PE3
!
ip cef
!
!
ip vrf REDES
 rd 200:200
 route-target export 200:200
 route-target import 200:200
!
!
no ip domain lookup
no ipv6 cef
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
!
interface gigabitEthernet0/0
 description PE3 - P
 ip address 10.10.30.1 255.255.255.252
 duplex auto
 speed auto
 mpls ip
 no cdp enable
 no shutdown
!
interface gigabitEthernet0/1
 description PE3 - CE3
 ip vrf forwarding REDES
 ip address 192.168.3.1 255.255.255.252
 duplex auto
 speed auto
```

```
 no shutdown
!
router ospf 200
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 10.10.30.0 0.0.0.3 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  redistribute bgp 200 metric 10
  network 192.168.3.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 200
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf REDES
  redistribute rip metric 50
  no synchronization
 exit-address-family
!
!
snmp-server community publicPE3 RO
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.1.6 *Router* CE2

```
!
hostname CE2
!
ip cef
!
!
ip vrf REDES
 rd 200:200
!
no ip domain lookup
no ipv6 cef
!
interface gigabitEthernet0/0
 description CE2 - PE2
 ip vrf forwarding REDES
 ip address 192.168.2.2 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface gigabitEthernet0/1
 description CE2 - LAN2
 ip vrf forwarding REDES
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 no shutdown
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  network 192.168.2.0
  network 192.168.20.0
  no auto-summary
  version 2
 exit-address-family
!
!
snmp-server community publicCE2 RO
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.1.7 *Router* CE3

```
!
hostname CE3
!
ip cef
```

```
!
!
ip vrf REDES
 rd 200:200
!
!
no ip domain lookup
no ipv6 cef
!
!
interface gigabitEthernet0/0
 description CE3 - PE3
 ip vrf forwarding REDES
 ip address 192.168.3.2 255.255.255.252
 duplex auto
 speed auto
 no shutdown
!
interface gigabitEthernet0/1
 description CE3 - LAN3
 ip vrf forwarding REDES
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 no shutdown
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  network 192.168.3.0
  network 192.168.30.0
  no auto-summary
  version 2
 exit-address-family
!
!
snmp-server community publicCE3 RO
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

A.2 *MULTICAST*

A.2.1 *Router* CE1

```
hostname CE1
!
no ipv6 cef
ip source-route
```

```
ip cef
!
ip vrf REDES
 route-target both 200:200
 rd 200:200
!
ip multicast-routing
ip multicast-routing vrf REDES
!
no ip domain lookup
!
interface GigabitEthernet0/0
 description CE1 - PE1
 ip vrf forwarding REDES
 ip address 192.168.1.2 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet0/1
 description CE1 - LAN1
 ip vrf forwarding REDES
 ip address 192.168.10.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  network 192.168.1.0
  network 192.168.10.0
  no auto-summary
  version 2
 exit-address-family
!
ip forward-protocol nd
!
ip pim vrf REDES rp-address 192.168.1.2 50
no ip http server
no ip http secure-server
!
access-list 50 permit 228.0.0.0 0.255.255.255
!
snmp-server community publicCE1 RO
snmp-server enable traps mvpn
!
control-plane
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 transport input all
!
```

```
scheduler allocate 20000 1000
end
```

A.2.2 *Router* PE1

```
hostname PE1
!
no ipv6 cef
ip source-route
ip cef
!
ip vrf REDES
 rd 200:200
 mdt default 232.1.1.1
 route-target export 200:200
 route-target import 200:200
!
ip multicast-routing
ip multicast-routing vrf REDES
!
no ip domain lookup
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet0/0
 description PE1 - CE1
 ip vrf forwarding REDES
 ip address 192.168.1.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
interface serial0/1/0
 description PE1 - P
 ip address 10.10.10.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 mpls ip
 no shutdown
!
router ospf 200
 network 1.1.1.1 0.0.0.0 area 0
 network 10.10.10.0 0.0.0.3 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  redistribute bgp 200 metric 10
  network 192.168.1.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
```

```
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 200
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 2.2.2.2 activate
  neighbor 3.3.3.3 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf REDES
  redistribute rip metric 50
 exit-address-family
!
ip forward-protocol nd
!
ip pim ssm default
ip pim vrf REDES rp-address 192.168.1.2 50
!
access-list 50 permit 228.0.0.0 0.255.255.255
!
!
snmp-server community publicPE1 RO
snmp-server enable traps mvpn
!
control-plane
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

A.2.3 *Router* P

```
!
hostname P
!
!
no ipv6 cef
```

```
ip source-route
ip cef
!
!
ip multicast-routing
!
!
no ip domain lookup
!
interface GigabitEthernet0/0
 description P - PE2
 ip address 10.10.20.2 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 mpls ip
 no shutdown
!
interface GigabitEthernet0/1
 description P - PE3
 ip address 10.10.30.2 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 mpls ip
 no shutdown
!
interface Serial0/1/0
 description P - PE1
 bandwidth 100000
 ip address 10.10.10.2 255.255.255.252
 ip pim sparse-mode
 mpls ip
 clock rate 8000000
 no shutdown
!
!
router ospf 200
 network 10.10.20.0 0.0.0.3 area 0
 network 10.10.30.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.3 area 0
!
ip forward-protocol nd
!
ip pim ssm default
!
!
snmp-server community publicP RO
snmp-server enable traps mvpn
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 transport input all
```

```
!
scheduler allocate 20000 1000
end
```

A.2.4 *Router* PE2

```
!
hostname PE2
!
no ipv6 cef
ip source-route
ip cef
!
!
ip vrf REDES
 rd 200:200
 mdt default 232.1.1.1
 route-target export 200:200
 route-target import 200:200
!
ip multicast-routing
ip multicast-routing vrf REDES
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ip pim sparse-mode
!
!
interface GigabitEthernet0/0
 description PE2 - P
 ip address 10.10.20.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 mpls ip
 no shutdown
!
interface GigabitEthernet0/1
 description PE2 - CE2
 ip vrf forwarding REDES
 ip address 192.168.2.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
!
router ospf 200
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.20.0 0.0.0.3 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  redistribute bgp 200 metric 10
  network 192.168.2.0
  no auto-summary
```

```
  version 2
 exit-address-family
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 200
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 3.3.3.3 remote-as 200
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 3.3.3.3 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf REDES
  redistribute rip metric 50
 exit-address-family
!
ip forward-protocol nd
!
ip pim ssm default
ip pim vrf REDES rp-address 192.168.1.2 50
!
!
access-list 50 permit 228.0.0.0 0.255.255.255
!
!
snmp-server community publicPE2 RO
snmp-server enable traps mvpn
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

A.2.5 *Router* PE3

```
!
hostname PE3
!
!
no ipv6 cef
ip source-route
ip cef
!
!
ip vrf REDES
 rd 200:200
 mdt default 232.1.1.1
 route-target export 200:200
 route-target import 200:200
!
ip multicast-routing
ip multicast-routing vrf REDES
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 ip pim sparse-mode
!
!
interface GigabitEthernet0/0
 description PE3 - P2
 ip address 10.10.30.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 mpls ip
 no shutdown
!
interface GigabitEthernet0/1
 description PE3 - CE3
 ip vrf forwarding REDES
 ip address 192.168.3.1 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
!
router ospf 200
 network 3.3.3.3 0.0.0.0 area 0
 network 10.10.30.0 0.0.0.3 area 0
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  redistribute bgp 200 metric 10
  network 192.168.3.0
  no auto-summary
  version 2
 exit-address-family
!
router bgp 200
```

```
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 200
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 200
 neighbor 2.2.2.2 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  neighbor 2.2.2.2 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 mdt
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf REDES
  redistribute rip metric 50
 exit-address-family
!
ip forward-protocol nd
!
ip pim ssm default
ip pim vrf REDES rp-address 192.168.1.2 50
!
!
access-list 50 permit 228.0.0.0 0.255.255.255
!
!
snmp-server community publicPE3 RO
snmp-server enable traps mvpn
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

A.2.6 *Router* CE2

```
!
hostname CE2
!
```

```
!
no ipv6 cef
ip source-route
ip cef
!
!
ip vrf REDES
 rd 200:200
!
ip multicast-routing
ip multicast-routing vrf REDES
!
!
interface GigabitEthernet0/0
 description CE2 - PE2
 ip vrf forwarding REDES
 ip address 192.168.2.2 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet0/1
 description CE2 - LAN2
 ip vrf forwarding REDES
 ip address 192.168.20.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  network 192.168.2.0
  network 192.168.20.0
  no auto-summary
  version 2
 exit-address-family
!
ip forward-protocol nd
!
ip pim vrf REDES rp-address 192.168.1.2 50
no ip http server
no ip http secure-server
!
!
access-list 50 permit 228.0.0.0 0.255.255.255
!
!
snmp-server community publicCE2 RO
snmp-server enable traps mvpn
!
control-plane
!
!
line con 0
 password cisco
```

```
 login
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

A.2.7 *Router* CE3

```
!
hostname CE3
!
!
no ipv6 cef
ip source-route
ip cef
!
!
ip vrf REDES
 route-target 200:200
 rd 200:200
!
ip multicast-routing
ip multicast-routing vrf REDES
!
!
no ip domain lookup
!
!
interface GigabitEthernet0/0
 description CE3 - PE3
 ip vrf forwarding REDES
 ip address 192.168.3.2 255.255.255.252
 ip pim sparse-mode
 duplex auto
 speed auto
 no shutdown
!
interface GigabitEthernet0/1
 description CE3 - LAN3
 ip vrf forwarding REDES
 ip address 192.168.30.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 no cdp enable
 no shutdown
!
!
router rip
 version 2
 !
 address-family ipv4 vrf REDES
  network 192.168.3.0
  network 192.168.30.0
  no auto-summary
  version 2
```

```
 exit-address-family
!
ip forward-protocol nd
!
ip pim vrf REDES rp-address 192.168.1.2 50
no ip http server
no ip http secure-server
!
!
access-list 50 permit 228.0.0.0 0.255.255.255
!
!
snmp-server community publicCE3 RO
snmp-server enable traps mvpn
!
control-plane
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

ANEXO B

MANUAL DE GENERACIÓN DE TRÁFICO UTILIZANDO JPERF

B.1 GENERACIÓN DE TRÁFICO *UNICAST* TCP……B-1

B.2 GENERACIÓN DE TRÁFICO *UNICAST* UDP……...…B-3

B.3 GENERACIÓN DE TRÁFICO *MULTICAST*……....B-4

B.1 GENERACIÓN DE TRÁFICO *UNICAST* TCP

B.1.1 Desde la fuente se inicializan dos sesiones de Jperf, una por cada receptor. Se selecciona el modo 'Cliente' (*Client*) y se ingresa la dirección IP del receptor en el campo 'dirección del servidor' (*Server address).* La primera sesión tendrá la dirección IP 192.168.20.20 con el puerto 5001, por defecto; y la segunda, la dirección IP 192.168.30.30 con el puerto 5002.

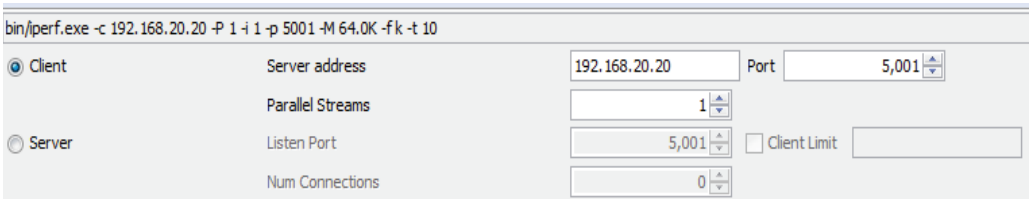

Figura B.1 Configuración del receptor 1

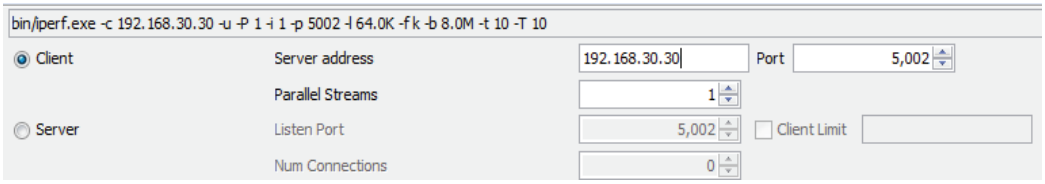

Figura B.2 Configuración del receptor 2

B.1.2 Posteriormente, desde cada receptor se apertura una sesión Jperf. Se selecciona el modo 'Servidor' (*Server*) y no se ingresa ninguna dirección IP. Lo que se escoge es el número de puerto de acuerdo al fijado para cada uno de los receptores. La primera sesión escuchará por el puerto 5001, y la segunda, por el puerto 5002.

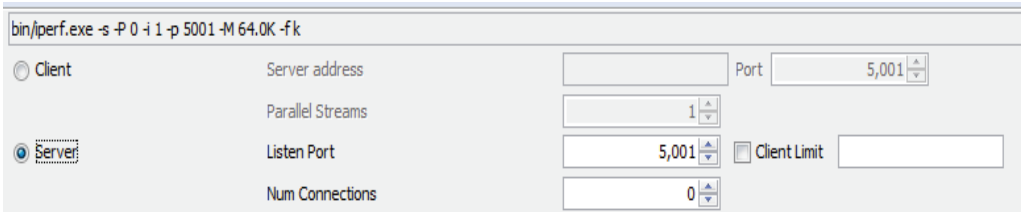

Figura B.3 Configuración del emisor para el receptor 1

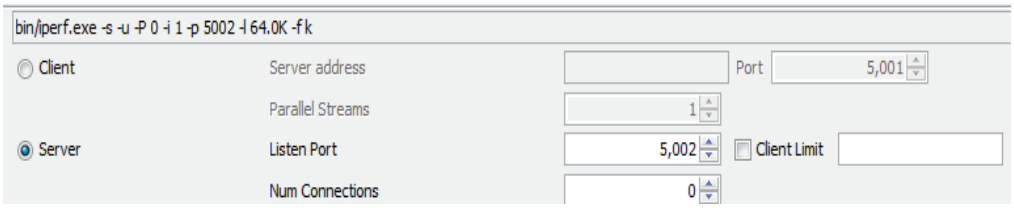

Figura B.4 Configuración del emisor para el receptor 2

B.1.3 Luego, en la parte correspondiente a 'Opciones de capa Transporte' (*Transport layer options*) de la fuente, se selecciona la opción TCP y se escoge el 'tamaño máximo del segmento' a transmitir (*Max segment size*). Para este ejemplo se coloca a 64 KBytes.

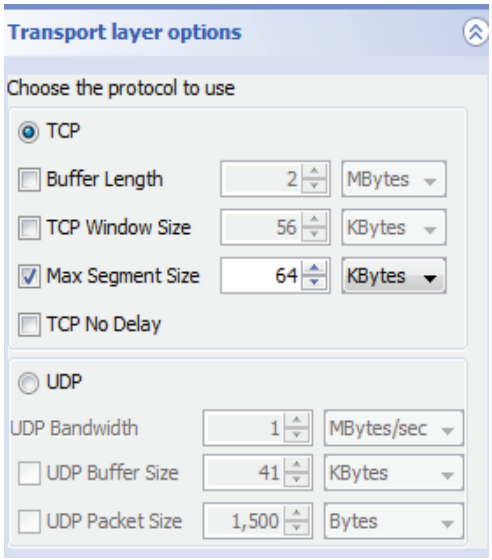

Figura B.5 Opciones a escoger para el protocolo TCP

B.1.4 Finalmente, para ejecutar el programa, se hace clic sobre '*Run IPerf*' tanto en los receptores como en la fuente, y se obtendrá en pantalla la forma de la señal a lo largo del tiempo. Además se visualizarán las estadísticas de

intervalos de tiempo, cantidad de información enviada/recibida en KBytes, y el ancho de banda enviado/recibido.

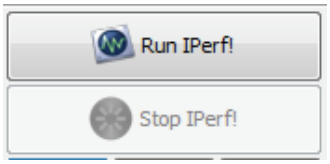

Figura B.6 Botón principal para ejecutar la generación de tráfico

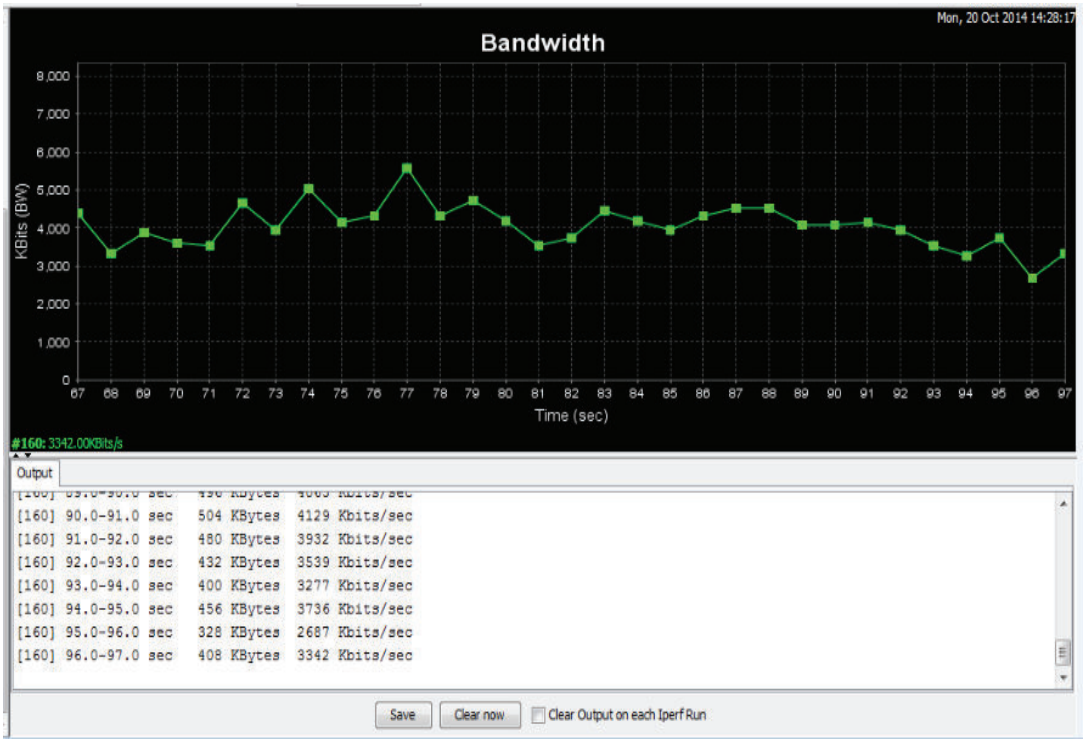

Figura B.7 Visualización del *throughput* del tráfico y sus estadísticas

B.2 GENERACIÓN DE TRÁFICO *UNICAST* UDP

B.2.1 Para este caso se repiten los dos primeros pasos correspondientes a la generación de tráfico unicast TCP.

B.2.2 Posteriormente, en la parte correspondiente a 'Opciones de capa Transporte' (*Transport layer options*) de la fuente, se selecciona la opción UDP y se escoge el 'tamaño del paquete UDP' a transmitir (*UDP packet size*). Para este ejemplo se coloca a 64 KBytes; además se fija el 'ancho de banda'

(*Bandwidth*) a 8 MBytes/sec; aunque en la práctica, Jperf expresa la unidad de medida del ancho de banda en Mbits/sec.

B.2.3 Luego, en la parte correspondiente a 'Opciones de capa IP' (*IP layer options*), se sitúa el valor del TTL (*Time To Live*) a 10, según el número de saltos que se quiera alcanzar hasta el destino.

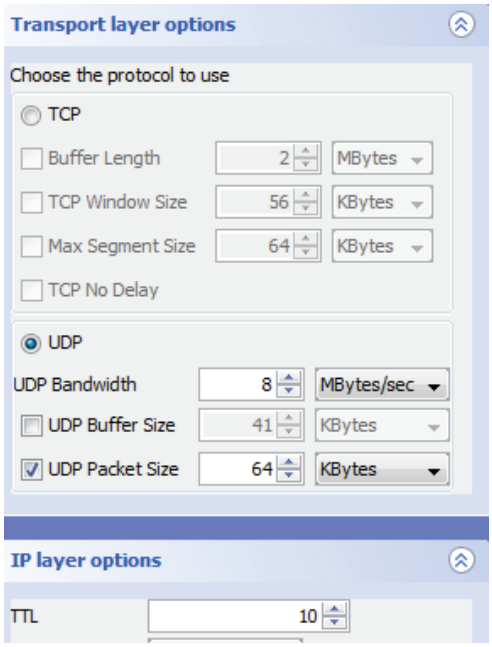

Figura B.8 Opciones a escoger para el protocolo UDP

B.2.4 Finalmente, para ejecutar el programa, se hace clic sobre '*Run IPerf*' tanto en los receptores como en la fuente, y se obtendrá en pantalla la forma de la señal a lo largo del tiempo. Además se visualizarán las estadísticas de intervalos de tiempo, cantidad de información enviada/recibida en KBytes, el ancho de banda enviado/recibido, el *jitter* expresado en milisegundos y el porcentaje de paquetes perdidos.

B.3 GENERACIÓN DE TRÁFICO *MULTICAST*

B.3.1 Desde la fuente se inicializan dos sesiones de Jperf, una por cada receptor. Se selecciona el modo 'Cliente' (*Client*) y se ingresa la dirección IP del grupo *multicast* en el campo 'dirección del servidor' (*Server address).* Ambas sesiones tendrán la dirección IP 228.1.1.1 con el puerto 5001, por defecto.

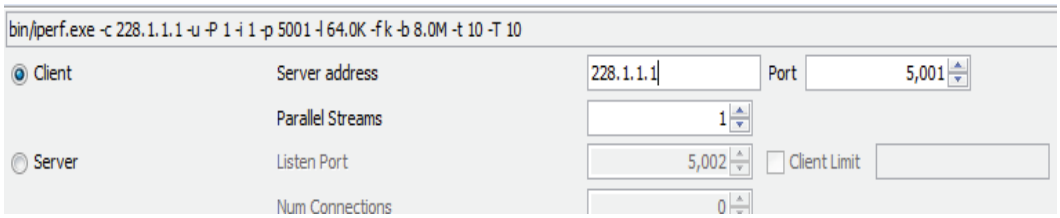

Figura B.9 Configuración del receptor *multicast*

B.3.2 Posteriormente, desde cada receptor se apertura una sesión Jperf. Se selecciona el modo 'Servidor' (*Server*) y no se ingresa ninguna dirección IP. Lo que se escoge es el número de puerto, que por defecto es el 5001. En la parte de 'Opciones de capa IP' (*IP layer options*), se asocia al receptor al grupo *multicast* 228.1.1.1 en el campo 'Asociar al *Host*' (*Bind to Host*).

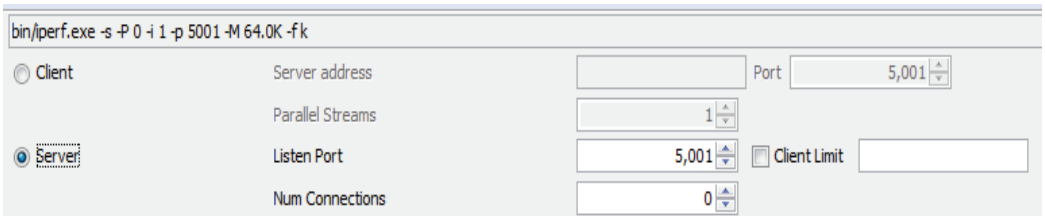

Figura B.10 Configuración del emisor *multicast*

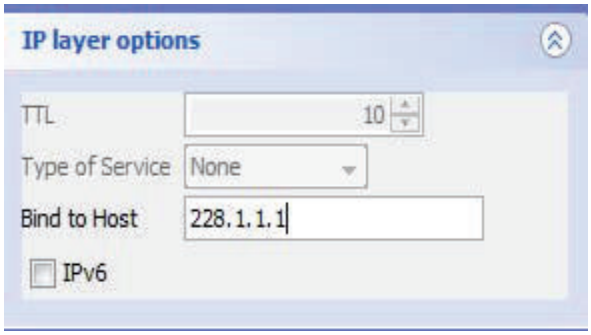

Figura B.11 Configuración de la dirección del grupo *multicast*

B.3.3 Luego, en la parte que corresponde a 'Opciones de capa Transporte' (*Transport layer options*) de la fuente, se selecciona la opción UDP y se escoge el 'tamaño del paquete UDP' a transmitir (*UDP packet size*). Para este ejemplo se coloca a 64 KBytes; además se fija el 'ancho de banda' (*Bandwidth*) a 8 MBytes/sec; aunque en la práctica, Jperf expresa la unidad de medida del ancho de banda en Mbits/sec.

B.3.4 Además, en la parte correspondiente a 'Opciones de capa IP' (*IP layer options*), se sitúa el valor del TTL (*Time To Live*) a 10, según el número de saltos que se quiera alcanzar hasta el destino.

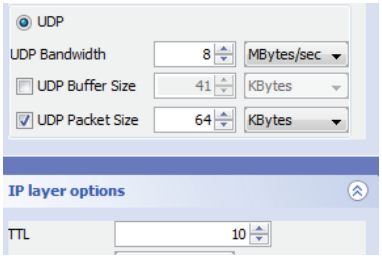

Figura B.12 Configuración del valor de TTL

B.3.5 Finalmente, para ejecutar el programa, se hace clic sobre '*Run IPerf*' tanto en los receptores como en la fuente, y se obtendrá en pantalla la forma de la señal a lo largo del tiempo. Además se visualizarán las estadísticas de intervalos de tiempo, cantidad de información enviada/recibida en KBytes, el ancho de banda enviado/recibido, el *jitter* expresado en milisegundos y el porcentaje de paquetes perdidos.

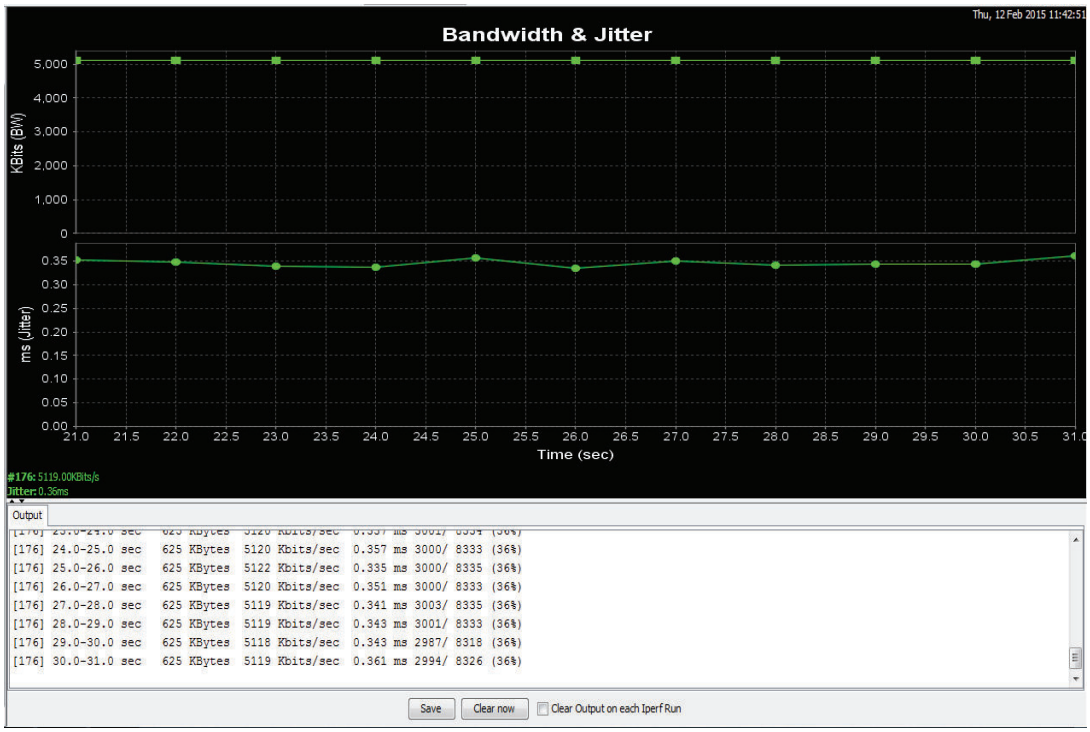

Figura B.13 Visualización del *throughput* y *jitter* del tráfico y sus estadísticas en el receptor

ANEXO C

MANUAL DE EMISIÓN DE VIDEO UTILIZANDO VLC

C.1 EMISIÓN DE VIDEO *UNICAST*……..C-1

C.2 EMISIÓN DE VIDEO *MULTICAST*……C-4

C.1 EMISIÓN DE VIDEO *UNICAST*

C.1.1 Desde la fuente se abren dos sesiones de emisión de video VLC, una por cada receptor. Se selecciona 'Medio' y luego 'Emitir'. Posteriormente se agrega el archivo de video que se desea transmitir.

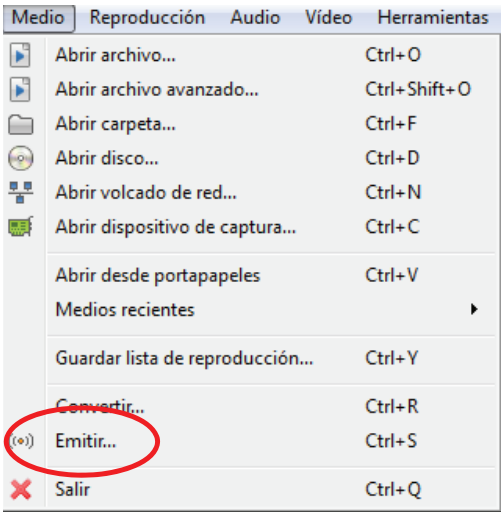

Figura C.1 Opción 'Emitir' de la fuente

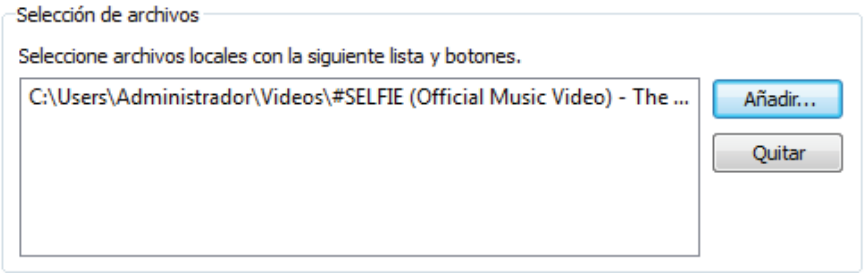

Figura C.2 Selección del archivo a emitir

C.1.2 Se escoge un protocolo para la transmisión de video, ya sea RTP o UDP. Se deshabilita los dos casilleros correspondientes a 'Mostrar en local' y 'Habilitar

transcodificar'; ya que por defecto, en la fuente, no se visualiza el video y, además, no es necesario transcodificar el video elegido para transmitir.

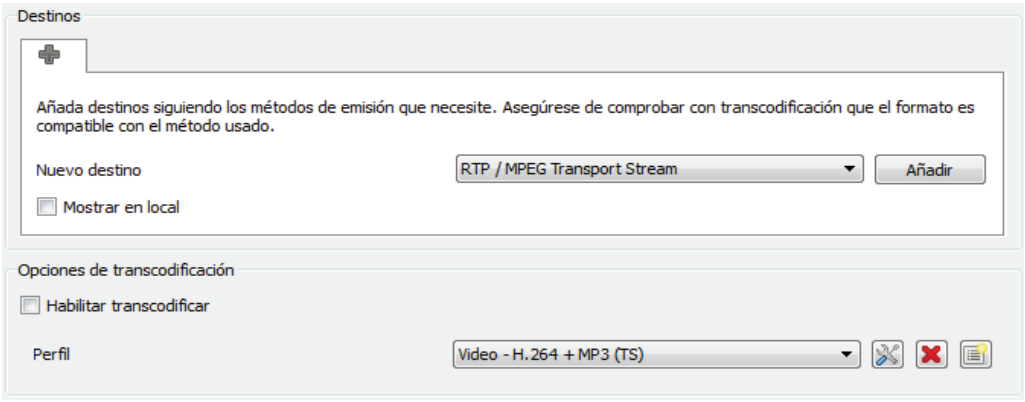

Figura C.3 Protocolos de emisión y opciones de transcodificación

C.1.3 Se introducen las direcciones IP 192.168.20.20 y 192.168.30.30. El número de puerto que utiliza RTP en VLC, por defecto, es el 5004.

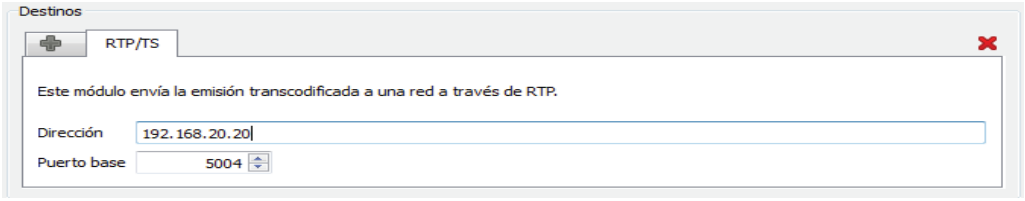

Figura C.4 Configuración del receptor 1

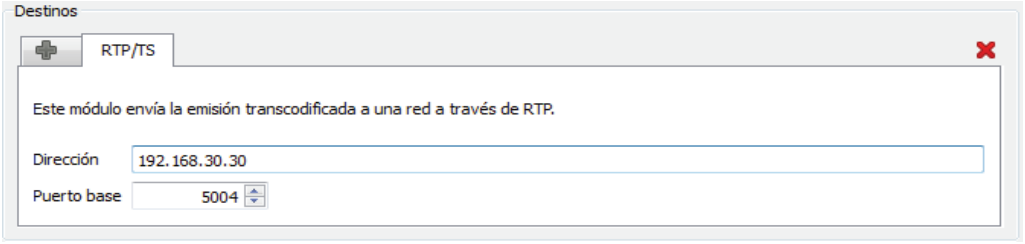

Figura C.5 Configuración del receptor 2

C.1.4 El valor de TTL se lo fija a 10, dependiendo del número de saltos que son necesarios para llegar al receptor.

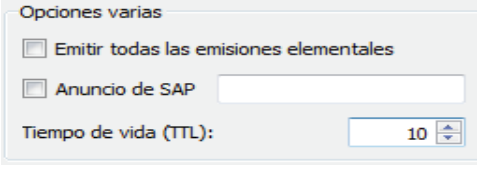

Figura C.6 Configuración del valor de TTL

C.1.5 Finalmente, se selecciona el botón ‘Emitir’ para iniciar la transmisión de video.

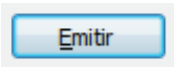

Figura C.7 Botón principal para ejecutar la emisión de video

C.1.6 Por otro lado, desde cada receptor, se selecciona ‘Medio’ y luego ‘Abrir volcado de red’.

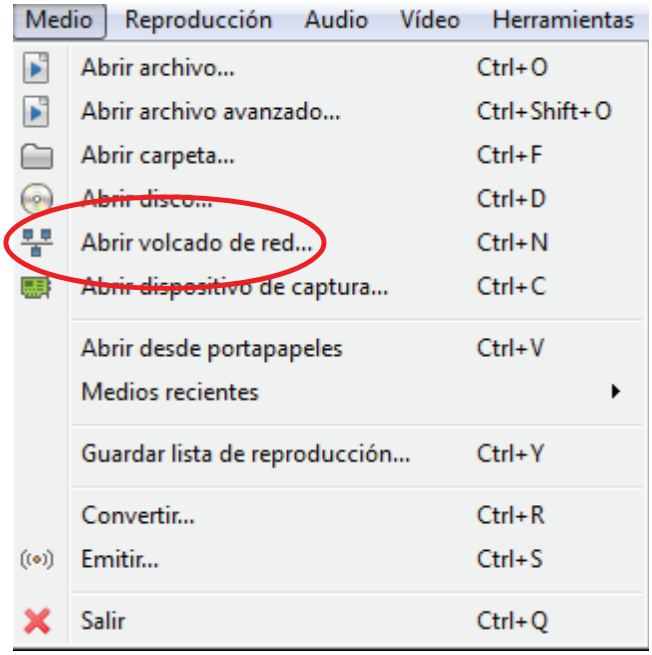

Figura C.8 Opción ‘Abrir volcado de red’ del lado del receptor

C.1.7 Posteriormente se agrega el número del puerto RTP, 5004, por el cual se va a recibir el video, y se selecciona el botón ‘Reproducir’.

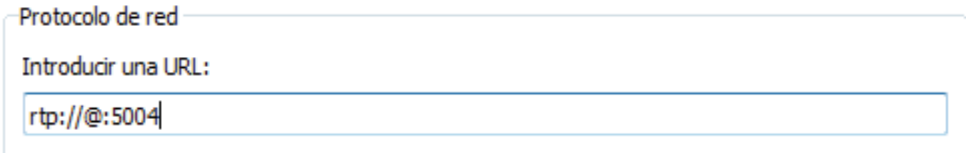

Figura C.9 Configuración del protocolo y puerto por el que se recibe el video *unicast*

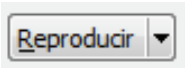

Figura C.10 Botón principal para recibir o reproducir el video

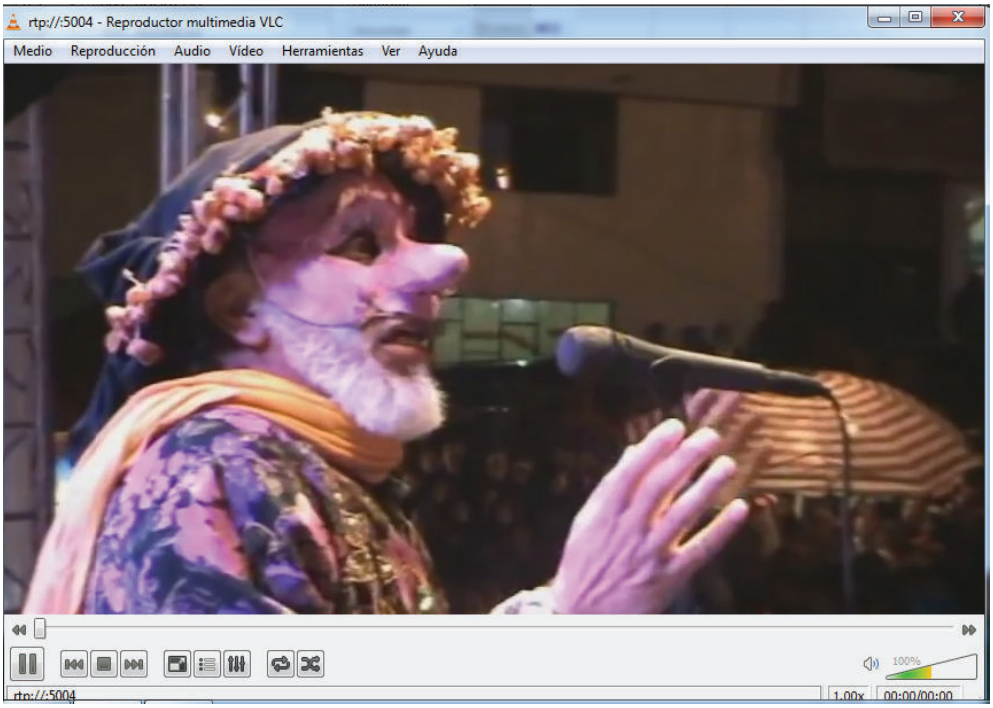

Figura C.11 Reproducción del video *unicast*

C.2 EMISIÓN DE VIDEO *MULTICAST*

C.2.1 Desde la fuente se abren una única sesión de emisión de video VLC, para el grupo multicast. A continuación se procede a seguir con los dos primeros pasos de la emisión de video unicast. Una vez escogido el protocolo para la emisión de video, se introduce la dirección IP del grupo multicast 228.1.1.1, con el mismo puerto por defecto.

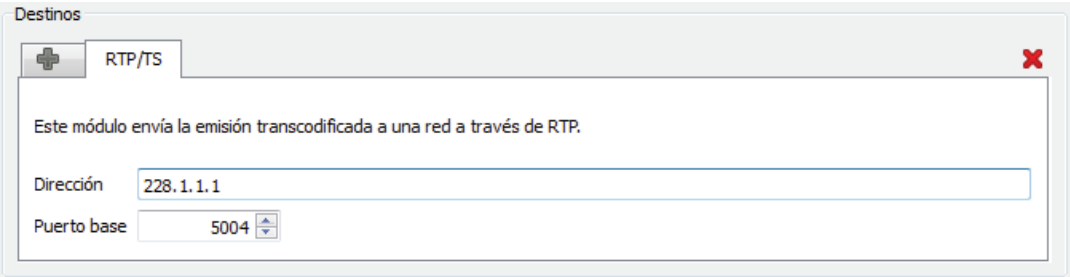

Figura C.12 Configuración del receptor *multicast*

C.2.2 De la misma manera, se repiten los pasos 4, 5 y 6. Finalmente, para recibir el video desde cada receptor, se ingresa la dirección IP conjuntamente con el número de puerto RTP.

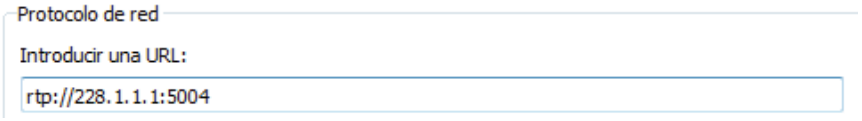

Figura C.13 Configuración del protocolo y puerto por el que se recibe el video *multicast*

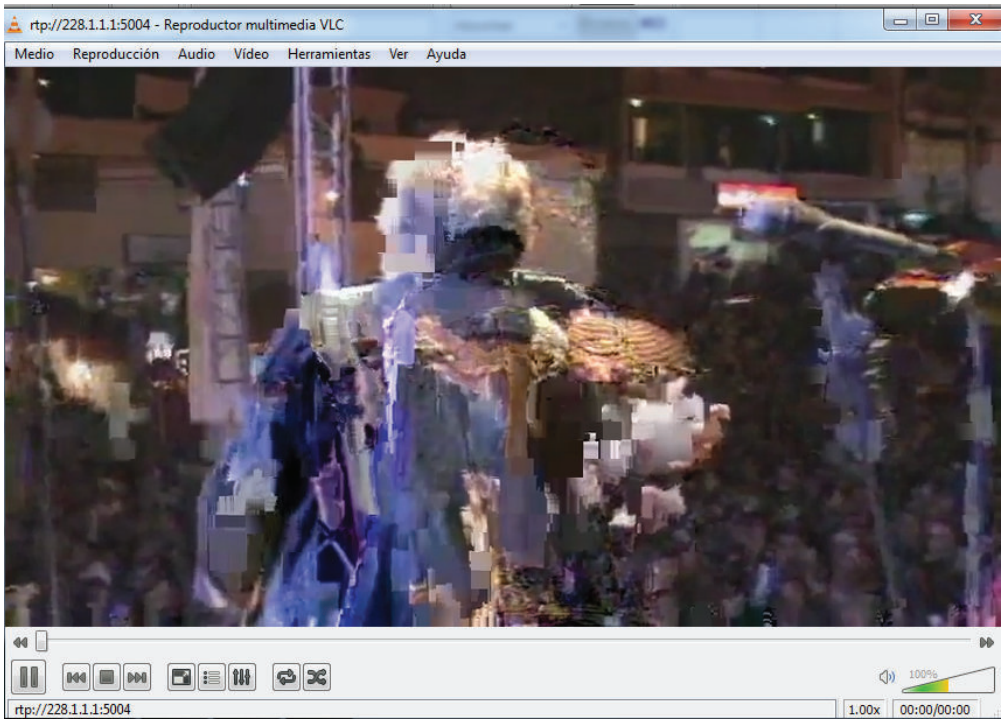

Figura C.14 Reproducción del video *multicast*

ANEXO D

TABULADOS CORRESPONDIENTES A LA GENERACIÓN DE TRÁFICO *UNICAST* Y *MULTICAST* CON JPERF Y VLC

D.1 GENERACIÓN DE TRÁFICO *UNICAST* TCP……D-1

D.2 GENERACIÓN DE TRÁFICO *UNICAST* UDP……D-2

D.3 GENERACIÓN DE TRÁFICO *MULTICAST*……....D-8

D.4 EMISIÓN DE VIDEO *UNICAST* …..……...…D-14

D.5 EMISIÓN DE VIDEO *MULTICAST*……..……..…D-14

D.1 GENERACIÓN DE TRÁFICO *UNICAST* TCP

Payload	Tamaño [KB]	*Throughput* [Kb/s]	Paquetes generados	Paquetes recibidos
64 bytes	48634	3984	779	760
128 bytes	49727	4000	398	389
256 bytes	48600	3981	195	190
512 bytes	49820	4000	100	94
1024 bytes	48408	3965	49	48
1400 bytes	48088	3939	36	35

Tabla D.1 Promedio de los parámetros estudiados en la generación de tráfico *unicast* TCP con Jperf

D.2 GENERACIÓN DE TRÁFICO *UNICAST* UDP

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2275	0,014	943	5858	16,0
Máximo	2524	0,389	1535	5978	26,0
Media	2398,9	0,14	1201	5886	20,5
Mediana	2397	0,084	1188	5875	20,0
Desv. Est.	63,3	0,13	135,75	34,65	2,3

Tabla D.2 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 64 B @ 3 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2805	0	0	2914	0,0
Máximo	3085	1,088	189	3015	6,5
Media	2991	0,356	13,4	2934,1	0,5
Mediana	2995	0,315	4	2928	0,1
Desv. Est.	42,59	0,27	37,86	20,35	1,3

Tabla D.3 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 128 B @ 3 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2806	0	0	1442	0,0
Máximo	3045	1,622	91	1487	6,2
Media	2995	0,945	3,7	1465,9	0,3
Mediana	2998	1,149	0	1464	0,0
Desv. Est.	41,71	0,61	16,89	9,89	1,2

Tabla D.4 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 256 B @ 3 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2839	1,841	0	712	0,0
Máximo	3043	3,146	29	743	4,0
Media	2994	2,657	1,6	732,6	0,2
Mediana	2998	2,69	0	732	0,0
Desv. Est.	40,68	0,29	6,22	5,47	0,9

Tabla D.5 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 512 B @ 3 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2933	3,103	0	364	0,0
Máximo	3039	5,815	13	371	3,5
Media	2998	5,199	0,4	366,4	0,1
Mediana	2998	5,46	0	366	0,0
Desv. Est.	19,01	0,71	2,37	1,98	0,6

Tabla D.6 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 1024 B @ 3 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2979	3,108	0	266	0,0
Máximo	3058	7,883	0	273	0,0
Media	3002	6,831	0	268,0	0,0
Mediana	3002	7,08	0	268	0,0
Desv. Est.	19,13	0,96	0	1,69	0,0

Tabla D.7 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 1400 B @ 3 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2111	0,018	2945	7659	38,0
Máximo	2523	0,128	3535	7937	46,0
Media	2358,4	0,043	3198	7804,5	41,0
Mediana	2352	0,04	3212	7803	41,0
Desv. Est.	82,32	0,02	139,28	62,64	1,9

Tabla D.8 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 64 B @ 4 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2806	0,095	829	3845	21,0
Máximo	3143	0,278	1160	3963	30,0
Media	2990,8	0,175	986	3906,3	25,2
Mediana	2992,5	0,181	981	3900	25,0
Desv. Est.	79,9	0,04	76,36	24,08	2,1

Tabla D.9 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 128 B @ 4 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3351	0,045	219	1926	11,0
Máximo	3598	1,104	316	2027	16,0
Media	3445,8	0,563	275	1954,8	14,1
Mediana	3430,5	0,568	274	1951,5	14,0
Desv. Est.	61,66	0,22	24,47	17,61	1,4

Tabla D.10 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 256 B @ 4 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3588	1,319	17	969	1,6
Máximo	4260	2,384	100	1057	10,0
Media	3727,2	2,000	69	979,3	7,1
Mediana	3707	2,11	69	976	7,1
Desv. Est.	108,26	0,32	12,71	15,77	1,3

Tabla D.11 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 512 B @ 4 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3809	1,05	11	484	2,3
Máximo	3957	4,036	21	496	4,3
Media	3875,8	3,452	15	488,4	3,1
Mediana	3871	3,554	15	488	3,1
Desv. Est.	32,10	0,60	2,91	3,08	0,6

Tabla D.12 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 1024 B @ 4 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3864	1,659	0	348	0,0
Máximo	4917	5,812	12	439	3,4
Media	3947,3	4,326	7	359,4	1,9
Mediana	3909	4,664	8	357	2,2
Desv. Est.	185,64	1,18	3,74	15,33	1,1

Tabla D.13 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 1400 B @ 4 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2268	0,03	4718	9639	48,0
Máximo	2597	1,046	5346	9974	55,0
Media	2403,9	0,241	5110	9804,7	52,1
Mediana	2391,5	0,109	5131	9791	52,5
Desv. Est.	76,33	0,26	154,89	64,43	1,6

Tabla D.14 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 64 B @ 5 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	2711	0	1407	4886	28,0
Máximo	3669	1,04	2246	4990	46,0
Media	3008,3	0,590	1962	4904,5	40,1
Mediana	3003	0,464	1955	4894	40,0
Desv. Est.	176,57	0,32	163,76	29,03	3,4

Tabla D.15 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 128 B @ 5 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3099	0	563	2390	23,0
Máximo	3846	1,764	923	2486	38,0
Media	3391,3	0,504	789	2444,8	32,2
Mediana	3353	0,546	805	2443	33,0
Desv. Est.	181,70	0,41	91,56	18,60	3,8

Tabla D.16 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 256 B @ 5 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3387	0	230	1217	17,0
Máximo	4489	2,383	392	1326	32,0
Media	3723,7	1,775	316	1225,4	25,7
Mediana	3729	1,817	321	1220	26,0
Desv. Est.	176,28	0,41	29,82	19,99	2,6

Tabla D.17 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 512 B @ 5 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3760	1,078	116	603	19,0
Máximo	4178	50,18	200	710	28,0
Media	3873,1	3,733	142	614,4	23,0
Mediana	3846	3,771	142	611	23,0
Desv. Est.	91,26	0,63	14,48	18,67	1,9

Tabla D.18 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 1024 B @ 5 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	3494	2,809	57	444	12,0
Máximo	5410	6,738	134	547	30,0
Media	3957,7	5,277	97	450,0	21,5
Mediana	3959	5,13	92	446	20,5
Desv. Est.	401,75	0,88	26,68	18,52	6,0

Tabla D.19 Valores estadísticos de los parámetros estudiados en la generación de tráfico *unicast* UDP con 1400 B @ 5 Mb/s

D.3 GENERACIÓN DE TRÁFICO *MULTICAST*

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	4151	0,042	3617	11743	31,0
Máximo	4226	0,252	3683	11930	31,0
Media	4166,9	0,090	3632	11770,7	31,0
Mediana	4158,5	0,05	3627	11746	31,0
Desv. Est.	22,97	0,07	19,65	63,37	0,0

Tabla D.20 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 64 B @ 6 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5381	0,553	516	5871	8,8
Máximo	5572	0,984	619	5965	11,0
Media	5491,8	0,827	522	5885,4	8,9
Mediana	5484,5	0,865	519	5873	8,8
Desv. Est.	36,84	0,10	18,42	31,50	0,4

Tabla D.21 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 128 B @ 6 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5992	0,168	0	2926	0,0
Máximo	6091	0,279	0	2974	0,0
Media	6009	0,235	0	2933,9	0,0
Mediana	5997	0,245	0	2928	0,0
Desv. Est.	32,55	0,04	0	15,88	0,0

Tabla D.22 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 256 B @ 6 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5919	0,726	0	1463	0,0
Máximo	6095	0,883	19	1488	1,3
Media	6000	0,809	2,27	1467	0,2
Mediana	5997	0,816	0	1464	0,0
Desv. Est.	42,38	0,03	5,38	7,97	0,4

Tabla D.23 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 512 B @ 6 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5792	0,308	0	731	0,0
Máximo	6087	2,196	25	743	3,4
Media	5967	1,896	4,70	733	0,6
Mediana	5988	2,09	1	732	0,1
Desv. Est.	61,68	0,51	6,90	3,99	0,9

Tabla D.24 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 1024 B @ 6 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5869	3,083	0	535	0,0
Máximo	6082	3,332	18	544	3,3
Media	5974	3,177	3,3	536	0,6
Mediana	5992	3,169	0	535	0,0
Desv. Est.	47,64	0,08	4,90	3,10	0,9

Tabla D.25 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 1400 B @ 6 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	4036	0,002	7479	15595	48,0
Máximo	4222	0,019	7720	15845	49,0
Media	4160	0,008	7507,7	15633	48,0
Mediana	4156	0,005	7483	15601	48,0
Desv. Est.	31,04	0,01	61,59	84,26	0,2

Tabla D.26 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 64 B @ 8 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5328	0	2439	7793	31,0
Máximo	5570	0,984	2597	7923	33,0
Media	5480	0,272	2465,2	7816	31,3
Mediana	5484	0,129	2448	7800	31,0
Desv. Est.	39,56	0,34	39,34	41,72	0,5

Tabla D.27 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 128 B @ 8 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	6402	0,576	713	3899	18,0
Máximo	6629	0,94	773	3962	20,0
Media	6532	0,804	718,5	3908	18,1
Mediana	6525	0,852	714	3900	18,0
Desv. Est.	44,36	0,11	11,69	21,37	0,4

Tabla D.28 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 256 B @ 8 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	7062	0,511	190	1949	9,7
Máximo	7324	0,831	225	1981	12,0
Media	7210	0,674	193,9	1654	9,9
Mediana	7207	0,664	191	1950	9,8
Desv. Est.	46,92	0,12	8,73	10,35	0,5

Tabla D.29 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 512 B @ 8 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	7602	1,829	45	973	4,6
Máximo	7725	2,169	48	991	4,8
Media	7622	2,010	46,7	977	4,8
Mediana	7610	2,03	47	976	4,8
Desv. Est.	41,21	0,09	0,70	5,40	0,1

Tabla D.30 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 1024 B @ 8 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	7717	2,037	23	712	3,2
Máximo	7840	2,963	27	724	3,8
Media	7736	2,618	23,9	715	3,4
Mediana	7717	2,589	24	713	3,4
Desv. Est.	41,88	0,24	1,05	3,9	0,2

Tabla D.31 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 1400 B @ 8 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	4157	0	11445	19567	58,0
Máximo	4227	0,007	11635	19891	59,0
Media	4169	0,003	11476,6	19618	58,5
Mediana	4160	0,003	11454	19577	58,0
Desv. Est.	23,17	0,002	61,76	106,73	0,5

Tabla D.32 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 64 B @ 10 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	5431	0,01	4430	9782	45,0
Máximo	5569	0,015	4514	9945	46,0
Media	5490	0,013	4451,8	9816	45,1
Mediana	5482	0,013	4439	9793	45,0
Desv. Est.	32,61	0,001	28,08	57,62	0,3

Tabla D.33 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 128 B @ 10 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	6296	0,19	1707	4893	35,0
Máximo	6627	0,276	1821	4971	37,0
Media	6494	0,232	1733,4	1904	35,4
Mediana	6522	0,233	1719	4894	35,0
Desv. Est.	70,40	0,018	31,10	26,33	0,6

Tabla D.34 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 256 B @ 10 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	7127	0,574	681	2440	28,0
Máximo	7320	0,696	721	2480	29,0
Media	7207	0,658	686,7	2446	28,1
Mediana	7205	0,659	682	2441	28,0
Desv. Est.	37,42	0,033	8,67	12,95	0,3

Tabla D.35 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 512 B @ 10 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	7266	1,883	289	1217	24,0
Máximo	7725	2,277	350	1239	28,0
Media	7534	2,070	301,7	1221	24,7
Mediana	7561	2,065	296	1219	24,0
Desv. Est.	96,08	0,130	14,42	6,66	1,1

Tabla D.36 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 1024 B @ 10 Mb/s

	Throughput [Kb/s]	*Jitter* [ms]	Paquetes perdidos	Paquetes generados	Porcentaje pérdida de paquetes [%]
Mínimo	7426	2,195	201	890	23,0
Máximo	7840	2,879	229	907	26,0
Media	7685	2,528	207,1	893	23,4
Mediana	7717	2,494	203	891	23,0
Desv. Est.	101,35	0,240	8,08	5,20	0,8

Tabla D.37 Valores estadísticos de los parámetros estudiados en la generación de tráfico *multicast* con 1400 B @ 10 Mb/s

D.4 EMISIÓN DE VIDEO *UNICAST*

	Payload	Throughput [bps]	Paquetes generados [pps]	Paquetes perdidos [pps]	Jitter [us]
Mínimo	188	210580	115,4	0	4
Máximo	188	282310	187,7	0	12
Promedio	188	246308	158,8	0	6,6
Mediana	188	239986	158,2	0	5,9
Desv. Est.	0	17830,6	18,36	0	2,5

Tabla D.38 Valores estadísticos de los parámetros estudiados en la emisión de video *unicast* con VLC

D.5 EMISIÓN DE VIDEO *MULTICAST*

	Payload	Throughput [bps]	Paquetes generados [pps]	Paquetes perdidos [pps]	Jitter [us]
Mínimo	188	211312	140,5	0	7,8
Máximo	188	308066	204,6	0	14,8
Promedio	188	248017	164,9	0	10,8
Mediana	188	245944	163,5	0	10,6
Desv. Est.	0	23388,5	15,48	0	1,7

Tabla D.39 Valores estadísticos de los parámetros estudiados en la emisión de video *multicast* con VLC

ANEXO E

MANUAL DE ANÁLISIS DE DATOS CON SPSS *STATISTICS*

E.1 CÁLCULO DE CORRELACIONES……E-1

E.1 CÁLCULO DE CORRELACIONES

E.1.1 Para obtener el coeficiente de correlación de Spearman en este programa, se dirige al menú ‘Analizar’, ‘Correlaciones’ y luego en ‘Bivariadas’ ya que se trata de dos variables a estudiar.

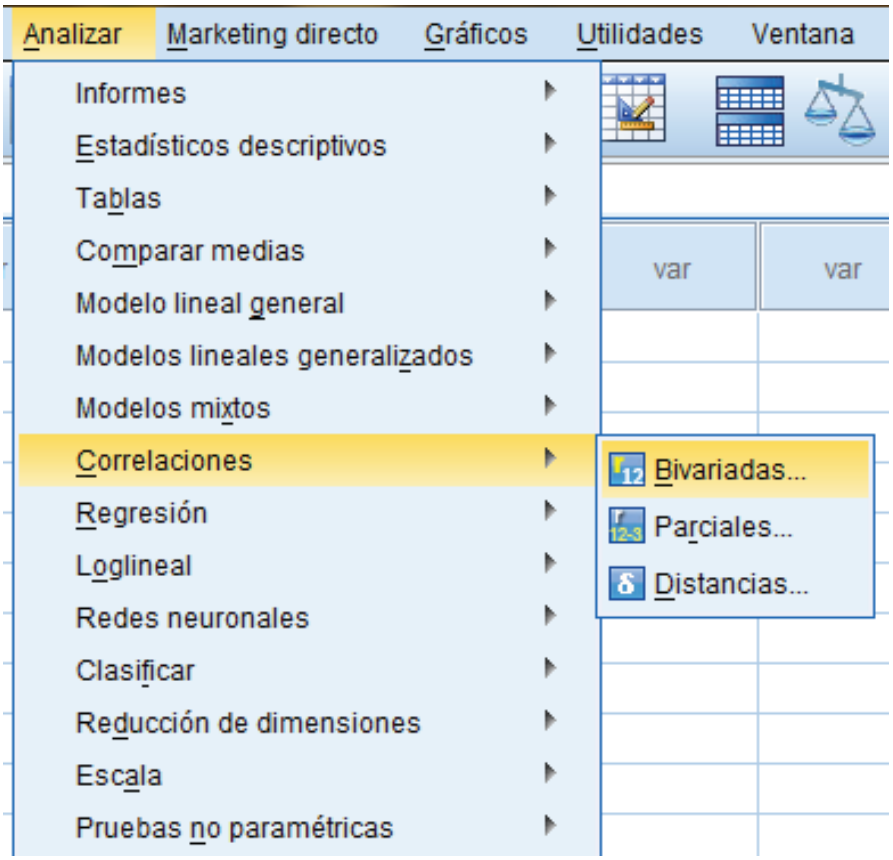

Figura E.1 Menú de opciones en la opción ‘Analizar’

E.1.2 A continuación se ingresan las dos variables a tratar, que en este caso son el *jitter* extremo a extremo y el tiempo de permanencia en el sistema. Además se selecciona la casilla ‘Spearman’ para obtener su correlación.

Figura E.2 Ventana donde se escoge las variables a analizar dentro de la correlación de Spearman

E.1.3 Finalmente se obtiene tanto el factor de correlación *Rho* de Spearman, así como el valor de probabilidad, de acuerdo al criterio de las hipótesis planteadas.

Correlaciones

			JITTER	PERMANENCIA
Rho de Spearman	JITTER	Coeficiente de correlación	1,000	,829*
		Sig. (bilateral)	.	,042
		N	6	6
	PERMANENCIA	Coeficiente de correlación	,829*	1,000
		Sig. (bilateral)	,042	.
		N	6	6

*. La correlación es significativa en el nivel 0,05 (2 colas).

Tabla E.1 Obtención de los resultados en base de las variables JITTER y PERMANENCIA