PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIONES

ANÁLISIS DE RENDIMIENTO DE TRÁFICO MULTICAST EN REDES IPv4 E IPv6

SILVA CASTELLANOS DIEGO FERNANDO

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN REDES DE COMUNICACIONES

Quito, octubre de 2016

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO I. INTRODUCCIÓN

1.1 INTRODUCCIÓN

Multicast es una tecnología de conservación de ancho de banda que permite reducir el tráfico mediante el envío de paquetes a un conjunto de hosts establecidos en un grupo, en lugar de tener que enviar los paquetes a cada usuario de manera individual. Con esto se logra enviar el tráfico de aplicaciones utilizando el mínimo ancho de banda y evitando la sobrecarga de los servidores fuente de tráfico permitiendo desplegar aplicaciones escalables y económicas.

Cada vez más proveedores de servicios de internet se van sumando a la implementación de multicast en su infraestructura de red con el objetivo de proveer conexión y servicios de multicast, siendo en la actualidad la difusión de video con el servicio de IPTV o las conferencias multimedia, las aplicaciones más populares y con las cuales la gente relaciona en primera instancia al hablar de multicast. Debido a que en la actualidad internet va siendo cada vez más fácil de acceder y de una manera rápida y eficiente, las aplicaciones multicast no se limitan a las descritas con anterioridad. Hoy en día las aplicaciones multicast incluyen la radio por internet, difusión de cotizaciones de la bolsa y el comercio de acciones, publicidad, juegos en línea, emisión de películas y conciertos. Sin embargo, los servicios de multicast no solo pueden ser empleados con fines de entretenimiento. Otras áreas de aplicación son, entre otras, educación, salud, comunicaciones corporativas, vigilancia, vigilancia y cuidado de niños y la milicia.

1.2 ANTECEDENTES

A principios de los años 80 en la Universidad de Stanford, el estudiante de doctorado Steve Deering trabajaba en un proyecto de un sistema operativo distribuido para comunicar varias máquinas de multiprocesamiento acoplado interconectadas por un solo segmento ethernet. Las máquinas eran capaces de trabajar en conjunto a través del segmento de red intercambiando, a nivel de sistema operativo, mensajes especiales. Uno de los sistemas operativos primitivos permitía que una computadora enviara mensajes a un grupo de computadoras mediante mensajes multicast de la capa MAC.

A media que el proyecto fue progresando, hubo la necesidad de incluir más computadoras. Sin embargo, las computadoras disponibles se encontraban en otro sitio del campus separadas por routers, es decir, en otros segmentos de red. Por lo tanto, la capacidad multiprocesamiento que se venía realizando en capa 2 del modelo OSI se la debía trasladar a la capa 3. Luego de estudiar los protocolos OSPF y RIP, el Dr. Deering concluye que los mecanismos de estado de enlace de OSPF puede brindar soporte para extender la comunicación multicast. Además, visualiza que los mecanismos básicos de RIP pueden ser usados como base para un nuevo protocolo de enrutamiento multicast basado en la métrica de vector-distancia. Esta idea se convierte en su tesis doctoral denominada como *"Multicast Routing in a Datagram Network",* publicada en diciembre de 1991. En esta tesis, el Dr. Deering describe las bases de un protocolo de membresía de host, lo que llegó a convertirse en la base del protocolo IGMP. También describe un protocolo de enrutamiento de multicast de

vector distancia, el cual fue la base del protocolo *Distance Vector Multicast Routing Protocol (DVMRP).*

Posterior a estos acontecimientos, se han realizado avances en la tecnología IP multicast, tal es el caso de *Protocol Independent Multicast (PIM)* y varias extensiones de *Border Gateway Protocol (BGP).* Estos protocolos permiten extender a multicast a la capa 3 del modelo OSI superando así las limitaciones iniciales y poder ejecutar multicast a través de internet.

1.3 JUSTIFICACIÓN

Con el consabido agotamiento del direccionamiento de IPv4, se hace cada vez más necesario la implementación a nivel mundial de la siguiente generación del protocolo IP, es decir, IPv6. Dada esta transición, el reto de los proveedores de servicios de internet está en ofrecer servicios sobre redes y plataformas de IPv6 a usuarios conectados con terminales y redes IPv4, por consiguiente, los servicios de multicast IPv4 los cuales son parte del llamado “servicio de Internet IPv4” deben ser mantenidos. Tal es así que en el evento del IETF 82 en noviembre de 2011, proveedores de servicios de internet, académicos y fabricantes expusieron la necesidad de la continuidad del servicio de multicast IPv4.

En la actualidad existen varios estudios de las tecnologías de transición y convivencia de IPv4 e IPv6 en cuanto a rendimiento, capacidad, interoperabilidad y demás. Dichos estudios, sin embargo, están diseñados y realizados para tráfico

unicast. Dada la importancia de la coexistencia de redes IPv4 e IPv6, en este proyecto se plantea el estudio del rendimiento del enrutamiento de tráfico de multicast IPv4 e IPv6, con el cual se pretende evaluar a dichos protocolos con la finalidad de realizar diseños de red híbridos (con redes Dual Stack) más eficientes para la entrega de servicios multicast.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Evaluar y comparar el rendimiento que el enrutamiento de tráfico multicast presenta en redes IPv4 e IPv6, mediante la experimentación con tráfico simulado y tráfico real.

1.4.2 OBJETIVOS ESPECÍFICOS

- Describir los fundamentos del tráfico de multicast en redes IPv4 e IPv6.
- Describir los mecanismos de coexistencia e interoperabilidad para el tráfico multicast entre redes IPv4 e IPv6.
- Analizar y comparar el rendimiento de una red de datos dual stack IPv4-IPv6 mediante la generación y evaluación de tráfico real de video y tráfico simulado, tanto con emisiones multicast IPv4, así como con emisiones multicast IPv6.

1.5 RESUMEN DEL CONTENIDO DE LOS CAPÍTULOS

En el capítulo primero se describen la introducción, antecedentes, justificación y objetivos de la tesis.

En el capítulo segundo se describen los fundamentos de la comunicación multicast. Se empieza por describir las nociones de la comunicación multicast junto con sus ventajas, desventajas y aplicaciones más usadas en la actualidad. A continuación, se detallan las direcciones de multicast tanto de IPv4 como de IPv6, haciendo referencia a sus formatos, rangos y usos. Luego se procede a explicar los protocolos de membresía de multicast IPv4 e IPv6, IGMP y MLD respectivamente, analizando las versiones que tienen cada uno de los mencionados protocolos. Seguidamente el trabajo se centra en detallar los fundamentos de enrutamiento de multicast, revisando los árboles de distribución, el método de reenvío de path reverso para evitar loops en la red y analizando el protocolo de enrutamiento PIM junto con sus versiones principales como son PIM-SM, PIM-DM, PIM-SSM y Bidir-PIM. Por último, se realiza la revisión de las tecnologías y mecanismos principales existentes para la interacción y transición de multicast IPv4 a IPv6.

En el capítulo tercero se examinan en primera instancia los parámetros que permiten analizar y evaluar el rendimiento de las redes de datos. Estos parámetros son la latencia, pérdida de paquetes, jitter, tasa de transferencia de datos y throughput. Posteriormente se realiza una descripción de las herramientas a ser utilizadas para la evaluación de los parámetros de rendimiento de red descritos con anterioridad. Las mencionadas herramientas son, el reproductor de video multimedia

VLC, el analizador de protocolos Wireshark y el generador de tráfico JPERF. Finalmente, se describe la topología de red a ser utilizada en la evaluación del rendimiento de multicast IPv4 e IPv6 junto con los escenarios que serán puestos a prueba, tanto para tráfico simulado y controlado, como para tráfico real de video.

En el capítulo cuarto se presentan, describen y analizan los resultados experimentales obtenidos en las pruebas efectuadas con la topología de red y escenarios propuestos descritos en el capítulo tercero.

En el capítulo quinto se emiten conclusiones y se realizan recomendaciones acerca de los resultados de las pruebas experimentales realizadas.

CAPÍTULO II. FUNDAMENTOS DE MULTICAST IPv4 E IPv6

2.1 INTRODUCCIÓN

En la comunicación IP, en uno de sus extremos, por así decirlo, se encuentra la comunicación unicast, en la cual un host IP de origen envía paquetes a un host de destino específico y en cuyo caso, la dirección IP de destino del paquete corresponde a un único host en la red. Los paquetes IP son transportados a través de la red mediante los routers, quienes mediante su tabla de enrutamiento toman decisiones de envío de unicast basadas en la dirección IP de destino del paquete.

En el otro extremo de la comunicación IP se encuentra la comunicación broadcast, en la cual, un host envía paquetes IP hacia todos los demás hosts pertenecientes a su segmento de red. En este tipo de comunicación, la dirección de destino del paquete de broadcast tiene todos sus bits de host configurados como unos y la porción de red se encuentra configurada con la dirección IP del segmento de red al que pertenece el host origen. Todos los equipos en la subred, hosts y routers, entienden y procesan los paquetes de destino con dirección de broadcast, sin embargo, y a menos que se configure de otra forma, los routers no reenvían paquetes de broadcast y por lo tanto, la comunicación broadcast queda limitada únicamente a la subred local.

Situada entre los tipos de comunicación IP anteriormente descritos se encuentra la comunicación multicast, la misma que permite a un host enviar paquetes a un grupo de hosts en cualquier red que éstos se encuentren. Para lograr este cometido,

la dirección IP de destino tiene un formato especial y se denomina *dirección IP de grupo multicast* de tal forma que, los routers renvían los paquetes a través de las interfaces que son miembros de un grupo multicast.

Un miembro de un grupo multicast es el host que expresa su interés en recibir paquetes enviados a una dirección de grupo multicast específica. A dicho miembro también se lo conoce como receptor u oyente.

En la figura mostrada a continuación se presentan las características descritas anteriormente para los tres tipos de transmisión sobre una red IP.

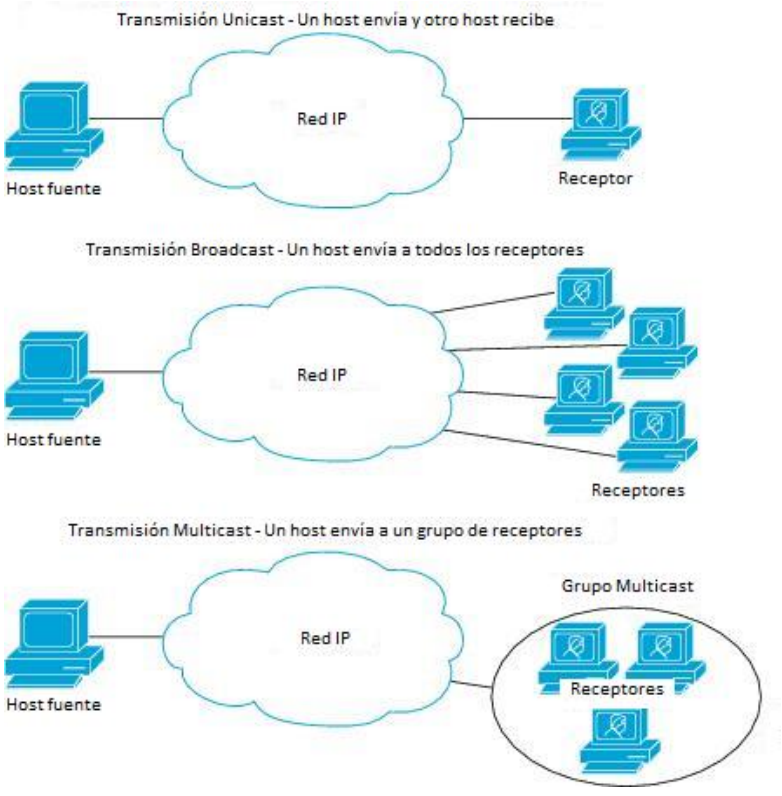


Figura 1. Métodos de transmisión sobre una red IP

Fuente: Cisco Systems. (s.f.). *IP Multicast Technology Overview*. Recuperado el 6 de marzo de 2016 de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/xe-3s/asr903/imc-pim-xe-3s-asr903-book/ip_multicast_technology_overview.html

2.2 VENTAJAS DE MULTICAST

2.2.1 OPTIMIZACIÓN DE ANCHO DE BANDA, CARGA DE PROCESAMIENTO DE SERVIDOR Y CARGA DE RED

En los últimos tiempos, el Internet y tal es el caso de ciertas compañías, han tenido un crecimiento acelerado en lo referente a número de usuarios conectados a la red, los mismos que requieren tener acceso a la misma información y aproximadamente al mismo tiempo, sobre todo en lo que respecta a contenidos Web y multimedia. Usando técnicas de multicast se posibilita la distribución de la información reduciendo significativamente la demanda total de ancho de banda sobre la red y optimizando la carga del servidor que provee el servicio.

Para ilustrar mejor lo mencionado anteriormente, consideremos un servidor de video que provee un stream típico de 1.5 Mbps. En transmisión unicast dicho servidor debería proporcionar tantos streams como clientes lo requieran. Para un enlace ethernet de 10 Mbps únicamente 6 clientes podrían hacer uso del servicio de video y aun si se dispone de un enlace de capacidad superior tal como de 1 Gbps, el límite sería de 665 streams de video de 1.5 Mbps. Entonces, con el crecimiento en el número de clientes, se tiene mayor demanda de ancho de banda y por supuesto, mayor carga de CPU en los servidores.

Por otro lado, en un ambiente multicast el servidor únicamente debe transmitir un solo stream de video por cada grupo multicast sin importar el número de clientes que dentro de él se encuentren, haciendo un uso eficiente del ancho de banda y del

CPU del servidor. Por último, es notorio que si se reduce el ancho de banda de la red también se reduce la carga en los elementos de la misma, es decir, en los routers y switches y demás elementos presentes en la red.

En la figura siguiente se observa la comparativa en el uso de ancho de banda para el envío de tráfico de video tanto en unicast como en multicast. Para ambos casos, todos los clientes reciben el video a 1.5 Mbps.

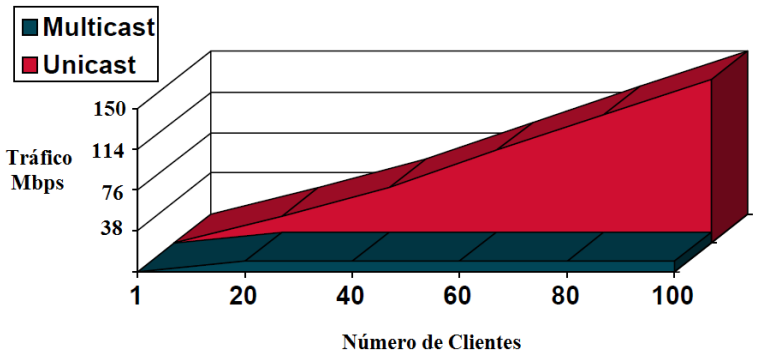


Figura 2. Streaming de video unicast vs multicast

Fuente: Cisco Systems. (2006). *Introduction to IP Multicast.* Recuperado el 6 de marzo de 2016 de http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ip-multicast/prod_presentation0900aecd80310883.pdf

En la figura 3 se puede apreciar que con tráfico de multicast tanto los elementos de red como los servidores no se ven sobrecargados.

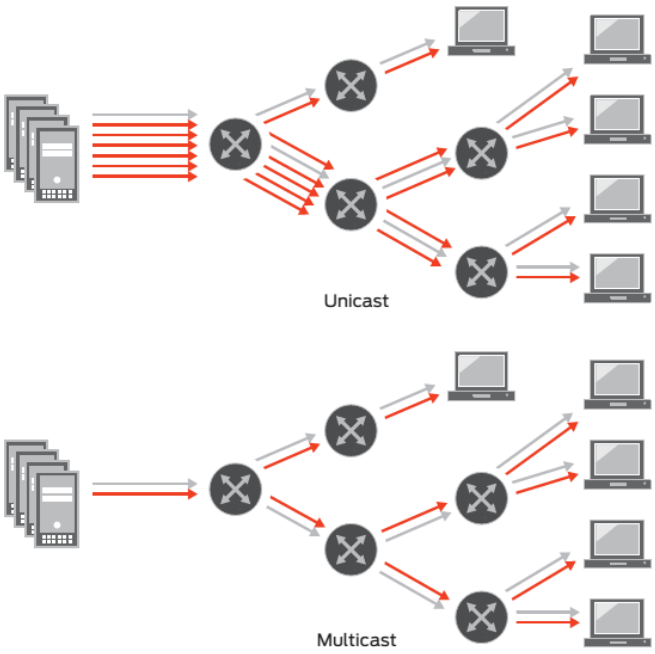


Figura 3. Unicast vs multicast. Comparación de carga de servidor y de red

Fuente: Juniper Networks. (2013). *It's time to rethink what you know about multicast.* Recuperado el 12 de marzo de 2016 de https://www.octoshape.com/wp-content/uploads/2013/06/Juniper-Octoshape-White-Paper.pdf

Si se analiza el método de broadcast, éste requiere enviar un solo paquete, sin embargo, esto acarrea problemas en la red y en sus componentes. Si los receptores se encuentran en un dominio diferente de broadcast que el transmisor, los routers necesitan transmitir broadcast. Esto causaría un desperdicio de ancho de banda en los enlaces e incrementaría la carga de procesamiento de todos los elementos de la red si solo un pequeño grupo de host estaría interesado en recibir el paquete.

En la figura 4 se aprecia como el router que se encuentra en medio de los switches envía tráfico de broadcast por todas sus interfaces de salida desperdiciando ancho de banda y cargando su CPU. Adicionalmente, esto causa un desperdicio de ancho de banda en las interfaces de los hosts que no están interesados en recibir el

tráfico y genera carga innecesaria en sus CPUs debido a que de todas formas deben procesar el tráfico no requerido.

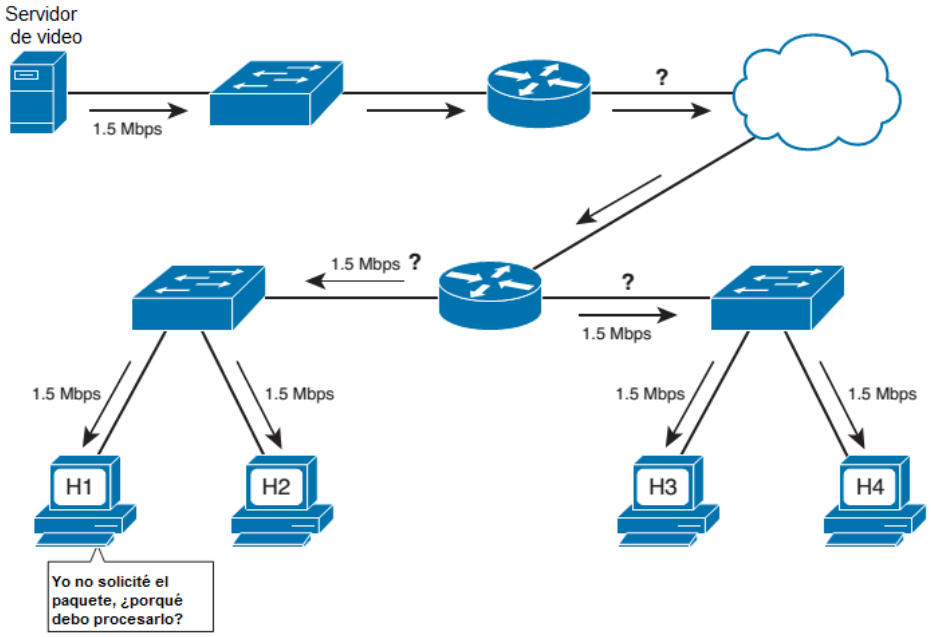


Figura 4. Incremento de la carga de CPU y desperdicio de ancho de banda por broadcast

Fuente: Kocharians, N., & Vinson, T. (2015). *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2* (Quinta ed.). Cisco Press.

2.2.2 ESCALABILIDAD

Tomando como referencia la figura 4, si el host 1 (H1) decide recibir el tráfico de video enviado por el servidor, mediante IGMP Snooping[1] el switch aprende que dicho host desea unirse al grupo multicast y procede a reenviar el tráfico por el puerto que conecta a H1. El host adicional que se acaba de unir al grupo multicast recibe el trafico

[1] IGMP Snooping: Protocolo usado para escuchar los mensajes IGMP entre hosts y routers con el objetivo de que los switches reenvíen trafico multicast únicamente por los puertos con hosts interesados en recibirlo.

deseado, al mismo tiempo que la demanda de ancho de banda de los links de WAN y la carga del servidor de video y los demás elementos de la red permanecen invariables. El switch que interconecta al host 1 incrementaría su carga de procesamiento, sin embargo, estaría a la par del switch del otro segmento de LAN y en ningún caso conllevaría a una sobre carga de procesamiento puesto que los switches de hoy en día se encuentran preparados para manejar tráfico full dúplex por todos sus puertos.

Como se puede inferir, es posible seguir incrementando receptores multicast tanto como el número de puertos de los switches lo permitan sin causar impacto en el ancho de banda y carga de procesamiento en los elementos de red, lo que permite que multicast sea altamente escalable.

2.3 DESVENTAJAS DE MULTICAST

2.3.1 ENTREGA DE PAQUETES NO CONFIABLE

Las transmisiones tanto multicast como unicast son inherentemente no confiables. La confiabilidad de unicast está basada en el protocolo TCP de la capa transporte o en protocolos de capas superiores. Por otro lado, multicast a ser de naturaleza *uno a muchos* no fue diseñado para usar mecanismos de control *end to end* tal como TCP. Los paquetes de multicast utilizan como transporte el protocolo UDP cuya naturaleza es de mejor esfuerzo. Por lo tanto, las aplicaciones que usen

multicast deben estar preparadas ya sea para aceptar pérdidas de paquetes o manejarlas mediante algún protocolo de las capas superiores.

2.3.2 DUPLICACIÓN DE PAQUETES

En multicast los routers intencionalmente envían copias de paquetes hacia todas las interfaces que se encuentran configuradas en este modo de transmisión, lo que incrementa la probabilidad de que un receptor reciba varias copias de un paquete multicast. Este caso resulta ser de mayor notoriedad en las redes que en su topología implementan paths redundantes. Puesto que un paquete multicast tiene varios caminos para llegar al receptor, éste recibirá eventualmente varias copias del mismo paquete hasta que el protocolo de ruteo de multicast converja y elimine las rutas redundantes.

2.3.3 CONGESTIÓN DE RED

En unicast, TCP automáticamente ajusta la velocidad de transmisión mediante los algoritmos de slow-start y ventana deslizante (TCP windowing) para proveer un grado de control de congestión en la red. Dado que multicast es un protocolo no orientado a conexión y es de naturaleza *uno a muchos*, no existe mecanismo para controlar la saturación de red. Por tanto, en lo posible las aplicaciones deben intentar detectar y controlar las condiciones de congestión.

2.4 APLICACIONES DE MULTICAST

2.4.1 IPTV

La IPTV hoy en día es un término amplio que abarca a cualquier tipo de video transportado por el protocolo IP. Entre las aplicaciones de IPTV más populares se encuentran el entretenimiento, la educación a distancia en ambientes educativos y empresariales, y últimamente se ha presentado un gran auge en video conferencias en entornos corporativos e industriales.

IPTV comprende la convergencia de voz, datos y video de manera que permite a los proveedores brindar sus servicios mediante una sola red, obteniendo de esta forma eficiencia en la infraestructura de transporte. Para el cliente esto representa que su servicio de comunicación y entretenimiento es provisto mediante un solo acceso y por una fracción del costo.

La publicidad dirigida (target advertisement) se ha hecho muy popular en los últimos tiempos y grandes compañías como Amazon y Google ha hecho de ella toda una ciencia logrando grandes beneficios comerciales. Con la tecnología multicast de IPTV se puede lograr el envío de publicidad por segmentos o regiones, por ejemplo, propaganda electoral en ciertos sectores demográficos o segmentar la publicidad de acuerdo a los patrones de uso de internet de los usuarios.

Sin embargo, IPTV no es únicamente comunicación de una vía hacia el cliente. Por medio del canal de comunicación, el suscriptor puede comunicarse con su proveedor de servicios para comprar productos que ha conocido mediante la

publicidad, para enviar retroalimentación acerca de la programación o para el envío automático de patrones de comportamiento de usuario. La interacción del usuario permite la creación de contenido dinámico lo cual hace que el usuario consuma solo contenido de su interés.

Gracias a la accesibilidad a internet que es cada día mayor y desde cualquier lugar, y a la proliferación de teléfonos móviles, es posible tener acceso a la TV móvil. Acorde a lo publicado por Naciones Unidas a finales del año 2015, el número de teléfonos móviles alcanzó los 7.000 millones de unidades, lo que representa aproximadamente el 97% de la población mundial actual. La convergencia de comunicación, información y entretenimiento provista por los teléfonos móviles sumado a su ubicuidad ha cambiado el estilo de vida de las personas, de modo que siempre es posible ejecutar cualquier aplicación, a cualquier hora y en cualquier lugar.

2.4.2 VIDEO BAJO DEMANDA

El video bajo demanda permite a los subscriptores seleccionar películas o contenido multimedia teniendo la posibilidad de mirarlo en tiempo real o descargarlo para ser visto en cualquier otro momento. En la actualidad, con las tecnologías de multicast es tecnológicamente posible y económico que el video bajo demanda se aplique también a dispositivos móviles. Dentro del video bajo demanda se distinguen tres tipos, los cuales se indican a continuación:

- VoD Transaccional. - Permite alquilar el contenido o descargarlo previo un pago. En esta categoría se encuentran Google Play, iTunes, Amazon.
- VoD por subscripción. – Se debe pagar una subscripción anual o mensual para tener acceso al contenido. Aquí se encuentran Netflix, Mubi, MoviCityPlay
- VoD con publicidad. - El contenido es gratuito, pero con la aparición de publicidad. Ejemplos de esta categoría son YouTube, Crackle, Popcorn Time.

2.4.3 RADIO MULTIMEDIA

En ocasiones, para la radio multimedia se usa el término *radio visual.* Este término hace referencia a la agregación a la programación de radio convencional contenido interactivo y visual. Junto con el stream de audio es posible enviar información acerca de la canción y del artista. Además, se puede adjuntar contenido interactivo tales como sistemas de votaciones, chat, e incluso juegos.

2.4.4 DATOS BAJO DEMANDA

El contenido es ofrecido a petición. Los usuarios tienen la posibilidad de descargar o visualizar en tiempo real contenido de audio, video, o documentos expuestos en un listado de un portal. Los usuarios solicitan la misma información en tiempos similares desde un grupo multicast.

2.4.5 EMISIÓN DE CONTENIDO

Se trata de subscripciones generalmente a contenidos noticiosos. La información es enviada a los suscriptores de manera automática mediante RSS (*Really Simple*

Syndication). RSS es un formato XML utilizado para compartir contenido web que se actualiza con frecuencia.

2.4.6 JUEGOS EN LÍNEA Y SIMULACIONES

Los juegos en línea requieren una conexión con un servidor para el intercambio de información. La información intercambiada puede ser actualizaciones tales como niveles o puntuaciones de otros jugadores. Las simulaciones son utilizadas tanto como para entretenimiento como para entrenamiento militar. Un grupo multicast puede ser un grupo de participantes o jugadores en una sala de simulación y solo ellos reciben datos de lo que ocurre en dicha sala. Cuando abandonen la sala y requieran unirse a otra, abandonan el grupo multicast actual y se unen a otro.

2.4.7 MULTI VIDEOCONFERENCIA

Las videoconferencias son utilizadas por las corporaciones con el objetivo de reducir los costos y tiempo de viajes de sus ejecutivos. En la multi videoconferencia es un participante el que actúa como anfitrión, el mismo que tiene como responsabilidades el poner nombre a la videoconferencia, incluir a los participantes, empezar y terminar la misma. Este host envía las características de la conferencia a un servidor y los usuarios proceden a unirse a la reunión a través de dicho servidor.

2.4.8 DISTRIBUCIÓN MÁQUINA A MÁQUINA

Este tipo de comunicación multicast es utilizada para actualizaciones de software y configuración de dispositivos con el objetivo de modificar su operación o rendimiento. En este tipo de comunicación generalmente se encuentran dispositivos

de características comunes tales como, el mismo fabricante, modelo y versión de software; conformando un grupo de multicast.

2.5 DIRECCIONAMIENTO MULTICAST DE IPv4

La Autoridad de Asignación de Números de Internet, IANA por sus siglas en inglés, asigna la clase D para las direcciones IPv4 de multicast. Los 4 primeros dígitos de la clase D son siempre 1110, de modo que el rango completo se encuentra entre 224.0.0.0 hasta 239.255.255.255. Puesto que estas direcciones no representan hosts individuales sino grupos multicast, no hay necesidad de utilizar máscaras de subred debido a que estas direcciones no son jerárquicas. Dentro del rango de direcciones IP multicast de IPv4 descrito anteriormente existen sub rangos o subgrupos asignados por la IANA para motivos de clasificación dado que cada subgrupo es asignado para propósitos específicos. Estos subgrupos mencionados se describirán a continuación.

2.5.1 DIRECCIONES DE ENLACE LOCAL

El rango entre 224.0.0.0 hasta 224.0.0.255 es reservado para el uso de protocolos de red en una red local. Los paquetes con estas direcciones no son reenviados por los routers dado que tiene un valor de TTL igual a 1. Los protocolos de red utilizan este tipo de direcciones multicast para intercambiar información importante de enrutamiento tales como descubrimiento de routers, cambios de topología de red, estado de los links, etc. En la tabla 1 se muestran algunas direcciones de multicast de enlace local conocidas.

Tabla 1. Direcciones multicast IPv4 de enlace local

224.0.0.1	Todos los host multicast
224.0.0.2	Todos los routers multicast
224.0.0.4	Routers DV MRP
224.0.0.5	Todos los routers OSPF
224.0.0.6	OSPF designated routers
224.0.0.9	Routers RIP
224.0.0.10	Routers EIGRP
224.0.0.13	Routers PIM
224.0.0.22	IGMPv3
224.0.0.25	RGMP

2.5.2 DIRECCIONES DE ALCANCE GLOBAL

Las direcciones de alcance global comprenden el rango entre 224.0.1.0 hasta 224.0.1.255 y son destinadas para enviar tráfico multicast entre organizaciones y a través de internet. En la tabla 2 se presentan algunas direcciones IP de multicast correspondientes a este subgrupo.

Tabla 2. Direcciones multicast IPv4 de alcance global

224.0.1.1	NTP Network Time Protocol
224.0.1.24	Microsoft-ds
224.0.1.33	RSVP-encap-1
224.0.1.34	RSVP-encap-2
224.0.1.39	Cisco-rp-announce
224.0.1.40	Cisco-rp-discovery
224.0.1.75	SIP
224.0.1.173	host-request
224.0.1.174	host-announce

2.5.3 DIRECCIONES DE FUENTE ESPECÍFICA

Para las aplicaciones y protocolos SSM (*Source Specific Multicast*), IANA tiene reservado el subgrupo de direcciones comprendido entre 232.0.0.0. hasta 232.255.255.255. El propósito de estas aplicaciones es permitir que un host pueda seleccionar una fuente de multicast de mejor calidad en el grupo en el que se encuentra, haciendo el ruteo multicast eficiente y ayudando al administrador de red a prevenir ataques de denegación de servicio.

2.5.4 DIRECCIONES GLOP

Para este tipo de direcciones se tiene reservado el rango comprendido entre 233.0.0.0 hasta 233.255.255.255, las mismas que pueden ser utilizadas por quien sea dueño y tenga registrado un número de sistema autónomo (ASN). Estas direcciones tienen alcance global y su uso es similar a una dirección unicast de clase C, es decir, se tendrían por cada ASN 256 direcciones. Puesto que IANA reserva las direcciones con el objetivo de que sean únicas y dado que las direcciones GLOP son ruteables a través de internet, es necesario que el ASN también sea único.

Para obtener la dirección GLOP se utiliza el sistema autónomo tal y como se describe a continuación en el siguiente ejemplo. Si se tiene el ASN 6586, a éste se lo debe descomponer en su equivalente binario, el cual es 0001100110111010. Los primeros 8 dígitos corresponden al segundo octeto de la dirección multicast GLOP, los cuales en notación decimal representan 25, y los 8 dígitos restantes corresponden al tercer octeto, cuya equivalencia decimal es 186. De esta manera, el rango de direcciones GLOP para este caso estará comprendido entre 233.25.186.0 y 233.25.186.255.

2.5.5 DIRECCIONES DE ALCANCE LIMITADO

Para este tipo de direcciones el rango reservado va desde 239.0.0.0 hasta 239.255.255.255 y son usadas en dominios privados de multicast, de manera similar a como se utilizan las direcciones privadas de unicast. Los administradores de red son libres de emplear estas direcciones siempre y cuando se aseguren de que el tráfico

no debe sobrepasar los límites del dominio multicast. Para esto, los routers deben ser configurados con filtros para evitar que el tráfico multicast fluya hacia fuera de un sistema autónomo o cualquier dominio defino por el administrador.

Resumiendo, los rangos de direcciones multicast IPv4 reservados por la IANA más utilizados se presenta en la siguiente tabla.

Tabla 3. Tipos de direcciones multicast IPv4

Tipo de Direcciones	**Rango**
Direcciones de enlace local	224.0.0.0 – 224.0.0.255
Direcciones de alcance global	224.0.1.0 – 224.0.1.255
Direcciones de fuente específica	232.0.0.0 – 232.255.255.255
Direcciones GLOP	233.0.0.0 – 233.255.255.255
Direcciones de alcance limitado	239.0.0.0 – 239.255.255.55

2.6 DIRECCIONAMIENTO MULTICAST DE IPv6

Aunque las nociones básicas de multicast son las mismas tanto para IPv4 como para IPv6, multicast IPv6 posee nuevas y mejoradas características basadas en las experiencias operacionales de su contraparte IPv4 como, por ejemplo, resuelve el problema de la unicidad de las direcciones multicast de alcance global. Además, dado que el espacio de direcciones IPv6 es más amplio, facilita la gestión de los grupos de

multicast y permite a los administradores de red asignar y administrar grandes rangos de grupos de multicast sin tener que preocuparse de que existan colisiones.

2.6.1 DIRECCIÓN GENÉRICA DE GRUPO MULTICAST

Acorde al RFC 3513, la dirección genérica de multicast IPv6 es como se describe a continuación.

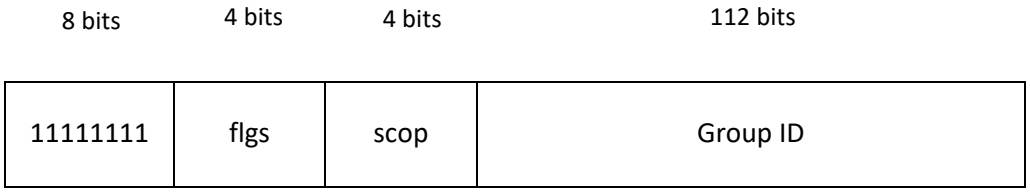


Figura 5. Dirección multicast IPv6

El primer campo que consta de 8 unos identifica a la dirección como de multicast.

2.6.1.1 Campo flgs

Este campo tiene la siguiente estructura:

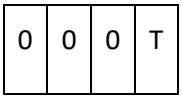


Figura 6. Campo flgs de la dirección multicast IPv6

En donde

T = 0 significa que la dirección es reservada y asignada por la IANA para ser usada, por ejemplo, por los protocolos de ruteo o protocolos de redundancia como VRRP.

T=1 significa que la dirección puede ser usada para transmisiones multicast por los administradores de red.

2.6.1.2 Campo scop

Con este campo se define el alcance de la dirección multicast IPv6 de acuerdo a la siguiente tabla:

Tabla 4. Definiciones del campo scop de la dirección multicast IPv6

0	Reservado
1	Alcance Interface-Local
2	Alcance Link-Local
3	Reservado
4	Alcance Admin-Local
5	Alcance Site-Local
6 - 7	Sin asignar
8	Alcance Organization-Local
9 - D	Sin asignar
E	Alcance Global
F	Reservado

- **Alcance Interface-Local. -** Este alcance se extiende a una sola interfaz en un nodo, y es útil solo para transmisiones multicast de loopback.

Tabla 5. Direcciones multicast IPv6 Interface-Local

FF01::1	Todos los nodos
FF01::2	Todos los Routers
FF01::FB	mDNSv6

- **Alcances Link-Local y Site-Local.** - Abarcan las mismas regiones topológicas tal como sus correspondientes direcciones de unicast, es decir, las direcciones de Link-Local son configuradas en un solo enlace y las direcciones Site-Local se configuran dentro de sucursales que no necesiten direcciones globales.

Tabla 6. Direcciones multicast IPv6 Link-Local

FF02::1	Todos los nodos
FF02::2	Todos los routers
FF02::5	OSPFIGP
FF02::6	OSPFIGP Designated Routers
FF02::9	Routers RIP
FF02::A	Routers EIGRP
FF02::12	VRRP
FF02::1:2	Todos los clientes DHCP

Tabla 7. Direcciones multicast IPv6 Site-Local

FF05::2	Todos los routers
FF05::FB	mDNSv6
FF05::1:3	Todos los servidores DHCP

- **Alcance Admin-Local. -** Corresponde al alcance más pequeño que debe ser configurado administrativamente. Es decir, no se deriva de forma automática de alguna configuración física u otra configuración no relacionada con multicast.
- **Alcance Organization-Local. -** Abarca a múltiples sucursales dentro de una misma organización.
- **Alcance Global. -** Es usado para identificar las interfaces unívocamente en internet.

Los valores determinados como *sin asignar* están disponibles para que los administradores de red definan regiones multicast adicionales.

De la tabla 4 se puede inferir que los paquetes multicast que pertenezcan a los alcances 1 y 2 no son reenviados más allá del enlace local. Únicamente el tráfico que tenga configurado en el campo scop un valor de 4 o superior será distribuido a través de los routers.

2.6.1.3 Campo group ID

Identifica a los grupos multicast, tanto si son reservados por la IANA o definidos por el administrador de red.

2.6.2 DIRECCIONES BASADAS EN PREFIJOS UNICAST

En IPv4 se tiene el problema de que las direcciones multicast de alcance global pueden repetirse a través de internet. Las direcciones GLOP vinieron a solucionar en parte este problema puesto que el proveedor de servicios puede introducir su número de sistema autónomo (ASN) de BGP en los 2 octetos intermedios de la dirección de multicast 233/8 tal como se vio en el subcapítulo 2.5.4. De este modo, el ISP obtiene 256 direcciones de grupo multicast únicas basadas en su sistema autónomo.

El RFC 3306 define una alternativa similar a las direcciones GLOP para IPv6, pero en lugar de utilizar el sistema autónomo en medio de la dirección de multicast se utiliza un prefijo unicast para identificar al grupo multicast. Además, permite que usuarios que no posean un sistema autónomo puedan conectarse a internet.

A continuación, en la siguiente figura se presenta el formato de la dirección multicast IPv6 basada en prefijo unicast.

8 bits	4 bits	4 bits	8 bits	8 bits	64 bits	32 bits
11111111	Flgs	Scop	Reserved	Plen	Network prefix	Group ID

Figura 7. Formato de la dirección multicast IPv6 basada en prefijo unicast

El primer campo de 8 bits en unos identifica a la dirección IPv6 como de multicast.

2.6.2.1 Campo flgs

El campo flgs tiene la estructura siguiente:

0	0	P	T

Figura 8. Campo flgs de la dirección IPv6 multicast basa en prefijo unicast

En donde

P = 0 indica que se trata de una dirección IPv6 multicast que no está basad en prefijo unicast, es decir, es una dirección acorde al RFC 3513.

P = 1 indica que es una dirección multicast IPv6 basada en prefijo unicast.

Si P = 1, T debe configurarse en 1, de lo contrario la configuración de éste bit está definida por el RFC 3513.

2.6.2.2 Campo Plen

Este campo indica la longitud, es decir, el número de bits que tiene el prefijo que se usará en el campo *Network prefix* cuando P = 1.

2.6.2.3 Campo Network prefix

Este campo identifica el prefijo de la subnet unicast de propiedad del proveedor de servicios. Los bits no significantes del prefijo unicast deben ser configurados como ceros. Conforme a su asignación en cuanto a número de bits, el prefijo a ser utilizado no puede exceder los 64 bits.

2.6.2.4 Campo Group ID

Este campo contiene 32 bits correspondientes al ID de grupo multicast de IPv6, el mismo que es asignado por el dueño del prefijo unicast.

2.6.2.5 Campo scop

Los valores de este campo tienen las mismas definiciones que el campo scop especificado por el RFC 3513 y descritos en la tabla 4.

A continuación, se propone a manera de ejemplo construir la dirección multicast IPv6 que tenga un alcance global basada en el prefijo unicast 2001:BF25:79CE::/48 y con grupo de multicast 5050.

	flgs	**scop**	**reserved**	**plen**	**Network prefix**	**Group ID**
8 bits en 1	P=1 y T=1	Global=E	8 bits en 0	48 = x30	Prefijo unicast dado	ID definido por el admin. de red
FF	3	E	00	30	2001:BF25:79CE:0000	0000:5050

Figura 9. Ejemplo de dirección multicast IPv6 basa en un prefijo unicast

De la figura 10, la dirección multicast IPv6 basada en prefijo unicast quedaría como sigue:

FF3E:30:2001:BF25:79CE::5050

2.7 PROTOCOLOS DE MEMBRESÍA DE GRUPO MULTICAST

Los protocolos de membresía de grupos multicast permiten que los routers puedan saber cuándo un host, que pertenece a una subred de una de sus interfaces, se encuentra interesado en recibir tráfico de un cierto grupo de multicast. Aun cuando más de un host se encuentre interesado, el router envía solo una copia del paquete por la interface hacia el grupo multicast. Cuando el protocolo de membresía informa a los routers que no existen hosts en la subred interesados en recibir tráfico de multicast, los paquetes son retenidos y consecuentemente el router dejará de enviar el tráfico multicast para ese grupo.

Existen 2 protocolos de membresía de grupos multicast los cuales son estándares. Para IPv4 se tiene el protocolo *Internet Group Management Protocol (IGMP)* y para IPv6 es el protocolo *Multicast Listener Discovery (MLD)*. Los

mencionados protocolos y sus correspondientes versiones se describen en los subtemas siguientes.

2.7.1 INTERNET GROUP MANAGEMENT PROTOCOL (IGMP)

El protocolo IGMP es un protocolo estándar de la industria diseñado para administrar membresías de grupos multicast de IPv4, registrando dinámicamente a hosts individuales en un grupo multicast en una LAN en particular. Los hosts identifican membresías de grupos multicast enviando mensajes IGMP a su router multicast local. Por otra parte, a más de escuchar los mensajes enviados por los hosts, los routers envían periódicamente mensajes de consulta para detectar que grupos están activos o inactivos en cada subred.

Los mensajes IGMP son enviados en datagramas mediante el protocolo IP número 2 con un TTL de valor 1 por lo que, los paquetes IGMP circulan a través de la LAN pero no son reenviados por los routers.

Existen 3 versiones de este protocolo, las cuales se describen a continuación.

2.7.1.1 IGMP versión 1

La versión 1 de IGMP maneja solo 2 mensajes, los cuales son:

- Membership Query
- Membership Report

Los hosts envían mensajes *membership report* a un grupo de multicast determinado para indicar que están interesados en unirse a dicho grupo. Cuando una

aplicación abre un socket multicast, el stack TCP/IP automáticamente envía estos mensajes.

Los routers envían periódicamente mensajes IGMP de *membership query* para verificar que al menos un host aún sigue interesado en recibir el tráfico de grupo multicast. Cuando el router no recibe respuesta a tres mensajes consecutivos de *membership query*, deja de transmitir el tráfico que estaba dirigido al grupo de multicast.

2.7.1.2 IGMP versión 2

En la versión 2 de IGMP se tiene los siguientes tipos de mansajes:

- Membership Query
- Membership Report version 1
- Membership Report version 2
- Leave Group

La versión 2 de IGMP trabaja de manera similar a la versión 1, con la diferencia de que existe el mensaje *leave group*. Con este mensaje el host comunica al router local su intención de abandonar el grupo de multicast. Cuan el router recibe este mensaje, envía un mensaje de *membership query* para determinar si existen todavía hosts interesados en recibir el tráfico. Si no recibe respuesta, el router deja de transmitir el tráfico a ese grupo específico.

Gracias a la versión 2, se reduce en gran medida la latencia en la que un host abandona un grupo de multicast específico, lo que significa que el tráfico innecesario que circule por la red sea detenido mucho más rápido.

IGMP v2 ha sido diseñado para ser compatible con IGMP v1, de acuerdo al RFC 2236.

2.7.1.3 IGMP versión 3

En IGMP versión 2 y versión 1, cuando un host realiza un requerimiento para unirse a un grupo, el router multicast reenvía el tráfico del mencionado grupo sin importar la dirección fuente de los paquetes. Esta característica en redes grandes, tales como redes de broadcast de internet puede causar problemas puesto que es susceptible de que en un grupo de multicast pueda introducirse tráfico no deseado desde una dirección IP de origen desconocida que pueda causar DoS en los enlaces de una compañía.

IGMP v3 permite a los hosts indicar el interés de recibir paquetes solo desde una dirección IP de origen específica, a través de la característica denominada como *Source-Specific Multicast (SSM)*.

En la figura que se muestra a continuación, se observa que el host 1 envía el reporte de membresía de IGMPv3 indicando el interés de unirse al grupo 226.1.1.1 para recibir tráfico de multicast únicamente del servidor con dirección IP 209.165.201.2 por lo que, el router multicast local bloquea el tráfico de la dirección IP fuente 209.165.202.130.

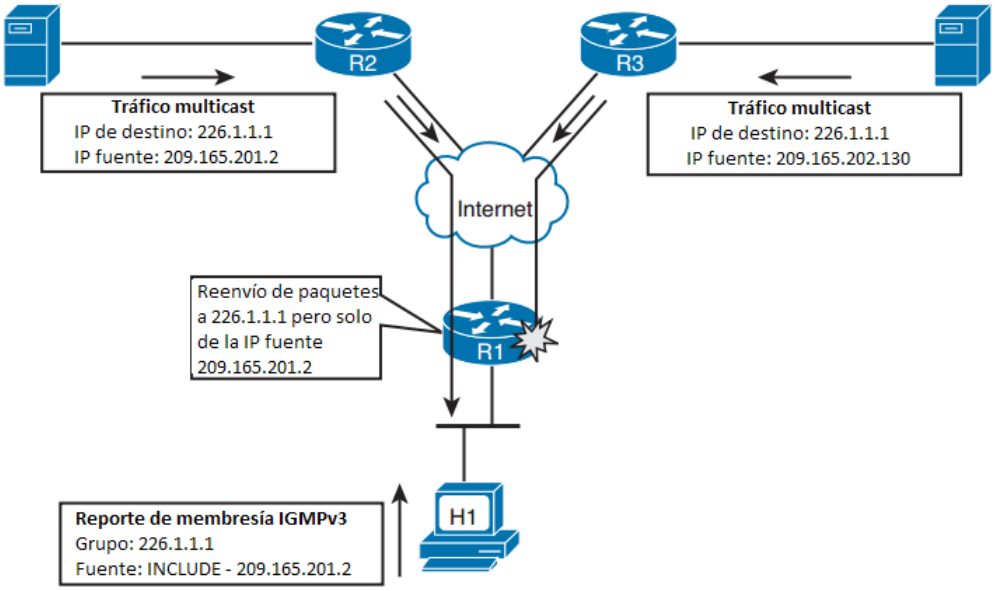


Figura 10. Reporte de membresía de IGMPv3

Fuente: Kocharians, N., & Vinson, T. (2015). *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2* (Quinta ed.). Cisco Press.

IGMPv3 maneja 2 tipos de mensajes:

- Membership Query version 3
- Membership Report version 3

Para IGMPv3 existen 2 modos de selección de la fuente, los cuales se describen a continuación.

Modo Inclusivo. - Los hosts especifican una lista de fuentes de las cuales desean recibir paquetes para un grupo multicast determinado. De manera implícita, cualquier otra fuente que no se encuentre en la lista se considera como no deseada.

Modo Exclusivo. - Los hosts especifican una lista con fuentes no deseadas. En este modo, las fuentes que no se encuentren en la lista se considerarán implícitamente fuentes deseadas.

Dados estos dos modos, el rol del router es más complejo debido a que, para un determinado grupo debe analizar y sintetizar las lista inclusivas y exclusivas de varios hosts. La meta es que los paquetes de una fuente de interés ya sea implícita o explícita indicada por al menos un host sea reenviada.

Sean L_1 y L_2 listas enviadas por los hosts de un grupo de multicast, las posibles combinaciones que el router debe manejar son las siguientes:

$$\text{INCLUDE } L_1 \text{ ^ INCLUDE } L_2 \Rightarrow \text{INCLUDE } L_1 \cup L_2$$

$$\text{EXCLUDE } L_1 \text{ ^ EXCLUDE } L_2 \Rightarrow \text{EXCLUDE } L_1 \cap L_2$$

$$\text{INCLUDE } L_1 \text{ ^ EXCLUDE } L_2 \Rightarrow \text{EXCLUDE } L_2 \setminus L_1$$

De lo anteriormente indicado, cabe señalar que MODE_IS_INCLUDE y MODE_IS_EXCLUDE son los valores que puede tomar el campo *Record type* del mensaje de reporte de membresía de IGMPv3.

Por último, se indica que IGMPv3 es compatible hacia atrás con IGMPv2 e IGMPv1.

2.7.2 MULTICAST LISTENER DISCOVERY PROTOCOL (MLD)

El protocolo MLD es utilizado por los routers IPv6 para descubrir la presencia de oyentes multicast que se encuentran directamente conectados a sus interfaces, es

decir, nodos que tienen interés de recibir paquetes de multicast; así como también descubrir la dirección multicast específica que es de interés para los nodos mencionados anteriormente.

Existen 2 tipos de elementos para el protocolo MLD, los cuales son:

Querier. - Es un dispositivo de red, tal como un router, el cual envía mensajes de consulta para descubrir que dispositivos de red son miembros de un grupo de multicast determinado.

Host. – Es un receptor, incluidos los routers, los mismos que envían mensajes de reporte para notificar al *querier* de una membresía de host.

El conjunto de hosts y *queriers* que reciben paquetes multicast desde una misma fuente es llamado un grupo de multicast. Hosts y *queriers* usan los mensajes de reporte de MLD para unirse o abandonar los grupos, así como también, para empezar a recibir tráfico de grupo.

MLD utiliza el protocolo *Internet Control Message Protocol versión 6* (ICMPv6) para transportar sus mensajes, siendo estos de alcance link-local con TTL igual a 1. Los paquetes MLD tienen cabeceras de extensión[2] de *Hop-by-Hop Options* en la cual se encuentra configurada la opción *router alert.* Esta bandera indica a los routers que

[2] Las cabeceras de extensión son cabeceras que se insertan entre la cabecera principal y el payload de la trama IPv6 con el objetivo de incluir parámetros adicionales tales como fragmentación, autenticación, seguridad, ruteo, y solo son insertadas si son necesarias dichas opciones.

no deben ignorar al paquete, aun cuando no se encuentren escuchando a la dirección de grupo multicast al que pertenece el paquete en cuestión.

2.7.2.1 MLD versión 1

En esta versión de MLD existen 3 tipos de mensajes, los mismos que se describen a continuación.

Multicast Listener Query. – Este mensaje es utilizado por los routers con el propósito de averiguar si existen membresías de grupos multicast sobre un link. Este mensaje es el equivalente al mensaje de IGMPv2 *Memebership Query*. De estos mensajes se distinguen 2 tipos, los cuales son:

- *General Query.* - Mensaje enviado periódicamente a los hosts de una subred para averiguar si existen oyentes o miembros de grupo de cualquier dirección de multicast.

- *Multicast-address-specific Query.* - Mensaje enviado a los hosts de una subred para determinar si son miembros de un grupo multicast específico.

En la cabecera IPv6 del mensaje Multicast Listener Query se distingue la siguiente información:

- El campo Hop Limit es configurado en 1.
- La dirección fuente es configurada con la dirección link-local de la interface sobre la cual se envía el mensaje.

- La dirección de destino es la dirección multicast específica a la que se envía el *query*. Para el caso del mensaje general query, la dirección de destino es configurada como link-local *all nodes* FF02::1. Para el mensaje multicast address-specifc query, la dirección de destino es la dirección de multicast específica a la que el router está realizando el *query*.

Multicast Listener Report. - Este mensaje es utilizado por los oyentes para indicar su interés en recibir tráfico para una dirección multicast específica o para responder al mensaje multicast *listener query* de cualquiera de sus 2 tipos. Este mensaje es el equivalente al mensaje de IGMPv2 *Membership Report.*

En la cabecera IPv6 de este mensaje se tiene la siguiente información:

- El campo Hop Limit es configurado en 1.
- En el campo de la dirección fuente se encuentra configurada la dirección link-local de la interface por la cual el mensaje de reporte está siendo enviado.
- La dirección de destino se encuentra configurada con la dirección multicast específica a la cual se envía el reporte.

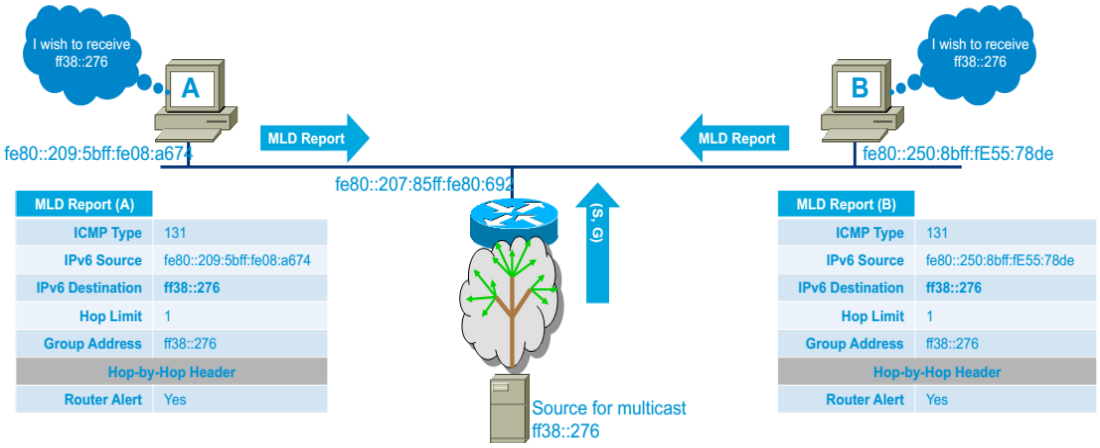


Figura 11. Operación del mensaje Multicast Listener Report

Fuente: Martin, T. (2015). *Cisco "Tech Session" IPv6 Has New Friends*. Recuperado el 15 de abril de 2016, de http://documents.tips/download/link/fedv6tf-ipv6-new-friends

Multicast Listener Done. – Este mensaje es el equivalente al mensaje *Leave Group* de IGMPv2 y es utilizado para informar al router local que puede ser que no existan más miembros de un grupo de una dirección multicast específica en una subred. El router local realiza la verificación de que no hay más miembros de un grupo multicast mediante el mensaje *Multicast Listener Query*.

El mensaje es enviado cuando el miembro del grupo que respondió al último mensaje *Multicast Listener Query* para una dirección multicast de una subred, abandona el grupo. Debido a que los routers multicast no realizan un seguimiento sobre cuántos miembros existen en un grupo sobre una subred, cada subred puede ser tratada como si hubiera múltiples miembros de grupo presentes. Cuando el router multicast recibe el mensaje *Multicast Listener Done*, inmediatamente envía el mensaje *Multicast Address-specific Query* para la dirección multicast específica que

está siendo reportada por el mensaje *Multicast Listener Done*. Si existen aún miembros del grupo, uno de ellos enviará el mensaje *Multicast Listener Report.*

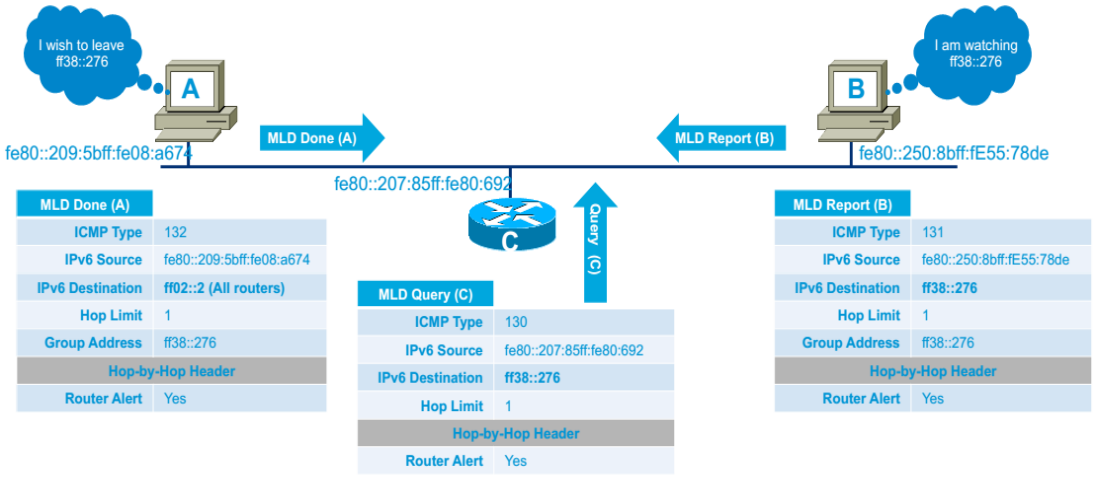


Figura 12. Operación del mensaje Multicast Listener Done

Fuente: Martin, T. (2015). *Cisco "Tech Session" IPv6 Has New Friends*. Recuperado el 15 de abril de 2016, de http://documents.tips/download/link/fedv6tf-ipv6-new-friends

En la cabecera IPV6 de este mensaje, se pueden encontrar las siguientes configuraciones:

- El campo Hop Limit es configurado en 1.
- La dirección fuente está configurada con la dirección link-local de la interface por la cual el mensaje se está enviando.
- La dirección de destino se encuentra configurada con la dirección de multicast link-local all-routers FF02::2.

2.7.2.2 MLD versión 2

Así como MLDv1, MLDv2 utiliza los menajes de ICMPv6 y ambos tienen la misma estructura de paquetes consistiendo en una cabecera IPv6, una cabecera de extensión de *Hop-by-Hop Options* con la opción *Router Alert* y el mensaje MLDv2. En esta versión existen 2 tipos de mensajes, siendo éstos los descritos a continuación.

Multicast Listener Query modificado. – Este mensaje es enviado por los routers para averiguar si en un link existe alguna membresía de grupo multicast. Existen tres tipos de mensajes:

- General Query
- Multicast-address-specifc Query
- Multicast-address-and-source-specific Query

Los dos primeros mensajes son similares a los descritos para MLDv1. El mensaje *multicast-address-and-source-specific query* es enviado a todos los hosts de una subred para averiguar si son miembros de un grupo multicast específico y para saber si están escuchando tráfico de una lista específica de fuentes multicast.

En la cabecera de este mensaje se pueden encontrar las siguientes configuraciones:

- El campo Hop Limit es configurado en 1.
- La dirección fuente es configurada con la dirección link-local de la interface sobre la cual se envía el mensaje.

- La dirección de destino se configura con la dirección específica que está siendo consultada. Para el mensaje *general query*, la dirección es la de multicast link-local all-nodes FF02::1. Para los tipos de mensajes *multicast-address-specific* y *multicast-address-and-source-specific,* la dirección de destino es la dirección de multicast específica que está siendo consultada.

MLDv2 Multicast Listener Report. – Este mensaje es enviado por un oyente para reportar su interés en recibir tráfico de una dirección multicast específica, o para responder a los mensajes multicast *listener query* de cualquiera de sus tipos. Es equivalente al mensaje *Listener Report* de MLDv1.

Con el mensaje MLDv2 *multicast listener report*, un host puede registrar interés en múltiples direcciones multicast y especificar una lista con direcciones incluidas o excluidas, tal como IGMPv3.

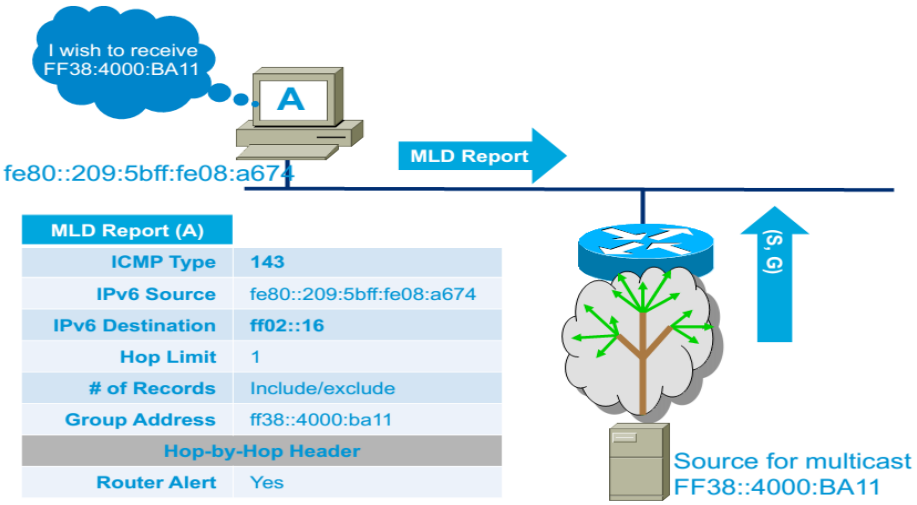


Figura 13. Operación del mensaje MLDv2 Multicast Listener Report

Fuente: Martin, T. (2015). *Cisco "Tech Session" IPv6 Has New Friends*. Recuperado el 15 de abril de 2016, de http://documents.tips/download/link/fedv6tf-ipv6-new-friends

En la cabecera IPv6 de este mensaje se puede notar la siguiente configuración.

- El campo Hop Limit es configurado en 1.
- La dirección fuente es configurada con la dirección link-local de la interface sobre la cual el reporte se envía.
- La dirección de destino es configurada con la dirección FF02::16 reservada por la IANA para todos routers MLDv2.

Para mantener la compatibilidad con MLDv1, los equipos de MLDv2 también soportan los mensajes multicast *Listener Rport* y *Listener Done.*

2.8 FUNDAMENTOS DE ENRUTAMIENTO MULTICAST

Tanto el enrutamiento como el forwarding en multicast son bastante diferentes comparados con unicast. Debido a que existen múltiples receptores de tráfico enviado desde una única fuente, el camino que recorren los paquetes tiene más de una opción para llegar a sus destinos, haciendo que el path de entrega sea un árbol de distribución. Otro punto a considerar es que el comportamiento de los hosts que reciben el tráfico multicast afecta directamente la información de enrutamiento a través de los protocolos entre los hosts y los routers tales como MLD o IGMP. Por último, cabe señalar que a diferencia de unicast, en multicast la información de la dirección de la fuente posee un rol importante en el reenvío de los paquetes de multicast.

2.8.1 ÁRBOLES DE DISTRIBUCIÓN MULTICAST

Los routers multicast crean los árboles de distribución con la finalidad de controlar la ruta que el tráfico toma a través de la red para llegar a todos los destinatarios. Los 2 tipos básicos de árboles de distribución son los árboles fuente y los árboles compartidos. Ambos tipos son libres de loops y el tráfico es replicado únicamente a través de las ramas de los árboles.

2.8.1.1 Árboles Fuente

El árbol de distribución fuente consta de un nodo raíz que actúa como fuente y de ramas que conforman un árbol de expansión a través de la red hacia los nodos receptores. Puesto que este tipo de árbol de distribución utiliza el path más corto a través de la red, también se lo conoce como *shortest path tree* (SPT).

En el gráfico mostrado a continuación, se tiene un árbol de distribución SPT el cual tiene como fuente el servidor A y dos receptores de tráfico multicast, host A y host B.

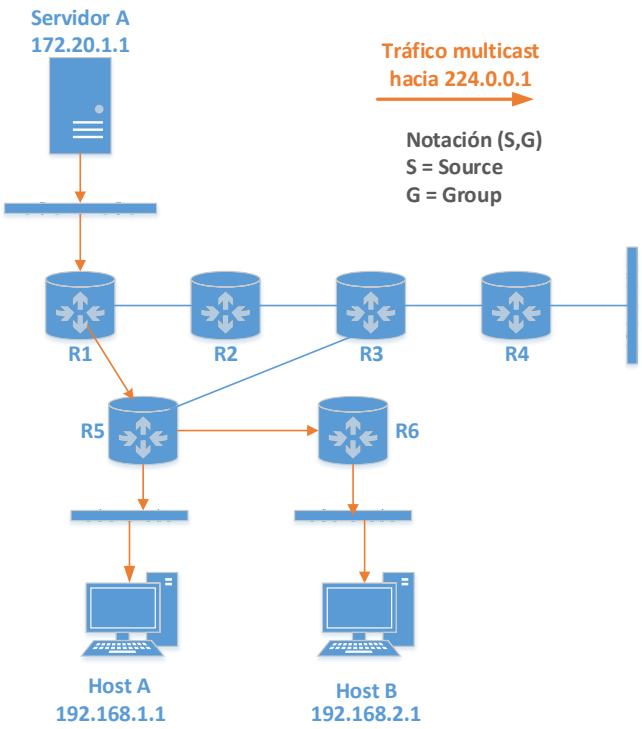


Figura 14. Distribución de tráfico multicast a través de un Árbol Fuente

Fuente: Cisco Systems. (18 de abril de 2002*). IP Multicast Technology Overview*. Recuperado el 20 de marzo de 2016, de http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

En este árbol de distribución se tiene la notación (S,G) en la cual S viene de *Source* y G de *Group*. Entonces, S representa la dirección IP de la fuente de tráfico y G representa la dirección IP multicast del grupo. Para el ejemplo mostrado en el gráfico anterior se tendría la notación como (172.20.1.1, 224.0.0.1).

De la notación (S,G) se infiere que, para cada fuente que envía tráfico multicast existe un árbol de expansión SPT individual. Por ejemplo, si existiera otro host con IP 192.168.0.1 enviando tráfico multicast a los hosts A y B, habría un SPT cuya notación sería (192.168.0.1, 224.0.0.1).

2.8.1.2 Árboles compartidos

A diferencia de los árboles fuente, lo cuales tienen el nodo raíz como fuente, los árboles compartidos utilizan un único y común nodo raíz ubicado en cierto lugar predeterminado de la red. Este nodo raíz compartido es denominado como ***Rendezvous Point*** **(RP).**

En la figura 15, se tiene un árbol de distribución compartido para el grupo 224.0.0.1 y el nodo raíz es el router R3. El tráfico multicast es enviado desde los dos servidores fuente A y B hacia el RP para alcanzar a los hosts A y B interesados en recibir el tráfico. Cabe indicar que, si el host receptor estuviera ubicado entre la fuente y el RP, dicho host recibirá el tráfico directamente.

Puesto que todos los nodos fuente en el grupo multicast utilizan un árbol compartido común, la notación que representa al árbol es descrita como (*, G). En esta notación, * representa a todas las fuentes y G al grupo multicast. Para el ejemplo de la figura anterior, la notación se expresa como (*, 224.0.0.1).

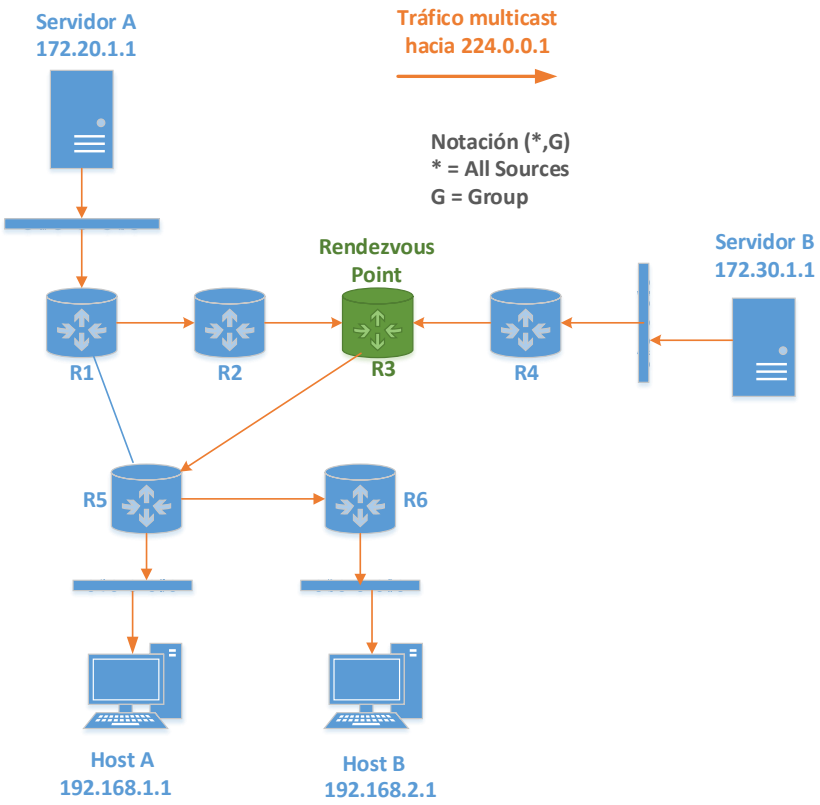


Figura 15. Distribución de tráfico multicast a través de un Árbol Compartido

Fuente: Cisco Systems. (18 de abril de 2002). *IP Multicast Technology Overview*. Recuperado el 20 de marzo de 2016, de http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

2.8.2 REVERSE PATH FORWARDING (RPF)

El algoritmo Reverse Path Forwarding es una noción fundamental en el enrutamiento multicast. RPF verifica si un paquete multicast es recibido sobre una interface para la cual el router podría enviar paquetes unicast a la dirección IP fuente del paquete multicast, por lo tanto, el router solo acepta y reenvía paquetes multicast si éstos provienen de la interface apropiada. La verificación de RPF garantiza que el árbol de distribución se encuentre libre de loops.

Para el tráfico que fluye hacia abajo en el árbol de distribución, el chequeo RPF se ejecuta de la siguiente manera:

1. El router busca en su tabla de enrutamiento unicast la dirección IP fuente del paquete multicast para determinar si el paquete ha arribado en una interfaz tal que por ésta se pueda llegar hacia la fuente.

2. Si el paquete ha arribado a una interfaz que conduzca de nuevo hacia la fuente, el chequeo RPF es exitoso y el paquete es reenviado.

3. Si el chequeo RFP en el punto 2 falla, el paquete es descartado.

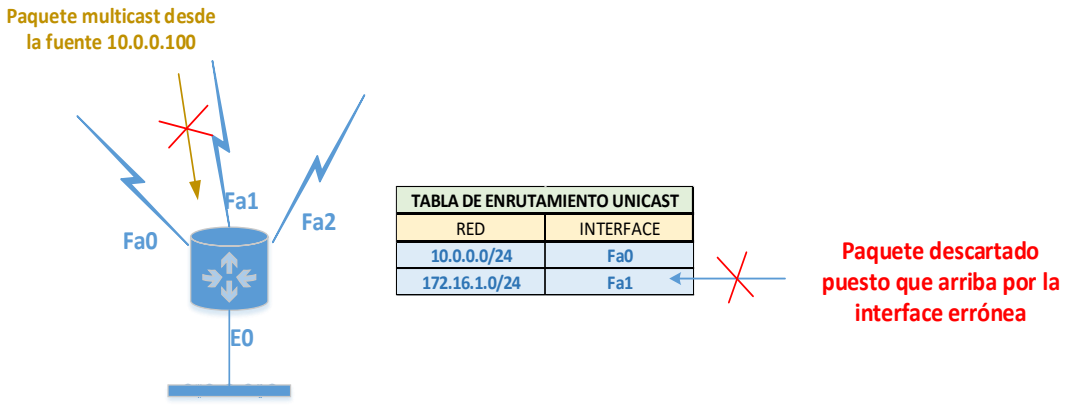


Figura 16. Chequeo fallido de Reverse Path Forwarding

Fuente: Cisco Systems. (18 de abril de 2002*). IP Multicast Technology Overview*. Recuperado el 20 de marzo de 2016, de http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

En la figura 17 se muestra el chequeo fallido del algoritmo RPF. Un paquete multicast con dirección fuente 10.0.0.100 arriba en la interface Fast Ethernet 1 (Fa1). El router en la revisión de la tabla de enrutamiento unicast verifica que para enviar

paquetes hacia la dirección 10.0.0.100 debería utilizar la interface Fast Ethernet 0 (Fa0). Puesto que el paquete ha arribado en la interface Fa1 el paquete es descartado.

En el gráfico siguiente, el paquete multicast ha arribado a la interface Fa0. En la revisión de la tabla de enrutamiento unicast, el router encuentra que es la interface correcta por lo que el chequeo RPF es exitoso y el paquete es reenviado.

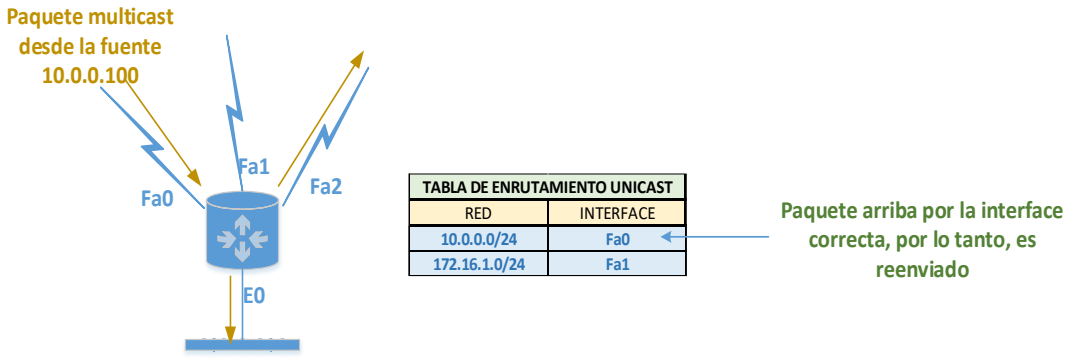


Figura 17. Chequeo exitoso de Reverse Path Forwarding

Fuente: Cisco Systems. (18 de abril de 2002). *IP Multicast Technology Overview*. Recuperado el 20 de marzo de 2016, de http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

2.8.3 PROTOCOL INDEPENDENT MULTICAST – DENSE MODE (PIM-DM)

El protocolo de enrutamiento PIM-DM utiliza un mecanismo de inundamiento y corte. Cuando una fuente envía tráfico a una dirección de multicast, los routers que reciben el paquete multicast crean una entrada de reenvío (S,G) e inicialmente reenvían el paquete por las interfaces que cumplan con lo siguiente:

- El chequeo RPF sea exitoso.
- Tengan oyentes IGMP o MLD, o tengan neighbors PIM.

En el caso de que existan varios paths y los costos sean iguales, se escogerá el enlace con la dirección IP más alta del neighbor. Además, cuando existan múltiples routers enviando tráfico multicast sobre la misma subred, PIM ejecuta un proceso de elección de un *Designated Router* (DR) para que éste sea el único en reenviar el tráfico y evitar tramas duplicadas.

Cuando una entrada de estado de reenvío (S,G) es creada en los routers conforme al chequeo RFP, un árbol de distribución SPT es establecido, dando como resultado que los paquetes viajen por el árbol tomando los paths óptimos a través de la red y sin duplicidad. Los routers reenvían el tráfico a través de las interfaces que se encuentren en la lista denominada como outgoing interface list (OIL).

PIM-DM inicialmente inunda la red con el tráfico multicast. Los routers que no poseen hosts interesados en recibir tráfico multicast o neighbors PIM recortan el tráfico por lo cual no lo retransmiten; siendo este proceso periódico ejecutándose cada 3 minutos.

Puesto que las entradas de reenvío son de tipo (S,G), PIM-DM únicamente soporta árboles de distribución fuente.

Dada la naturaleza de PIM-DM, no es adecuado para implementarlo en redes grandes.

En la figura mostrada a continuación se observa que el router R3 envía el mensaje PIM de corte (prune) puesto que el host en una de sus interfaces no está interesado en recibir el tráfico multicast del grupo G.

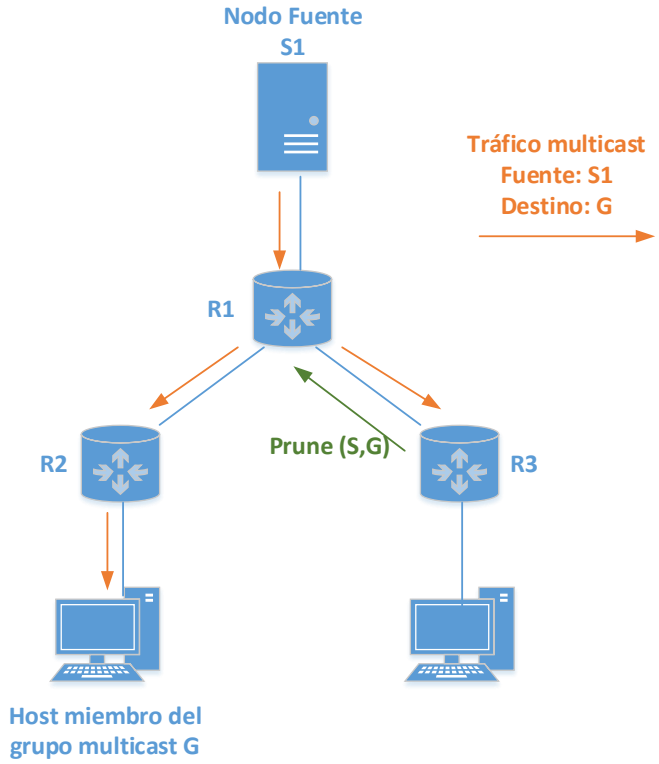


Figura 18. Implementación de inundamiento y corte (flood & prune) de PIM-DM

Fuente: Joseph, V., & Mulugu, S. (2011). *Deploying Next Generation Multicast-Enabled Applications.* Waltham, Estados Unidos: Elsevier.

2.8.4 PROTOCOL INDEPENDENT MULTICAST – SPARSE MODE (PIM-SM)

En PIM-SM únicamente los routers que posean en sus interfaces receptores activos se unirán a grupos de multicast, siendo ésta una ventaja obvia frente al mecanismo de inundamiento y corte de PIM-DM. PIM-SM usa un punto de control conocido como *Rendezvous Point (RP)*. Los routers que en sus interfaces se

encuentran conectados los nodos fuente son conocidos como *First Hop Designated Routers,* los cuales proceden a registrar en el RP las direcciones IP fuente. Cuando hacia el RP fluye tráfico de alguna fuente, éste construye un SPT hacia la mencionada fuente, por lo tanto existirá entradas del tipo (S,G) entre el RP y el nodo fuente.

Los routers que en sus interfaces se encuentran conectados los nodos receptores son denominados como *Last Hop Designated Routers*. Estos routers se unen al RP creando un árbol de distribución compartido con entradas (*,G).

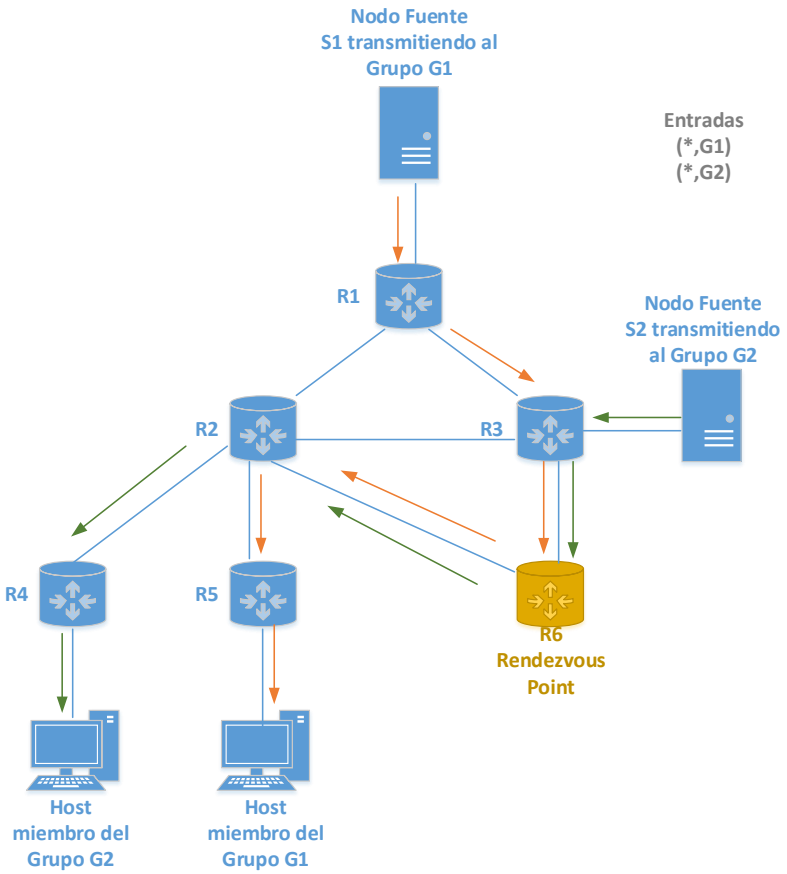


Figura 19. Operación del árbol de distribución compartido en PIM-SM

Fuente: Joseph, V., & Mulugu, S. (2011). *Deploying Next Generation Multicast-Enabled Applications*. Waltham, Estados Unidos: Elsevier.

Teniendo en cuenta las arquitecturas de distribución descritas anteriormente, cuando el nodo fuente transmite tráfico multicast, lo envía hacia el RP mediante el SPT. Este a su vez reenvía el tráfico hacia los receptores mediante el árbol de distribución compartido, siendo el RP el nodo raíz. En la Figura 20 se puede apreciar lo descrito en este párrafo.

Este tipo arquitectura puede dar como resultado la creación de una ruta no óptima hacia determinado receptor, dependiendo de dónde sea posicionado el RP.

2.8.4.1 Embedded RP para IPv6 PIM-SM

En el estándad RFC 3956 se especifica un método para codificar la dirección de un RP de un grupo multicast IPv6 dentro de una dirección multicast basada en prefijo unicast. Para el protocolo PIM-SM este método es un mecanismo para el mapeo de grupo multicast y RP. Con esto se logra una escalable implementación de multicast inter dominio y simplifica la configuración de multicast intra dominio. Para la implementación del RP embebido se debe añadir un nuevo campo para la dirección RP y se ha definido una nueva bandera en el campo flgs.

A continuación, en la figura siguiente se presenta el formato de la dirección IPv6 basada en prefijo unicast modificada.

8 bits	4 bits	4 bits	4 bits	4 bits	8 bits	64 bits	32 bits
11111111	Flgs	Scop	Rsvd	RIID	Plen	Network prefix	Group ID

Figura 20. Formato de la dirección IPv6 basada en prefijo unicast modificada

El primer campo de 8 unos identifica a la dirección como de multicast.

Campo Flgs. - Este campo posee el formato siguiente:

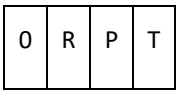


Figura 21. Campo Flgs de la dirección IPv6 RFC 3956

Donde

R = 1 indica que es una dirección multicast *embedded RP* y contiene la dirección de un *Rendezvous Point* de PIM-SM. Cuando R=1, P debe ser 1 y por consiguiente T también debe ser 1, de acuerdo a lo especificado en el RFC 3306 (direcciones IPv6 multicast basadas en prefijos unicast). Por lo indicado anteriormente, el prefijo de este tipo de direcciones es FF70::/12.

Campo RIID. – Este campo corresponde a los cuatro últimos bits de la dirección IPv6 del Rendezvous Point.

Campo Plen. – Define el número de dígitos o longitud que tiene el prefijo de la dirección RP.

Campo Network prefix. – Campo que contiene el prefijo de red unicast IPv6 (justificado a la izquierda) de la dirección RP. Hay que recalcar que este prefijo no debe exceder los 64 bits.

Campo Group ID. – Este campo contiene los 32 bits del ID de grupo multicast IPv6.

A continuación, se propone un ejemplo en el que a partir de una dirección de RP dada se construye la dirección de multicast. La dirección del RP es FCAB:1020:3040::EA/48 y la dirección multicast tendrá alcance de Silte-Local para el grupo multicast 60.

	Flgs	**scop**	**Rsvd**	**RIID**	**plen**	**Network prefix**	**Group ID**
8 bits en 1	R=P=T=1	Site-Local	4 bits en 0	Últimos 4 bits del RP	48 = x3	Prefijo unicast dado	ID definido por el admin. de red
FF	7	5	0	A	30	FCAB:1020:3040	0000:0060

Figura 22. Ejemplo de dirección multicast IPv6 con RP embebido

De la figura anterior, la dirección multicast basada en RP embebido quedaría de la siguiente manera:

FF75:A30:FCAB:1020:3040::60

2.8.5 PROTOCOL INDEPENDENT MULTICAST – SOURCE SPECIFIC MULTICAST (PIM-SSM)

Source Specific Multicast es una extensión de PIM en donde el tráfico es enviado a los receptores únicamente de las fuentes a las cuales dichos oyentes se han unido de manera explícita. En PIM-SSM únicamente se crean árboles de distribución fuente, es decir, con los estados de reenvío (S,G).

En PIM-SSM, el router que se encuentra más cerca al nodo receptor (el *last Hop designated router*) escucha el requerimiento para unirse a una fuente particular de multicast. El nodo receptor realiza el requerimiento a través del modo INCLUDE existente en IGMPv3 o MLDv2 descrito anteriormente. El router multicast envía el requerimiento directamente al nodo fuente en lugar de enviarlo a un RP como lo haría en el caso de PIM-SM. Puesto que el nodo fuente recibe directamente el requerimiento del receptor, la fuente envía el tráfico directamente al receptor a través de SPT.

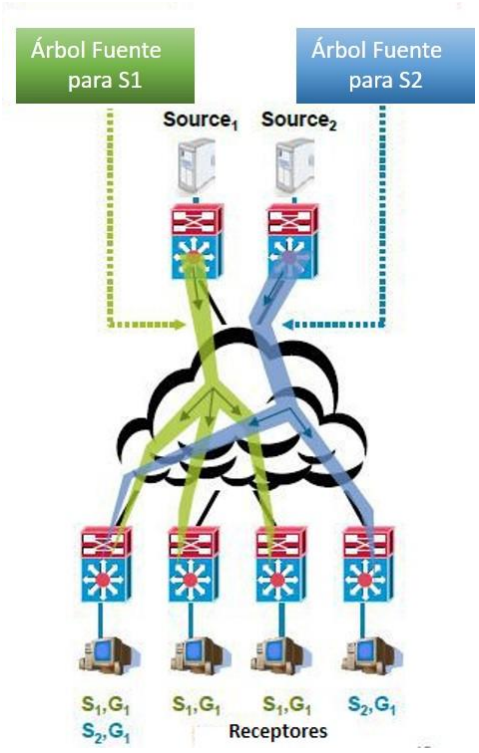


Figura 23. Distribución de tráfico multicast a través de PIM-SSM

Fuente: Ciscohite. (2012). *Multicast Pim Modes – Quick Reference*. Recuperado el 28 de mayo de 2016, de https://ciscohite.wordpress.com/tag/pim-ssm/

Gracias a la característica de tener listas de inclusión y exclusión de fuentes particulares, PIM-SSM posee un cierto grado de seguridad. El tráfico de una fuente a un grupo multicast que no se encuentre en la lista INCLUDE no será reenviado a nodos receptores que no se encuentren interesados.

2.8.6 BIDIRECTIONAL PROTOCOL INDEPENDENT MULTICAST (Bidir-PIM)

Bidir-PIM es una mejora de PIM y su diseño fue pensado para comunicaciones del tipo *muchos-a-muchos*, es decir, varias fuentes y receptores comunicándose entre sí unos con otros al mismo tiempo. Un ejemplo típico de este tipo de comunicaciones es la videoconferencia, en la cual todos los participantes se comunican entre sí.

Bidir PIM utiliza únicamente árboles de distribución compartidos, por lo tanto, existen solamente entradas (*,G) y para evitar loops no utiliza el chequeo RPF. En su lugar utiliza el denominado *Designated Forwarder (DF),* el mismo que es el único router que se encarga de enviar el tráfico de multicast hacia el RP en un segmento de red. La elección del DF sigue el siguiente mecanismo:

- El router con la métrica más baja hacia el RP será el DF
- Si la métrica es igual, el router con la IP más alta en ese segmento de red será el DF.

En el gráfico siguiente se puede apreciar el DF en el segmento de S1, en tanto que para S2, éste también es un receptor por lo que el segmento que lo conecta al RP es un link bidireccional.

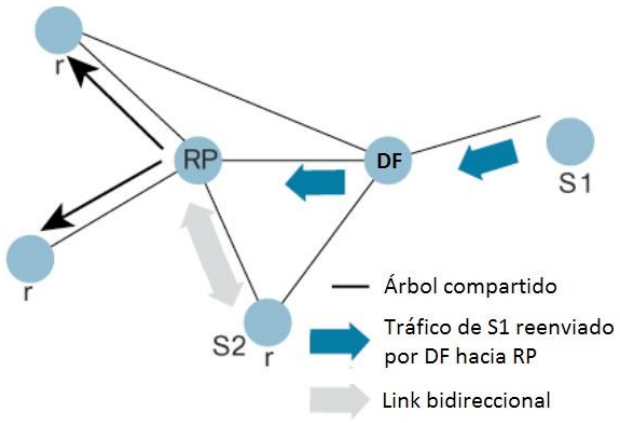


Figura 24. Bidir PIM - Designated Forwarder y Link bidireccional

Fuente: Cisco Systems. (febrero de 2008). *Bidirectional PIM Deployment Guide*. Recuperado el 30 de abril de 2016, de http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multicast-enterprise/prod_white_paper0900aecd80310db2.pdf

Si en el ejemplo de la gráfica anterior la comunicación se diera entre todos los participantes, el árbol de distribución pasaría a ser un árbol de distribución bidireccional, tal como se muestran en la figura a continuación.

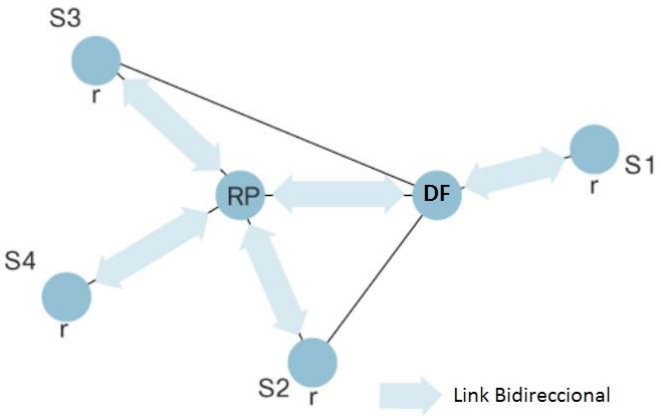


Figura 25. Bidir PIM - Árbol de distribución bidireccional

Fuente: Cisco Systems. (febrero de 2008). *Bidirectional PIM Deployment Guide.* Recuperado el 30 de abril de 2016, de http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multicast-enterprise/prod_white_paper0900aecd80310db2.pdf

2.9 MECANISMOS DE INTEROPERACIÓN Y TRANSICIÓN DE MULTICAST IPv4 A IPv6

La necesidad de transmitir tráfico de multicast IPv6 ha ido incrementándose en los últimos años, especialmente con el auge de las redes de Internet de siguiente generación. Pese a que el número de nodos de IPv6 ha ido en aumento, aún quedan varios años en los cuales las redes IPv6 e IPv4 deban coexistir e interactuar. Con base en esto, se han desarrollado varios mecanismos que permiten la comunicación e interoperabilidad directa entre nodos IPv4 e IPv6 en lo referente a transmisión unicast, no así para la transmisión multicast. Sin embargo, esto está cambiando actualmente puesto que los organismos reguladores y de normalización han visualizado la importancia de la interoperabilidad multicast IPv4 e IPv6. Es así que dichas instituciones y fabricantes se encuentran realizando estudios y pruebas para evaluar la funcionalidad de los mecanismos de transición que se han venido desarrollando en años recientes. A continuación, se describen los dos mecanismos de interoperación y transición más importantes.

2.9.1 DUAL STACK

El mecanismo de dual stack se basa en la combinación de redes multicast IPv4 e IPv6 independientes. Por lo mencionado anteriormente, pueden existir nodos fuente de tráfico multicast independientes, es decir fuentes de IPv4 e IPv6 o nodos dual stack que generen tráfico para ambos grupos IPv4 e IPv6. Así como los nodos fuente pueden ser dual stack, los hosts y routers pueden también correr multicast IPv4 e

IPv6 simultáneamente y lo pueden hacer sobre los mismos links. Las implementaciones más comunes son las del tipo PIM SSM y PIM-SM. En este último tipo de enrutamiento, un router puede fungir como RP para ambos grupos, IPv4 e IPv6.

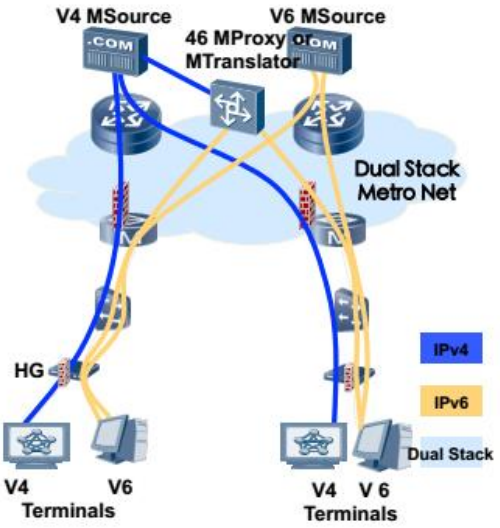


Figura 26. Mecanismo de transición multicast IPv4-IPv6 Dual Stack

Fuente: Jiang, S. (23 de febrero de 2011). *IPv4/IPv6 multicast interoperation*. Recuperado el 15 de octubre de 2015, de Huawei: https://meetings.apnic.net/__data/assets/pdf_file/0013/31315/JiangSheng-Multicast-in-46transition.pdf

Una de las desventajas que tiene el mecanismo de dual stack es en la implementación de videoconferencia debido a que casi todos los elementos que la conforman envía y reciben datos. Puesto que en una red dual stack habrá hosts IPv4 y hosts IPv6, existirán hosts que no se puedan comunicar con otros hosts.

Otro punto adicional a tener en cuenta es que la comunicación en la red dual stack requiere de doble ancho de banda.

2.9.2 MECANISMOS DE TRADUCCIÓN

Con los mecanismos de traducción, hosts IPv6 pueden comunicarse con grupos IPv4 sin ser necesaria la modificación de la infraestructura de red. Para ello, entre los nodos fuente y receptores se deben colocar dispositivos de traducción que entiendan ambos protocolos puesto que deben realizar el mapeo de cada paquete que arribe. El mapeo de direcciones se da como sigue:

- Las direcciones IPv4 son embebidas dentro de las direcciones IPv6
- Las direcciones IPv6 son traducidas a direcciones IPv4

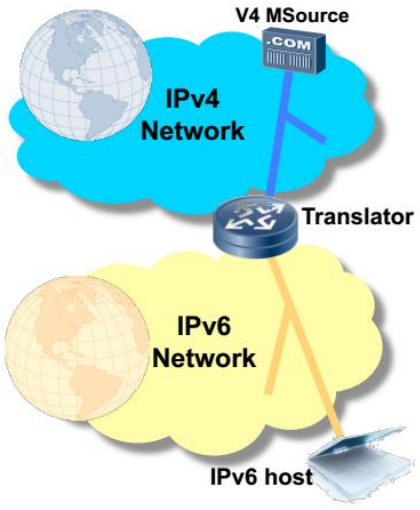


Figura 27. Mecanismo de transición multicast IPv4-IPv6 de Traducción

Fuente: Jiang, S. (23 de febrero de 2011). *IPv4/IPv6 multicast interoperation*. Recuperado el 15 de octubre de 2015, de Huawei: https://meetings.apnic.net/__data/assets/pdf_file/0013/31315/JiangSheng-Multicast-in-46transition.pdf

El mecanismo de traducción puede efectuarse en dos maneras principales, las cuales se describen a continuación.

2.9.2.1 Multicast Reflector

Tal y como su nombre lo sugiere, el reflector multicast refleja la comunicación entre el tráfico IPv4 e IPv6. Para un grupo IPv4 y puertos dados, así como para un grupo IPv6 y sus respectivos puertos de comunicación; el reflector une a ambos grupos de tal forma que escucha y monitorea a los puertos de modo que todo el tráfico que es recibido de un grupo es retransmitido hacia el otro grupo.

El uso de multicast reflector es de utilidad para los proveedores de servicios, en el caso de que éstos brinden sus servicios a través de un protocolo que no sea soportado por el cliente.

La desventaja de los reflectores radica en su bajo rendimiento, por lo cual no es conveniente su implementación para aplicaciones multicast de gran escala. Adicionalmente, el reflector necesita correr una instancia por cada sesión establecida, enviando y recibiendo tráfico aun cuando no existan nodos receptores interesados. Puesto que las conexiones se basan en sesiones, se pueden corren solamente una cantidad limitada de grupos.

Si multicast reflector es usado en redes privadas corporativas, los usuarios típicamente deben contactar con el administrador de red y solicitar una sesión específica para usarla por un tiempo limitado. Una alternativa para automatizar el uso de las sesiones podría ser el acceso mediante una interfaz web.

2.9.2.2 Multicast Gateway

En el Gateway multicast, la dirección IPv4 es embebida en una dirección IPv6 de prefijo /96. Dado el prefijo indicado, los 32 últimos bits de la dirección IPv6 corresponden a la dirección de IPv4, de tal manera que, para cada dirección multicast IPv4 existe su correspondiente dirección multicast IPv6.

Sean

a.b.c.d la dirección de grupo multicast IPv4

PREFIJO el prefijo de 96 bits de la dirección multicast de IPv6

Entonces

- Un host IPv6 puede recibir tráfico de un grupo IPv4 a.b.c.d uniéndose al grupo multicast IPv6 PREFIJO:a.b.c.d/96
- Un host Ipv6 puede enviar tráfico a un grupo IPv4 a.b.c.d uniéndose al grupo multicast IPv6 PREFIJO:a.b.c.d/96

El Gateway está conformado de la siguiente manera:

- En IPv4 el Gateway es un host multicast usando IGMP
- En IPv6 el Gateway es un router PIM y es el RP para el prefijo /96

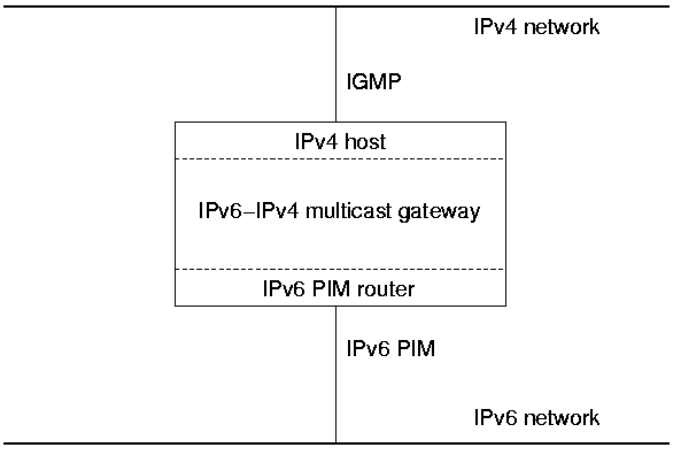


Figura 28. IPv4-IPv6 Multicast Gateway

Fuente: Venaas, S. (s.f.). *IPv4 - IPv6 Multicast Gateway.* Recuperado el 1 de mayo de 2016, de http://www.internet2.edu/presentations/jt2006feb/20060206-mcgw-venaas.ppt

Los hosts IPv6 dentro del dominio de PIM pueden enviar y recibir tráfico multicast a los grupos de IPv4 usando los grupos respectivos de IPv6 a través del multicast Gateway que también es el RP. El Gateway RP conoce si están presentes fuentes IPv6 y recibe todo el tráfico IPv6 enviado para a su vez reenviar este tráfico al correspondiente grupo de IPv4; y si existen receptores de IPv6 los unirá con el grupo de IPv4 y reenviará el tráfico que ha recibido para los mencionados hosts IPv6.

Usando Gateways multicast se pueden implementar videoconferencias con participantes IPv4 e IPv6 tal forma que todos pueden enviar y recibir tráfico teniendo de esta forma una conectividad total de dos vías.

La principal limitación para este tipo de mecanismo es que los usuarios de IPv4 únicamente pueden acceder a las sesiones multicast de IPv6 solamente si usan un grupo de multicast previamente establecido para un prefijo de longitud /96 dado.

CAPÍTULO III. PARÁMETROS DE ANÁLISIS, HERRAMIENTAS Y ESCENARIOS PROPUESTOS PARA LA EVALUACIÓN DE RENDIMIENTO DE TRÁFICO MULTICAST IPv4 E IPv6

3.1 PARÁMETROS DE ANÁLISIS PARA EL RENDIMIENTO DE REDES

3.1.1 THROUGHPUT

Acorde al RFC 1242, el throughput se define como la máxima velocidad a la cual ninguna de las tramas ofrecidas es descartada por el dispositivo. El throughput puede ser medido en octetos por segundo, tramas por segundo y lo más habitual, en bits por segundo (bps).

El throughput puede ser afectado por varios factores, como por ejemplo, al medio físico por el cual se transporte la información, la capacidad de procesamiento de los componentes del sistema de comunicación e incluso por el comportamiento del usuario final.

En términos más amplios, el throughput de una red está definido por el monto de throughput disponible para una aplicación en cualquier momento dado a través de los enlaces de red. Puesto que en una red existen más de una aplicación, el throughput que use una aplicación hará decrecer el throughput disponible para las demás aplicaciones.

La determinación del throughput de red permite a los administradores detectar cuellos de botella que produzcan la disminución de rendimiento en determinados

links que conectan clientes y servidores. El cálculo y determinación del throughput es dependiente de la aplicación y como ésta carga a la red en el tiempo. La mejor práctica consiste en realizar las mediciones en diferentes horas del día y en diferentes días de la semana con lo cual se obtiene una información más amplia de todas las aplicaciones que se encuentran corriendo en la red.

3.1.2 TASA DE TRANSFERENCIA DE DATOS

La tasa de transferencia de datos es una medida de la cantidad de datos enviados entre dos puntos de una red en un periodo de tiempo determinado, siendo su unidad de medida los bits por segundo (bps).

Es necesario indicar que la tasa de transferencia de datos y el ancho de banda son dos conceptos diferentes. La tasa de transferencia representa la cantidad de datos que han sido transferidos realmente entre dos puntos de la red en un tiempo determinado, mientras que el ancho de banda es una medida de la capacidad teórica máxima de transferencia de un dispositivo de la red.

El concepto de tasa de transferencia de datos es importante en la evaluación de dispositivos y tecnologías, reflejando los cambios y mejoras que van teniendo en el tiempo. Así, nuevos dispositivos o tecnologías van presentando tasas de transferencia de datos mucho más altas en cada vez menos tiempo.

3.1.3 LATENCIA

La latencia es el tiempo que le toma a una señal particular, a menudo en forma de paquetes de datos o señales de voz, en alcanzar desde un punto de origen de red

hasta un punto de destino. Este tiempo es medido generalmente en milisegundos. La latencia es un tiempo acumulativo que conlleva el procesar un paquete o señal a través de los diferentes elementos de la red, entre los cuales se encuentran los enlaces de red, switches, routers, Access points, hosts, servidores y cualquier otro dispositivo o componente de red que requiera procesar la transmisión.

Entre los factores que contribuyen a la latencia se incluyen los indicados a continuación:

- *Encripción y desencripción de paquetes*, especialmente los que ingresan y egresan de los routers, los cuales requieren tiempo de procesamiento adicional agregando latencia.
- *Latencia de propagación*, incluyendo el retardo de transmisión de la señal más el tiempo de procesamiento de los dispositivos de transmisión.
- *Saltos de red*, los cuales son puntos de conexión entre redes y que son capaces de aumentar la latencia a medida que crecen en número. Dentro de esta clasificación se encuentran los routers y firewalls, típicamente situados en los bordes de las redes, los mismos que inspeccionan cada paquete que circulan a través de ellos, agregando latencia.
- *Desacople entre los dispositivos de red y los links* pueden contribuir a aumentar la latencia. El desequilibrio en el rendimiento en un path de transmisión a través de redes diferentes puede llegar a disminuir el throughput de una aplicación. Un host podría estar procesando una aplicación

cuyo throughput no se ajuste con otros dispositivos de la red, con lo cual se generaría un cuello de botella en el path de transmisión.

3.1.3.1 Tiempo de respuesta

Dependiendo del contexto, la latencia es usada como como sinónimo de tiempo de respuesta; siendo este último, el tiempo que transcurre desde que un requerimiento es enviado hasta que la respuesta es recibida. El tiempo de respuesta puede ser interpretado como la latencia de ida y vuelta (*Round Trip Time, RTT*) desde la perspectiva del usuario o desde la perspectiva del dispositivo que envía el requerimiento. El tiempo de respuesta afecta directamente a la rapidez de las aplicaciones para trabajar en la red. Aplicaciones tales como Telnet, las cuales requieren que el usuario espere el eco de cada pulsación de una tecla por parte del host remoto, son extremadanamente vulnerables al bajo tiempo de respuesta de red.

En grandes redes, existen muchos factores que pueden afectar los tiempos de respuesta entre el cliente y el servidor. Estos factores pueden ser los siguientes:

- Tormentas de broadcast
- Dispositivos de red defectuosos
- Hosts sobrecargados
- Cableado de red defectuoso
- Errores en la red
- Segmentos de red sobrecargados

Si bien el tiempo de respuesta permite conocer el estado de procesamiento de la red, el retardo de transmisión, el enrutamiento, entre otros, la evaluación del estado del servicio de red también involucra el procesamiento de CPU de los dispositivos, el procesamiento de la aplicación, la transferencia de datos desde el sistema de storage, etc., por lo que estos parámetros también deben ser considerados.

3.1.4 JITTER

El jitter es definido como la variación en el retardo de los paquetes recibidos. Desde la perspectiva del lado desde donde se envían los paquetes, éstos son enviados en un flujo continuo y uniformemente espaciados. Debido a la congestión presente en la red, encolamiento inapropiado o errores de configuración, el estado uniforme de flujo de paquetes puede corromperse haciendo que el retardo entre cada paquete varíe en lugar de permanecer constante.

Las aplicaciones de servicios en tiempo real, tales como transmisiones de voz y video, son sensibles al jitter y por consiguiente requieren una variación de latencia mínima, de lo contrario el servicio puede verse impactado negativamente en el rendimiento. Para manejar el jitter en aplicaciones en tiempo real se usa el buffer de de-jitter, el cual es el encargado de compensar el jitter que se encuentra en el flujo de paquetes que recibe. En la figura presentada a continuación se observa como los paquetes llegan al buffer de de-jitter con cierto grado de variación de retardo, para luego ser corregido.

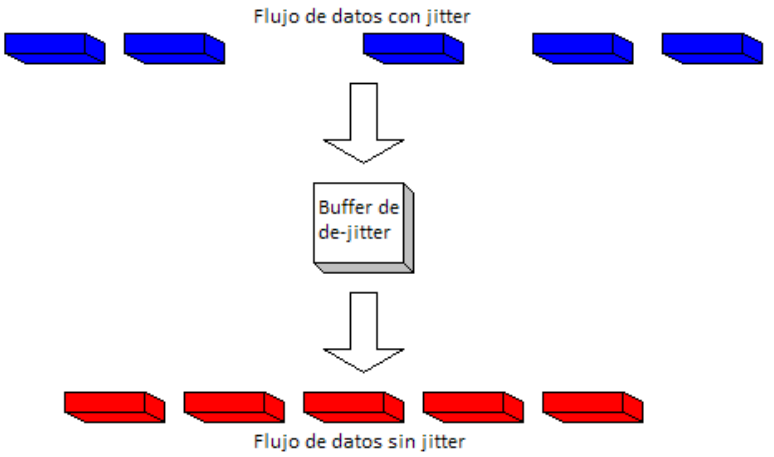


Figura 29. Funcionamiento del buffer de de-jitter

Fuente: Cisco Systems. (2 de febrero de 2006). *Understanding Jitter in Packet Voice Networks.* Recuperado el 8 de mayo de 2016, de http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html

El jitter total está compuesto de acuerdo a un modelo jerárquico tal y como se muestra en la figura a continuación, cuyos componentes se explican seguidamente.

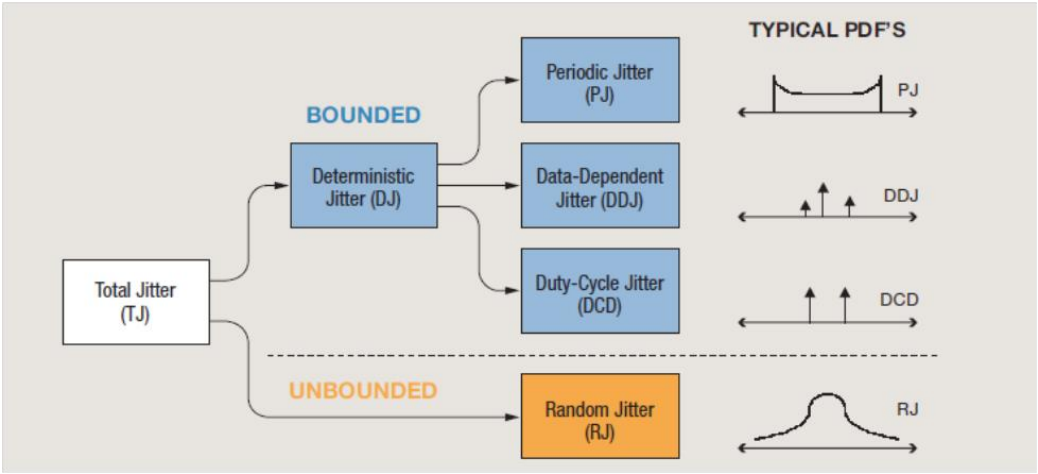


Figura 30. El Jitter y sus componentes

Fuente: National Instruments. (17 de abril de 2013*). Understanding and Characterizing Timing Jitter.* Recuperado el 8 de mayo de 2016, de http://www.ni.com/white-paper/14227/en/

3.1.4.1 Jitter Aleatorio

Es un ruido en el tiempo que no puede ser pronosticado, puesto que no tiene un patrón discernible. Para propósitos de modelamiento matemático, se asume que puede ser representado mediante una distribución de tipo Gaussiana. La razón para asumir aquello se basa en que la fuente primaria de ruido aleatorio en los circuitos eléctricos es el ruido termal (conocido también como ruido de Jhonson) el cual es representado mediante una distribución Gaussiana.

3.1.4.2 Jitter Determinístico

Este tipo de jitter es repetitivo y predictivo, por lo que sus valores pico-pico pueden ser pronosticados con un alto grado de exactitud con un número razonablemente bajo de observaciones. Dentro de esta categoría se encuentran las subdivisiones siguientes.

- **Jitter periódico**. - Es el tipo de jitter que se repite en forma periódica. Puesto que una forma de onda periódica puede descomponerse en una serie de Fourier de sinusoides relacionadas armónicamente, este tipo de jitter suele llamarse como jitter sinusoidal. El jitter periódico es causado por fuentes de ruido externo determinístico acoplados al sistema, tales como fuentes de poder de switches o fuentes de portadoras de RF.
- **Jitter dependiente de datos**. - Jitter correlacionado con la secuencia de bits en un flujo de datos y es normalmente causado por la respuesta de frecuencia de un cable o un dispositivo de red. Dado que los cambios de estado son predecibles

y se encuentran relacionados con los datos, este tipo de jitter es llamado también como interferencia inter-símbolo o ISI.

- **Jitter dependiente del ciclo de operación**. - Jitter que puede ser pronosticado con base a su asociación al flanco de subida o de bajada. La primera causa para este tipo de jitter se da cuando la máxima velocidad de respuesta para los flancos de subida es diferente para los flancos de bajada. La segunda causa se presenta cuando el umbral de decisión[3] para una forma de onda es más alta o más baja de la que debería ser.

3.1.5 PÉRDIDA DE PAQUETES

Las pérdidas de paquetes se presentan cuando uno o más paquetes de datos no consiguen arribar a su destino. Existen algunas causas que provocan la pérdida de paquetes, sin embargo, las más comunes son descritas a continuación.

Congestión. - Ocurre cuando el buffer de un dispositivo se sobrecarga. Muchas aplicaciones son capaces de manejar la congestión, reduciendo la tasa de transferencia o con retransmisión de datos. En aplicaciones que no son en tiempo real, como por ejemplo el correo electrónico o descargas, el efecto de pérdida de paquetes es mínimo para el usuario, no así en aplicaciones en tiempo real, como la voz sobre IP en la cual no es posible el reenvío de paquetes y por consiguiente el usuario experimenta cortes en la comunicación, y ante una severa pérdida de paquetes el corte total de la misma. Caso similar ocurre con la videoconferencia.

[3] Umbral de decisión: Valor mínimo de una magnitud que provoca una determinada respuesta.

Para manejar la congestión se puede aumentar el ancho de banda de los links o se puede dar calidad de servicio QoS al tráfico de tiempo real.

Rendimiento de dispositivos de red. – En dispositivos de red tales como routers, switches, firewalls, etc., es común que se realicen upgrades de hardware, como sería el caso de una tarjeta de red para soportar mayor ancho de banda. Sin embargo, puede darse el caso de que el CPU del equipo no se encuentre preparado para manejar el nuevo volumen de tráfico que ingresa y/o egresa al dispositivo producto de la mencionada actualización.

Problemas de software en los dispositivos de red. – Los IOS no son perfectos y ocasionalmente presentan bugs que causan que nuevas aplicaciones desarrolladas no funcionen del todo bien. Para remediar estos inconvenientes siempre se deben tener instaladas las últimas versiones estables recomendadas por el fabricante.

Fallas en el medio de transmisión o hardware. – Si los reportes de monitoreo indican que los enlaces no se encuentran saturados y la utilización de hardware se encuentra dentro de las especificaciones, la causa más común de pérdida de paquetes es asociada a inconvenientes con las interfaces de red, ya sea en el hardware como tal o en los enlaces. Ante esto, tanto el hardware defectuoso como el medio físico, ya sea cobre o fibra óptica deben ser reemplazados.

Para el caso de comunicaciones inalámbricas, se deben observar parámetros como la potencia de recepción; la atenuación de la señal causada por el clima, fuentes de RF cercanas u obstáculos.

3.2 HERRAMIENTAS UTILIZADAS PARA LA EVALUACIÓN DE LOS PARÁMETROS DE ANÁLISIS

3.2.1 JPERF

Jperf provee una interfaz gráfica en Java de Iperf, la cual es una herramienta bajo línea de comandos que permite evaluar el rendimiento de redes IPv4 e IPv6. Con Iperf es posible llevar a cabo diferentes tipos de pruebas de paquetes TCP y UDP, las mismas que son ejecutadas entre 2 hosts en la modalidad cliente-servidor. Tanto Jperf como Iperf pueden correr bajo Linux y Windows. Cada opción de línea de comandos que se puede ejecutar en Iperf se encuentra disponible en la interfaz gráfica Jperf mediante botones o cajas de texto.

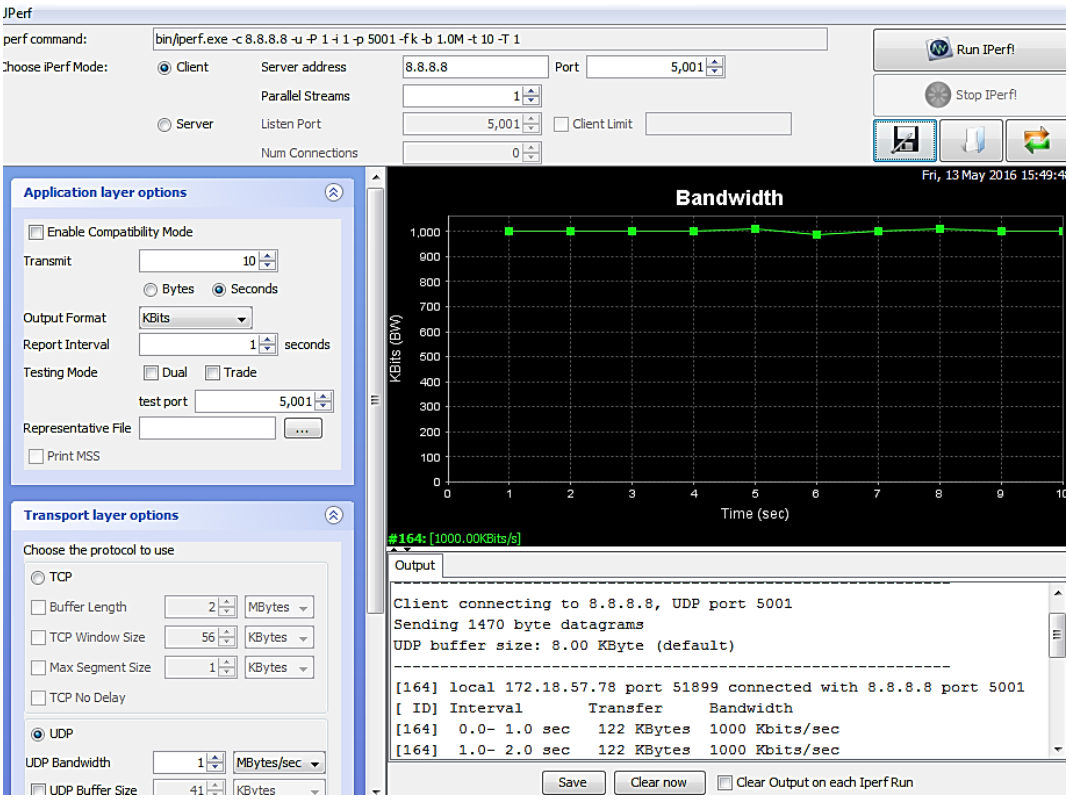


Figura 31. Interfaz gráfica de usuario de Jperf

Dentro de las mediciones con paquetes TCP que se pueden realizar con Jperf se encuentran las siguientes:

- Ancho de banda total
- Ancho de banda asignado a múltiples conexiones
- Tamaño de ventana TCP por defecto usado por el host de prueba
- Valor por defecto de Path MTU Discovery usado por el host de prueba
- Manejo de paquetes ToS efectuados por un router

Además de las pruebas descritas, Jperf tiene modos que permiten determinar automáticamente el tamaño óptimo de ventana TCP y el tamaño de MTU usado por los sockets. Estas características pueden ser de gran utilidad al memento de configurar aplicaciones de red.

Jperf también puede ser usado para las mediciones de las siguientes características UDP:

- Rendimiento UDP para un determinado ancho de banda
- Pérdida de paquetes UDP en un flujo de datos
- Delay y jitter en un flujo de datos UDP
- Rendimiento de paquetes UDP multicast

Jperf permite realizar pruebas de rendimiento de tráfico multicast mediante el envío de paquetes por parte del cliente a una dirección específica de multicast y configurar uno o más servidores que escuchen la misma dirección de multicast,

permitiendo de este modo probar el rendimiento multicast en diferentes segmentos de red.

3.2.1.1 Modo Cliente

Para utilizar a la herramienta Jperf en modo cliente en el presente trabajo se habilitan y configuran las siguientes características que se encuentran mostradas en la figura 32 y que se describen a continuación.

En la *opción Choose iPerf Mode* se selecciona *Client* y seguidamente en la caja de texto *Server address* se introduce la dirección IPv4 o IPv6 del host que actuará en modo servidor al cual se envía el tráfico de prueba, o como en este caso, se pueden introducir direcciones de multicast.

En la opción *Transmit* de la sección *Application Layer Options* se selecciona la opción *Seconds* y en la caja de texto se coloca el valor de tiempo en segundos que se requiera transmitir el tráfico de prueba.

En la sección *Transport Layer Options* se escoge UDP, en la caja de texto *UDP Bandwidth* se coloca el valor de la tasa de transferencia de datos deseada y finalmente se habilita la opción *UDP Packet Size* para configurar el tamaño de paquete UDP de acuerdo a las pruebas realizadas más adelante.

En la caja de texto TTL de la sección *IP Layer OIptions* se configura para este caso, un valor de 4 (o mayor) puesto que son cuatro los saltos que los paquetes UDP deben recorrer para llegar hacia el host receptor de los paquetes multicast, de acuerdo a la figura 49.

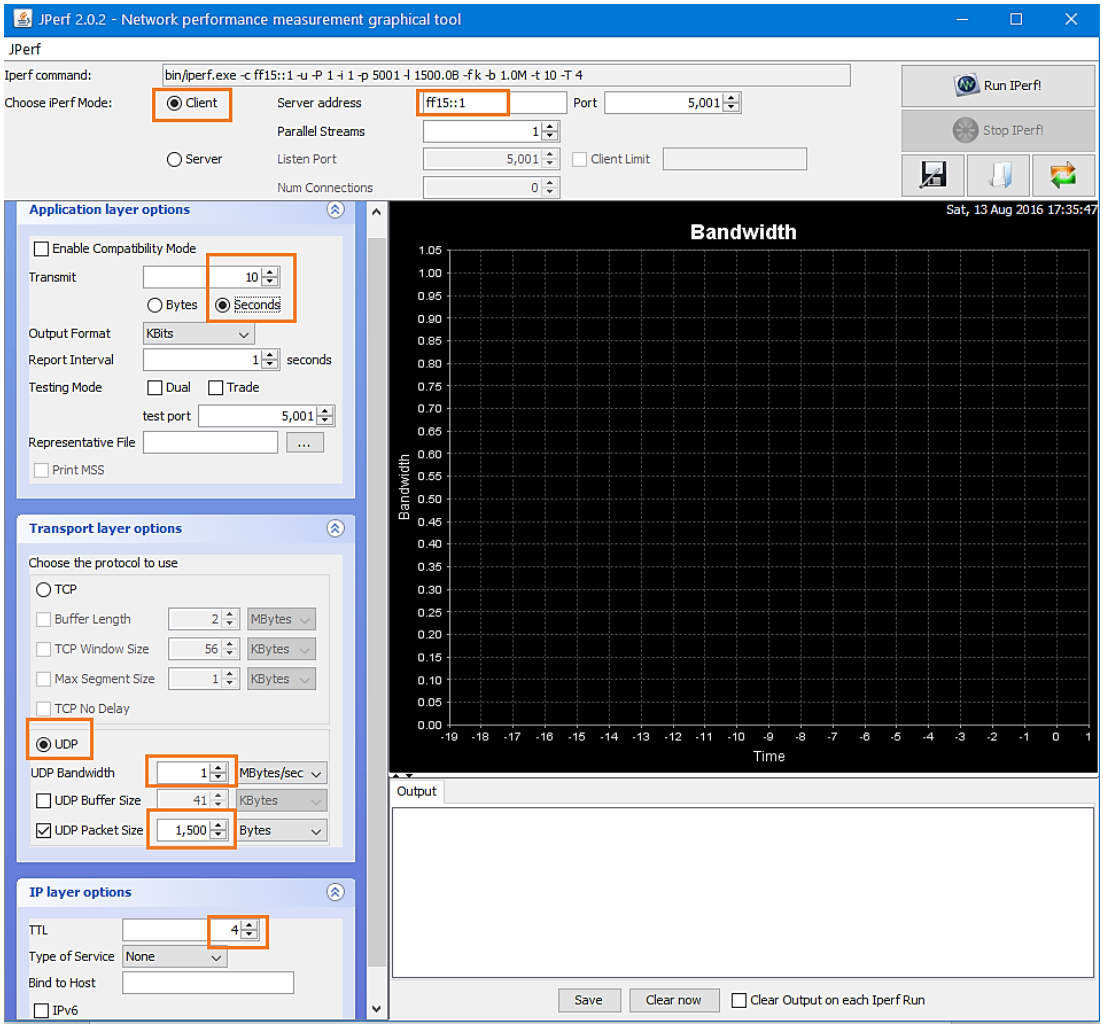


Figura 32. Parámetros de configuración de Jperf en modo cliente

3.2.1.2 Modo Servidor

Para la configuración de Jperf en modo servidor, se realizan las configuraciones descritas a continuación.

En la *opción Choose iPerf Mode* se selecciona *Server.*

En la sección *Transport Layer Options* se escoge UDP.

En la caja de texto *Bind to Host* de la sección *IP Layer Options* se debe colocar la dirección IP multicast a la cual se envía el tráfico de prueba. Si la dirección multicast es IPv6 se debe habilitar la correspondiente opción, tal como se muestra en la figura siguiente.

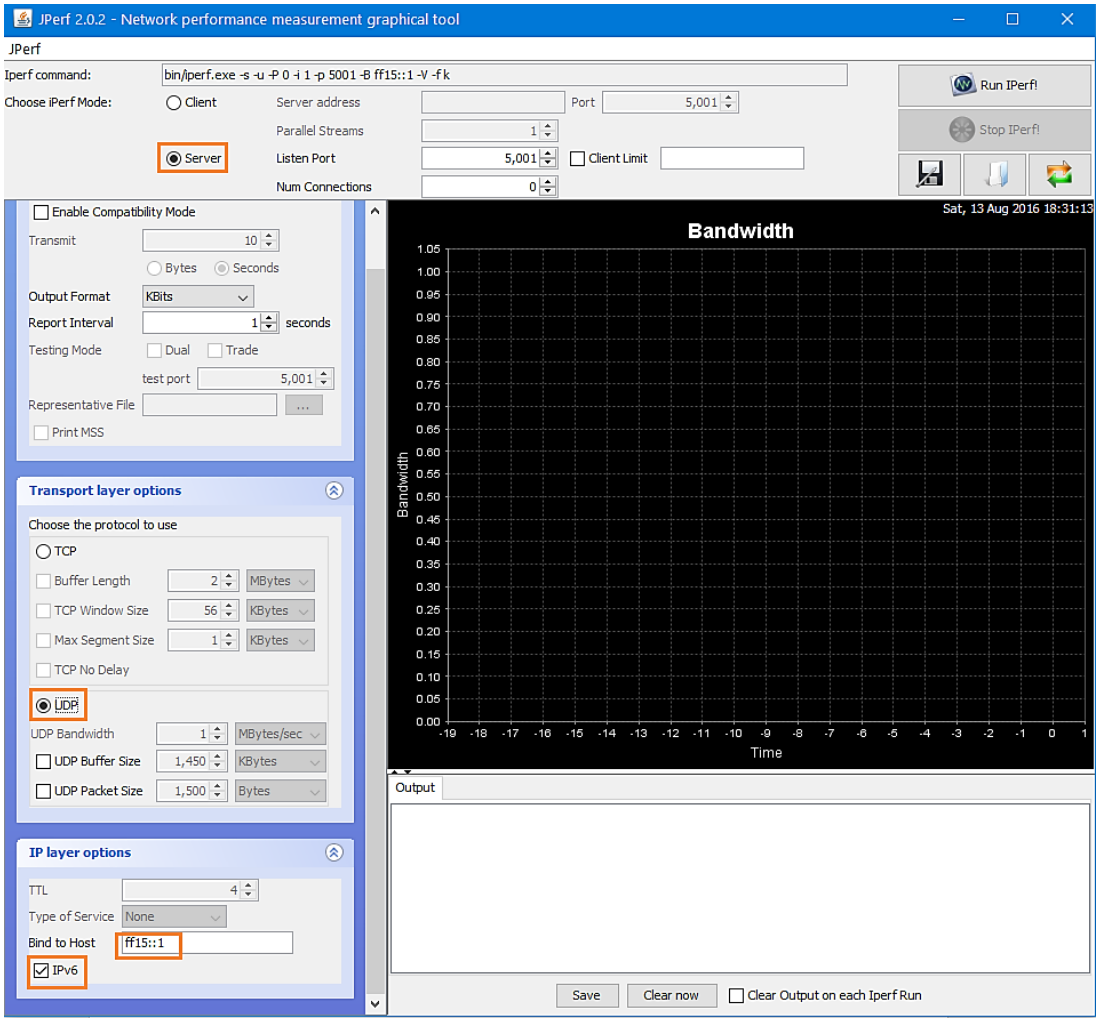


Figura 33. Parámetros de configuración de Jperf en modo servidor

3.2.2 REPRODUCTOR MULTIMEDIA VIDEOLAN VLC

VideoLAN VLC, más conocido como VLC, es un popular reproductor multimedia bajo licencia GNU usado por un gran número de personas y organizaciones para reproducir varios formatos de audio y video, así como también varios protocolos de transmisión. En sus inicios, VLC fue concebido como un proyecto estudiantil de ingeniería en la universidad de École Centrale de Paris en 1996, pero en la actualidad es un proyecto global con contribuyentes de alrededor de 20 países. Originalmente, VLC fue diseñado para transmitir videos en formato MPEG en redes de banda ancha, sin embargo, en los últimos años ha llegado a convertirse en un potente servidor de transmisión de video en varios formatos en vivo o bajo de manda, ya sea sobre una red privada o a través de internet.

Figura 34. Interfaz gráfica de usuario del reproductor multimedia VLC

VLC es soportado por sistemas operativos tales como Windows, Linux, Mac OS X, Android, Solaris, entre otros. Es capaz de reproducir los formatos de video y audio más populares, entre los que se pueden destacar MPEG-1/2, MPEG-4/DivX, h264, webm, mkv, WMA, WMW, AVI, DVD, ACC, MP3.

En cuanto a la transmisión por la red, VLC es capaz de realizar transmisiones unicast UDP y RTP, multicast UDP y RTP, HTTP, RTSP, MMS, entre otras.

3.2.2.1 Emisión de video

Con la finalidad de ejecutar el análisis de rendimiento de multicast IPv4 e IPv6 se efectuarán emisiones de tráfico de archivos de video, para lo cual se utilizará el reproductor VLC.

Para realizar las emisiones de video mencionadas, primeramente, en la barra de herramientas se debe escoger la opción *Medio* y luego *Emitir…*

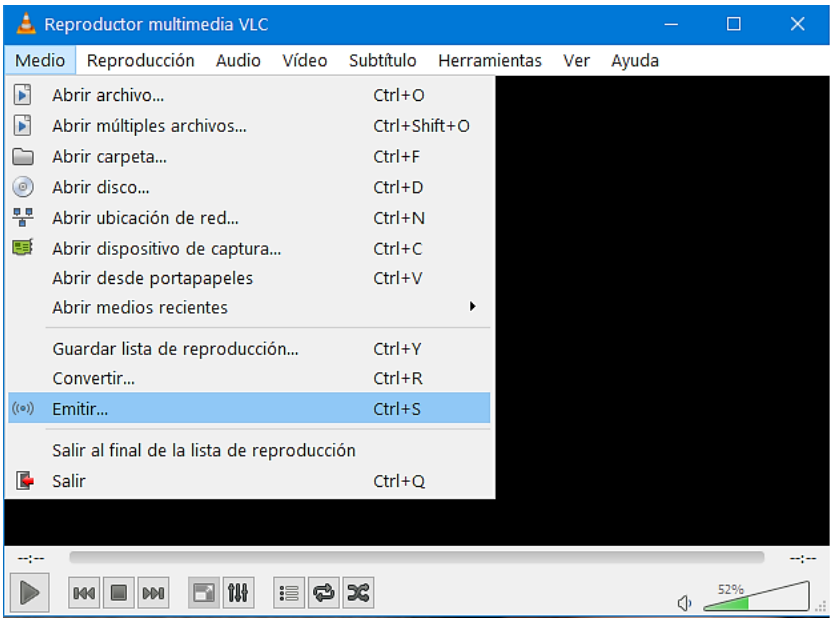


Figura 35. Selección de la opción de emisión de video en VLC

Posterior a la selección de emisión y del archivo de video a transmitir, se debe escoger el método de emisión. En este caso se selecciona *RTP / MPEG Transport Stream* puesto que se usará el procedimiento de análisis de flujos RTP con Wireshark como se explicará más adelante.

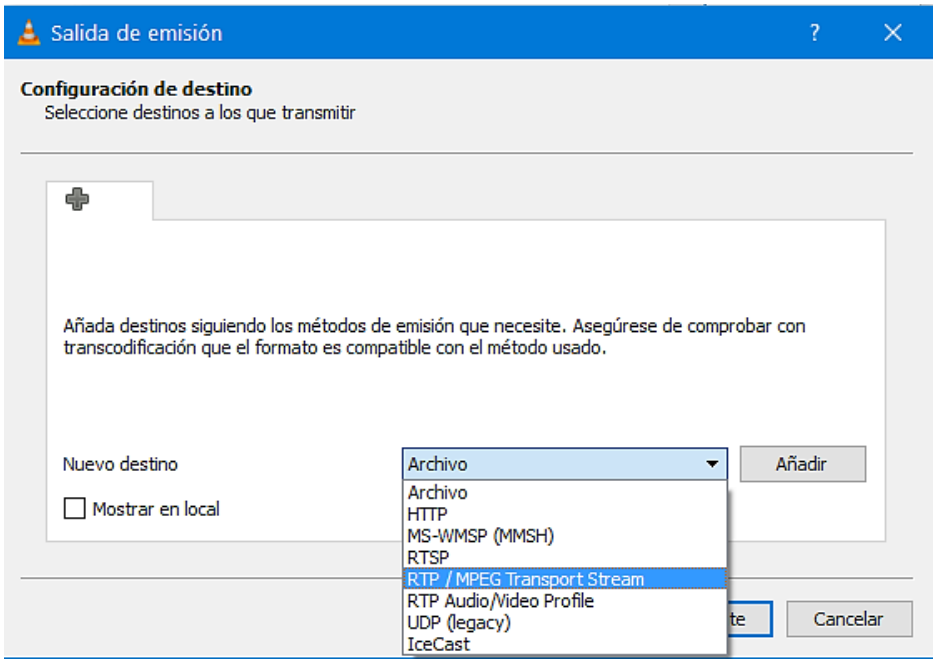


Figura 36. Selección del método de emisión de video en VLC

Luego de la selección del método de transmisión se debe indicar la dirección IPv4 o IPv6 a la cual irá dirigido el tráfico de video con su respectivo puerto de destino. En este caso es la dirección multicast IPv4 239.1.1.1 con puerto de destino 5004.

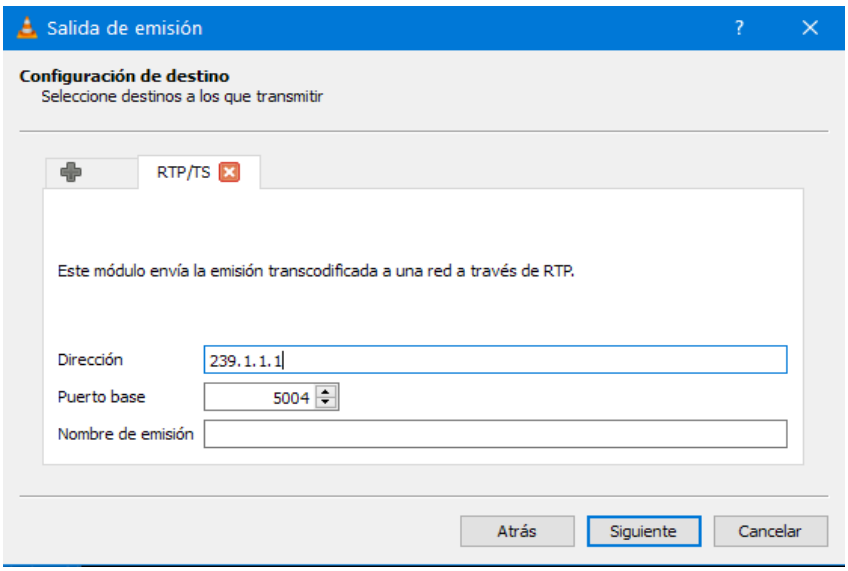


Figura 37. Especificación de la dirección IP y puerto de destino para transmisión de video en VLC

Es necesario indicar que para el caso de la evaluación de rendimiento se ha deshabilitado la opción de transcodificar debido a que es necesario enviar el flujo de video tal como es, sin compresión ni calidad de servicio para obtener los valores reales de rendimiento de la red.

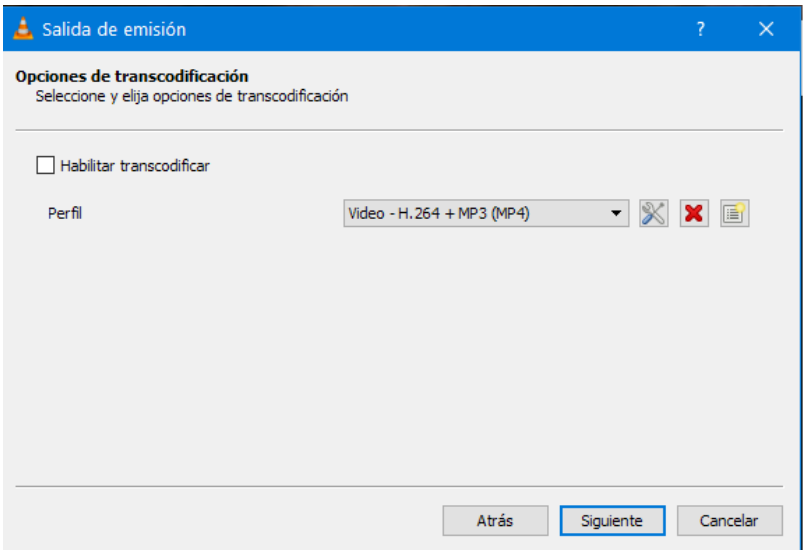


Figura 38. Des habilitación de la opción transcodificar video en VLC

Finalmente, y de manera similar a la configuración de Jperf, es preciso incluir el valor de TTL, el cual que tendrá un valor mínimo de 4.

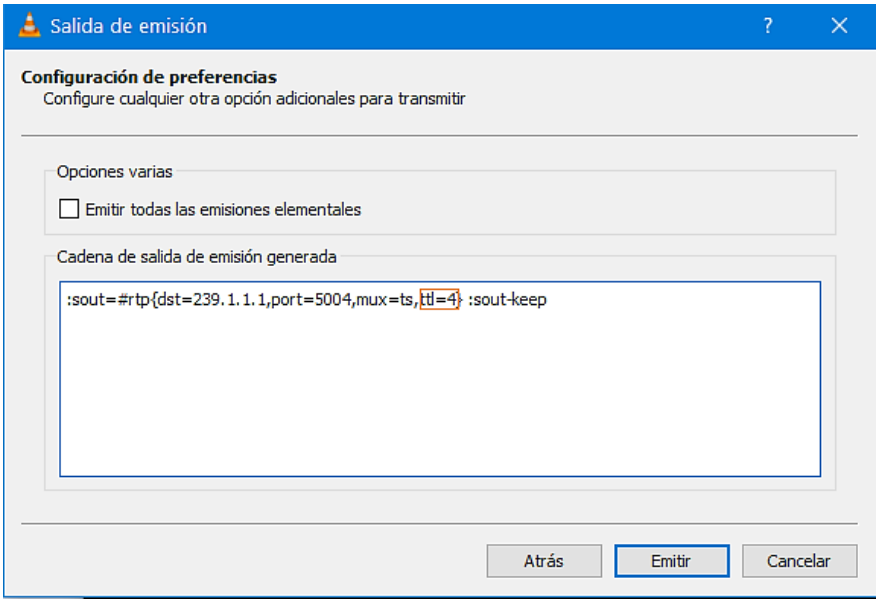


Figura 39. Configuración del valor de TTL para la emisión de video en VLC

3.2.2.2 Reproducción de video

Para configurar a VLC en modo de reproductor de video de red, primeramente, hay que situarse en la barra de herramientas y hacer click en *Medio, Abrir ubicación de red…*

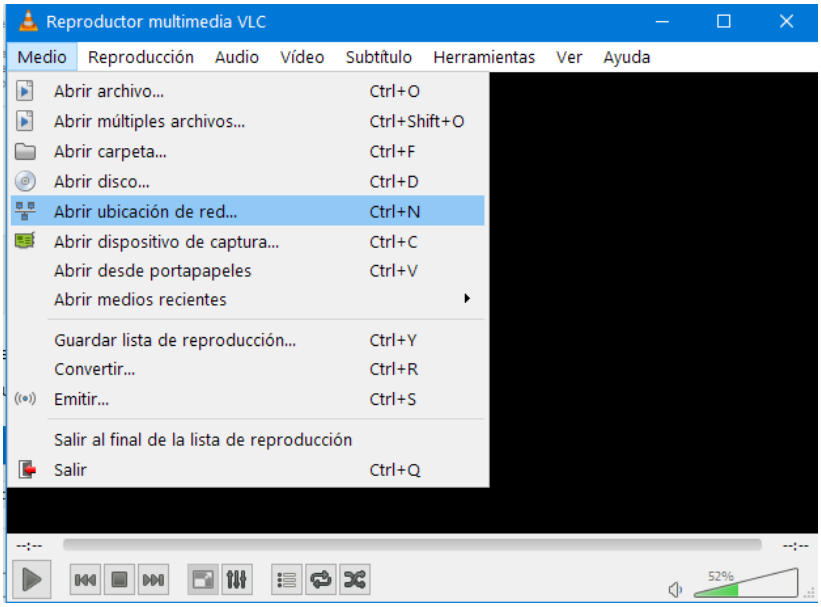


Figura 40. Selección de la opción de reproducción de video de red de VLC

En la caja de texto se debe introducir la dirección IP que recibe el tráfico de video seguido del puerto de destino. Debido a que el tráfico recibido es multicast RTP, la sintaxis es la que se muestra en la figura siguiente.

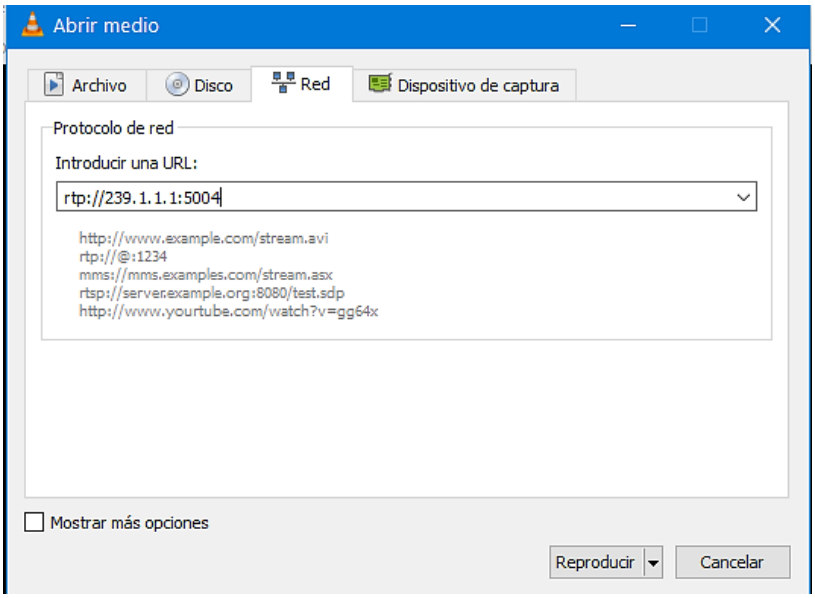


Figura 41. Especificación de la dirección IPv4 y puerto de destino para reproducir video con VLC

Si se trata de una dirección de multicast IPv6, ésta debe ser encerrada entre paréntesis cuadrados, tal como se muestra a continuación.

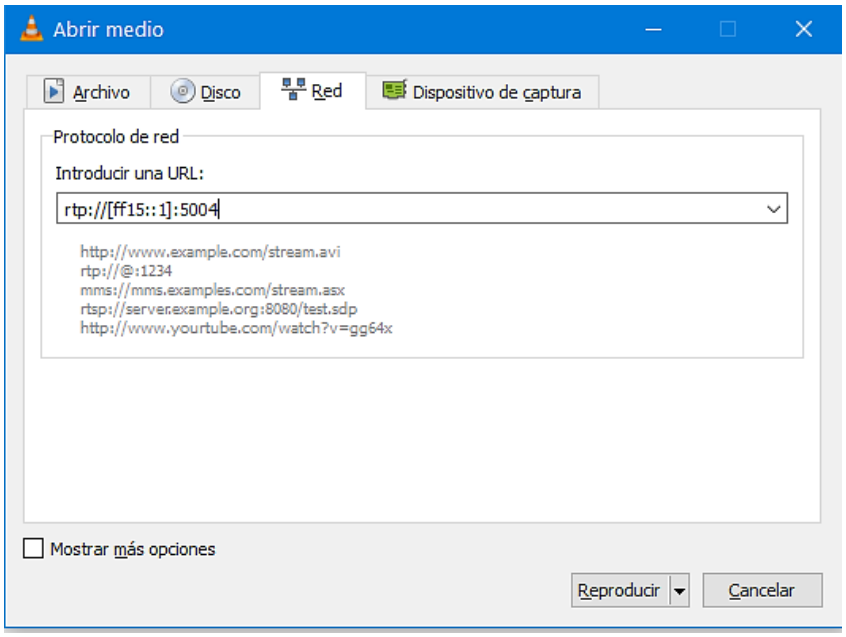


Figura 42. Especificación de la dirección IPv6 y puerto de destino para reproducir video con VLC

3.2.3 WIRESHARK

El análisis de red y/o protocolos es utilizado para estudiar las propiedades de las redes, tales como la capacidad, conectividad y rendimiento. En tal virtud, el análisis de red puede ser usado para estimar la capacidad de una red existente, verificar las características de rendimiento o planear futuras aplicaciones o mejoras. Una de las mejores herramientas para el análisis de rendimiento de redes es Wireshark.

Wireshark es un analizador de paquetes de red utilizado para realizar la captura de los mencionados paquetes para luego desplegarlos de una manera detallada para su correspondiente análisis interpretando los diferentes protocolos en uso. Los datos decodificados son mostrados en un formato de modo que sean fáciles de entender fuera del encapsulamiento de las capas que los contienen. Wireshark también está en la capacidad de capturar solamente tráfico que coincida con el criterio de un filtro definido por el administrador de red, permitiendo así capturar solo tráfico relevante.

En la figura mostrada a continuación, se pueden apreciar los tres paneles principales de Wireshark. Desde arriba hacia abajo, se encuentran los paneles de Resumen, Detalle y Hexadecimal. El panel de Resumen muestra en detalle de alto nivel la secuencia numérica de los paquetes capturados, la hora a la que fueron capturados, las direcciones IP fuente y destino, protocolo usado, longitud del paquete y otra información. Al seleccionar un paquete de este panel se puede observar información con detalle más granular en el panel de Detalle. En el panel Hexadecimal se puede observar la data hexadecimal específica capturada del paquete en cuestión.

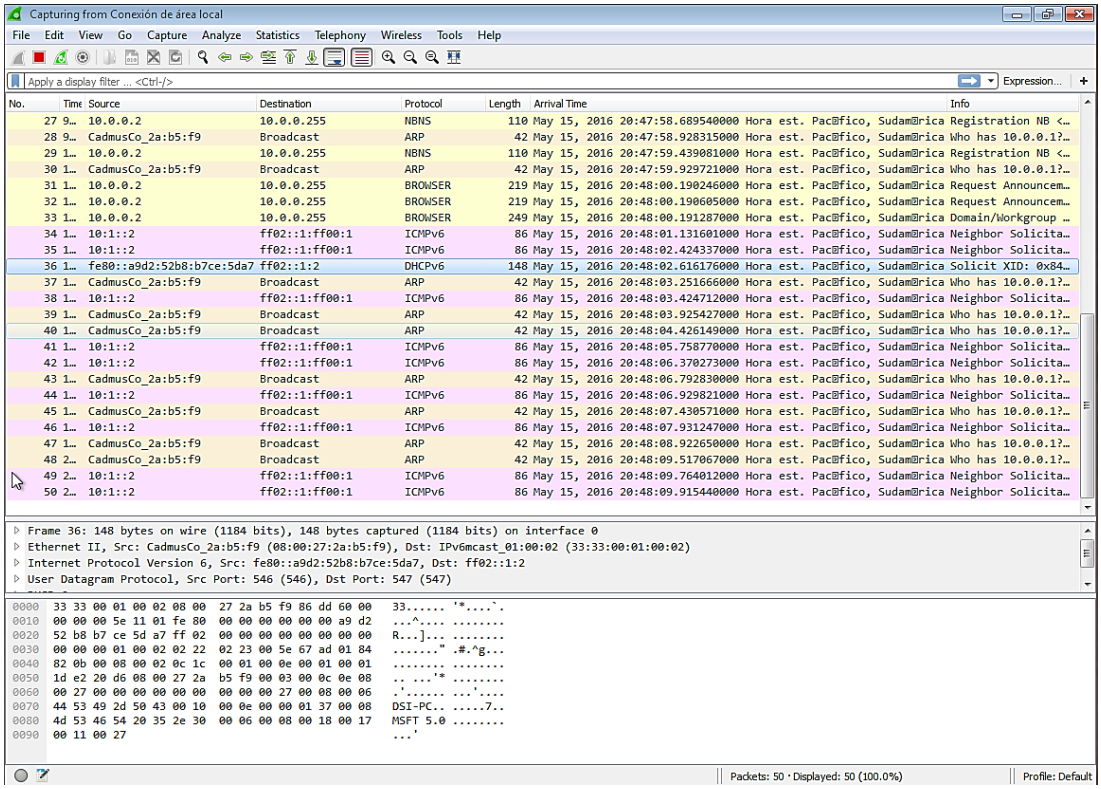


Figura 43. Interfaz gráfica de usuario de Wireshark. Paneles de Resumen, Detalle y Hexadecimal

Un punto a tener en cuenta es que la tarjeta de red que sea utilizada para la captura de los paquetes debe ser usada en modo promiscuo, para lo cual se debe instalar la aplicación WinPcap, siendo ésta una librería para Windows. Sistemas distintos pueden usar la aplicación Libcap.

A continuación, se presentan algunas de las características más relevantes de Wireshark

- Disponible para Windows y Linux
- Captura de paquetes en tiempo real

- Apertura y lectura de archivos que contienen paquetes de datos capturados con tcpdump, WinDump y otros programas de captura de paquetes
- Importación de paquetes desde archivos de texto que contienen paquetes de datos en formato hexadecimal
- Despliegue de paquetes con información muy detallada acerca de los protocolos
- Posibilidad de guardar los paquetes de datos capturados.
- Exportar algunos o todos los paquetes en otros formatos de archivo
- Filtrar y buscar paquetes de acuerdo a muchos criterios
- Colorear paquetes de acuerdo a filtros
- Creación de varias estadísticas

3.2.3.1 Obtención de jitter y pérdida de paquetes

Con la finalidad de obtener los datos de jitter y pérdida de paquetes referentes a las pruebas con video multicast, se utilizará el análisis de telefonía del cual dispone Wireshark, puesto que esta opción permite realizar el análisis de paquetes RTP en función de jitter y pérdida de paquetes.

Para ejecutar el análisis de los paquetes RTP, en primera instancia se deben decodificar como RTP los datos obtenidos en la captura. Para esto, se debe dar click derecho sobre un paquete parte del flujo que se desee decodificar y a continuación da click en *Decode As…*

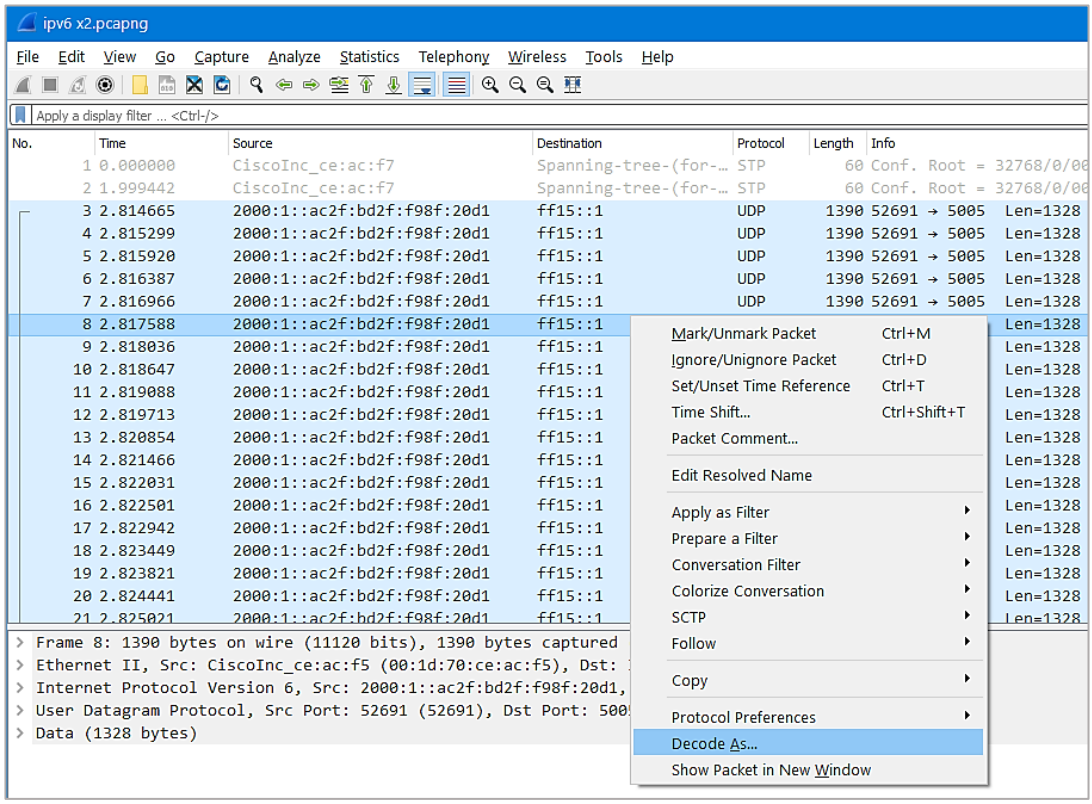


Figura 44. Opción de Wireshark para decodificar paquetes

En la pestaña *Current* se debe buscar y escoger el protocolo RTP y luego dar click en *OK.*

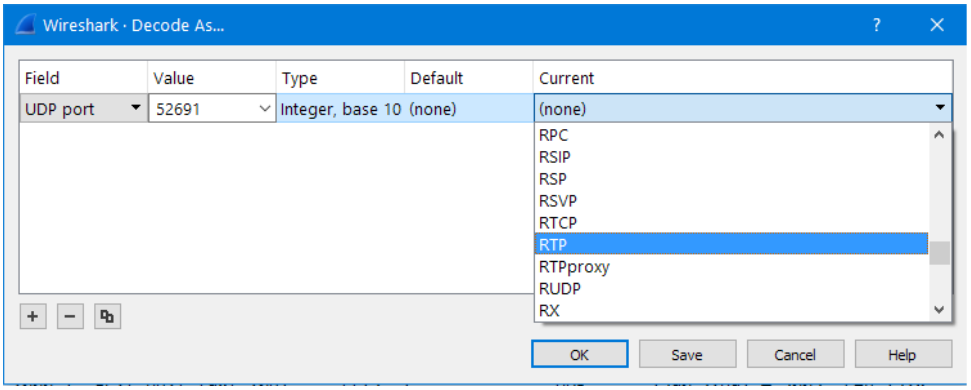


Figura 45. Opción de Wireshark para decodificar paquetes a RTP

En el panel de resumen los paquetes capturados aparecerán ya no como UDP sino como paquetes MPEG. Luego de decodificar los paquetes hay que ir a la barra de herramientas para escoger *Telephony, RTP, RTP Streams.*

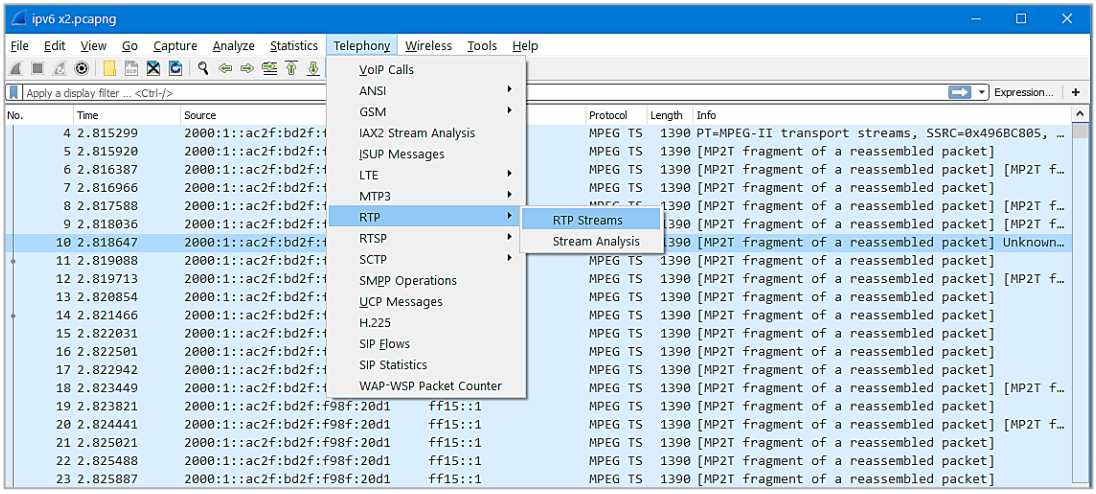


Figura 46. Opción de Wireshark para el análisis de paquetes RTP

A continuación, se debe escoger el flujo de datos RTP a analizar y luego dar click en *Analyze*. Nótese que en esta presentación ya se muestra el valor de pérdida de paquetes, sin embargo, en la siguiente pantalla el mencionado parámetro se muestra con más detalle.

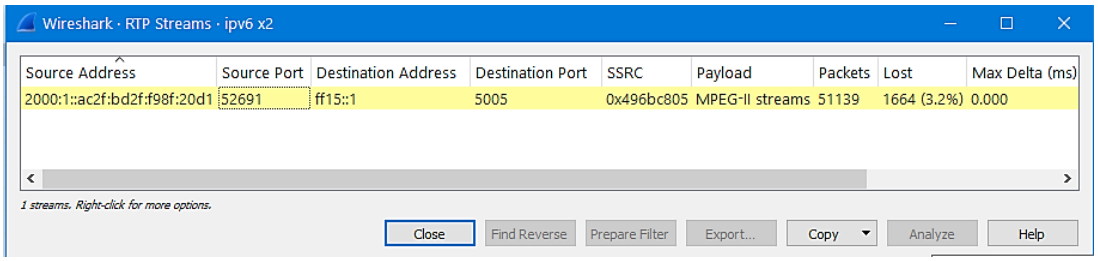


Figura 47. Análisis de flujos RTP con Wireshark

Finalmente, se obtienen los datos de pérdida de paquetes y jitter. Puesto que los valores de jitter están dados para cada paquete, es necesario guardar los datos obtenidos en un archivo de formato CSV con la finalidad de posteriormente procesarlo con una hoja de cálculo y encontrar, como en el caso del presente trabajo, su valor promedio y desviación estándar.

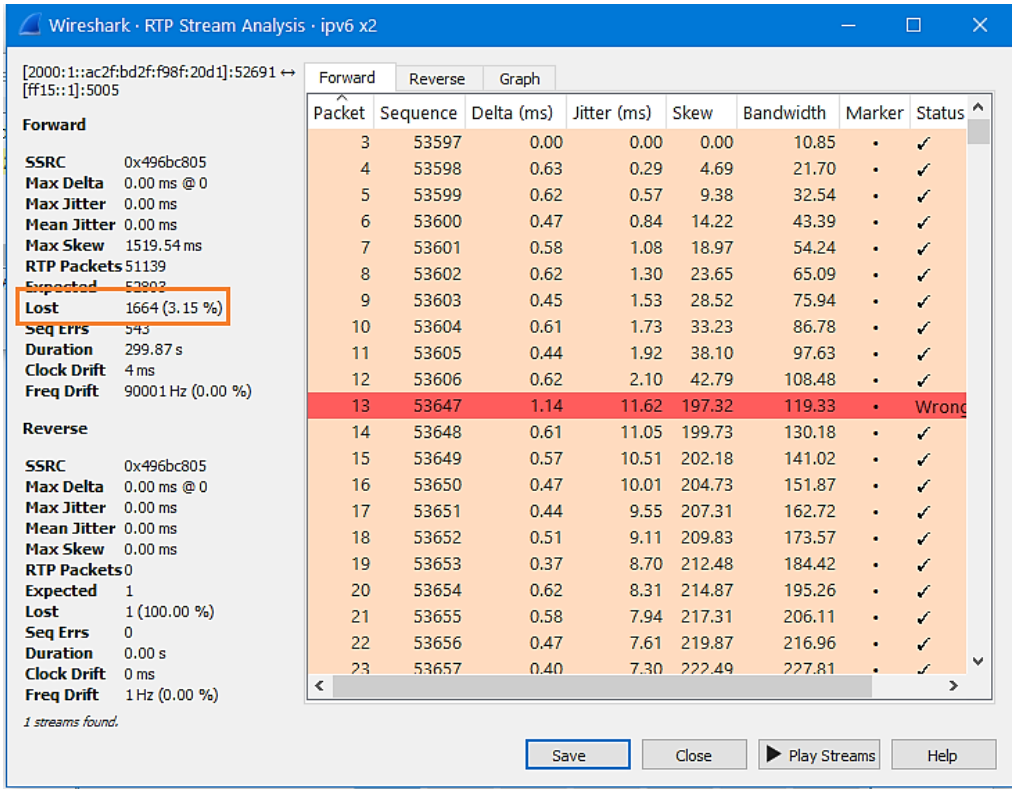


Figura 48. Análisis de flujo RTP detallado con Wireshark

3.3 TOPOLOGÍA DE RED Y ESCENARIOS PROPUESTOS PARA EL ANÁLISIS

3.3.1 TOPOLOGÍA DE RED

Con el propósito de realizar el análisis de rendimiento y comparación de multicast para los protocolos IPv4 e IPv6 se propone una topología de red dual-stack con el objetivo de evaluar a los protocolos en igualdad de condiciones, es decir, sobre la misma topología física y lógica. La topología propuesta es la que se muestra a continuación.

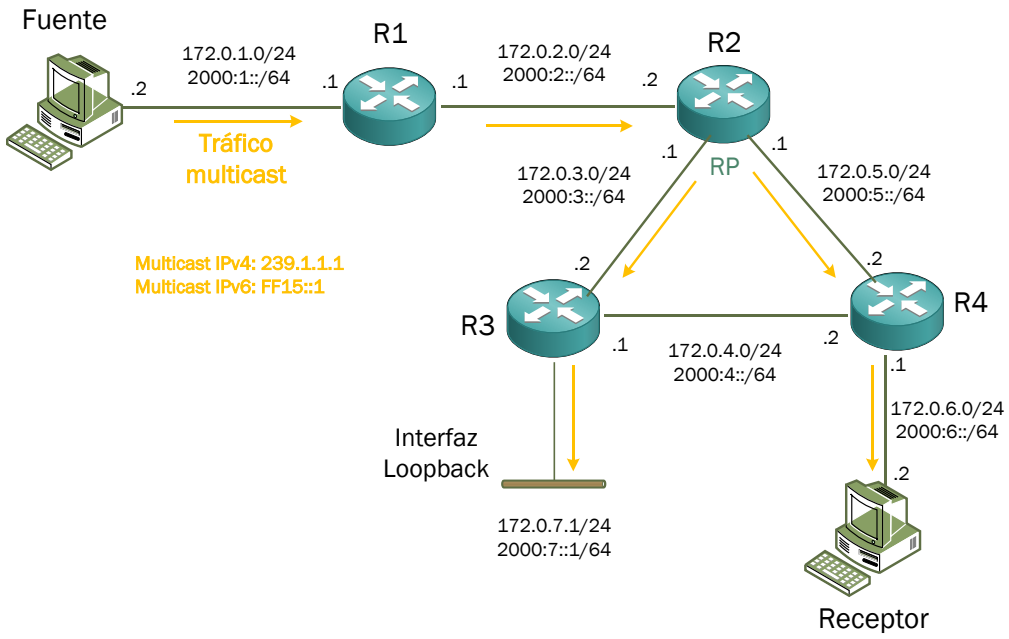


Figura 49. Topología de red utilizada para el análisis

De la topología presentada se realizan las siguientes precisiones.

Routers. - Todos los routers son de marca Cisco cuyos modelos son los siguientes:

- R1 y R4 son de modelo 877-M
- R2 es de modelo 871
- R3 es de modelo 2811

En el Anexo 2 se puede apreciar a los routers utilizados para el análisis.

En lo referente al rendimiento de los routers en su proceso de *switcheo* o procesamiento de datos, Cisco establece para los routers de la plataforma o serie que se utilizan en la presente tesis los siguientes valores máximos de paquetes por segundo y megabits por segundo que pueden procesar:

Tabla 8. Valores máximos de procesamiento de PPS y Mbps de los routers 870 y 2811

Plataforma	Paquetes por segundo (PPS)	Megabits por segundo (Mbps)
870	25.000	12,80
2811	120.000	61,44

Fuente: Cisco Systems. (3 de noviembre de 2009). *Portable Product Sheets – Routing Performance*. Recuperado el 14 de julio de 2016, de http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf

Los valores indicados en la tabla anterior son importantes en el sentido de que el rendimiento en cuanto al throughput estará limitado por los routers de la plataforma

870, en otras palabras, no se podrá exceder los 12,80 Mbps (máximo teórico) en ningún caso o comenzará a existir pérdidas de paquetes.

Enrutamiento. – El enrutamiento unicast tanto para IPv4 como para IPv6 está basado en OSPF. El enrutamiento para multicast IPv4 e IPv6 se basa en PIM-SM siendo R2 el RP para el árbol compartido. En el Anexo 1 se encuentra la configuración de cada uno de los routers.

Interfaz loopback. – Es una interfaz virtual creada en el router R3 y configurada para generar paquetes tanto IGMP como MLD con el propósito de que el router (o la interfaz loopback) forme parte de los grupos de multicast IPv4 e IPv6 para que de esta forma no solamente fluya tráfico hacia el receptor en R4 sino también hacia R3, haciendo de esta manera que R2 efectivamente envíe tráfico multicast sin necesidad de que exista un receptor físico conectado a R3.

Fuente. – La fuente es una PC con Windows 8.1 que genera tráfico multicast IPv4 e IPv6 tanto real a través del reproductor multimedia VLC como simulado a través de Jperf.

Receptor. – Es una PC con Windows 10 en la cual se recibe y analiza el tráfico multicast IPv4 e IPv6 con las herramientas Wireshark y Jperf.

3.3.2 ESCENARIOS PROPUESTOS

El análisis de rendimiento de multicast IPv4 e IPv6 será efectuado con dos tipos de tráfico. Por un lado, se procederá a analizar el rendimiento con tráfico UDP controlado mediante la herramienta Jperf configurada en modo cliente en el nodo

fuente y como servidor en el nodo receptor. Un segundo análisis se llevará acabo inyectando en la red tráfico de video mediante el reproductor de video VLC en el nodo fuente, para receptar y analizar el tráfico en el nodo receptor con la herramienta Wireshark.

A continuación, se realiza la descripción de los escenarios que se pondrán en práctica para la ejecución del análisis del rendimiento propuesto.

3.3.2.1 Análisis con tráfico multicast simulado

En primera instancia, se procederá a determinar el throughput de cada protocolo mediante la generación de tráfico UDP con Jperf. Para lograr este cometido, se utilizará el tamaño máximo de segmento que cada protocolo pueda manejar para luego verificar que no existan pérdidas de paquetes a la máxima velocidad que se pueda alcanzar, de conformidad con el RFC 1242 en el cual se encuentra definido el throughput.

Como segunda prueba, se realizarán mediaciones de pérdidas de paquetes y jitter mediante Jperf en modo servidor. Para esto, con la ayuda de Jperf en modo cliente se enviarán a través de la red paquetes UDP de tamaños incrementales, con el objetivo de verificar la respuesta a tráfico multicast de paquetes de tamaños distintos para los parámetros de evaluación de redes antes mencionados.

Por último, mediante el router R1 se procederá a generar tráfico ICMP de tamaños de paquete incrementales mediante el comando Ping con el objetivo de evaluar el tiempo de respuesta de ida y vuelta RTT (*Round Trip Time*).

Las tres pruebas antes mencionadas serán ejecutas individualmente tanto para IPv4 como para IPv6 y sometidas a comparación.

3.3.2.2 Análisis con tráfico multicast real de video

Como primera prueba, se procederá a enviar a través de la red tráfico multicast de video a través de la herramienta VLC, primero de IPv4 y luego de IPv6 para tomar datos de valores de jitter, pérdida de paquetes y tasa de transferencia de datos de ambos protocolos con la herramienta Wireshark con el objetivo de verificar el comportamiento de los protocolos de manera individual.

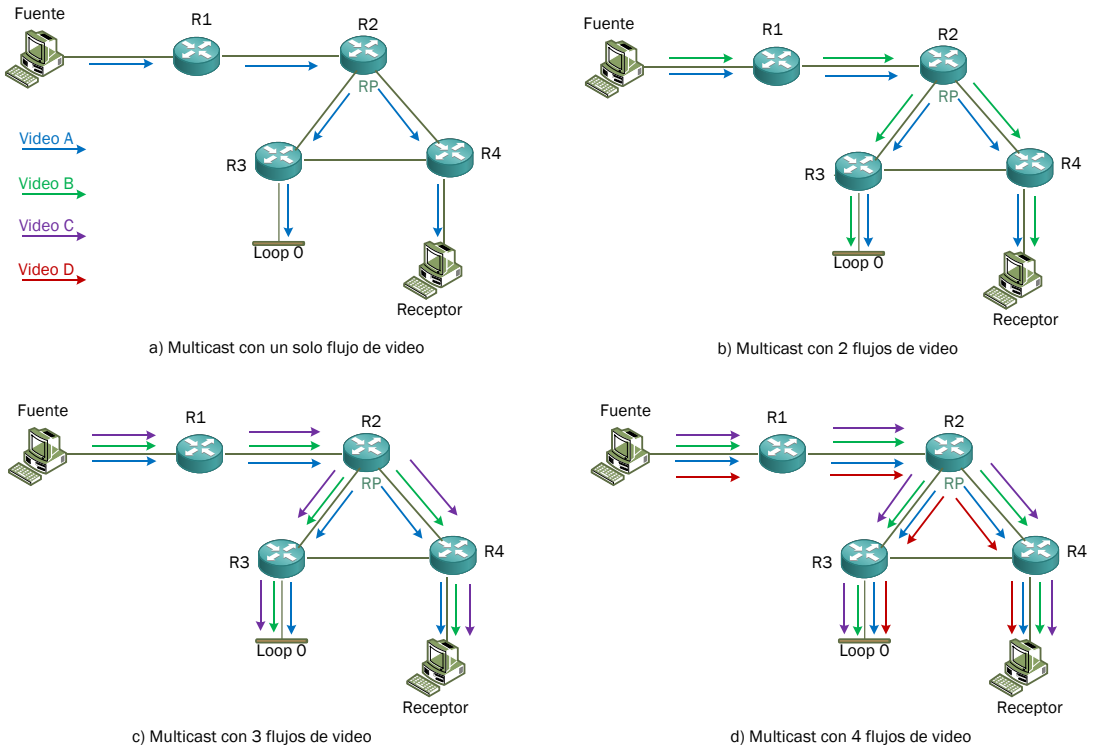
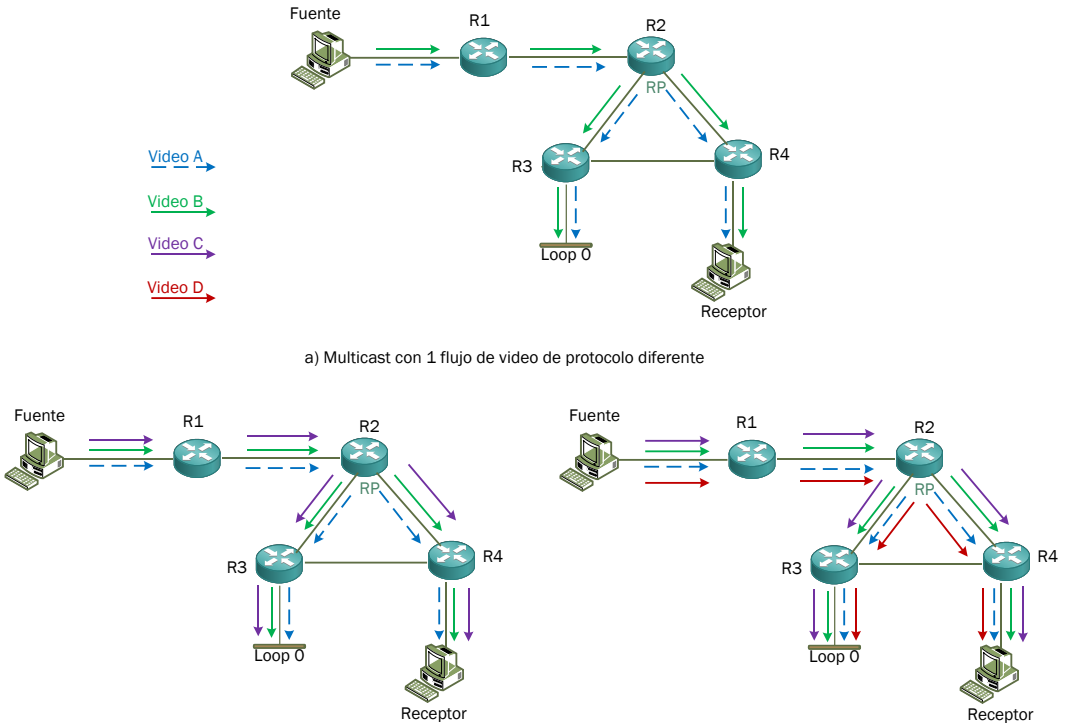


Figura 50. Análisis con diferentes flujos simultáneos de tráfico multicast de video

La siguiente prueba consiste en incrementar paulatinamente flujos de tráfico de video de un mismo tipo de protocolo tanto para IPv4 como para IPv6, es decir, para IPv4 se empezará con 2 flujos de video hasta alcanzar los 4 flujos, e ir tomando valores de jitter, pérdida de paquetes y tasa de transferencia de datos para el video de referencia A, tal como se muestra en la figura 50, con la finalidad de evaluar su comportamiento frente a otras fuentes de video del mismo protocolo de capa 3. Pruebas similares se realizarán con IPv6. Para los análisis de multi tráfico se trabajará con cuatro fuentes de tráfico de video distintas.

Finalmente, se realizarán pruebas y análisis combinando un flujo de video multicast de un protocolo de capa de red con flujos de otro protocolo. Precisando lo señalado, a la transmisión de un flujo de tráfico de video de IPv4 se le añadirá un flujo de video de IPv6 para tomar datos de jitter, pérdida de paquetes y transferencia de datos. Así hasta llegar a 3 flujos de video de IPv6. El análisis anterior también se aplicará para IPv6, adicionando los correspondientes flujos IPv4 uno a uno hasta completar los 3 de igual manera. Estos análisis tienen la finalidad de evaluar el rendimiento de cada protocolo frente a múltiples flujos del otro protocolo.



a) Multicast con 1 flujo de video de protocolo diferente

b) Multicast con 2 flujos de video de protocolo video diferente

c) Multicast con 3 flujos de video video de protocolo diferente

Figura 51. Análisis con tráfico simultáneo de video multicast de protocolos combinados

En la figura 51, la línea azul punteada representa el tráfico de video de referencia A que puede ser, según las pruebas, video IPv4 o IPv6. Sobre éste se tomarán los datos de jitter, pérdida de paquetes y tasa de transferencia de datos. Cuando en el análisis, el tráfico de video de referencia A sea IPv4, los otros flujos B, C y D serán IPv6; por consiguiente, cuando en las pruebas A sea IPv6, los flujos restantes serán IPv4.

CAPÍTULO IV. RESULTADOS EXPERIMENTALES DEL ANÁLISIS DE TRÁFICO MULTICAST IPv4 E IPv6

4.1 RESULTADOS EXPERIMENTALES DEL ANÁLISIS CON TRÁFICO MULTICAST SIMULADO

4.1.1 ANÁLISIS DE THROUGHPUT

4.1.1.1 Tamaño de paquetes UDP

Para el análisis de throughput se consideró ajustar el tamaño de los paquetes UDP al tamaño máximo de Bytes de segmento que ambos protocolos pueden manejar. Teniendo en cuenta que la cabecera de IPv4 posee 20 Bytes[4], la de IPv6 40 Bytes y la de UDP 8 Bytes;

Entonces se tiene que

$$UDP = MTU - Cabecera\ IP - Cabecera\ UDP$$

$$UDP_{IPv4} = 1500\ Bytes - 20\ Bytes - 8\ Bytes = 1472\ Bytes$$

$$UDP_{IPv6} = 1500\ Bytes - 40\ Bytes - 8\ Bytes = 1452\ Bytes$$

La razón de manejar el máximo tamaño de segmento radica en que de esta manera los routers procesarán el mínimo número de segmentos posibles por lo que

[4] La cabecera IPv4 tiene un tamaño variable de entre 20 y 24 bytes. Está variación la da el campo de Opciones, el cual puede o no existir. Para las pruebas ejecutas no se utilizó ninguna opción del campo mencionado.

sus procesadores e interfaces no estarán sobrecargados permitiendo así obtener su máximo rendimiento.

4.1.1.2 Procedimiento

Para efectuar este análisis, se procedió con el envío de tráfico desde el nodo fuente con Jperf en modo cliente iniciando con la velocidad máxima de procesamiento de los routers de la plataforma 870, es decir, desde 12,8 Mbps para luego ir disminuyendo hasta verificar que en el nodo receptor no existan pérdidas de paquetes. Puesto que Jperf permite pasos de 1 Mbps, la prueba se inició en 13 Mbps.

El tiempo para el envío de tráfico que fue utilizado para esta prueba fue de 3 minutos por cada valor de velocidad en Mbps que se iba seleccionando. Esto debido a que es un ambiente controlado, con tráfico predecible y libre de perturbaciones.

4.1.1.3 Resultados

A continuación, se presentan los resultados obtenidos en las pruebas realizadas con la herramienta Jperf.

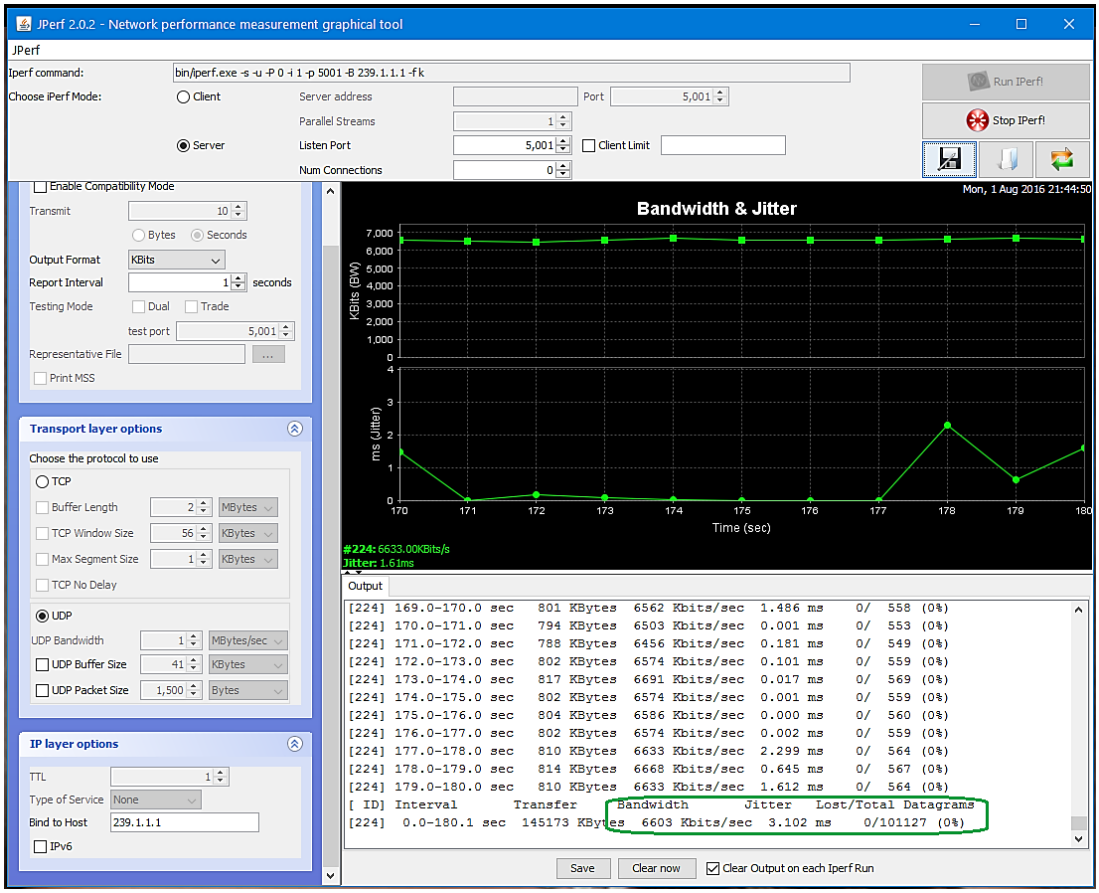


Figura 52. Captura de tráfico multicast de IPv4 sin pérdida de paquetes

De acuerdo a los datos obtenidos en las pruebas efectuadas, el throughput para el tráfico multicast IPv4 hacia la IP 239.1.1.1 es de 6,60 Mbps, conforme lo mostrado en la figura 52. En la figura 53 se muestra que para un valor ligeramente mayor de velocidad comienza a existir pérdidas de paquetes, en este caso, para un valor de 7,52 Mbps ya existe 0,13% de pérdida.

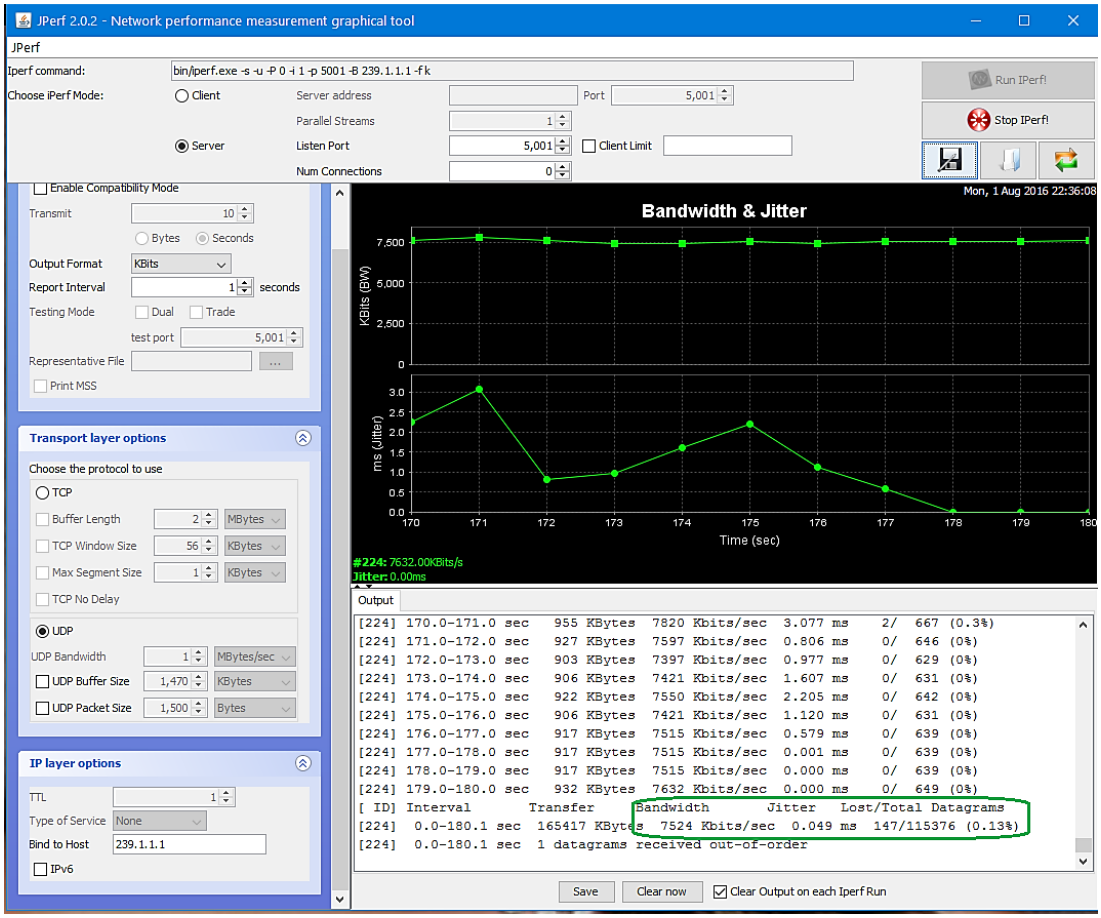


Figura 53. Captura de tráfico multicast de IPv4 con pérdida de paquetes

Para la obtención del valor de throughput de IPv6 se procedió de manera similar a lo efectuado en IPv4, esto es, enviando tráfico de manera descendente hacia la dirección IPv6 multicast de prueba FF15::1 partiendo desde la máxima velocidad teórica para los routers de la plataforma 870; siendo los resultados los que se presentan en las figuras descritas a continuación.

En la figura 54 se observa que para un valor de velocidad de 8,46 Mbps no existen pérdidas de paquetes; sin embargo, en la figura 55 se evidencia que si el ancho de banda llega a ser 9,38 Mbps comienzan a presentarse pérdidas del orden de 0,0021%.

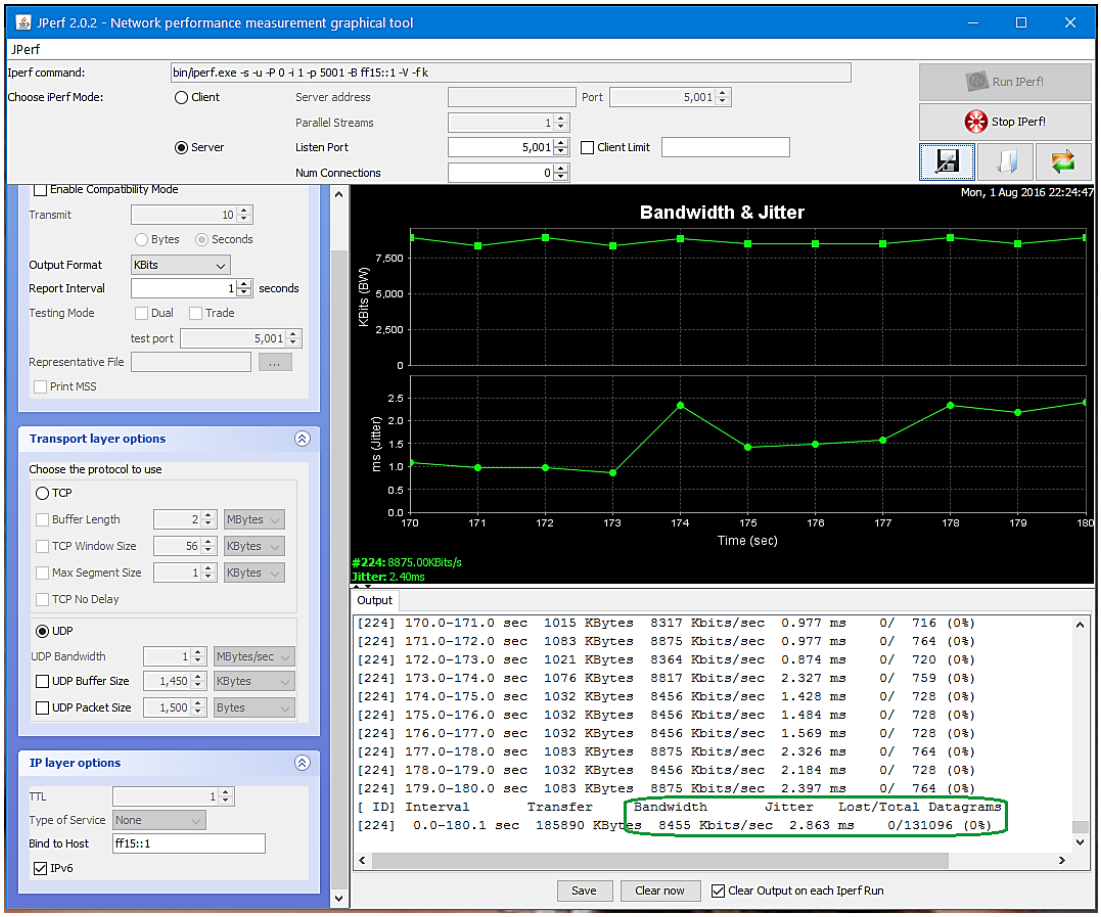


Figura 54. Captura de tráfico multicast de IPv6 sin pérdida de paquetes

En la siguiente tabla se muestran los valores de throughput obtenidos en las pruebas para los flujos de tráfico multicast IPv4 e IPv6. Como se puede observar, IPv6 posee un valor de throughput mayor.

Tabla 9. Comparativa de throughput multicast IPv4 e IPv6

Protocolo	Throughput (Mbps)
IPv4	6,60
IPv6	8,46

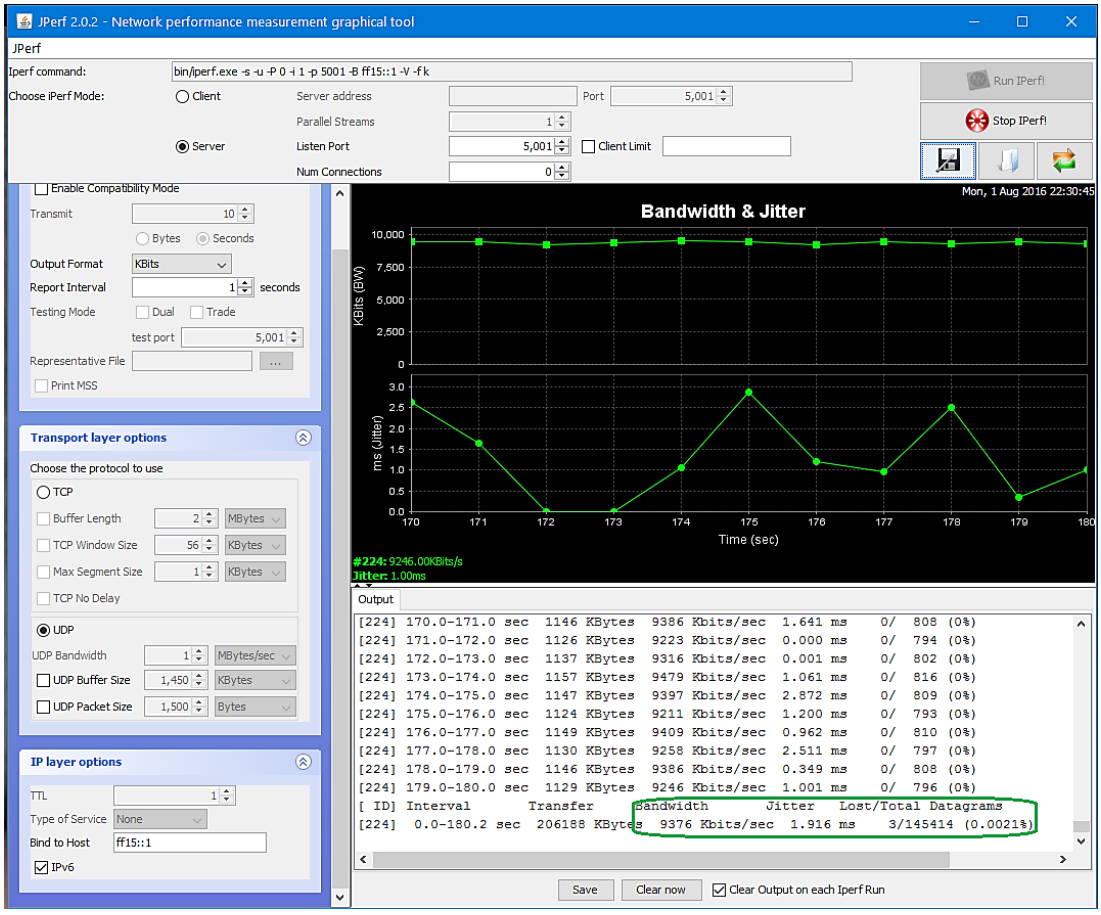


Figura 55. Captura de tráfico multicast de IPv6 con pérdida de paquetes

4.1.1.4 Análisis de los resultados

De los resultados obtenidos en las pruebas ejecutadas se tiene que con respecto de IPv4, IPv6 tiene mayor throughput en un 28,18%.

4.1.2 ANÁLISIS DE JITTER Y PÉRDIDA DE PAQUETES

4.1.2.1 Procedimiento

Con el objetivo de realizar las pruebas y mediciones de jitter y pérdida de paquetes, con la ayuda de Jperf, se procedió a enviar paquetes UDP de tamaños

incrementales, empezando por 64 Bytes hasta 1470 Bytes, valor máximo que permite configurar la herramienta de prueba.

La tasa de transferencia de datos utilizada para estas pruebas fue del 70% del valor del throughput obtenido anteriormente para ambos protocolos. Este porcentaje de ocupación de canal es el recomendado por Cisco para que no existan problemas de saturación ni pérdida de paquetes. Por lo mencionado anteriormente, el ancho de banda para IPv4 debería ser 4,6 Mbps y para IPv6 5,9 Mbps, sin embargo, dadas las limitaciones de la herramienta para ajustar la velocidad, estos valores fueron aproximados a 5 y 6 Mbps respectivamente.

En lo que respecta al tiempo de cada prueba, para cada tamaño de paquete se configuró un intervalo de tiempo de 3 minutos, tiempo adecuado ya que es un ambiente controlado.

4.1.2.2 Resultados

En las figuras presentadas a continuación, se muestran valores de jitter y pérdida de paquetes tomados con la herramienta Jperf en el nodo receptor para tráfico multicast IPv4 e IPv6 con paquetes UDP de tamaño de 512 bytes.

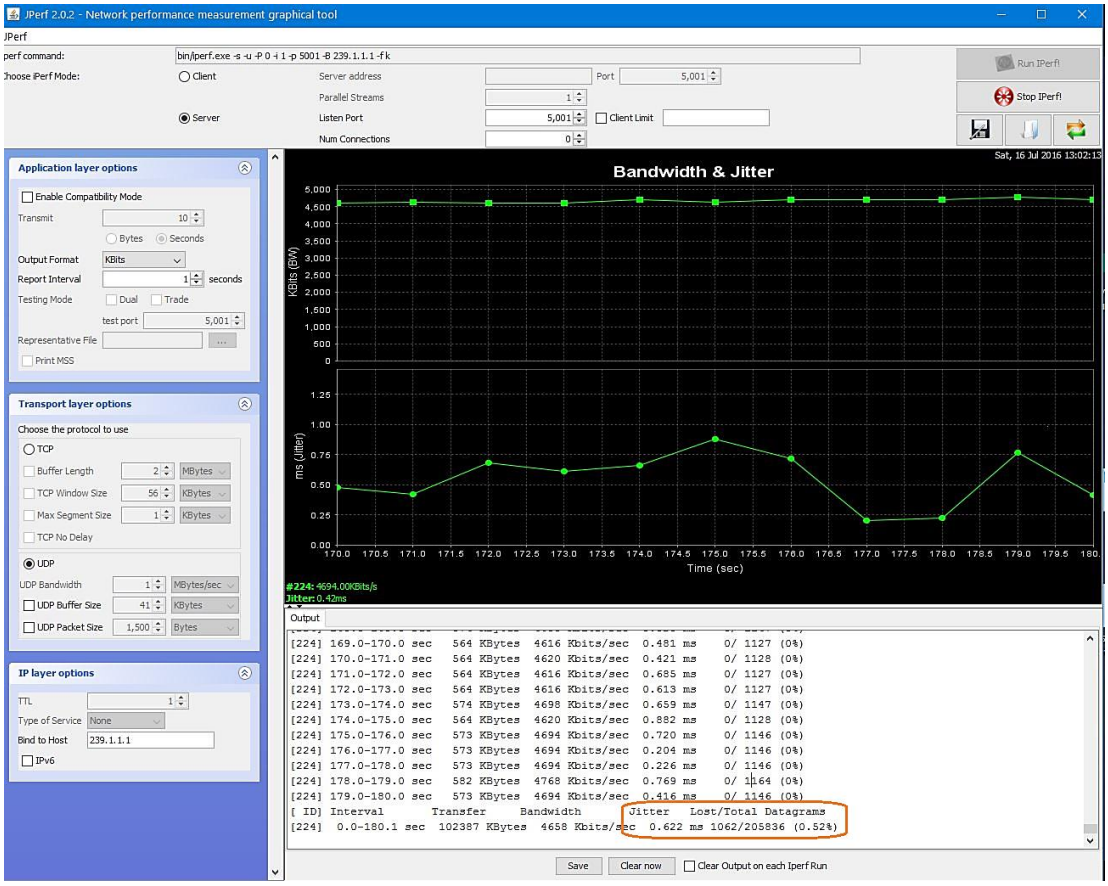


Figura 56. Captura de jitter y pérdida de paquetes de multicast IPv4 con paquetes UDP de 512 Bytes

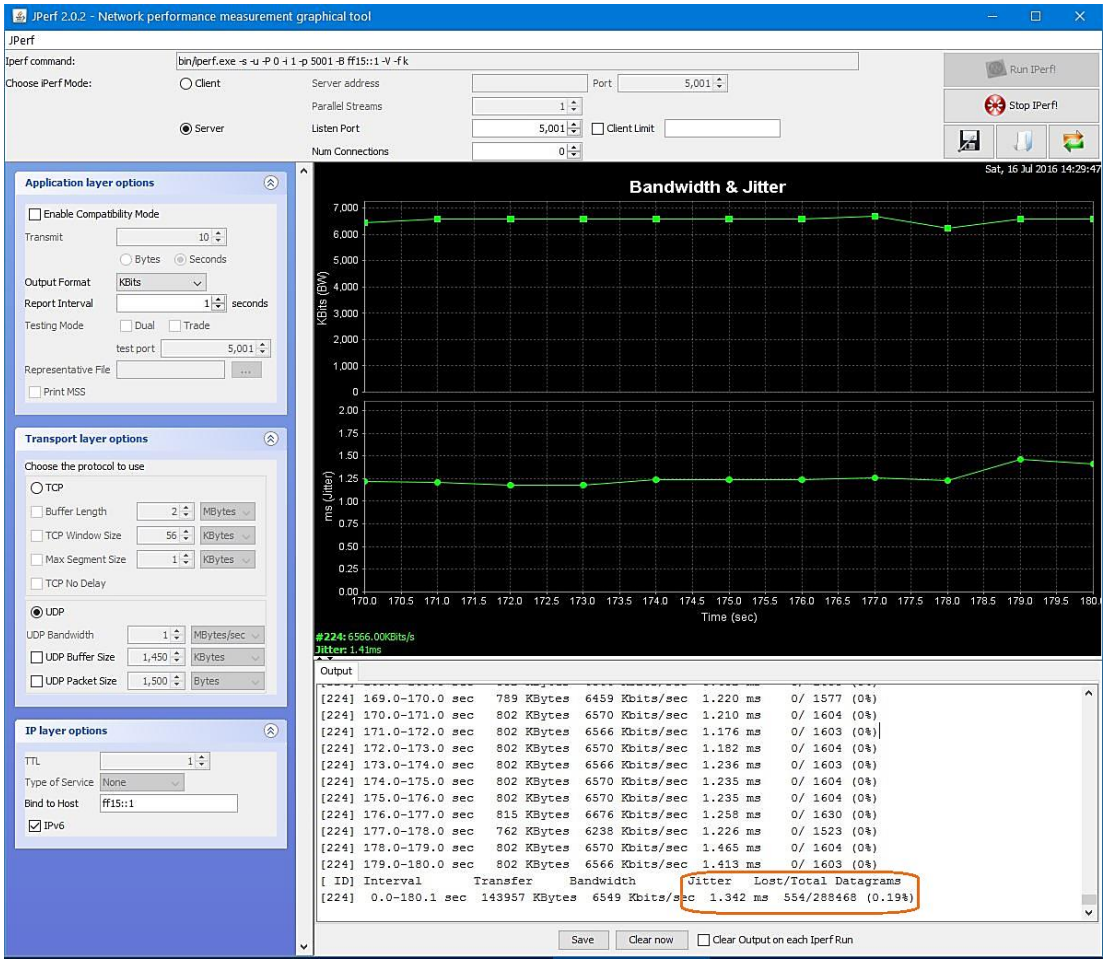


Figura 57. Captura de jitter y pérdida de paquetes de multicast IPv6 con paquetes UDP de 512 Bytes

En las tablas 10 y 11 se muestran los valores de jitter y pérdida de paquetes respectivamente, obtenidos en las pruebas correspondientes para los protocolos IPv4 e IPv6 para cada tamaño de paquete UDP. En la figura 58 se observa gráficamente los datos obtenidos de jitter de la tabla 10, en tanto que en la figura 59 se encuentran representados gráficamente los valores de la tabla 11 referente a la pérdida de paquetes. En la figura 60 se puede observar los datos de pérdida de paquetes, pero iniciando desde 384 bytes debido a que a partir de este tamaño de

paquete, las pérdidas de pequeño valor son comparables entre ambos protocolos y se las puede examinar más de cerca para observar su comportamiento.

Tabla 10. Valores de jitter para tráfico multicast IPv4 e IPv6

Tamaño de paquete (Bytes)	Jitter IPv4 (ms)	Jitter IPv6 (ms)
64	2,99	3,08
128	3,24	2,59
256	1,27	2,95
384	1,1	1,78
512	0,62	1,34
640	1,18	1,39
768	0,73	2,21
896	1,69	1,53
1024	1,8	1,88
1152	0,95	0,78
1280	1,87	2,46
1408	0,52	1,1
1470	1,97	1,11

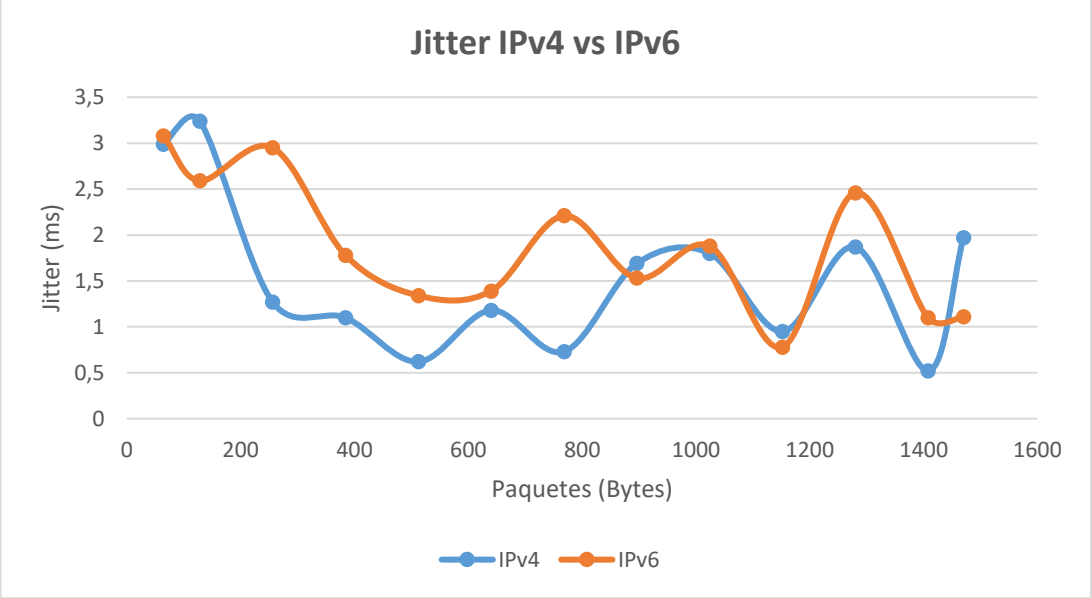


Figura 58. Jitter multicast IPv4 vs IPv6

Tabla 11. Valores de pérdida de paquetes para tráfico multicast IPv4 e IPv6

Tamaño de paquetes (Bytes)	Pérdida de paquetes IPv4 (%)	Pérdida de paquetes IPv6 (%)
64	92	83
128	80	67
256	5,9	30
384	0,42	1,1
512	0,52	0,19
640	0,21	0,04
768	0,4	0,01
896	0,13	0
1024	0,05	0,06
1152	0,003	0
1280	0,005	0
1408	0	0,005
1470	0,007	0,03

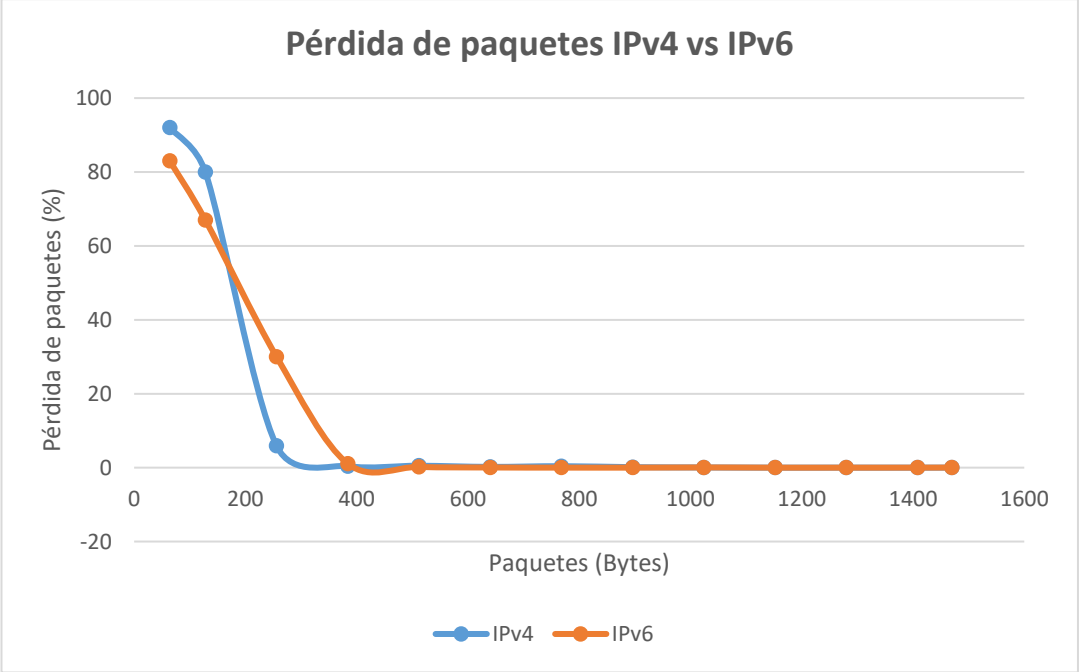


Figura 59. Pérdida de paquetes multicast IPv4 vs IPv6

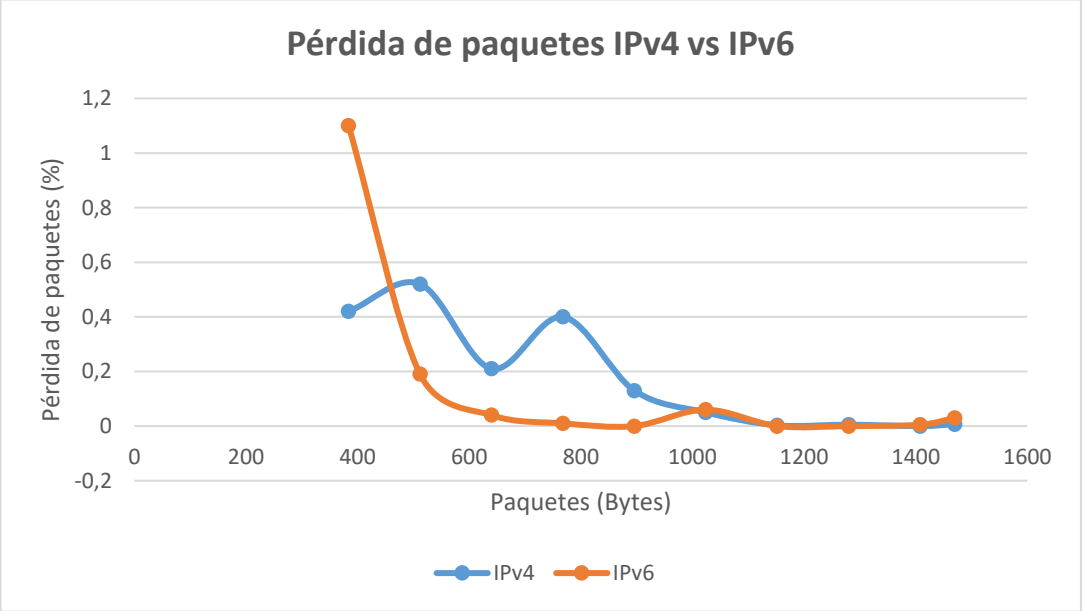


Figura 60. Pérdida de paquetes multicast IPv4 vs IPv6 desde 384 Bytes

4.1.2.3 Análisis de los resultados

Jitter. – Se observa que, para casi todos los tamaños de paquetes enviados en la transmisión multicast, el jitter de IPv4 presenta valores menores comparados con los de IPv6 y adicionalmente, se distingue que ambas curvas poseen similar tendencia.

Pérdida de paquetes. - De los datos obtenidos se nota que, para paquetes de pequeño tamaño, ambos protocolos presentan grandes pérdidas de paquetes que si bien IPv4 parece mejorar más rápido mientras los paquetes aumentan de tamaño, en la gráfica ampliada se puede apreciar que IPv6 responde de mejor manera ya que a partir de 700 bytes aproximadamente las pérdidas tienden a cero, mientras que para IPv4 esta tendencia la alcanza a partir de los 1100 bytes aproximadamente.

4.1.3 ANÁLISIS DE TIEMPO DE IDA Y VUELTA (*RTT - ROUND TRIP TIME*)

4.1.3.1 Procedimiento

Con el objetivo de evaluar el tiempo de ida y vuelta de multicast IPv4 e IPv6, mediante R1 se procedió a enviar paquetes ICMP de tamaños incrementales, empezando por 64 Bytes hasta finalizar con 18024 Bytes, tamaño máximo que permite el IOS del router mediante el comando ping. Los paquetes fueron enviados hacia las direcciones multicast de prueba 239.1.1.1 y FF15::1. Las peticiones ICMP fueron respondidas por los routers R3 y R4 ya que éstos se encuentran configurados para recibir y procesar tráfico multicast tanto IPv4 como IPv6.

El número de paquetes enviados para cada prueba fue de 10; esto debido a que por ser un entorno controlado y siendo éste el único tráfico significativo, los tiempos de respuesta para cada paquete tienden a ser iguales en casi todos los casos y similares en los restantes. Para la obtención del valor que representa al de RTT para cada prueba, se promedia los valores de las 10 muestras.

4.1.3.2 Resultados

En la figura presentada a continuación se muestran los ensayos realizados hacia las direcciones IPv4 e IPv6 multicast de prueba. Se observa como en ambos casos responden a las peticiones de echo ICMP los routers R4 y R5, y adicionalmente se puede apreciar como para paquetes de 2048 Bytes los tiempos de respuesta no varían en el tiempo; siendo esto válido para ambos protocolos.

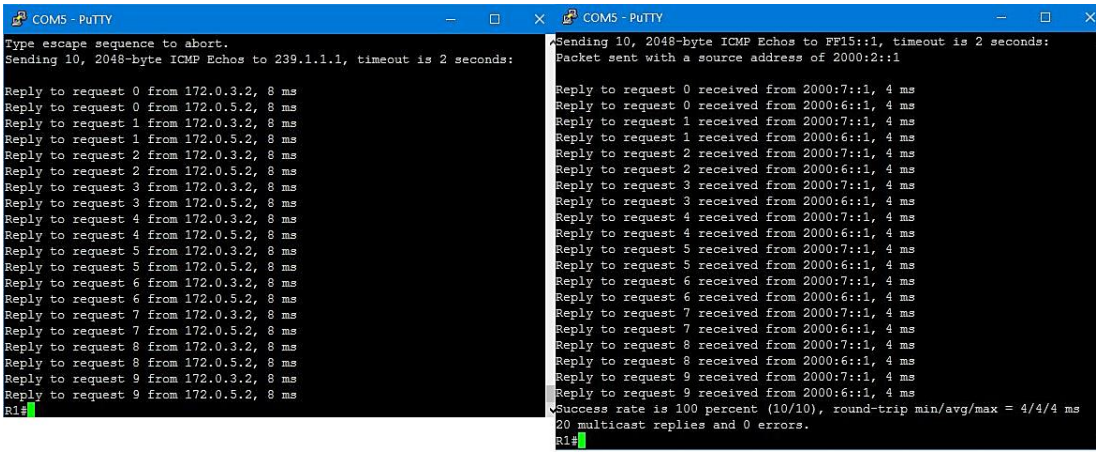


Figura 61. Tiempo de respuesta de ida y vuelta multicast IPv4 e IPv6 para paquetes de 2048 Bytes

Para paquetes de mayor tamaño, los tiempos de respuesta varían dependiendo del destino, pero de manera similar al caso anterior, poseen un valor casi invariable dependiendo del router que responde a las peticiones de echo ICMP, tal como se muestra en las figuras siguientes.

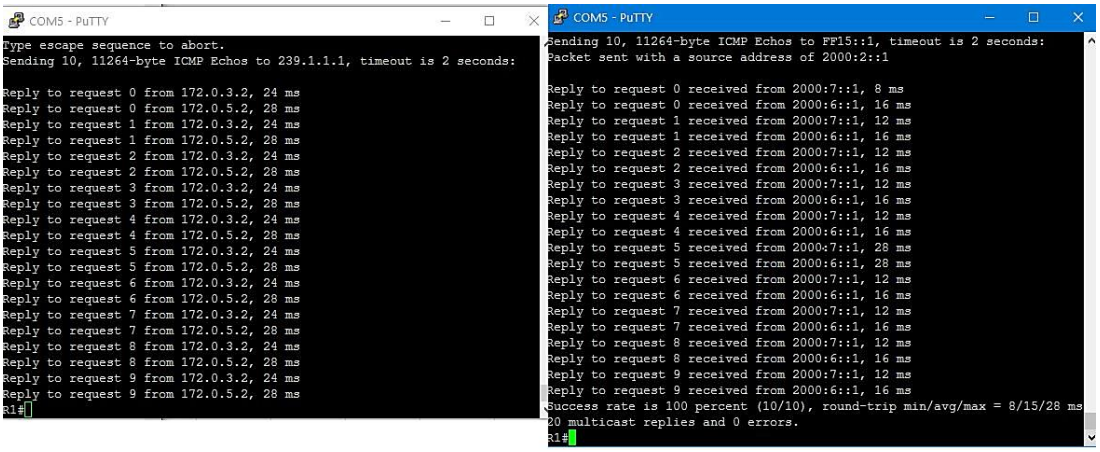


Figura 62. Tiempo de respuesta de ida y vuelta multicast IPv4 e IPv6 para paquetes de 11264 Bytes

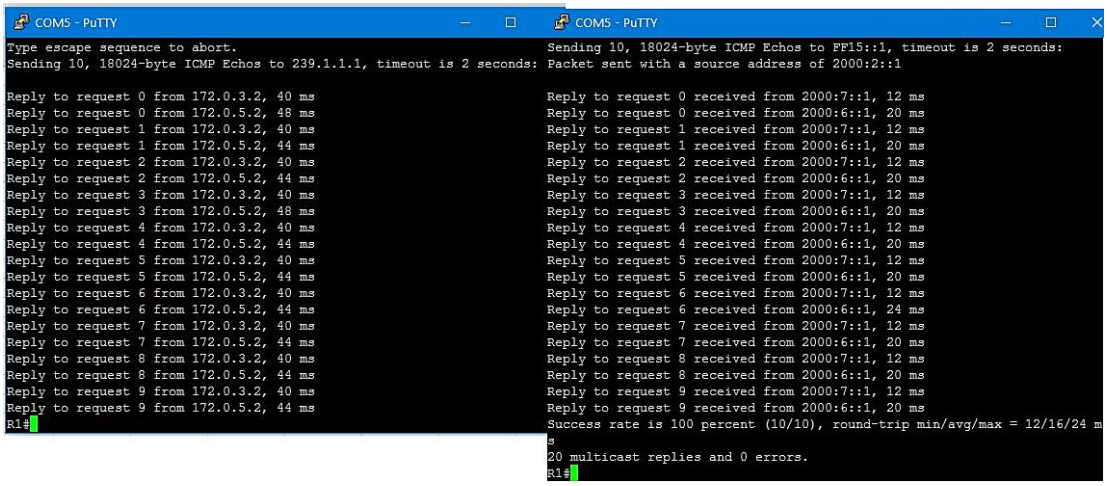


Figura 63. Tiempo de respuesta de ida y vuelta multicast IPv4 e IPv6 para paquetes de 18024 Bytes

En la tabla mostrada a continuación se presentan los valores de tiempo de ida y vuelta obtenidos en las pruebas realizadas.

Tabla 12. Valores de tiempo de ida y vuelta para tráfico multicast IPv4 e IPv6

Tamaño de paquete (Bytes)	Tiempo de ida y vuelta IPv4 (ms)	Tiempo de ida y vuelta IPv6 (ms)
64	1,3	0,4
128	1,15	1
256	1	0,8
512	1,7	0,4
1024	4	0,4
2048	8	4
3072	8,4	5,8
4096	8,2	6
5120	16	6
7168	24,8	10
9216	24	11,8
11264	26	15,2
13312	31,2	16,2
15360	37,8	17,33
18024	42,4	16,2

La figura siguiente es la representación gráfica de la tabla anterior, en la cual se muestra la respuesta de tiempo de ida y vuelta que ambos protocolos presentan respecto de la variación del tamaño de paquetes de petición de echo ICMP.

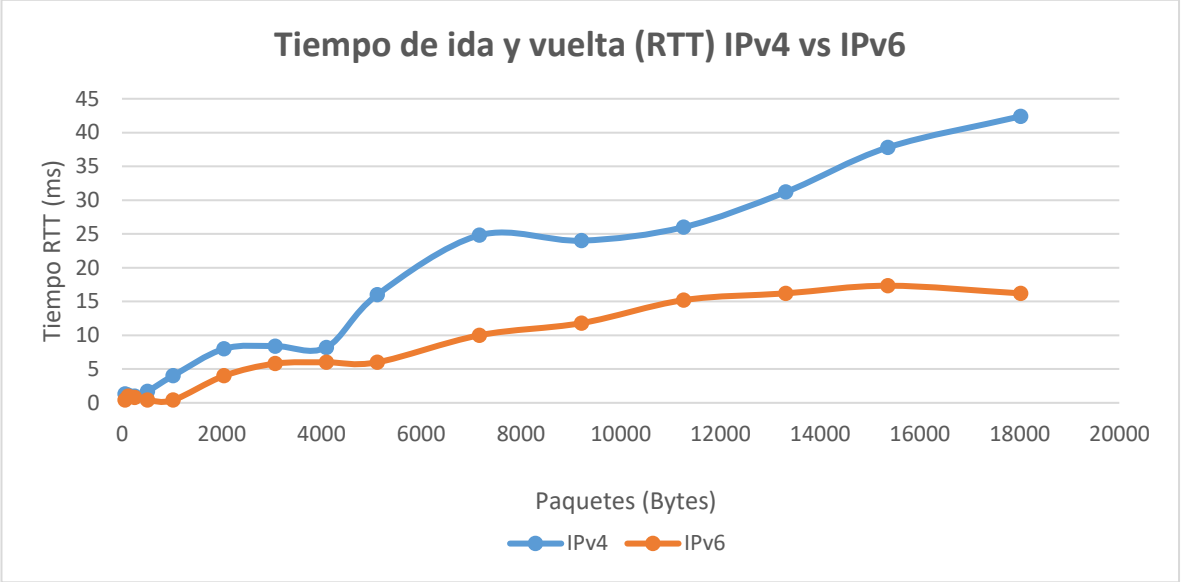


Figura 64. Tiempo de ida y vuelta multicast IPv4 e IPv6

4.1.3.3 Análisis de los resultados

De los resultados se observa que para todo tamaño de paquete ICMP utilizado para las pruebas, IPv6 presenta un mejor tiempo de respuesta de ida y vuelta, es decir, tiempos menores que IPv4, y adicionalmente se tiene que mientras los paquetes aumentan de tamaño, la tendencia a crecer en tiempo de respuesta de IPv6 se hace mínima, mientras que para IPv4 la tendencia de crecimiento de tiempo de respuesta aumenta.

4.2 RESULTADOS EXPERIMENTALES DEL ANÁLISIS CON TRÁFICO MULTICAST REAL DE VIDEO

4.2.1 CARACTERÍSTICAS DE LOS VIDEOS UTILIZADOS PARA EL ANÁLISIS

Con la finalidad de realizar el análisis de tráfico multicast con tráfico real, se utilizaron 4 archivos de video diferentes, cuyas características son descritas en la tabla 13.

Tabla 13. Características de los archivos de video utilizados para las pruebas de multicast

Nombre	Formato	Tamaño de payload UDP (Bytes)	Velocidad de transmisión (Mbps)
Video A	AVI	1328	2,34
Video B	AVI	1328	2,34
Video C	AVI	1328	2,34
Video D	AVI	1328	1,86

Sobre el tamaño de *payload* UDP es necesario precisar que esta información hace referencia al *payload* o carga útil del datagrama UDP; en otras palabras, es el tamaño de la porción del datagrama que transporta los datos propiamente de video (y audio).

Para ejecutar tanto el análisis de protocolo único como el de protocolos combinados se utilizó el video A como referencia, es decir, sobre éste se obtuvieron los datos de jitter, pérdida de paquetes y tasa de transferencia de datos al efectuarse todas las pruebas concernientes a ambos estudios.

4.2.2 ANÁLISIS DE JITTER, PÉRDIDA DE PAQUETES Y TASA DE TRANSFERENCIA DE DATOS CON FLUJOS DE VIDEO DE PROTOCOLO ÚNICO

4.2.2.1 Procedimiento

Mediante el reproductor de video VLC se transmitieron los flujos de video hacia las direcciones de prueba IPv4 e IPv6, abriendo una sesión de VLC por cada archivo de video. En el receptor mediante la herramienta Wireshark se realizó la captura del trafico multicast para su posterior análisis.

En primera instancia las pruebas fueron elaboradas con IPv4 en donde, en primer lugar, se transmitió solamente el video A por 5 minutos para la toma de resultados de los parámetros de análisis. En segundo lugar, se transmitió el video A y el video B. Como tercera prueba a los videos anteriores se agregó el video C y finalmente, para el cuarto ensayo se agregó a los videos A,B y C el video D. Para el análisis con IPv6 se procedió de la misma manera.

Para todos los experimentos, en cuanto al tiempo de duración de los mismos, éstos se efectuaron en un intervalo de transmisión de video de 5 minutos.

Debido a que se realizaron pruebas con múltiples flujos de tráfico simultáneo con el mismo protocolo; para diferenciarlos fue necesario utilizar diferentes puertos UDP de destino para cada flujo de video. El puerto UDP 5004 fue utilizado siempre para el video de referencia A, el puerto 5005 para el video B y así sucesivamente.

4.2.2.2 Resultados

En las figuras que se presentan a continuación se muestran las capturas realizadas con la herramienta Wireshark para los flujos multicast IPv4 e IPv6 para el video de referencia.

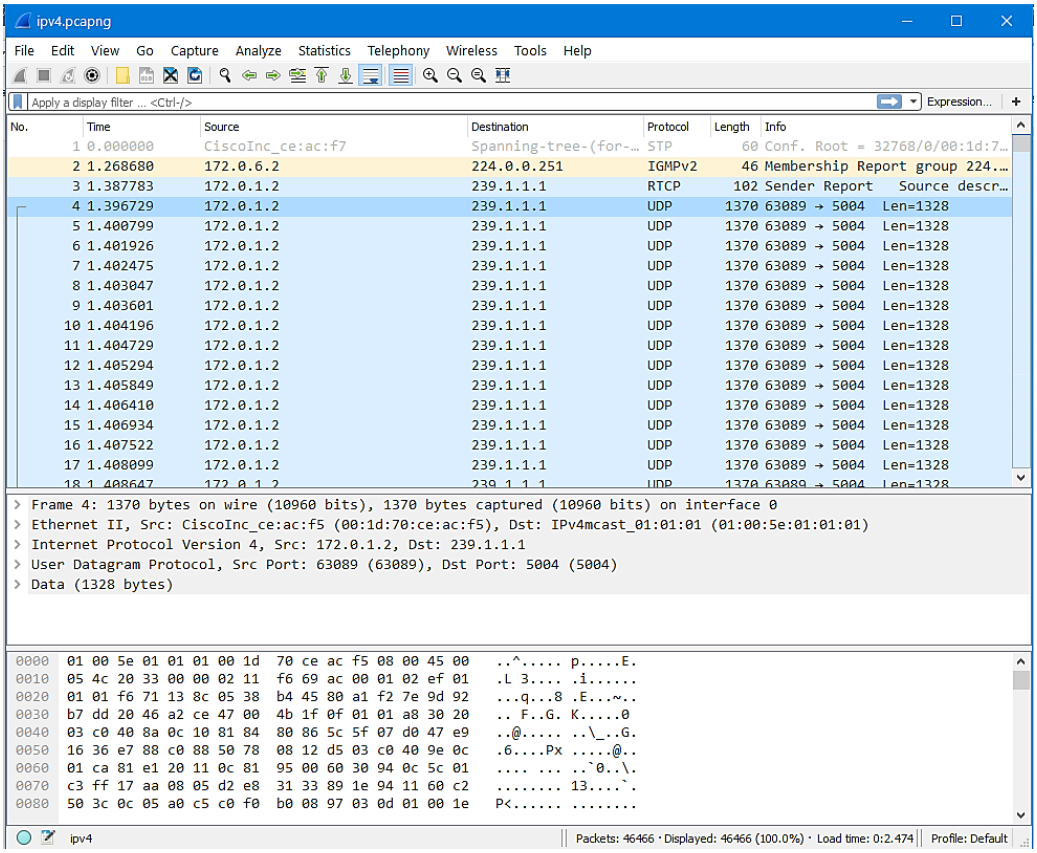


Figura 65. Captura de tráfico multicast IPv4 de un solo flujo de video

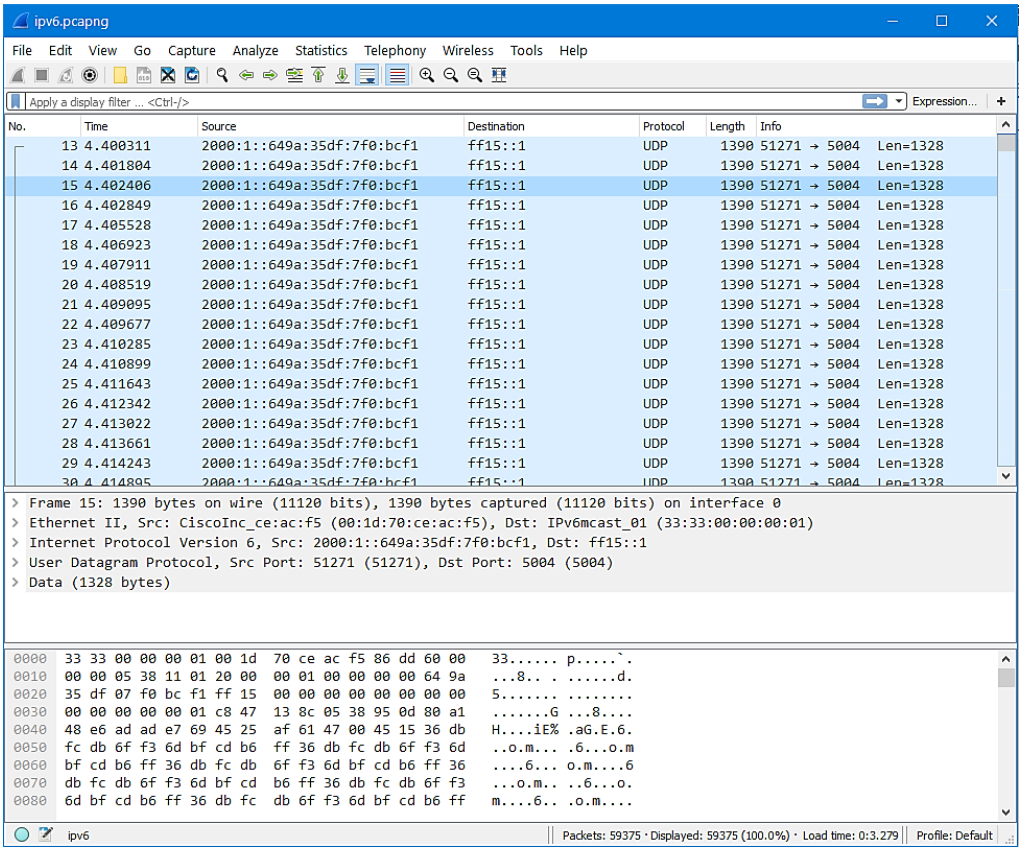


Figura 66. Captura de tráfico multicast IPv6 de un solo flujo de video

En las gráficas 67 y 68 que se muestran a continuación, se puede apreciar como para el mismo flujo de video A, el tráfico multicast IPv6 presenta una mayor tasa de transferencia de datos que el tráfico de IPv4.

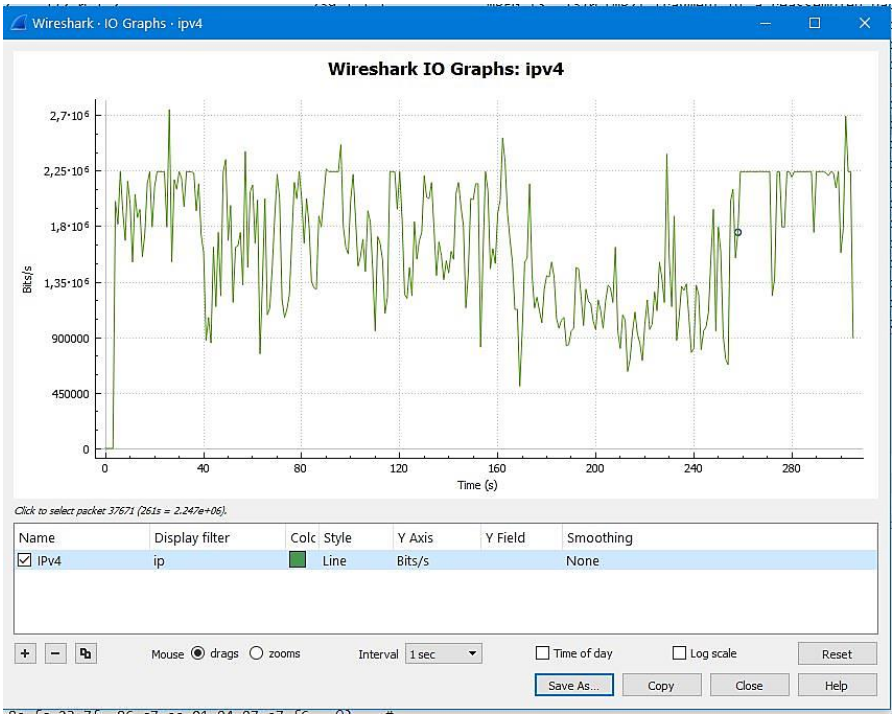


Figura 67. Tasa de transferencia de datos de tráfico multicast IPv4 de un solo flujo de video

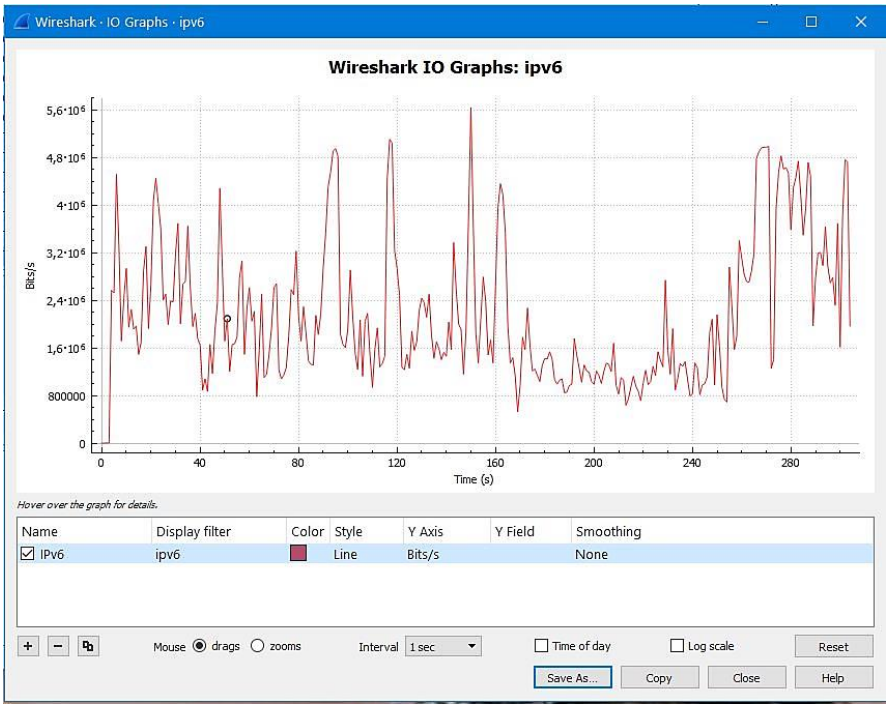


Figura 68. Tasa de transferencia de datos de tráfico multicast IPv6 de un solo flujo de video

Adicionalmente, en las figuras 69 y 70 se observa como para un mismo fotograma, IPv6 presenta mayor calidad que IPv4 puesto que la primera imagen aparece un tanto borrosa y *pixeleada* mientras que para la segunda, la imagen resulta ser clara.

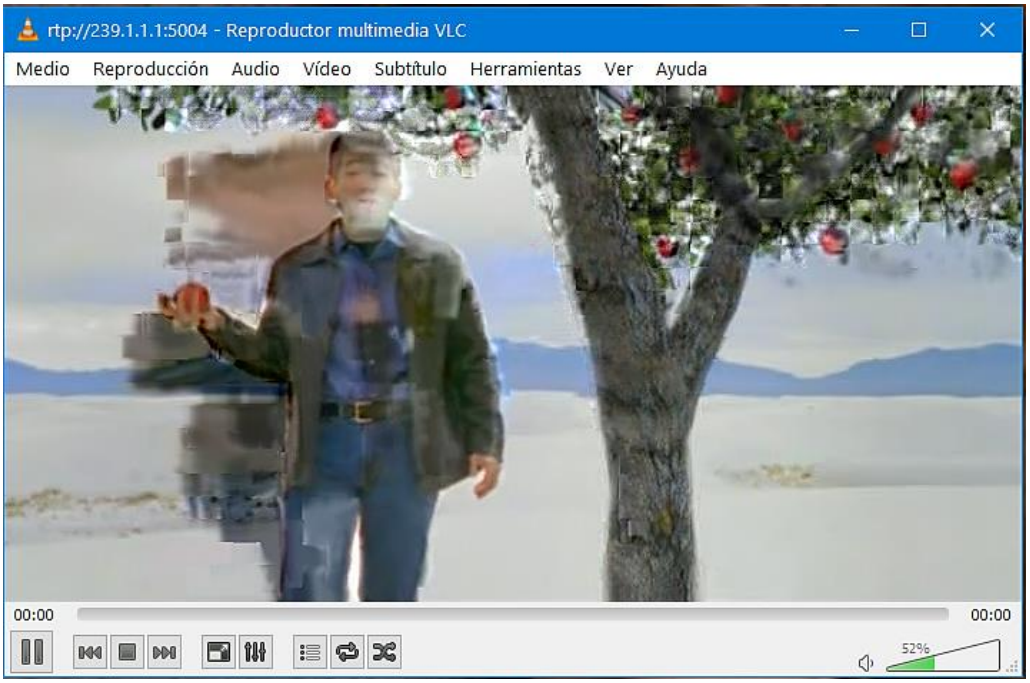


Figura 69.Fotograma de video multicast IPv4 pixelada

Figura 70. Fotograma de video multicast IPv6 clara

Para obtener la tasa de transferencia de datos promedio de los flujos de tráfico de video se utilizó el análisis de flujos de multicast UDP de Wireshark ubicado en el menú de Estadísticas, como se muestra en las figuras 71 y 72.

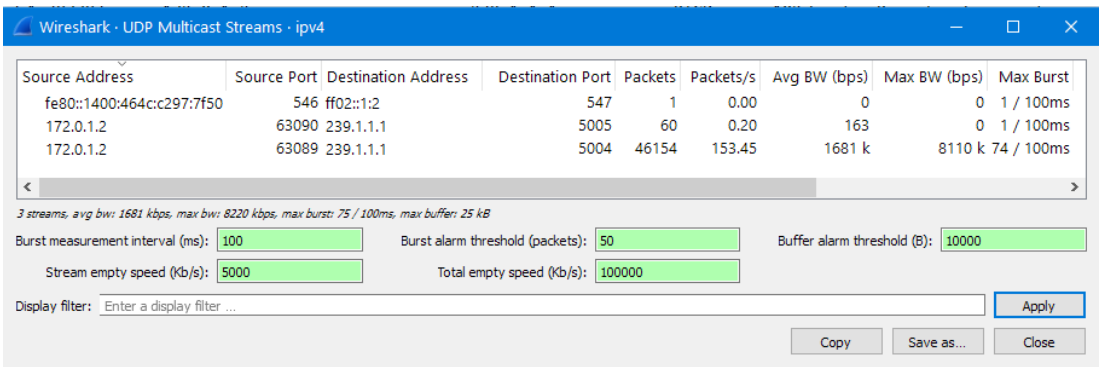


Figura 71. Análisis de flujos multicast UDP para IPv4

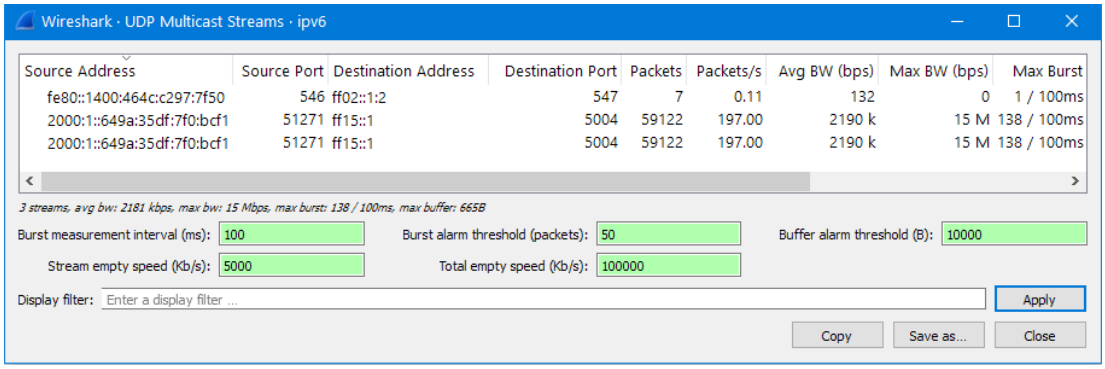


Figura 72. Análisis de flujos multicast UDP para IPv6

Posterior a la obtención de la tasa de transferencia de datos de los flujos de tráfico multicast IPv4 e IPv6, se procedió a adquirir los valores de la medición de pérdida de paquetes y jitter valiéndonos del análisis de flujos RTP en el menú de Telefonía, tal como fue explicado en la sección de Wireshark en el capítulo anterior.

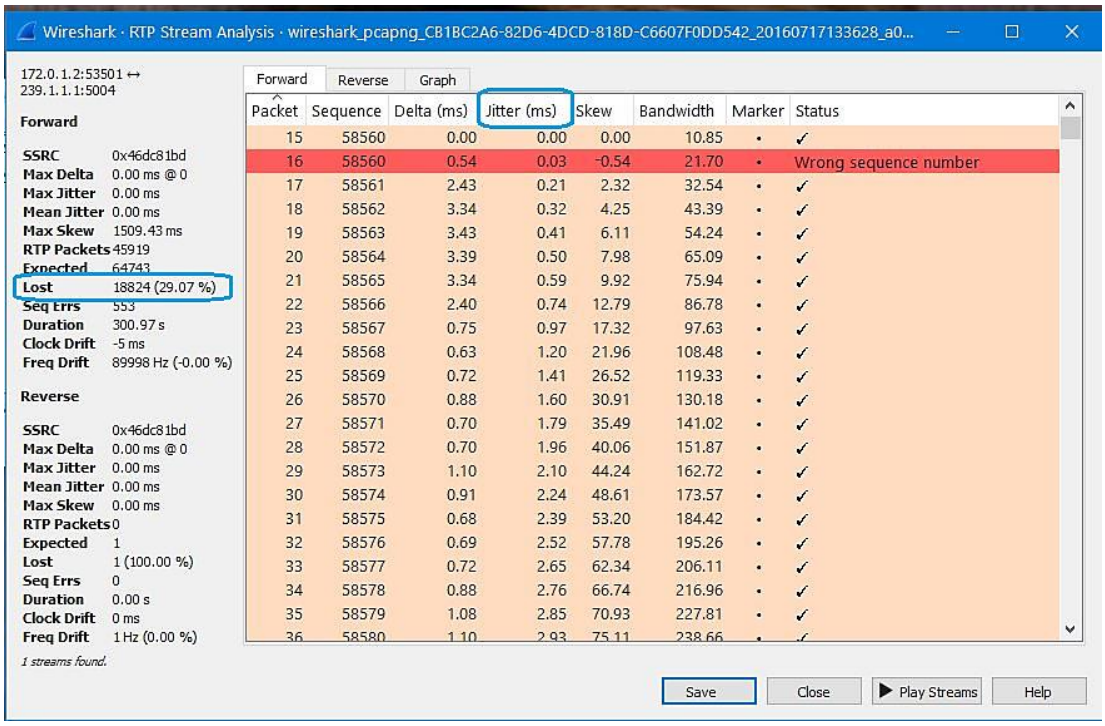


Figura 73. Datos obtenidos de jitter y pérdidas de paquetes para video multicast IPv4

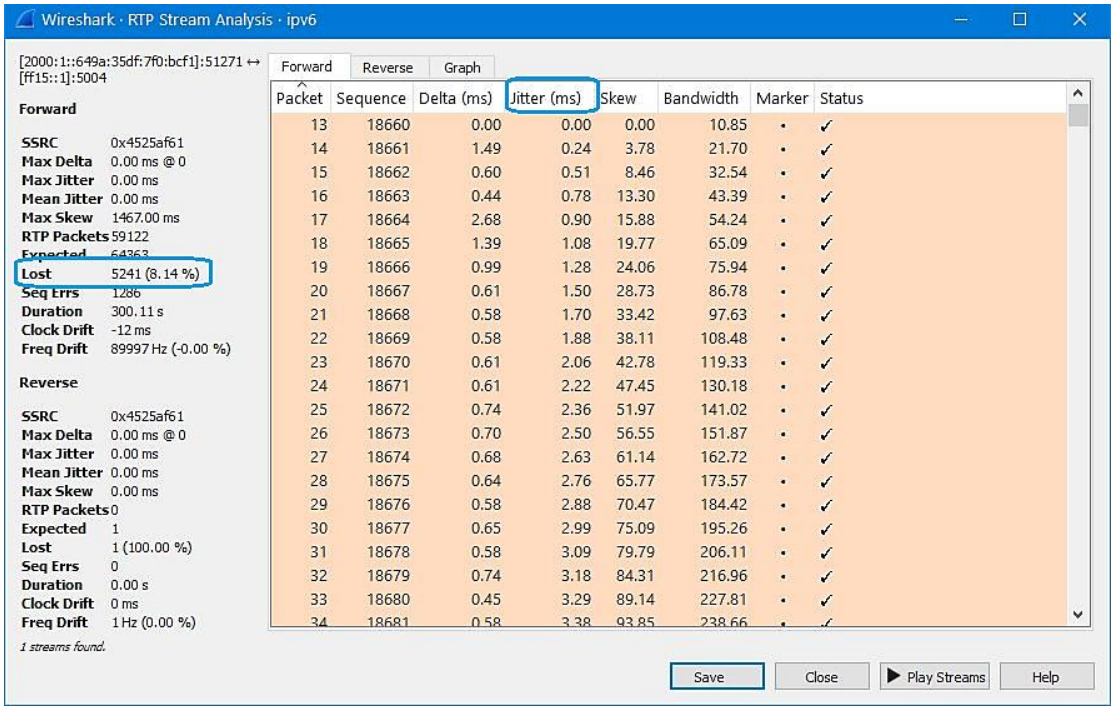


Figura 74. Datos obtenidos de jitter y pérdidas de paquetes para video multicast IPv6

Como se puede apreciar en las figuras anteriores, los valores de jitter son dados para cada paquete UDP, por lo que dichas mediciones deben ser procesadas mediante hojas de cálculo dada la gran cantidad de paquetes obtenidos en la captura de tráfico, muestras que se encuentran entre 46.000 y 214.000 paquetes. Con el procesamiento de los datos se obtiene el valor promedio y su correspondiente desviación estándar. Este último cálculo estadístico indica el grado de dispersión de los valores de jitter en torno al promedio, obteniendo una medida de la estabilidad del protocolo referente a esta unidad de medición de rendimiento.

En la tabla siguiente se presentan los valores obtenidos de jitter con sus correspondientes desviaciones estándar y seguidamente se muestran sus respectivos gráficos.

Tabla 14. Valores de jitter y desviación estándar IPv4 e IPv6 de flujos de video multicast de protocolo único

IPv4			IPv6		
Flujos de video	**Jitter (ms)**	**Desviación estándar (ms)**	**Flujos de video**	**Jitter (ms)**	**Desviación estándar (ms)**
IPv4	9,88	8,9	IPv6	8,46	6,3
IPv4 x 2	9,68	6,5	IPv6 x 2	8,55	6,4
IPv4 x 3	12,42	107,7	IPv6 x 3	10,42	64,78
IPv4 x 4	12,98	120,9	IPv6 x 4	11,39	99,97

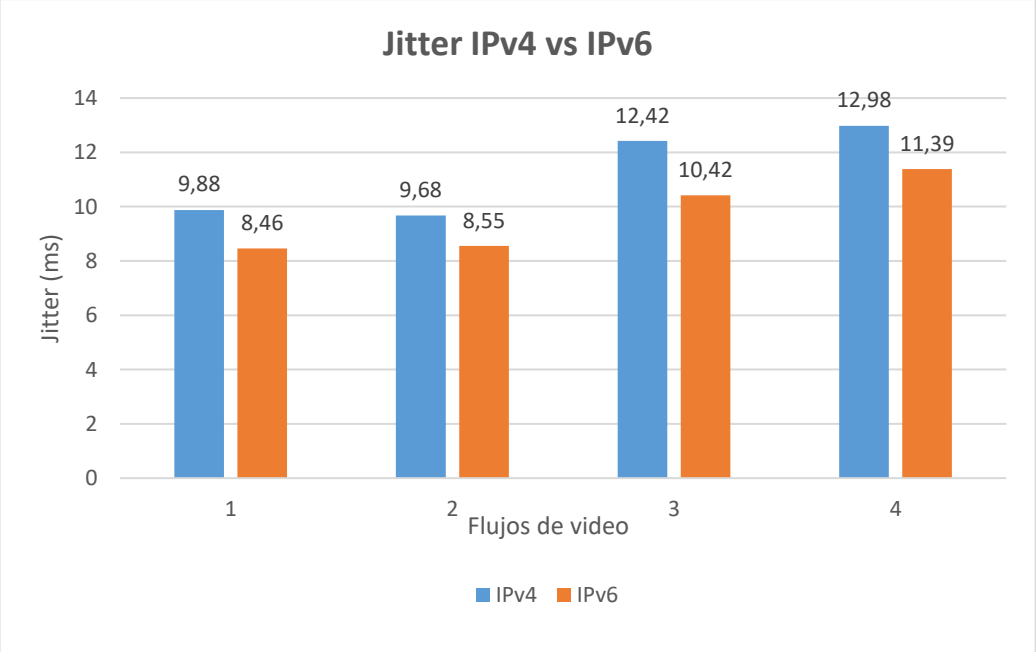


Figura 75. Jitter IPv4 e IPv6 de flujos de video multicast de protocolo único

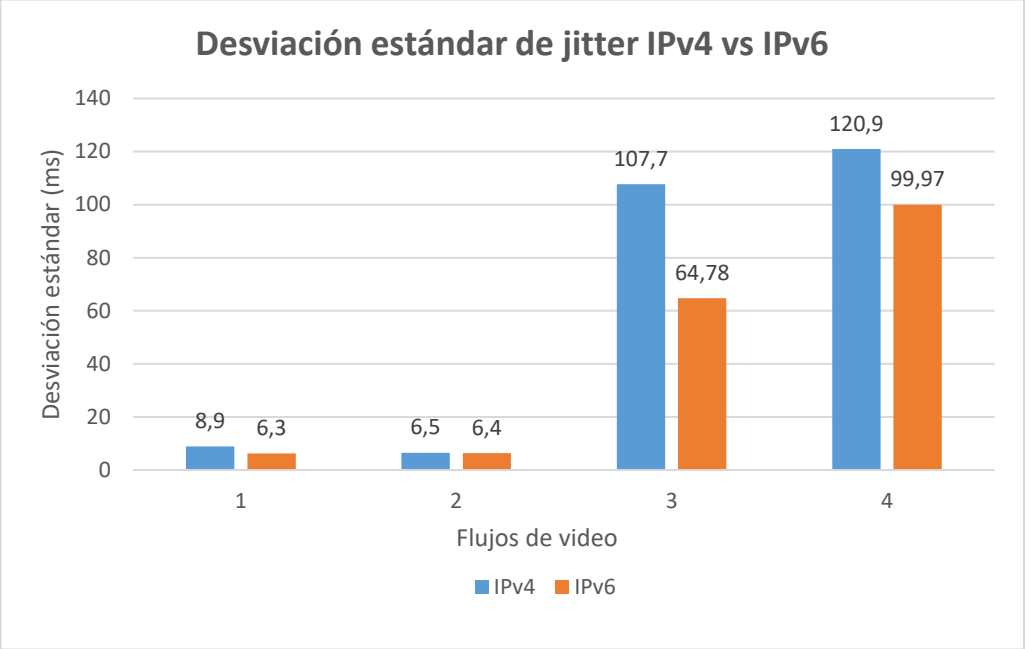


Figura 76. Desviación estándar de jitter IPv4 e IPv6 de flujos de video multicast de protocolo único

En la tabla 15 se presentan los valores de pérdida de paquetes del tráfico de video multicast IPv4 e IPv6 seguida del gráfico que representa dichas mediciones.

Tabla 15.Valores de pérdida de paquetes IPv4 e IPv6 de flujos de video multicast de protocolo único

IPv4		IPv6	
Flujos de video	**Pérdida de paquetes (%)**	**Flujos de video**	**Pérdida de paquetes (%)**
IPv4	28	IPv6	8,1
IPv4 x 2	29,6	IPv6 x 2	7,6
IPv4 x 3	27,9	IPv6 x 3	12,3
IPv4 x 4	29,9	IPv6 x 4	12,1

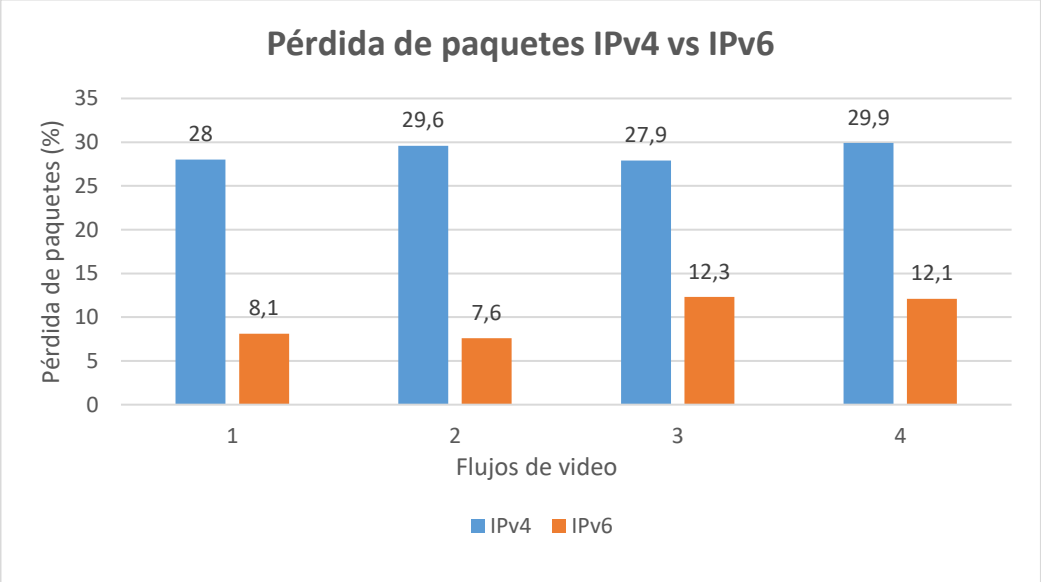


Figura 77. Pérdida de paquetes IPv4 e IPv6 de flujos de video multicast de protocolo único

En la tabla 16 se presentan los valores de tasa de transferencia de datos obtenidos, seguida de su respectivo gráfico que los representa.

Tabla 16. Valores de tasa de transferencia de datos IPv4 e IPv6 de flujos de video multicast de protocolo único

IPv4		IPv6	
Flujos de video	**Tasa de transferencia de datos (Mbps)**	**Flujos de video**	**Tasa de transferencia de datos (Mbps)**
IPv4	1,68	IPv6	2,19
IPv4 x 2	1,68	IPv6 x 2	2,18
IPv4 x 3	1,6	IPv6 x 3	2,08
IPv4 x 4	1,61	IPv6 x 4	2,06

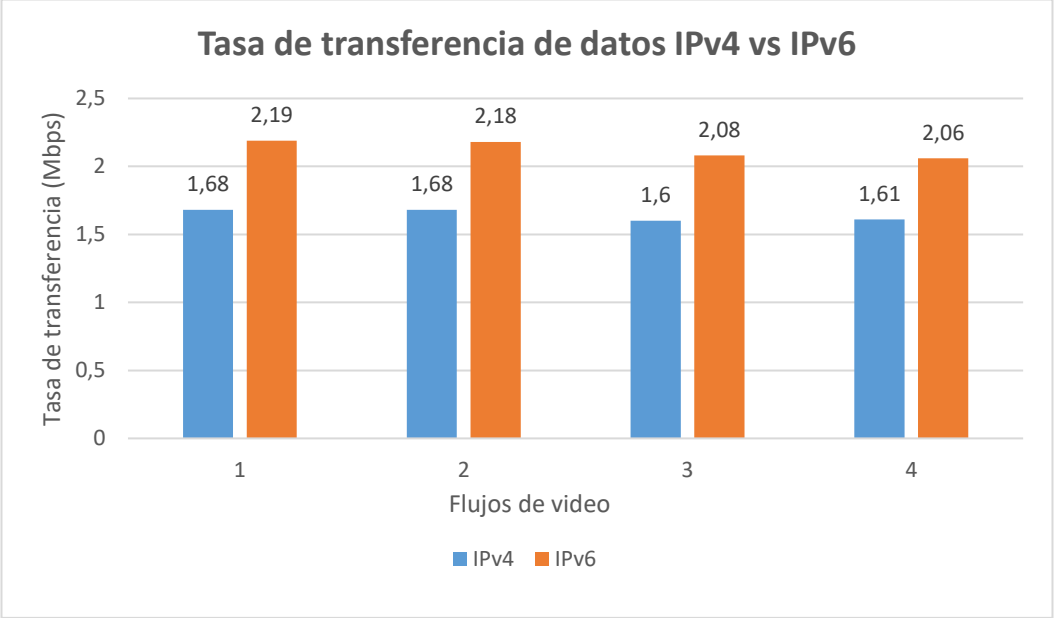


Figura 78. Tasa de transferencia de datos IPv4 e IPv6 de flujos de video multicast de protocolo único

4.2.2.3 Análisis de los resultados

Jitter. – IPv4 posee valores ligeramente superiores a IPv6 para todos los flujos de video. Tanto el jitter de IPv4 como el de IPv6 crece toda vez que se incrementa un flujo de video. Se observa que ambos protocolos incrementan aproximadamente 3 ms de jitter con 4 flujos de video respecto de lo observado con un solo flujo.

Pérdida de paquetes. - IPv4 presenta pérdidas de paquetes superiores a IPv6 en aproximadamente un 20% para todos los flujos de video. Ambos protocolos presentan una tendencia alcista, pero en ligero mayor grado IPv6, dado que para 4 flujos de video, IPv4 aumenta aproximadamente 2%, mientras que IPv6 sube en 4%.

Tasa de transferencia de datos. – IPv6 presenta mayor tasa de transferencia de datos que IPv4 en aproximadamente 500 kbps para todos los flujos de video lo que

equivale un aumento de 30%. Al adicionar flujos de video se observa que para ambos casos la tasa de transferencia de datos disminuye ligeramente.

Desviación estándar de jitter. - Para ambos protocolos se verifica que para un flujo de video multicast adicional, la desviación estándar posee un valor bajo; sin embargo, cuando se adiciona a partir del tercer flujo de video, la desviación estándar incrementa notablemente su valor, pero IPv6 se conserva por debajo de los valores de IPv4.

4.2.3 ANÁLISIS DE JITTER, PÉRDIDA DE PAQUETES Y TASA DE TRANSFERENCIA DE DATOS CON FLUJOS DE VIDEO DE PROTOCOLOS COMBINADOS

4.2.3.1 Procedimiento

Para la ejecución del análisis de rendimiento del tráfico multicast de video IPv4 e IPv6 de protocolos combinados, se procedió de manera similar a lo realizado con el tráfico de protocolo único, con la diferencia de que al momento de transmitir el video de referencia A con protocolo IPv4, los demás flujos de video fueron transmitidos con protocolo IPv6. Lo propio para el caso cuando el video de referencia fue transmitido con protocolo IPv6.

De igual manera que las pruebas anteriores, éstas también tuvieron una duración de 5 minutos cada una.

La primera prueba consistió en transmitir el video de referencia A con IPv4 como protocolo de capa 3 y el segundo flujo de video B con IPv6. La segunda prueba se

realizó transmitiendo el flujo de video A con IPv4 y los 2 flujos de video B y C con IPv6. Finalmente, para la tercera prueba, el flujo de video A con IPv4 se transmitió junto con los 3 flujos B, C y D con IPv6. De esta manera, para el video de referencia transmitido habrá hasta 3 videos con distinto protocolo interactuando al mismo tiempo de tal forma que, se podrá observar y evaluar la interacción entre ellos en cuanto al rendimiento se refiere.

Las pruebas para obtener los datos de rendimiento para IPv6 fueron elaboradas siguiendo la misma metodología que la descrita anteriormente para IPv4.

4.2.3.2 Resultados

En la tabla 17 se muestran los valores de jitter y sus correspondientes desviaciones estándar para flujos de video multicast combinados de IPv4 e IPv6, mientras que en las figuras 79 y 80 se presentan sus gráficos equivalentes.

Tabla 17. Valores de jitter y desviación estánadar IPv4 e IPv6 de flujos de video multicast de protocolos combinados

IPv4			IPv6		
Flujos de video	**Jitter (ms)**	**Desviación estándar (ms)**	**Flujos de video**	**Jitter (ms)**	**Desviación estándar (ms)**
IPv4 + IPv6	9,63	6,5	IPv6 + IPv4	8,67	6,4
IPv4 + IPv6 x 2	9,83	17,1	IPv6 + IPv4 x 2	8,78	10,3
IPv4 + IPv6 x 3	10,49	40,5	IPv6 + IPv4 x 3	8,89	13,1

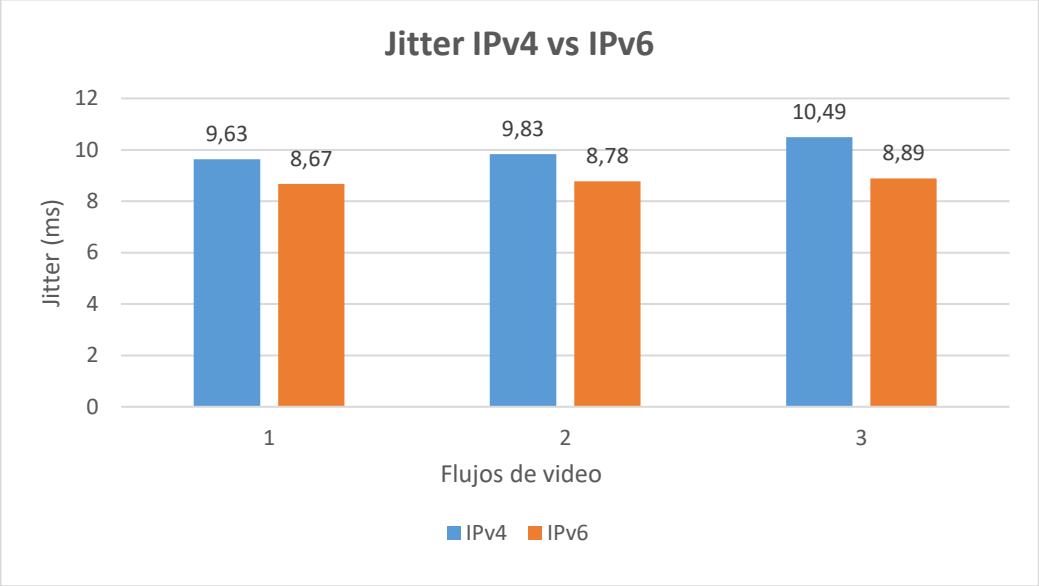


Figura 79. Jitter IPv4 e IPv6 de flujos de video multicast de protocolos combinados

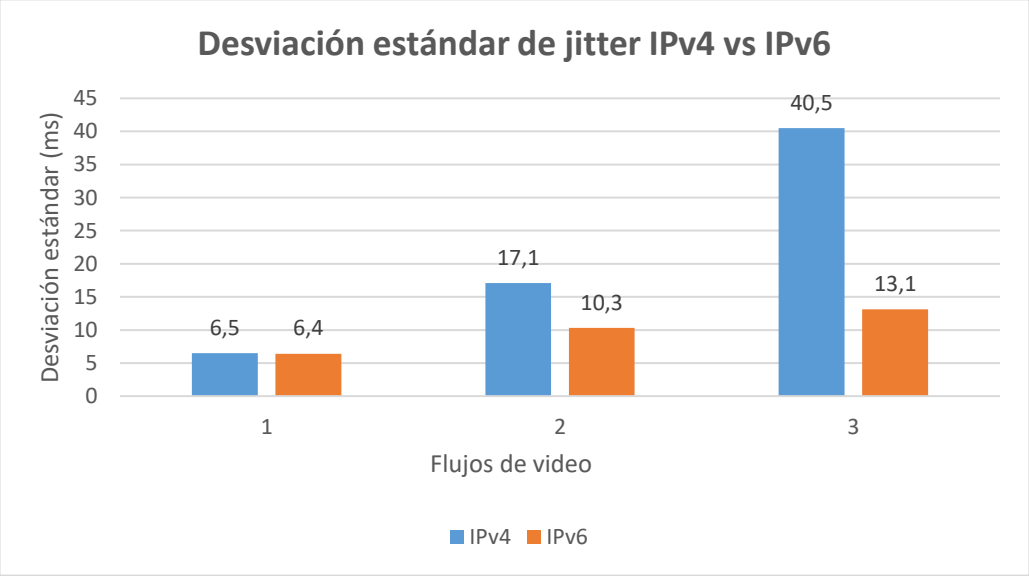


Figura 80. Desviación estándar de jitter IPv4 e IPv6 de flujos de video multicast de protocolos combinados

En la tabla 18 se presentan los valores de pérdida de paquetes obtenidos en las pruebas de flujos de video multicast de protocolos combinados para IPv4 e IPv6 y seguidamente se muestra su correspondiente gráfico.

Tabla 18. Valores de pérdida de paquetes IPv4 e IPv6 de flujos de video multicast de protocolos combinados

IPv4		IPv6	
Flujos de video	**Pérdida de paquetes (%)**	**Flujos de video**	**Pérdida de paquetes (%)**
IPv4 + IPv6	28,4	IPv6 + IPv4	8,4
IPv4 + IPv6 x 2	27,8	IPv6 + IPv4 x 2	8,1
IPv4 + IPv6 x 3	26,7	IPv6 + IPv4 x 3	9

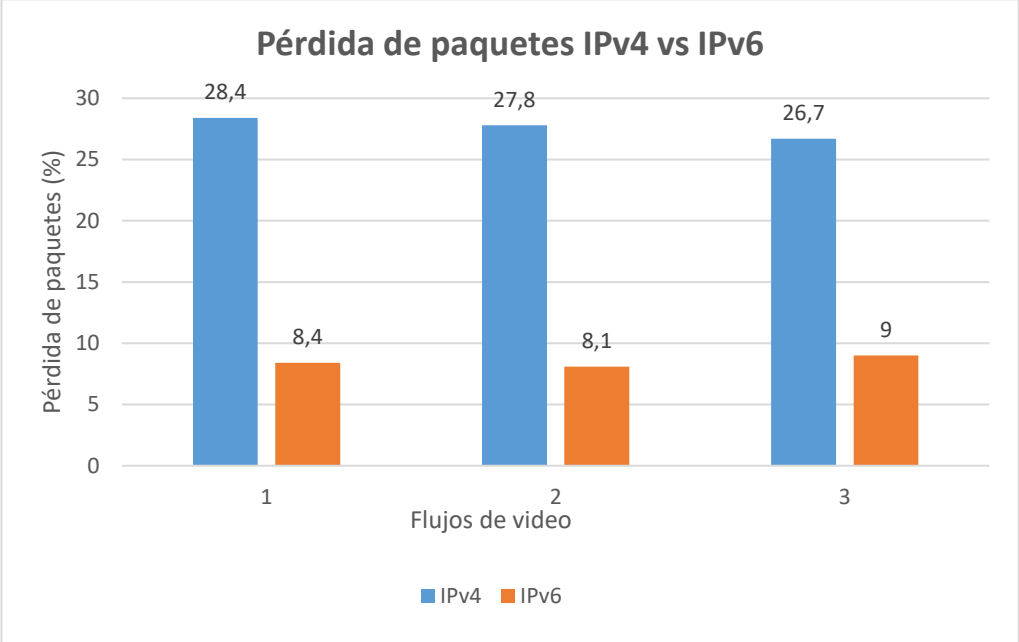


Figura 81. Pérdida de paquetes IPv4 e IPv6 de flujos de video multicast de protocolos combinados

En la tabla 19 constan los resultados obtenidos referentes a la tasa de transferencia de datos para IPv4 e IPv6 con flujos de video multicast de protocolos combinados y luego se presenta el gráfico correspondiente.

Tabla 19. Valores de tasa de transferencia de datos IPv4 e IPv6 de flujos de video multicast de protocolos combinados

IPv4		IPv6	
Flujos de video	**Tasa de transferencia de datos (Mbps)**	**Flujos de video**	**Tasa de transferencia de datos (Mbps)**
IPv4 + IPv6	1,69	IPv6 + IPv4	2,16
IPv4 + IPv6 x 2	1,72	IPv6 + IPv4 x 2	2,18
IPv4 + IPv6 x 3	1,85	IPv6 + IPv4 x 3	2,16

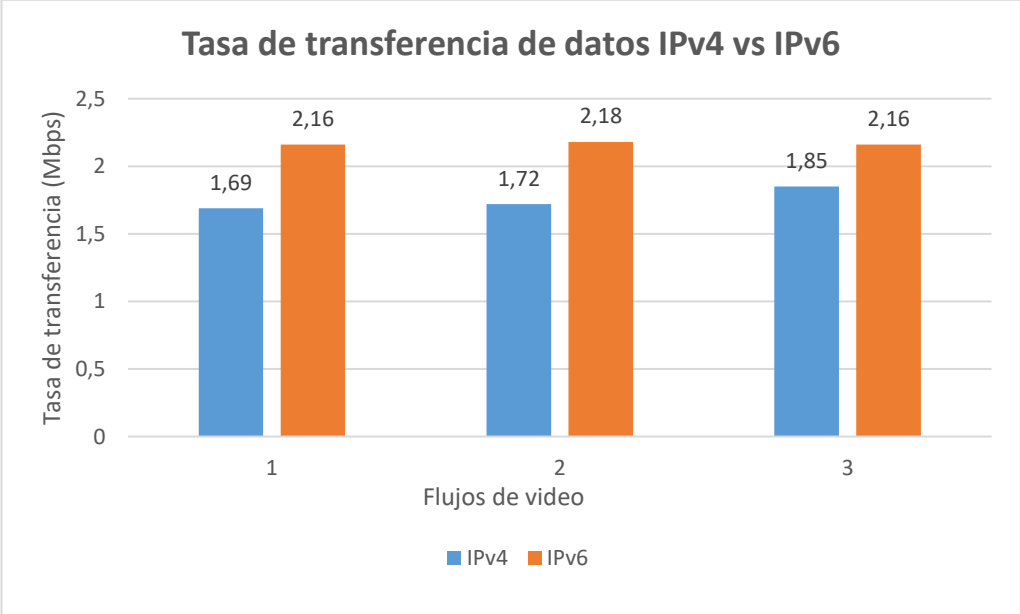


Figura 82. Tasa de transferencia de datos IPv4 e IPv6 de flujos de video multicast de protocolos combinados

4.2.3.3 Análisis de los resultados

Jitter. - IPv4 presenta valores ligeramente mayores que IPv6 para todos los flujos de video. Adicionalmente, se observa que para ambos protocolos existe una tendencia en aumento, pero de menor crecimiento a la observada en las pruebas de protocolo único.

Pérdida de paquetes. – IPv4 presenta valores mayores que IPv6 de aproximadamente un 20% para todos los flujos de video. Se observa también que para el caso de IPv4, el porcentaje de pérdida de paquetes disminuye ligeramente y para IPv6 éstas aumentan apenas un 0,6% cuando se adicionan 3 flujos de video de IPv4.

Tasa de transferencia de datos. – IPv6 presenta mayor tasa de transferencia de datos que IPv4 para todos los flujos de video. Para IPv6 se observa que la tasa de transferencia de datos permanece invariable mientras que IPv4 aumenta su valor cada vez que se adiciona un flujo de video IPv6.

Desviación estándar de jitter. – Los valores de IPv4 son mayores que los de IPv6 para todos los flujos de video. Para IPv6 se observa una tendencia creciente lineal, mientras que para IPv4 se tiene una tendencia exponencial, planteando de esta manera una marcada diferencia entre ambos protocolos al momento de adicionar un flujo de video de protocolo diferente.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

5.1.1 CONCLUSIONES DE LAS PRUEBAS CON TRÁFICO SIMULADO

Tanto el valor mayor de throughput, así como los valores menores de pérdidas de paquetes y tiempo de respuesta de ida y vuelta que las pruebas de tráfico multicast IPv6 presentan frente a IPv4, tienen que ver con la velocidad de procesamiento de las cabeceras que los routers ejecutan. Puesto que la cabecera de IPv6 es más simple que la de IPv4, los routers la procesan más rápidamente dando como resultado un mayor rendimiento de IPv6 para tráfico multicast. En la figura presentada a continuación se muestra las cabeceras IPv4 e IPv6 con sus campos correspondientes.

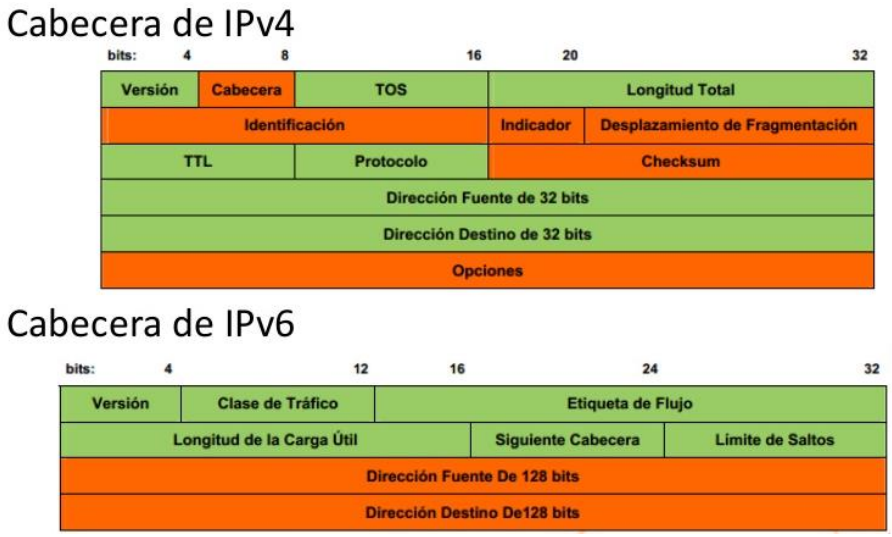


Figura 83. Cabeceras IPv4 e IPv6

Fuente: http://image.slidesharecdn.com/1ipv6-130314173450-phpapp01/95/ipv6-19-638.jpg?cb=1363282614

Por otro lado, como se pudo apreciar en los datos adquiridos referentes a la prueba de jitter para distintos tamaños de paquetes y velocidad constante, multicast IPv4 tiene un ligero mejor rendimiento que IPv6, lo que lo haría óptimo para difundir tráfico de publicidad, noticias, o encuestas que los proveedores de servicio deseen hacer llegar a sus clientes; así como también órdenes o comandos a equipos del proveedor del servicio, y todo tipo de tráfico multicast enmarcado en las características de tráfico multicast de velocidad constante. No obstante, el hecho de la diferencia tan marcada en cuanto a las pérdidas de paquetes que presenta frente a IPv6 junto con la desviación estándar de jitter hace que IPv6 sea superior en rendimiento para la transmisión de tráfico multicast para velocidad constante.

Para minimizar las pérdidas de paquetes en la trasmisión de tráfico multicast IPv4 e IPv6 se deben configurar las aplicaciones y/o los equipos de red de tal forma que los paquetes de datos no sean de tamaño inferior a 1000 bytes puesto que en las pruebas se verificó que con paquetes de tamaño pequeño, menores a 400 bytes, las pérdidas de paquetes son altamente significativas causando un gran deterioro en el rendimiento del tráfico multicast.

Dado que en las pruebas de tiempo de ida y vuelta el tráfico multicast IPv6 demuestra tener tiempos de respuesta más bajos que IPv4 para cualquier tamaño de paquete, se concluye que IPv6 posee mejor rendimiento para aplicaciones interactivas como por ejemplo, juegos en línea, simulaciones, y aplicaciones en las cuales se requiere de un tiempo de respuesta lo más bajo posible para una adecuada experiencia de usuario.

5.1.2 CONCLUSIONES DE LAS PRUEBAS CON TRÁFICO REAL DE VIDEO

Si bien las pruebas con velocidad constante y tamaños de paquete variable realizadas con tráfico simulado demostraron que multicast IPv6 presenta mayor jitter que IPv4, con las pruebas de tráfico multicast de video se evidencia que, con tamaños de paquete constantes y velocidad de transferencia de datos variable, el jitter y pérdida de paquetes de multicast IPv6 en todos los casos examinados son menores que los valores que presenta IPv4.

Tanto para tráfico multicast de protocolo único como tráfico multicast de protocolos combinados, la diferencia de jitter entre IPv4 e IPv6 no es muy notoria, ya que se encuentra en promedio de 1,5 ms de diferencia. No así el caso de los valores de pérdida de paquetes, puesto que la diferencia se encuentra en 20% aproximadamente; siendo este porcentaje muy considerable y sin duda marca una gran diferencia en cuanto a rendimiento se refiere entre ambos protocolos haciendo a IPv6 muy superior.

Con base a los análisis realizados a los resultados de pérdidas de paquetes, jitter y desviación estándar de jitter, se concluye que IPv6 presenta un mejor rendimiento al tiempo de adicionar flujos de video multicast del mismo protocolo debido a que comparado con IPv4 posee menor jitter y sobre todo, menor desviación estándar de jitter lo que indica que los paquetes al arribar a su destino se encuentran menos dispersos en tiempo de llegada, dándole a multicast IPv6 mayor estabilidad y por consiguiente, mayor rendimiento. Adicionalmente, IPv6 posee valores mucho menores de porcentaje de pérdida de paquetes.

Conforme a los resultados obtenidos en las pruebas realizadas con tráfico multicast IPv4 e IPv6 con protocolos combinados, se evidencia que con IPv6 se puede obtener un mejor rendimiento puesto que posee un menor jitter y mucho menor pérdida de paquetes, aunque utiliza un mayor ancho de banda del canal. Las respuestas a adiciones de flujos de video de protocolos diferentes resultan ser muy similares a las presentadas en los resultados derivados de protocolo único, sin embargo, en los resultados de desviación estándar de jitter se aprecia que IPv6 tiene una mejor tolerancia a la adición de flujo de video de multicast IPv4 dado que su respuesta es lineal, no así IPv4, ya que su respuesta es exponencial. Estos resultados denotan que IPv6 presenta mayor inmunidad frente a tráfico multicast IPv4 que se transmita por su mismo canal.

Con estos resultados se infiere que IPv6 posee mejor rendimiento para la transmisión de tráfico multicast de tiempo real, tales como voz y video en aplicaciones como videoconferencia, IPTV, video bajo demanda, video streaming, etc., aunque el precio que se debe pagar es utilizar un mayor ancho de banda del canal de datos, siendo éste excedente de aproximadamente 30% en las pruebas ejecutadas.

5.2 RECOMENDACIONES

Puesto que las pruebas efectuadas con video multicast muestran que la desviación estándar de jitter aumenta con la adición de flujos de video, ya sean estos del mismo protocolo o diferente, es recomendable usar para la trasmisión multicast buffers de de-jitter, sobre todo para los casos de tráfico sensible al jitter como lo es el de tiempo real. Adicionalmente, se debe implementar calidad de servicio QoS en las redes que ofrecen los servicios de multicast con el objetivo de maximizar los recursos limitados de red disponibles de tal modo de entregar la máxima calidad de servicio disponible al usuario.

Se recomienda realizar pruebas de tráfico multicast con otros formatos (más precisamente, contenedores) de video, tales como MPEG, MP4, MOV, WMV, MKV, FLV, etc., con el objetivo de compararlos bajo los parámetros y lineamientos utilizados en el presente trabajo y determinar de esta manera el formato que mejor rendimiento presente ya que cada contenedor posee diferentes códecs de audio y video con gran variedad de relación entre compresión y calidad.

Debido a que en el presente trabajo el protocolo de enrutamiento multicast utilizado para realizar las pruebas fue PIM-SM, se recomienda ejecutar las mismas con el protocolo PIM-DM con la finalidad de evaluar si el cambio de protocolo de enrutamiento multicast tiene incidencia en el rendimiento de la transmisión de tráfico.

Se recomienda mantener actualizados los IOS de los routers a las últimas versiones estables liberadas por el fabricante, ya que en los inicios de las pruebas se presentaron problemas con la conformación y distribución de la tabla de enrutamiento de multicast IPv4 en R1 debido a que este router se encontraba con una versión de IOS antigua comparada con los demás sistemas operativos de los routers restantes.

BIBLIOGRAFÍA

Aghvami, H., Gluhak, A., & Rümmler, R. (2009). *Multicast in Third-Generation Mobile Networks.* Reino Unido: Wiley.

Benslimane, A. (2007). *Multimedia Multicast on the Internet.* Newport Beach, Estados Unidos: ISTE Ltd.

Blum, R. (2003). *Network Performance Open Source Toolkit.* Indianapolis: Wiley Publishing, Inc.

Cebas, B. (8 de abril de 2015). *Los 4 tipos de Video On Demand*. Recuperado el 16 de marzo de 2016, de http://beatrizcebas.com/2015/04/08/los-4-tipos-del-video-on-demand/

Cisco Systems. (18 de abril de 2002). *IP Multicast Technology Overview.* Recuperado el 20 de marzo de 2016, de http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_pap

ers/mcst_ovr.html

Cisco Systems. (2004). *IPv6 Multicast deployment and configuration guide.* Recuperado el 21 de marzo de 2016, de http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/ipv6-multicast/product_data_sheet0900aecd80320fb8.pdf

Cisco Systems. (2 de febrero de 2006). *Understanding Jitter in Packet Voice Networks*. Recuperado el 8 de mayo de 2016, de http://www.cisco.com/c/en/us/support/docs/voice/voice-quality/18902-jitter-packet-voice.html

Cisco Systems. (Febrero de 2008). *Bidirectional PIM Deployment Guide.* Recuperado el 30 de abril de 2016, de

http://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multicast-enterprise/prod_white_paper0900aecd80310db2.pdf

Cisco Systems. (3 de noviembre de 2009). *Portable Product Sheets – Routing Performance*. Recuperado el 14 de julio de 2016, de http://www.cisco.com/web/partners/downloads/765/tools/quickreference/routerperformance.pdf

Cisco Systems. (31 de julio de 2012). *Implementing IPv6 Multicast*. Recuperado el 10 de abril de 2016, de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-multicast.pdf

Cisco Systems. (s.f.). *Overview of IP Multicast*. Recuperado el 6 de marzo de 2016, de http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a0080092942.shtml

Davies, J. (2012). *Understanding IPv6* (Tercera ed.). Sebastopol, Estados Unidos: O'Reilly Media, Inc.

Edwards, B., Giuliano, L., & Wright, B. (2002). *Interdomain Multicast Routing: Practical Juniper Networks and Cisco.* Addison Wesley.

Hurley, M. (28 de abril de 2015). *4 causes of packet loss and how to fix them*. Recuperado el 10 de mayo de 2016, de http://www.annese.com/blog/what-causes-packet-loss

IANA. (7 de marzo de 2016). *IPv4 Multicast Address Space Registry.* Recuperado el 20 de marzo de 2016, de http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml

IANA. (7 de marzo de 2016). *IPv6 Multicast Address Space Registry.* Recuperado el 27 de marzo de 2016, de http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

IETF. (Julio de 1991). *RFC 1242. Benchmarking Terminology for Network Interconnection Devices*. Recuperado el 7 de mayo de 2016, de https://www.ietf.org/rfc/rfc1242.txt

IETF. (agosto de 2002). *RFC 3306. Unicast-Prefix-based IPv6 Multicast Addresses.* Recuperado el 27 de marzo de 2016, de https://tools.ietf.org/html/rfc3306

IETF. (abril de 2003). *RFC 3513. Internet Protocol Version 6 (IPv6) Addressing Architecture.* Recuperado el 21 de marzo de 2016, de https://www.ietf.org/rfc/rfc3513.txt

IETF. (Noviembre de 2004). *RFC 3956. Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address.* Recuperado el 22 de Abril de 2016, de https://tools.ietf.org/html/rfc3956

Jiang, S. (23 de febrero de 2011). *IPv4/IPv6 multicast interoperation.* Recuperado el 15 de octubre de 2015, de Huawei: https://meetings.apnic.net/__data/assets/pdf_file/0013/31315/JiangSheng-Multicast-in-46transition.pdf

Jinmei, T., Li, Q., & Shima, K. (2007). *IPv6 Advanced Protocols Implementation.* San Francisco: Elsevier.

Joseph, V., & Mulugu, S. (2011). *Deploying Next Generation Multicast-Enabled Applications.* Waltham, Estados Unidos: Elsevier.

Juniper Networks. (8 de enero de 2014). *Understanding Group Membership Protocols*. Recuperado el 4 de abril de 2016, de http://www.juniper.net/documentation/en_US/junos13.3/topics/concept/multicast-group-membership.html

Kocharians, N., & Vinson, T. (2015). *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2* (Quinta ed.). Indianapolis, Estados Unidos: Cisco Press.

Liotine, M. (2003). *Mission-Critical Network Planning.* Boston: Artech House, Inc.

Martin, T. (2015). *Cisco "Tech Session" IPv6 Has New Friends.* Recuperado el 15 de Abril de 2016, de http://documents.tips/download/link/fedv6tf-ipv6-new-friends

National Instruments. (17 de abril de 2013). *Understanding and Characterizing Timing Jitter*. Recuperado el 8 de mayo de 2016, de http://www.ni.com/white-paper/14227/en/

Pinizzotto, A., & Rossi, L. (15 de julio de 2003). *IPv4/IPv6 Multicast Interoperability.* Recuperado el 3 de octubre de 2015, de 6NET: https://www.6net.org/publications/deliverables/D3.4.4.pdf

Shimonski, R. (2013). *The Wireshark Field Guide.* Waltham, Estados Unidos: Elsevier.

Venaas, S. (s.f.). *IPv4 - IPv6 Multicast Gateway.* Recuperado el 1 de mayo de 2016, de http://www.internet2.edu/presentations/jt2006feb/20060206-mcgw-venaas.ppt

Walton, A. (2016). *Importance of Data Transfer Rate in Computer Networks*. Recuperado el 8 de mayo de 2016, de http://smallbusiness.chron.com/importance-data-transfer-rate-computer-networks-69614.html

Wiki.org. (21 de octubre de 2014). *VLC media player*. Recuperado el 16 de mayo de 2016, de https://wiki.videolan.org/VLC_media_player

Williamson, B. (2000). *Developing IP Multicast Networks.* Indianapolis: Cisco Press.

Xianfeng, Y., & Zheng, C. (2013). *IPv4-IPv6 Multicast Transition Technologies.* Recuperado el 5 de octubre de 2015, de ZTE Corporation: http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2006year/no3/articles/200610/t20061010_162407.html

ANEXOS

ANEXO 1. CONFIGURACIONES DE LOS ROUTERS

Router R1

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
dot11 syslog
ip cef
!

ip multicast-routing
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 multicast-routing
multilink bundle-name authenticated
!
!
vtp mode transparent
!
!
archive
 log config
  hidekeys
!
!
vlan 2
 name VLAN-2
!
vlan 3
 name VLAN-3
!
```

```
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface FastEthernet0
 switchport access vlan 2
!
interface FastEthernet1
 switchport access vlan 3
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
interface Vlan2
 ip address 172.0.1.1 255.255.255.0
 ip pim sparse-mode
 ipv6 address 2000:1::1/64
 ipv6 ospf 1 area 0
!
interface Vlan3
 ip address 172.0.2.1 255.255.255.0
 ip pim sparse-mode
 ipv6 address 2000:2::1/64
 ipv6 ospf 1 area 0
!
router ospf 1
 log-adjacency-changes
 passive-interface Vlan2
 network 172.0.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip pim rp-address 172.0.2.2
!
no cdp run
!
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface Vlan2
!
```

```
ipv6 pim rp-address 2000:2::2
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Router R2

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef
!
ip multicast-routing
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface FastEthernet0
 switchport access vlan 2
!
interface FastEthernet1
 switchport access vlan 3
!
interface FastEthernet2
```

```
!
interface FastEthernet3
!
interface FastEthernet4
 ip address 172.0.2.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 ipv6 address 2000:2::2/64
 ipv6 ospf 1 area 0
!
interface Vlan1
 no ip address
 no ipv6 mfib forwarding
!
interface Vlan3
 ip address 172.0.5.1 255.255.255.0
 ip pim dense-mode
 ipv6 address 2000:5::1/64
 ipv6 ospf 1 area 0
!
interface Vlan2
 ip address 172.0.3.1 255.255.255.0
 ip pim dense-mode
 ipv6 address 2000:3::1/64
 ipv6 ospf 1 area 0
!
router ospf 1
 log-adjacency-changes
 network 172.0.0.0 0.0.255.255 area 0
!
!
no ip http server
no ip http secure-server
ip pim rp-address 172.0.2.2
!
no cdp run
!
!
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
!
ipv6 pim rp-address 2000:2::2
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
```

```
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Router R3

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
ip cef
!
!
ip multicast-routing
!
ipv6 unicast-routing
ipv6 multicast-routing
!
voice-card 0
 no dspfarm
!
!
interface Loopback0
 ip address 172.0.7.1 255.255.255.0
 ip pim sparse-mode
 ip igmp join-group 239.1.1.1
 ipv6 address 2000:7::1/64
 ipv6 mld join-group FF15::1
 ipv6 ospf 1 area 0
!
interface FastEthernet0/0
 ip address 172.0.3.2 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 ipv6 address 2000:3::2/64
```

```
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 172.0.4.1 255.255.255.0
 ip pim sparse-mode
 duplex auto
 speed auto
 ipv6 address 2000:4::1/64
 ipv6 ospf 1 area 0
!
router ospf 1
 log-adjacency-changes
 network 172.0.0.0 0.0.255.255 area 0
!
!
ip http server
no ip http secure-server
ip pim rp-address 172.0.2.2
!
no cdp run
ipv6 router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
!
ipv6 pim rp-address 2000:2::2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
!
end
```

Router R4

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
```

```
boot-end-marker
!
!
no aaa new-model
!
!
dot11 syslog
ip cef
!
!
ip multicast-routing
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ipv6 unicast-routing
ipv6 multicast-routing
multilink bundle-name authenticated
!
!
vtp mode transparent
!
!
archive
 log config
  hidekeys
!
!
vlan 2
 name VLAN-2
!
vlan 3
 name VLAN-3
!
vlan 4
 name VLAN-4
!
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface FastEthernet0
 switchport access vlan 2
!
interface FastEthernet1
 switchport access vlan 3
!
interface FastEthernet2
 switchport access vlan 4
!
```

```
interface FastEthernet3
!
interface Vlan1
 no ip address
!
interface Vlan2
 ip address 172.0.5.2 255.255.255.0
 ip pim sparse-mode
 ipv6 address 2000:5::2/64
 ipv6 ospf 1 area 0
!
interface Vlan3
 ip address 172.0.4.2 255.255.255.0
 ip pim sparse-mode
 ipv6 address 2000:4::2/64
 ipv6 ospf 1 area 0
!
interface Vlan4
 ip address 172.0.6.1 255.255.255.0
 ip pim sparse-mode
 ip igmp join-group 239.1.1.1
 ipv6 address 2000:6::1/64
 ipv6 mld join-group FF15::1
 ipv6 ospf 1 area 0
!
router ospf 1
 log-adjacency-changes
 passive-interface Vlan4
 network 172.0.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip pim rp-address 172.0.2.2
!
no cdp run
!
!
ipv6 router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 passive-interface Vlan4
!
ipv6 pim rp-address 2000:2::2
!
!
control-plane
!
!
line con 0
```

```
 no modem enable
line aux 0
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

ANEXO 2. ROUTERS UTILIZADOS PARA EL ANÁLISIS

En la fotografía mostrada a continuación se presentan los routers Cisco utilizados para efectuar el análisis de rendimiento objeto de la presente tesis.

De arriba hacia abajo constan los siguientes routers:

- Cisco 877-M
- Cisco 871
- Cisco 877-M
- Cisco 2811