



La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.
- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.
- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

**FACULTAD DE INGENIERÍA ELÉCTRICA Y
ELECTRÓNICA**

**ANÁLISIS DE LOS PARÁMETROS DE CALIDAD
EN UNA RED DE DISTRIBUCIÓN PARA
PROPORCIONAR IPTV CON IPV6.**

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

**CARLOS ANDRES VELOZ CISNEROS
carlosandresveloz@gmail.com**

**DIRECTOR: ING. MSC. CARLOS ROBERTO EGAS ACOSTA
cegas@epn.edu.ec**

Quito, Septiembre 2014

DECLARACIÓN

Yo Carlos Andrés Veloz Cisneros, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

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

Carlos Andrés Veloz Cisneros

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Carlos Andrés Veloz Cisneros, bajo mi supervisión.

ING. MSC. CARLOS EGAS
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios, por la fortaleza durante toda mi vida para superar cualquier reto que se me ha presentado, sabiduría para luchar por las cosas que anhelo y por la salud, el regalo más grande e imprescindible para poder culminar este reto.

Un agradecimiento muy grande para mi familia, pero de manera especial a mi padre Carlos Vinicio y a mi madre María Carlota, quienes siempre me brindaron su apoyo incondicional en todas las etapas de mi vida, y sobretodo fueron el motor que hizo posible que cumpla esta meta, esto es por ellos.

A profesores, amigos y compañeros de Universidad, quienes forman parte importante de mi vida y con quienes compartí mi etapa estudiantil y ahora compartiré mi etapa profesional.

DEDICATORIA

Este trabajo final, que representa el esfuerzo y sacrificio de muchos años, se lo dedico de manera muy especial a mi padre Carlos Vinicio y a mi madre María Carlota, todo este esfuerzo durante estos años ha sido también su sacrificio y en gran medida este logro es gracias a ellos.

ÍNDICE DE CONTENIDOS

RESUMEN	1
PRESENTACIÓN	3
CAPÍTULO I	5
FUNDAMENTOS TEÓRICOS	5
1.1 CONCEPTOS IPv6.....	5
1.1.1 MOTIVOS PARA IPv6.....	5
1.1.2 LA SOLUCIÓN IPv6.....	6
1.1.2.1 Características de IPv6.....	7
1.1.3 LA BASE DE IPv6.....	7
1.1.4 DIRECCIONES Y DIRECCIONAMIENTO EN IPv6	11
1.1.4.1 Definición de dirección en IPv6.....	11
1.1.4.2 Reservas de espacio de direccionamiento en IPv6	12
1.1.4.3 Direcciones especiales en IPv6	13
1.1.5 REPRESENTACIÓN DE LAS DIRECCIONES IPv6	14
1.1.5.1 Direcciones unicast locales	15
1.1.5.2 Direcciones anycast.....	17
1.1.5.3 Direcciones multicast.....	19
1.1.6 DIRECCIONES REQUERIDAS PARA CUALQUIER NODO	21
1.1.7 CONCEPTOS DE ENRUTAMIENTO.....	22
1.1.7.1 Tipos de protocolos de enrutamiento.....	22
1.1.7.2 Criterios de selección IGP	23
1.1.7.3 Enrutamiento IPv6	23
1.1.7.4 RIP.....	24
1.1.7.5 EIGRP IPv6	24
1.1.7.6 OSPF.....	25
1.1.7.7 IS-IS.....	27
1.1.7.8 BGP.....	27
1.1.8 MULTICAST.....	29

1.1.8.1	Conceptos multicast	29
1.1.8.1.1	Multicast Distribution Tree (MDT).....	30
1.1.8.1.2	Shortest Path Tree (SPT).....	30
1.1.8.1.3	Shared Tree (ST)	30
1.1.8.2	Funcionamiento	30
1.1.8.3	Aplicaciones de multicast	31
1.1.8.4	Protocolo MLD.....	31
1.1.8.4.1	El paquete MLD	32
1.1.8.4.2	MLDv2.....	32
1.1.8.5	PIM Protocol Independent Multicast	32
1.1.8.5.1	PIM-DM – PIM Dense Mode	33
1.1.8.5.2	PIM-SM – PIM Sparse Mode.....	33
1.1.8.5.3	RP - Rendezvous Point.....	33
1.1.8.5.4	MBGP - Multi Protocol BGP	33
1.1.8.5.5	MSDP - Multicast Source Discovery Protocol	33
1.1.8.6	Multicast interdominio	34
1.1.8.6.1	Embedded-RP.....	34
1.2	PARÁMETROS DE CALIDAD DE UNA RED DE DISTRIBUCIÓN	36
1.2.1	VELOCIDAD DE TRANSMISIÓN	36
1.2.1.1	Tasa de transferencia teórica en una red Ethernet.....	37
1.2.1.2	Tasa de Transferencia Real	37
1.2.2	LATENCIA	37
1.2.2.1	Ecuaciones relacionadas a la latencia.....	38
1.2.2.2	Latencia y la tasa de transferencia	38
1.2.3	JITTER.....	38
1.2.4	PÉRDIDA DE PAQUETES.....	41
1.2.4.1	Compensación de pérdida de paquetes	41
1.3	IPTV	42
1.3.1	¿QUÉ ES IPTV?	42
1.3.2	VENTAJAS DE IPTV	43
1.3.2.1	Interactividad	43
1.3.2.2	Cambio de tiempo (Time shifting)	43
1.3.2.3	Integración.....	44

1.3.2.4	Personalización	44
1.3.2.5	Bajos requerimientos de ancho de banda	44
1.3.2.6	Accesible por múltiples dispositivos.....	44
1.3.2.7	Video bajo demanda.....	44
1.3.3	DESVENTAJAS DE IPTV	45
1.3.3.1	Pérdida de paquetes.....	45
1.3.3.2	Cobertura.....	45
1.3.4	SERVICIOS DE IPTV.....	45
1.3.4.1	Canales de broadcast.....	45
1.3.4.2	Contenidos bajo demanda (VoD).....	46
1.3.5	ARQUITECTURA IPTV	46
1.3.5.1	Contribución de señales de vídeo.....	46
1.3.5.2	Servidores VoD.....	47
1.3.5.3	Red de distribución	47
1.3.5.4	Red de acceso del cliente.....	48
1.3.5.5	CPE	48
1.3.5.6	Cliente IPTV.....	48
1.4	GNS3.....	49
1.4.1	REQUERIMIENTOS DEL SISTEMA.....	50
1.4.1.1	Requerimientos del sistema en Windows XP	50
1.4.1.1.1	Memoria RAM:	50
1.4.1.1.2	CPU	51
1.4.1.1.3	Disco	51
1.4.1.2	Requerimientos del sistema en Linux (Ubuntu 9.4)	53
1.4.1.2.1	Memoria RAM	53
1.4.1.2.2	CPU	53
1.4.1.2.3	Disco	53
1.4.2	ARQUITECTURA DEL EMULADOR	55
1.4.2.1	Dynamips.....	55
1.4.2.2	IDLE-PC	56
1.4.2.3	Herramientas de optimización del uso de memoria	56
1.4.2.3.1	Ghostios	56
1.4.2.3.2	Sparsemem.....	57

1.4.2.3.3 Mmap.....	57
1.4.2.4 Dynagen	57
1.4.2.5 Network File.....	58
1.5 WIRESHARK.....	58
1.5.1 ANALIZADOR DE RED.....	58
1.5.2 EVALUACIÓN DE UN ANALIZADOR DE PAQUETES.....	59
1.5.3 VENTAJAS WIRESHARK.....	59
1.5.4 MARCO CONCEPTUAL	60
1.5.4.1 Paquete de datos.....	60
1.5.4.2 Red	60
1.5.4.3 Protocolos.....	61
1.5.4.4 Programas empaquetados con Wireshark.....	61
CAPÍTULO II	62
SIMULACIÓN.....	62
2.1 EXPLICACION DE LA SIMULACIÓN.....	62
2.1.1 CARACTERÍSTICAS TÉCNICAS DEL PC HOST	63
2.1.2 SISTEMAS OPERATIVOS A UTILIZAR	64
2.1.2.1 Sistema Operativo del simulador GNS3	64
2.1.2.2 Características técnicas y Sistema Operativo del Servidor VLC	65
2.1.2.3 Características técnicas y Sistema Operativo de los Clientes	66
2.1.2.4 Programa a utilizar como servidor de streaming y su configuración. 66	
2.1.2.4.1 VLC	66
2.1.2.4.2 Configuración del Servidor VLC	67
2.1.2.4.3 Protocolo RTP.....	68
2.1.2.4.4 Transporte del flujo RTP	68
2.1.2.5 Programa a utilizar para receptor el streaming y su configuración. ..	69
2.1.2.6 Topologías propuestas	70
2.1.2.7 Routers que formarán la red de distribución.....	70
2.1.2.8 Direccinamiento a implementar en routers c1751.....	71
2.1.2.9 Comandos a implementar en routers c1751.....	74
2.1.2.10 Explicación de los comandos más importantes.....	74

2.2	TOPOLOGÍAS A IMPLEMENTAR EN GNS3	76
2.2.1	TOPOLOGÍA TIPO MALLA A IMPLEMENTAR.....	76
2.2.1.1	Direccionamiento de la topología tipo malla	77
2.2.1.2	Comandos implementados en la topología.....	78
2.2.1.3	Capturas de pantalla de la red.....	84
2.2.1.4	Cálculo de los parámetros de calidad en la red de distribución	102
2.2.1.4.1	Cálculos de la Velocidad de Transmisión	104
2.2.1.4.2	Cálculos de Latencia.....	105
2.2.1.4.3	Cálculos de Jitter.....	111
2.2.1.4.4	Cálculos de Pérdida de Paquetes	113
2.2.2	TOPOLOGÍA TIPO ESTRELLA A IMPLEMENTAR	114
2.2.2.1	Direccionamiento de la topología tipo estrella	115
2.2.2.2	Capturas de pantalla de la red de distribución.....	116
2.2.2.3	Cálculo de los parámetros de calidad en la red de distribución	129
2.2.2.3.1	Cálculos de la Velocidad de Transmisión	129
2.2.2.3.2	Cálculos de Latencia.....	129
2.2.2.3.3	Cálculos de Jitter.....	132
2.2.2.3.4	Cálculos de Pérdida de Paquetes	133
2.2.3	TOPOLOGÍA TIPO HÍBRIDA A IMPLEMENTAR	134
2.2.3.1	Direccionamiento de la topología tipo Híbrida	135
2.2.3.2	Capturas de pantalla de la red de distribución.....	136
2.2.3.3	Cálculo de los parámetros de calidad en la red de distribución	150
2.2.3.3.1	Cálculos de la Velocidad de Transmisión	150
2.2.3.3.2	Cálculos de Latencia.....	150
2.2.3.3.3	Cálculos de Jitter.....	153
2.2.3.3.4	Cálculos de Pérdida de Paquetes	154
2.2.4	CÁLCULOS DE PARÁMETROS DE CALIDAD EN TOPOLOGÍA TIPO MALLA DONDE SE AUMENTAN Y DISMINUYEN ROUTERS MIENTRAS SE ENVÍA EL STREAMING DE VIDEO.....	155
2.2.4.1	Topología tipo malla a implementar.....	155
2.2.4.2	Direccionamiento de la topología tipo malla	156
2.2.4.3	Capturas de pantalla de la red de distribución.....	157
2.2.4.4	Cálculo de los parámetros de calidad en la red de distribución	170

2.2.4.4.1	Cálculos de la Velocidad de Transmisión	170
2.2.4.4.2	Cálculos de Latencia.....	171
2.2.4.4.3	Cálculos de Jitter.....	176
2.2.4.4.4	Cálculos de Pérdida de Paquetes	177
CAPÍTULO III	180
DESARROLLO DEL PROTOTIPO	180
3.1	DISEÑO DEL PROTOTIPO PROPUESTO	180
3.1.1	DIRECCIONAMIENTO DE LA RED FÍSICA Y VIRTUAL A IMPLEMENTAR.	181
3.1.1.1	Capturas de pantalla de la red virtual	181
3.1.1.2	Cálculo de los parámetros de calidad en la red de distribución	189
3.1.1.2.1	Cálculos de la Velocidad de Transmisión	189
3.1.1.2.2	Cálculos de Latencia.....	190
3.1.1.2.3	Cálculos de Jitter.....	192
3.1.1.2.4	Cálculos de Pérdida de Paquetes	193
3.2	IMPLEMENTACIÓN DEL PROTOTIPO EN EL LABORATORIO	194
3.2.1	ELEMENTOS A UTILIZAR EN EL LABORATORIO:	194
3.2.2	DATOS OBTENIDOS EN EL LABORATORIO	196
3.2.2.1	Topología a implementar en el laboratorio	196
3.2.2.2	Direccionamiento de la red física a implementar	196
3.2.2.3	Capturas de pantalla de la red física	197
3.2.2.4	Cálculo de los parámetros de calidad en la red de distribución	212
3.2.2.4.1	Cálculos de la Velocidad de Transmisión	212
3.2.2.4.2	Cálculos de Latencia.....	212
3.2.2.4.3	Cálculos de Jitter.....	215
3.2.2.4.4	Cálculos de Pérdida de Paquetes	216
3.3	DENEGACIÓN DE SERVICIO	216
3.3.1	STREAMING DE VIDEO Y FLUJO DE PAQUETES SYN	216
3.3.2	DENEGACIÓN DE SERVICIO.....	217
3.3.2.1	Denegación de servicio de aplicación.....	217
3.3.2.2	Denegación de servicio de red	217
3.3.2.3	SYN Flooding (inundación de SYNs).....	217
3.3.2.4	UDP Flooding (inundación UDP)	218

3.3.2.5 Fragmentación de paquetes	218
3.3.2.6 Denegación de servicio distribuida	219
3.3.2.7 Scapy.....	219
3.3.2.8 Paquetes enviados a la red de distribución	223
3.3.2.9 Prueba de streaming de video enviado a la red de distribución	226
3.3.2.10 Capturas de pantalla de la red	228
3.3.2.11 Cálculo de los parámetros de calidad en la red de distribución...	237
3.3.2.11.1 Cálculos de la Velocidad de Transmisión	237
3.3.2.11.2 Cálculos de Latencia	237
3.3.2.11.3 Cálculos de Jitter.....	240
3.3.2.11.4 Cálculos de Pérdida de Paquetes	241
CAPÍTULO IV	243
PRUEBAS Y ANÁLISIS DE RESULTADOS.....	243
CAPÍTULO V	270
CONCLUSIONES Y RECOMENDACIONES	270
BIBLIOGRAFÍA	273

RESUMEN

El presente proyecto tiene como propósito realizar un análisis de los parámetros de calidad, involucrados a nivel de red, en una red de distribución con IPv6 como protocolo de red, mediante simulación con el GNS3. Para cumplir con este objetivo, se han implementado varios escenarios, con el fin de realizar la medición y análisis técnico de los parámetros: latencia, variación de retardo, velocidad de transmisión efectiva y pérdida de paquetes, involucrados en la difusión de IPTV, tomando como factor fundamental, el retardo debido al procesamiento de la información en los nodos internos de la red.

En el primer capítulo, se da a conocer los conceptos básicos relacionados con: IPv6, conceptos de enrutamiento, multicast, parámetros de calidad en una red de distribución, IPTV, GNS3 y Wireshark.

En el segundo capítulo, se realiza la simulación de cada uno de los escenarios propuestos, en este proyecto se simularán 3 tipos de escenarios: Tipo malla, Tipo estrella y Tipo híbrido; el número de routers variará dependiendo de la validez de los resultados obtenidos.

Se explica también en detalle, todas las características técnicas de cada uno de los dispositivos a utilizar en la simulación.

En el tercer capítulo, se desarrolla un prototipo de red para IPTV, el cual contendrá 2 routers implementados IPv6, un servidor de IPTV y un cliente para acceder al servicio. Para comprobar la validez de los datos se comparará los resultados obtenidos entre la simulación y el prototipo.

Se realiza también la denegación de servicio en la red, con el fin de comprobar los efectos de un flujo de datos diferente a la transmisión de un streaming de video en la red de distribución propuesta, dicha denegación se logra inundando la red con un flujo continuo de cualquier tipo de datos diferente al streaming de video, provocando así alteraciones en la red y por tanto en el cliente.

En el cuarto capítulo se realizan las pruebas y análisis de resultados de la simulación y del prototipo, para realizar las pruebas se utilizará un software libre (Wireshark) para realizar las mediciones de los parámetros involucrados en el acceso al servicio desde el servidor hacia el cliente, tomando en cuenta cada escenario aquí propuesto.

En el quinto capítulo, se da a conocer las conclusiones que se obtuvieron en el desarrollo del proyecto, así como las recomendaciones que pueden ayudar a una mejor comprensión del mismo.

PRESENTACIÓN

Los servicios de comunicaciones y telecomunicaciones en el entorno doméstico, han estado limitado únicamente a la telefonía básica durante mucho tiempo. La inclusión de nuevos servicios en este entorno ha sufrido un intensivo aumento en los últimos años y esto se debe fundamentalmente a que a lo largo de los años se han ido incorporando nuevas y numerosas mejoras técnicas. Las posibilidades que introducen las tecnologías digitales y todas las mejoras incorporadas en las nuevas redes de comunicaciones, facilitan el despliegue de nuevas redes de comunicaciones aptos de proporcionar la capacidad de transmisión necesaria para proporcionar nuevos servicios, tal es el caso de la IPTV.

Actualmente nos enfrentamos a un problema global en el campo de las telecomunicaciones, el agotamiento de direcciones IPv4, este tema no es algo nuevo y en los últimos años, una de las medidas adoptadas ha sido el uso de traductores de direcciones (NAT). Estos traductores de direcciones implican que no es posible la conexión directa extremo a extremo y como consecuencia, solo funcionan correctamente las aplicaciones cliente-servidor, y por tanto Internet se ha convertido en una red mucho más compleja, cara y difícil de gestionar, por tanto la solución para este problema es IPv6, el cual es un sistema de direcciones mucho más escalable, potente y amplio que IPv4. La ventaja más importante de este nuevo sistema es, obviamente, el aumento del número de direcciones disponibles, sin embargo IPv6 posee varias ventajas más que lo hacen aún más aceptado. Gracias al nuevo sistema de empaquetamiento tenemos una mejora en el direccionamiento que nos posibilita crear redes mucho más eficientes; también permite la autoconfiguración de direcciones gracias a mensajes entre los router e incluso podemos realizar muy eficientemente el multicast, que consiste en enviar un paquete a varios destinatarios.

Debido a que experimentar en las redes de comunicaciones con dispositivos como: Routers, Switches, Servidores, etc., reales es muy costoso, se puede recurrir a una alternativa más sencilla y barata, a un simulador de redes de comunicación.

GNS3 es un simulador gráfico de redes, que permite diseñar de manera sencilla redes simples o muy complejas y luego ejecutar sus simulaciones. Es un programa Open Source que trabaja con IOS de routers CISCO reales, agregando todas las potencialidades y características de un router real, por tanto, elimina el problema de comandos no reconocidos o no funcionales. Si bien GNS3 posee varias de las características de los routers reales, GNS3 no pretende reemplazarlos, sino proporcionar una buena herramienta para el aprendizaje en el laboratorio.

Gracias a estas herramientas se ha podido implementar de manera puramente virtual, varios escenarios, en una red de distribución para abordar aspectos básicos del servicio IPTV, como son: velocidad de transmisión, Latencia, Jitter y Pérdida de paquetes; mediante la simulación de una red de distribución implementada en un ambiente simulado a través del programa GNS3, utilizando IPv6 como protocolo de red.

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

1.1 CONCEPTOS IPv6

1.1.1 MOTIVOS PARA IPv6

La organización internacional abierta de normalización IETF (Internet Engineering Task Force), que tiene como objetivos el contribuir a la ingeniería de Internet, ve la necesidad de crear un nuevo protocolo (que en un primer momento se denominó IPng “Internet Protocol Next Generation”, o “Siguiendo Generación del Protocolo Internet”), cuyo principal motivo fue la evidente falta de direcciones:

IPv4 tiene un espacio de direcciones de 32 bits, es decir:

$$2^{32} = 4.294.967.296$$

En cambio, IPv6 nos ofrece un espacio de:

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

Además, IPv6 soluciona o mejora los problemas IPv4.

Las Tecnologías de la Información han evolucionado de un modo mucho más acelerado de lo esperado, debido a esto y a las nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear y añadir nuevos “parches” al protocolo básico.

Entre los “parches” más conocidos, podemos mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

El obstáculo más importante de estas ampliaciones de IPv4, es que utilizar cualquiera de ellos es muy sencillo, pero cuando intentamos usar al mismo tiempo dos “añadidos” se vuelve una tarea complicada, o más bien, se convierte en prácticamente imposible y muy poco práctico el uso simultáneo de tres o más, llegando a ser prácticamente inútil¹.

1.1.2 LA SOLUCIÓN IPv6

La ventaja fundamental de IPv6 es el espacio de direcciones.

La falta de direcciones no se aprecia por igual en todos los puntos de la red, de hecho, en Estados Unidos de América es poco apreciable por el momento. Sin embargo, en zonas geográficas como Asia y Europa, el problema se agrava cada vez más e incluso llega a ser crítica.

Algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los PSI's se ven obligados a delegar tan sólo reducidos números de direcciones IP públicas para sus grandes clientes corporativos².

RTP y RTCP (“Real-time Transport Protocol” y “Real Time Control Protocol”) usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).

La autenticación Kerberos necesita la dirección fuente, que es modificada por NAT en la cabecera IP.

IPsec pierde integridad, debido a que NAT cambia la dirección en la cabecera IP Multicast, aunque es posible, técnicamente, su configuración es tan complicada con NAT, que en la práctica no se emplea³.

¹ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pag.1-

² <http://www.publicaciones.urbe.edu/index.php/telematique/article/viewFile/766/1843>

³ http://www.6sos.org/lista_faqs.php#faq4

1.1.2.1 Características de IPv6

Las características principales por las cuales el protocolo IPv6 se distingue son:

- Mayor espacio de direcciones.
- “Plug & Play”: Autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: Envío de un mismo paquete a un grupo de receptores.
- Anycast: Envío de un paquete a un receptor dentro de un grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del encaminador (router).
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Encaminado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y “multi-homing”, que facilita el cambio de proveedor de servicios.
- Características de movilidad⁴.

NOTA IMPORTANTE: Estas son las características básicas de IPv6, y que la propia estructura del protocolo permite que este crezca, dicho de otra manera, sea escalable, según las nuevas necesidades y aplicaciones o servicios lo vayan requiriendo.

1.1.3 LA BASE DE IPv6

Los criterios para el desarrollo de IPv6 han sido fundamentales para obtener un protocolo sencillo y al mismo tiempo extremadamente consistente y escalable.

⁴ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pag.5-

La cualidad más destacada de IPv6 es la especial habilidad para ser soportado por plataformas existentes, y una evolución que permite su uso concurrente con IPv4. No es necesario realizar un cambio instantáneo en una fecha “X”, sino que el cambio es transparente.

Estos criterios se han alcanzado gracias a la ortogonalidad y simplificación de la cabecera de longitud fija, lo que mejora la eficiencia de su enrutamiento, tanto en pequeños como en los más grandes enrutadores, con soportes de ancho de banda muy superiores a los 100 Gbytes con los dispositivos actuales⁵.

1.1.3.1 Especificaciones básicas de IPv6.

A continuación la descripción de la cabecera de un paquete IPv4:

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño de Cabecera	Tipo de Servicio	Longitud Total	
Indicador			Banderas	Posición de Fragmento
Time to Live		Protocolo	Suma de Control de Cabecera	
Dirección Origen				
Dirección destino				
Opciones				Relleno

Figura 1.1: Cabecera IPv4

La figura 1.1 muestra que la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla admite 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso.

⁵ <http://www.rau.edu.uy/IPv6/queesIPv6.htm>

Ahora, IPv6 realiza algunas innovaciones en algunos campos y anula otros, dando como resultado, de tener 12 campos en IPv4, a tan solo 8 en IPv6.

El motivo principal por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 se facilita la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.).

El campo de "Fragmentación", es diferente. En IPv6 los enrutadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo.

Algunos de los campos son renombrados:

- Longitud total longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
- Protocolo siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los enrutadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
- Tiempo de vida límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

- Clase de Tráfico (Traffic Class), también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- Etiqueta de Flujo (Flow Label), para permitir tráfico con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, son los que permiten una de las características principales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios⁶.

Por tanto, la cabecera del paquete IPv6, sería de la siguiente forma:

0-3	4-7	8-15	16-31
Tipo	Clase de tráfico	Etiqueta de flujo	
Tamaño de carga útil		Siguiente Cabecera	Límite de salto
Dirección Origen			
Dirección destino			

Figura 1.2: Cabecera IPv6

La longitud de esta cabecera es de 40 bytes, el doble que la cabecera IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, la longitud fija de la cabecera, facilita el procesado en routers y conmutadores, incluso mediante hardware, lo que implica mayores prestaciones. Los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores de 64 bits, puedan procesar mucho más eficientemente la cabecera IPv6.

El campo “siguiente cabecera”, indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino únicamente en el nodo(s) destino final(es). Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de proceso y examinado “salto a salto” (hop-by-hop).

⁶ <http://docs.oracle.com/cd/E19957-01/820-2981/IPv6-ref-2/index.html>

Por tanto, las cabeceras con información de enrutamiento, fragmentación, opciones de destino, autenticación, encriptación, etc., serán procesadas en el orden riguroso en que aparecen en el paquete.

La Unidad Máxima de Transmisión (MTU) mínimo, debe ser de 1.280 bytes, pero se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se presagia así una optimización de los paquetes y del número de cabeceras, debido al continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.

IPv6 no realiza verificación de errores de la cabecera en tráfico UDP, por tanto, se requiere el empleo de un mecanismo de checksum propio en las capas superiores⁷.

1.1.4 DIRECCIONES Y DIRECCIONAMIENTO EN IPv6

1.1.4.1 Definición de dirección en IPv6

Las direcciones IPv6 son identificadores de un grupo de 128 bits para interfaces y conjuntos de interfaces. Se clasifican en tres tipos:

- Unicast: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el semejante a las direcciones IPv4 actuales.
- Anycast: Identificador para un conjunto de interfaces (comúnmente pertenecen a diferentes nodos). Los paquetes enviados a una estación con dirección anycast es entregado en una (no importa cuál) de las interfaces identificadas con dicha dirección (la más cercana, según las medidas de distancia del protocolo de encaminado). Permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera “cae”.

⁷ <http://docs.oracle.com/cd/E19957-01/820-2981/IPv6-ref-2/index.html>

- Multicast: Identificador para un conjunto de interfaces (generalmente pertenecientes a diferentes nodos). Un paquete enviado a una estación con dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. El objetivo de este tipo de paquetes es para aplicaciones de retransmisión múltiple (broadcast)⁸.

1.1.4.2 Reservas de espacio de direccionamiento en IPv6

En el direccionamiento IPv6, se ha reservado, al rededor del 15%, con el fin permitir una fácil transición (caso del protocolo IPX), como para mecanismos requeridos por el propio protocolo.

Estado	Prefijo (en binario)	Fracción del espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 0010	1/128
No Asignado	0000 0011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	110	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1024
Direcciones Multicast	1111 1111	1/256

Tabla 1.1: Direcciones reservadas en IPv6

⁸ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf>

De esta forma se permite la asignación directa de direcciones de agregación, direcciones locales, y direcciones multicast, con reservas para OSI NSAP e IPX.

El 85% restante queda reservado para futuros requerimientos.

Existe una manera muy fácil de diferenciar las direcciones unicast de las direcciones multicast, esto es, por el valor del octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multicast). En el caso de las direcciones anycast, no hay ninguna diferencia, sintácticamente hablando, y por tanto, son tomadas del espacio de direcciones unicast.

1.1.4.3 Direcciones especiales en IPv6

1.1.4.3.1 Dirección de auto-retorno o Loopback (::1)

Al igual que para el direccionamiento IPV4, la dirección de loopback no puede ser asignada a una interfaz física; se trata de una interfaz “virtual”, en otras palabras, se trata de paquetes que no salen de la máquina que los emite, con el objetivo de confirmar la correcta inicialización del protocolo (dentro de una determinada máquina).

1.1.4.3.2 Dirección no especificada (::)

Nunca debe ser asignada a ningún nodo, ya que se utiliza para indicar que no existe una dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que se está iniciando, antes de que haya aprendido su propia dirección.

1.1.4.3.3 Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>)

Son aquellas direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	16 bits	32 bits
0000....0000	0000	Dirección IPv4

1.1.4.3.4 Representación automática de direcciones IPv4 sobre IPv6 (::

Permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan “direcciones IPv6 mapeadas desde IPv4”.

80 bits	16 bits	32 bits
0000....0000	FFFF	Dirección IPv4

1.1.5 REPRESENTACIÓN DE LAS DIRECCIONES IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

- a) x:x:x:x:x:x:x, donde “x” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo.
- b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPv6.

Las direcciones:

- 2020:0:0:0:5:500:500C:222A (una dirección unicast)
- FF01:0:0:0:0:0:222 (una dirección multicast)
- 0:0:0:0:0:0:1 (la dirección loopback)
- 0:0:0:0:0:0:0 (una dirección no especificada)

Pueden representarse como:

- 2020::5:500:500C:222A (una dirección unicast)
- FF01::222 (una dirección multicast)
- ::1 (la dirección loopback)
- :: (una dirección no especificada)

- c) Una forma alternativa cuando nos encontremos en un entorno mixto IPv4 e IPv6, es $x:x:x:x:x:d:d:d$, donde “x” representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y “d” representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4).

La representación de los prefijos IPv6 se realiza de la siguiente manera:

Dirección-IPv6/longitud-del-prefijo donde:

- Dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas.
- Longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo.

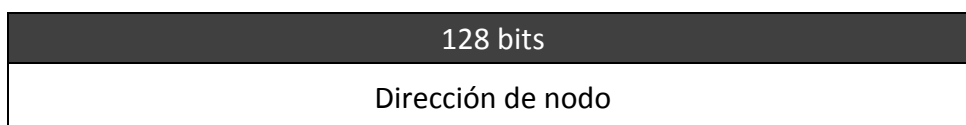
Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

- 22AA:0:0:BB10:123:4567:89AB:CDEF/60

1.1.5.1 Direcciones unicast locales

Las direcciones unicast, son agregables con máscaras de bits contiguos, equivalentes al caso de IPv4, con CIDR (Class-less Interdomain Routing). Hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el corto o largo plazo⁹.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura¹⁰:



⁹ <http://ipv4to6.blogspot.com/p/tipos-de-direcciones-IPv6-unicast.html>

¹⁰ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 15-

Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que está conectado:

n bits	128-n bits
Prefijo de subred	0000000000000000

Los dispositivos de mayor capacidad pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

El “identificador de interfaz” se emplea, para identificar interfaces en un enlace, y deben ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Generalmente, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6¹¹.

Se han definido dos tipos de direcciones unicast de uso local: Local de Enlace (Link-Local) y Local de Sitio (Site-Local).

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers.

Por tanto, los enrutadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local). Tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Se trata de direcciones FE80::<ID de interfaz>/10.

¹¹ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 16-

Las direcciones locales de sitio permiten direccionar los paquetes dentro de un “sitio” local u organización, sin la desventaja de incluir un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los enrutadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea “local de sitio” (su ámbito está limitado a la red local o de la organización).

10 bits	38 bits	16 bits	64 bits
1111111010	0	ID de subred	Identificador de interfaz

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10.

1.1.5.2 Direcciones anycast

Las direcciones anycast tienen el mismo rango de direcciones que las unicast.

Cuando a más de un host se asigna una dirección unicast de interfaz, esta se convierte en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser configurados explícitamente para que reconozcan que se trata de una dirección anycast¹².

Para cada subred existe una dirección anycast requerida, que se denomina “dirección anycast del router de la subred” (subnet-router anycast address)¹³.

Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

n bits	128-n bits
Prefijo de subred	0000000000000000

¹² <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 16-

¹³ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 17-

Todos los routers deben soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la “dirección anycast del router de la subred”, serán enviados a un router (cualquiera) de la subred.

Las aplicaciones de movilidad son dirigidas mayormente a estas características. Por ejemplo, imaginemos nodos que necesitan comunicarse con un router en el conjunto de los disponibles de su subred.

En cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred.

La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred.

Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit “universal/local” igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local)¹⁴.

En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo:

64 bits	57 bits	7 bits
Prefijo de subred	1111110111...111	ID Anycast
Identificador de interfaz		

Con todos los demás casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema:

n bits	121 bits	7 bits
Prefijo de subred	1111111...1111111	ID Anycast
Identificador de interfaz		

¹⁴ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 17-

1.1.5.3 Direcciones multicast

Una dirección multicast en IPv6 se define como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast¹⁵.

Las direcciones multicast tienen el siguiente formato:

8 bits	4 bits	4 bits	112 bits
11111111	000T	Ámbito	Identificador de Grupo

El bit “T” indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones¹⁶.

Los bits “ámbito” tienen los siguientes significados:

0	Reservado
1	Ámbito Local de Nodo
2	Ámbito Local de Enlace
3	No asignado
4	No asignado
5	Ámbito Local de Sitio
6	No asignado
7	No asignado
8	Ámbito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ámbito Global
F	Reservado

Tabla 1.2: Asignación de direcciones en el campo “ámbito” de Multicast IPv6¹⁷

¹⁵ <http://ipv4to6.blogspot.com/p/tipos-de-direcciones-IPv6-multicast.html>

¹⁶ http://lacnic.net/documentos/lacnicx/introduccion_IPv6_v11.pdf -pág. 29-

¹⁷ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> -pág. 18-

El “Identificador de Grupo”, como lo indica su nombre, identifica el grupo de multicast determinado al que se refiere, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si fijamos una dirección multicast permanente, con el identificador de grupo 111 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

- FF01::111 significa todos los NTS en el mismo nodo que el paquete origen
- FF02::111 significa todos los NTS en el mismo enlace que el paquete origen
- FF05::111 significa todos los NTS en el mismo sitio que el paquete origen
- FF0E::111 significa todos los NTS en Internet

Las direcciones multicast no-permanentes o temporales, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local de sitio FF15::101, no tiene relación alguna con un grupo usando la misma dirección en otro lugar, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo¹⁸.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado.

Las principales direcciones multicast reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0.

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited-Node Address”, o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original¹⁹.

Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.

¹⁸ <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 19-

¹⁹ <http://www.rau.edu.uy/IPv6/queesIPv6.htm>

Cada nodo se debe calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

1.1.6 DIRECCIONES REQUERIDAS PARA CUALQUIER NODO

Todos los nodos, en el proceso de identificación, al acoplarse a la red, deben asegurarse de verificar como mínimo las siguientes direcciones:

- Sus direcciones locales de enlace para cada interfaz
- Las direcciones unicast asignadas
- La dirección de loopback
- Las direcciones multicast de todos los nodos
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas
- Las direcciones multicast de todos los grupos a los que dicho host pertenece

Además, en el caso de los routers, tienen que reconocer también:

- La dirección anycast del router de la subnet, para las interfaces en las que está configurado para actuar como router
- Todas las direcciones anycast con las que el router ha sido configurado
- Las direcciones multicast de todos los routers
- Las direcciones multicast de todos los grupos a los que el router pertenece

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

- Dirección no especificada
- Dirección de loopback
- Prefijo de multicast (FF)
- Prefijos de uso local (local de enlace y local de sitio)
- Direcciones multicast predefinidas

Se debe asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

1.1.7 CONCEPTOS DE ENRUTAMIENTO

- Los enrutadores deben saber cómo llegar al punto o destino final de los paquetes que se le reenvían.
- Las rutas estáticas no son adecuadas para redes medianas ni grandes
- Tampoco para las pequeñas si se producen cambios.
- Los protocolos de enrutamiento proporcionan un método automático de generar las tablas de enrutamiento.
- Tienen en cuenta cambio de la topología de red²⁰.

1.1.7.1 Tipos de protocolos de enrutamiento

Por ámbito:

- IGP (Interior Border Gateway)
- EGP (Exterior Border Gateway)

En los de tipo IGP

Por metodología de propagación

- Vector Distancia
- Estado de Enlace

Por tipo de rutas que propagan

- Classful
- Classless

²⁰ http://lacnic.net/documentos/lacnicx/introduccion_IPv6_v11.pdf -pág. 30-

1.1.7.2 Criterios de selección IGP

La selección de uno u otro depende de varios factores:

- Topología de la intranet
- Tipos de rutas a propagar
- Tiempo de convergencia
- Criterio de cálculo de métricas de la ruta.
- Escalabilidad
- Seguridad

	VD	LS	CLASSFUL	CLASSLESS	SEGURIDAD
RIPv1	X		X		
RIPv2	X			X	
IGRP	X		X		
EIGRP	X			X	X
OSPF		X		X	X
IS - IS		X		X	

Tabla 1.3: Tabla comparativa de los protocolos de enrutamiento²¹.

1.1.7.3 Enrutamiento IPv6

- Igual mecanismo CIDR que en IPv4 actual.
- Cambios mínimos respecto a los protocolos existentes
- Cambios mínimos respecto a los protocolos existentes para encaminado en IPv4 (gestión de direcciones mayores)
 - Unicast: RIP, OSPF, IS-IS, BGP4+...
 - Multicast: MOSPF, PIM,...
- Se puede utilizar la cabecera de routing con direcciones
- Se puede utilizar la cabecera de routing con direcciones unicast para encaminar paquetes a través de regiones concretas²².

²¹ http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/Walc2011-Consulintel_IPv6_ES_ROUTING_CHOOF.pdf -pág. 7-

²² <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> -pág. 38-

1.1.7.4 RIP

RIPng para IPv6

Basado en RIPv2, RIPng es muy parecido al usado para IPv4

- Vector distancia, máx. 15 hops, split-horizon, etc.
- Extiende RIPv1 y RIPv2 para soportar
- Direcciones de 128 bits (Next Hop)
- Enrutamiento de prefijos IPv6
- Uso de la dirección FF02::9 del grupo multicast all-RIP-routers, como la dirección destino de los mensajes de update de RIP
- En un entorno de doble-pila, si se usa RIP harán falta dos procesos distintos: RIPv 2 (IPv4) y RIPng (IPv6).²³

1.1.7.5 EIGRP IPv6

- Enhanced Interior Gateway Routing Protocol (EIGRP) desarrollado por Cisco es una versión mejorada del IGRP
- EIGRP usa al igual que IGRP el algoritmo de vector de distancias e información de distancia, además de usar algunas características asociadas normalmente con los protocolos del estado de enlace.
- Las propiedades de convergencia y la eficiencia operativa son mejores en EIGRP que en IGRP
- EIGRP para IPv4 se ejecuta sobre transporte IPv4, comunica solo peers IPv4 y anuncia solo rutas IPv4, mientras que EIGRP para IPv6 hace lo mismo pero para IPv6
- EIGRP para IPv4 y EIGRP para IPv6 se configuran y gestionan de manera separada, aunque la configuración es similar en ambos casos
- EIGRP para IPv6 esta soportado desde las versiones de IOS.²⁴

²³ http://cs.mty.itesm.mx/lab/redes2/IPv6/P6_IPv6_RIPng.pdf

²⁴ http://cs.mty.itesm.mx/lab/redes2/IPv6/P7_IPv6_EIGRP.pdf

1.1.7.6 OSPF

Protocolo de enrutamiento IGP de tipo “link-state” que pretende dar solución a las necesidades más avanzadas de los Sistemas Autónomos más exigentes:

- Soporte VLSM (Variable Length Subnet Masking)
- Autenticación
- Rápida convergencia cuando se producen cambios en la topología de la red
- Propagación de rutas por medio de multicast
- Consideración del ancho de banda en la elección de la mejor ruta

Se divide la red en varias áreas, todas conectadas al área de backbone para una mejor escalabilidad²⁵.

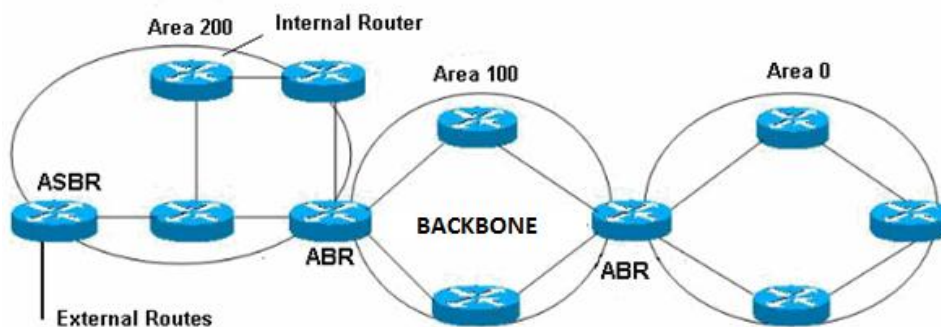


Figura 1.3: Diagrama esquemático del protocolo OSPF.²⁶

OSPF utiliza el protocolo Hello para determinar:

- Qué interfaces recibirán los LSAs
- Qué otros enrutadores vecinos existen
- Si los enrutadores vecinos siguen activos (keepalive)

²⁵ http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/Walc2011-Consulintel_IPv6_ES_ROUTING_CHOOF.pdf -pág. 13-

²⁶ <http://www.simulationexams.com/tutorials/ccna/ospf-routing-fundamentals.htm>

Los enrutadores envían LSAs (Link State Advertisements) a todos los enrutadores de la misma unidad jerárquica a través de una dirección multicast e incluyen entre otros: Prefijo de red, máscara de red, tipo de red, enrutadores conectados, etc.

OSPF versión 3, extiende la versión 2 de OSPF para soportar el enrutamiento de prefijos IPv6 y las direcciones de 128 bits

Nuevas características:

- Se ejecuta directamente sobre IPv6
- Se distribuyen prefijos IPv6
- Nuevos tipos de LSA
- Utiliza direcciones Multicast

Ya que en IPv6 una interfaz de red puede tener una o más direcciones, los LSAs en OSPFv3 difieren de los de la versión 4 para IP.

	LSA	LINK-STATE ID
1	Router LSA	Originating router ID of the router. En IPv6 no tienen información de la red y son independientes del protocolo de red.
2	Network LSA	Interface IP address of the DR. En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red
3	Interarea-prefix LSAs for ABRs	Destination network number. En IPv6 se expresa como prefijo, longitud de prefijo.
4	Interarea-router LSAs for ABRs	Router ID of AS boundary router
5	Autonomous system external LSAs	Redistributing routers from another AS. En IPv6 se expresa como longitud de prefijo y la ruta por defecto, de longitud 0.
8	Link LSA	Local-link flooding scope. Informa de las direcciones link-local de todos los enrutadores del segmento de red
9	Intra-Area-Prefix LSA	Describes association to the router LSA

Tabla 1.4: Tabla de los diferentes LSAs que utiliza el protocolo OSPF²⁷

²⁷ http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/Walc2011-Consulintel_IPv6_ES_ROUTING_CHOOF.pdf -pág. 15-

1.1.7.7 IS-IS

- IS-IS es un protocolo de enrutamiento OSI
- Diseñado para soportar el protocolo CLNP
- Protocolo de la capa de red similar a IP
- Se ha extendido para soportar también IPv4 y IPv6 (RFC5308)

Características

- Enrutamiento jerárquico
- Soporte “classless”
- Uso de direcciones multicast
- Autenticación mediante password
- Soporte de múltiples métricas
- Cálculo SPF local²⁸

Se basa en dos niveles jerárquicos (backbone y stub)

Se envían LSP (Link State Packets)

La información se envía mediante TLVs (Tag / Length / Value)

Se definen dos nuevos TLVs para IPv6:

- IPv6 Reachability
- IPv6 Interface Address

Se define un nuevo identificador de red para IPv6:

- IPv6 NLPID

1.1.7.8 BGP

BGP “Border Gateway Protocol”

- estándar “de facto”

²⁸ <http://www.labs.lacnic.net/drupal/sites/default/files/ospf-isis-IPv6.pdf>

Se basa en el PVP (Path Vector Protocol)

- Similar al vector distancia.
- Cada encaminador frontera envía a sus vecinos (“peerings”) la ruta completa a un destino, no solo la distancia
- El camino (path) es una secuencia de ASs hasta el destino

Sistema Autónomo (AS):

- Conjunto de redes con políticas de enrutamiento comunes
- El mismo protocolo de enrutamiento
- Usualmente bajo el control administrativo de la misma entidad

El enrutamiento en Internet se hace a dos niveles:

- Intra-AS => IGP

La gestión de cada AS es local, lo cual incluye el tipo de protocolo de enrutamiento usado

- Inter-AS => EGP

Requiere una estandarización para que todos los ASs sean alcanzados por todos.

Ejemplo: Path (X,Z)=X, Y1, Y2, Y3, Y5, Z

Se utiliza TCP para el intercambio de mensajes BGP

- OPEN – abre una conexión TCP
- UPDATE – anuncia o confirma un nuevo camino
- KEEPALIVE –en ausencia de UPDATES sirve para mantener abierta la conexión TCP y como ACK de un mensaje OPEN
- NOTIFICATION – informa de errores en mensajes precedentes y para cerrar conexiones²⁹

²⁹ http://www.6deploy.eu/workshops2/20121015_panama_panama/DIA2-1-Consulintel_Curso-IPV6_WALC2012.pdf

1.1.8 MULTICAST

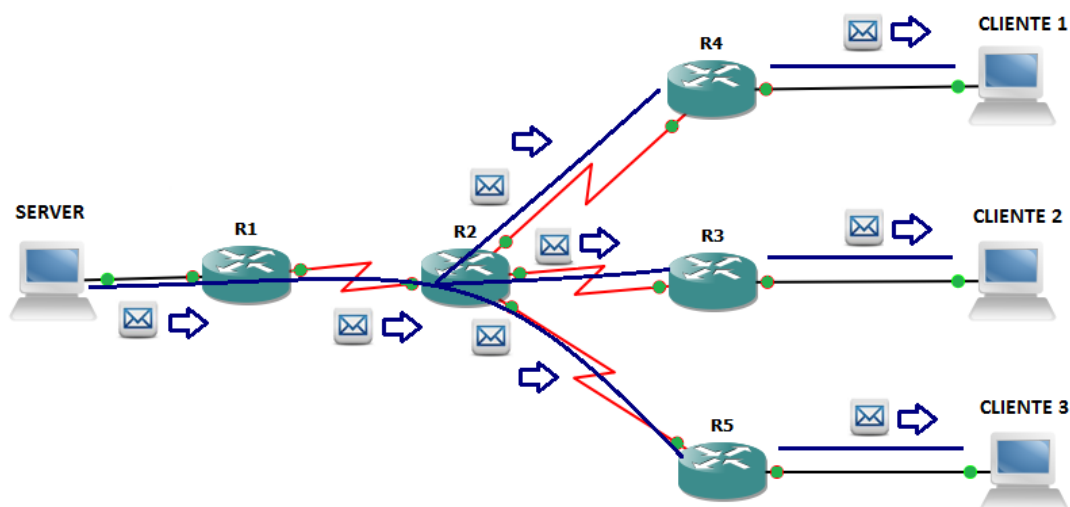


Figura 1.4: Diagrama general de envío de paquetes multicast³⁰

1.1.8.1 Conceptos multicast

La comunicación multicast está compuesta por una fuente y un conjunto de destinatarios y la correspondencia es uno-a-muchos. En este tipo de comunicación, la dirección de la fuente es una dirección unicast, pero la dirección de destino es una dirección de grupo, un grupo de uno o más destinatarios/receptores. La dirección de grupo define a los miembros del grupo, que pueden estar localizados en cualquier sitio en internet o en una red privada. La figura 1.4, muestra esta forma de transmisión de datos.

Un paquete multicast se envía desde la fuente hacia todos los destinatarios que forman parte del grupo. En la comunicación multicast, cuando un enrutador recibe un paquete, puede reenviarlo a través de varias de sus interfaces.³¹

³⁰ http://www.net130.com/CMS/Pub/network/network_protocal/2005_08_21_36977_3.htm

³¹ http://eprints.ucm.es/10051/1/PROYECTO_MII_TREJO.pdf pág. 28

1.1.8.1.1 Multicast Distribution Tree (MDT)

- Es la vía de distribución que se usa para entregar información multicast en las redes que tienen clientes multicast
- Su forma de árbol con el fin de evitar bucles multicast cerrados en la red
- La raíz del MDT es la fuente del grupo multicast

1.1.8.1.2 Shortest Path Tree (SPT)

- Es el MDT que tiene la fuente del grupo multicast como raíz y a los clientes multicast como hojas del árbol
- Se representa como (S,G)

1.1.8.1.3 Shared Tree (ST)

- Es el MDT resultado de tener una única raíz, denominada “Rendezvous Point” cuando hay más de una fuente para el mismo grupo multicast

1.1.8.2 Funcionamiento

- Un nodo se une/abandona un grupo multicast.
- La restricción es nula respecto del número de grupos o del número de miembros por grupo.
- La dirección de destino es una dirección multicast que representa a todo el grupo multicast.
- Enviar paquetes al grupo no significa que se pertenezca a él.
- Los servicios multicast no están orientados a conexión por lo que no se puede emplear TCP³².

³² http://www.6deploy.org/workshops/20101011_santa_cruz_bolivia/multicast-IPv6-walc.pdf -pág. 28-

1.1.8.3 Aplicaciones de multicast

La comunicación multicast puede aprovecharse en diversas situaciones:

- Acceso a base de datos distribuidas.
- Distribución de software y de información.
- Replicación de base de datos.
- Video y audio streaming.
- Servicios de nombre, como DNS.
- Servicios de tiempo.
- Servicios de descubrimiento.
- Educación a distancia.
- Computación distribuida.

1.1.8.4 Protocolo MLD

En IPv4 utilizábamos IGMP, en IPv6 MLD Protocolo para “señalización” entre:

- Router multicast en el enlace local
- Hosts multicast en el enlace local

Un host indica: “Quiero sumarme al grupo FF0E::1234 y comenzar a recibir el flujo de datos”.

MLDv1

- MLD <-> IGMPv2 <-> sólo modelo ASM

MLDv2

- MLDv2 <-> IGMPv3 <-> SSM + ASM
- Mensajes MLD enviados en paquetes ICMPv6

1.1.8.4.1 El paquete MLD

CABECERA IPV6	HOP-by-HOP EXTENSION	MENSAJE MLD
Siguiente cabecera = 0 (Hop-by-Hop)	Opción = Router alert	Mensaje tipo: ICMPv6
	Siguiente cabecera = 58 (ICMPv6)	

Figura 1.5: Paquete MLD

1.1.8.4.2 MLDv2

Las características principales son:

Manejo de grupos y fuentes

- INCLUDE: para recibir paquetes de emisores especificados en el mensaje MLDv2
- EXCLUDE: para recibir de cualquier emisor excepto los especificados en el mensaje MLDv2

2 tipos de mensajes:

- Multicast listener query messages
- Multicast listener report messages

Interoperable con MLDv1

1.1.8.5 PIM Protocol Independent Multicast

Es un protocolo de ruteo multicast inter-dominio. Llamado “independiente” porque usa la tabla de ruteo unicast para RPF, pero es independiente del protocolo de ruteo unicast que se utiliza para armar dicha tabla³³.

³³ http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf -pág. 34-

1.1.8.5.1 PIM-DM – PIM Dense Mode

Variante “densa” de PIM. Trabaja con el método “inundar y cortar” (flood-and-prune) en vez de enviar sólo a donde es requerido.

1.1.8.5.2 PIM-SM – PIM Sparse Mode

Variante “sparse” de PIM. Sólo envía el tráfico dónde se lo solicita.

1.1.8.5.3 RP - Rendezvous Point

Para PIM-SM, es usado para descubrir fuentes de emisión.

1.1.8.5.4 MBGP - Multi Protocol BGP

Es una extensión de BGP para soportar address family multicast.

Permite emplear distintas topologías multicast y unicast.

Usando MBGP se pueden tener peers (pares) que intercambien prefijos unicast y multicast independientemente uno del otro³⁴.

1.1.8.5.5 MSDP - Multicast Source Discovery Protocol

Es utilizado en IPv4 para conectar RPs en diferentes dominios, de tal forma que la información sobre nuevas fuentes de emisión pueda ser distribuida entre los RPs³⁵.

³⁴ http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA5-1-6-Consulintel_Curso-IPv6_WALC2011.pdf

³⁵ http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf -pág. 38-

1.1.8.6 Multicast interdominio

SSM: Los árboles con fuente específica son creados desde los emisores a los receptores cruzando distintos dominios.

ASM: En IPv4 el problema se resolvió utilizando MSDP (Multicast Source Discovery Protocol)

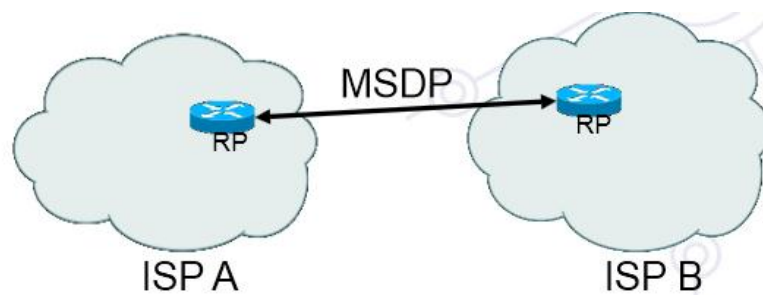


Figura 1.6: Diagrama de protocolo multicast interdominio³⁶

1.1.8.6.1 Embedded-RP

Embedded RP define una política de asignación de la dirección en la que la dirección del RP se codifica en una dirección de grupo multicast IPv6. Lo que facilita una implementación de multicast escalable entre dominios y simplifica la configuración multicast intra-dominio también. Grupo Multicast direcciones IPv6 integrado con RP inicio información con ff70::/12, donde el valor del indicador de 7 significa incrustado RP.

11111111	Flag	Scop	Res	Rpad	Longitud de Prefijo	Prefijo de Red	ID Grupo
8 bits	4 bits	4 bits	4 bits	4 bits	8 bits	64 bits	32 bits

Figura 1.7: Paquete con dirección embedded-RP³⁷

³⁶ http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf -pág. 39-

³⁷ http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf

Flag: 0RPT

- R=1 → Dirección Embedded-RP
- Si R=1 → P=1 → T=1

Prefijo de direcciones FF7x::/16

Res: 0

Rpad: últimos 4 bits de la dirección del RP

E.g. RP address 2001:660:3001:104::8

Dirección multicast: FF7E:0820:2001:660:3001:104:1234:abcd

La información de RP puede ser extraída por los routers de forma automática y utilizarla en la dirección de grupo multicast IPv6, permitiendo un gran número de RPs para ser desplegado en cualquier parte de Internet. Embedded RP no requiere ningún cambio en las opciones del protocolo. Se puede considerar una sustitución automática para la configuración RP estática³⁸.

- El router puede aprender una única dirección RP para un grupo multicast usando RP alojados. No puede soportar redundancia de RP.
- Embedded RP no soporta PIM bidireccional.
- Embedded RP permite la aplicación de establecer qué router es el RP.
- Cabe la posibilidad de que un router de gama baja podría llegar a convertirse en el punto de encuentro de cientos de fuentes de alta velocidad de datos si la aplicación define una dirección equivocada RP (esto se puede evitar mediante la desactivación de Embedded de aprendizaje RP)³⁹.

³⁸http://translate.google.com.ec/translate?hl=es&sl=en&u=http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/whitepaper_c11-508498.html&prev=/search%3Fq%3DEmbedded-RP%26sa%3DX%26tab%3D0%26biw%3D1360%26bih%3D678

³⁹ http://www.6deploy.org/workshops/20101011_santa_cruz_bolivia/multicast-IPv6-walc.pdf

1.2 PARÁMETROS DE CALIDAD DE UNA RED DE DISTRIBUCIÓN

Debido al número de usuarios de las redes, la cantidad de datos transmitida por una red aumenta, así como a la complejidad de los datos transmitidos.

Existen cuatro parámetros para medir la capacidad de transmisión:

- Velocidad de transmisión.
- Latencia
- Jitter
- Pérdida de Paquetes

1.2.1 VELOCIDAD DE TRANSMISIÓN

La velocidad de transmisión o tasa de transferencia se refiere a la velocidad con la cual es posible enviar o transferir información (paquetes), se mide en bits / seg.

- Comúnmente se llama ancho de banda a la capacidad de enviar o transferir información, sin embargo, no es posible conocer los bits / seg si se cuenta solamente con el ancho de banda, ya que se debe considerar la modulación empleada.

La velocidad de transmisión varía dependiendo del concepto al cual se haga referencia:

- Velocidad de transferencia teórica: es la máxima velocidad que se puede lograr considerando el ancho de banda del medio utilizado
- Velocidad de transferencia real: es la velocidad de transferencia tomando en cuenta las limitantes del medio empleado⁴⁰.

⁴⁰ http://www.cs.buap.mx/~iolmos/redes/3_Rendimiento.pdf -pág. 1-

1.2.1.1 Tasa de transferencia teórica en una red Ethernet

No toma en cuenta retardos de transmisión, ruido, etc.

Por ejemplo:

- Tasa de transferencia teórica: 10 Mbps.
- 10 millones de bits por segundo.
- Lo anterior implica que cada 0.1 microsegundos (0.1µs) se transmite un bit.
- Longitud de cada bit: 0.1 µs l medio empleado.

1.2.1.2 Tasa de Transferencia Real

La velocidad es menor a la teórica por varios factores:

- El medio se tiene que multiplexar. La tasa de transferencia real es variable del número de estaciones que compiten.
- Señales de control⁴¹.
- La transferencia real se calcula como:

$$\text{Transferencia real} = \frac{\text{Tamaño de la transferencia}}{\text{Tiempo de la transferencia}}$$

1.2.2 LATENCIA

Se define como la relación del tiempo que toma un bit en recorrer de un extremo de un medio al otro

Depende de tres factores:

- Tiempo de propagación del bit por el medio, que depende del tiempo de propagación de la corriente o luz por el medio, además de la distancia recorrida.

⁴¹ http://www.cs.buap.mx/~iolmos/redes/3_Rendimiento.pdf -pág. 2-

- Máxima cantidad de datos que pueden ser transmitidos por la red sin fraccionarse. Al tiempo de propagación del bit en un paquete se le llama tiempo de transmisión
- Tiempos de espera para transmitir un paquete a través de un conmutador, además del tráfico de la red. A este tiempo se le denomina tiempo de cola.

1.2.2.1 Ecuaciones relacionadas a la latencia

Latencia = Tiempo de propagación + Tiempo de transmisión + Tiempo de cola

$$\text{Tiempo de propagación} = \frac{\textit{distancia a recorrer}}{\textit{velocidad de la luz}}$$

$$\text{Tiempo de transmisión} = \frac{\textit{tamaño del paquete}}{\textit{tasa de transferencia teórica}}$$

1.2.2.2 Latencia y la tasa de transferencia

El producto de la latencia por la tasa de transferencia sirve para determinar el tamaño de los buffers para almacenar datos en los sistemas conectados a una red.

Un correcto cálculo del tamaño de buffer evitará la pérdida de datos al momento de ser transferidos⁴².

1.2.3 JITTER

“Jitter” es un término utilizado en el dominio digital, aún si sus causas y efectos resultantes sean muy parecidos a los de naturaleza análoga.

⁴² http://www.cs.buap.mx/~iolmos/redes/3_Rendimiento.pdf -pág. 4-

La información binaria es transmitida como bits en un flujo de datos de unos y ceros aleatorios.

Idealmente estos bits estarán rigurosamente en un lugar y en un cierto momento y estarán presentes exactamente para un periodo predeterminado.

Sin embargo, habrá niveles altos y bajos uniformes. Desafortunadamente, el mundo real está muy lejos de ser ideal. Por tanto, es esencial tomar en cuenta una variedad y cantidad de componentes influyentes y la calidad de la señal de datos transmitidos que son una fuente de jitter. Comúnmente el Jitter es reconocido como una cantidad de alta frecuencia. El comportamiento del jitter a frecuencias por debajo de 10Hz es llamado "wander" y "drift" aún a frecuencia más bajas.

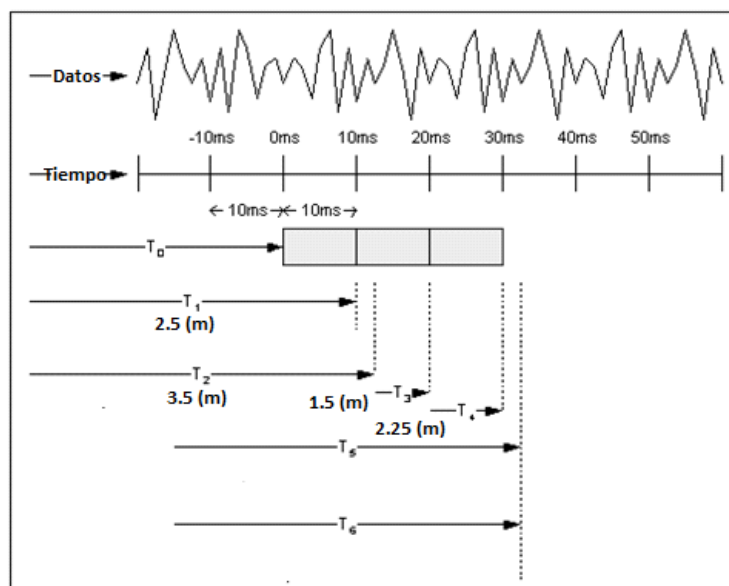


Figura 1.8: Muestra la variación de transmisión de un bit, a esto se conoce como Jitter⁴³

El Jitter cuantifica el efecto del retardo total en la red causado por los paquetes que llegan al receptor. Los paquetes transmitidos a intervalos iguales desde el gateway de la izquierda llegan al gateway de la derecha a intervalos irregulares. El excesivo jitter hace que la voz sea entrecortada y con problemas para entenderse.

⁴³ http://www.eetimes.com/document.asp?doc_id=1277196

El jitter es calculado basado, en el tiempo de llegada entre paquete y paquete de los paquetes exitosos.

Para una alta calidad de voz, el promedio del tiempo de llegada entre los paquetes en el receptor debería ser casi igual a la diferencia entre los paquetes en el transmisor y el estándar de desviación debería ser bajo.

El jitter buffer (el buffer sirve para mantener paquetes entrantes por una determinada cantidad de tiempo) es usado para neutralizar los efectos de las fluctuaciones de la red y crear un fácil flujo de paquetes en la recepción.

Además, es también la variación de tiempo entre los paquetes causada por la red. Para que el jitter sea removido se requiere la recolección y retención de paquetes el tiempo suficiente para que el paquete más lento llegue a tiempo para ser interpretado en la secuencia correcta.

El problema que se genera al querer mezclar el retardo con la supresión del jitter, ha ocasionado la creación varios esquemas para adaptar el tamaño del buffer de jitter a los requerimientos de variaciones de tiempo de la red. Esta adaptación tiene el propósito explícito de minimizar el tamaño y retardo del buffer de jitter mientras que al mismo tiempo previene el sobre flujo del buffer causado por el jitter. Se han hecho dos aproximaciones para adaptar el tamaño del buffer, la selección de la aproximación depende del tipo de red de paquetes usada.⁴⁴

La primera aproximación es medir la variación del nivel de paquetes en el buffer de jitter en una fase de tiempo e incrementalmente adaptar el tamaño del buffer para que coincida con el jitter calculado. Esto funciona mejor con redes que tienen jitter constante en un periodo de tiempo, como las redes ATM.

La segunda aproximación es contabilizar el número de paquetes que llegan tardíamente y crear una relación de estos paquetes al número de paquetes que son procesados exitosamente. Esta relación es usada para ajustar el buffer de jitter a una relación permisible de paquetes tardíos predeterminada. Esto mejora el funcionamiento en redes que tengan intervalos de arribo de paquetes altamente variable, como las redes IP.

⁴⁴ <http://primeraunidad-multimedia.blogspot.com/2009/09/retardo-jitter-latencia.html>

Además de estas técnicas, la red debe estar configurada y gestionada para que tenga retardos y jitter mínimos, permitiendo así un alto QoS.⁴⁵

1.2.4 PÉRDIDA DE PAQUETES.

La pérdida de paquetes se ocasiona en ráfagas o periódicamente debido a una red regularmente congestionada. La pérdida periódica en exceso de 5-10% de todos los paquetes de datos transmitidos puede degradar la calidad del mensaje (voz, datos, video) significativamente. La pérdida ocasional de grupos de paquetes da lugar a hacer difícil la comprensión del mensaje.

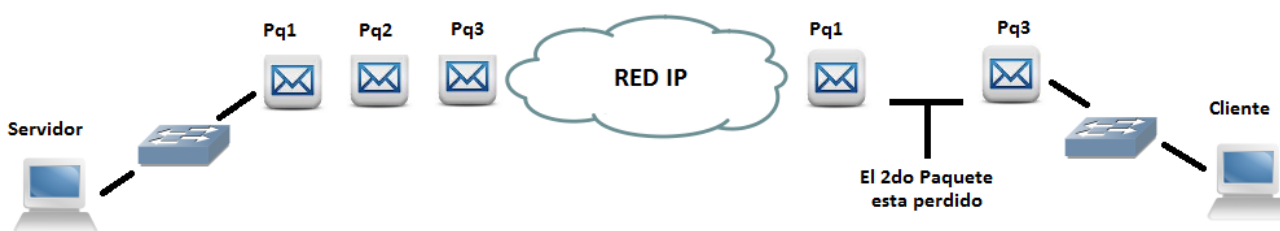


Figura 1.9: Diagrama general de pérdida de paquetes⁴⁶

1.2.4.1 Compensación de pérdida de paquetes

El problema de la pérdida de paquetes puede ser aún mayor dependiendo del tipo de red de paquetes que esté siendo usada. Ya que la red IP no garantiza el servicio, usualmente tiene mayor pérdida de paquetes que las redes ATM. En redes IP actuales, todos los marcos de voz son tratados como datos.

⁴⁵http://noisecom.com/~media/Noisecom/Manuals%20and%20Software/WTG_Intro_to_%20Jitter_SP.ash

x

⁴⁶<http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones3.shtml#ixzz2fHLRWaK>

k

Bajo congestión, los marcos de voz serán descartados al igual que los de datos, con la ventaja que estos últimos no son sensibles al tiempo, y los paquetes descartados pueden ser recuperados con la retransmisión, a diferencia de los paquetes de voz no pueden ser tratados de esta manera.⁴⁷

1.3 IPTV

1.3.1 ¿QUÉ ES IPTV?

“Internet Protocol Television”, trata de la difusión de servicios multimedia como televisión / video / audio a través de redes IP.

IPTV es un modo de emisión de TV más cercano al modelo de negocio de televisiones, por cable y por satélite, es decir, IPTV envuelve la adquisición, procesado y la distribución segura de un contenido sobre una infraestructura IP.

El uso del protocolo IP para la transmisión de vídeo, permite la utilización de los recursos dedicados por operadores para la transmisión de otro tipo de tráfico, lo que evita una gran inversión en equipamiento de red para ésta tarea. Ésta solución a simple vista, no parecería ser la más apropiada, ya que IP no podría proporcionar la calidad necesaria, sin embargo se debe tener en cuenta lo siguiente:

Los elementos de conmutación IP, han crecido en prestaciones, y los convencionales routers que hacían la conmutación de paquetes por software están dejando paso a los llamados conmutadores de nivel 3, que hacen parte de ésta conmutación por hardware.

De la misma manera, han aparecido de forma comercial técnicas que permiten ajustar y garantizar calidades de servicios en redes IP, factor primordial, ya que el tráfico de vídeo es extremadamente sensible a cualquier degradación en las prestaciones de la red.

⁴⁷<http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones3.shtml#ixzz2fHLRWaKk>

Además, al continuar trabajando con IP, el encapsulado de los contenidos se realiza sobre RTP y UDP, utilizando tecnologías IP multicast para su distribución. La ventaja de estas tecnologías es que cada canal de TV se transmite una sola vez y se difunde en todos los puntos de la red donde se dividen los caminos para alcanzar a los distintos usuarios que han sintonizado éste canal. Es decir, permite la comunicación “uno a varios” en redes IP. Así, cada canal multicast es configurado con una dirección IP multicast y para sintonizar un canal cualquiera, nuestro STB sólo debe suscribirse (hacer join) al grupo multicast correspondiente.⁴⁸

1.3.2 VENTAJAS DE IPTV

1.3.2.1 Interactividad

IPTV crea la posibilidad de tener una gran cantidad de nuevos tipos de servicios que anteriormente no estaban disponibles en otras redes. En este caso tanto vídeo como servicios interactivos son transmitidos a través de la red IP facilitando el solapamiento de productos, ya que todo se trasmite en paquetes IP.

Además, un punto a favor es la capacidad de comunicación bidireccional que tiene, permitiendo a los proveedores desarrollar una gran variedad de aplicaciones interactivas en los que no es necesario un desarrollo adicional para obtener el canal de retorno, ya que el usuario dispone de un módem/router con capacidad para comunicarse desde la casa al proveedor.⁴⁹

1.3.2.2 Cambio de tiempo (Time shifting)

Es posible realizar la combinación de IPTV con los grabadores de vídeo, permitiendo una grabación programada de contenidos para una posterior reproducción.

⁴⁸ <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>

⁴⁹ <http://www.ecured.cu/index.php/IPTV>

1.3.2.3 Integración

Provee a muchas empresas/proveedores la opción de ofrecer varios servicios en un sólo paquete integrado lo que reduce costos directos al cliente.

1.3.2.4 Personalización

Un sistema IPTV end-to-end reconoce a cada cliente, una comunicación bidireccional y permite personalizar sus hábitos de consumo de TV permitiéndole decidir qué es lo que quiere ver y cuándo.

1.3.2.5 Bajos requerimientos de ancho de banda

Actualmente se realiza la distribución de todos los canales a cada uno de los usuarios, mientras que la tecnología IPTV permite a los proveedores de servicio servir sólo el stream de vídeo que el usuario ha solicitado. Ésta característica se hace muy atractiva a los operadores ya que permite ahorrar el ancho de banda en su red.⁵⁰

1.3.2.6 Accesible por múltiples dispositivos

Ver IPTV no está limitado al uso del televisor. Los consumidores pueden acceder al servicio a través del PC o de móviles inteligentes.

1.3.2.7 Video bajo demanda

VoD es un elemento interactivo clave de la nueva tecnología IPTV. Nos permite realizar compras de contenidos (películas, documentales, series, etc.) a conveniencia, visualizarlo cuando más nos convenga y realizar sobre él las funciones tradicionales de un reproductor de vídeo, tales como pausar, avanzar, retroceder, etc.⁵¹

⁵⁰ http://www.scielo.org.co/scielo.php?pid=S0123-921X2011000100010&script=sci_arttext

⁵¹ http://aat.inictel-uni.edu.pe/files/AAT-03_Sistema_IPTV_para_Investigacion.pdf

1.3.3 DESVENTAJAS DE IPTV

IPTV ofrece todas las ventajas anteriores mencionadas, convirtiéndolo en un producto muy atractivo, sin embargo, es necesario poner en conocimiento algunos inconvenientes:

1.3.3.1 Pérdida de paquetes

La tecnología que IPTV utiliza es la misma que el acceso a páginas Web, transmisión de datos, para su objetivo. Dado que este protocolo no está orientado a conexión se pueden experimentar en ocasiones pérdida de paquetes o retrasos, imposibilitando ver y escuchar correctamente la TV, en aquellos casos en la que la pérdida de paquetes es considerablemente elevada.

1.3.3.2 Cobertura

La posibilidad que un cliente pueda acceder a un servicio de IPTV, es inversamente proporcional a la distancia a la que se encuentre este cliente con la central. Mientras que en países de Europa como Italia la distancia media no supera los 800 m. en otros países como Francia o España, esta distancia media, supera 2,5 km lo que supone una limitación para que la señal llegue sin pérdidas de paquetes y la IPTV sea una realidad.⁵²

1.3.4 SERVICIOS DE IPTV

Los servicios que se ofrecen tradicionalmente a través de IPTV son dos:

1.3.4.1 Canales de broadcast

El usuario dispone de una gran variedad de canales de televisión/radio digital con una gran calidad y que son ofertados por el operador en forma de paquetes, suscripciones, etc. En este sentido, el operador de IPTV se comporta como cualquier operador de TV por satélite o cable.

⁵² <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>

1.3.4.2 Contenidos bajo demanda (VoD)

Éste es el servicio clave que se distingue de los operadores de satélite o cable. Permite el acceso a un catálogo de contenidos audiovisuales con las mismas prestaciones que si el contenido estuviese disponible en un DVD.

Es decir, el cliente tiene control absoluto sobre la reproducción del programa (parada, avance, retroceso) no es posible compartir el mismo flujo entre múltiples usuarios, por lo que se utilizan las técnicas habituales de unicast (RTP). Lo que obliga en cierta para conseguir la adecuada escalabilidad del sistema medida, a colocar los servidores de VoD en puntos relativamente cercanos a los usuarios.⁵³

1.3.5 ARQUITECTURA IPTV

1.3.5.1 Contribución de señales de vídeo

Se encarga de recibir todas las señales de vídeo, que van a componer la oferta de TV de dicho operador. Esto es lo conocido normalmente como Cabecera de Video (Vídeo Headend) y no se diferencia en absoluto del equipamiento de cualquier otro operador de contenidos de TV tradicionales tales como Operadores de Cable, Operadores de Satélite, etc. Se compone de una etapa de recepción (recepción de canales a través de satélite cable, recepción de contenidos por IP, etc.) en donde se define un Line-Up con los servicios de broadcast TV de la oferta.

Una segunda etapa de codificación en la que se codifica y comprime la señal de video en el estándar establecido (generalmente MPEG-4, H264 que consigue una disminución del ancho de banda en algunos casos a niveles tan bajos como 1,5 Mbit/s por canal). La elección del codec adecuado es vital ya que es determinante al momento de establecer un buen equilibrio entre la calidad de video, la tasa de bit necesaria, la complejidad del algoritmo de codificación/decodificación, la robustez frente a pérdidas de datos y errores y otro gran número de factores.

⁵³ <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>

En esta etapa, también se suele adecuar la señal de vídeo, encapsulándola en IP para que pueda ser transportado y posteriormente entregarla al multiplexor donde se formará el Transport Stream de la oferta total de TV, y así pueda recibir el flujo adecuadamente el abonado.⁵⁴

1.3.5.2 Servidores VoD

Esta etapa se encarga de la recepción de contenidos de formatos diferentes, bien a través de Internet, transferencia de ficheros a un servidor central (FTP), etc. Es en esta etapa y normalmente en un módulo a parte de la cabecera donde estos contenidos son codificados y almacenados en servidores, dejándolos listos para que los clientes accedan a ellos. Dichos servidores pueden estar distribuidos o centralizados en nodos locales donde los usuarios pueden acceder a contenidos específicos en su zona. Normalmente estos servidores están basados en plataformas de servidores IP con sistemas operativos Linux o Windows, los cuales son capaces de entregar a la vez, múltiples flujos de vídeo, aunque para impedir una posible saturación por el aumento de la demanda, se utiliza el balanceo de carga, de modo que se reparten las sesiones de entrega de vídeo.⁵⁵

1.3.5.3 Red de distribución

La red de distribución trata de la red de transporte de alta capacidad que permite la transmisión unidireccional de los contenidos, donde cada uno de los canales está formado por una trama de transporte MPEG-2 encapsulada sobre IP y utilizando el protocolo UDP/multicast.

La disponibilidad de alta capacidad de transferencia es fundamental ya que esto garantiza tener tasas de transmisión estables con la finalidad de ofrecer la suficiente calidad a los clientes.

⁵⁴ <http://www.idolamedia.com/documentos/estudio-IPTV.pdf>

⁵⁵ <http://www.idolamedia.com/documentos/estudio-IPTV.pdf>

La red de transporte siempre es responsable de garantizar el servicio de transporte y es el caballo de batalla de los grandes operadores de telefonía/acceso a Internet ya que continuamente están mejorándola e introduciendo equipamiento nuevo para asegurar esta calidad de servicio.

1.3.5.4 Red de acceso del cliente

La red de Acceso es el punto donde termina la red de transporte del operador y comienza la parte de cliente, no obstante sigue siendo propiedad de la compañía. Generalmente está sobre ADSL2+ o VDSL, gracias a lo cual los clientes pueden recibir los contenidos de TV sobre las líneas de cobre de sus casas (tradicionalmente líneas de teléfono).⁵⁶

1.3.5.5 CPE

Además del par de abonado el cliente necesita el equipamiento de una conexión ADSL normal. Proporciona la terminación de red, y permite separar las conexiones de voz de las de datos. Generalmente, conectado al módem ADSL se encuentra el decodificador, el PC y normalmente también el teléfono.

1.3.5.6 Cliente IPTV

Es el equipo final de cliente donde termina el tráfico IPTV, generalmente es un único dispositivo, conocido como STB, que admite el establecimiento de la conexión, establecer la calidad de servicio con el nodo central, decodifica el vídeo y muestra el contenido en concreto al cliente. Generalmente este cliente o STB, dispone de un software capaz de presentar las funcionalidades del servicio al usuario final, así como aplicaciones interactivas. Normalmente el cliente interactúa con todos los servicios a través del mando a distancia de este STB, convirtiéndose en la puerta de entrada a los servicios que el proveedor le esté ofreciendo.

Este equipo es uno de los más importantes de todo el sistema, que se encuentra al alcance del cliente.

⁵⁶ http://www.scielo.org.co/scielo.php?pid=S0123-921X2011000100010&script=sci_arttext

Tomando en cuenta todos estos puntos y debido al costo de dicho equipo, el objetivo a la hora de seleccionar un equipo u otro por el proveedor, será el de asegurar el cumplimiento de todos los requisitos software y hardware del servicio.⁵⁷

1.4 GNS3

GNS3 es una aplicación realizada en Python que usa las librerías de Dynagen para crear una interfaz gráfica (GUI). Sus funciones principales son editar el archivo de texto .net y realizar las operaciones del CLI hechas por Dynagen y Dynamips. Adicionalmente incorpora la capacidad de simular PCs.

La unión de Dynamips-Dynagen-GNS3, como se observa en la figura 1.10, crea una plataforma que facilita el diseño de topologías de red complejas ya que se realizan tan sólo arrastrando los componentes y dibujando líneas entre routers de forma intuitiva. Por tanto, GNS3 proporciona un ambiente ideal para el adiestramiento con dispositivos de red.



Figura 1.10: Estructura de GNS3

GNS3 se caracteriza por:

- Está disponible de forma gratuita en la página oficial.
- Su instalación es sencilla, ya que todos los programas que necesita para funcionar se encuentran en un solo paquete de instalación.
- Su actualización es constante y periódica, por tanto, se puede encontrar versiones de la aplicación más robustas y con nuevas funcionalidades.

⁵⁷ <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>

- Permite la conexión Telnet a la consola de un router virtual, de forma fácil directamente desde la interfaz gráfica.
- Alternativamente también permite trabajar directamente desde consola de gestión de Dynagen.
- Permite la comunicación entre redes virtuales con redes del mundo real.
- Es adecuado para simular redes de grandes tamaños ya que permite que un cliente GNS3 pueda correr en una máquina diferente a la que contiene al emulador Dynamips, repartiendo el procesamiento entre diferentes PCs.
- Permite la captura de los paquetes que pasan por enlaces virtuales y escribir los resultados de la captura en archivos que pueden ser interpretados por aplicaciones como Wireshark o tcpdumps.
- Los foros de Internet evidencian que es una aplicación ampliamente utilizada.⁵⁸

1.4.1 REQUERIMIENTOS DEL SISTEMA

1.4.1.1 Requerimientos del sistema en Windows XP

1.4.1.1.1 Memoria RAM:

Dynamips asigna por defecto 16MB de memoria RAM al compilador JIT para que realice la compilación del código del simulador en sistema Windows. Además, cada imagen IOS de un router real requiere una cantidad determinada de memoria RAM para funcionar correctamente, por lo tanto, inicialmente, la suma de los valores anteriores sería la cantidad de memoria RAM real necesaria para la simulación de un router.

En la práctica este valor es mucho menor debido a que Dynamips implementa herramientas que permiten una optimización del uso de la memoria del simulador.

⁵⁸http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf

1.4.1.1.2 CPU

En un principio, Dynamips usará mucha cantidad de CPU porque no sabe cuándo el CPU virtual del router está inactivo, por lo tanto, ejecuta todas las instrucciones de las rutinas de inactividad de la IOS como si fueran instrucciones que realizan un trabajo real.

El cálculo del valor de IDLE-PC hará que el consumo de CPU del emulador baje drásticamente. Si se elige un buen valor, la utilización de CPU por cada router será baja con lo cual el funcionamiento de del emulador sea óptimo.

1.4.1.1.3 Disco

Se necesita 39,65 MB de espacio de disco para almacenar a la aplicación GNS3 y a sus dependencias y emuladores asociados. Además se necesita 0,19 MB para almacenar WinPCAP, lo que hace un aproximado de 40 MB de disco necesario.

Este factor no es determinante al momento de elegir un buen host donde montar nuestra red virtual debido a que para la mayoría de PCs estos valores resulta fácilmente alcanzable.

Para poder estimar las capacidades recomendables para el buen funcionamiento de un equipo emulador, haremos un análisis comparativo donde se refleje el consumo de recursos cuando se emulen ciertos números de routers en equipos con características de procesamiento diferentes.

La tabla 1.5, y la figura 1.11, muestran las características del escenario usado para la prueba y los resultados finales obtenidos en 2 emuladores diferentes.



CARACTERISTICAS PC	
Sistema Operativo	Windows XP
RAM	0,99 GB
Procesador	Intel®
CPU	1,66 Ghz.
Plataforma	c2621
IOS	c2600-i-mz-123-3h
IOS RAM	48 MB
Valor IDLE-PC	0x80501884

Tabla 1.5: Características del PC donde se realizó las pruebas

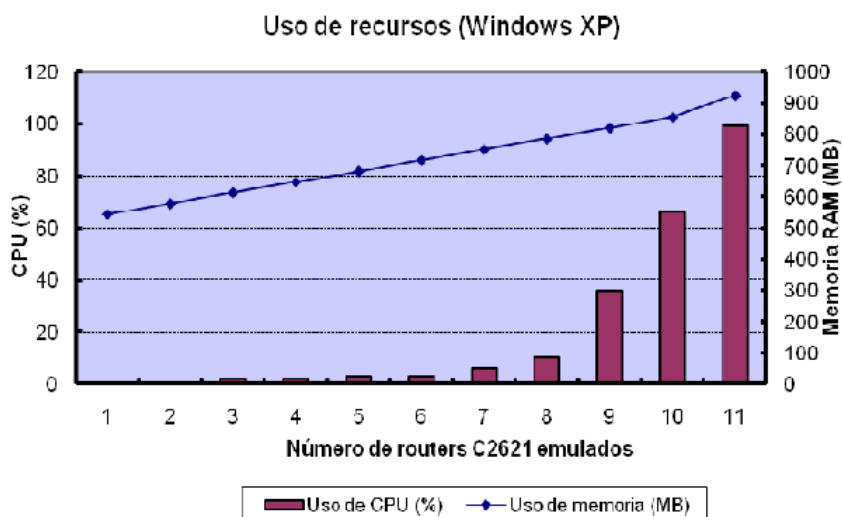


Figura 1.11: Muestra la utilización de CPU y Memoria RAM a medida que aumentan los routers en el simulador⁵⁹

Referente al comportamiento de GNS3 durante la prueba es importante mencionar que, pese a que la utilización de CPU parece que ha sido mínima durante gran parte de la prueba, esto no ha sido así, cada vez que se añadía un router o se abría una ventana de Telnet, la utilización de CPU subía de forma abrupta y fluctuaba por unos instantes, después se estabilizaba y descendía a valores mínimos nuevamente.

⁵⁹ <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>

Cabe señalar que todas las pruebas fueron realizadas cuando el emulador sólo tenía corriendo la aplicación GNS3 y el monitor de sistema de Windows para efectuar las mediciones. Además los routers no tenían ninguna configuración.

1.4.1.2 Requerimientos del sistema en Linux (Ubuntu 9.4)

1.4.1.2.1 Memoria RAM

En Linux, la memoria RAM requerida teórica para la emulación de un router sería la que Dynamips asigna por defecto al compilador JIT (64MB) y la cantidad de RAM que cada imagen IOS requiere para funcionar en un equipo real, aunque, como ya hemos explicado, en la práctica se necesitan valores inferiores.

1.4.1.2.2 CPU

En Linux también se toma en cuenta el valor de IDLE-PC para estimar los requerimientos de CPU del emulador.

1.4.1.2.3 Disco

El espacio total necesario en disco para la instalación de GNS3 en Linux es de aproximadamente 117,2MB, valor que es mayor al requerido en Windows debido a la necesidad de instalación adicional de dependencias. Este parámetro no es determinante al momento de elegir un buen host de trabajo.

Repetimos las mismas pruebas realizadas en el apartado anterior con dos equipos de características de procesamiento diferentes. La tabla 1.6, y la figura 1.12, muestran los resultados obtenidos.⁶⁰

⁶⁰ http://upcommons.upc.edu/pfc/bitstream/2099.1/9989/1/PFC_Lisset_D%C3%ADaz.pdf



CARACTERISTICAS PC	
Sistema Operativo	Ubuntu 9.10
RAM	1.2 GB
Procesador	Intel®
CPU	1,86 Ghz
Plataforma	c2621
IOS	c2600-i-mz-123-3h
IOS RAM	48 MB
Valor IDLE-PC	0x80501884

Tabla 1.6: Características del PC donde se realizó las pruebas

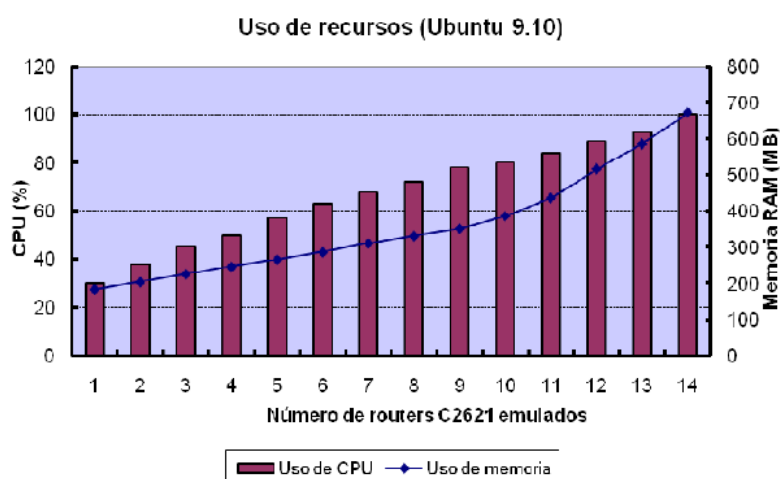


Figura 1.12: Muestra la utilización de CPU y Memoria RAM a medida que aumentan los routers en el simulador⁶¹

⁶¹ <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>

1.4.2 ARQUITECTURA DEL EMULADOR

1.4.2.1 Dynamips

Dynamips es el motor de emulación que permite emular diferentes plataformas hardware usando imágenes de sistemas operativos de CISCO en un mismo host.

Entre dichas plataformas se encuentran los Routers 1700, 2600, 3600, 3700 y 7200. También, puede emular switches Ethernet, Frame-Relay y ATM con funcionalidades básicas.

En cuando a la emulación de switches, Dynamips no es capaz de emular switches Catalyst sino que provee una versión limitada de un switch virtual, cuyas limitaciones pueden ser resueltas usando métodos alternativos como la emulación de NM-16ESW que el emulador sí soporta. Por otro lado, Dynamips tampoco es capaz de emular Firewalls PIX, para ello se usa el emulador PEMU a través de Dynagen.

Inicialmente Dynamips consume grandes cantidades de CPU del PC emulador, esto se debe esencialmente a que realiza la emulación de los routers instrucción por instrucción y a que no puede saber cuándo un router virtual está inactivo, de modo que ejecuta instrucciones como si la imagen del IOS estuviera realizando algún trabajo útil.

Dynamips también consume memoria RAM del PC emulador, ya que, en teoría cada router virtual debe tener a su disposición, como mínimo, toda la cantidad de memoria RAM que necesita para poder trabajar, por lo tanto, esta cantidad se hace impráctica si se requieren emular redes con varios routers. Para resolver el problema del excesivo uso de memoria del PC emulador se usan herramientas que permiten compartir la memoria del mismo entre varios routers emulados con la misma IOS, y herramientas que usan el disco en vez de la memoria del emulador.⁶²

⁶² http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf

1.4.2.2 IDLE-PC

Se trata de una herramienta que realiza un análisis en el código de una imagen IOS para determinar los puntos más probables que representen un bucle de inactividad, de modo que, cuando se detecten, haga que los routers virtuales “duerman” durante ese instante. Es decir, IDLE-PC ayuda a Dynamips a emular el estado inactivo de la CPU virtual de un router.

Algunas características adicionales de este proceso son las siguientes:

- La aplicación de un mal valor de IDLE-PC hace que la PC del emulador trabaje entre 60% - 100% cuando emula un solo un router, mientras que un buen valor hace que sólo trabaje entre 1% -10% de la capacidad. Estos valores dependen de lo potente que sea el emulador usado.
- Está ligado a la versión de Dynamips que se usa, si se cambia de versión, es muy probable que se necesita cambiar de valor de IDLE-PC.
- Será diferente para IOS de diferentes versiones y por supuesto para diferentes plataformas. Se aplicará a un router virtual cada vez que use esa IOS.
- No son exclusivos de un PC o sistema operativo, por lo tanto, los archivos “dynagenidledb.ini” pueden ser copiados y compartidos y el valor de seguirá siendo bueno.⁶³

1.4.2.3 Herramientas de optimización del uso de memoria

Las herramientas que Dynamips usa para optimizar el uso de memoria, tanto real como virtual, del host emulador son las siguientes:

1.4.2.3.1 *Ghostios*

Se encarga de reducir la cantidad de memoria real que se necesita del emulador para crear topologías con routers que corran a la vez, es decir, permite que el emulador comparta una parte de su memoria entre todos los routers que usen una misma imagen IOS de modo que cada router emulado no tenga que almacenar

⁶³ http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf

una copia idéntica de un mismo IOS en su memoria virtual. El resultado, en nuestro caso, es un archivo que contiene la región de memoria compartida ubicado en el directorio “working”, llamado c2600-i-mz.123-3h.image.ghost.

1.4.2.3.2 Sparsemem

Se encarga de reducir la cantidad de memoria virtual que usa un router emulado, es decir, la memoria necesaria para la ejecución de una IOS, ya que sólo asigna la cantidad de memoria que la IOS va a usar en un momento determinado y no toda la memoria RAM configurada, lo que permite crear más routers virtuales por proceso dynamips. Esta herramienta no está habilitada por defecto.

1.4.2.3.3 Mmap

Realiza la correspondencia de archivos temporales del disco con la memoria virtual configurada en los routers emulados, para que cuando se requiera leer estos archivos, el sistema operativo ponga en caché sólo las secciones de los mismos que están siendo utilizados. Estos archivos tienen la extensión “ram”.

1.4.2.4 Dynagen

Dynagen es una interfaz escrita en Python que provee la gestión, mediante línea de comando (CLI), de las plataformas emuladas por Dynamips haciendo más fácil su uso. Usa el modo “Hypervisor” para comunicarse con Dynamips y ambas pueden correr en la misma o en diferente PC. También simplifica la gestión de las redes virtuales ya que implementa comandos para listar, iniciar, parar, reiniciar, suspender, reanudar los diferentes dispositivos emulados, además determina los valores de IDLEPC y realiza capturas de paquetes.⁶⁴

A partir de sus últimas versiones, Dynagen es capaz de trabajar con el emulador de firewalls PEMU, el cual viene integrado en GNS3 dotando al emulador de capacidad de añadir Firewalls CISCO en las topologías.

⁶⁴ <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>

Además es capaz de conectar de forma transparente a Dynamips los diferentes dispositivos virtuales como switches Ethernet, Frame-Relay y ATM soportados por Dynamips.

Dynagen usa un archivo de texto de fácil interpretación llamado "Network File", con extensión ".net", para conocer todas las características de hardware de los dispositivos de red a emular y realizar las interconexiones entre ellos.

1.4.2.5 Network File

Se trata de un archivo, escrito usando sintaxis INI (INI file syntax), que almacena la configuración de todos los dispositivos de red de la topología virtual a simular, como son los routers, switches y las interconexiones entre ellos. Este archivo puede especificar valores tan concretos como los descriptores de los adaptadores de red (NIO) que se encargan de la conexión con equipos reales o los puertos en los que trabajan dichos adaptadores de red de red, etc.⁶⁵

1.5 WIRESHARK

1.5.1 ANALIZADOR DE RED

Un programa es considerado un analizador de red, cuando se utiliza para:

- La conversión de los paquetes datos binarios a un formato legible
- Resolución de problemas en la red
- Analizar el rendimiento de una red para descubrir cuellos de botella
- Detección de intrusos en una red
- Registro de tráfico de red para la argumentación y las pruebas
- El análisis de las operaciones de las aplicaciones
- El descubrimiento de tarjetas de red defectuosas
- Descubrir el origen de los brotes de virus o de denegación de servicio (DoS)
- Validar el cumplimiento de las políticas de seguridad de la empresa
- Como un recurso educativo en el aprendizaje acerca de los protocolos

⁶⁵ http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf

1.5.2 EVALUACIÓN DE UN ANALIZADOR DE PAQUETES

Un analizador de paquetes debe tener en cuenta una serie de factores al seleccionar un sniffer de paquetes, incluyendo los siguientes:

Todos los protocolos soportados para capturar paquetes de datos pueden interpretar los distintos protocolos.

Aunque un analizador de paquetes puede interpretar protocolos de red comunes como por ejemplo, IPv4 e ICMP, la capa de transporte protocolos como TCP y UDP, y protocolos de la capa de aplicación como DNS y HTTP, debe ser capaz de soportar protocolos nuevos como el IPv6, SMBv2 y SIP.

El programa debe ajustarse al nivel de experiencia del usuario. Es decir, si se tiene muy poca experiencia en análisis de paquetes, sería más conveniente evitar un programa de línea de comandos sniffers más avanzados como tcpdump.

Soporte para programas incluso después de haber dominado los fundamentos de un programa de sniffing, Se puede necesitar ayuda para resolver nuevos problemas, buscar documentación para desarrolladores, foros públicos y listas de correo.

Un programa analizador de paquetes debe soportar todos los sistemas operativos.⁶⁶

1.5.3 VENTAJAS WIRESHARK

Wireshark es un analizador de protocolos *open-source* diseñado por Gerald Combs y que actualmente está disponible para múltiple plataformas. Inicialmente conocido como Ethereal, fue creado con el objetivo de analizar el tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.

⁶⁶ <http://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/>

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para más de 1100 protocolos y una interfaz simple e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark “entiende” la estructura de los protocolos, se puede visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proveyendo un gran abanico de posibilidades al administrador de redes al momento de realizar las tareas de análisis de tráfico.⁶⁷

1.5.4 MARCO CONCEPTUAL

Wireshark es un analizador de paquetes de red. Un analizador de paquetes de red captura los paquetes de datos y tratara de mostrar los paquetes lo más detallado posible, es decir, tratará de examinar lo que está pasando en el interior de un cable de red.

1.5.4.1 Paquete de datos

La unidad fundamental de transporte de información es el paquete de datos en todas las redes de computadoras modernas.

Un paquete está compuesto de tres elementos: una cabecera que contiene la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos que contiene los datos que se desean trasladar, y la cola, donde se incluye un código de detección de errores.⁶⁸

1.5.4.2 Red

Una red de computadores, está formado por dispositivos o equipos informáticos conectados entre ellos por medio de dispositivos físicos o inalámbricos, creada con el propósito de transportar datos para compartir información y recursos.⁶⁹

⁶⁷ www.inteco.es/file/5j9r8LaoJvwuB2ZrJ-Xl7g

⁶⁸ http://es.wikipedia.org/wiki/Paquete_de_datos

⁶⁹ http://es.wikipedia.org/wiki/Red_de_computadoras

1.5.4.3 Protocolos

Las redes actuales se conforman de una gran variedad de sistemas que se ejecutan en diferentes plataformas. Para poder realizar la comunicación entre ellos de una forma sencilla, se utiliza un conjunto de lenguajes comunes llamados protocolos.

- Protocolo de Control de Transmisión (TCP),
- Protocolo de Internet (IP),
- Address Resolution Protocol (ARP),
- Dynamic Host Configuration Protocol (DHCP).

Un protocolo puede ser muy simple o muy complejo, dependiendo de su función.

1.5.4.4 Programas empaquetados con Wireshark

Wireshark viene con una interfaz gráfica de usuario (GUI).

Al momento de la instalación, Wireshark también contiene otros programas de apoyo: la versión de línea de comandos de Wireshark, llamado tshark, y otros cinco programas para ayudarle en la manipulación, la evaluación y la creación de archivos de captura.

- Tshark
- editcap,
- mergecap,
- capinfos,
- Dumpcap.

Estos programas de sustento se pueden utilizar juntos para proveer una manipulación muy potente de los archivos de captura. Estos archivos pueden ser capturados con tshark, editado con editcap y se combinan en un archivo de captura de paquetes individuales con mergecap.⁷⁰

⁷⁰<http://186.42.96.211:8080/jspui/bitstream/123456789/473/1/An%C3%A1lisis%20de%20Captura%20de%20Paquetes%20de%20Datos%20-%20Wireshark.pdf>

CAPÍTULO II

SIMULACIÓN

2.1 EXPLICACION DE LA SIMULACIÓN

Este documento tiene como objetivo, realizar un análisis de los parámetros de calidad involucrados a nivel de red, en una red de distribución con IPv6 como protocolo de red, en un ambiente puramente virtual mediante el uso del simulador GNS3, donde se transmitirá un streaming de video desde un Server VLC para simular una transmisión de IPTV.

Para este fin se debe tomar algunas consideraciones:

- Características del PC donde se va instalar el Servidor, el simulador GNS3, los clientes y el software analizador de redes.
- Sobre qué sistema operativo se trabajará tanto en el servidor, el GNS3 y los clientes.
- Características técnicas del servidor y los clientes a implementar para la simulación.
- Que programa servirá para realizar la emisión de video streaming.
- Que programa servirá para la recepción en los clientes del video streaming.
- Cuáles son las topologías propuestas para realizar las mediciones
- Que routers son escogidos para formar la red de distribución y realizar la simulación en GNS3
- Que versión de IOS deben tener los routers
- Comandos utilizados en los routers
- Explicación de los comandos

2.1.1 CARACTERÍSTICAS TÉCNICAS DEL PC HOST

La elaboración de esta red de distribución, demanda gran cantidad de recursos en un PC, una de las opciones, es dividir la carga en algunas máquinas, separando en un PC el Servidor, en otra los clientes y en otra el simulador GNS3; sin embargo, si bien es una opción accesible, es poco práctica, ya que se debería tener al menos 3 PCs a disposición en todo momento, además el inconveniente que al fallar uno de los PCs se deberá implementar un nuevo.

Para la elaboración de esta red se ha escogido un solo PC, el cual posee características necesarias y suficientes para poder alojar tanto al servidor, clientes, simulador GNS3 y Wireshark.

Las características técnicas del PC son:

CARACTERÍSTICAS PC	
Marca	Toshiba
Sistema Operativo	Windows 7
RAM	8,00 GB
Procesador	Intel® Core i7
CPU	2.3 Ghz
Tipo Sistema	64 bits

Tabla 2.1: Características técnicas del PC.

[View basic information about your computer](#)

Windows edition

Windows 7 Home Premium
 Copyright © 2009 Microsoft Corporation. All rights reserved.
 Service Pack 1
[Get more features with a new edition of Windows 7](#)



System

Manufacturer: TOSHIBA
 Model: Satellite S855
 Rating: Windows Experience Index
 Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz 2.30 GHz
 Installed memory (RAM): 8,00 GB
 System type: 64-bit Operating System

TOSHIBA
 Leading Innovation >>>

Figura 2.1: Captura de pantalla de las características del PC host

2.1.2 SISTEMAS OPERATIVOS A UTILIZAR

Puesto que el PC host donde se alojaran todos los componentes de la red, tiene un sistema operativo Windows 7, es sobre éste que se instalarán todos los programas, máquinas virtuales y simuladores necesarios para la práctica.

2.1.2.1 Sistema Operativo del simulador GNS3

Anteriormente se realizó el análisis de las ventajas y desventajas del GNS3 en los sistemas operativos Windows y Linux, básicamente la utilización de recursos, y comparando las figura 1.11 y figura 1.12, del Capítulo I, se puede observar que la utilización de recursos en el sistema operativo Windows es menor que en Linux, es decir, en Windows se necesita menos recursos que en Linux para funcionar de la misma manera, dejando libre recursos que pueden utilizarse en el resto de complementos de la red.

El simulador GNS3 se instalará sobre el sistema operativo Windows 7, que es el sistema que se encuentra en el host.

La versión del GNS3, será la última versión proporcionada por la página web del simulador (www.gns3.net), hasta la fecha de inicio de este proyecto.

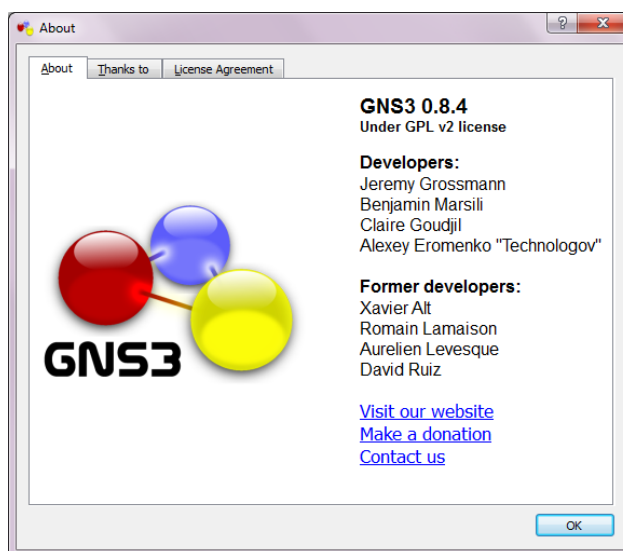


Figura 2.2: Captura de pantalla de la versión de GNS3 utilizada.

Esta versión de GNS3, incorpora el programa Oracle VM Virtual Box, el cual permite instalar máquinas virtuales (sean Windows o Linux) donde se alojaran el servidor y los clientes.



Figura 2.3: Captura de pantalla de la versión de Oracle VM Virtual Box utilizada.

2.1.2.2 Características técnicas y Sistema Operativo del Servidor VLC

Para el servidor de streaming de video, se utilizará el programa gratuito VLC (posteriormente se detalla las ventajas de utilizar este programa), el cual se instalará sobre el sistema operativo Linux, más concretamente sobre la extensión Ubuntu 10.1. Esta extensión fue instalada como máquina virtual en Oracle VM Virtual Box, es decir, el servidor de streaming de video será VLC en Ubuntu 10.1.

Las características técnicas configuradas para el Server VLC son:

CARACTERÍSTICAS SERVER	
Máquina Virtual	Server VLC
Sistema Operativo	Ubuntu 10.1
RAM	1 GB
Procesador	Intel® Core i7
Límite del procesador	100%
CPU	2.3 Ghz
Tipo Sistema	64 bits

Tabla 2.2: Características del PC servidor.

2.1.2.3 Características técnicas y Sistema Operativo de los Clientes

Con el fin de que tanto el Servidor funcione como Cliente, como los Clientes se conviertan en el Servidor, dependiendo de la necesidad de la red, se ha configurado los clientes con las mismas características técnicas que el Server VLC, es decir, todos pueden funcionar como clientes o como servidores.

CARACTERÍSTICAS CLIENTES	
Máquina Virtual	Clientes
Sistema Operativo	Ubuntu 10.1
RAM	1 GB
Procesador	Intel® Core i7
Límite del procesador	100%
CPU	2.3 Ghz
Tipo Sistema	64 bits

Tabla 2.3: Características de los PC Clientes.

2.1.2.4 Programa a utilizar como servidor de streaming y su configuración

El Servidor de IPTV será implementado mediante un servidor de Streaming de video, utilizando para este fin, el reproductor de libre acceso VLC.

2.1.2.4.1 VLC

VLC es multiplataforma (existen versiones para Windows, Linux, Mac, Solaris, FreeBSD, etc.), es de código libre, soporta la gran mayoría de formatos multimedia sin necesidad de codecs y es gratuito.

VLC incorpora la gran ventaja que puede ser configurado como servidor de streaming con características avanzadas como vídeo bajo demanda y transcodificación en tiempo real o que puede leer directamente flujos de vídeo de tarjetas sintonizadoras de satélite, entre otras características.⁷¹

⁷¹ <http://www.visualbeta.es/3009/software-libre/vlc-el-mejor-reproductor-multimedia/>

2.1.2.4.2 Configuración del Servidor VLC

A continuación se muestra la configuración para la emisión de video streaming en el Servidor VLC, la dirección utilizada será la Dirección Embedded-RP FF7E:140:2001:1:1::1.

La emisión del video streaming empieza cuando se reproduce el video con la dirección señalada anteriormente, la difusión se realiza desde el servidor mediante el protocolo RTP / MPEG TRANSPORT STREAM, el cual es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia o en este caso, video streaming en tiempo real.

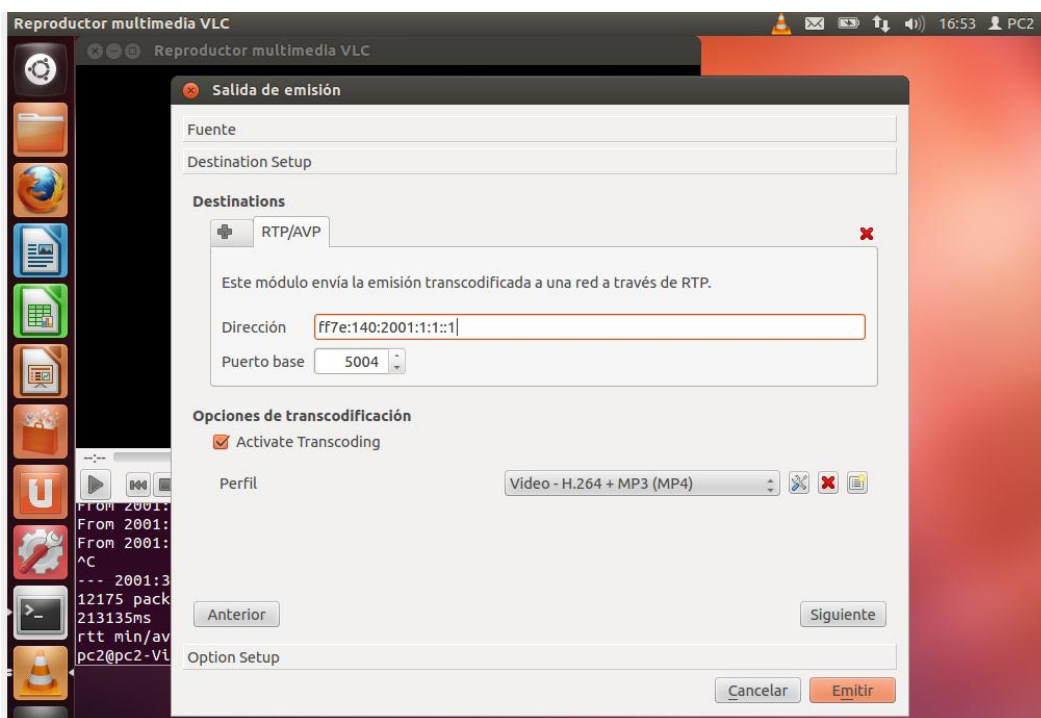


Figura 2.4: Dirección multicast Embedded-RP asignada al streaming de video

La dirección multicast Embedded-RP asignada al streaming de video, fue calculada específicamente para esta red, mediante la forma mencionada anteriormente en este documento. El protocolo por el cual se debe enviar el streaming es RTP y el puerto puede ser cualquiera a partir del 1024, en este caso se escogió el puerto 5004.

2.1.2.4.3 *Protocolo RTP*

RTP se encuentra sobre el transporte UDP/TCP, pero prácticamente sobre UDP. RTP es un protocolo de sesión, pero se encuentra en la aplicación. Es el desarrollador que lo tiene que integrar.

2.1.2.4.4 *Transporte del flujo RTP*

RTP no tiene nada que ver con el tipo de flujo. Se encuentra sobre UDP, que está sobre IP. El tipo de flujo teóricamente se utiliza en IP.

RTP lleva un número de secuencia, una marca de tiempo y un identificador único de la fuente (SSRC).⁷²

Una vez que se ha configurado el Server VLC con la dirección multicast asignada al video streaming, se procede a la emisión del mismo.

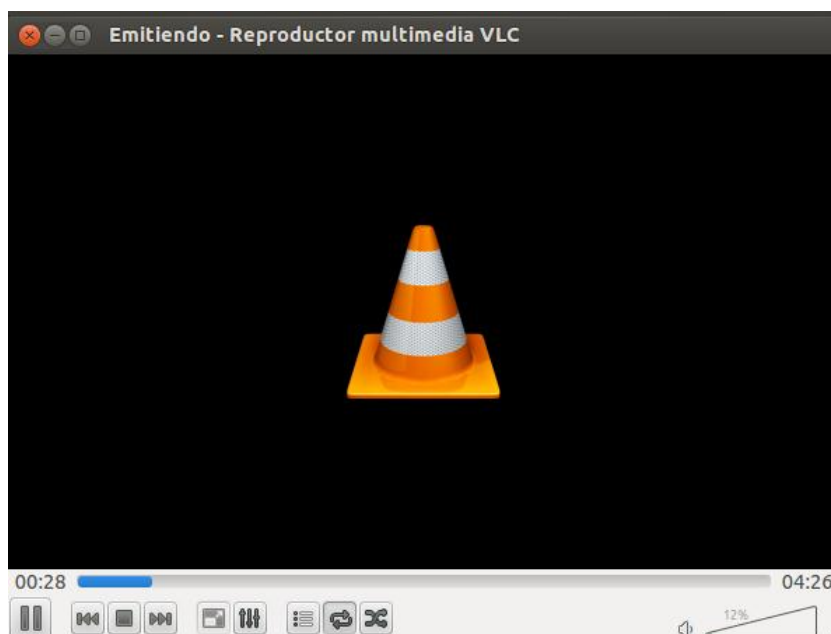


Figura 2.5: VLC emitiendo video a la red

⁷² <http://www.slideshare.net/manuelfloresv/analisis-de-los-protocolos-de-tiempo-real-rtp-rtcp-y-rtsp>

2.1.2.5 Programa a utilizar para recibir el streaming y su configuración.

Gracias a las ventajas mencionadas anteriormente sobre el programa gratuito VLC, se lo ha implementado también en los clientes para recibir la señal de streaming de video, además, esto permite que en todo momento un cliente pueda funcionar como servidor y/o viceversa.

Para captar la señal del streaming de video del Server VLC, en el cliente únicamente se debe abrir la opción de red y añadir la dirección multicast Embedded-RP asignada ha dicho streaming junto con el protocolo y el puerto especificados en el servidor:

- `rtp://[ff7e:140:2001:1:1::1]:5004`

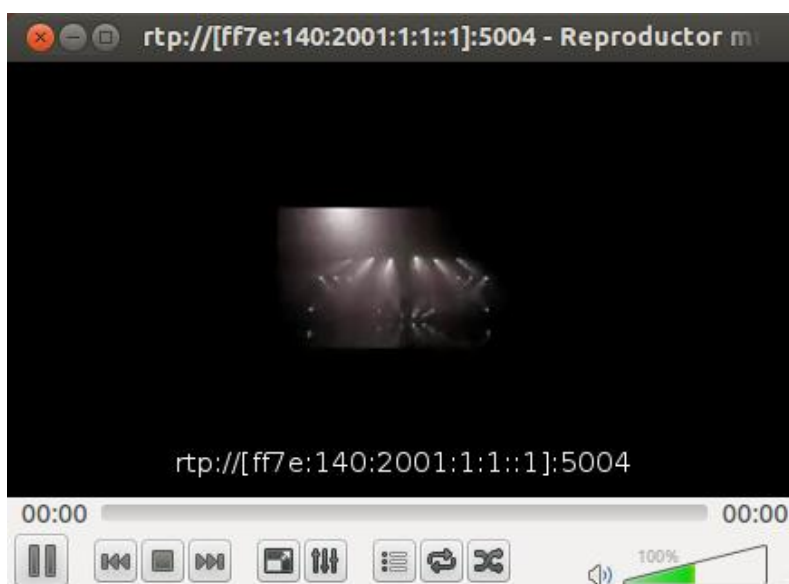


Figura 2.6: Recepción del streaming de video en un cliente

La figura 2.6 muestra la pantalla del VLC una vez que está recibiendo la señal del streaming de video, se puede observar que la dirección por la que tiene acceso al streaming, es la misma puesta en el servidor, también se observa que la señal de video está siendo transmitida por el protocolo RTP y el puerto es el 5004.

2.1.2.6 Topologías propuestas

En las redes de información, existen varios tipos de topologías de red en un ambiente de distribución, en el presente trabajo se propone 3 tipos de topología tomando en cuenta que son las más comúnmente implementadas y las más óptimas para implementar IPTV:

- Topología tipo malla
- Topología tipo estrella
- Topología tipo híbrida.

2.1.2.7 Routers que formarán la red de distribución

En la actualidad se tiene múltiples marcas de routers con la capacidad necesaria para procesar la gran cantidad de información que una red de IPTV necesita, la marca más conocida y familiar es CISCO.

El GNS3 permite implementar únicamente routers CISCO en el simulador, y si bien, hay varias opciones de routers a escoger, para este proyecto se optó por el router CISCO 1751 de la serie c1700.

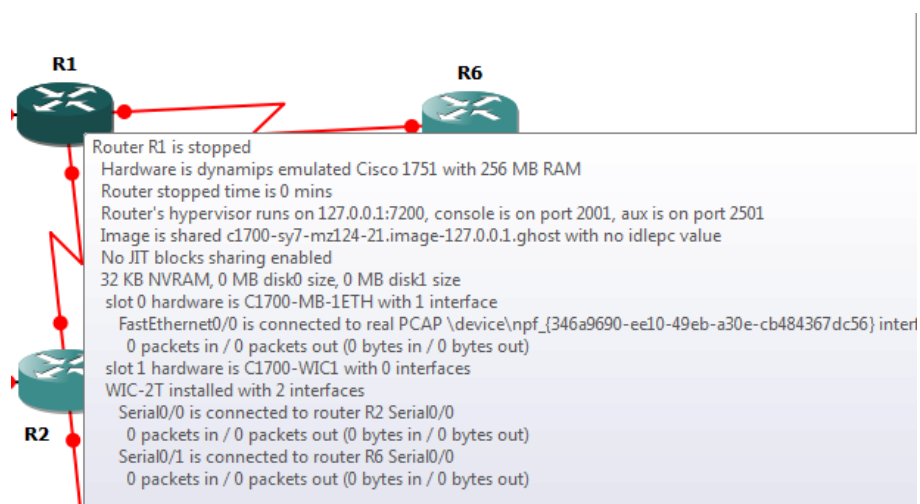


Figura 2.7: Características del router R1 c1751 de la red de distribución.

En internet existe varios sitios donde es posible descargar las IOS para los CISCO c1700, estos IOS funcionan tanto en GNS3 como en los routers físicos. Para esta práctica se debe utilizar la versión de IOS v12.4, ya que las versiones anteriores no permiten ingresar los comandos IPv6 multicast necesarias para la red.

```

R1
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

      cisco Systems, Inc.
      170 West Tasman Drive
      San Jose, California 95134-1706

Cisco IOS Software, C1700 Software (C1700-SY7-M), Version 12.4(21), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Wed 09-Jul-08 23:01 by prod_rel_team

Cisco 1751-V (MPC860T) processor (revision 0x202) with 131072K/16384K bytes of memory.
Processor board ID FTX0945W0MY (4279256517), with hardware revision 0000
MPC860T processor: part number 0, mask 0
 1 FastEthernet interface
 2 Serial(sync/async) interfaces
 32K bytes of NVRAM.
4096K bytes of processor board System flash (Read/Write)

```

Figura 2.8: Versión de router R1 c1751 de la red de distribución

2.1.2.8 Direccionamiento a implementar en routers c1751

Los comandos a implementar en cada uno de los routers son prácticamente los mismos, la única diferencia serán algunos comandos en el router R1 de cada topología, ya que este router, servirá como RP (Rendezvous Point), es decir, será el router distribuidor de la transmisión multicast.

El direccionamiento en cada una de las topologías, está distribuida de una manera fácil e intuitiva, empezando por el primer grupo de 4 caracteres hexadecimales, como una dirección unicast global (2001::) y el resto de grupos hexadecimales, dependerá de la red (router inicio y router destino en dirección de la transmisión del streaming).

Ejemplo:

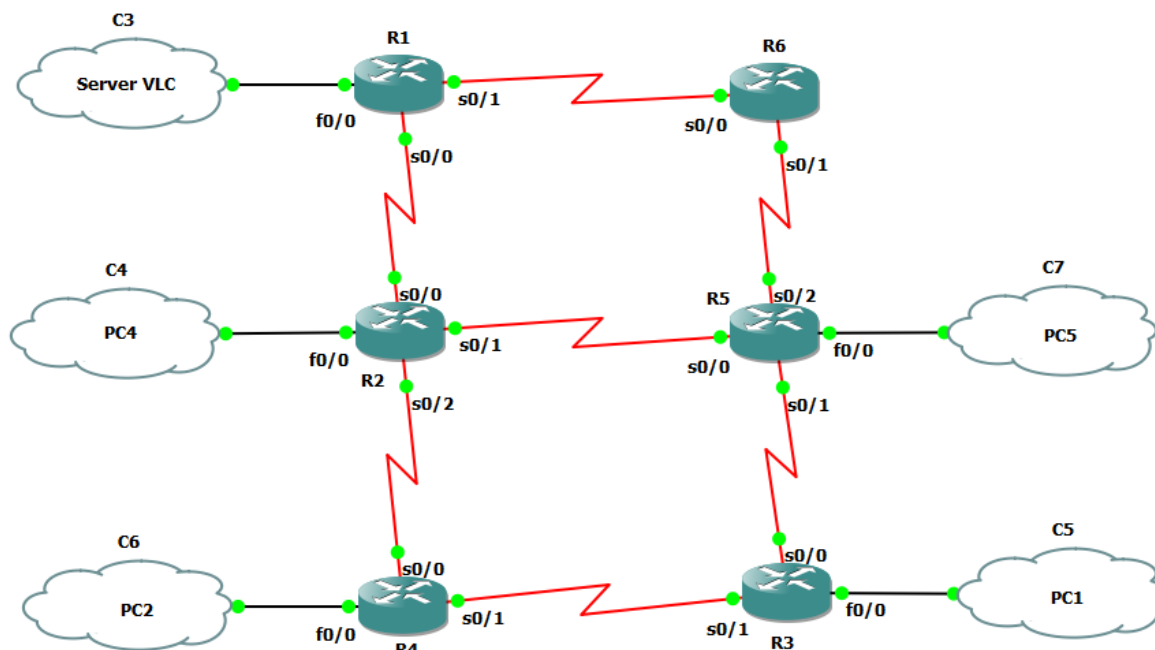


Figura 2.9: Diagrama de la topología tipo malla a implementar

En esta topología tipo malla como muestra la figura 2.9, se tomará como ejemplo al router R1, a este router se encuentran conectados directamente los routers R2 y R6, entonces el direccionamiento será el siguiente:

ROUTER R1	
Serial 0/0	2001:1:2::1/64
Serial 0/1	2001:1:6::1/64
ROUTER R2	
Serial 0/0	2001:1:2::2/64
ROUTER R6	
Serial 0/0	2001:1:6::6/64

Tabla 2.4: Ejemplo de direccionamiento para el router R1.

En la red Router – Router la dirección se compone de 4 grupos hexadecimales:

- a) Primer grupo hexadecimal: 2001:1:2::1/64 (dirección unicast global)
- b) Segundo grupo hexadecimal: es el número del router origen en dirección del streaming: 2001:1:2::1/64 (va de R1 a R2)
- c) Tercer grupo hexadecimal: es el número del router destino en dirección del streaming: 2001:1:2::1/64 (va de R1 a R2)
- d) Último grupo hexadecimal: es el número de router: 2001:1:2::1/64 (R1)

En la red entre Router – PC, el direccionamiento es:

- a) Primer grupo hexadecimal: 2001:1:2::1/64 (dirección unicast global)
- b) Segundo y tercer grupo hexadecimal: es el número del router origen en dirección del streaming: 2001:1:1::1/64 (va de R1 a R2)
- c) Último grupo hexadecimal: para este último grupo se tiene dos parámetros
 - En los routers es el número de router: 2001:1:1::1/64 (R1)
 - En los PCs (servidor o cliente) es el número 10: 2001:1:1::10/64 (Server VLC)

Este direccionamiento se aplica en cada topología propuesta.

2.1.2.9 Comandos a implementar en routers c1751

ROUTER 1	ROUTER 2
Configure terminal	Configure terminal
Interface f0/0	Interface f0/0
IPv6 enable	IPv6 enable
IPv6 address 2001:1:1::1/64	IPv6 address 2001:2:2::2/64
No shut	No shut
Interface s0/0	Interface s0/0
IPv6 enable	IPv6 enable
IPv6 address 2001:1:2::1/64	IPv6 address 2001:1:2::2/64
No shut	No shut
Exit	Exit
IPv6 unicast-routing	IPv6 unicast-routing
IPv6 cef	IPv6 cef
IPv6 router ospf 1	IPv6 router ospf 1
Router-id 1.1.1.1	Router-id 2.2.2.2
Interface f0/0	Interface f0/0
IPv6 ospf 1 area 0	IPv6 ospf 1 area 0
Interface s0/0	Interface s0/0
IPv6 ospf 1 area 0	IPv6 ospf 1 area 0
Exit	Exit
IPv6 multicast-routing	IPv6 multicast-routing
IPv6 pim spt-threshold infinity	IPv6 pim spt-threshold infinity
Exit	Exit
IPv6 access-list ERP	IPv6 access-list ERP
permit IPv6 any ff7e:140:2001:1:1::/96	permit IPv6 any ff7e:140:2001:1:1::/96
exit	Exit
IPv6 pim rp-address 2001:1:1::1 ERP	IPv6 pim rp-address 2001:1:1::1 ERP
end	End
wr	Wr

Tabla 2.5: Comandos a implementar en los routers

2.1.2.10 Explicación de los comandos más importantes

- **IPv6 enable:** Configura automáticamente una dirección local de enlace IPv6 en la interfaz a la vez que habilita a la interfaz para el procesamiento de IPv6. La dirección local de red sólo se puede utilizar para comunicarse con nodos en la misma red.

- **IPv6 address 2001:1:1::1/64:** Asignación de una dirección IPv6 a la interface seleccionada.
- **IPv6 unicast-routing:** Permite el envío de datagramas IPv6 unicast.
- **IPv6 router ospf 1:** Habilita protocolo OSPF como protocolo de enrutamiento.
- **Router-id 1.1.1.1:** Identificación del router para el protocolo OSPF.
- **IPv6 multicast-routing:** Habilita el enrutamiento multicast en todas las interfaces habilitadas para IPv6 y permite el reenvío de multidifusión para PIM y MLD en todas las interfaces habilitadas del enrutador.
- **IPv6 pim spt-threshold infinity:** configura cuando un router PIM se une al SPT para los grupos especificados.
- **IPv6 access-list ERP:** Define una lista de acceso IPv6 y coloca el router en el modo de configuración de lista de acceso IPv6.
- **permit IPv6 any ff7e:140:2001:1:1::/96:** Permite la difusión IPv6 desde y hacia la dirección especificada.
- **IPv6 pim rp-address 2001:1:1::1 ERP:** Configura la dirección de un RP PIM para un rango determinado grupo.

Los comandos implementados en los routers R3, R4, R5 y R6 son los mismos que el router R2, únicamente se debe respetar el direccionamiento establecido.

2.2 TOPOLOGÍAS A IMPLEMENTAR EN GNS3

2.2.1 TOPOLOGÍA TIPO MALLA A IMPLEMENTAR

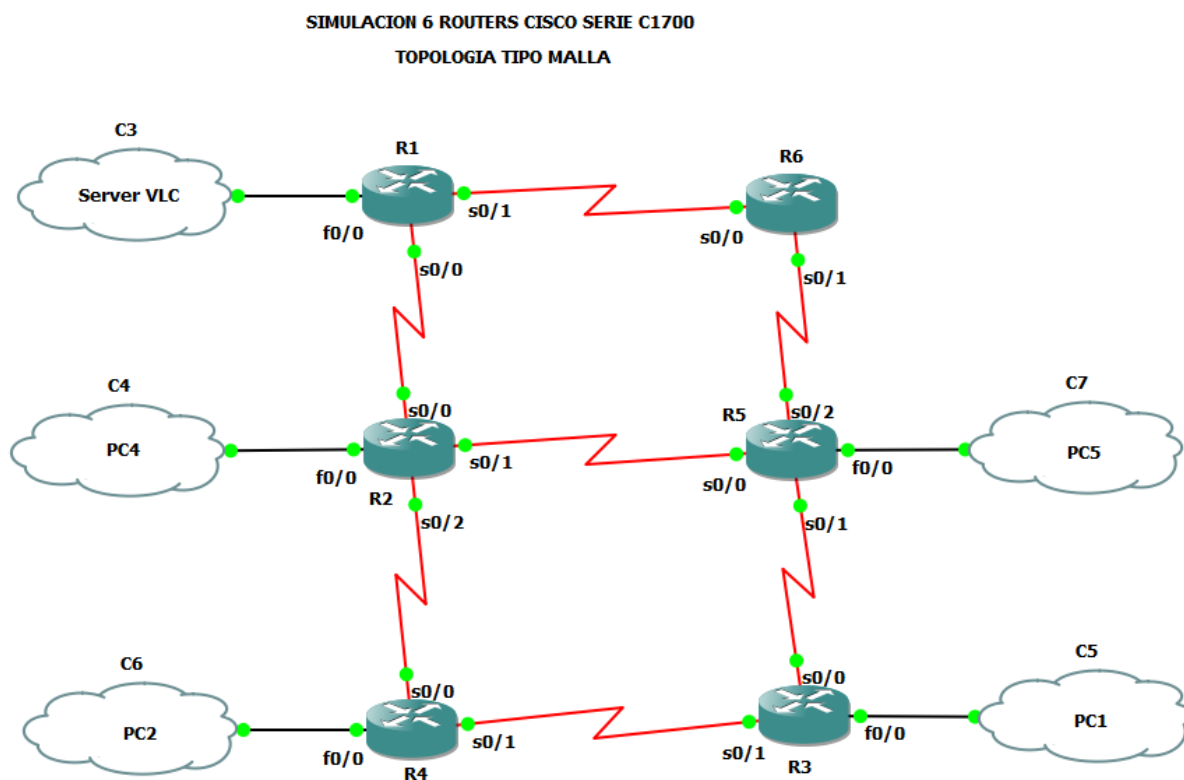


Figura 2.10: Diagrama de la topología tipo malla a implementar

2.2.1.1 Direccionamiento de la topología tipo malla

DISPOSITIVO	DIRECCION IPV6	GATEWAY
Server VLC	2001:1:1::10/64	2001:1:1::1
CLIENTE PC1	2001:3:3::10/64	2001:3:3::3
CLIENTE PC2	2001:4:4::10/64	2001:4:4::4
CLIENTE PC4	2001:2:2::10/64	2001:2:2::2
CLIENTE PC5	2001:5:5::10/64	2001:5:5::5
ROUTER R1		
Fastethernet 0/0	2001:1:1::1/64	
Serial 0/0	2001:1:2::1/64	
Serial 0/1	2001:1:6::1/64	
ROUTER R2		
Fastethernet 0/0	2001:2:2::2/64	
Serial 0/0	2001:1:2::2/64	
Serial 0/1	2001:2:5::2/64	
Serial 0/2	2001:2:4::2/64	
ROUTER R3		
Fastethernet 0/0	2001:3:3::3/64	
Serial 0/0	2001:3:5::3/64	
Serial 0/1	2001:4:3::3/64	
ROUTER R4		
Fastethernet 0/0	2001:4:4::4/64	
Serial 0/0	2001:2:4::4/64	
Serial 0/1	2001:4:3::4/64	
ROUTER R5		
Fastethernet 0/0	2001:5:5::5/64	
Serial 0/0	2001:2:5::5/64	
Serial 0/1	2001:3:5::5/64	
Serial 0/2	2001:5:6::5/64	
ROUTER R6		
Serial 0/0	2001:1:6::6/64	
Serial 0/1	2001:5:6::6/64	
DIRECCIÓN EMBEDDED MULTICAST A UTILIZAR		
Grupo Multicast Embedded	FF07:140:2001:1:1::1	
PROTOCOLO DE ENRUTAMIENTO UTILIZADO		
PROTOCOLO:	OSPFv6	
GRUPO:	1	
AREA:	0	
ROUTERS IMPLEMENTADOS:	Todos los Routers de la red de distribución	
RP SELECCIONADO		
ROUTER:	R1 (Conectado directamente al Server VLC)	

Tabla 2.6: Direccionamiento de la topología tipo malla.

ROUTER 3

```
R3
R3#show running-config
Building configuration...

Current configuration : 1063 bytes
!
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
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
ip cef
no ip domain lookup
ip domain name lab.local
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
!
!
!
!
interface FastEthernet0/0
no ip address
speed auto
ipv6 address 2001:3:3::3/64
ipv6 enable
ipv6 ospf 1 area 0
```

```
R3
interface Serial0/0
no ip address
ipv6 address 2001:3:5::3/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface Serial0/1
no ip address
ipv6 address 2001:4:3::3/64
ipv6 enable
ipv6 ospf 1 area 0
!
ip forward-protocol nd
no ip http server
!
!
!
ipv6 router ospf 1
router-id 3.3.3.3
log-adjacency-changes
!
ipv6 pim spt-threshold infinity
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

R3#
*Mar  1 00:00:32.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
```

ROUTER 4

```
R4
R4#show running-config
Building configuration...

Current configuration : 1063 bytes
!
version 12.4
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
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
ip cef
no ip domain lookup
ip domain name lab.local
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
!
!
!
!
interface FastEthernet0/0
no ip address
speed auto
ipv6 address 2001:4:4::4/64
ipv6 enable
ipv6 ospf 1 area 0
```

```
R4
interface Serial0/0
no ip address
ipv6 address 2001:2:4::4/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface Serial0/1
no ip address
ipv6 address 2001:4:3::4/64
ipv6 enable
ipv6 ospf 1 area 0
!
ip forward-protocol nd
no ip http server
!
!
!
ipv6 router ospf 1
router-id 4.4.4.4
log-adjacency-changes
!
ipv6 pim spt-threshold infinity
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

R4#
*Mar  1 00:00:32.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
```

ROUTER 5

```
R5
R5#show running-config
Building configuration...

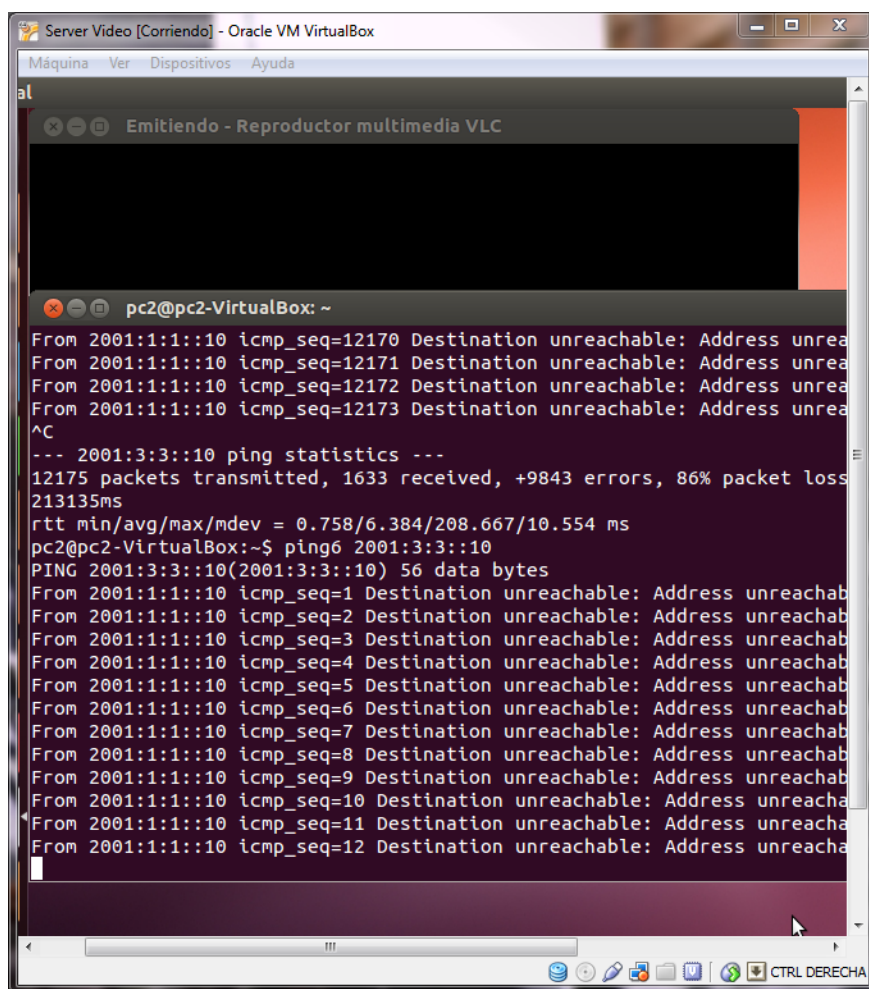
Current configuration : 1209 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
ip cef
no ip domain lookup
ip domain name lab.local
ipv6 unicast-routing
ipv6 cef
ipv6 multicast-routing
!
!
!
!
!
interface FastEthernet0/0
no ip address
speed auto
ipv6 address 2001:5:5::5/64
ipv6 enable
ipv6 ospf 1 area 0
```

```
R5
interface Serial0/0
no ip address
ipv6 address 2001:2:5::5/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface Serial0/1
no ip address
ipv6 address 2001:3:5::5/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface Serial1/0
no ip address
ipv6 address 2001:5:6::5/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface Serial1/1
no ip address
shutdown
!
ip forward-protocol nd
no ip http server
!
!
!
!
!
ipv6 router ospf 1
router-id 5.5.5.5
log-adjacency-changes
!
ipv6 pim spt-threshold infinity
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
```


2.2.1.3 Capturas de pantalla de la red

Una vez que se ha configurado el Server VLC con la dirección multicast asignada al video streaming, se procede a la emisión del mismo.

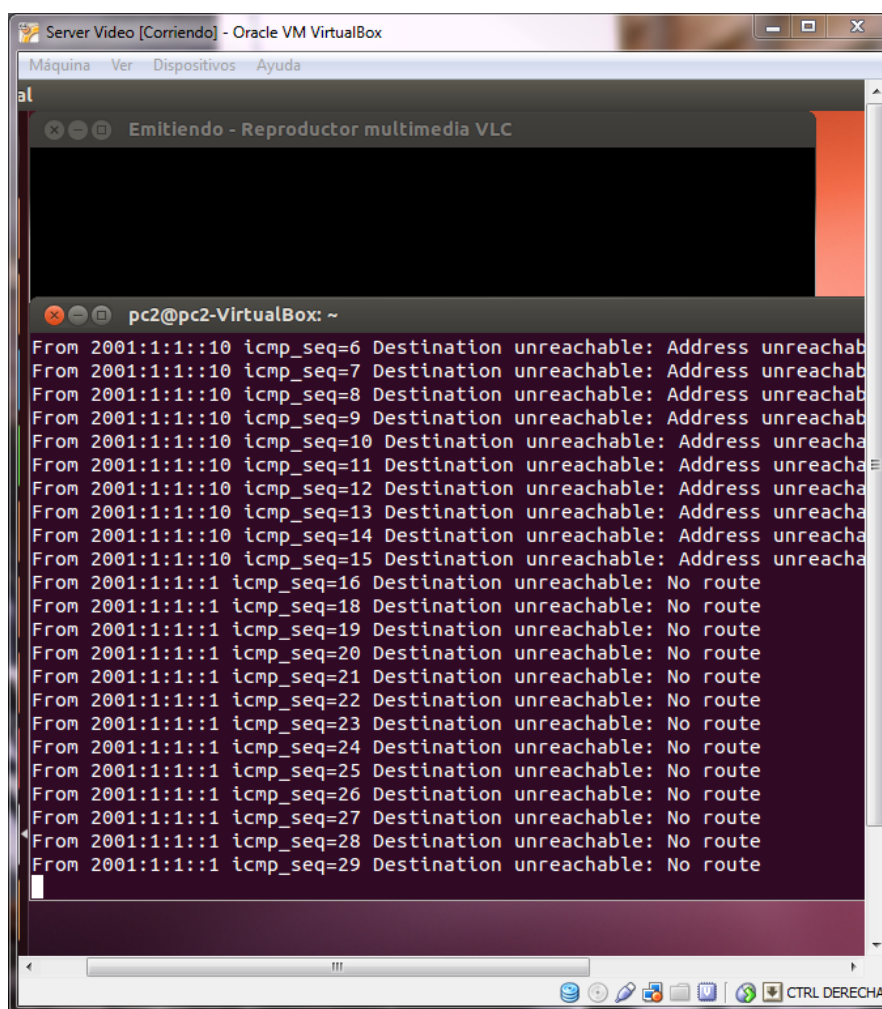
Se puede observar en las capturas de pantalla que antes del proceso de encendido de los routers en la red de distribución, no existe conectividad entre el Servidor y clientes, es decir la respuesta de un ping desde el Server VLC hacia los Clientes será: ADDRESS UNREACHABLE.



```
Server Video [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
al
Emitiendo - Reproductor multimedia VLC
pc2@pc2-VirtualBox: ~
From 2001:1:1:10 icmp_seq=12170 Destination unreachable: Address unrea
From 2001:1:1:10 icmp_seq=12171 Destination unreachable: Address unrea
From 2001:1:1:10 icmp_seq=12172 Destination unreachable: Address unrea
From 2001:1:1:10 icmp_seq=12173 Destination unreachable: Address unrea
^C
--- 2001:3:3:10 ping statistics ---
12175 packets transmitted, 1633 received, +9843 errors, 86% packet loss
213135ms
rtt min/avg/max/mdev = 0.758/6.384/208.667/10.554 ms
pc2@pc2-VirtualBox:~$ ping6 2001:3:3:10
PING 2001:3:3:10(2001:3:3:10) 56 data bytes
From 2001:1:1:10 icmp_seq=1 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=2 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=3 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=4 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=5 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=6 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=7 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=8 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=9 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=10 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=11 Destination unreachable: Address unreachab
From 2001:1:1:10 icmp_seq=12 Destination unreachable: Address unreachab
```

Figura 2.12: Ping hacia el cliente cuando los routers se están iniciando

En el momento que se encienden los routers en el Simulador GNS3, en el Server VLC, el comando ping pasa de emitir una señal de destino inalcanzable a emitir una señal de NO ROUTE, el cual indica que si bien aún no hay conectividad entre Servidor y Cliente, los routers se están encendiendo y están empezando a construir las tablas de direccionamiento.



```
pc2@pc2-VirtualBox: ~
From 2001:1:1::10 icmp_seq=6 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=7 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=8 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=9 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=10 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=11 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=12 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=13 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=14 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::10 icmp_seq=15 Destination unreachable: Address unreachable: Address unreachable
From 2001:1:1::1 icmp_seq=16 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=18 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=19 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=20 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=21 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=22 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=23 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=24 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=25 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=26 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=27 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=28 Destination unreachable: No route
From 2001:1:1::1 icmp_seq=29 Destination unreachable: No route
```

Figura 2.13: Ping hacia el cliente cuando los routers están aprendiendo las tablas de enrutamiento.

Luego que los routers se encienden totalmente, se puede observar que existe conectividad entre cualquier punto de la red.

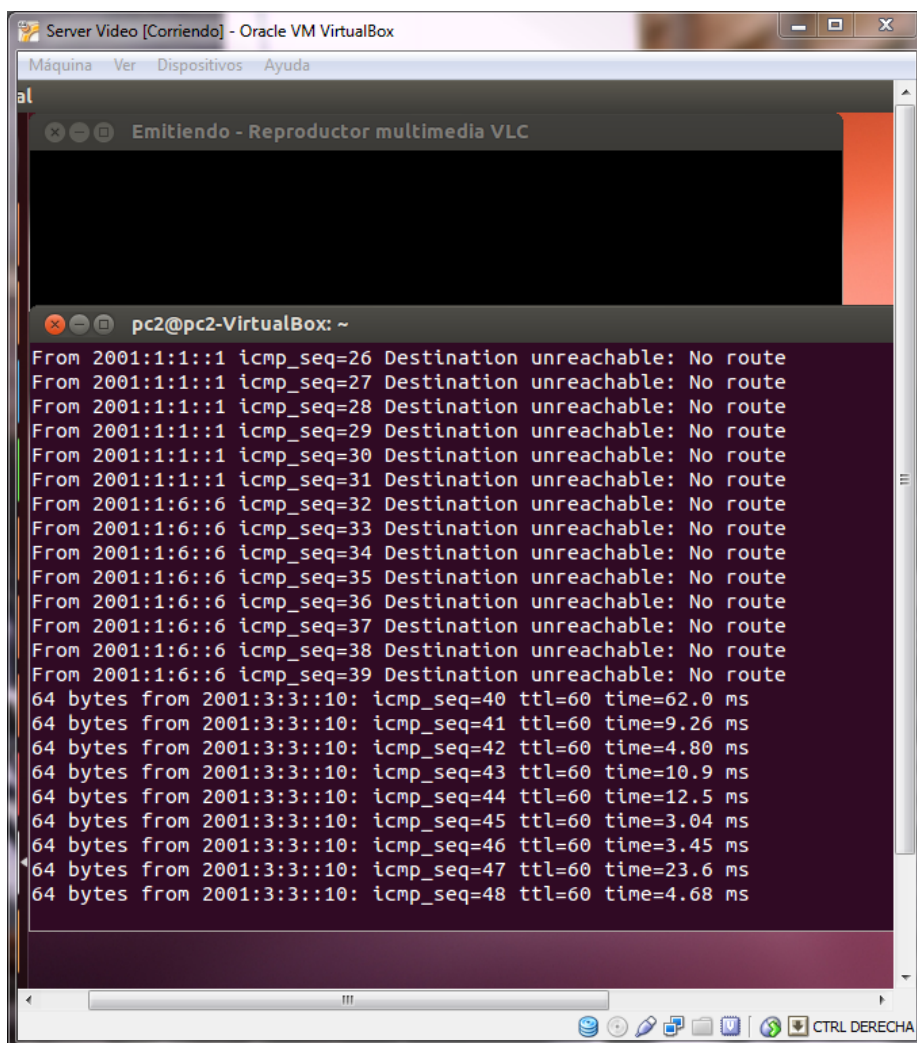


Figura 2.14: Ping exitoso hacia el cliente.

Una vez que se ha comprobado la conectividad entre todos puntos de la red, se realiza la emisión de video mediante el Server VLC, al lado derecho se puede observar que la señal es captada por dos clientes (PC1 y PC5) simultáneamente.

Para acceder a esta señal de streaming es necesario que el cliente se encuentre incluido en un grupo específico de multicast y además que en el Cliente Multicast se ingrese la dirección correcta asignada al video streaming deseado.

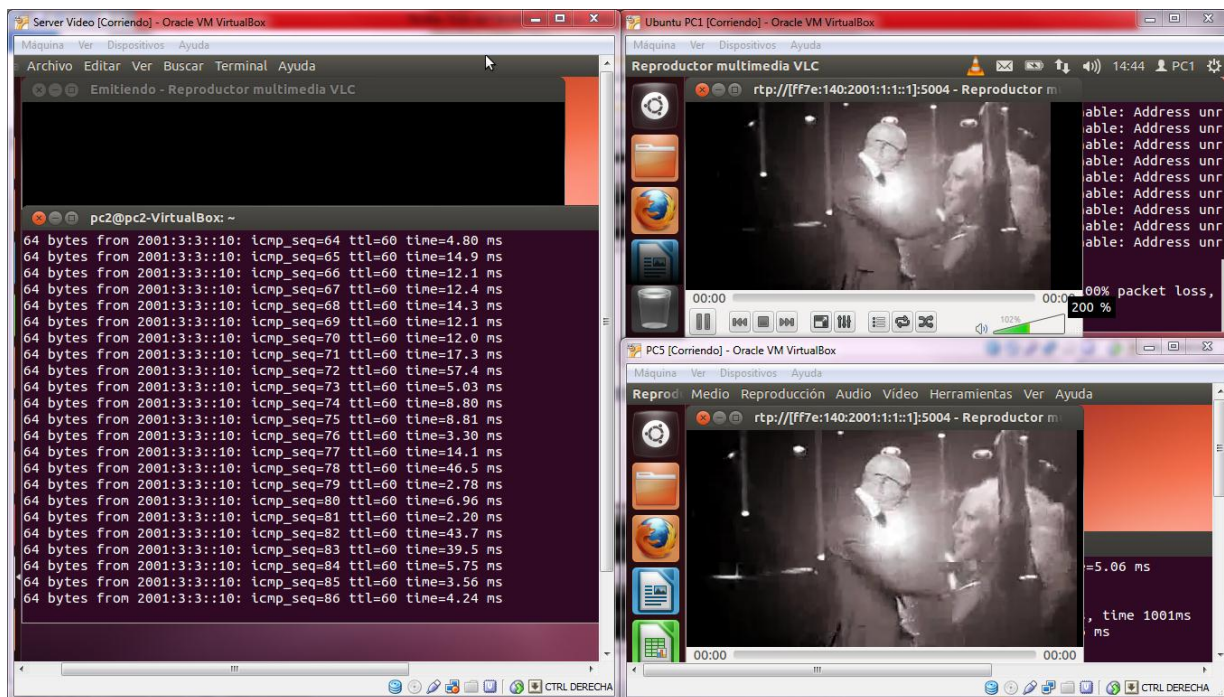


Figura 2.15: Emisión y recepción del streaming de video.

Mediante el programa libre WIRESHARK podemos capturar los paquetes que se están transmitiendo a través de toda la red, a continuación se presenta todos los datos capturados mediante este software incluyendo los parámetros de calidad mencionados anteriormente.

Para poder comparar los datos de la red, es necesario tomar dichos datos desde 3 puntos fundamentales simultáneamente:

- Server VLC.- Se capturará los paquetes enviados por el Server VLC y que ingresan por el puerto Fastethernet 0/0 del router R1.
- Cliente PC5.- Se capturará los paquetes recibidos por el cliente PC5 y que ingresan por el puerto Fastethernet 0/0 del router R5.
- Cliente PC1.- Se capturará los paquetes recibidos por el cliente PC1 y que ingresan por el puerto Fastethernet 0/0 del router R3.

Para tomar los datos simultáneamente, nos ayudamos del mismo programa WIRESHARK, el cual nos facilita, iniciar y detener la captura de paquetes simultáneamente en los puertos que se desee.

Server VLC

Mediante WIRESHARK se ha capturado los paquetes que se envían a la red desde el Server VLC:

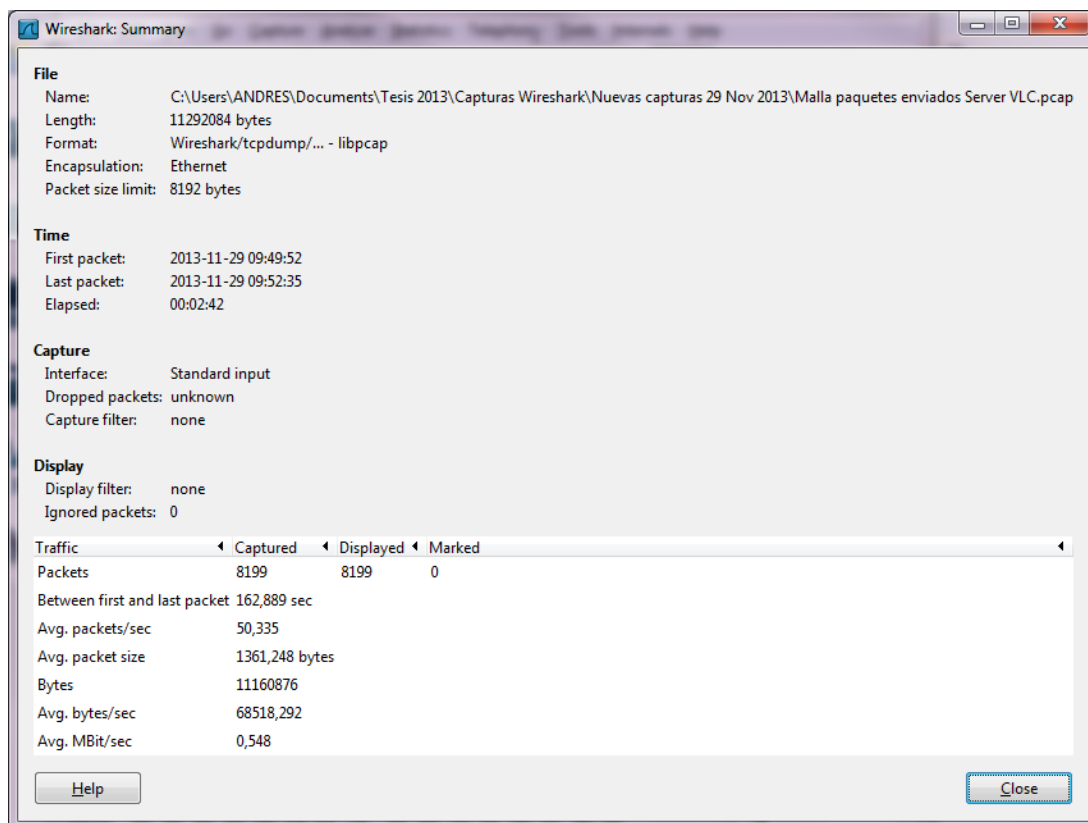


Figura 2.16: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	2 min 42 seg.
TIEMPO EN SEGUNDOS:	162.889 seg.
PAQUETES CAPTURADOS:	8199.00
PAQUETES MOSTRADOS:	8199.00
BYTES TOTALES:	11160876.00
PROMEDIO PAQUETES/SEG:	50335.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1361.248
PROMEDIO BYTES/SEG:	68518.292
PROMEDIO MBITS/SEG:	0,548

Tabla 2.7: Resumen de los datos mostrados en Wireshark

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100,00 %	8199	100,00 %	11160876	0,548	0	0	0	0,000		
Ethernet	100,00 %	8199	100,00 %	11160876	0,548	0	0	0	0,000		
Internet Protocol Version 6	98,83 %	8103	99,84 %	11142989	0,547	0	0	0	0,000		
User Datagram Protocol	98,39 %	8067	99,81 %	11139355	0,547	0	0	0	0,000		
Data	98,01 %	8036	99,71 %	11128328	0,547	8036	11128328	0,547			
Hypertext Transfer Protocol	0,22 %	18	0,09 %	9885	0,000	18	9885	0,000			
Domain Name Service	0,16 %	13	0,01 %	1142	0,000	13	1142	0,000			
Open Shortest Path First	0,21 %	17	0,01 %	1530	0,000	17	1530	0,000			
Internet Control Message Protocol v6	0,17 %	14	0,01 %	1424	0,000	14	1424	0,000			
Protocol Independent Multicast	0,06 %	5	0,01 %	680	0,000	5	680	0,000			
Configuration Test Protocol (loopback)	0,20 %	16	0,01 %	960	0,000	0	0	0,000			
Data	0,20 %	16	0,01 %	960	0,000	16	960	0,000			
Internet Protocol Version 4	0,95 %	78	0,14 %	16115	0,001	0	0	0,000			
User Datagram Protocol	0,95 %	78	0,14 %	16115	0,001	0	0	0,000			
Hypertext Transfer Protocol	0,40 %	33	0,11 %	12024	0,001	33	12024	0,001			
Dropbox LAN sync Discovery Protocol	0,06 %	5	0,01 %	725	0,000	5	725	0,000			
Domain Name Service	0,16 %	13	0,01 %	882	0,000	13	882	0,000			
NetBIOS Name Service	0,33 %	27	0,02 %	2484	0,000	27	2484	0,000			
Logical-Link Control	0,02 %	2	0,01 %	812	0,000	0	0	0,000			
Cisco Discovery Protocol	0,02 %	2	0,01 %	812	0,000	2	812	0,000			

Buttons: Help, Close

Figura 2.17: Resumen detallado de los paquetes capturados por Wireshark.

La figura 2.17 muestra en detalle el tipo de paquete (IPv6, UDP, paquetes de datos, paquetes OSPF, etc.) y el porcentaje de paquetes capturados respecto del total.

WIRESHARK brinda una herramienta de estadística muy completa incluida en su programa, los gráficos anteriores muestran en forma resumida pero muy completa, el número de paquetes totales capturados por el software, así como el tiempo transcurrido desde el primer paquete hasta el último y por tanto, mostrando una velocidad de transmisión promedio.

Estos datos son suficientes para poder realizar los cálculos que permitan establecer los parámetros de calidad de la transmisión de video, los cuales son: Latencia, Velocidad de transmisión, Jitter y Pérdida de paquetes; sin embargo, es posible tener datos más exactos a cerca de cada tipo de paquete que está atravesando la red.

A continuación se muestra los datos exactos de los paquetes capturados en la transmisión de video streaming:

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets B-A	Bytes B-A	Rel Start	Duration	bps A-B	bps B-A
CadmusCo_02:11:4a	IPv6mcast_00:00:00:01	8 036	11 128 328	8 036	11 128 328	0	0	0,000000000	162,8890	546547,80	N/A
IPv4mcast_7fff:fa	CadmusCo_00:20:93	33	12 024	0	0	33	12 024	10,408000000	151,7130	N/A	634,04
CadmusCo_00:20:93	Broadcast	32	3 209	32	3 209	0	0	12,808000000	149,2150	172,05	N/A
CadmusCo_00:20:93	IPv6mcast_00:00:00:0c	18	9 885	18	9 885	0	0	10,408000000	6,0210	13134,03	N/A
IPv6mcast_00:00:00:05	d0:02:12:64:00:00	17	1 530	0	0	17	1 530	0,429000000	161,8200	N/A	75,64
d0:02:12:64:00:00	d0:02:12:64:00:00	16	960	16	960	0	0	7,610000000	151,7350	50,61	N/A
CadmusCo_00:20:93	IPv6mcast_00:01:00:03	13	1 142	13	1 142	0	0	85,619000000	77,2510	118,26	N/A
IPv4mcast_00:00:fc	CadmusCo_00:20:93	13	882	0	0	13	882	85,619000000	77,2510	N/A	91,34
IPv6mcast_00:00:00:d	d0:02:12:64:00:00	5	680	0	0	5	680	21,752000000	120,5410	N/A	45,13
CadmusCo_00:20:93	IPv6mcast_00:00:00:16	4	360	4	360	0	0	83,019000000	4,5000	640,00	N/A
CadmusCo_00:20:93	IPv6mcast_ff:64:00:00	3	258	3	258	0	0	14,040000000	93,5890	22,05	N/A
CadmusCo_00:20:93	d0:02:12:64:00:00	3	258	1	86	2	172	107,669000000	5,0280	N/A	273,67
CDP/VTP/DTP/PagP/UDLD	d0:02:12:64:00:00	2	812	0	0	2	812	52,943000000	60,6200	N/A	107,16
IPv6mcast_00:00:00:01	d0:02:12:64:00:00	2	208	0	0	2	208	80,155000000	19,6940	N/A	84,49
CadmusCo_02:11:4a	IPv6mcast_00:00:00:16	1	130	1	130	0	0	80,786000000	0,0000	N/A	N/A
IPv6mcast_00:00:00:16	d0:02:12:64:00:00	1	210	0	0	1	210	83,695000000	0,0000	N/A	N/A

Figura 2.18: Paquetes Ethernet que atravesaron la red al momento de la captura

El gráfico anterior muestra detalladamente los paquetes Ethernet capturados por Wireshark, estos paquetes son: paquetes de búsqueda y descubrimiento, paquetes de configuración, paquetes de establecimiento de rutas, paquetes IPv6 y paquetes IPv4, estos paquetes se muestran en grupos (número de paquetes enviados, bytes totales, velocidad de transmisión y duración de la transmisión desde el punto de origen hasta el destino y viceversa).

A continuación se muestra únicamente los paquetes IPv6 que atravesaron la red al momento de la captura:

Conversations: Malla paquetes enviados Server VLC.pcap

Ethernet: 16 | Fibre Channel | FDDI | IPv4: 3 | IPv6: 11 | IPX | JXTA | NCP | RSVP | SCTP | TCP | Token Ring | UDP: 33 | USB | WLAN

IPv6 Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	ff7e:140:2001:1:1::1	8 036	11 128 328	8 036	11 128 328	0	0	0,000000000	162,8890	546547,80	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::c	18	9 885	18	9 885	0	0	10,408000000	6,0210	13134,03	N/A
fe80::d202:12ff:fe64:0	ff02::5	17	1 530	17	1 530	0	0	0,429000000	161,8200	75,64	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:3	13	1 142	13	1 142	0	0	85,619000000	77,2510	118,26	N/A
fe80::d202:12ff:fe64:0	ff02::d	5	680	5	680	0	0	21,752000000	120,5410	45,13	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::16	4	360	4	360	0	0	83,019000000	4,5000	640,00	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:ff64:0	3	258	3	258	0	0	14,040000000	93,5890	22,05	N/A
fe80::c5d6:8a3:f8d5:1fe8	fe80::d202:12ff:fe64:0	3	258	1	86	2	172	107,669000000	5,0280	N/A	273,67
fe80::d202:12ff:fe64:0	ff02::1	2	208	2	208	0	0	80,155000000	19,6940	84,49	N/A
fe80::a00:27ff:fe02:114a	ff02::16	1	130	1	130	0	0	80,786000000	0,0000	N/A	N/A
fe80::d202:12ff:fe64:0	ff02::16	1	210	1	210	0	0	83,695000000	0,0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 2.19: Paquetes IPv6 que atravesaron la red al momento de la captura

Como se mencionó en la parte teórica de este documento, el streaming de video viaja utilizando el protocolo IPv6 como medio de comunicación y este a su vez, utiliza UDP como medio de transporte, para llegar desde el Servidor hasta cada cliente.

Los paquetes UDP llevan la información del streaming de video que se está transmitiendo, es decir, la información de los paquetes UDP que atraviesa la red, es la información pura de los datos, sin tomar en cuenta paquetes de búsqueda o descubrimiento de vecinos, paquetes de enrutamiento, paquetes de sincronización multicast, etc., sino únicamente la información pura del mensaje.

Esta información es valiosa para calcular los parámetros de calidad reales que se están dando en la red, ya que el fin de la transmisión es la recepción de la DATA de un paquete.

El grafico siguiente muestra los únicamente los paquetes UDP que atravesaron la red al momento de la captura:

Conversations: Malla paquetes enviados Server VLC.pcap

Ethernet: 16 Fibre Channel FDDI IPv4: 3 IPv6: 11 JXTA NCP RSVP SCTP TCP Token Ring UDP: 33 USB WLAN

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	47118	ff7e:140:2001:1:1::1	avt-profile-1	8 003	11 124 170	8 003	11 124 170	0	0	0,000000000	162,8890	546343,58	N/A
2001:1:1::10	47119	ff7e:140:2001:1:1::1	avt-profile-2	33	4 158	33	4 158	0	0	0,613000000	159,9970	207,90	N/A
192.168.199.1	netbios-ns	192.168.199.255	netbios-ns	27	2 484	27	2 484	0	0	85,820000000	76,2030	260,78	N/A
192.168.199.1	ssdp	239.255.255.250	ssdp	18	9 399	18	9 399	0	0	10,408000000	6,0210	12488,29	N/A
fe80::c5d6:8a3:f8d5:1fe8	ssdp	ff02::c	ssdp	18	9 885	18	9 885	0	0	10,408000000	6,0210	13134,03	N/A
192.168.199.1	60021	239.255.255.250	ssdp	15	2 625	15	2 625	0	0	95,031000000	67,0900	313,01	N/A
192.168.199.1	db-lsp-disc	192.168.199.255	db-lsp-disc	5	725	5	725	0	0	12,808000000	120,2720	48,22	N/A
fe80::c5d6:8a3:f8d5:1fe8	50992	ff02::1:3	llmnr	1	92	1	92	0	0	85,619000000	0,0000	N/A	N/A
192.168.199.1	56318	224.0.0.252	llmnr	1	72	1	72	0	0	85,619000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	62735	ff02::1:3	llmnr	1	92	1	92	0	0	86,121000000	0,0000	N/A	N/A
192.168.199.1	49299	224.0.0.252	llmnr	1	72	1	72	0	0	86,121000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	52905	ff02::1:3	llmnr	1	92	1	92	0	0	86,565000000	0,0000	N/A	N/A
192.168.199.1	55714	224.0.0.252	llmnr	1	72	1	72	0	0	86,565000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	59589	ff02::1:3	llmnr	1	92	1	92	0	0	86,858000000	0,0000	N/A	N/A
192.168.199.1	49775	224.0.0.252	llmnr	1	72	1	72	0	0	86,858000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	65165	ff02::1:3	llmnr	1	86	1	86	0	0	95,125000000	0,0000	N/A	N/A
192.168.199.1	62858	224.0.0.252	llmnr	1	66	1	66	0	0	95,125000000	0,0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 2.20: Paquetes UDP que atravesaron la red al momento de la captura

Otra herramienta muy útil es “Packet Lengths”, el cual, como su nombre lo dice, muestra una tabla con las diferentes longitudes que formaron parte de la comunicación, esta herramienta muestra, un rango de longitudes de paquete que atravesaron la red, el número de paquetes en cada rango, la velocidad del paquete y el porcentaje de paquetes con ese rango respecto del total.

Packet Lengths

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	8199	0,050335	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	29	0,000178	0,35%
80-159	113	0,000694	1,38%
160-319	16	0,000098	0,20%
320-639	38	0,000233	0,46%
640-1279	0	0,000000	0,00%
1280-2559	8003	0,049132	97,61%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Close

Figura 2.21: Rangos de las diferentes longitudes de los paquetes capturados

En el gráfico anterior se detalla: rango de longitud, número de paquetes en esos rangos, velocidad del paquete y porcentaje de paquetes con respecto al total transmitido.

Si se desea observar de forma gráfica la transmisión que ha sido capturada, se puede utilizar “IO Graphs” donde muestra con un gráfico la captura de todos los paquetes de en el tiempo.

IO Graphs permite filtrar el gráfico para que muestre únicamente un tipo de protocolo, para este ejemplo no se ha hecho ningún tipo de filtro, por tanto, la figura 2.21, muestra todo el rango de valores transmitidos.

Se puede observar que el gráfico no es constante, es decir, existen picos de altas y bajas velocidades de transmisión.

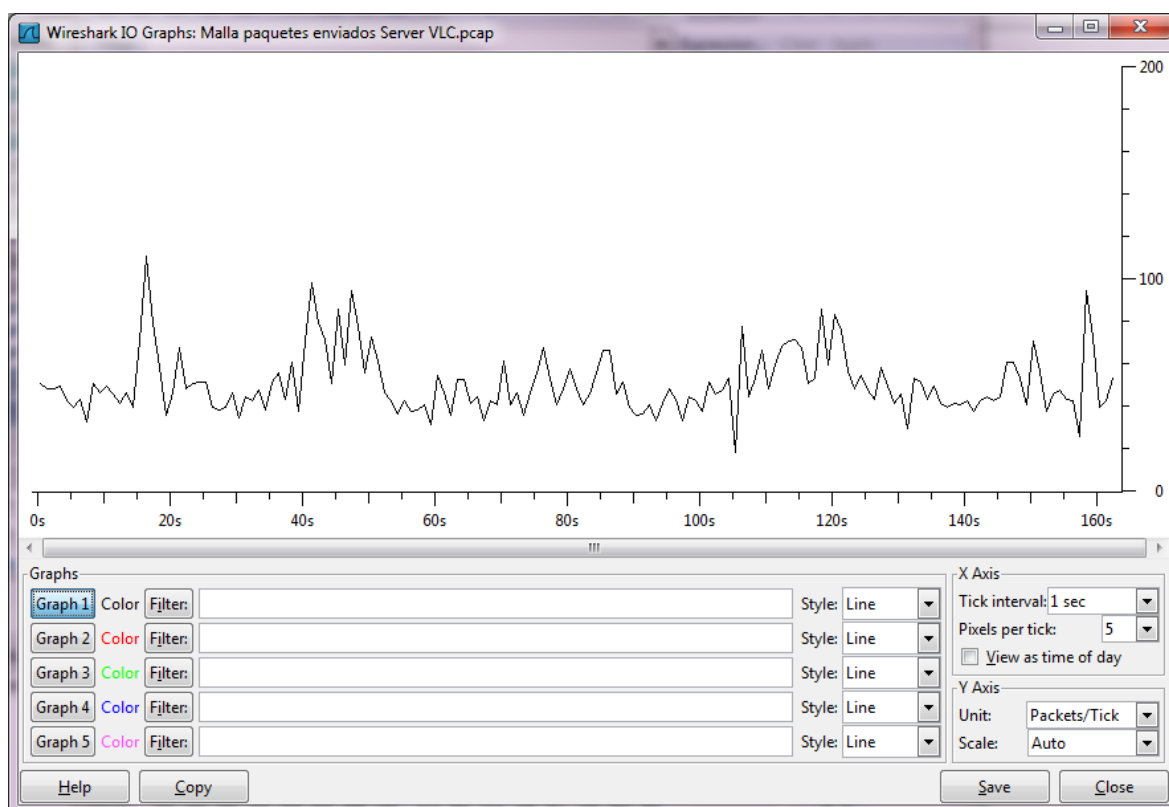


Figura 2.22: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

Ciente PC5

Los datos aquí presentados, son paquetes capturados en el puerto FASTETHERNET del CLIENTE PC5, es decir, fueron capturados en el puerto final de la transmisión del video streaming, el cual nos asegura, capturar los paquetes totales que se transmitieron a través de la red de distribución hasta llegar al punto final que es el CLIENTE PC5.

A continuación un resumen general de los paquetes transmitidos a través de la red:

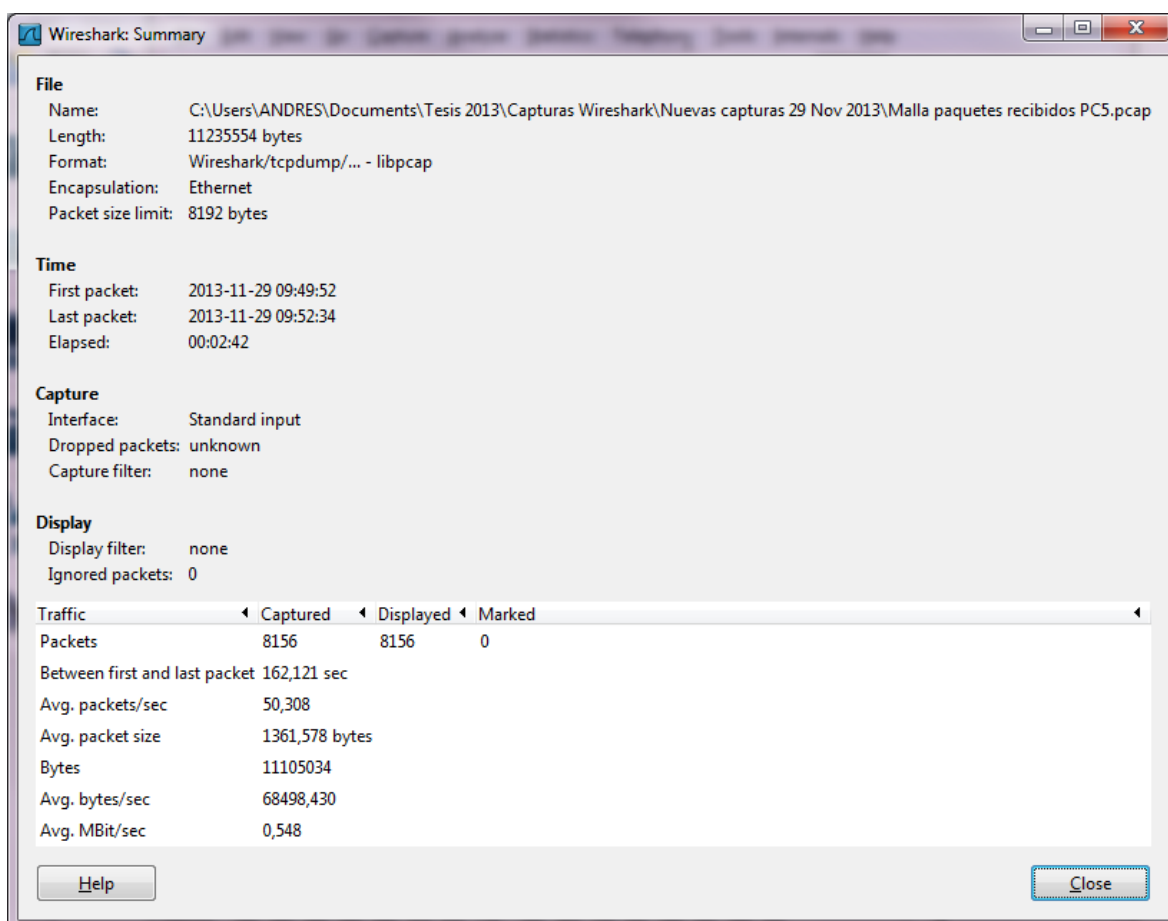


Figura 2.23: Resumen de los paquetes totales capturados por Wireshark, recibidos por el Cliente PC5 en el puerto Fastethernet 0/0 del router R5

PC:	CLIENTE PC5
INTERFACE:	Fastethernet R5
TIEMPO DE CAPTURA DE PAQUETES:	2 min 42 seg.
TIEMPO EN SEGUNDOS:	162.121 seg.
PAQUETES CAPTURADOS:	8156.00
PAQUETES MOSTRADOS:	8156.00
BYTES TOTALES:	11105034.00
PROMEDIO PAQUETES/SEG:	50308.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1361.578
PROMEDIO BYTES/SEG:	68498.430
PROMEDIO MBITS/SEG:	0,548

Tabla 2.8: Resumen de los datos mostrados en Wireshark

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	8156	100,00 %	11105034	0,548	0	0	0,000
Ethernet	100,00 %	8156	100,00 %	11105034	0,548	0	0	0,000
Internet Protocol Version 6	98,84 %	8061	99,84 %	11087213	0,547	0	0	0,000
User Datagram Protocol	98,41 %	8026	99,81 %	11083669	0,547	0	0	0,000
Data	98,04 %	7996	99,71 %	11072728	0,546	7996	11072728	0,546
Hypertext Transfer Protocol	0,22 %	18	0,09 %	9885	0,000	18	9885	0,000
Domain Name Service	0,15 %	12	0,01 %	1056	0,000	12	1056	0,000
Open Shortest Path First	0,20 %	16	0,01 %	1440	0,000	16	1440	0,000
Internet Control Message Protocol v6	0,17 %	14	0,01 %	1424	0,000	14	1424	0,000
Protocol Independent Multicast	0,06 %	5	0,01 %	680	0,000	5	680	0,000
Configuration Test Protocol (loopback)	0,20 %	16	0,01 %	960	0,000	0	0	0,000
Data	0,20 %	16	0,01 %	960	0,000	16	960	0,000
Internet Protocol Version 4	0,94 %	77	0,14 %	16049	0,001	0	0	0,000
User Datagram Protocol	0,94 %	77	0,14 %	16049	0,001	0	0	0,000
Hypertext Transfer Protocol	0,40 %	33	0,11 %	12024	0,001	33	12024	0,001
Dropbox LAN sync Discovery Protocol	0,06 %	5	0,01 %	725	0,000	5	725	0,000
Domain Name Service	0,15 %	12	0,01 %	816	0,000	12	816	0,000
NetBIOS Name Service	0,33 %	27	0,02 %	2484	0,000	27	2484	0,000
Logical-Link Control	0,02 %	2	0,01 %	812	0,000	0	0	0,000
Cisco Discovery Protocol	0,02 %	2	0,01 %	812	0,000	2	812	0,000

Help Close

Figura 2.24: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.24 se encuentra en la página 103

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
CadmusCo_02:11:4a	IPv6mcast_00:00:00:01	7 996	11 072 728	7 996	11 072 728	0	0	0,000000000	162,0820	546524,75	N/A
IPv4mcast_7fff:fa	CadmusCo_00:20:93	33	12 024	0	0	33	12 024	10,408000000	151,7130	N/A	634,04
CadmusCo_00:20:93	Broadcast	32	3 209	32	3 209	0	0	12,808000000	149,2150	172,05	N/A
CadmusCo_00:20:93	IPv6mcast_00:00:00:0c	18	9 885	18	9 885	0	0	10,408000000	6,0210	13134,03	N/A
IPv6mcast_00:00:00:05	d0:02:12:64:00:00	16	1 440	0	0	16	1 440	0,429000000	151,6280	N/A	75,98
d0:02:12:64:00:00	d0:02:12:64:00:00	16	960	16	960	0	0	7,610000000	151,7350	50,61	N/A
CadmusCo_00:20:93	IPv6mcast_00:01:00:03	12	1 056	12	1 056	0	0	85,619000000	74,7030	113,09	N/A
IPv4mcast_00:00:fc	CadmusCo_00:20:93	12	816	0	0	12	816	85,619000000	74,7030	N/A	87,39
IPv6mcast_00:00:0d	d0:02:12:64:00:00	5	680	0	0	5	680	21,752000000	120,5410	N/A	45,13
CadmusCo_00:20:93	IPv6mcast_00:00:00:16	4	360	4	360	0	0	83,019000000	4,5000	640,00	N/A
CadmusCo_00:20:93	IPv6mcast_ff:64:00:00	3	258	3	258	0	0	14,040000000	93,5890	22,05	N/A
CadmusCo_00:20:93	d0:02:12:64:00:00	3	258	1	86	2	172	107,669000000	5,0280	N/A	273,67
CDP/VTP/DTP/PAgP/UDLD	d0:02:12:64:00:00	2	812	0	0	2	812	52,943000000	60,6200	N/A	107,16
IPv6mcast_00:00:00:01	d0:02:12:64:00:00	2	208	0	0	2	208	80,155000000	19,6940	N/A	84,49
CadmusCo_02:11:4a	IPv6mcast_00:00:00:16	1	130	1	130	0	0	80,786000000	0,0000	N/A	N/A
IPv6mcast_00:00:00:16	d0:02:12:64:00:00	1	210	0	0	1	210	83,695000000	0,0000	N/A	N/A

Figura 2.25: Paquetes Ethernet que atravesaron la red al momento de la captura

* La explicación de la figura 2.25 se encuentra en la página 104

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	ff7e:140:2001:1:1::1	7 996	11 072 728	7 996	11 072 728	0	0	0,000000000	162,0820	546524,75	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::c	18	9 885	18	9 885	0	0	10,408000000	6,0210	13134,03	N/A
fe80::d202:12ff:fe64:0	ff02::5	16	1 440	16	1 440	0	0	0,429000000	151,6280	75,98	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:3	12	1 056	12	1 056	0	0	85,619000000	74,7030	113,09	N/A
fe80::d202:12ff:fe64:0	ff02::d	5	680	5	680	0	0	21,752000000	120,5410	45,13	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:6	4	360	4	360	0	0	83,019000000	4,5000	640,00	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:ff64:0	3	258	3	258	0	0	14,040000000	93,5890	22,05	N/A
fe80::c5d6:8a3:f8d5:1fe8	fe80::d202:12ff:fe64:0	3	258	1	86	2	172	107,669000000	5,0280	N/A	273,67
fe80::d202:12ff:fe64:0	ff02::1	2	208	2	208	0	0	80,155000000	19,6940	84,49	N/A
fe80::a00:27ff:fe02:114a	ff02::1:6	1	130	1	130	0	0	80,786000000	0,0000	N/A	N/A
fe80::d202:12ff:fe64:0	ff02::1:6	1	210	1	210	0	0	83,695000000	0,0000	N/A	N/A

Figura 2.26: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 2.26 se encuentra en la página 105

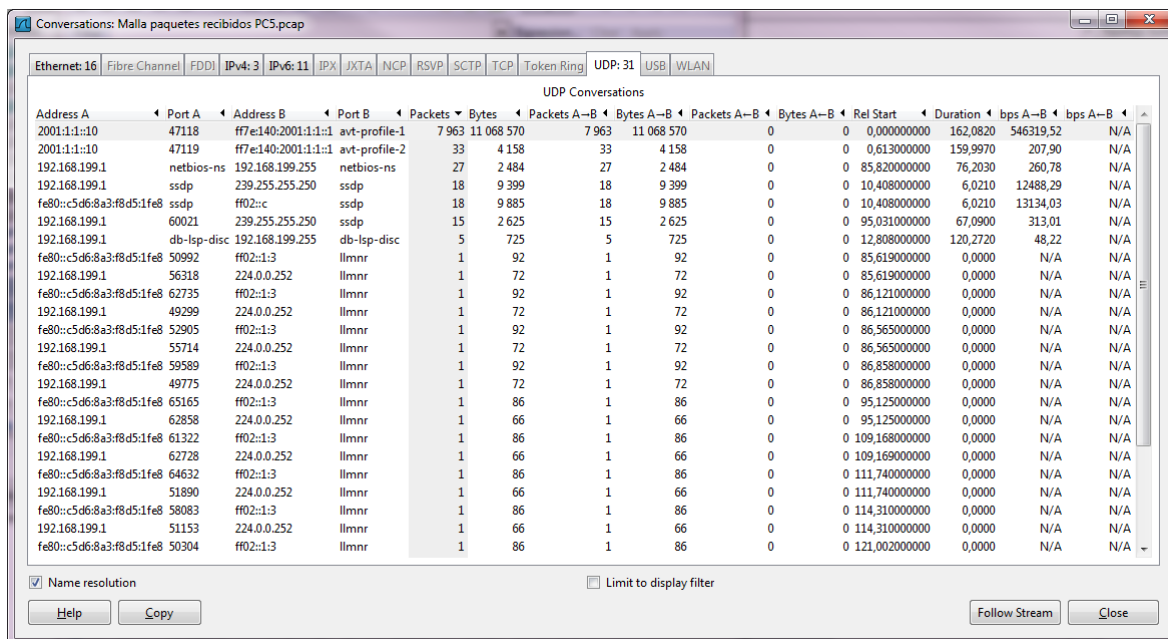


Figura 2.27: Paquetes UDP que atravesaron la red al momento de la captura

* La explicación de la figura 2.27 se encuentra en la página 105

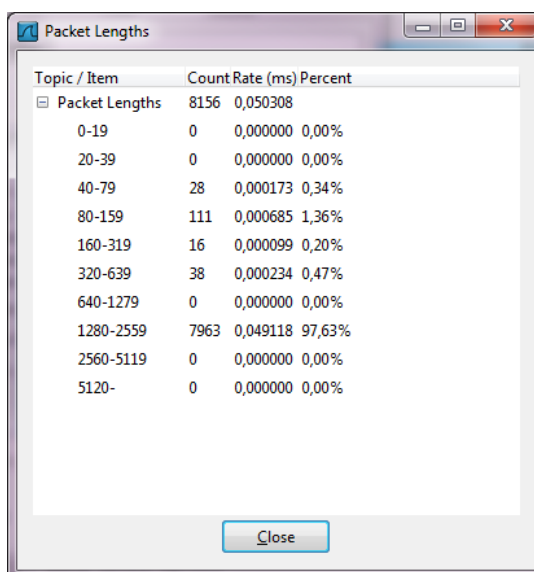


Figura 2.28: Rangos de las diferentes longitudes de los paquetes capturados

* La explicación de la figura 2.28 se encuentra en la página 106

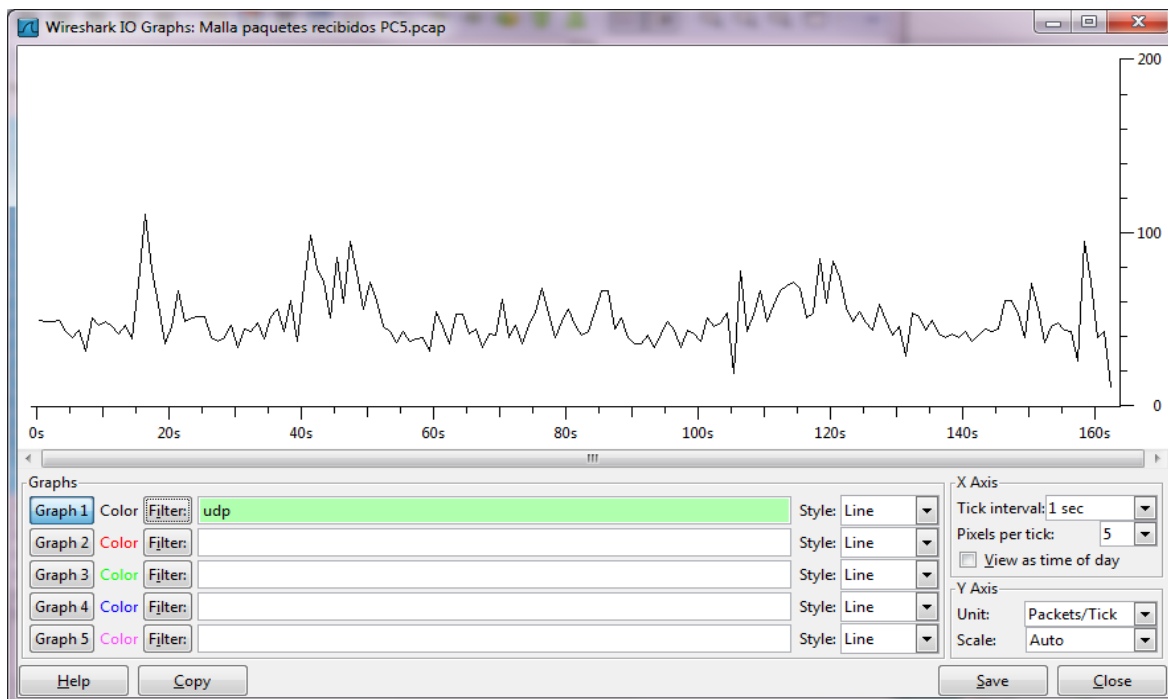


Figura 2.29: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

Cliente PC1

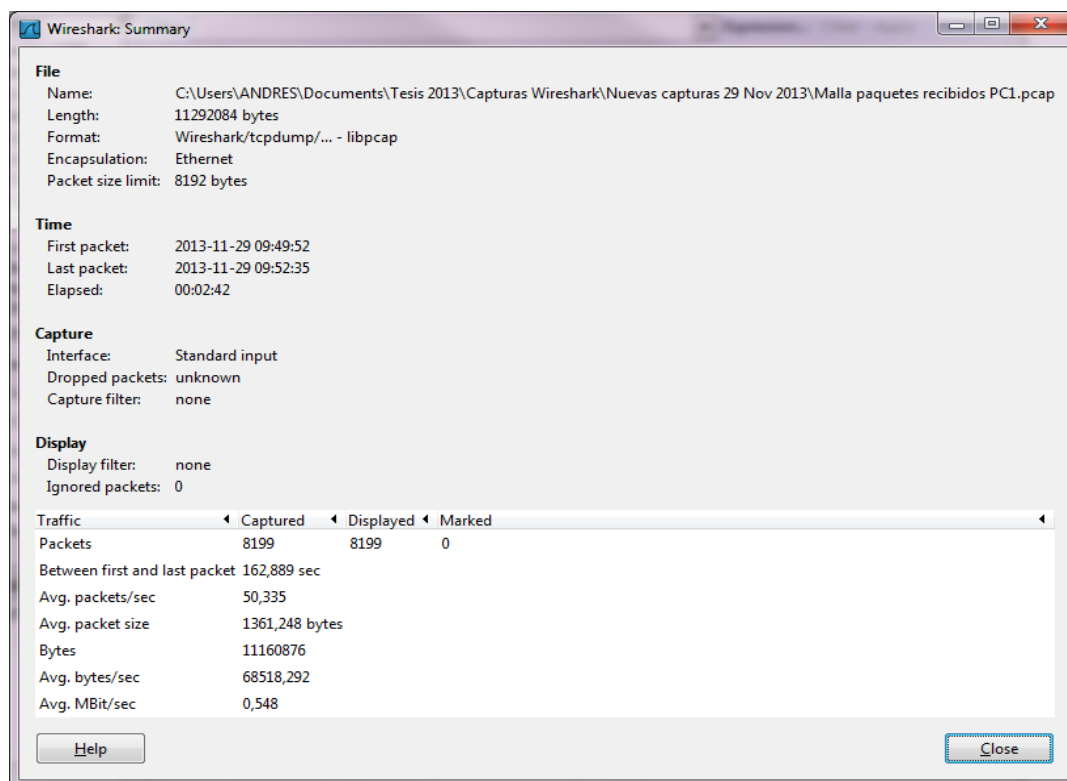


Figura 2.30: Resumen de los paquetes totales capturados por Wireshark, recibidos por el Cliente PC1 en el puerto Fastethernet 0/0 del router R3

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	2 min 42 seg.
TIEMPO EN SEGUNDOS:	162.889 seg.
PAQUETES CAPTURADOS:	8199.00
PAQUETES MOSTRADOS:	8199.00
BYTES TOTALES:	11160876.00
PROMEDIO PAQUETES/SEG:	50335.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1361.248
PROMEDIO BYTES/SEG:	68518.292
PROMEDIO MBITS/SEG:	0,548

Tabla 2.9: Resumen de los datos mostrados en Wireshark

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100,00 %	8199	100,00 %	11160876	0,548	0	0	0	0,000		
Ethernet	100,00 %	8199	100,00 %	11160876	0,548	0	0	0	0,000		
Internet Protocol Version 6	98,83 %	8103	99,84 %	11142989	0,547	0	0	0	0,000		
User Datagram Protocol	98,39 %	8067	99,81 %	11139355	0,547	0	0	0	0,000		
Data	98,01 %	8036	99,71 %	11128328	0,547	8036	11128328	0,547			
Hypertext Transfer Protocol	0,22 %	18	0,09 %	9885	0,000	18	9885	0,000			
Domain Name Service	0,16 %	13	0,01 %	1142	0,000	13	1142	0,000			
Open Shortest Path First	0,21 %	17	0,01 %	1530	0,000	17	1530	0,000			
Internet Control Message Protocol v6	0,17 %	14	0,01 %	1424	0,000	14	1424	0,000			
Protocol Independent Multicast	0,06 %	5	0,01 %	680	0,000	5	680	0,000			
Configuration Test Protocol (loopback)	0,20 %	16	0,01 %	960	0,000	0	0	0,000			
Data	0,20 %	16	0,01 %	960	0,000	16	960	0,000			
Internet Protocol Version 4	0,95 %	78	0,14 %	16115	0,001	0	0	0,000			
User Datagram Protocol	0,95 %	78	0,14 %	16115	0,001	0	0	0,000			
Hypertext Transfer Protocol	0,40 %	33	0,11 %	12024	0,001	33	12024	0,001			
Dropbox LAN sync Discovery Protocol	0,06 %	5	0,01 %	725	0,000	5	725	0,000			
Domain Name Service	0,16 %	13	0,01 %	882	0,000	13	882	0,000			
NetBIOS Name Service	0,33 %	27	0,02 %	2484	0,000	27	2484	0,000			
Logical-Link Control	0,02 %	2	0,01 %	812	0,000	0	0	0,000			
Cisco Discovery Protocol	0,02 %	2	0,01 %	812	0,000	2	812	0,000			

Figura 2.31: Resumen más detallado de los paquetes capturados por Wireshark

* La explicación de la figura 2.31 se encuentra en la página 103

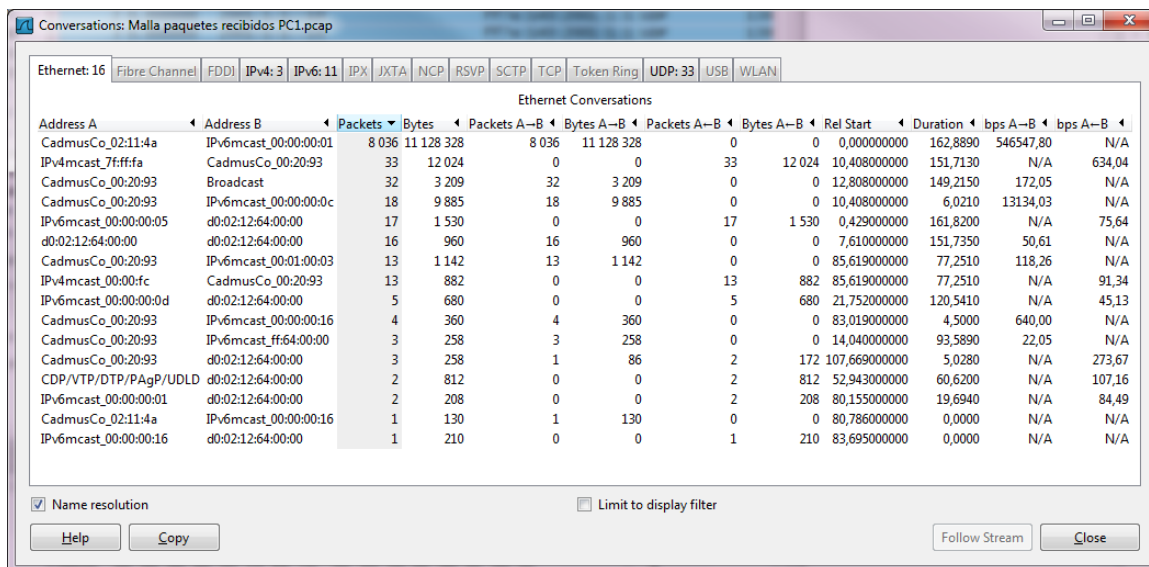


Figura 2.32: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 2.32 se encuentra en la página 104

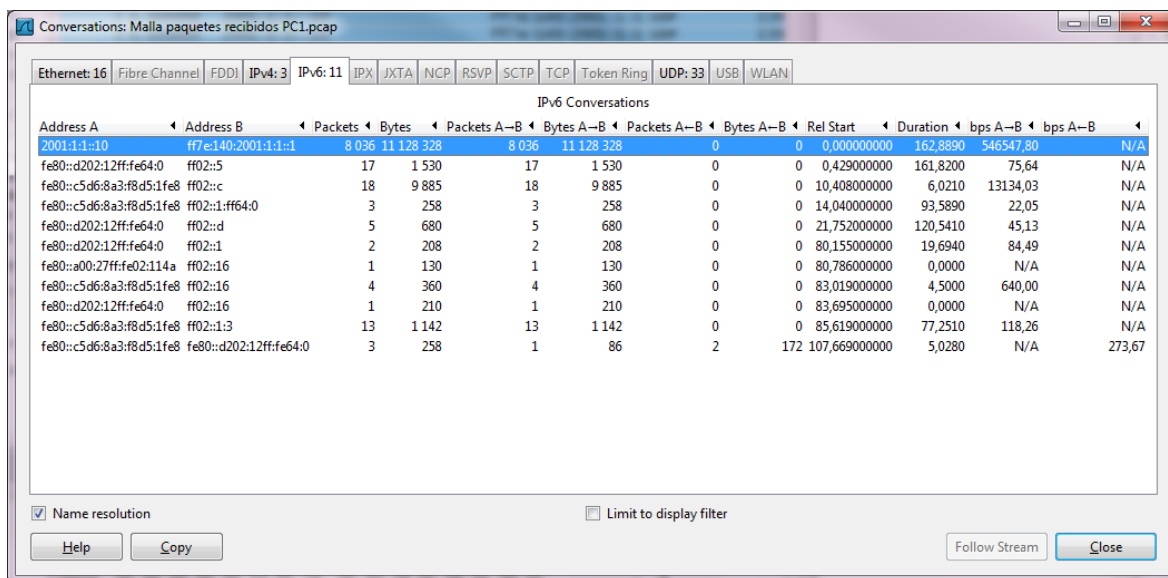


Figura 2.33: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 2.33 se encuentra en la página 105

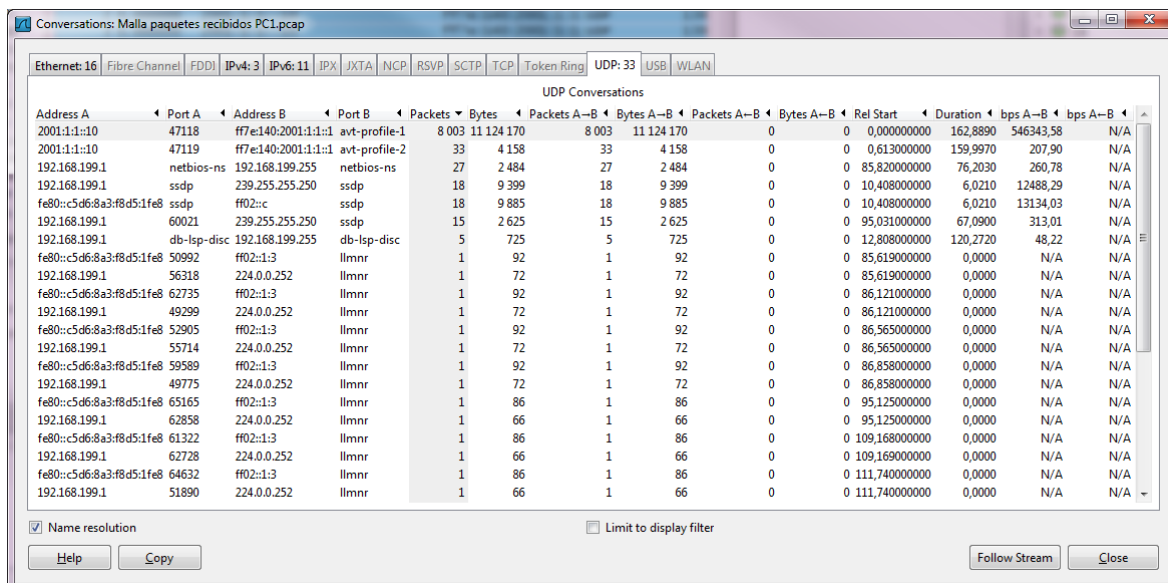


Figura 2.34: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.34 se encuentra en la página 105

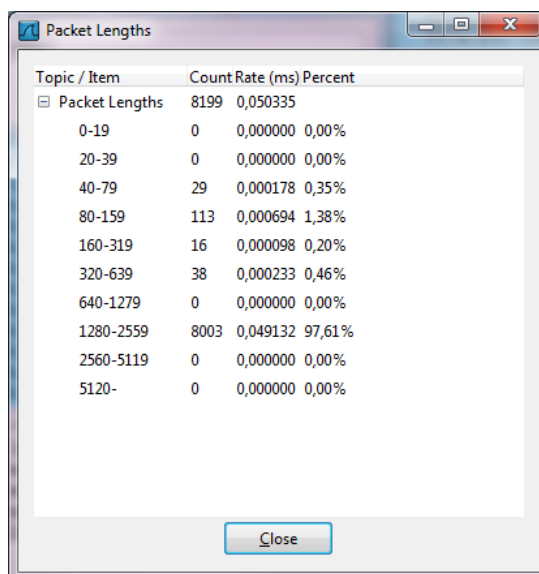


Figura 2.35: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.35 se encuentra en la página 106

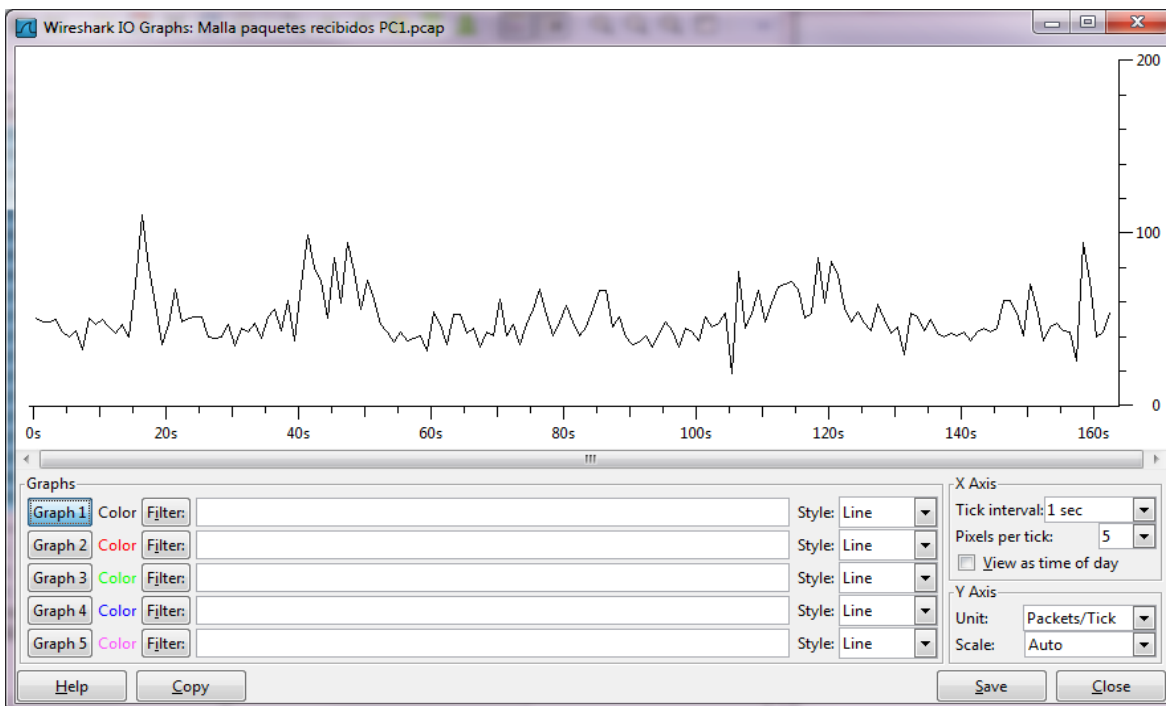


Figura 2.36: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

2.2.1.4 Cálculo de los parámetros de calidad en la red de distribución

Para realizar los cálculos de los parámetros de calidad, debemos comparar los cuadros de datos anteriormente mostrados:

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISIÓN DE VIDEO STREAMING			
TOPOLOGIA:	6 ROUTERS TIPO MALLA		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	2 min 42 seg.	2 min 42 seg.	2 min 42 seg.
TIEMPO EN SEGUNDOS:	162.889 seg.	162.121 seg.	162.889 seg.
PAQUETES CAPTURADOS:	8199.00	8156.00	8199.00
PAQUETES MOSTRADOS:	8199.00	8156.00	8199.00
BYTES TOTALES:	11160876.00	11105034.00	11160876.00
PROMEDIO PAQUETES/SEG:	50335.00	50308.00	50335.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.361.248	1.361.578	1.361.248
PROMEDIO BYTES/SEG:	68.518.292	68.498.430	68.518.292
PROMEDIO MBITS/SEG:	0,548	0,548	0,548

Tabla 2.10: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la topología tipo malla.

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING									
TOPOLOGIA:	6 ROUTERS TIPO MALLA								
RESUMEN POR PROTOCOLOS									
PC:	SERVER VLC			CLIENTE PC5			CLIENTE PC1		
	N° PAQUETES	BYTES	MBITS/SEG	N° PAQUETES	BYTES	MBITS/SEG	N° PAQUETES	BYTES	MBITS/SEG
ETHERNET	8199,00	11160876,00	0,548	8156,00	11105034,00	0,548	8199,00	11160876,00	0,548
PROTOCOLO IPV6	8103,00	11142989,00	0,547	8061,00	11087213,00	0,547	8103,00	11142989,00	0,547
PROTOCOLO UDP	8067,00	11139355,00	0,547	8026,00	11083669,00	0,547	8067,00	11139355,00	0,547
PROTOCOLO OSPF	17,00	1530,00	0,000	16,00	1440,00	0,000	17,00	1530,00	0,000
PROTOCOLO IPV4	78,00	16115,00	0,001	77,00	16049,00	0,001	78,00	16115,00	0,001
PROTOCOLO LLC	2,00	812,00	0,000	2,00	812,00	0,000	2,00	812,00	0,000

Tabla 2.11: Tabla comparativa de valores obtenidos en la transmisión de video streaming por protocolos, en la topología tipo malla.

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING									
TOPOLOGIA:	6 ROUTERS TIPO MALLA								
RESUMEN DETALLADO DE LOS PROTOCOLOS IPV6 Y UDP									
PC:	SERVER VLC			CLIENTE PC5			CLIENTE PC1		
	N° PAQUETES	BYTES	MBITS/SEG	N° PAQUETES	BYTES	MBITS/SEG	N° PAQUETES	BYTES	MBITS/SEG
PROTOCOLO IPV6	8036,00	11128328,00	0,547	7996,00	11072728,00	0,546	8036,00	11128328,00	0,547
PROTOCOLO UDP	8003,00	11124170,00	0,546	7963,00	11068570,00	0,546	8003,00	11124170,00	0,546

Tabla 2.12: Tabla comparativa de valores obtenidos en la transmisión de video streaming de los protocolos IPV6 y UDP, en la topología tipo malla.

Se debe tomar en cuenta que debido a que la simulación fue realizada en un ambiente puramente virtual, los datos mostrados son ideales.

Al comparar las tablas de resumen del servidor VLC y los clientes, podemos sacar algunos datos:

- Los datos obtenidos fueron medidos en un mismo intervalo de tiempo, sin embargo, existe una pequeña diferencia en milisegundos, pero esto no afecta de manera relevante a los cálculos.
- Se puede realizar cálculos de manera general, es decir, con la tabla de resumen general del servidor y los clientes, esta tabla incluye paquetes de descubrimiento, paquetes de enrutamiento, paquetes IPv4, IPv6, etc.
- Se puede realizar los cálculos únicamente con los paquetes IPv6, los cuales son los que llevan la información del streaming de video, o a su vez, más específicamente realizar los cálculos con los paquetes UDP que son realmente los paquetes que llevan la DATA de la transmisión.

2.2.1.4.1 Cálculos de la Velocidad de Transmisión

$$\text{Transferencia real} = \frac{\text{Tamaño de la transferencia}}{\text{Tiempo de la transferencia}}$$

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	6 ROUTERS TIPO MALLA			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	11160876,00	11128328,00	11124170,00	162,889
CLIENTE PC5	11105034,00	11072728,00	11068570,00	162,121
CLIENTE PC1	11160876,00	11128328,00	11124170,00	162,889
TABLA DE VELOCIDADES				
	SERVER VLC	CLIENTE PC5	CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	68518,29	68498,43	68518,29	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	68318,47	68299,16	68318,47	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	68292,95	68273,51	68292,95	

Tabla 2.13: Velocidades de transmisión obtenidas en la simulación.

2.2.1.4.2 Cálculos de Latencia

Para calcular la Latencia que presente la red, vamos a ayudarnos de una herramienta muy sencilla, esta herramienta se llama PING (Packet Internet Groper, que significa "Buscador o rastreador de paquetes en redes").

El comando ping sirve para verificar la conectividad de IP, el procedimiento es sencillo, el host origen realiza una solicitud de ping con la dirección IP del equipo destino, enviándole un paquete de solicitud de eco ICMP. El host remoto recibe el paquete y envía una respuesta de eco ICMP a cambio, comprobando que la conectividad entre ambos equipos es exitosa, es decir, el comando ping nos da como resultado, el tiempo que toma llegar al paquete desde su origen hasta el destino y de regreso pero dividido para a la mitad, para presentarnos únicamente el tiempo de ida del paquete.

Las siguientes capturas muestran el tiempo que el paquete ICMP se demora en llegar desde el Server VLC hacia el Cliente PC1, este mismo modelo se seguirá para establecer el tiempo de retardo para el Cliente PC5.

```

Server Video [Comando] - Oracle VM VirtualBox
Terminal
Reproductor multimedia VLC
pc2@pc2-VirtualBox: ~
From 2001:1:1:1 icmp_seq=11 Destination unreachable: No route
From 2001:1:1:1 icmp_seq=12 Destination unreachable: No route
From 2001:1:1:1 icmp_seq=13 Destination unreachable: No route
From 2001:1:1:1 icmp_seq=14 Destination unreachable: No route
From 2001:1:1:1 icmp_seq=15 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=16 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=17 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=18 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=19 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=20 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=21 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=22 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=23 Destination unreachable: No route
From 2001:1:6:6 icmp_seq=24 Destination unreachable: No route
64 bytes from 2001:3:3:10: icmp_seq=25 ttl=60 time=7.38 ms
64 bytes from 2001:3:3:10: icmp_seq=26 ttl=60 time=10.4 ms
64 bytes from 2001:3:3:10: icmp_seq=27 ttl=60 time=2.32 ms
64 bytes from 2001:3:3:10: icmp_seq=28 ttl=60 time=1.35 ms
64 bytes from 2001:3:3:10: icmp_seq=29 ttl=60 time=1.39 ms
64 bytes from 2001:3:3:10: icmp_seq=30 ttl=60 time=6.83 ms
64 bytes from 2001:3:3:10: icmp_seq=31 ttl=60 time=1.42 ms
64 bytes from 2001:3:3:10: icmp_seq=32 ttl=60 time=4.16 ms
64 bytes from 2001:3:3:10: icmp_seq=33 ttl=60 time=1.44 ms

Ubuntu PC1 [Comando] - Oracle VM VirtualBox
Terminal
rtsp://[FF7e:140:2001:1:1::]:5004 - Reproductor m
pc1@pc1-VirtualBox: ~
PING 2001:1:1:10(2001:1:1:10) 56 data bytes
From 2001:3:3:3 icmp_seq=2 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=3 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=4 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=5 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=6 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=7 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=8 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=9 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=10 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=11 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=12 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=13 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=14 Destination unreachable: No route
From 2001:3:3:3 icmp_seq=15 Destination unreachable: No route
64 bytes from 2001:1:1:10: icmp_seq=24 ttl=60 time=2.25 ms
64 bytes from 2001:1:1:10: icmp_seq=25 ttl=60 time=1.30 ms
64 bytes from 2001:1:1:10: icmp_seq=26 ttl=60 time=1.49 ms
64 bytes from 2001:1:1:10: icmp_seq=27 ttl=60 time=1.35 ms
64 bytes from 2001:1:1:10: icmp_seq=28 ttl=60 time=5.33 ms
64 bytes from 2001:1:1:10: icmp_seq=29 ttl=60 time=1.48 ms
64 bytes from 2001:1:1:10: icmp_seq=30 ttl=60 time=24.7 ms
64 bytes from 2001:1:1:10: icmp_seq=31 ttl=60 time=1.29 ms
  
```

Figura 2.37: Paquetes ICMP enviados mediante el comando PING desde el Server VLC hacia el Cliente PC1 y viceversa.

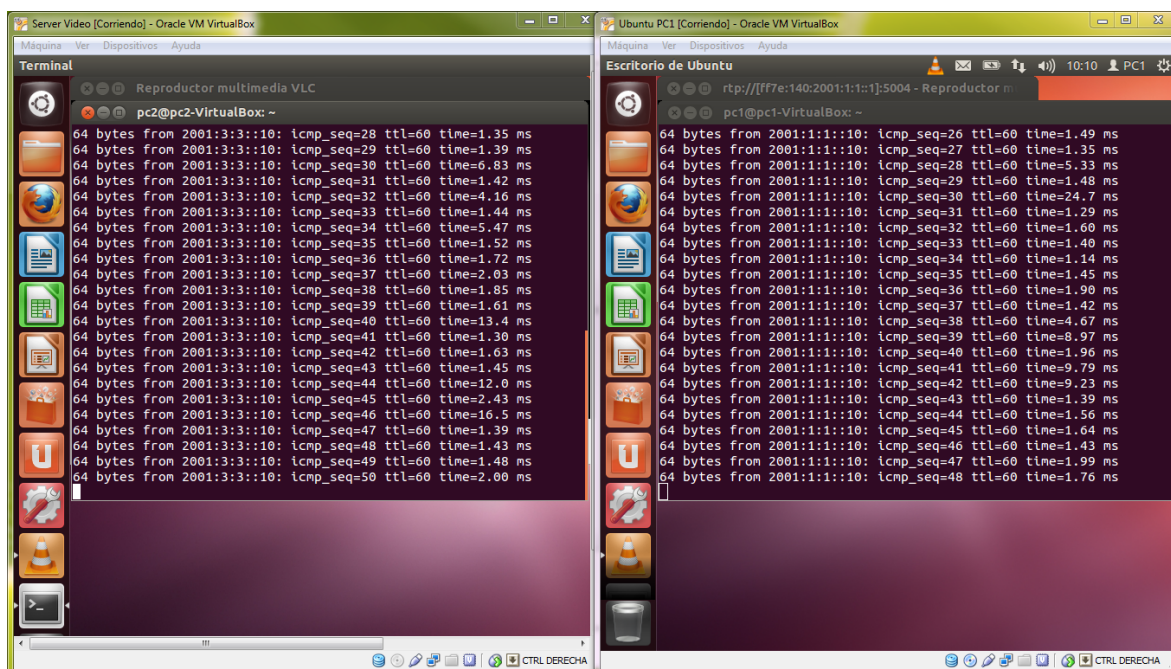


Figura 2.38: Paquetes ICMP enviados mediante el comando PING desde el Server VLC hacia el Cliente PC1 y viceversa.

Con el fin de validar los datos del retardo y llegar a un valor promedio, se ha realizado la toma de retardos en 3 pruebas para cada cliente (PC1 y PC5).

A continuación se presente una tabla con los valores de ping que se obtuvo en esta topología:

PRUEBA N° 1				
N°	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
1	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
2	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
8	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
9	NO ROUTE	2,25	NO ROUTE	NO ROUTE
10	7,38	1,30	NO ROUTE	NO ROUTE
11	10,40	1,49	NO ROUTE	NO ROUTE
12	2,32	1,35	17,90	NO ROUTE
13	1,35	5,33	1,45	1,39
14	1,39	1,48	1,48	1,58
15	6,83	24,70	1,36	1,85
16	1,42	1,29	11,50	10,50
17	4,16	1,60	12,30	3,67
18	1,44	1,40	2,43	1,41
19	5,47	1,14	2,51	3,75
20	1,52	1,45	1,51	1,41
21	1,72	1,90	1,41	1,44
22	2,03	1,42	1,40	1,53
23	1,85	4,67	1,75	10,90
24	1,61	8,97	1,46	1,53
25	13,40	1,96	1,17	10,90
26	1,30	9,79	1,36	1,53
27	1,63	9,23	13,10	1,48
28	1,45	1,39	2,62	1,66
29	12,00	1,56	12,10	11,10
30	2,43	1,64	1,50	1,81
31	16,50	1,43	16,00	1,77
32	1,39	1,99	7,04	1,62
33	1,43	1,76	1,88	1,38
34	1,48	1,42	1,46	1,66
35	2,00	1,40	1,45	7,31
36	1,76	1,69	1,51	1,42
37	2,10	1,46	1,41	2,36
38	1,38	1,38	9,78	1,50
39	3,13	1,52	1,49	1,73
40	1,50	1,48	1,50	1,47
41	5,36	1,40	1,79	1,40
42	1,44	1,73	1,47	1,50
43	1,51	4,78	1,54	1,73
44	1,81	1,40	1,40	1,47
45	24,80	4,84	15,40	1,40
46	1,37	1,41	18,60	1,53
47	8,34	4,05	5,71	1,59
48	1,86	1,49	1,99	1,42
49	1,48	1,59	1,56	11,40
50	1,36	1,47	2,12	1,50

**Tabla 2.14: Tabla de valores de tiempos de retardo,
Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.**

PRUEBA N° 2				
N°	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
1	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
2	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
8	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
9	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
10	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
11	NO ROUTE	NO ROUTE	1,26	10,20
12	NO ROUTE	18,80	1,89	9,64
13	NO ROUTE	2,22	3,62	12,90
14	1,51	3,37	1,30	1,84
15	11,70	1,48	1,29	19,90
16	1,52	2,30	1,28	4,75
17	1,59	2,61	1,24	1,70
18	19,50	1,54	1,30	3,87
19	1,58	12,30	1,35	1,13
20	1,86	1,49	1,25	11,40
21	1,55	1,56	11,40	1,28
22	1,72	1,48	1,40	1,27
23	9,82	17,70	1,38	1,40
24	1,55	1,46	1,15	1,52
25	2,47	1,46	8,62	11,40
26	1,52	2,50	1,19	7,53
27	1,54	1,87	1,24	1,28
28	1,43	1,13	1,24	1,21
29	24,00	1,70	1,27	10,70
30	1,56	7,17	7,93	1,20
31	1,50	1,47	7,27	1,27
32	1,61	1,55	1,29	1,24
33	1,69	22,30	1,31	1,51
34	1,83	1,63	1,40	1,35
35	1,53	1,75	1,27	1,58
36	1,44	1,62	1,27	1,31
37	1,72	2,34	1,25	1,99
38	1,39	2,25	1,27	1,30
39	1,51	1,50	1,30	1,20
40	1,57	1,53	1,25	1,28
41	1,35	1,66	1,18	1,28
42	2,01	1,28	1,27	1,30
43	1,49	9,58	1,30	1,83
44	1,72	1,54	1,25	15,50
45	1,92	1,44	1,18	20,10
46	1,48	6,32	1,27	4,50
47	4,42	14,00	1,42	1,69
48	2,03	1,78	1,22	1,35
49	1,88	2,10	1,30	1,46
50	1,78	1,98	1,25	1,38

Tabla 2.15: Tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3				
N°	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
1	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
2	NO ROUTE	NO ROUTE	NO ROUTE	NO ROUTE
8	NO ROUTE	NO ROUTE	22	NO ROUTE
9	NO ROUTE	NO ROUTE	22,6	NO ROUTE
10	8,94	NO ROUTE	1,50	NO ROUTE
11	10,40	NO ROUTE	1,81	6,88
12	1,40	15,2	2,16	7,41
13	1,48	20,80	1,41	1,61
14	10,10	1,38	1,43	21,40
15	1,54	1,48	19,50	14,80
16	1,46	1,63	1,47	1,39
17	1,44	16,50	1,71	1,75
18	1,66	9,67	1,43	4,70
19	1,52	7,46	1,40	1,45
20	1,45	1,39	1,75	7,13
21	1,81	1,60	1,47	5,26
22	1,49	1,73	1,79	2,20
23	1,68	1,41	1,54	1,36
24	1,63	1,48	1,42	1,34
25	9,70	1,53	1,53	18,50
26	1,45	12,40	2,03	7,64
27	1,73	1,54	3,71	1,86
28	16,10	1,49	1,99	1,55
29	9,44	1,60	1,64	1,46
30	16,80	1,49	1,45	33,50
31	1,56	9,23	1,54	1,76
32	1,59	1,62	1,54	1,74
33	1,80	2,19	1,39	1,59
34	2,15	1,75	1,51	1,45
35	1,66	1,53	1,41	1,45
36	1,52	1,51	2,45	1,48
37	1,75	1,48	1,77	1,50
38	1,59	1,43	1,44	1,44
39	1,69	1,54	1,51	1,39
40	1,45	2,50	1,59	5,25
41	1,49	1,59	2,31	2,70
42	1,08	2,39	1,99	1,60
43	1,95	1,61	1,40	1,71
44	13,90	1,66	1,78	2,05
45	1,66	1,62	2,24	14,10
46	8,78	33,00	1,59	7,46
47	1,72	25,30	1,41	6,03
48	1,53	1,50	1,44	1,45
49	2,01	20,40	1,46	1,51
50	1,67	9,84	1,52	1,40

Tabla 2.16: Tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 1	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg.)	165,10	127,00	185,41	116,60
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	41,00	42,00	39,00	38,00
PAQUETES PERDIDOS	9,00	8,00	11,00	12,00
PORCENTAJE DE PAQUETES PERDIDOS %	21,95	19,05	28,21	31,58
PAQUETE MIN TIEMPO (mseg.)	1,30	1,14	1,17	1,38
PAQUETE MAX TIEMPO (mseg.)	24,80	24,70	18,60	11,40
PAQUETE TIEMPO PROMEDIO (mseg.)	4,03	3,02	4,75	3,07

Tabla 2.17: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 2	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg.)	122,29	163,76	84,12	180,54
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	37,00	39,00	40,00	40,00
PAQUETES PERDIDOS	13,00	11,00	10,00	10,00
PORCENTAJE DE PAQUETES PERDIDOS %	35,14	28,21	25,00	25,00
PAQUETE MIN TIEMPO (mseg.)	1,30	1,14	1,17	1,38
PAQUETE MAX TIEMPO (mseg.)	24,80	24,70	18,60	11,40
PAQUETE TIEMPO PROMEDIO (mseg.)	4,21	5,78	3,30	5,06

Tabla 2.18: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg.)	155,77	225,47	132,03	202,25
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	40,00	38,00	42,00	41,00
PAQUETES PERDIDOS	10,00	12,00	8,00	9,00
PORCENTAJE DE PAQUETES PERDIDOS %	25,00	31,58	19,05	21,95
PAQUETE MIN TIEMPO (mseg.)	1,08	1,38	1,39	1,34
PAQUETE MAX TIEMPO (mseg.)	16,80	33,00	22,60	33,50
PAQUETE TIEMPO PROMEDIO (mseg.)	3,89	5,93	3,14	4,93

Tabla 2.19: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

A continuación se presenta un cuadro con el resumen de las 3 pruebas realizadas mediante el comando PING.

RESUMEN	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	443,16	516,23	401,56	499,39
PAQUETES TRANSMITIDOS	150,00	150,00	150,00	150,00
PAQUETES RECIBIDOS	118,00	119,00	121,00	119,00
PAQUETES PERDIDOS	32,00	31,00	29,00	31,00
PORCENTAJE DE PAQUETES PERDIDOS %	21,33	20,67	19,33	20,67
PAQUETE MIN TIEMPO (mseg)	1,08	1,14	1,17	1,34
PAQUETE MAX TIEMPO (mseg)	24,80	33,00	22,60	33,50
PAQUETE TIEMPO PROMEDIO (mseg)	4,04	4,91	3,73	4,35

Tabla 2.20: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING para cada cliente (PC1 y PC5) que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 4.04 mseg.
- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 4.91 mseg.
- Latencia calculada desde el Server VLC a Cliente PC5
Latencia = 3.73 mseg.
- Latencia calculada desde el Cliente PC5 al Server VLC
Latencia = 4.35 mseg.

2.2.1.4.3 Cálculos de Jitter

El JITTER es la variación del retardo o Latencia, por tanto, para calcular el Jitter debemos ayudarnos de la tabla 2.21, donde podemos calcular la variación de los tiempos ahí capturados:

CALCULO DE JITTER						
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER	CLIENTE PC5	JITTER
14	1,39	-0,04	1,48	3,85	1,58	-0,19
15	6,83	-5,44	24,70	-23,22	1,85	-0,27
16	1,42	5,41	1,29	23,41	10,50	-8,65
17	4,16	-2,74	1,60	-0,31	3,67	6,83
18	1,44	2,72	1,40	0,20	1,41	2,26
19	5,47	-4,03	1,14	0,26	3,75	-2,34
20	1,52	3,95	1,45	-0,31	1,41	2,34
21	1,72	-0,20	1,90	-0,45	1,44	-0,03
22	2,03	-0,31	1,42	0,48	1,53	-0,09
23	1,85	0,18	4,67	-3,25	10,90	-9,37
24	1,61	0,24	8,97	-4,30	1,53	9,37
25	13,40	-11,79	1,96	7,01	10,90	-9,37
26	1,30	12,10	9,79	-7,83	1,53	9,37
27	1,63	-0,33	9,23	0,56	1,48	0,05
28	1,45	0,18	1,39	7,84	1,66	-0,18
29	12,00	-10,55	1,56	-0,17	11,10	-9,44
30	2,43	9,57	1,64	-0,08	1,81	9,29
31	16,50	-14,07	1,43	0,21	1,77	0,04
32	1,39	15,11	1,99	-0,56	1,62	0,15
33	1,43	-0,04	1,76	0,23	1,38	0,24
34	1,48	-0,05	1,42	0,34	1,66	-0,28
35	2,00	-0,52	1,40	0,02	7,31	-5,65
36	1,76	0,24	1,69	-0,29	1,42	5,89
37	2,10	-0,34	1,46	0,23	2,36	-0,94
38	1,38	0,72	1,38	0,08	1,50	0,86
39	3,13	-1,75	1,52	-0,14	1,73	-0,23
40	1,50	1,63	1,48	0,04	1,47	0,26
41	5,36	-3,86	1,40	0,08	1,40	0,07
42	1,44	3,92	1,73	-0,33	1,50	-0,10
43	1,51	-0,07	4,78	-3,05	1,73	-0,23
44	1,81	-0,30	1,40	3,38	1,47	0,26
45	24,80	-22,99	4,84	-3,44	1,40	0,07
46	1,37	23,43	1,41	3,43	1,53	-0,13
47	8,34	-6,97	4,05	-2,64	1,59	-0,06
48	1,86	6,48	1,49	2,56	1,42	0,17
49	1,48	0,38	1,59	-0,10	11,40	-9,98
50	1,36	0,12	1,47	0,12	1,50	9,90
JITTER MIN (ms)		-22,99		-23,22		-9,98
JITTER MAX (ms)		23,43		23,41		9,90

Tabla 2.21: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

2.2.1.4.4 Cálculos de Pérdida de Paquetes

Para el cálculo de Pérdida de Paquetes, debemos recordar que esta práctica está hecha en un ambiente puramente virtual, es decir las condiciones de la transmisión del streaming de video son ideales.

Al tener condiciones ideales, y en base a los datos obtenidos anteriormente en las tablas, podemos ver que no existe pérdida de paquetes.

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING			
TOPOLOGIA:	6 ROUTERS TIPO MALLA		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	2 min 42 seg.	2 min 42 seg.	2 min 42 seg.
TIEMPO EN SEGUNDOS:	162.889 seg.	162.121 seg.	162.889 seg.
PAQUETES CAPTURADOS:	8199.00	8156.00	8199.00
PAQUETES MOSTRADOS:	8199.00	8156.00	8199.00
BYTES TOTALES:	11160876.00	11105034.00	11160876.00
PROMEDIO PAQUETES/SEG:	50335.00	50308.00	50335.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.361.248	1.361.578	1.361.248
PROMEDIO BYTES/SEG:	68.518.292	68.498.430	68.518.292
PROMEDIO MBITS/SEG:	0,548	0,548	0,548

Tabla 2.22: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la topología tipo malla.

Los paquetes capturados junto con los paquetes mostrados y los bytes totales, son exactamente iguales en el caso del Server VLC, Cliente PC5 y Cliente PC1.

Por tanto no hay pérdida de paquetes.

2.2.2 TOPOLOGÍA TIPO ESTRELLA A IMPLEMENTAR

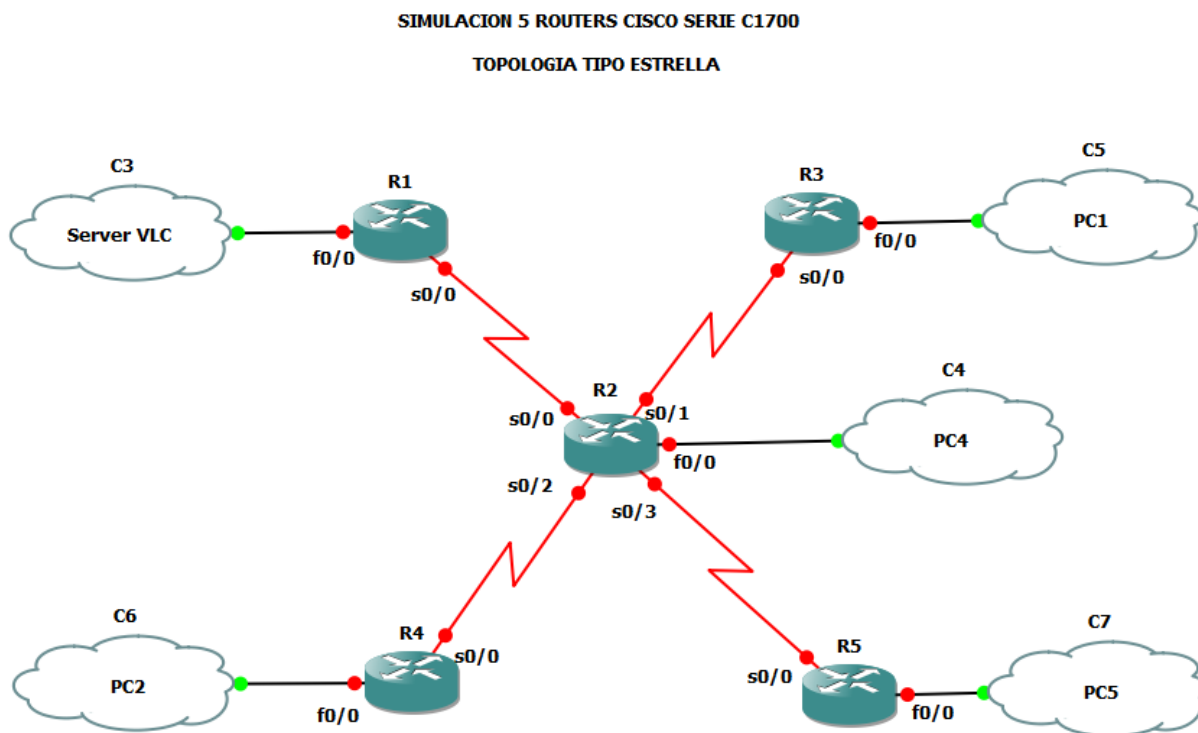


Figura 2.39: Diagrama de la topología tipo estrella a implementar.

2.2.2.1 Direccionamiento de la topología tipo estrella

DISPOSITIVO	DIRECCION IPV6	GATEWAY
Server VLC	2001:1:1::10/64	2001:1:1::1
CLIENTE PC1	2001:3:3::10/64	2001:3:3::3
CLIENTE PC2	2001:4:4::10/64	2001:4:4::4
CLIENTE PC4	2001:2:2::10/64	2001:2:2::2
CLIENTE PC5	2001:5:5::10/64	2001:5:5::5
ROUTER R1		
Fastethernet 0/0	2001:1:1::1/64	
Serial 0/0	2001:1:2::1/64	
ROUTER R2		
Fastethernet 0/0	2001:2:2::2/64	
Serial 0/0	2001:1:2::2/64	
Serial 0/1	2001:2:3::2/64	
Serial 0/2	2001:2:4::2/64	
Serial 0/3	2001:2:5::2/64	
ROUTER R3		
Fastethernet 0/0	2001:3:3::3/64	
Serial 0/0	2001:2:3::3/64	
ROUTER R4		
Fastethernet 0/0	2001:4:4::4/64	
Serial 0/0	2001:2:4::4/64	
ROUTER R5		
Fastethernet 0/0	2001:5:5::5/64	
Serial 0/0	2001:2:5::5/64	
DIRECCION EMBEDDED MULTICAST A UTILIZAR		
Grupo Multicast Embedded	FF07:140:2001:1:1::1	
PROCOLO DE ENRUTAMIENTO UTILIZADO		
PROTOCOLO:	OSPFv6	
GRUPO:	1	
AREA:	0	
ROUTERS IMPLEMENTADOS:	Todos los Routers de la red de distribución	
RP SELECCIONADO		
ROUTER:	R1 (Conectado directamente al Server VLC)	

Tabla 2.23: Direccionamiento de la topología tipo estrella.

2.2.2.2 Capturas de pantalla de la red de distribución

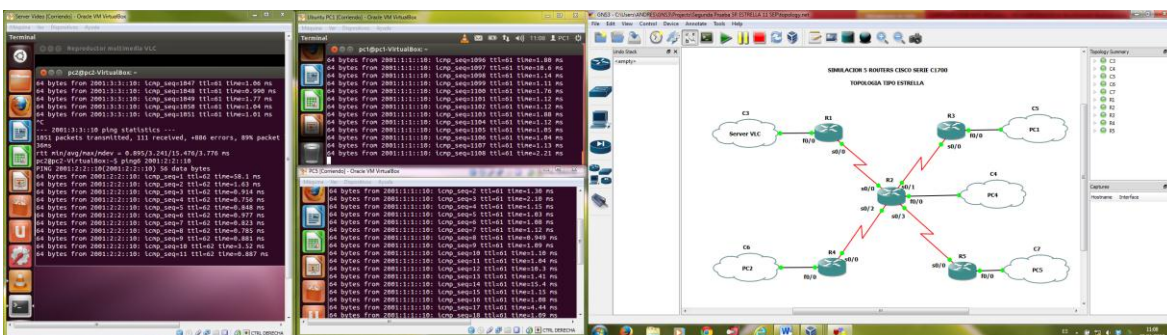


Figura 2.40: Paquetes ICMP enviados mediante el comando PING desde el Server VLC hacia los Clientes PC1 y PC5 y viceversa.

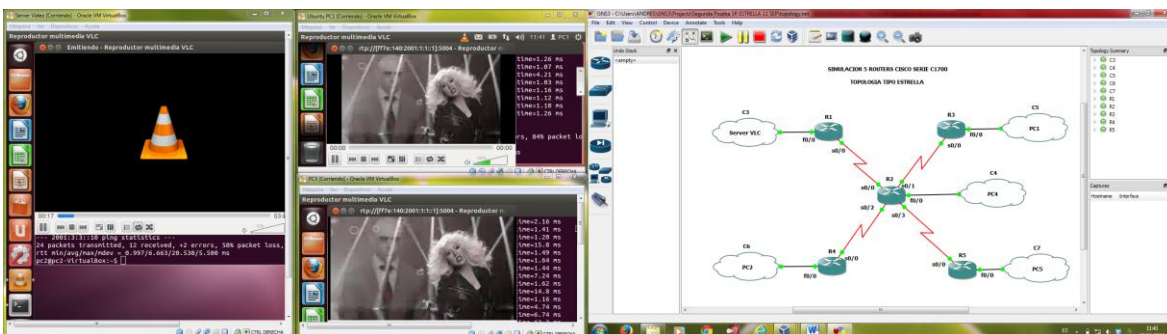


Figura 2.41: Recepción del streaming de video desde el Server VLC hacia los Clientes PC1 y PC5

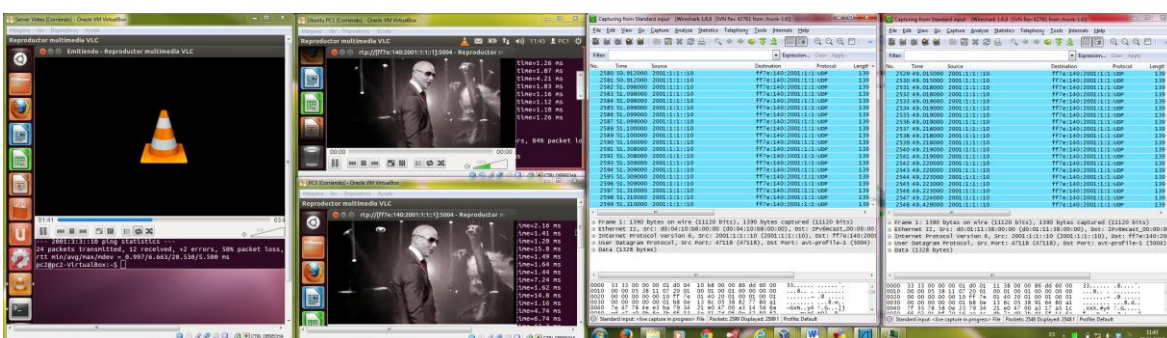


Figura 2.42: Paquetes UDP transmitidos desde el Server VLC hacia los Clientes PC1 y PC5 capturados con Wireshark

Datos recogidos mediante WIRESHARK durante la transmisión del streaming de video.

SERVER VLC

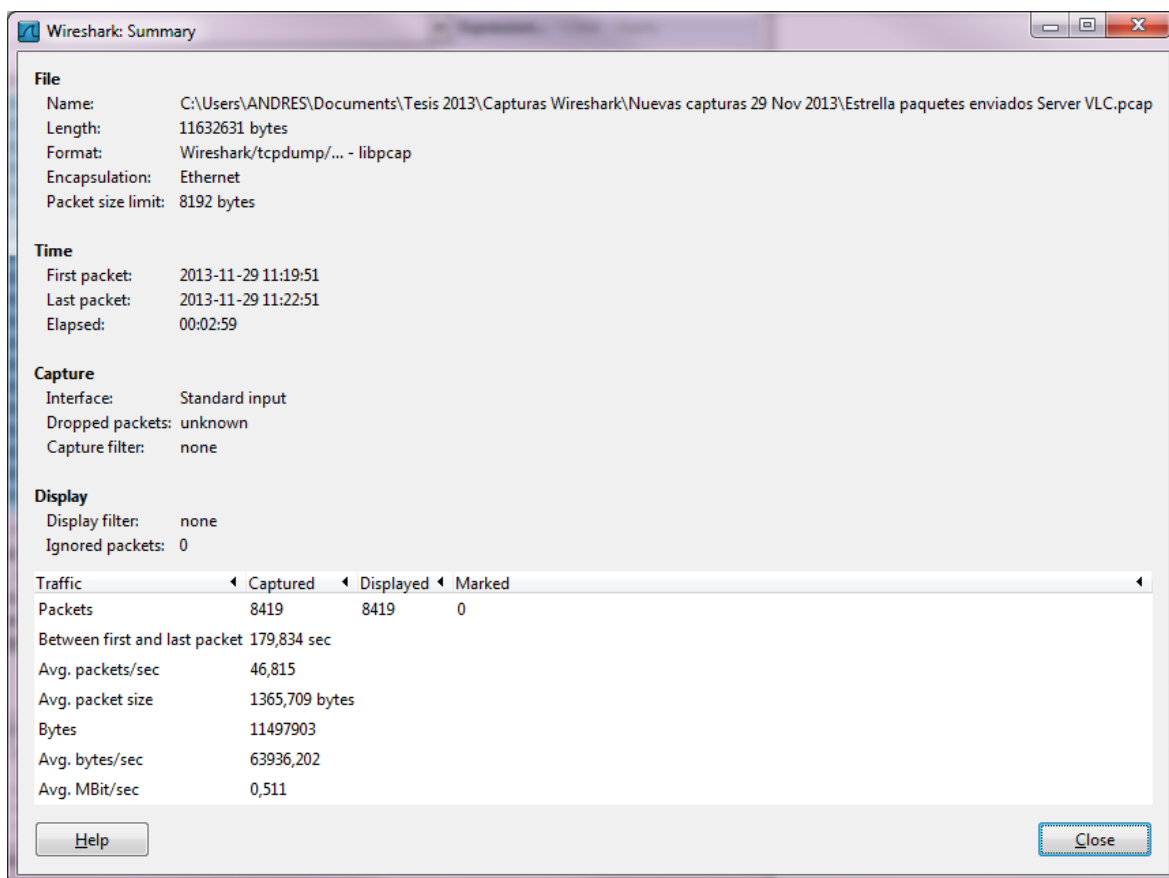


Figura 2.43: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	2 min 59 seg.
TIEMPO EN SEGUNDOS:	179.834 seg.
PAQUETES CAPTURADOS:	8419.00
PAQUETES MOSTRADOS:	8419.00
BYTES TOTALES:	11497903.00
PROMEDIO PAQUETES/SEG:	50335.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1361.248
PROMEDIO BYTES/SEG:	63936.202
PROMEDIO MBITS/SEG:	0,511

Tabla 2.24: Resumen de los datos mostrados en Wireshark

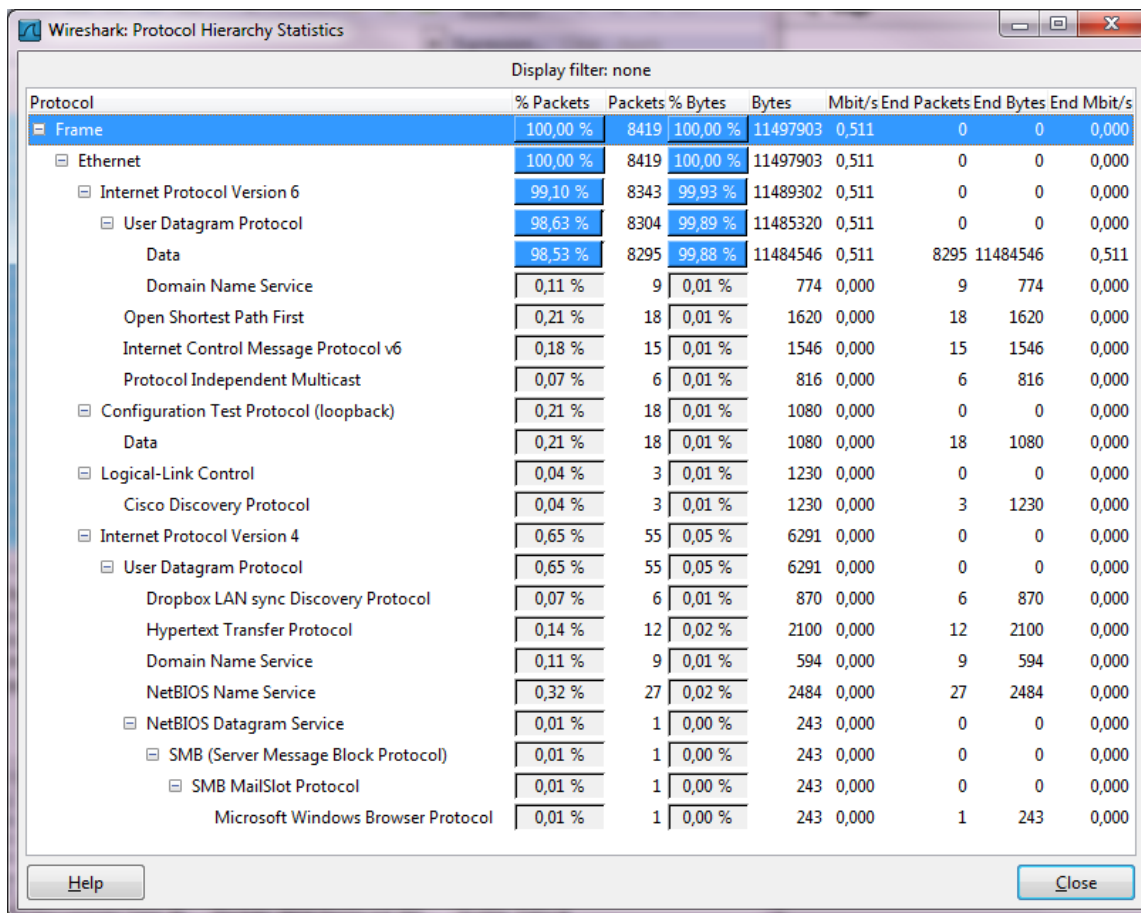


Figura 2.44: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.44 se encuentra en la página 103

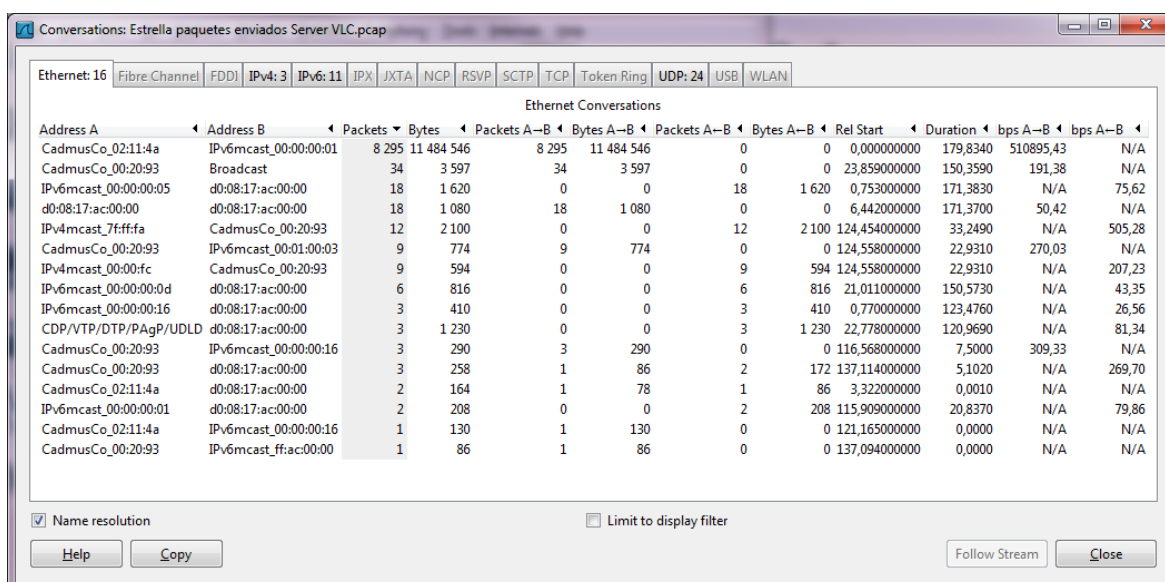


Figura 2.45: Paquetes Ethernet que atravesaron la red al momento de la captura

* La explicación de la figura 2.45 se encuentra en la página 104

Conversations: Estrella paquetes enviados Server VLC.pcap

Ethernet: 16 Fibre Channel FDDI IPv4: 3 IPv6: 11 IPX JXTA NCP RSVP SCTP TCP Token Ring UDP: 24 USB WLAN

IPv6 Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	ff7e:140:2001:1:1::1	8 295	11 484 546	8 295	11 484 546	0	0	0,000000000	179,8340	510895,43	N/A
fe80::d208:17ff:feac:0	ff02::5	18	1 620	18	1 620	0	0	0,753000000	171,3830	75,62	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:3	9	774	9	774	0	0	124,558000000	22,9310	270,03	N/A
fe80::d208:17ff:feac:0	ff02::d	6	816	6	816	0	0	21,011000000	150,5730	43,35	N/A
fe80::d208:17ff:feac:0	ff02::16	3	410	3	410	0	0	0,770000000	123,4760	26,56	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::16	3	290	3	290	0	0	116,568000000	7,5000	309,33	N/A
fe80::c5d6:8a3:f8d5:1fe8	fe80::d208:17ff:feac:0	3	258	1	86	2	172	137,114000000	5,1020	N/A	269,70
fe80::a00:27ff:fe02:114a	fe80::d208:17ff:feac:0	2	164	1	78	1	86	3,322000000	0,0010	N/A	N/A
fe80::d208:17ff:feac:0	ff02::1	2	208	2	208	0	0	115,909000000	20,8370	79,86	N/A
fe80::a00:27ff:fe02:114a	ff02::16	1	130	1	130	0	0	121,165000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:ffac:0	1	86	1	86	0	0	137,094000000	0,0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 2.46: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 2.46 se encuentra en la página 105

Conversations: Estrella paquetes enviados Server VLC.pcap

Ethernet: 16 Fibre Channel FDDI IPv4: 3 IPv6: 11 IPX JXTA NCP RSVP SCTP TCP Token Ring UDP: 24 USB WLAN

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	47118	ff7e:140:2001:1:1::1	avt-profile-1	8 259	11 480 010	8 259	11 480 010	0	0	0,000000000	179,8340	510693,64	N/A
2001:1:1::10	47119	ff7e:140:2001:1:1::1	avt-profile-2	36	4 536	36	4 536	0	0	3,796000000	175,0090	207,35	N/A
192.168.199.1	netbios-ns	192.168.199.255	netbios-ns	27	2 484	27	2 484	0	0	124,764000000	24,4220	813,69	N/A
192.168.199.1	60021	239.255.255.250	ssdp	12	2 100	12	2 100	0	0	124,454000000	33,2490	505,28	N/A
192.168.199.1	db-lsp-disc	192.168.199.255	db-lsp-disc	6	870	6	870	0	0	23,859000000	150,3590	46,29	N/A
fe80::c5d6:8a3:f8d5:1fe8	63366	ff02::1:3	llmnr	1	86	1	86	0	0	124,558000000	0,0000	N/A	N/A
192.168.199.1	53917	224.0.0.252	llmnr	1	66	1	66	0	0	124,558000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	56839	ff02::1:3	llmnr	1	86	1	86	0	0	127,111000000	0,0000	N/A	N/A
192.168.199.1	49553	224.0.0.252	llmnr	1	66	1	66	0	0	127,111000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	51881	ff02::1:3	llmnr	1	86	1	86	0	0	132,026000000	0,0000	N/A	N/A
192.168.199.1	58734	224.0.0.252	llmnr	1	66	1	66	0	0	132,027000000	0,0000	N/A	N/A
192.168.199.1	netbios-dgm	192.168.199.255	netbios-dgm	1	243	1	243	0	0	132,674000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	59696	ff02::1:3	llmnr	1	86	1	86	0	0	134,572000000	0,0000	N/A	N/A
192.168.199.1	64103	224.0.0.252	llmnr	1	66	1	66	0	0	134,572000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	55635	ff02::1:3	llmnr	1	86	1	86	0	0	137,220000000	0,0000	N/A	N/A
192.168.199.1	59375	224.0.0.252	llmnr	1	66	1	66	0	0	137,220000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	51794	ff02::1:3	llmnr	1	86	1	86	0	0	139,789000000	0,0000	N/A	N/A
192.168.199.1	49312	224.0.0.252	llmnr	1	66	1	66	0	0	139,789000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	60433	ff02::1:3	llmnr	1	86	1	86	0	0	142,370000000	0,0000	N/A	N/A
192.168.199.1	49535	224.0.0.252	llmnr	1	66	1	66	0	0	142,370000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	61105	ff02::1:3	llmnr	1	86	1	86	0	0	144,973000000	0,0000	N/A	N/A
192.168.199.1	55238	224.0.0.252	llmnr	1	66	1	66	0	0	144,973000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	49457	ff02::1:3	llmnr	1	86	1	86	0	0	147,489000000	0,0000	N/A	N/A
192.168.199.1	56053	224.0.0.252	llmnr	1	66	1	66	0	0	147,489000000	0,0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 2.47: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.47 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	8419	0,046815	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	28	0,000156	0,33%
80-159	115	0,000639	1,37%
160-319	14	0,000078	0,17%
320-639	3	0,000017	0,04%
640-1279	0	0,000000	0,00%
1280-2559	8259	0,045926	98,10%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.48: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.48 se encuentra en la página 106

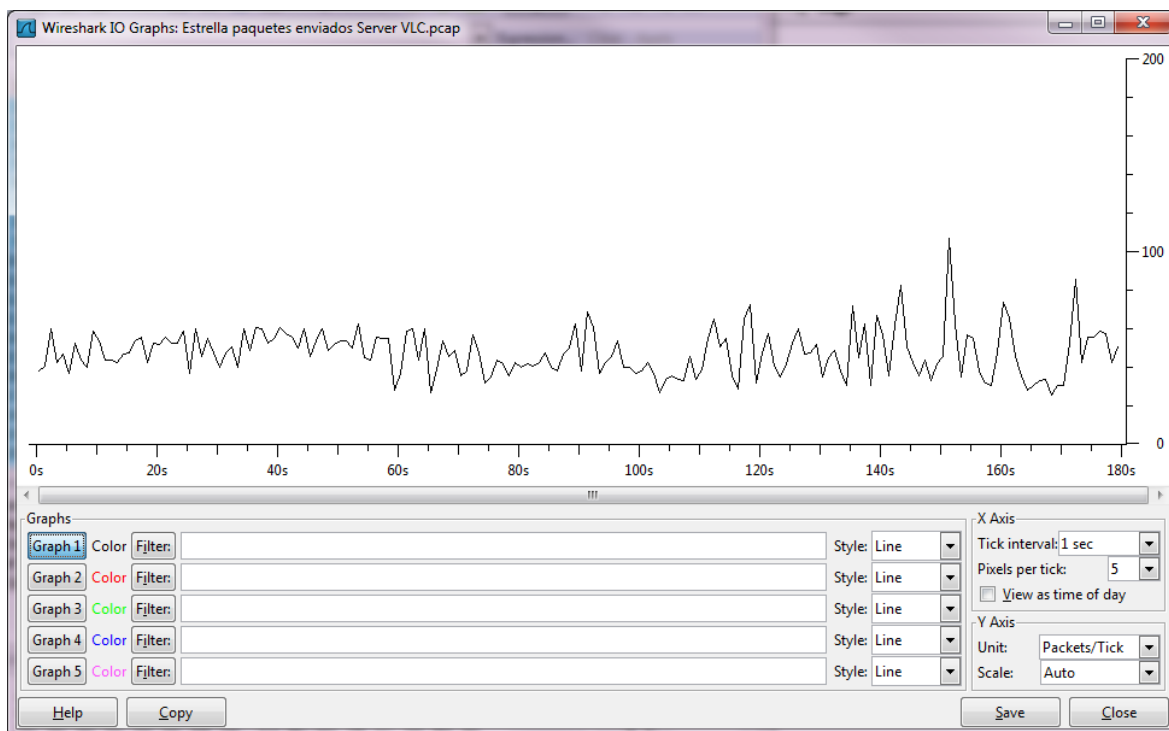


Figura 2.49: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC5

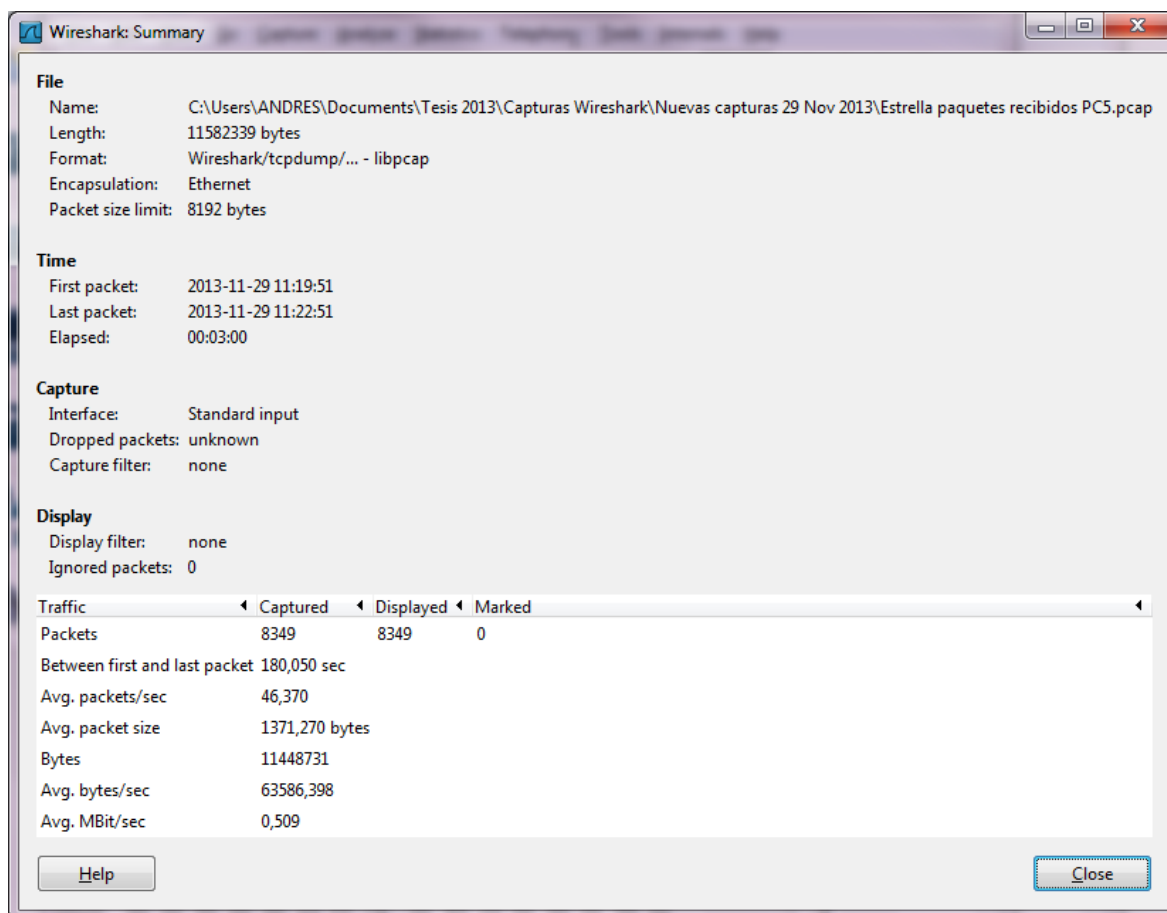


Figura 2.50: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1.

PC:	CLIENTE PC5
INTERFACE:	Fastethernet R5
TIEMPO DE CAPTURA DE PAQUETES:	3 min 0 seg.
TIEMPO EN SEGUNDOS:	180.050 seg.
PAQUETES CAPTURADOS:	8349.00
PAQUETES MOSTRADOS:	8349.00
BYTES TOTALES:	11448731.00
PROMEDIO PAQUETES/SEG:	46370.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1371.270
PROMEDIO BYTES/SEG:	63586.398
PROMEDIO MBITS/SEG:	0,509

Tabla 2.25: Resumen de los datos mostrados en Wireshark.

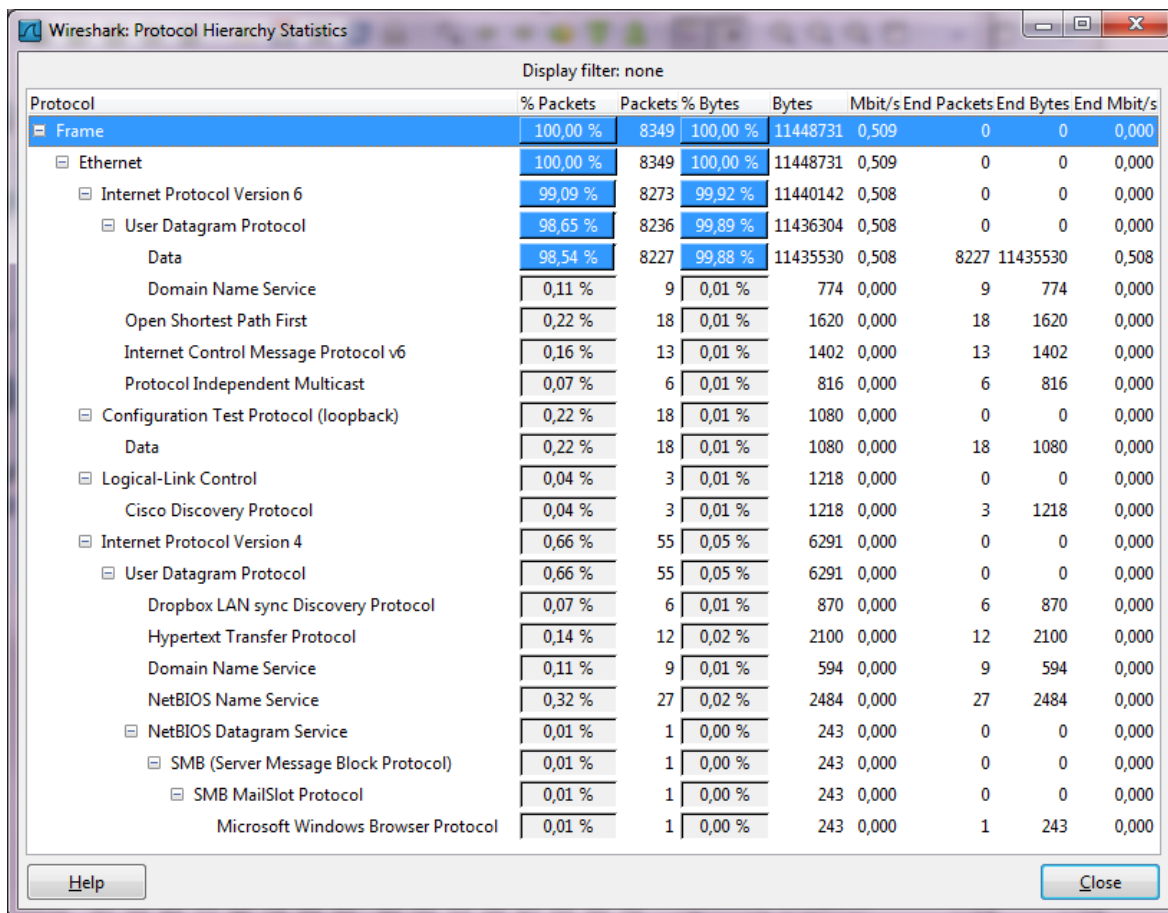


Figura 2.51: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.51 se encuentra en la página 103

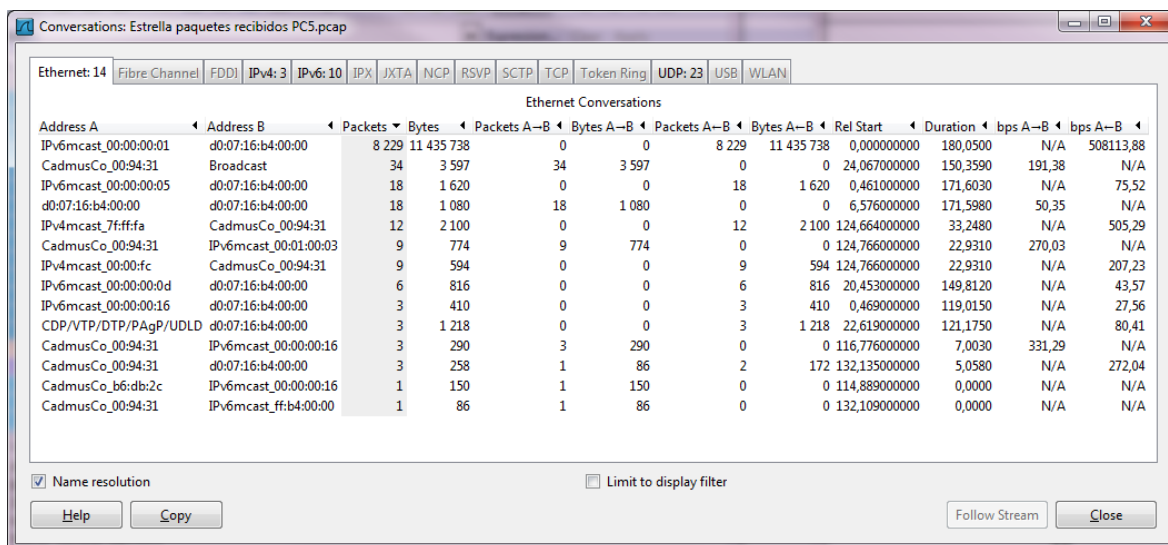


Figura 2.52: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 2.52 se encuentra en la página 104

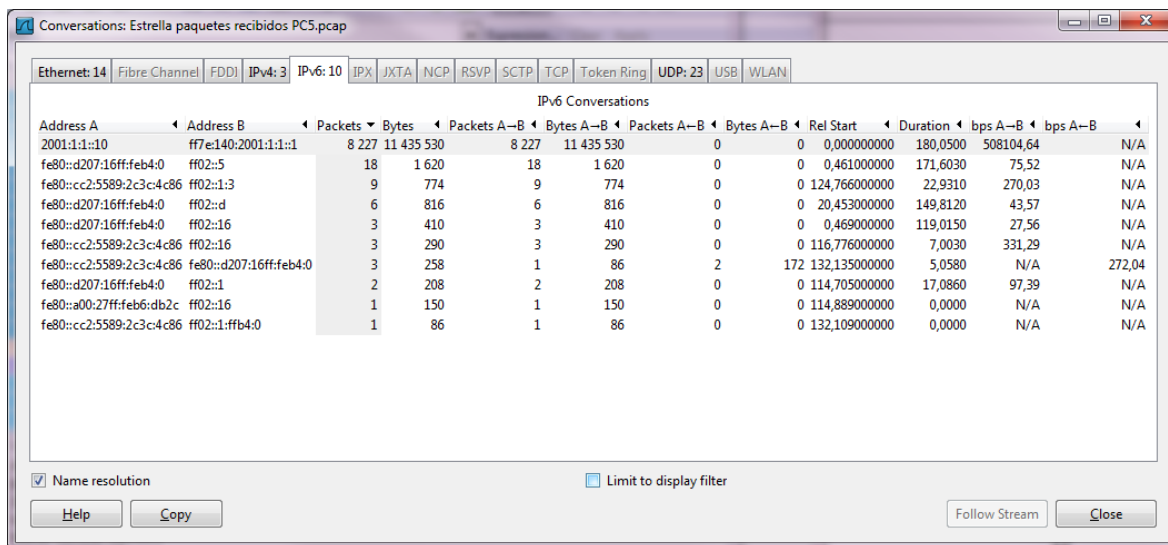


Figura 2.53: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 2.53 se encuentra en la página 105

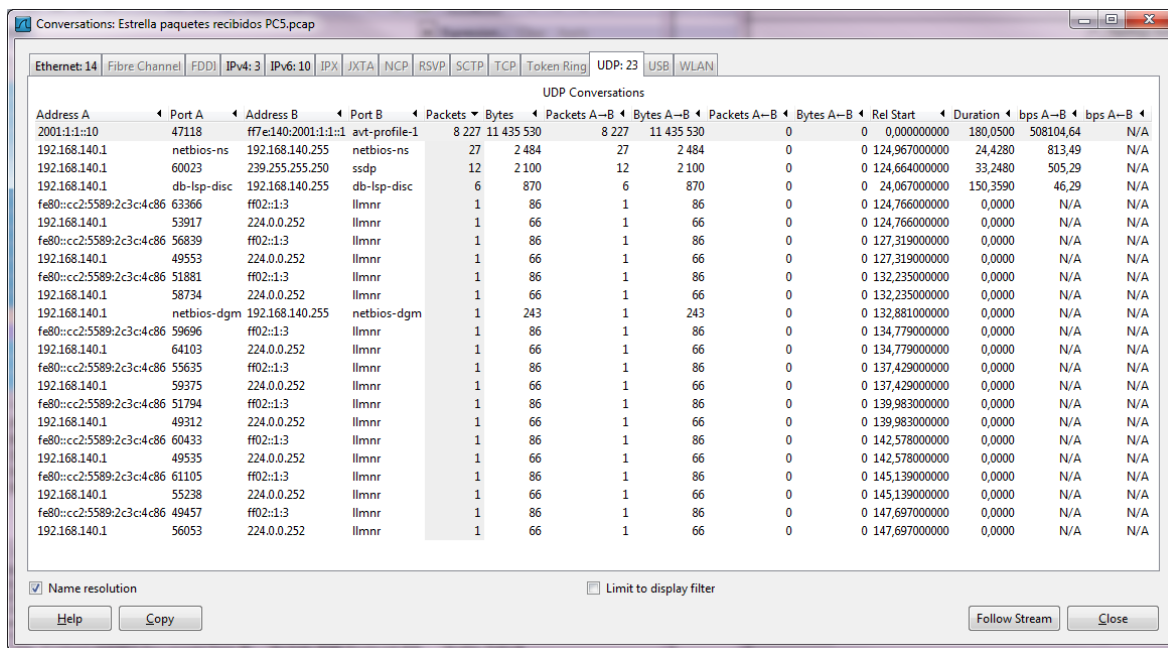


Figura 2.54: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.54 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	8349	0,046370	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	27	0,000150	0,32%
80-159	78	0,000433	0,93%
160-319	14	0,000078	0,17%
320-639	3	0,000017	0,04%
640-1279	0	0,000000	0,00%
1280-2559	8227	0,045693	98,54%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.55: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.55 se encuentra en la página 106

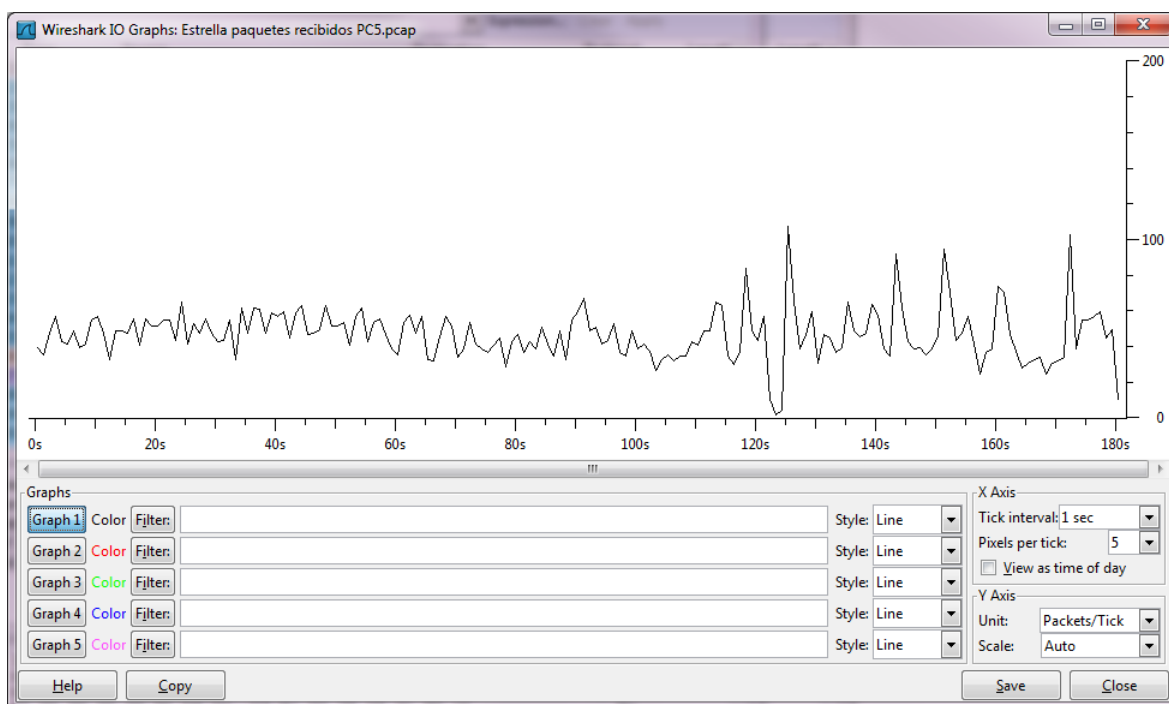


Figura 2.56: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC1

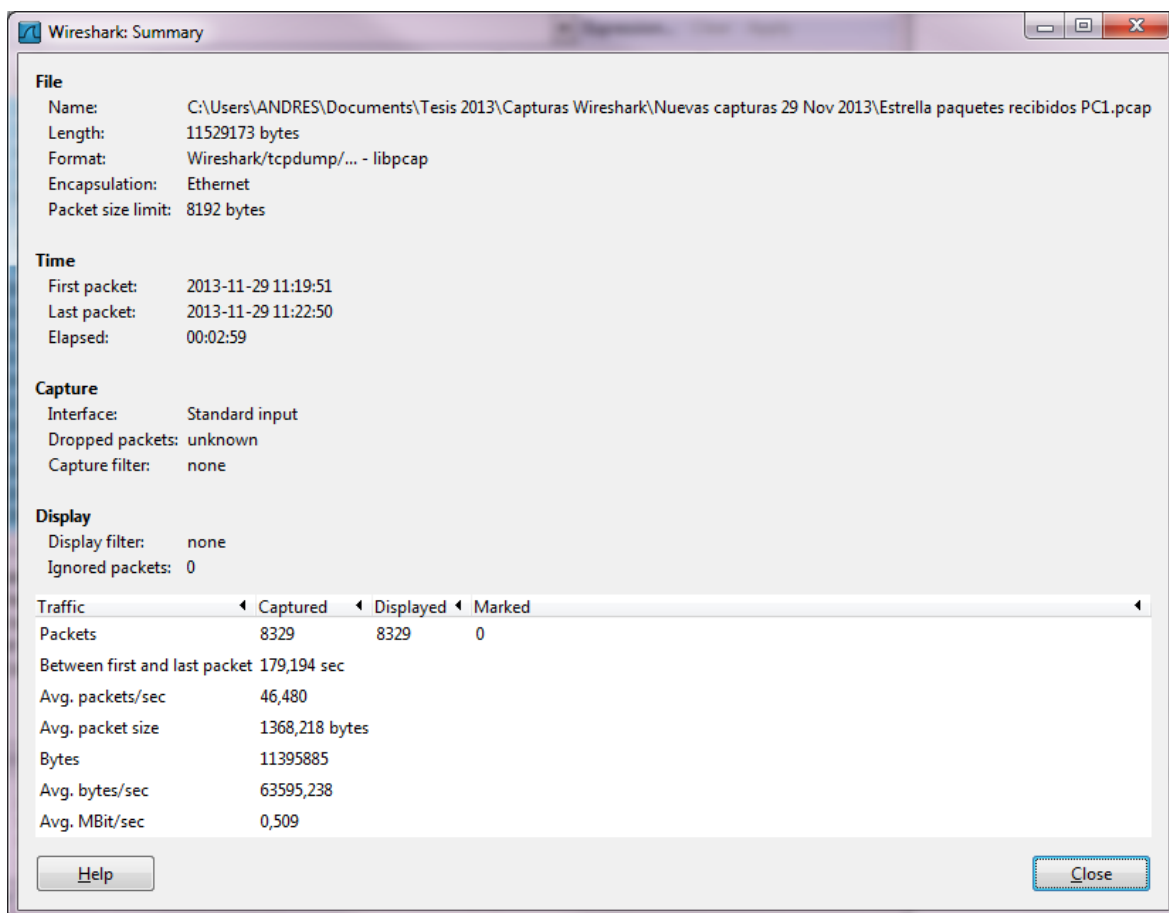


Figura 2.57: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1.

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	2 min 59 seg.
TIEMPO EN SEGUNDOS:	179.194 seg.
PAQUETES CAPTURADOS:	8329.00
PAQUETES MOSTRADOS:	8329.00
BYTES TOTALES:	11395885.00
PROMEDIO PAQUETES/SEG:	46480.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1368.218
PROMEDIO BYTES/SEG:	63595.238
PROMEDIO MBITS/SEG:	0,509

Tabla 2.26: Resumen de los datos mostrados en Wireshark

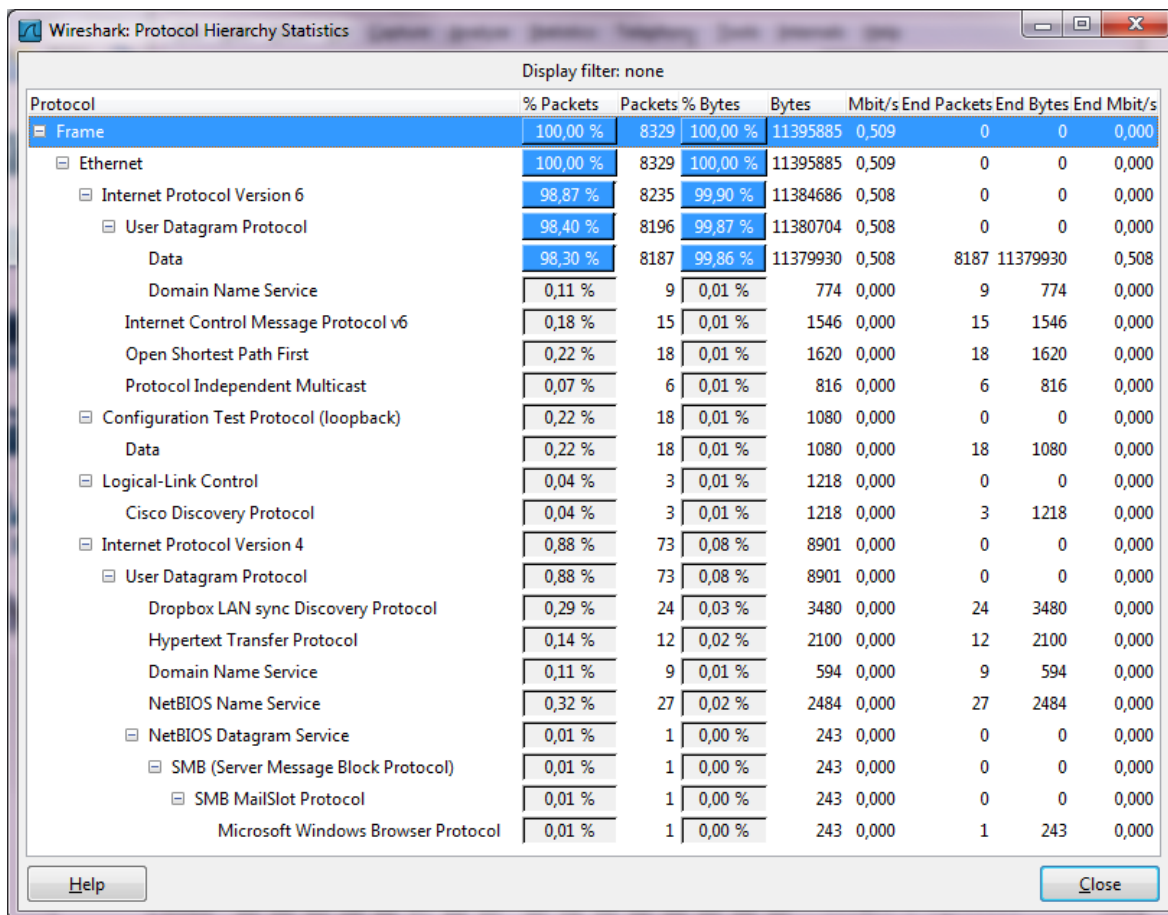


Figura 2.58: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.58 se encuentra en la página 103

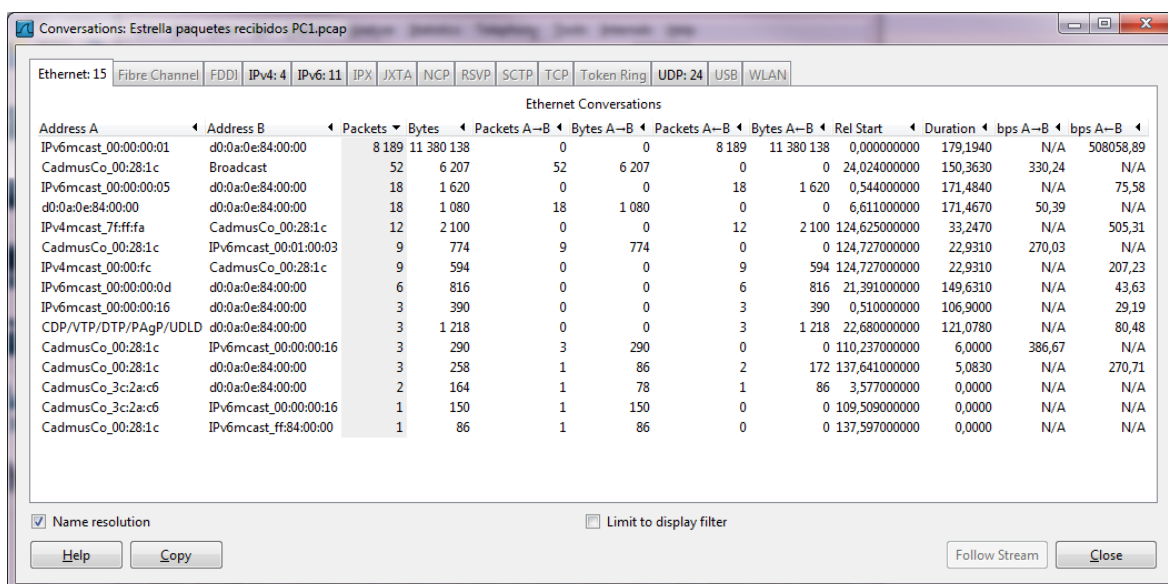


Figura 2.59: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 2.59 se encuentra en la página 104

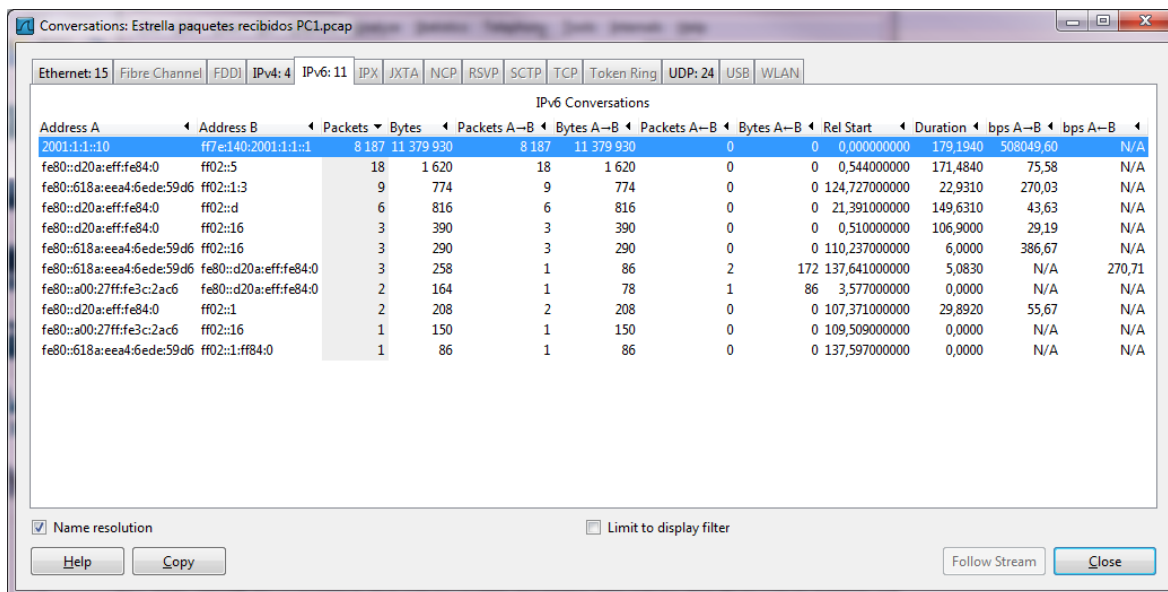


Figura 2.60: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 2.60 se encuentra en la página 105

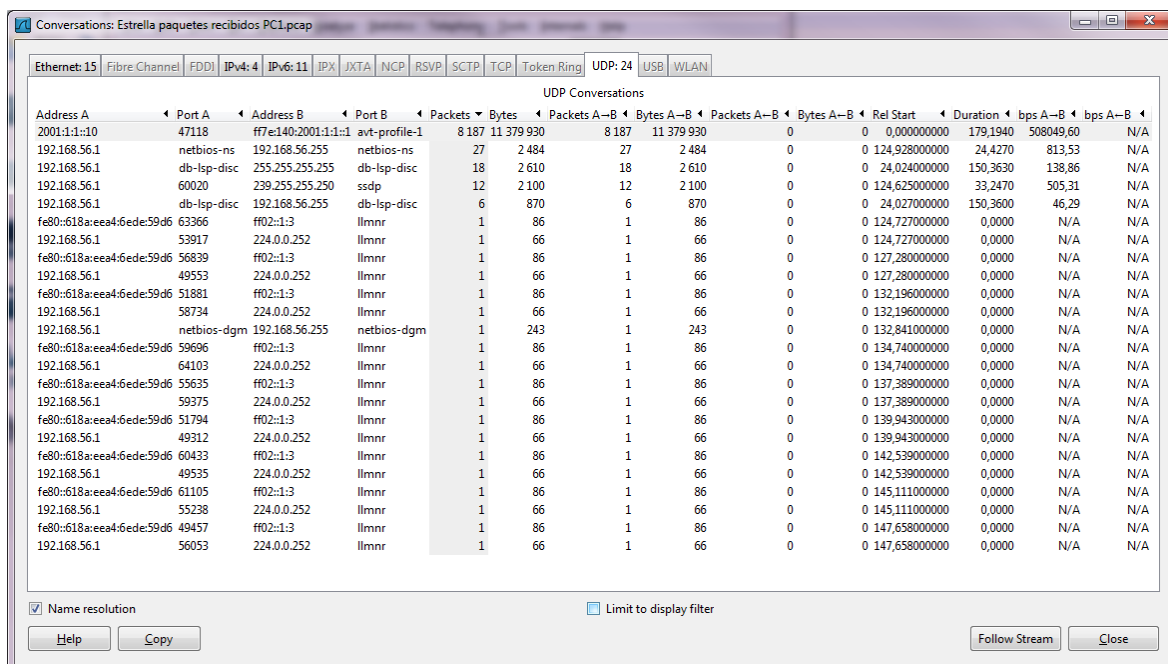


Figura 2.61: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.61 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	8329	0,046480	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	28	0,000156	0,34%
80-159	97	0,000541	1,16%
160-319	14	0,000078	0,17%
320-639	3	0,000017	0,04%
640-1279	0	0,000000	0,00%
1280-2559	8187	0,045688	98,30%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.62: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.62 se encuentra en la página 106

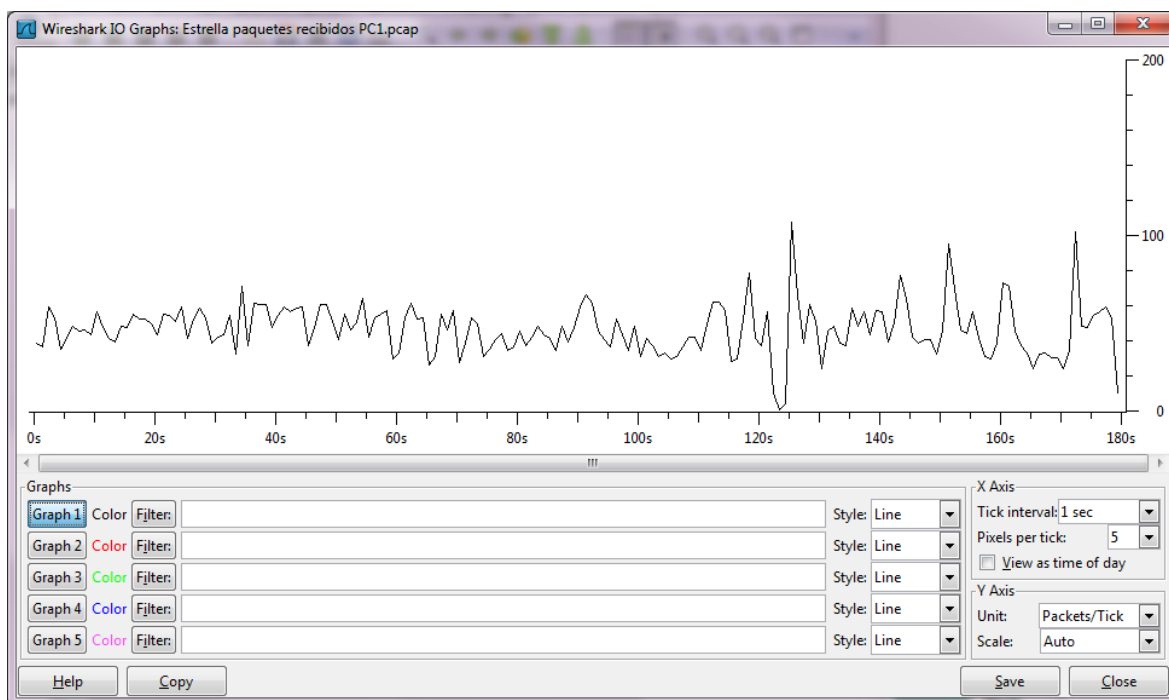


Figura 2.63: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

2.2.2.3 Cálculo de los parámetros de calidad en la red de distribución

2.2.2.3.1 Cálculos de la Velocidad de Transmisión

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	5 ROUTERS TIPO ESTRELLA			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	11497903,00	11484546,00	11480010,00	179,834
CLIENTE PC5	11448731,00	11435530,00	11435530,00	180,050
CLIENTE PC1	11395885,00	11379930,00	11379930,00	179,194
TABLA DE VELOCIDADES				
	SERVER VLC	CLIENTE PC5	CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	63936,20	63586,40	63595,24	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	63861,93	63513,08	63506,20	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	63836,70	63513,08	63506,20	

Tabla 2.27: Velocidades de transmisión obtenidas en la simulación.

2.2.2.3.2 Cálculos de Latencia

PRUEBA N° 1	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	135,44	141,87	160,91	155,38
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	44,00	44,00	45,00	44,00
PAQUETES PERDIDOS	6,00	6,00	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	13,64	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	0,87	1,03	0,90	0,97
PAQUETE MAX TIEMPO (mseg)	17,40	16,70	17,80	40,30
PAQUETE TIEMPO PROMEDIO (mseg)	3,08	3,22	3,58	3,53

Tabla 2.28: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PREBA N° 2	SERVER VLC	LIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	146,70	154,95	153,10	167,42
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	44,00	45,00	45,00	44,00
PAUETES PERDIDOS	6,00	5,00	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	11,11	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	1,05	1,13	1,08	1,13
PAQUETE MAX TIEMPO (mseg)	17,70	33,50	16,80	20,10
PAQUETE TIEMPO PROMEDIO (mseg)	3,33	3,44	3,40	3,81

Tabla 2.29: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	188,32	132,68	135,56	155,38
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	45,00	44,00	44,00	45,00
PAQUETES PERDIDOS	5,00	6,00	6,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	13,64	13,64	11,11
PAQUETE MIN TIEMPO (mseg)	1,08	0,99	1,13	0,92
PAQUETE MAX TIEMPO (mseg)	30,70	17,70	16,50	16,70
PAQUETE TIEMPO PROMEDIO (mseg)	4,18	3,02	3,08	3,45

Tabla 2.30: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

A continuación se presenta un cuadro con el resumen de las 3 pruebas realizadas mediante el comando PING.

RESUMEN	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	470,46	429,50	449,57	478,18
PAQUETES TRANSMITIDOS	150,00	150,00	150,00	150,00
PAQUETES RECIBIDOS	133,00	133,00	134,00	133,00
PAQUETES PERDIDOS	17,00	17,00	16,00	17,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,33	11,33	10,67	11,33
PAQUETE MIN TIEMPO (mseg)	0,87	0,99	0,90	0,92
PAQUETE MAX TIEMPO (mseg)	30,70	17,70	17,80	40,30
PAQUETE TIEMPO PROMEDIO (mseg)	3,53	3,23	3,35	3,60

Tabla 2.31: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING para cada cliente (PC1 y PC5) que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 3.53 mseg.
- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 3.23 mseg.
- Latencia calculada desde el Server VLC a Cliente PC5
Latencia = 3.35 mseg.
- Latencia calculada desde el Cliente PC5 al Server VLC
Latencia = 3.60 mseg.

2.2.2.3.3 Cálculos de Jitter

CALCULO DE JITTER						
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER	CLIENTE PC5	JITTER
14	0,87	0,28	1,48	4,25	15,00	-8,60
15	5,80	-4,93	1,35	0,13	1,14	13,86
16	1,16	4,64	1,44	-0,09	8,19	-7,05
17	2,29	-1,13	1,23	0,21	2,22	5,97
18	1,58	0,71	3,05	-1,82	2,46	-0,24
19	3,96	-2,38	4,09	-1,04	1,52	0,94
20	3,52	0,44	1,62	2,47	1,15	0,37
21	1,56	1,96	1,78	-0,16	1,73	-0,58
22	1,62	-0,06	16,70	-14,92	14,20	-12,47
23	3,42	-1,80	6,82	9,88	1,58	12,62
24	1,27	2,15	2,05	4,77	1,78	-0,20
25	1,90	-0,63	1,33	0,72	1,64	0,14
26	1,50	0,40	1,87	-0,54	2,81	-1,17
27	11,90	-10,40	1,14	0,73	1,65	1,16
28	2,21	9,69	1,80	-0,66	1,36	0,29
29	3,51	-1,30	2,08	-0,28	2,22	-0,86
30	3,29	0,22	3,34	-1,26	0,97	1,25
31	1,76	1,53	8,32	-4,98	2,30	-1,33
32	8,75	-6,99	1,13	7,19	1,71	0,59
33	2,72	6,03	1,63	-0,50	1,87	-0,16
34	1,10	1,62	1,19	0,44	10,90	-9,03
35	3,00	-1,90	1,30	-0,11	1,65	9,25
36	1,32	1,68	1,57	-0,27	1,83	-0,18
37	2,02	-0,70	3,46	-1,89	1,66	0,17
38	2,31	-0,29	2,07	1,39	1,39	0,27
39	6,29	-3,98	2,13	-0,06	40,30	-38,91
40	3,46	2,83	9,03	-6,90	1,66	38,64
41	17,40	-13,94	1,83	7,20	1,45	0,21
42	1,00	16,40	3,14	-1,31	1,43	0,02
43	1,11	-0,11	1,36	1,78	1,44	-0,01
44	2,12	-1,01	2,90	-1,54	1,44	0,00
45	1,43	0,69	1,30	1,60	2,12	-0,68
46	5,02	-3,59	1,15	0,15	1,55	0,57
47	2,75	2,27	2,31	-1,16	1,08	0,47
48	2,64	0,11	1,78	0,53	2,20	-1,12
49	1,56	1,08	8,34	-6,56	1,64	0,56
50	8,59	-7,03	1,46	6,88	1,16	0,48
JITTER MIN		-13,94		-14,92		-38,91
JITTER MAX		16,40		9,88		38,64

Tabla 2.32: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

2.2.2.3.4 Cálculos de Pérdida de Paquetes

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING			
TOPOLOGIA:	5 ROUTERS TIPO ESTRELLA		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	2 min 59 seg.	3 min 0 seg.	2 min 59 seg.
TIEMPO EN SEGUNDOS:	179.834 seg.	180.050 seg.	179.194 seg.
PAQUETES CAPTURADOS:	8419.00	8349.00	8329.00
PAQUETES MOSTRADOS:	8419.00	8349.00	8329.00
BYTES TOTALES:	11497903.00	11448731.00	11395885.00
PROMEDIO PAQUETES/SEG:	50335.00	46370.00	46480.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.361.248	1.371.270	1.368.218
PROMEDIO BYTES/SEG:	63.936.202	63.586.398	63.595.238
PROMEDIO MBITS/SEG:	0,511	0,509	0,509

Tabla 2.33: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la topología tipo estrella.

Los paquetes capturados junto con los paquetes mostrados y los bytes totales, son exactamente iguales en el caso del Server VLC, Cliente PC5 y Cliente PC1.

Por tanto no hay pérdida de paquetes.

2.2.3 TOPOLOGÍA TIPO HÍBRIDA A IMPLEMENTAR

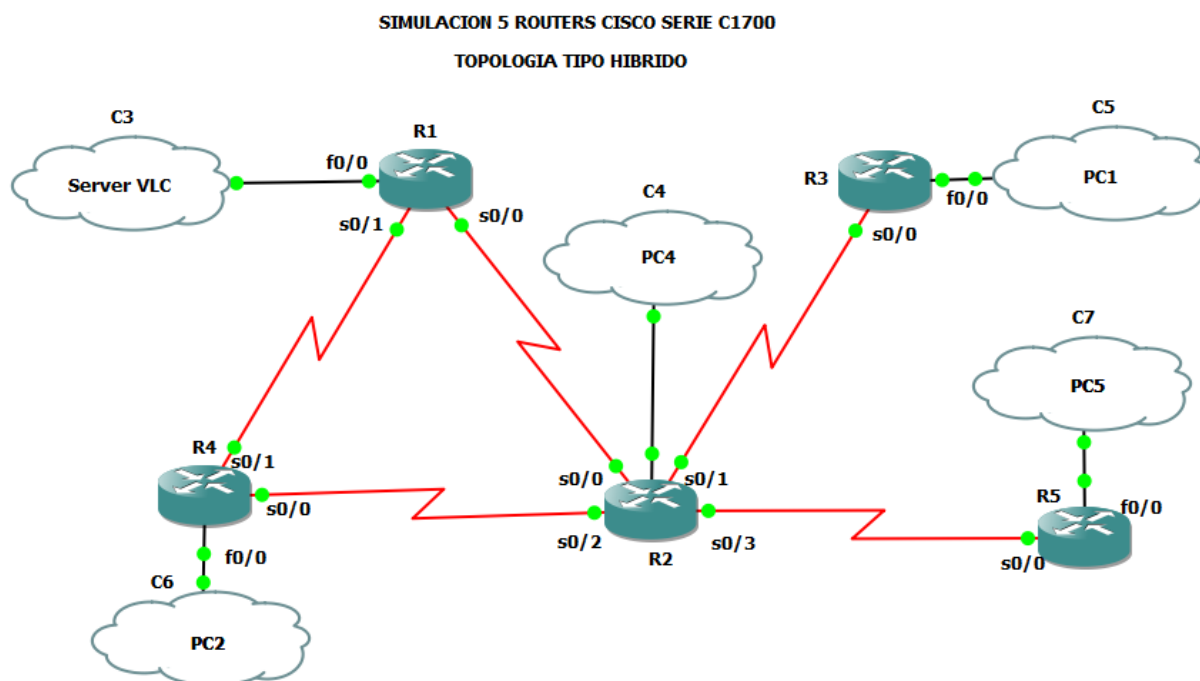


Figura 2.64: Diagrama de la topología tipo híbrido a implementar.

2.2.3.1 Direccionamiento de la topología tipo Híbrida

DISPOSITIVO	DIRECCION IPV6	GATEWAY
Server VLC	2001:1:1::10/64	2001:1:1::1
CLIENTE PC1	2001:3:3::10/64	2001:3:3::3
CLIENTE PC2	2001:4:4::10/64	2001:4:4::4
CLIENTE PC4	2001:2:2::10/64	2001:2:2::2
CLIENTE PC5	2001:5:5::10/64	2001:5:5::5
ROUTER R1		
Fastethernet 0/0	2001:1:1::1/64	
Serial 0/0	2001:1:2::1/64	
Serial 0/1	2001:1:4::1/64	
ROUTER R2		
Fastethernet 0/0	2001:2:2::2/64	
Serial 0/0	2001:1:2::2/64	
Serial 0/1	2001:2:3::2/64	
Serial 0/2	2001:2:4::2/64	
Serial 0/3	2001:2:5::2/64	
ROUTER R3		
Fastethernet 0/0	2001:3:3::3/64	
Serial 0/0	2001:2:3::3/64	
ROUTER R4		
Fastethernet 0/0	2001:4:4::4/64	
Serial 0/0	2001:2:4::4/64	
Serial 0/1	2001:1:4::4/64	
ROUTER R5		
Fastethernet 0/0	2001:5:5::5/64	
Serial 0/0	2001:2:5::5/64	
DIRECCION EMBEDDED MULTICAST A UTILIZAR		
Grupo Multicast Embedded	FF07:140:2001:1:1::1	
PROCOLO DE ENRUTAMIENTO UTILIZADO		
PROTOCOLO:	OSPFv6	
GRUPO:	1	
AREA:	0	
ROUTERS IMPLEMENTADOS:	Todos los Routers de la red de distribución	
RP SELECCIONADO		
ROUTER:	R1 (Conectado directamente al Server VLC)	

Tabla 2.34: Direccionamiento de la topología tipo híbrida.

2.2.3.2 Capturas de pantalla de la red de distribución

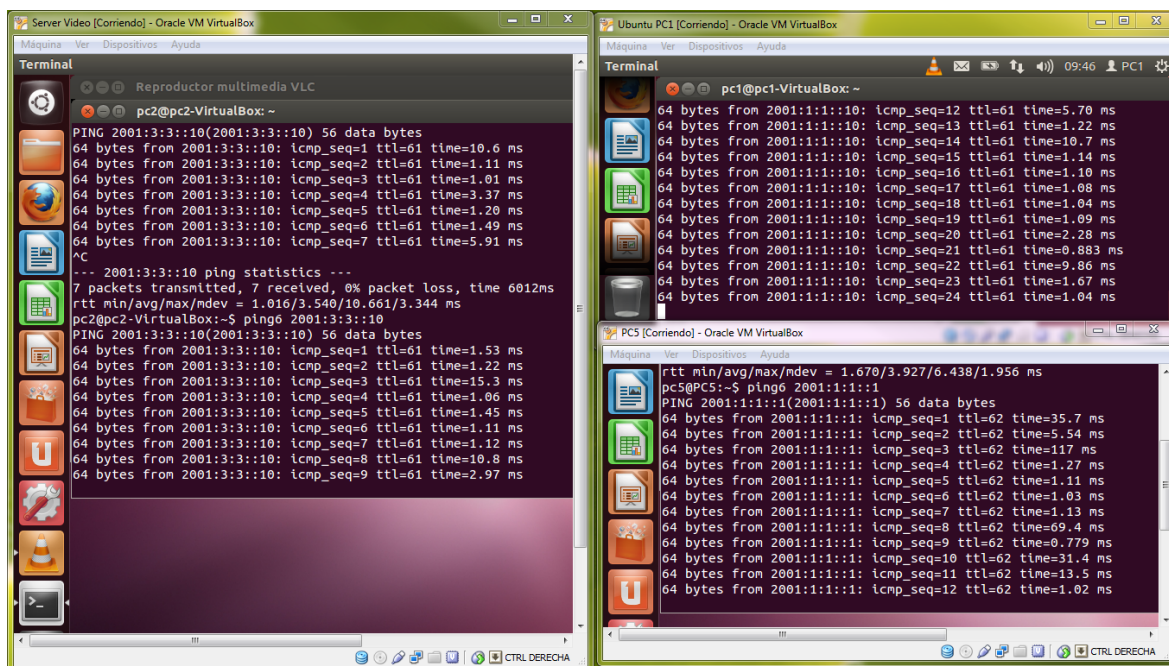


Figura 2.65: Ping desde el Server VLC hacia cada cliente en el extremo de la red de distribución (Cliente PC1 y Cliente PC5) y viceversa.

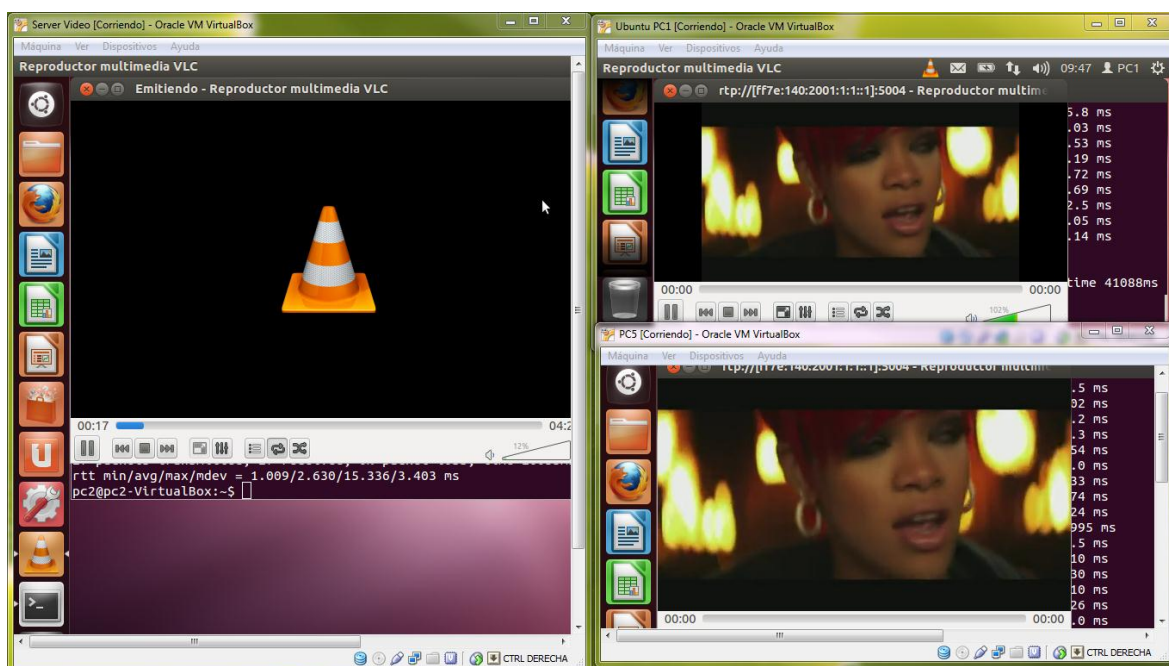


Figura 2.66: Video streaming transmitido desde el Server VLC y captado por los clientes PC1 y PC5 en los extremos de la red de distribución.

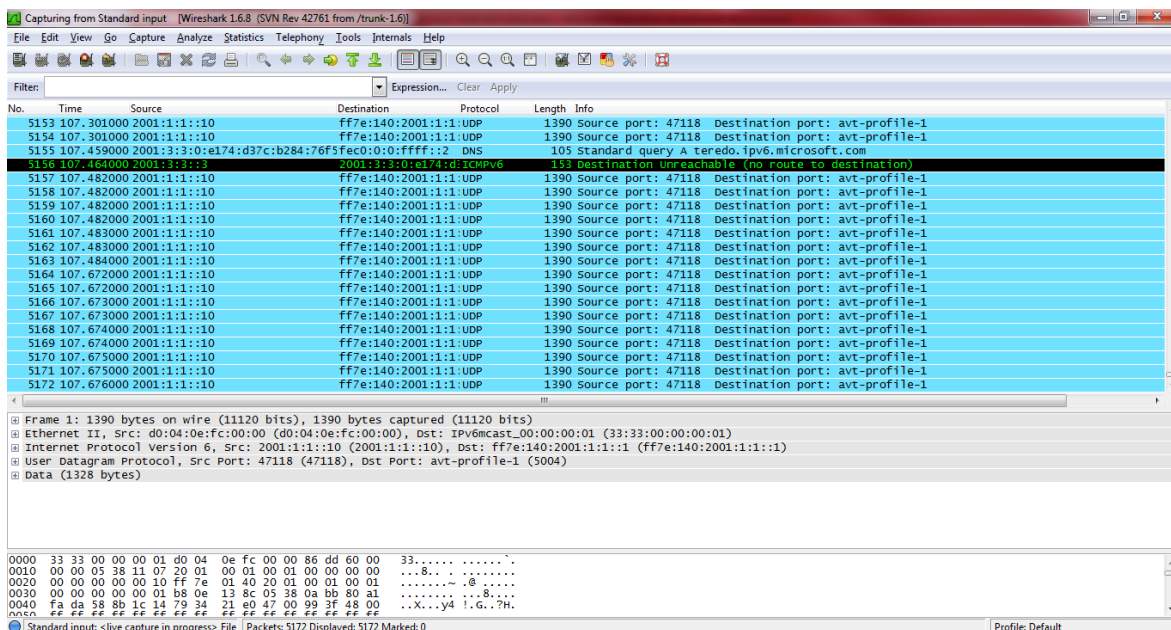


Figura 2.67: Ventana de WIRESHARK donde muestra la captura de los paquetes recibidos por el Cliente PC1

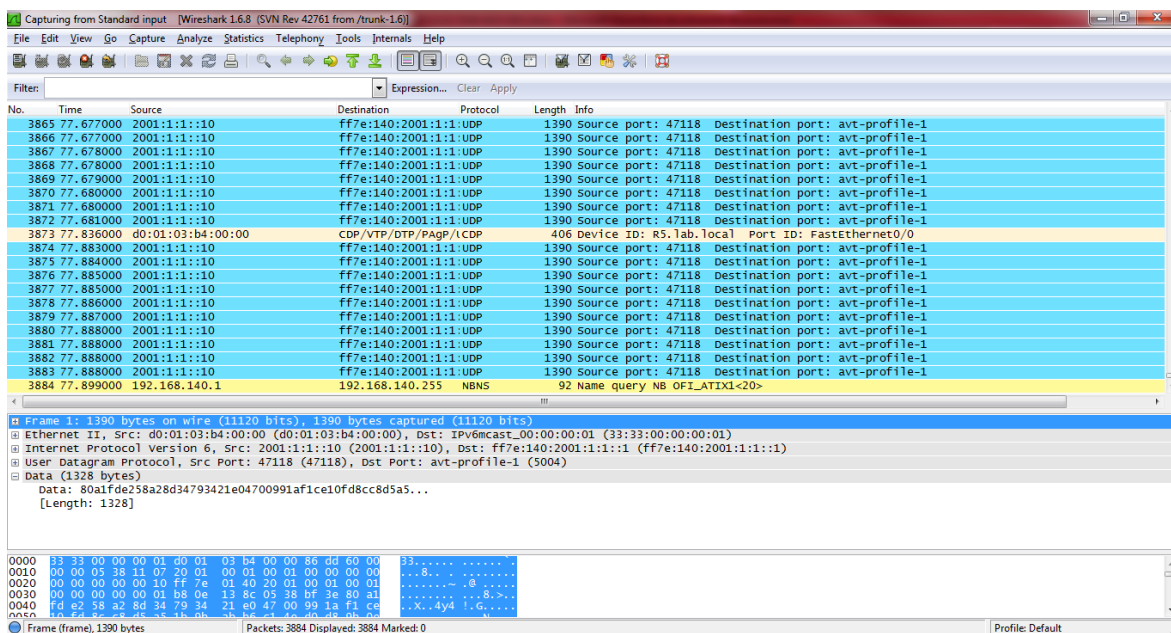


Figura 2.68: Ventana de WIRESHARK donde muestra la captura de los paquetes recibidos por el Cliente PC5

SERVER VLC

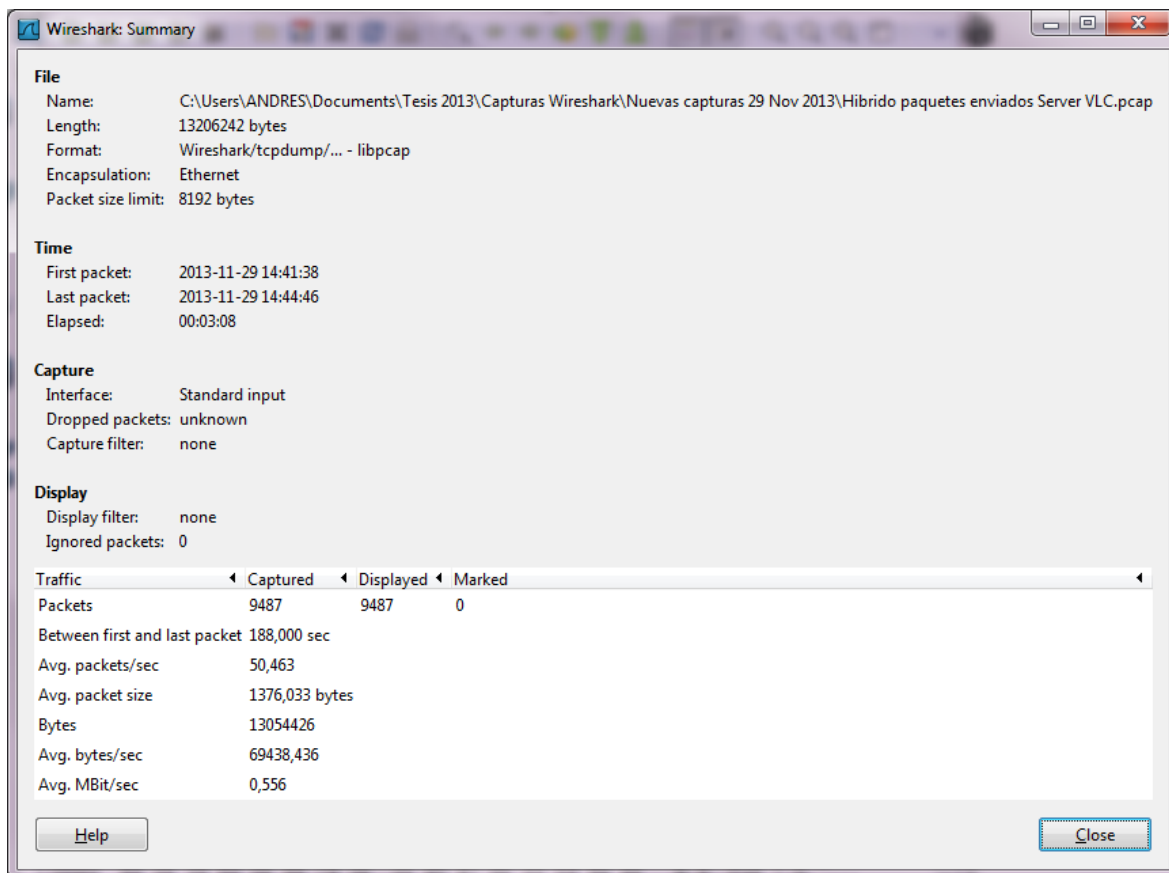


Figura 2.69: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 8 seg.
TIEMPO EN SEGUNDOS:	188.000 seg.
PAQUETES CAPTURADOS:	9487.00
PAQUETES MOSTRADOS:	9487.00
BYTES TOTALES:	13054426.00
PROMEDIO PAQUETES/SEG:	50463.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1376.033
PROMEDIO BYTES/SEG:	69438.436
PROMEDIO MBITS/SEG:	0,556

Tabla 2.35: Resumen de los datos mostrados en Wireshark.

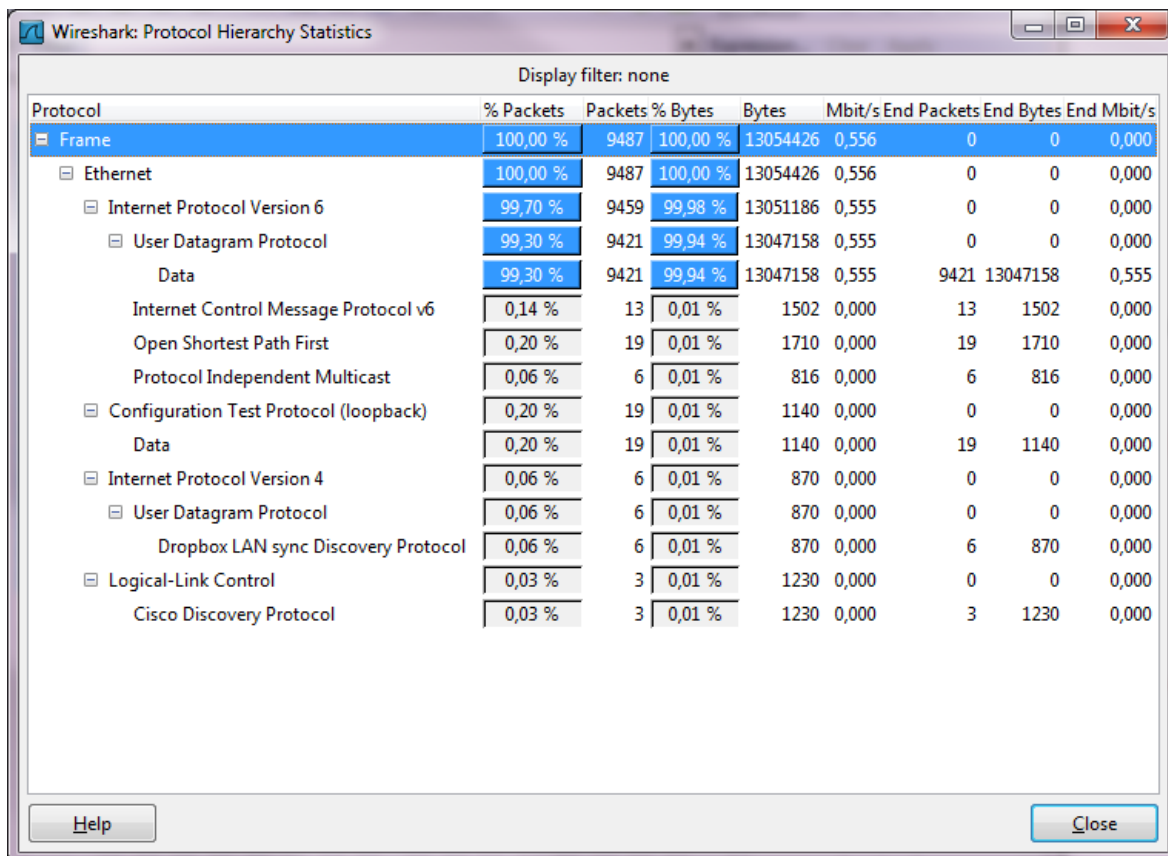


Figura 2.70: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.70 se encuentra en la página 103

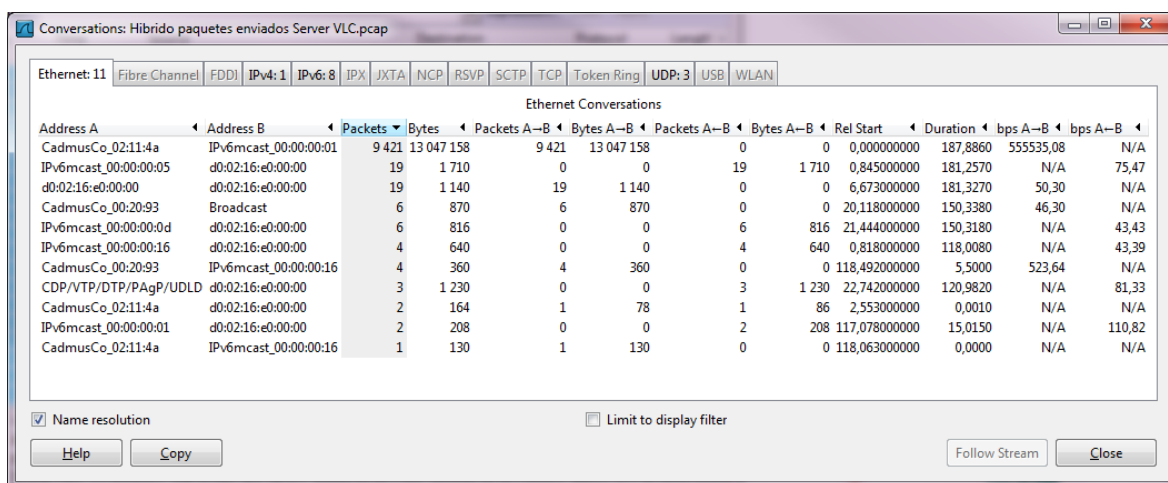


Figura 2.71: Paquetes Ethernet que atravesaron la red al momento de la captura

* La explicación de la figura 2.71 se encuentra en la página 104

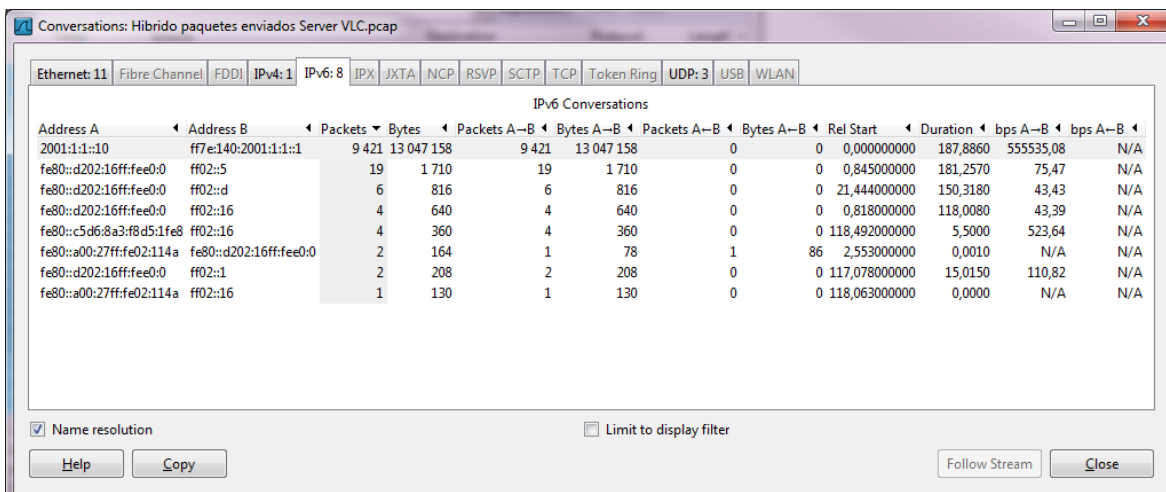


Figura 2.72: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 2.72 se encuentra en la página 105

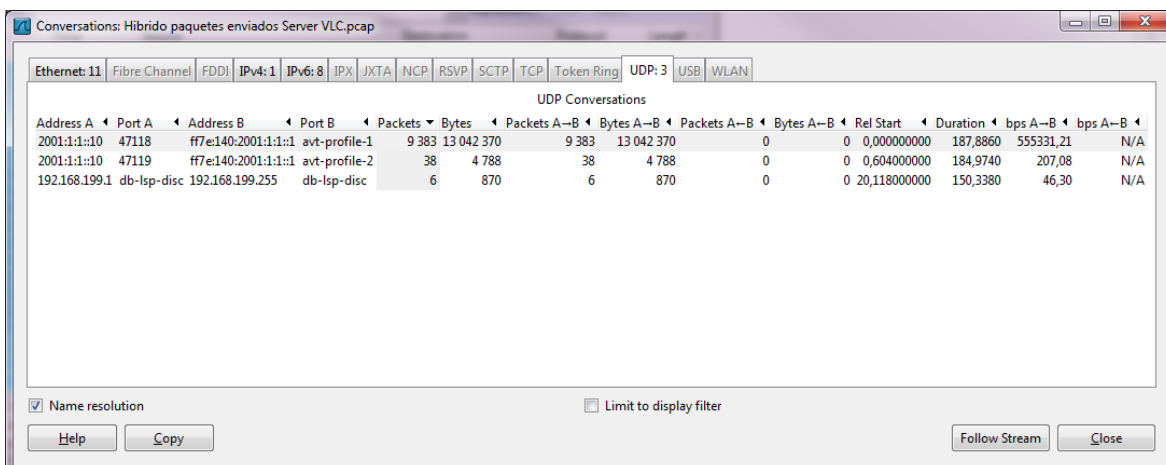


Figura 2.73: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.73 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	9487	0,050463	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	20	0,000106	0,21%
80-159	79	0,000420	0,83%
160-319	2	0,000011	0,02%
320-639	3	0,000016	0,03%
640-1279	0	0,000000	0,00%
1280-2559	9383	0,049910	98,90%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.74: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.74 se encuentra en la página 106

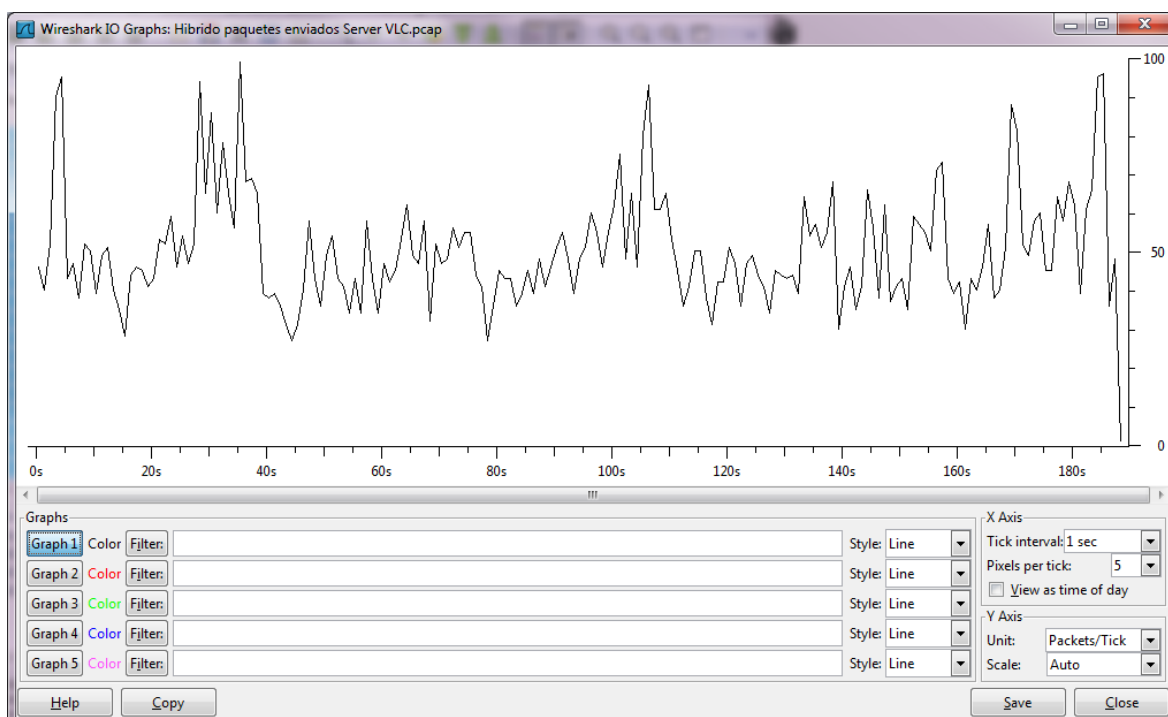


Figura 2.75: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC5

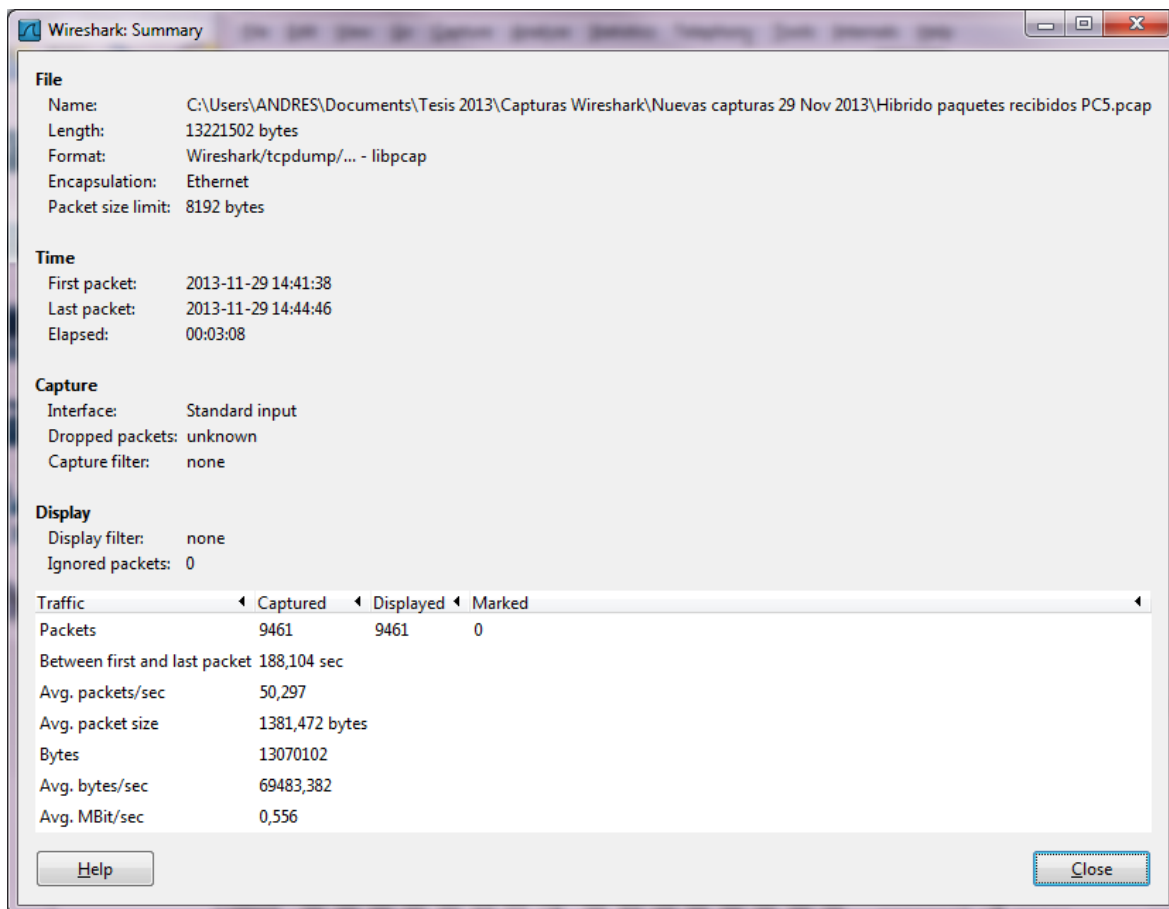


Figura 2.76: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1.

PC:	CLIENTE PC5
INTERFACE:	Fastethernet R5
TIEMPO DE CAPTURA DE PAQUETES:	3 min 8 seg.
TIEMPO EN SEGUNDOS:	188.104 seg.
PAQUETES CAPTURADOS:	9461.00
PAQUETES MOSTRADOS:	9461.00
BYTES TOTALES:	13070102.00
PROMEDIO PAQUETES/SEG:	50297.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1381.472
PROMEDIO BYTES/SEG:	69483.382
PROMEDIO MBITS/SEG:	0,556

Tabla 2.36: Resumen de los datos mostrados en Wireshark

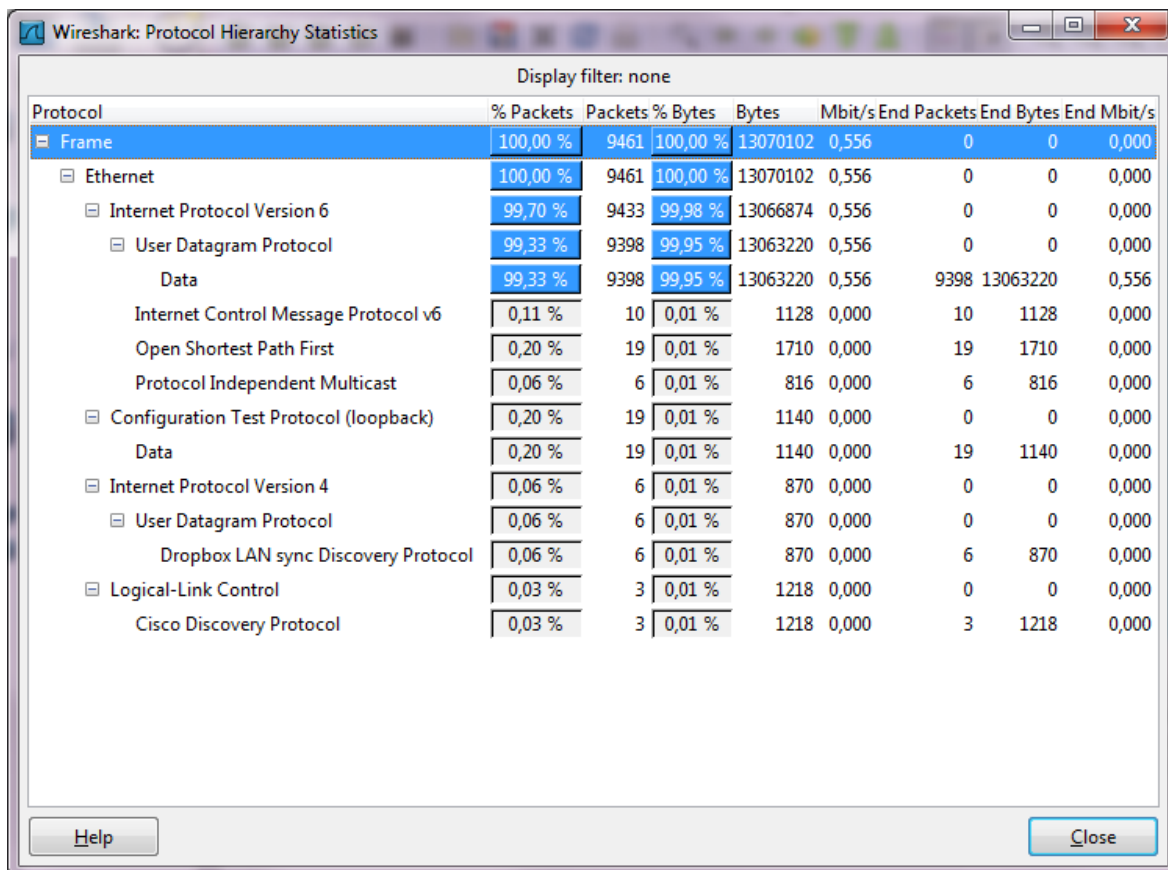


Figura 2.77: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.77 se encuentra en la página 103

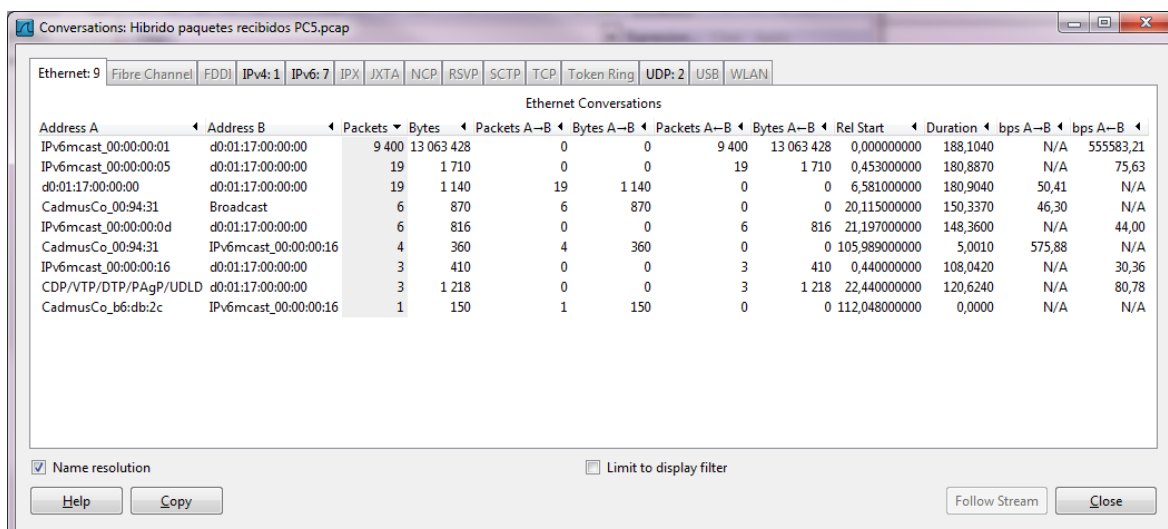


Figura 2.78: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 2.78 se encuentra en la página 104

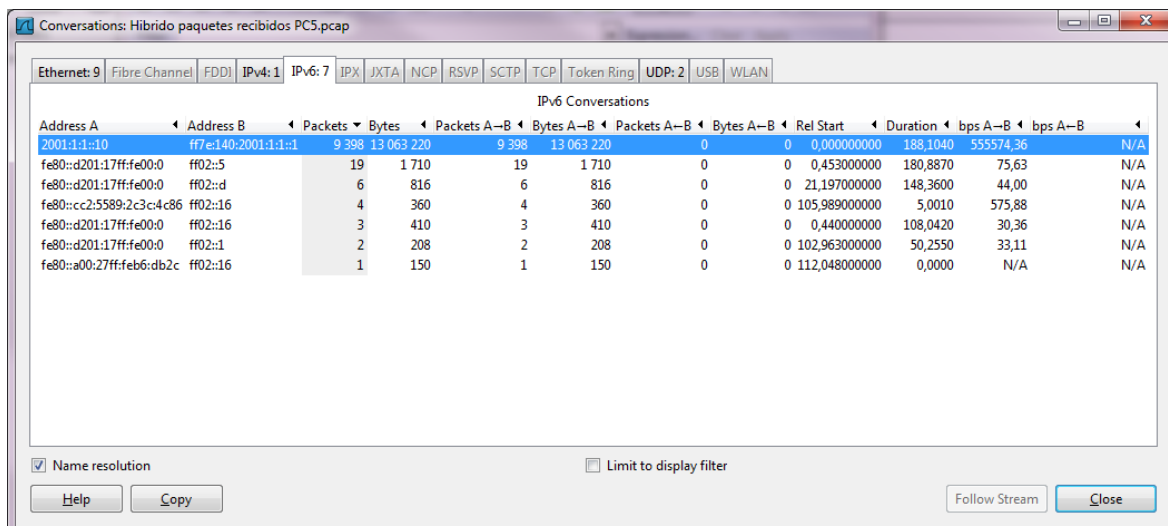


Figura 2.79: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 2.79 se encuentra en la página 105

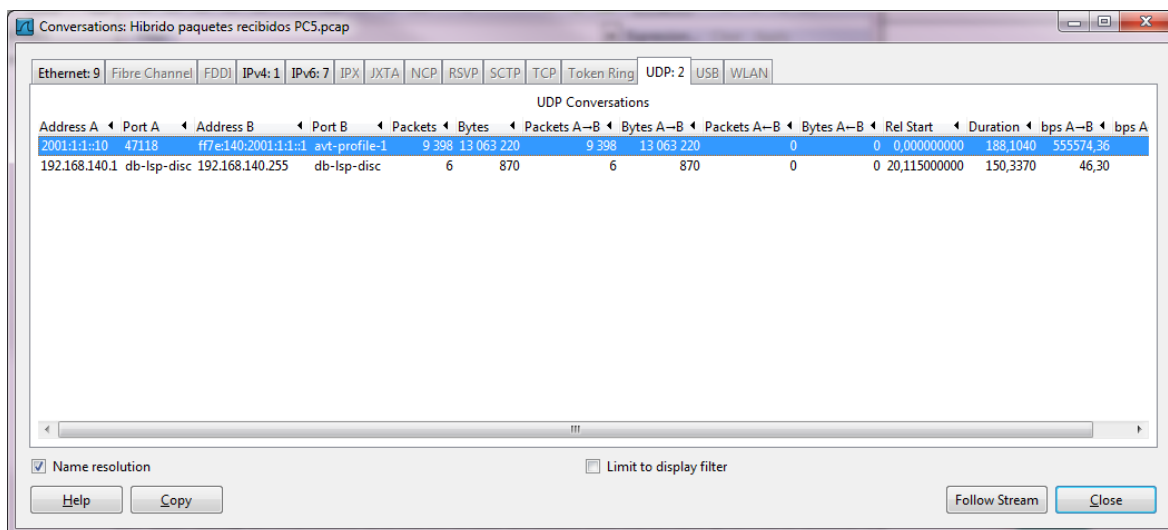


Figura 2.80: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.80 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	9461	0,050297	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	19	0,000101	0,20%
80-159	40	0,000213	0,42%
160-319	1	0,000005	0,01%
320-639	3	0,000016	0,03%
640-1279	0	0,000000	0,00%
1280-2559	9398	0,049962	99,33%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.81: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.81 se encuentra en la página 106

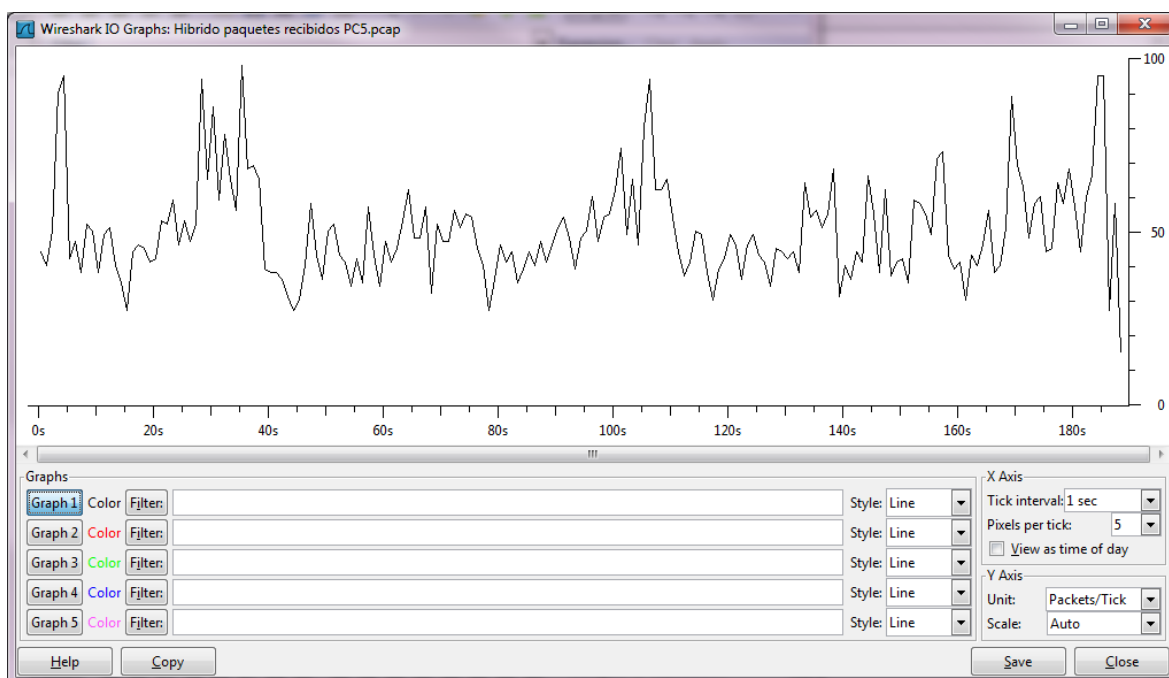


Figura 2.82: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC1

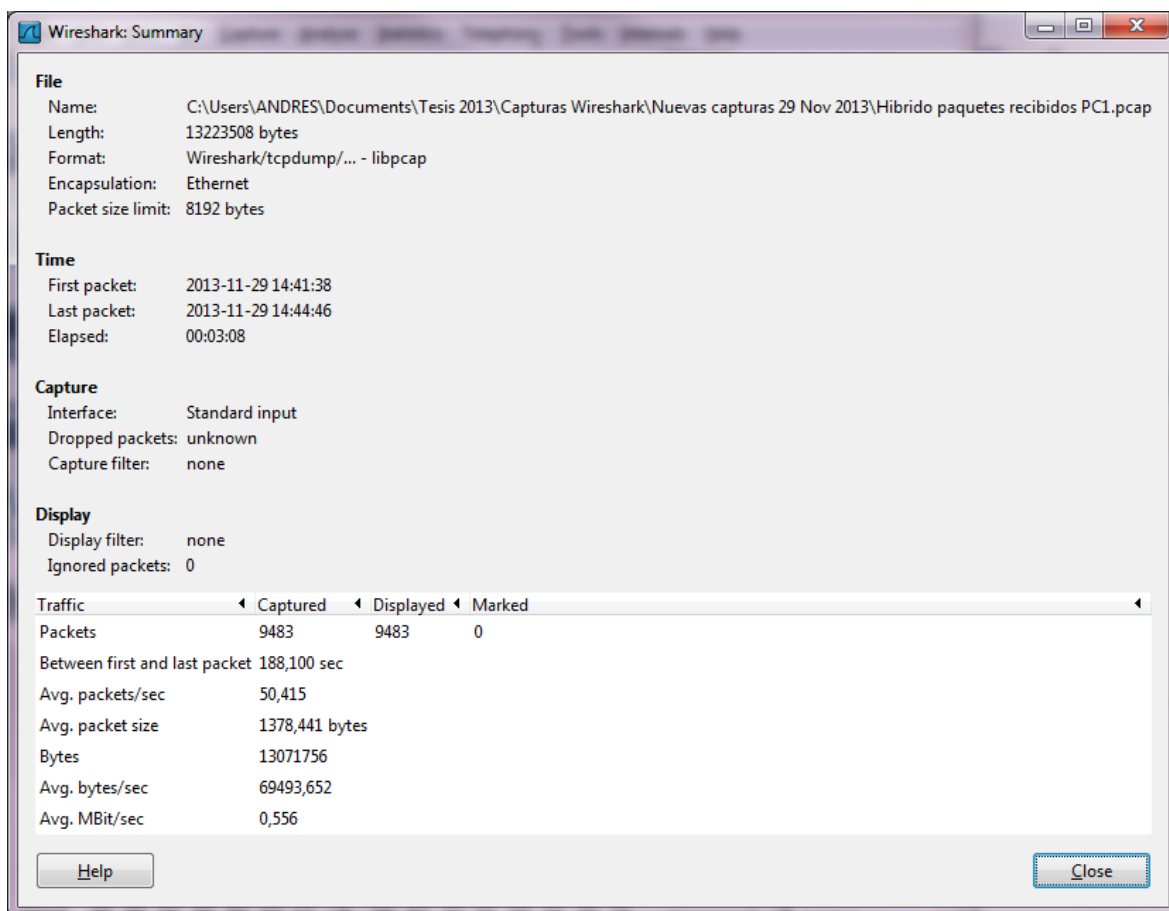


Figura 2.83: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1.

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	3 min 8 seg.
TIEMPO EN SEGUNDOS:	188100 seg.
PAQUETES CAPTURADOS:	9483.00
PAQUETES MOSTRADOS:	9483.00
BYTES TOTALES:	13071756.00
PROMEDIO PAQUETES/SEG:	50415.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1378.441
PROMEDIO BYTES/SEG:	69493.652
PROMEDIO MBITS/SEG:	0,556

Tabla 2.37: Resumen de los datos mostrados en Wireshark

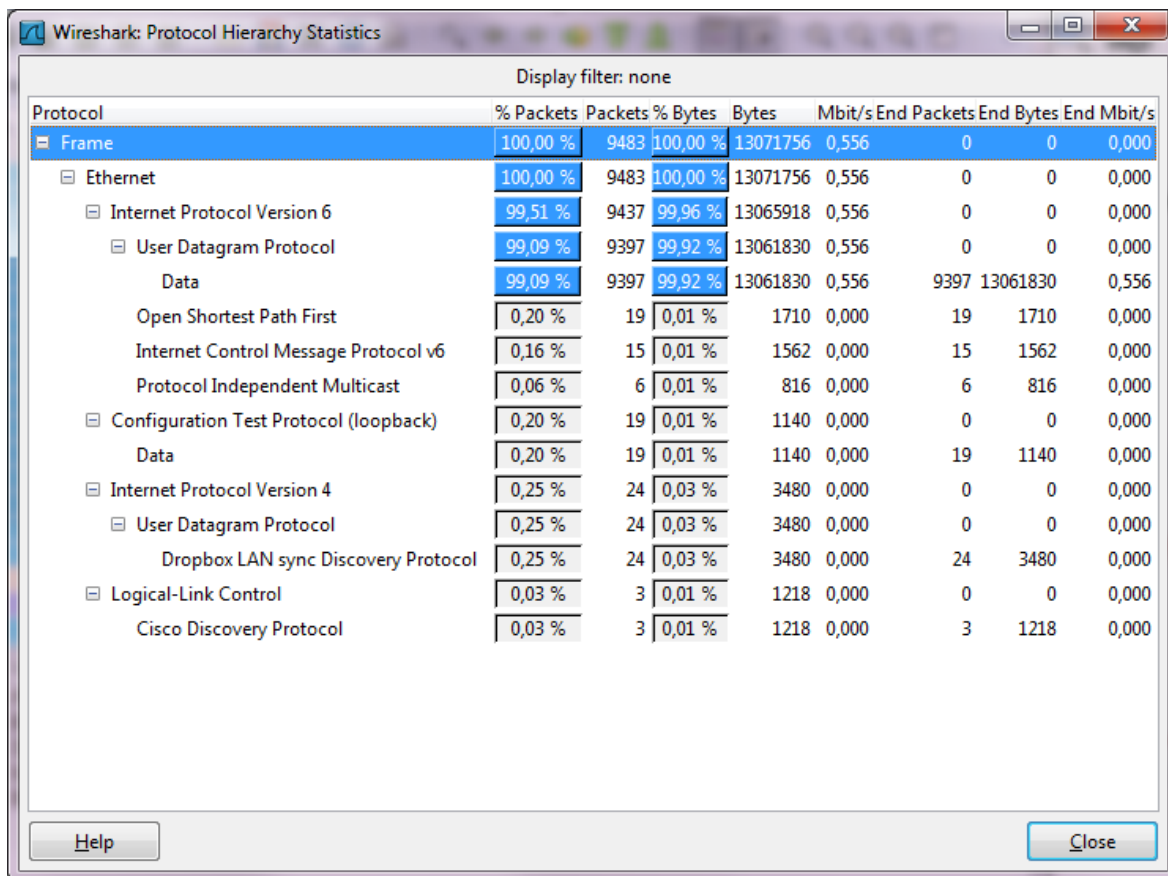


Figura 2.84: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.84 se encuentra en la página 103

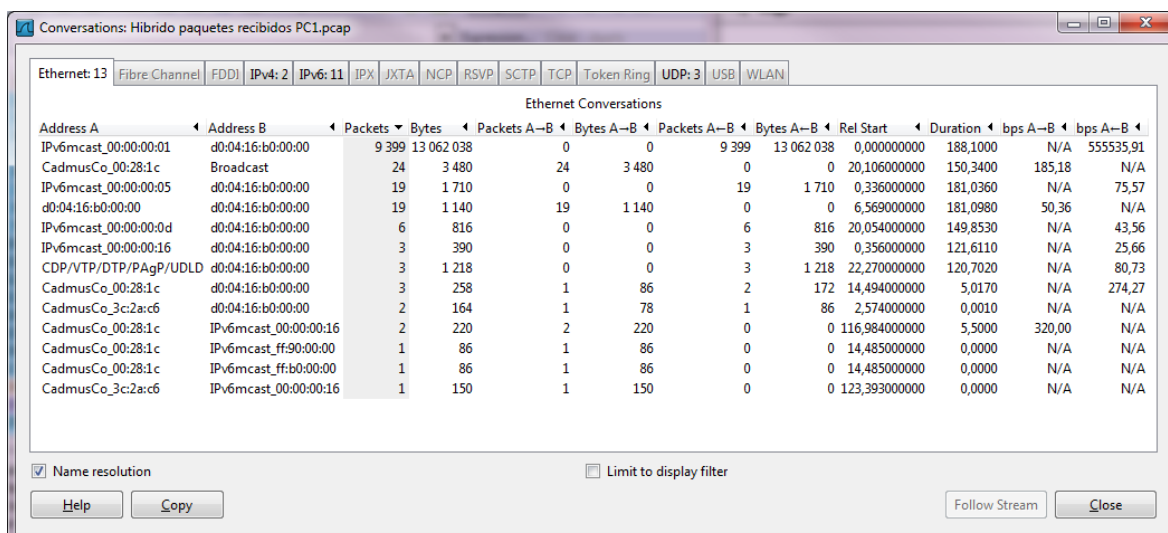


Figura 2.85: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 2.85 se encuentra en la página 104

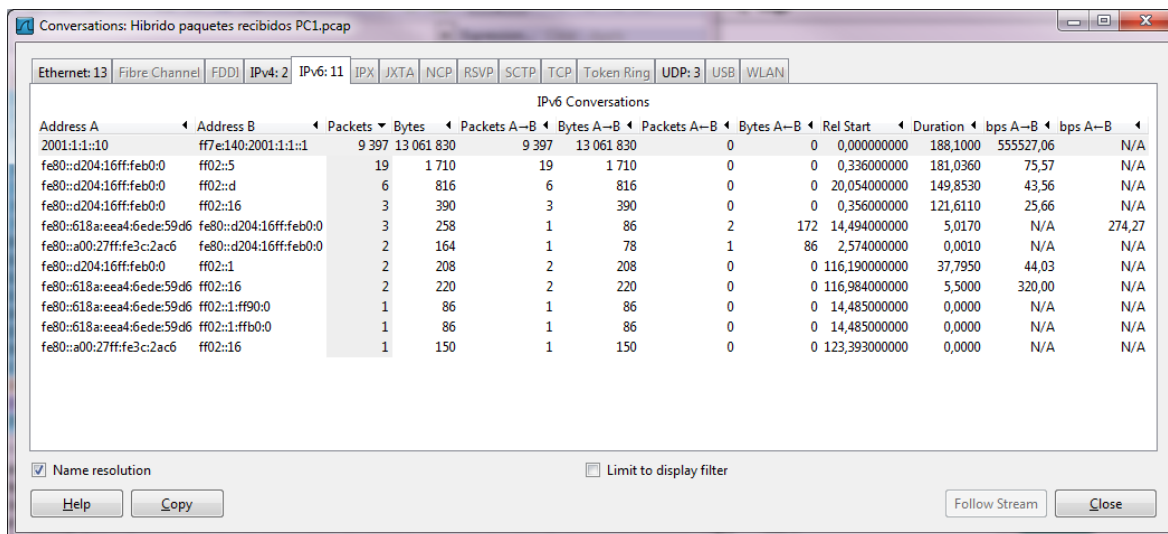


Figura 2.86: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 1.8 se encuentra en la página 105

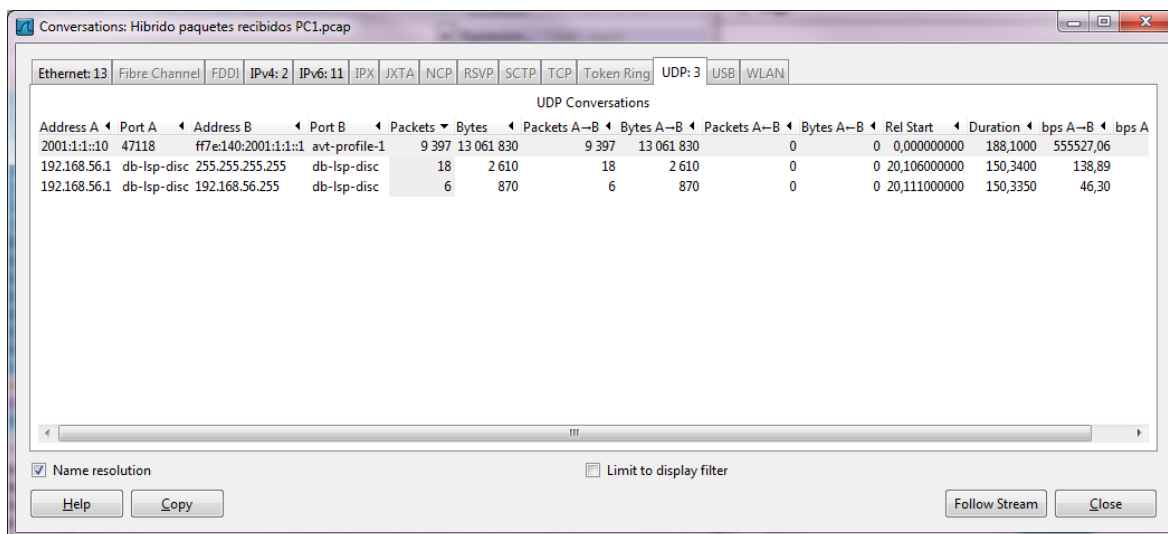


Figura 2.87: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.87 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	9483	0,050415	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	20	0,000106	0,21%
80-159	62	0,000330	0,65%
160-319	1	0,000005	0,01%
320-639	3	0,000016	0,03%
640-1279	0	0,000000	0,00%
1280-2559	9397	0,049957	99,09%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.88: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.88 se encuentra en la página 106

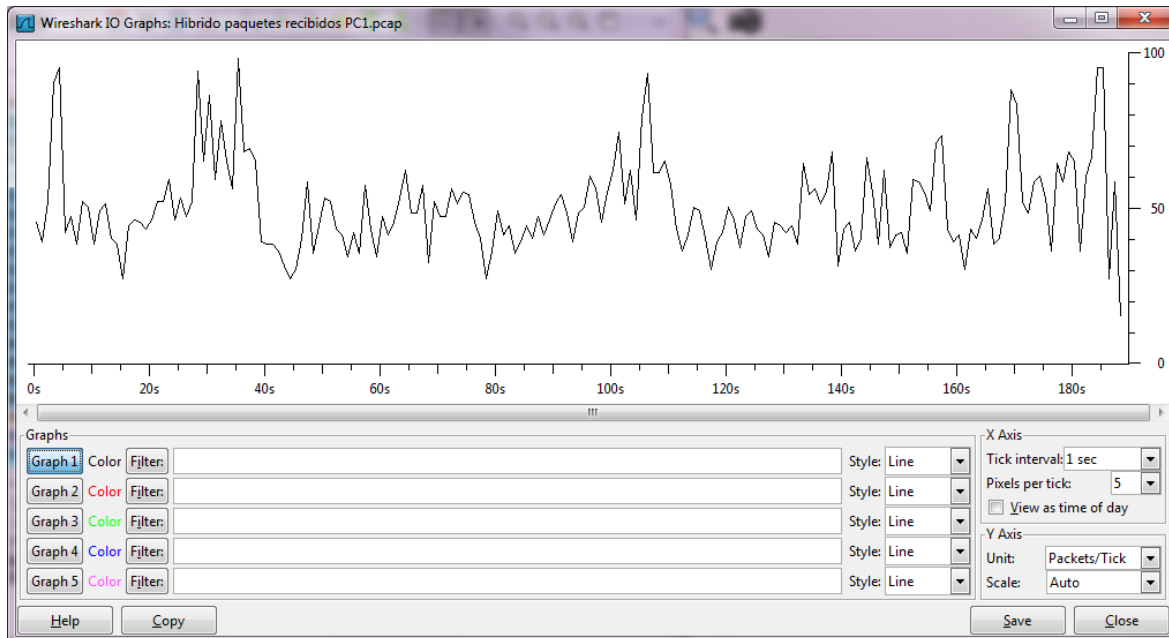


Figura 2.89: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

2.2.3.3 Cálculo de los parámetros de calidad en la red de distribución

2.2.3.3.1 Cálculos de la Velocidad de Transmisión

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	5 ROUTERS TIPO HIBRIDO			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	13054426,00	13051186,00	13047158,00	188,000
CLIENTE PC5	13070102,00	13066874,00	13063220,00	188,104
CLIENTE PC1	13071756,00	13065918,00	13061830,00	188,100
TABLA DE VELOCIDADES				
	SERVER VLC	CLIENTE PC5	CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	69438,44	69483,38	69493,65	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	69421,20	69466,22	69462,62	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	69399,78	69446,80	69440,88	

Tabla 2.38: Velocidades de transmisión obtenidas en la simulación.

2.2.3.3.2 Cálculos de Latencia

PRUEBA N° 1	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	117,79	272,36	106,15	109,25
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00	45,00	45,00
PAQUETES PERDIDOS	5,00	5,00	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	11,11	11,11	11,11
PAQUETE MIN TIEMPO (mseg)	0,87	1,06	0,89	0,88
PAQUETE MAX TIEMPO (mseg)	11,50	68,50	19,20	22,50
PAQUETE TIEMPO PROMEDIO (mseg)	2,62	6,05	2,36	2,43

Tabla 2.39: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 2	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	127,82	165,57	128,19	131,08
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	4,00	45,00	45,00	44,00
PAUETES PERDIDOS	6,00	5,00	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	11,11	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	0,91	1,05	1,03	0,90
PAQUETE MAX TIEMPO (mseg)	19,50	22,30	19,20	14,02
PAQUETE TIEMPO PROMEDIO (mseg)	2,91	3,68	2,85	2,98

Tabla 2.40: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	149,46	138,42	111,30	146,06
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00	45,00	45,00
PAQUETES PERDIDOS	5,00	5,00	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	11,11	11,11	11,11
PAQUETE MIN TIEMPO (mseg)	0,87	1,19	1,20	1,08
PAQUETE MAX TIEMPO (mseg)	16,10	22,80	10,70	19,22
PAQUETE TIEMPO PROMEDIO (mseg)	3,32	3,08	2,47	3,25

Tabla 2.41: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

A continuación se presenta un cuadro con el resumen de las 3 pruebas realizadas mediante el comando PING.

RESUMEN	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	395,07	576,35	345,64	386,39
PAQUETES TRANSMITIDOS	150,00	150,00	150,00	150,00
PAQUETES RECIBIDOS	134,00	135,00	135,00	134,00
PAQUETES PERDIDOS	16,00	15,00	15,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,00	10,00	10,67
PAQUETE MIN TIEMPO (mseg)	0,87	1,05	0,89	0,88
PAQUETE MAX TIEMPO (mseg)	19,50	68,50	19,20	22,50
PAQUETE TIEMPO PROMEDIO (mseg)	2,95	4,27	2,56	2,88

Tabla 2.42: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING para cada cliente (PC1 y PC5) que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 2.95 mseg.
- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 4.27 mseg.
- Latencia calculada desde el Server VLC a Cliente PC5
Latencia = 2.56 mseg.
- Latencia calculada desde el Cliente PC5 al Server VLC
Latencia = 2.88 mseg.

2.2.3.3 Cálculos de Jitter

CALCULO DE JITTER						
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER	CLIENTE PC5	JITTER
14	1,09	-0,10	1,13	0,08	1,20	-0,11
15	1,37	-0,28	1,24	-0,11	1,20	0,00
16	1,11	0,26	2,24	-1,00	1,89	-0,69
17	1,12	-0,01	2,81	-0,57	1,26	0,63
18	0,87	0,25	2,47	0,34	1,16	0,10
19	11,40	-10,53	6,40	-3,93	1,11	0,05
20	1,00	10,40	2,18	4,22	2,63	-1,52
21	1,31	-0,31	2,16	0,02	2,53	0,10
22	3,21	-1,90	2,54	-0,38	1,44	1,09
23	1,17	2,04	1,97	0,57	1,88	-0,44
24	11,50	-10,33	11,50	-9,53	1,27	0,61
25	1,66	9,84	1,24	10,26	1,18	0,09
26	1,10	0,56	2,00	-0,76	4,79	-3,61
27	1,23	-0,13	2,38	-0,38	1,12	3,67
28	1,82	-0,59	2,30	0,08	1,05	0,07
29	2,01	-0,19	6,58	-4,28	1,08	-0,03
30	1,08	0,93	1,68	4,90	1,05	0,03
31	11,20	-10,12	2,17	-0,49	2,09	-1,04
32	1,46	9,74	1,48	0,69	1,06	1,03
33	1,99	-0,53	19,30	-17,82	1,17	-0,11
34	0,91	1,08	2,69	16,61	1,04	0,13
35	1,14	-0,23	2,65	0,04	1,26	-0,22
36	1,37	-0,23	19,10	-16,45	1,20	0,06
37	1,90	-0,53	47,16	-49,40	0,88	0,32
38	5,52	-3,62	2,88	49,62	1,21	-0,33
39	4,35	1,17	5,75	-2,87	4,89	-3,68
40	1,64	2,71	12,00	-6,25	5,39	-0,50
41	1,42	0,22	5,42	6,58	1,62	3,77
42	0,87	0,55	21,40	-15,98	22,50	-20,88
43	1,26	-0,39	1,44	19,96	1,33	21,17
44	2,09	-0,83	10,20	-8,76	1,97	-0,64
45	1,56	0,53	2,01	8,19	1,72	0,25
46	7,80	-6,24	1,81	0,20	1,27	0,45
47	3,25	4,55	2,92	-1,11	1,21	0,06
48	3,42	-0,17	4,67	-1,75	1,74	-0,53
49	9,65	-6,23	5,23	-0,56	15,50	-13,76
50	1,33	8,32	1,69	3,54	1,55	13,95
JITTER MIN		-10,53		-49,40		-20,88
JITTER MAX		10,40		49,62		21,17

Tabla 2.43: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

2.2.3.3.4 Cálculos de Pérdida de Paquetes

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING			
TOPOLOGIA:	5 ROUTERS TIPO HIBRIDO		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	3 min 8 seg.	3 min 8 seg.	3 min 8 seg.
TIEMPO EN SEGUNDOS:	188.000 seg.	188.104 seg.	188100 seg.
PAQUETES CAPTURADOS:	9487.00	9461.00	9483.00
PAQUETES MOSTRADOS:	9487.00	9461.00	9483.00
BYTES TOTALES:	13054426.00	13070102.00	13071756.00
PROMEDIO PAQUETES/SEG:	50463.00	50297.00	50415.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.376.033	1.381.472	1.378.441
PROMEDIO BYTES/SEG:	69.438.436	69.483.382	69.493.652
PROMEDIO MBITS/SEG:	0,556	0,556	0,556

Tabla 2.44: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la topología tipo híbrida.

Los paquetes capturados junto con los paquetes mostrados y los bytes totales, son exactamente iguales en el caso del Server VLC, Cliente PC5 y Cliente PC1.

Por tanto no hay pérdida de paquetes.

2.2.4 CÁLCULOS DE PARÁMETROS DE CALIDAD EN TOPOLOGÍA TIPO MALLA DONDE SE AUMENTAN Y DISMINUYEN ROUTERS MIENTRAS SE ENVÍA EL STREAMING DE VIDEO.

2.2.4.1 Topología tipo malla a implementar

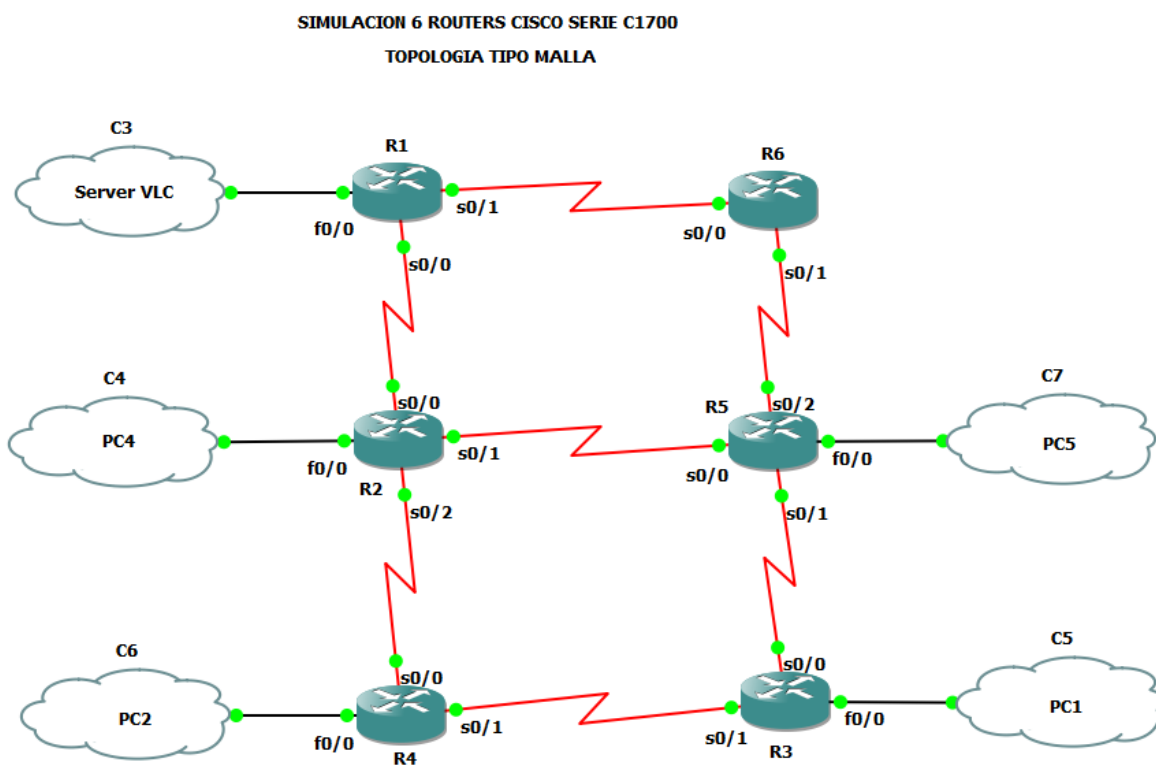


Figura 2.90: Diagrama de la topología tipo malla a implementar

2.2.4.2 Direccionamiento de la topología tipo malla

DISPOSITIVO	DIRECCION IPV6	GATEWAY
Server VLC	2001:1:1::10/64	2001:1:1::1
CLIENTE PC1	2001:3:3::10/64	2001:3:3::3
CLIENTE PC2	2001:4:4::10/64	2001:4:4::4
CLIENTE PC4	2001:2:2::10/64	2001:2:2::2
CLIENTE PC5	2001:5:5::10/64	2001:5:5::5
ROUTER R1		
Fastethernet 0/0	2001:1:1::1/64	
Serial 0/0	2001:1:2::1/64	
Serial 0/1	2001:1:6::1/64	
ROUTER R2		
Fastethernet 0/0	2001:2:2::2/64	
Serial 0/0	2001:1:2::2/64	
Serial 0/1	2001:2:5::2/64	
Serial 0/2	2001:2:4::2/64	
ROUTER R3		
Fastethernet 0/0	2001:3:3::3/64	
Serial 0/0	2001:3:5::3/64	
Serial 0/1	2001:4:3::3/64	
ROUTER R4		
Fastethernet 0/0	2001:4:4::4/64	
Serial 0/0	2001:2:4::4/64	
Serial 0/1	2001:4:3::4/64	
ROUTER R5		
Fastethernet 0/0	2001:5:5::5/64	
Serial 0/0	2001:2:5::5/64	
Serial 0/1	2001:3:5::5/64	
Serial 0/2	2001:5:6::5/64	
ROUTER R6		
Serial 0/0	2001:1:6::6/64	
Serial 0/1	2001:5:6::6/64	
DIRECCION EMBEDDED MULTICAST A UTILIZAR		
Grupo Multicast Embedded	FF07:140:2001:1:1::1	
PROCOLO DE ENRUTAMIENTO UTILIZADO		
PROTOCOLO:	OSPFv6	
GRUPO:	1	
AREA:	0	
ROUTERS IMPLEMENTADOS:	Todos los Routers de la red de distribución	
RP SELECCIONADO		
ROUTER:	R1 (Conectado directamente al Server VLC)	

Tabla 2.45: Direccionamiento de la topología tipo malla.

2.2.4.3 Capturas de pantalla de la red de distribución

La topología escogida para implementar el aumento o disminución de routers en la red de distribución, es la tipo malla.

Como anteriormente ya se realizó la práctica de streaming de video exitosamente en esta topología, lo primero es volver a enviar el video por la red como muestra la figura 2.91.

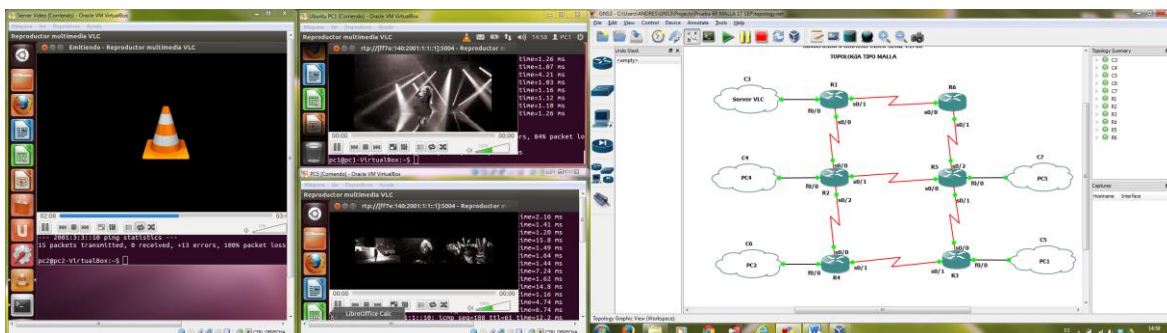


Figura 2.91: Envío de streaming de video

Como se observa en la figura 2.91, el streaming de video es enviado por el Server VLC y captado por los clientes PC1 y PC5, en el lado derecho de la figura se puede observar que en GNS3 están activados todos los routers (se prende la luz verde en todos los dispositivos de la red simulada).

Para conocer cuál es el camino que están atravesando los paquetes de datos por la red, nos ayudamos del comando *"traceroute"* el cual nos indicará cual es el camino que siguen los paquetes de streaming de video y as interfaces de entrada y salida de cada router.

A continuación se aplica un traceroute al cliente PC1 para averiguar cuál es el camino de los paquetes de datos.

```

pc2@pc2-VirtualBox: ~
pc2@pc2-VirtualBox:~$ traceroute 2001:3:3::10
traceroute to 2001:3:3::10 (2001:3:3::10), 30 hops max, 80 byte packets
 1  2001:1:1::1 (2001:1:1::1)  7.217 ms  7.215 ms  7.239 ms
 2  2001:1:2::2 (2001:1:2::2)  9.946 ms  9.940 ms  9.999 ms
 3  2001:2:4::4 (2001:2:4::4)  13.808 ms  15.237 ms  15.165 ms
 4  2001:4:3::3 (2001:4:3::3)  18.644 ms  3742.768 ms  493.949 ms
 5  2001:3:3::10 (2001:3:3::10)  14.960 ms  15.407 ms  15.440 ms
pc2@pc2-VirtualBox:~$

```

Figura 2.92: Comando traceroute desde Server VLC hacia cliente PC1

La figura 2.92 muestra que el camino utilizado es:

Server VLC → R1 → R2 → R4 → R3 → Cliente PC1

A continuación se aplica un traceroute al cliente PC5, para averiguar cuál es el camino de los paquetes de datos.

```

pc2@pc2-VirtualBox: ~
pc2@pc2-VirtualBox:~$ traceroute 2001:3:3::10
traceroute to 2001:3:3::10 (2001:3:3::10), 30 hops max, 80 byte packets
 1  2001:1:1::1 (2001:1:1::1)  7.217 ms  7.215 ms  7.239 ms
 2  2001:1:2::2 (2001:1:2::2)  9.946 ms  9.940 ms  9.999 ms
 3  2001:2:4::4 (2001:2:4::4)  13.808 ms  15.237 ms  15.165 ms
 4  2001:4:3::3 (2001:4:3::3)  18.644 ms  3742.768 ms  493.949 ms
 5  2001:3:3::10 (2001:3:3::10)  14.960 ms  15.407 ms  15.440 ms
pc2@pc2-VirtualBox:~$ traceroute 2001:5:5::10
traceroute to 2001:5:5::10 (2001:5:5::10), 30 hops max, 80 byte packets
 1  2001:1:1::1 (2001:1:1::1)  6.701 ms  6.667 ms  6.775 ms
 2  2001:1:2::2 (2001:1:2::2)  10.184 ms  10.112 ms  10.147 ms
 3  2001:2:5::5 (2001:2:5::5)  14.536 ms  16.883 ms  14.669 ms
 4  2001:5:5::10 (2001:5:5::10)  44.575 ms * *
pc2@pc2-VirtualBox:~$

```

Figura 2.93: Comando traceroute desde Server VLC hacia cliente PC5

La figura 2.93 muestra que el camino utilizado es:

Server VLC → R1 → R2 → R5 → Cliente PC5

Como se muestra en las figuras anteriores, el paso de los paquetes de datos es por el router R2 para ambos clientes.

Ahora, para conocer en qué tiempo se establece un nuevo camino de enrutamiento, vamos a apagar el router R2, cortando la transmisión de video por un momento hasta establecer nuevamente las tablas de enrutamiento, el nuevo camino debe ser obligatoriamente por el router R6.

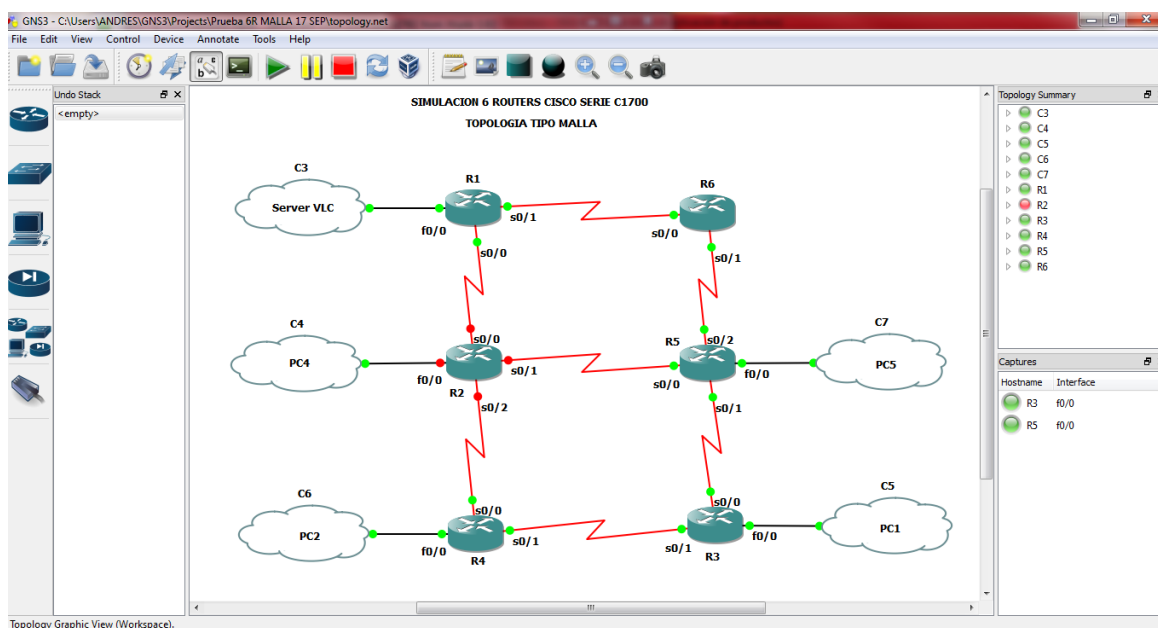


Figura 2.94: Router R2 es apagado en la transmisión de video streaming.

Al momento de parar el router R2, la transmisión de video se detiene porque el camino ha sido cortado, y ahora los routers restantes están buscando un nuevo camino.

Si nuevamente se emplea el comando traceroute, se puede observar que el camino aún no está establecido.

```

pc2@pc2-VirtualBox: ~
pc2@pc2-VirtualBox:~$ traceroute 2001:3:3::10
traceroute to 2001:3:3::10 (2001:3:3::10), 30 hops max, 80 byte
 1 2001:1:1::1 (2001:1:1::1)  8.068 ms  7.996 ms  8.072 ms
 2 2001:1:6::6 (2001:1:6::6)  9.153 ms  9.345 ms  9.401 ms
 3 2001:5:6::5 (2001:5:6::5) 13.241 ms 15.397 ms 13.547 ms
 4 2001:3:5::3 (2001:3:5::3) 20.948 ms 21.021 ms 21.130 ms
 5 2001:3:3::10 (2001:3:3::10) 14.926 ms 16.570 ms 18.158 ms
pc2@pc2-VirtualBox:~$ traceroute 2001:5:5::10
traceroute to 2001:5:5::10 (2001:5:5::10), 30 hops max, 80 byte
 1 2001:1:1::1 (2001:1:1::1)  7.759 ms  7.622 ms  7.733 ms
 2 2001:1:6::6 (2001:1:6::6)  3.300 ms  4.060 ms  4.127 ms
 3 2001:5:6::5 (2001:5:6::5) 11.486 ms 94.332 ms 12.174 ms
 4 2001:5:5::10 (2001:5:5::10) 94.304 ms 82.104 ms 2.787 ms
pc2@pc2-VirtualBox:~$ traceroute 2001:3:3::10
traceroute to 2001:3:3::10 (2001:3:3::10), 30 hops max, 80 byte
 1 2001:1:1::1 (2001:1:1::1) 40.756 ms 40.652 ms 40.741 ms
 2 2001:1:6::6 (2001:1:6::6) 24.260 ms 24.199 ms 24.128 ms
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 *

```

Figura 2.95: Traceroute desde Server VLC hacia cliente PC1

Luego de un tiempo se vuelve a establecer el camino.

```

pc2@pc2-VirtualBox: ~
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
pc2@pc2-VirtualBox:~$ traceroute 2001:3:3::10
traceroute to 2001:3:3::10 (2001:3:3::10), 30 hops max, 80 byte packets
 1 2001:1:1::1 (2001:1:1::1) 11.773 ms 11.787 ms 11.809 ms
 2 2001:1:6::6 (2001:1:6::6)  8.816 ms  8.921 ms  8.856 ms
 3 2001:5:6::5 (2001:5:6::5) 51.032 ms 51.101 ms 51.094 ms
 4 2001:3:5::3 (2001:3:5::3) 37.208 ms 38.261 ms 50.634 ms
 5 2001:3:3::10 (2001:3:3::10) 12.520 ms 12.578 ms 28.992 ms
pc2@pc2-VirtualBox:~$

```

Figura 2.96: Traceroute desde Server VLC hacia cliente PC1

La figura 2.96 muestra que el nuevo camino establecido por los routers restantes es:

Server VLC → R1 → R6 → R5 → R3 → Cliente PC1

```

pc2@pc2-VirtualBox: ~
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
pc2@pc2-VirtualBox:~$ traceroute 2001:3:3:10
traceroute to 2001:3:3:10 (2001:3:3:10), 30 hops max, 80 byte packets
 1 2001:1:1::1 (2001:1:1::1) 11.773 ms 11.787 ms 11.809 ms
 2 2001:1:6::6 (2001:1:6::6) 8.816 ms 8.921 ms 8.856 ms
 3 2001:5:6::5 (2001:5:6::5) 51.032 ms 51.101 ms 51.094 ms
 4 2001:3:5::3 (2001:3:5::3) 37.208 ms 38.261 ms 50.634 ms
 5 2001:3:3:10 (2001:3:3:10) 12.520 ms 12.578 ms 28.992 ms
pc2@pc2-VirtualBox:~$ traceroute 2001:5:5:10
traceroute to 2001:5:5:10 (2001:5:5:10), 30 hops max, 80 byte packets
 1 2001:1:1::1 (2001:1:1::1) 4.274 ms 4.279 ms 4.305 ms
 2 2001:1:6::6 (2001:1:6::6) 50.297 ms 51.990 ms 52.146 ms
 3 2001:5:6::5 (2001:5:6::5) 24.003 ms 38.084 ms 37.995 ms
 4 2001:5:5:10 (2001:5:5:10) 28.094 ms 28.017 ms 35.227 ms
pc2@pc2-VirtualBox:~$

```

Figura 2.97: Traceroute desde Server VLC hacia cliente PC5

Para el cliente PC5, el proceso es el mismo y se establece un nuevo camino el cual es:

Server VLC → R1 → R6 → R5 → Cliente PC5

Para conocer el tiempo que le toma a los routers de la red de distribución, actualizar las tablas de enrutamiento, ya que, manualmente se desconecta en router R2, se debe tomar datos mediante WIRESHARK en los puertos de los extremos del Servidor – Cliente, es decir, los datos deben tomarse en el puerto Fastethernet 0/0 del router R1 (el cual es el puerto de entrada de los paquetes de streaming de video hacia la red de distribución) y en el puerto Fastethernet 0/0 del router R3 (el cual es puerto de salida del streaming de video, luego de pasar por los routers de la red de distribución).

La toma de estos datos debe ser en el mismo periodo de tiempo, esto se logra, una vez que el streaming de video sea correcto, iniciar cada captura en cada puerto simultáneamente y de igual manera para detenerlos.

Los datos arrojados en un periodo de tiempo aproximado a 3 minutos con 25 segundos son los siguientes:

Server VLC

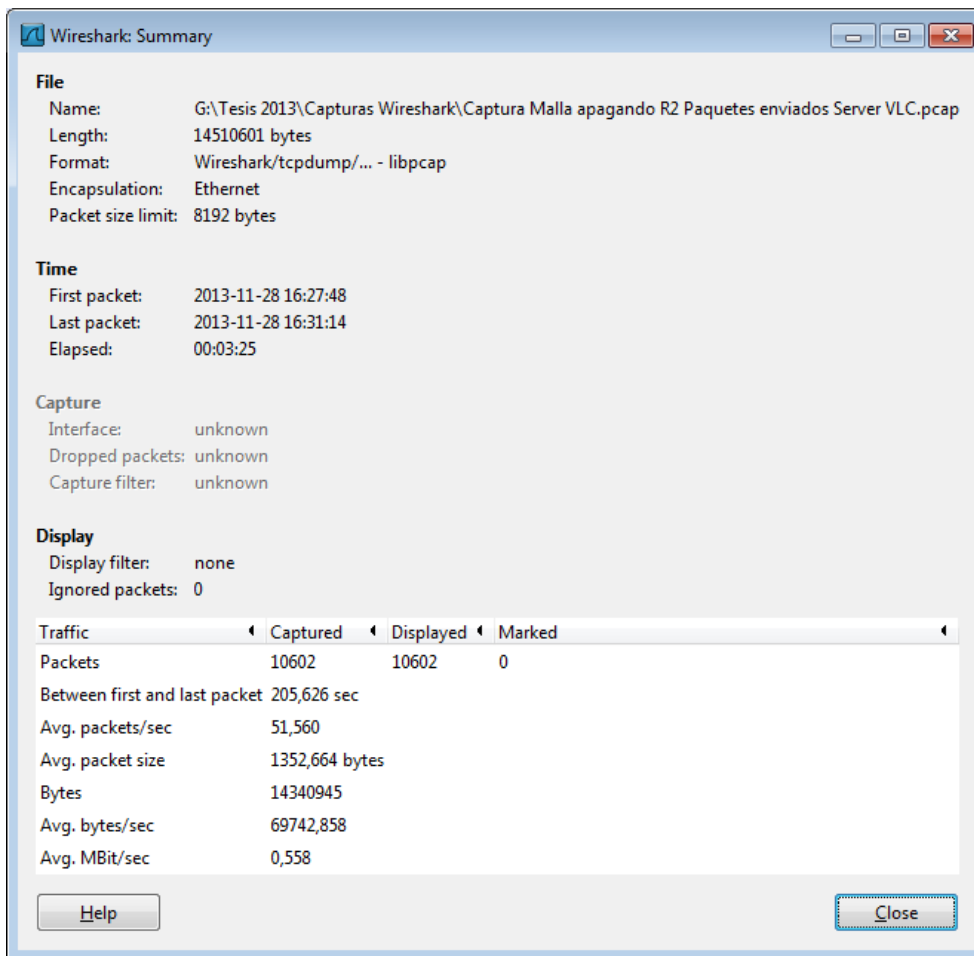


Figura 2.98: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 25 seg.
TIEMPO EN SEGUNDOS:	205.626 seg.
PAQUETES CAPTURADOS:	10602.00
PAQUETES MOSTRADOS:	10602.00
BYTES TOTALES:	14340945.00
PROMEDIO PAQUETES/SEG:	51560.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1352.664
PROMEDIO BYTES/SEG:	69742.858
PROMEDIO MBITS/SEG:	0,558

Tabla 2.46: Resumen de los datos mostrados en Wireshark.

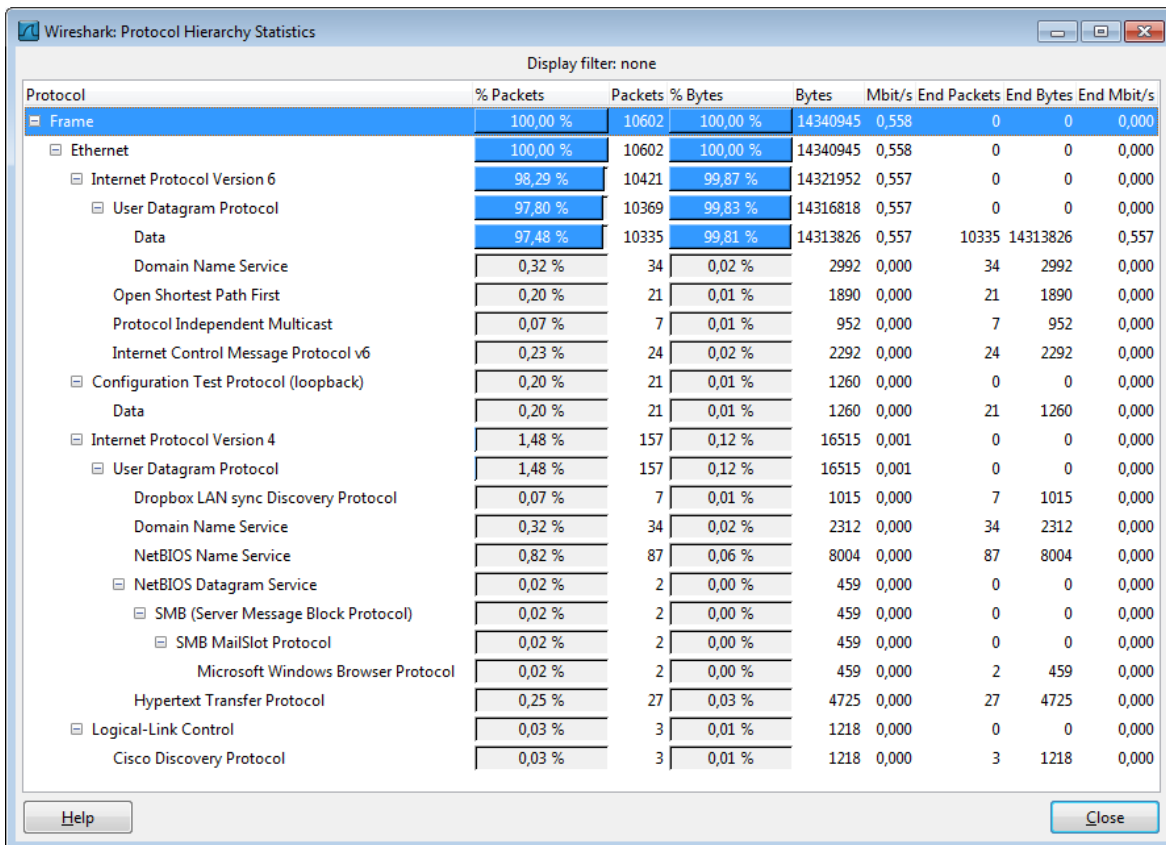


Figura 2.99: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 2.99 se encuentra en la página 103

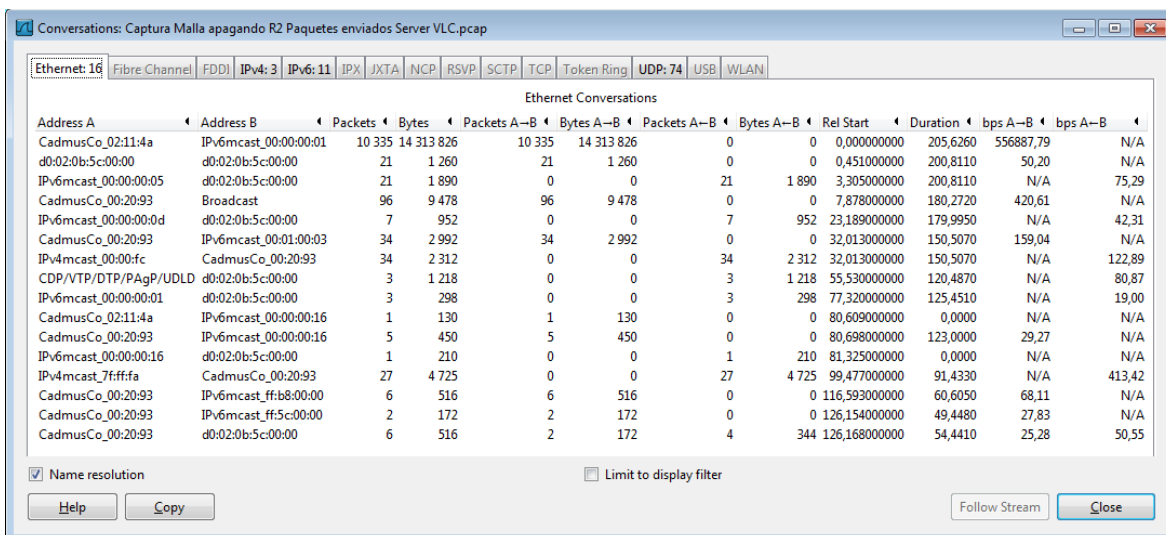


Figura 2.100: Paquetes Ethernet que atravesaron la red al momento de la captura

* La explicación de la figura 2.100 se encuentra en la página 104

Conversations: Captura Malla apagando R2 Paquetes enviados Server VLC.pcap

Ethernet: 16 Fibre Channel FDDI IPv4: 3 IPv6: 11 IPX JXTA NCP RSVP SCTP TCP Token Ring UDP: 74 USB WLAN

IPv6 Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	ff7e:140:2001:1:1::1	10 335	14 313 826	10 335	14 313 826	0	0	0,000000000	205,6260	556887,79	N/A
fe80::d202:bfff:fe5c:0	ff02::5	21	1 890	21	1 890	0	0	3,305000000	200,8110	75,29	N/A
fe80::d202:bfff:fe5c:0	ff02::d	7	952	7	952	0	0	23,189000000	179,9950	42,31	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:3	34	2 992	34	2 992	0	0	32,013000000	150,5070	159,04	N/A
fe80::d202:bfff:fe5c:0	ff02::1	3	298	3	298	0	0	77,320000000	125,4510	19,00	N/A
fe80::a00:27ff:fe02:114a	ff02::16	1	130	1	130	0	0	80,609000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::16	5	450	5	450	0	0	80,698000000	123,0000	29,27	N/A
fe80::d202:bfff:fe5c:0	ff02::16	1	210	1	210	0	0	81,325000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:ffb8:0	6	516	6	516	0	0	116,593000000	60,6050	68,11	N/A
fe80::c5d6:8a3:f8d5:1fe8	ff02::1:ff5c:0	2	172	2	172	0	0	126,154000000	49,4480	27,83	N/A
fe80::c5d6:8a3:f8d5:1fe8	fe80::d202:bfff:fe5c:0	6	516	2	172	4	344	126,168000000	54,4410	25,28	50,55

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 2.101: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 2.101 se encuentra en la página 105

Conversations: Captura Malla apagando R2 Paquetes enviados Server VLC.pcap

Ethernet: 16 Fibre Channel FDDI IPv4: 3 IPv6: 11 IPX JXTA NCP RSVP SCTP TCP Token Ring UDP: 74 USB WLAN

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1:1::10	47118	ff7e:140:2001:1:1::1	avt-profile-1	10 294	14 308 660	10 294	14 308 660	0	0	0,000000000	205,6260	556686,80	N/A
192.168.199.1	netbios-ns	192.168.199.255	netbios-ns	87	8 004	87	8 004	0	0	32,214000000	152,0090	421,24	N/A
2001:1:1::10	47119	ff7e:140:2001:1:1::1	avt-profile-2	41	5 166	41	5 166	0	0	2,510000000	199,9920	206,65	N/A
192.168.199.1	56077	239.255.255.250	ssdp	27	4 725	27	4 725	0	0	99,477000000	91,4330	413,42	N/A
192.168.199.1	db-lsp-disc	192.168.199.255	db-lsp-disc	7	1 015	7	1 015	0	0	7,878000000	180,2720	45,04	N/A
192.168.199.1	netbios-dgm	192.168.199.255	netbios-dgm	2	459	2	459	0	0	44,142000000	11,9380	307,59	N/A
fe80::c5d6:8a3:f8d5:1fe8	55594	ff02::1:3	llmnr	1	89	1	89	0	0	32,013000000	0,0000	N/A	N/A
192.168.199.1	51162	224.0.0.252	llmnr	1	69	1	69	0	0	32,013000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	63985	ff02::1:3	llmnr	1	92	1	92	0	0	33,443000000	0,0000	N/A	N/A
192.168.199.1	63894	224.0.0.252	llmnr	1	72	1	72	0	0	33,443000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	59328	ff02::1:3	llmnr	1	92	1	92	0	0	33,746000000	0,0000	N/A	N/A
192.168.199.1	54970	224.0.0.252	llmnr	1	72	1	72	0	0	33,746000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	54378	ff02::1:3	llmnr	1	92	1	92	0	0	34,255000000	0,0000	N/A	N/A
192.168.199.1	54870	224.0.0.252	llmnr	1	72	1	72	0	0	34,255000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	51510	ff02::1:3	llmnr	1	89	1	89	0	0	34,565000000	0,0000	N/A	N/A
192.168.199.1	50046	224.0.0.252	llmnr	1	69	1	69	0	0	34,565000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	50630	ff02::1:3	llmnr	1	89	1	89	0	0	37,119000000	0,0000	N/A	N/A
192.168.199.1	65501	224.0.0.252	llmnr	1	69	1	69	0	0	37,119000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	60883	ff02::1:3	llmnr	1	89	1	89	0	0	39,670000000	0,0000	N/A	N/A
192.168.199.1	51422	224.0.0.252	llmnr	1	69	1	69	0	0	39,670000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	61009	ff02::1:3	llmnr	1	92	1	92	0	0	47,462000000	0,0000	N/A	N/A
192.168.199.1	53657	224.0.0.252	llmnr	1	72	1	72	0	0	47,462000000	0,0000	N/A	N/A
fe80::c5d6:8a3:f8d5:1fe8	61612	ff02::1:3	llmnr	1	89	1	89	0	0	92 01 3000000	0 0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 2.102: Paquetes UDP que atravesaron la red al momento de la captura

* La explicación de la figura 2.102 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	10602	0,051560	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	55	0,000267	0,52%
80-159	220	0,001070	2,08%
160-319	30	0,000146	0,28%
320-639	3	0,000015	0,03%
640-1279	0	0,000000	0,00%
1280-2559	10294	0,050062	97,09%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.103: Rangos de las diferentes longitudes de los paquetes capturados

* La explicación de la figura 2.103 se encuentra en la página 106

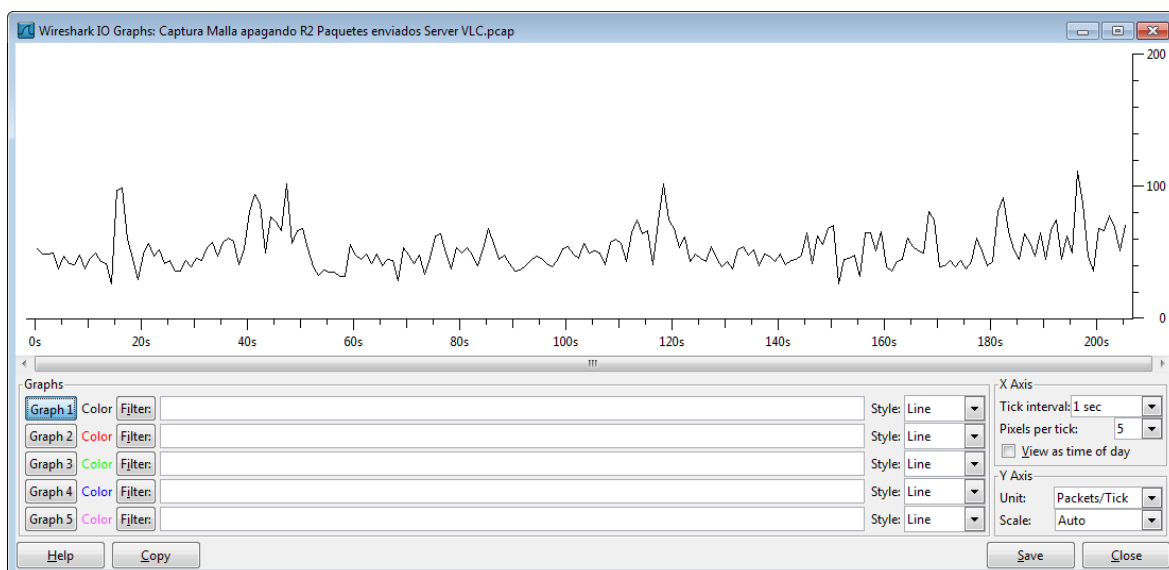


Figura 2.104: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

Ciente PC1

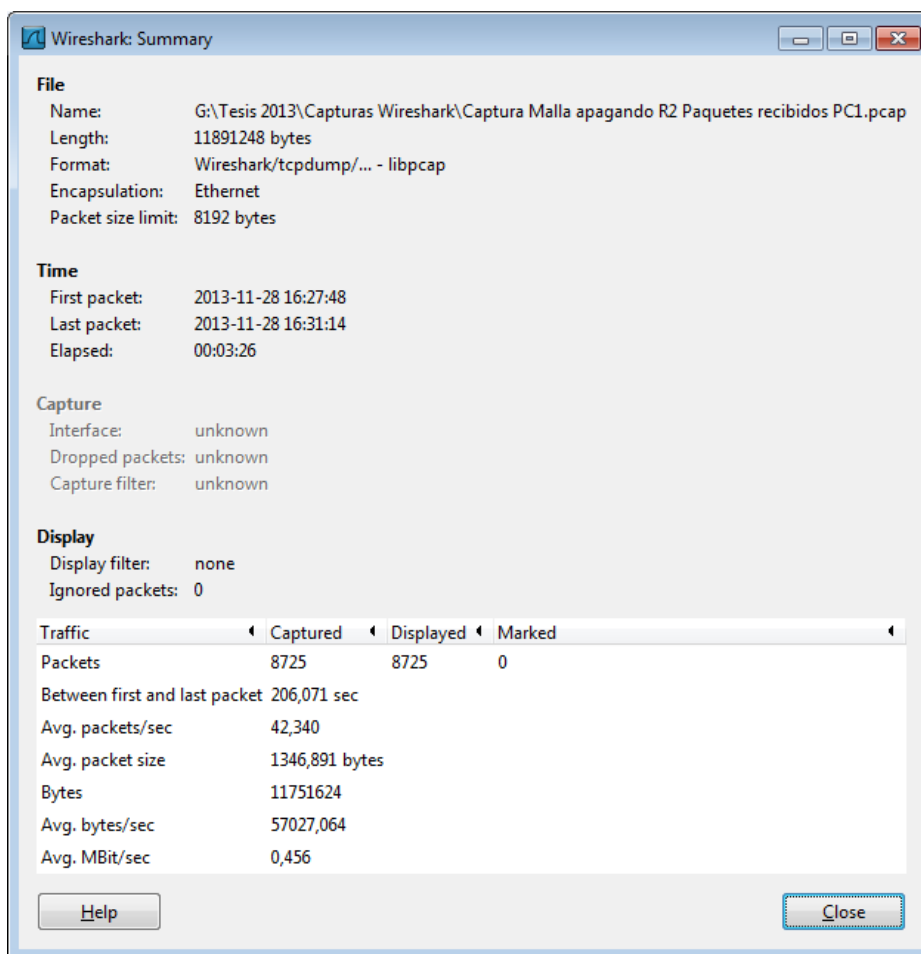


Figura 2.105: Resumen de los paquetes totales capturados por Wireshark, recibidos por el Cliente PC1 en el puerto Fastethernet 0/0 del router R3

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	3 min 26 seg.
TIEMPO EN SEGUNDOS:	206.071 seg.
PAQUETES CAPTURADOS:	8725.00
PAQUETES MOSTRADOS:	8725.00
BYTES TOTALES:	11751624.00
PROMEDIO PAQUETES/SEG:	42340.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1346.891
PROMEDIO BYTES/SEG:	57027.064
PROMEDIO MBITS/SEG:	0,456

Tabla 2.47: Resumen de los datos mostrados en Wireshark.

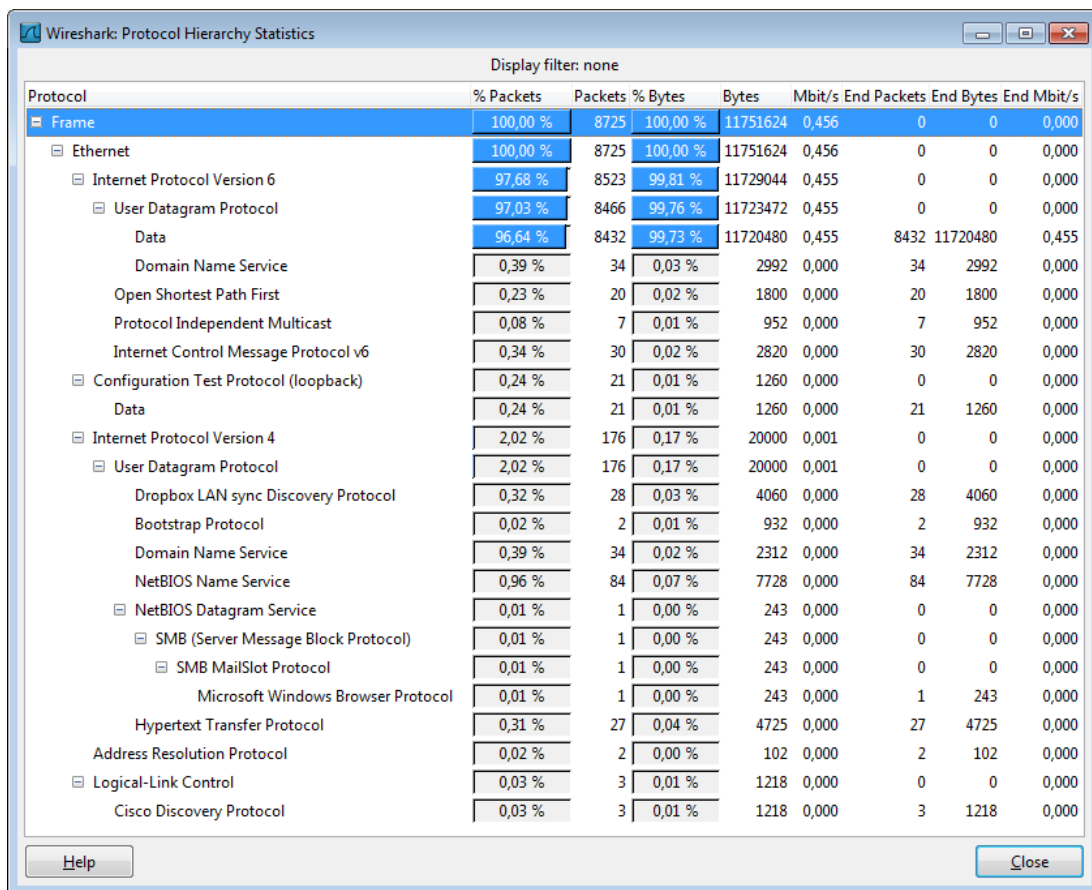


Figura 2.106: Resumen más detallado de los paquetes capturados por Wireshark

* La explicación de la figura 2.106 se encuentra en la página 103

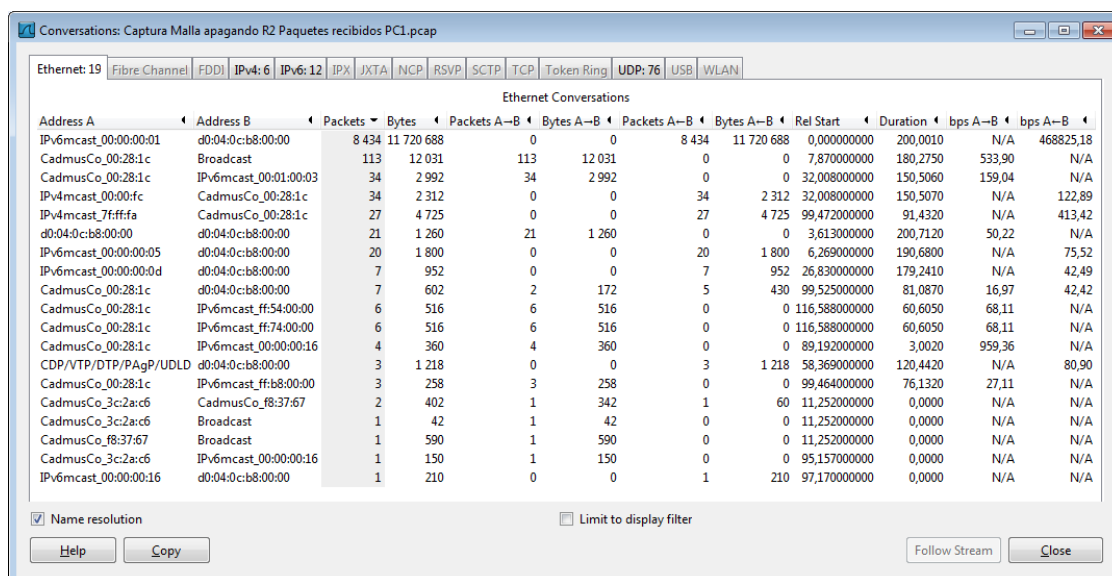


Figura 2.107: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 2.107 se encuentra en la página 104

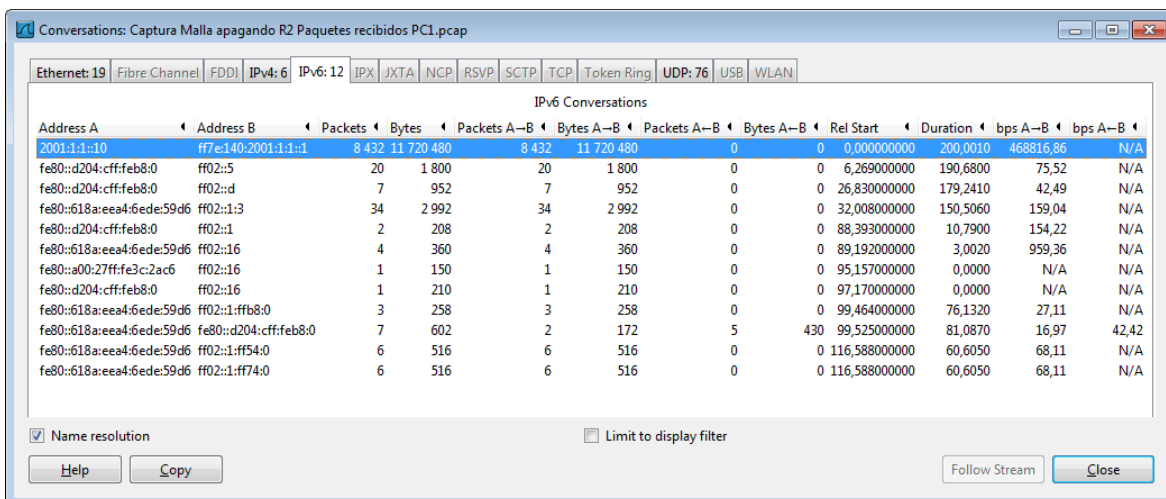


Figura 2.108: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 2.108 se encuentra en la página 105

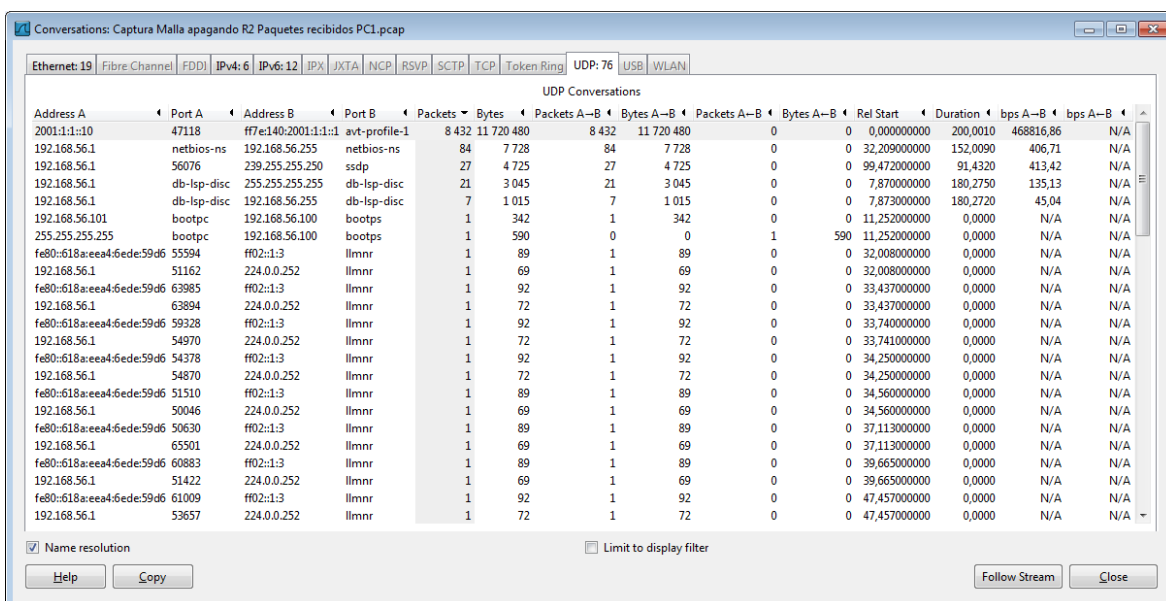


Figura 2.109: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 2.109 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	8725	0,042340	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	57	0,000277	0,65%
80-159	202	0,000980	2,32%
160-319	29	0,000141	0,33%
320-639	5	0,000024	0,06%
640-1279	0	0,000000	0,00%
1280-2559	8432	0,040918	96,64%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 2.110: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 2.110 se encuentra en la página 106

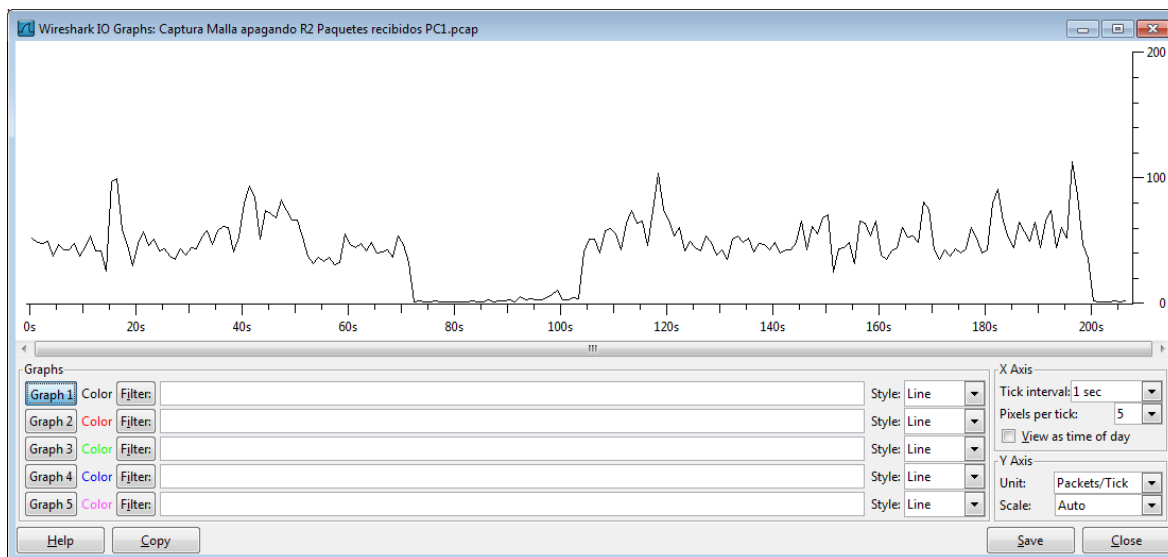


Figura 2.111: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

2.2.4.4 Cálculo de los parámetros de calidad en la red de distribución

2.2.4.4.1 Cálculos de la Velocidad de Transmisión

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	6 ROUTERS TIPO MALLA CON APAGADO DE 1 ROUTER			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	14340945,00	14321952,00	14313826,00	205,626
CLIENTE PC5	11746886,00	11708995,00	11672521,00	205,926
CLIENTE PC1	11751624,00	11729044,00	11720480,00	206,071
TABLA DE VELOCIDADES				
	SERVER VLC	CLIENTE PC5	CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	69742,86	57044,21	57027,06	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	69650,49	56860,21	56917,49	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	69610,97	56683,09	56875,93	

Tabla 2.48: Velocidades de transmisión obtenidas en la simulación.

2.2.4.4.2 *Cálculos de Latencia*

PRUEBA N° 1				
N°	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
6	35,00	1058,00	34,80	65,70
7	1009,00	1035,00	7,51	130,00
8	373,00	34,40	7,04	269,00
9	4,56	21,70	15,80	150,00
10	218,00	221,00	1,25	57,80
11	2,78	24,00	22,10	30,70
12	34,70	88,60	19,90	28,40
13	7,63	22,80	47,00	48,50
14	31,10	89,70	75,00	192,00
15	50,90	80,80	689,00	45,90
16	212,00	38,00	39,90	29,40
17	25,90	41,70	35,00	1,85
18	58,10	39,50	30,00	18,10
19	90,10	41,70	72,30	36,60
20	47,30	18,60	22,20	59,00
21	27,70	52,20	40,80	346,00
22	13,40	12,40	33,70	40,40
23	51,50	14,40	50,70	55,00
24	28,10	29,10	40,90	36,30
25	65,30	23,50	1,31	27,80
26	41,20	73,00	22,90	26,30
27	68,00	188,00	38,20	110,00
28	26,50	36,30	23,30	1,12
29	20,50	9,61	31,30	1,26
30	3,38	6,06	50,30	6,25
31	1,42	9,80	73,10	0,96
32	1,39	2,80	44,80	1,11
33	0,79	6,99	40,80	1,22
34	1,56	1,76	47,10	1,12
35	2,35	1,39	29,60	1,10
36	1,36	2,10	60,00	2,26
37	1,90	1,59	44,30	1,13
38	2,61	3,23	35,70	1,24
39	1,07	1,32	0,80	1,22
40	1,58	1,48	3,54	1,11
41	1,00	2,48	1,02	0,99
42	2,72	2,48	0,84	1,15
43	1,64	1,55	4,80	0,80
44	1,85	4,31	3,96	1,34

Tabla 2.49: Tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 2				
N°	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
6	44,00	3,44	39,50	682,00
7	12,00	2,18	41,70	205,00
8	750,00	2,16	1035,00	13,00
9	122,00	1014,00	52,20	18,70
10	1,70	122,00	124,00	137,70
11	7,17	11,40	14,40	10,90
12	22,90	5,00	291,00	45,60
13	38,20	5,54	23,50	107,00
14	23,30	3,31	131,00	19,20
15	31,30	8,62	1,25	109,00
16	50,30	41,70	11,40	11,80
17	73,10	18,60	1,40	285,00
18	19,50	52,20	1,29	145,00
19	1,58	12,40	57,80	83,50
20	1,86	14,40	30,70	16,10
21	1,55	29,10	28,40	9,44
22	1,72	23,50	48,50	10,90
23	36,30	73,00	19,20	17,10
24	27,80	1,20	1,15	1,49
25	26,30	1,28	23,30	3,98
26	1,10	1,28	90,10	36,30
27	1,12	1,30	47,30	9,61
28	1,26	18,50	27,70	6,06
29	6,25	15,50	13,40	9,80
30	0,96	7,17	51,50	2,80
31	1,11	24,00	7,27	4,12
32	1,22	1,55	1,29	0,90
33	1,12	22,30	1,31	2,67
34	1,83	1,63	10,70	1,05
35	845,00	17,50	19,20	29,10
36	1,44	2,58	1,09	23,50
37	1,72	1,51	1,18	1,99
38	8,56	1,05	2,23	1,30
39	6,22	11,10	2,56	1,20
40	4,50	1,74	2,25	1,28
41	98,00	85,00	4,85	1,28
42	250,00	77,00	0,90	1,62
43	1,49	9,58	3,30	7,06
44	11,20	54,00	1,25	2,25
45	1,46	1,44	1,50	1,50

**Tabla 2.50: Tabla de valores de tiempos de retardo,
Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.**

PRUEBA N° 3				
N°	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
6	47,30	155,00	75,30	139,00
7	277,00	201,00	128,00	52,50
8	1034,00	115,00	321,00	270,00
9	384,00	86,20	107,00	160,00
10	100,00	307,00	120,00	171,00
11	81,10	28,40	127,00	14,90
12	21,20	48,50	54,40	10,80
13	14,30	19,20	15,10	13,00
14	50,20	52,50	2,35	235,00
15	12,70	27,00	1,58	192,20
16	14,90	163,00	54,70	51,40
17	55,60	228,00	203,00	77,50
18	18,50	86,20	37,10	47,00
19	18,10	119,00	199,00	145,00
20	36,60	17,20	164,00	71,30
21	1,81	8,56	75,80	52,60
22	1,49	6,22	15,40	220,00
23	1,68	4,50	12,60	13,60
24	11,40	1,35	1,42	13,40
25	1,00	2,01	1,53	8,55
26	1,75	1,49	2,03	7,64
27	1,59	11,20	1,45	1,86
28	1,69	34,90	1,49	1,55
29	1,45	16,00	7,93	1,46
30	1,75	92,30	7,27	2,12
31	1,37	49,50	1,29	1,76
32	1,11	16,20	1,31	1,74
33	1,12	21,90	8,45	1,59
34	0,87	1,75	1,51	7,95
35	11,40	1,53	1,41	1,45
36	1,00	1,51	24,50	1,48
37	1,75	1,48	1,77	1,50
38	1,59	1,43	6,03	1,44
39	1,69	15,40	1,45	1,39
40	6,46	25,00	1,59	5,25
41	2,99	15,90	2,18	27,00
42	19,80	2,39	2,28	16,00
43	1,34	1,61	2,26	17,10
44	1,05	1,39	22,30	20,50
45	11,10	1,28	22,40	40,80

**Tabla 2.51: Tabla de valores de tiempos de retardo,
Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.**

PRUEBA N° 1	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	2596,04	3377,01	1860,28	1914,57
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00	45,00	45,00
PAQUETES ERDIDOS	5,00	5,00	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	11,11	11,11	11,11
PAQUETE MIN TIEMPO (mseg)	0,79	1,32	0,80	0,80
PAQUETE MAX TIEMPO (mseg)	1009,00	1058,00	689,00	346,00
PAQUETE TIEMPO PROMEDIO (mseg)	57,69	75,04	41,34	42,55

Tabla 2.52: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 2	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	2791,15	1827,85	2283,95	2117,35
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	44,00	45,00	45,00	44,00
PAQUETES PERDIDOS	6,00	5,00	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	11,11	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	0,96	1,05	0,90	0,90
PAQUETE MAX TIEMPO (mseg)	845,00	1014,00	1035,00	682,00
PAQUETE TIEMPO PROMEDIO (mseg)	61,26	40,62	50,75	48,12

Tabla 2.53: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	2276,26	2018,10	1865,10	2251,71
PAQUETES TRANSMITIDOS	50,00	50,00	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00	45,00	45,00
PAQUETES PERDIDOS	5,00	5,00	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	11,11	11,11	11,11
PAQUETE MIN TIEMPO (mseg)	0,87	1,28	1,29	1,39
PAQUETE MAX TIEMPO (mseg)	1034,00	307,00	321,00	270,00
PAQUETE TIEMPO PROMEDIO (mseg)	50,58	44,85	41,45	50,04

Tabla 2.54: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

A continuación se presenta un cuadro con el resumen de las 3 pruebas realizadas mediante el comando PING.

RESUMEN	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	7663,44	7222,96	6009,33	6283,63
PAQUETES TRANSMITIDOS	150,00	150,00	150,00	150,00
PAQUETES RECIBIDOS	134,00	135,00	135,00	134,00
PAQUETES PERDIDOS	16,00	15,00	15,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,00	10,00	10,67
PAQUETE MIN TIEMPO (mseg)	0,79	1,05	0,80	0,80
PAQUETE MAX TIEMPO (mseg)	1034,00	1058,00	1035,00	682,00
PAQUETE TIEMPO PROMEDIO (mseg)	56,51	53,50	44,51	46,90

Tabla 2.55: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING para cada cliente (PC1 y PC5) que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 56.51 mseg.
- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 53.50 mseg.
- Latencia calculada desde el Server VLC a Cliente PC5
Latencia = 44.51 mseg.
- Latencia calculada desde el Cliente PC5 al Server VLC
Latencia = 46.90 mseg.

2.2.4.4.3 Cálculos de Jitter

CALCULO DE JITTER						
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER	CLIENTE PC5	JITTER
14	1009,00	-974,00	1035,00	23,00	130,00	-64,30
15	373,00	636,00	34,40	1000,60	269,00	-139,00
16	4,56	368,44	21,70	12,70	150,00	119,00
17	218,00	-213,44	221,00	-199,30	57,80	92,20
18	2,78	215,22	24,00	197,00	30,70	27,10
19	34,70	-31,92	88,60	-64,60	28,40	2,30
20	7,63	27,07	22,80	65,80	48,50	-20,10
21	31,10	-23,47	89,70	-66,90	192,00	-143,50
22	50,90	-19,80	80,80	8,90	45,90	146,10
23	212,00	-161,10	38,00	42,80	29,40	16,50
24	25,90	186,10	41,70	-3,70	1,85	27,55
25	58,10	-32,20	39,50	2,20	18,10	-16,25
26	90,10	-32,00	41,70	-2,20	36,60	-18,50
27	47,30	42,80	18,60	23,10	59,00	-22,40
28	27,70	19,60	52,20	-33,60	346,00	-287,00
29	13,40	14,30	12,40	39,80	40,40	305,60
30	51,50	-38,10	14,40	-2,00	55,00	-14,60
31	28,10	23,40	29,10	-14,70	36,30	18,70
32	65,30	-37,20	23,50	5,60	27,80	8,50
33	41,20	24,10	73,00	-49,50	26,30	1,50
34	68,00	-26,80	188,00	-115,00	110,00	-83,70
35	26,50	41,50	36,30	151,70	1,12	108,88
36	20,50	6,00	9,61	26,69	1,26	-0,14
37	3,38	17,12	6,06	3,55	6,25	-4,99
38	1,42	1,96	9,80	-3,74	0,96	5,30
39	1,39	0,03	2,80	7,00	1,11	-0,16
40	0,79	0,60	6,99	-4,19	1,22	-0,11
41	1,56	-0,77	1,76	5,23	1,12	0,10
42	2,35	-0,79	1,39	0,37	1,10	0,02
43	1,36	0,99	2,10	-0,71	2,26	-1,16
44	1,90	-0,54	1,59	0,51	1,13	1,13
45	2,61	-0,71	3,23	-1,64	1,24	-0,11
46	1,07	1,54	1,32	1,91	1,22	0,02
47	1,58	-0,51	1,48	-0,16	1,11	0,11
48	1,00	0,58	2,48	-1,00	0,99	0,12
49	2,72	-1,72	2,48	0,00	1,15	-0,16
50	1,64	1,08	1,55	0,93	0,80	0,35
JITTER MIN		-974,00		-199,30		-287,00
JITTER MAX		636,00		1000,60		305,60

Tabla 2.56: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

2.2.4.4.4 Cálculos de Pérdida de Paquetes

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING			
TOPOLOGIA:	6 ROUTERS TIPO MALLA CON APAGADO DE 1 ROUTER		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	3 min 25 seg.	3 min 26 seg.	3 min 26 seg.
TIEMPO EN SEGUNDOS:	205.626 seg.	205.926 seg.	206.071 seg.
PAQUETES CAPTURADOS:	10602.00	8714.00	8725.00
PAQUETES MOSTRADOS:	10602.00	8714.00	8725.00
BYTES TOTALES:	14340945.00	11746886,00	11751624.00
PROMEDIO PAQUETES/SEG:	51560.00	42350.00	42340.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.352.664	1.347.986	1.346.891
PROMEDIO BYTES/SEG:	69.742.858	57.044.210	57.027.064
PROMEDIO MBITS/SEG:	0,558	0,456	0,456

Tabla 2.57: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la topología tipo malla.

En la tabla comparativa, podemos observar, que a diferencia de las tablas de las prácticas anteriores, existen pérdidas de paquetes, debido a la interrupción del camino trazado previamente por los paquetes de streaming de video.

Vemos que entre los Clientes PC1 y PC5, existe prácticamente la misma cantidad de paquetes recibidos en el mismo con una velocidad de transmisión iguales en ambos casos.

Para el caso del Server VLC, podemos observar claramente que éste envió mucho más paquetes de los que los clientes PC1 y PC5 pudieron receptor, esta pérdida de paquetes se produjo al momento de apagar el Router R2, lo cual produjo que la red vuelva a calcular una nueva ruta para el envío de paquetes, mientras tanto los paquetes que el Servidor VLC se encontraba enviando, eran descartados por la red.

En resumen, El Server VLC envió mucha más cantidad de paquetes a la red en el mismo tiempo de transmisión del video streaming, lo cual da como velocidad de transmisión promedio de 0.558 Mbits/seg. Para los clientes PC1 y PC5 si bien el tiempo de recepción de video streaming fue el mismo, la cantidad de paquetes fue menor, dando como resultado una velocidad de transmisión promedio de 0.456 Mbits/seg.

Es decir, la cantidad de pérdida de paquetes es:

PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
PAQUETES CAPTURADOS:	10602,00	8714,00	8725,00
BYTES TOTALES:	14340945	11746886	11751624
BYTES PERDIDOS:	0	2594059	2589321
PERDIDA DE PAQUETES:	0	1888,00	1877,00

Tabla 2.58: Tabla comparativa de valores de pérdida de paquetes.

A la vista del Usuario, esta pérdida de paquetes se puede resumir en:

- La señal de video streaming se interrumpe al 1min 1 seg. empezado la transmisión.
- La pantalla queda congelada con la última imagen captada por el usuario.
- Luego de un tiempo igual a:

$$\text{Velocidad de Transmisión} = \frac{\text{Bytes Totales}}{\text{Tiempo de la Transferencia}}$$

$$\text{Tiempo de la transferencia} = \frac{\text{Bytes Totales}}{\text{Velocidad de Transmisión}}$$

$$\text{Tiempo de la transferencia} = \frac{2594059 \text{ Bytes}}{0.456 \frac{\text{Mbits}}{\text{seg}}}$$

$$\textit{Tiempo de restauracion de la se\u00f1al} = \frac{2594059.00 \text{ Bytes}}{0.456 \frac{\text{MBits}}{\text{seg}}}$$

$$\textit{Tiempo de restauracion de la se\u00f1al} = \frac{2594059.00 \text{ Bytes}}{57027.064 \frac{\text{Bytes}}{\text{seg}}}$$

$$\textit{Tiempo de restauracion de la se\u00f1al} = \frac{2594059.00 \text{ Bytes}}{57027.064 \frac{\text{Bytes}}{\text{seg}}}$$

$$\textit{Tiempo de restauracion de la se\u00f1al} = 45.49 \text{ seg.}$$

El cliente vuelve a captar la se\u00f1al del streaming de video, luego de un tiempo aproximado de 45.49 seg.

CAPÍTULO III

DESARROLLO DEL PROTOTIPO

3.1 DISEÑO DEL PROTOTIPO PROPUESTO

Con el objetivo de comprobar la validez de los datos, se propone construir un prototipo sencillo de red para IPTV, el cual contendrá 2 routers implementados IPv6, un servidor de IPTV y una estación de trabajo para acceder al servicio de streaming de video.

El prototipo se construirá en el laboratorio de la facultad de Redes de Información, con dispositivos del mismo.

Simultáneamente se implementará el mismo diseño en GNS3, y compararán los resultados de la red virtual con la red física.

A continuación se muestra el diseño físico y virtual a implementar:

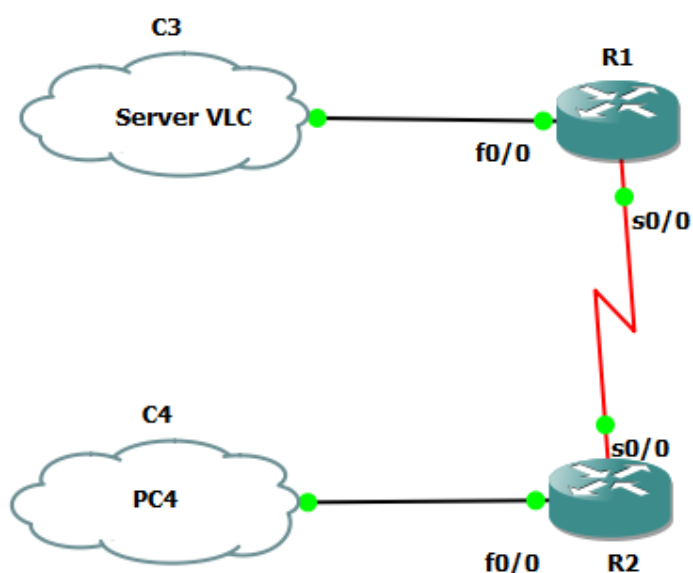


Figura 3.1: Diseño de la red a implementar en GNS3 y en el laboratorio.

3.1.1 DIRECCIONAMIENTO DE LA RED FÍSICA Y VIRTUAL A IMPLEMENTAR.

DISPOSITIVO	DIRECCION IPV6	GATEWAY
Server VLC	2001:1:1::10/64	2001:1:1::1
CLIENTE PC1	2001:2:2::10/64	2001:2:2::2
ROUTER R1		
Fastethernet 0/0	2001:1:1::1/64	
Serial 0/0	2001:1:2::1/64	
ROUTER R2		
Fastethernet 0/0	2001:2:2::2/64	
Serial 0/0	2001:1:2::2/64	
DIRECCION EMBEDDED MULTICAST A UTILIZAR		
Grupo Multicast Embedded	FF07:140:2001:1:1::1	
PROTOCOLO DE ENRUTAMIENTO UTILIZADO		
PROTOCOLO:	OSPFv6	
GRUPO:	1	
AREA:	0	
ROUTERS IMPLEMENTADOS:	Todos los Routers de la red de distribución	
RP SELECCIONADO		
ROUTER:	R1 (Conectado directamente al Server VLC)	

Tabla 3.1: Direccionamiento del prototipo.

3.1.1.1 Capturas de pantalla de la red virtual

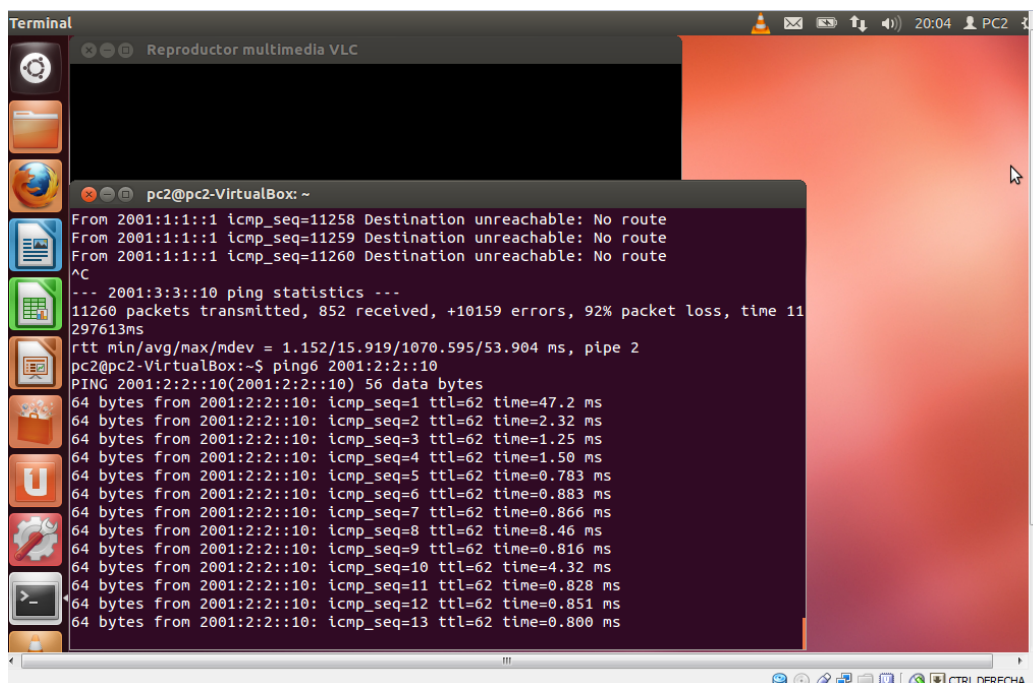


Figura 3.2: Ping desde Server VLC hacia Cliente PC1

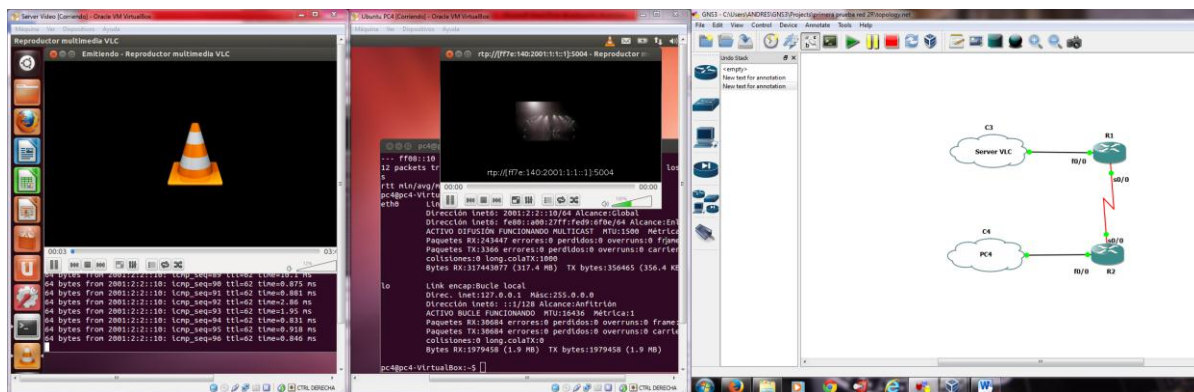


Figura 3.3: Streaming de video desde servidor VLC hacia Cliente PC1

La figura 3.3, muestra la red de distribución implementada, y el streaming de video enviado desde el Server VLC hacia el Cliente PC1.

Server VLC

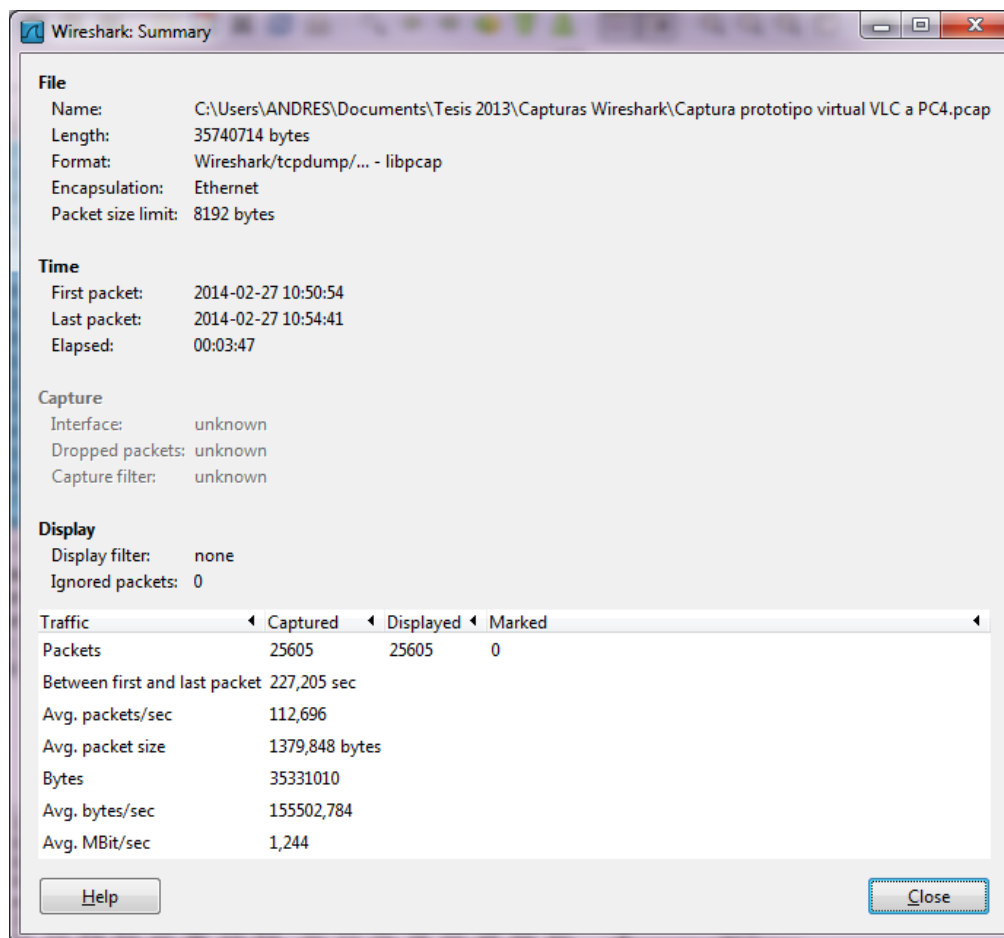


Figura 3.4: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 47 seg.
TIEMPO EN SEGUNDOS:	227.205 seg.
PAQUETES CAPTURADOS:	25605.00
PAQUETES MOSTRADOS:	25605.00
BYTES TOTALES:	35331010.00
PROMEDIO PAQUETES/SEG:	112696.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1379.848
PROMEDIO BYTES/SEG:	155502.784
PROMEDIO MBITS/SEG:	1.244

Tabla 3.2: Resumen de los datos mostrados en Wireshark.

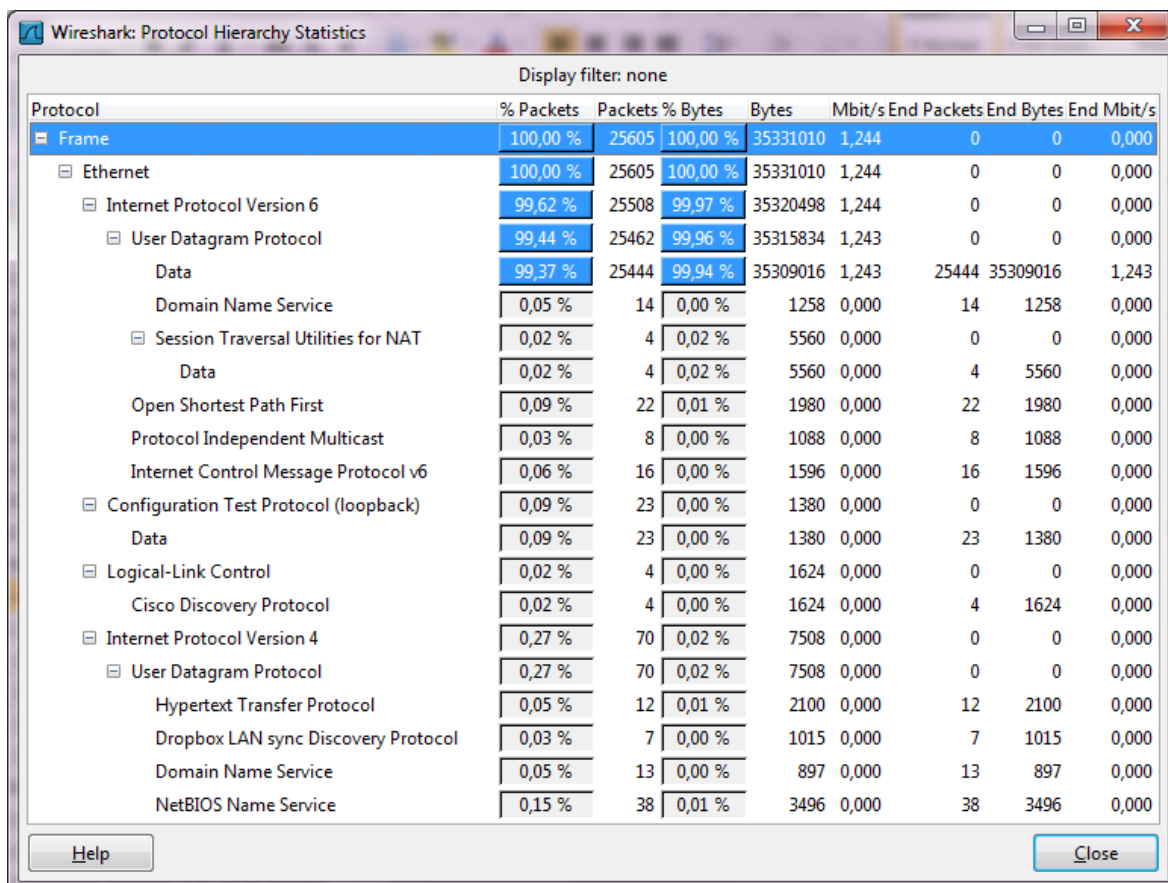


Figura 3.5: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 3.5 se encuentra en la página 103

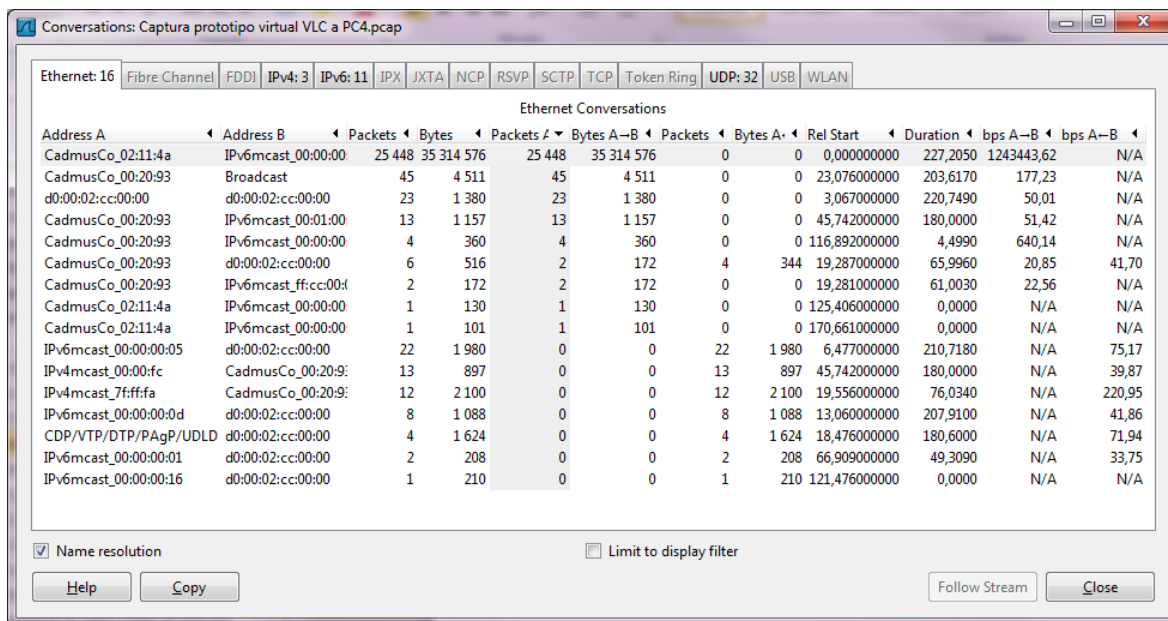


Figura 3.6: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 3.6 se encuentra en la página 104

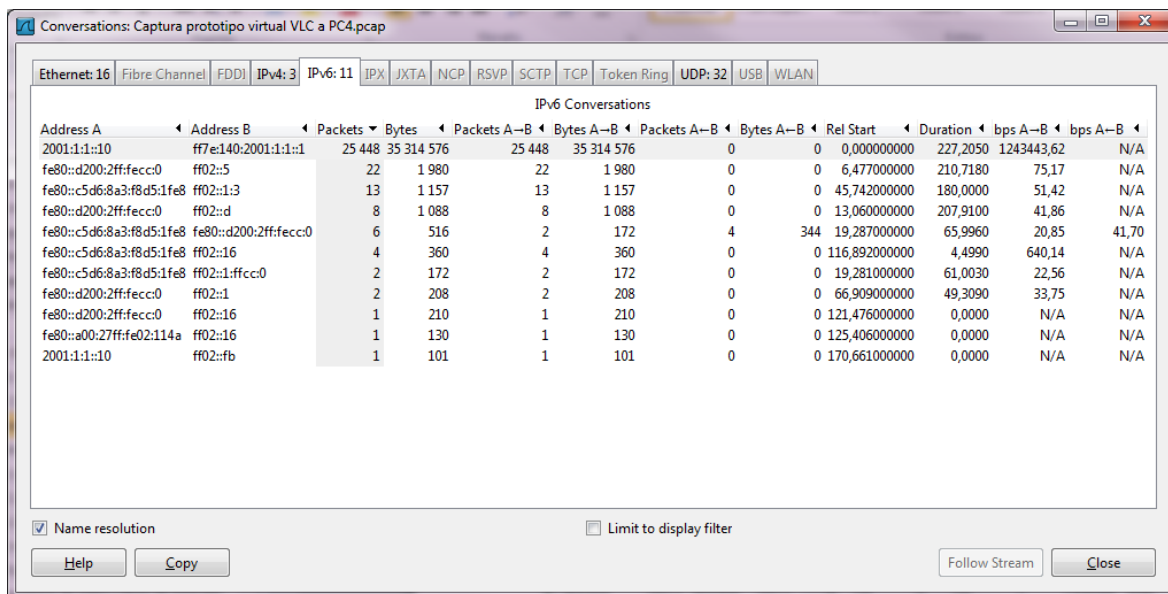


Figura 3.7: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 3.7 se encuentra en la página 105

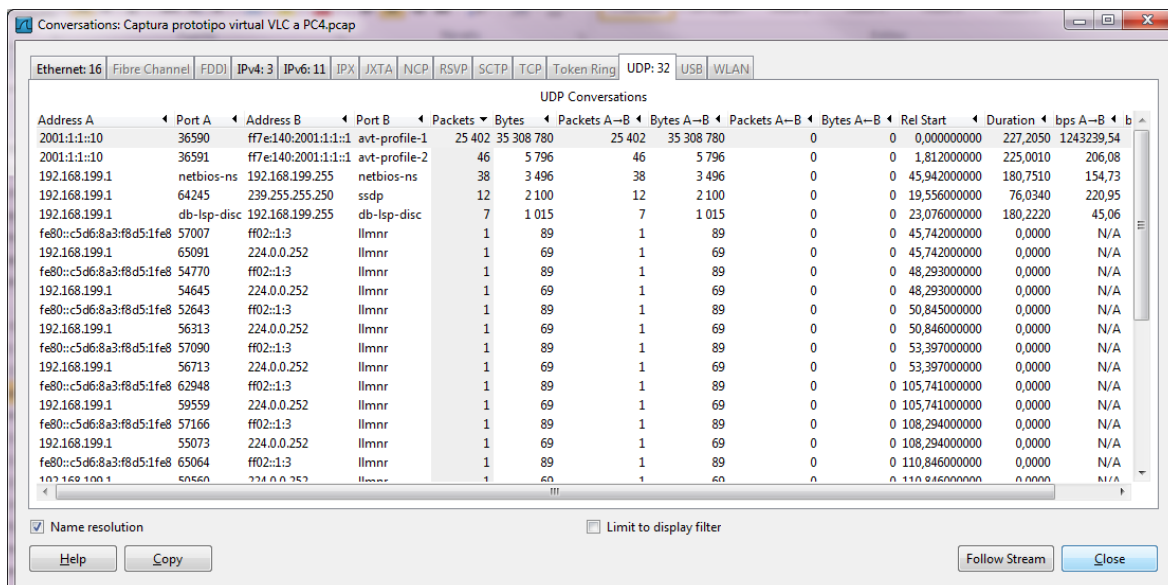


Figura 3.8: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 3.8 se encuentra en la página 105

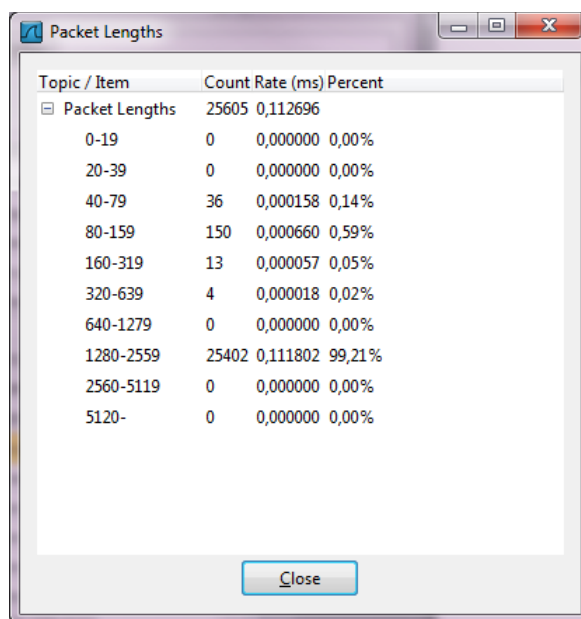


Figura 3.9: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 3.9 se encuentra en la página 106

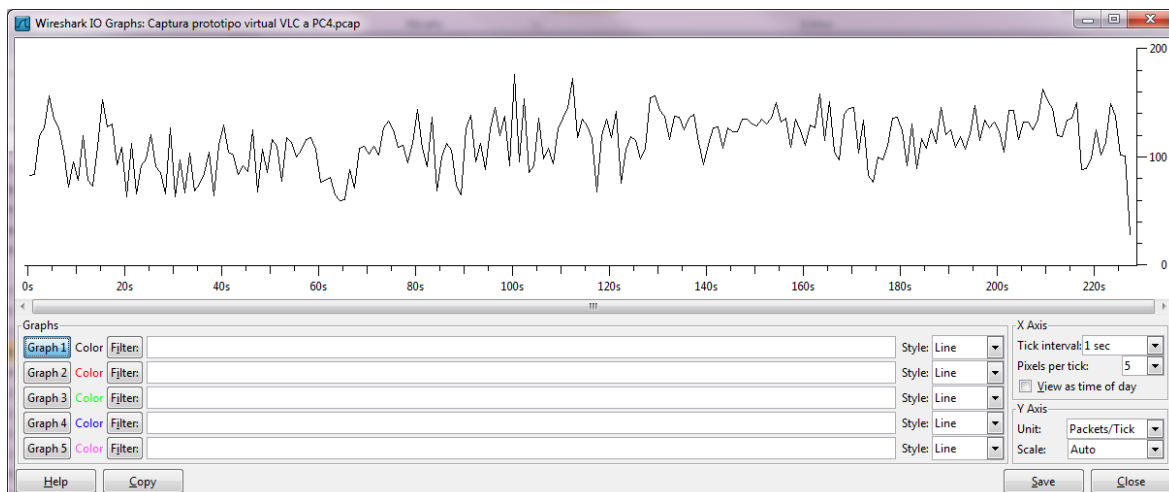


Figura 3.10: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC1

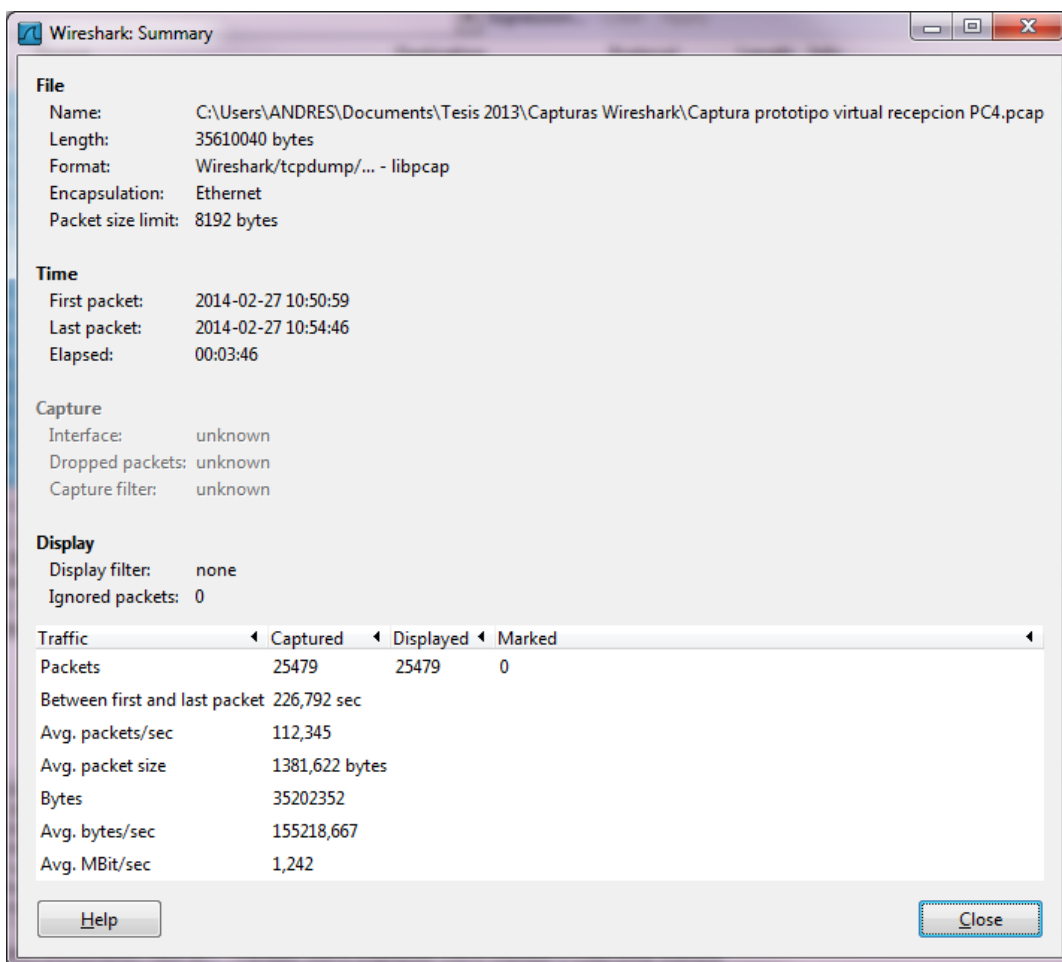


Figura 3.11: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R2.

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	3 min 46 seg.
TIEMPO EN SEGUNDOS:	226.792 seg.
PAQUETES CAPTURADOS:	25479.00
PAQUETES MOSTRADOS:	25479.00
BYTES TOTALES:	35202352.00
PROMEDIO PAQUETES/SEG:	112345.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1381.622
PROMEDIO BYTES/SEG:	155218.667
PROMEDIO MBITS/SEG:	1.242

Tabla 3.3: Resumen de los datos mostrados en Wireshark.

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	25479	100,00 %	35202352	1,242	0	0	0,000
Ethernet	100,00 %	25479	100,00 %	35202352	1,242	0	0	0,000
Internet Protocol Version 6	99,59 %	25375	99,97 %	35191210	1,241	0	0	0,000
User Datagram Protocol	99,41 %	25329	99,95 %	35186506	1,241	0	0	0,000
Data	99,33 %	25309	99,94 %	35179510	1,241	25309	35179510	1,241
Domain Name Service	0,06 %	16	0,00 %	1436	0,000	16	1436	0,000
Session Traversal Utilities for NAT	0,02 %	4	0,02 %	5560	0,000	0	0	0,000
Data	0,02 %	4	0,02 %	5560	0,000	4	5560	0,000
Open Shortest Path First	0,09 %	23	0,01 %	2070	0,000	23	2070	0,000
Protocol Independent Multicast	0,03 %	8	0,00 %	1088	0,000	8	1088	0,000
Internet Control Message Protocol v6	0,06 %	15	0,00 %	1546	0,000	15	1546	0,000
Configuration Test Protocol (loopback)	0,09 %	22	0,00 %	1320	0,000	0	0	0,000
Data	0,09 %	22	0,00 %	1320	0,000	22	1320	0,000
Logical-Link Control	0,02 %	4	0,00 %	1624	0,000	0	0	0,000
Cisco Discovery Protocol	0,02 %	4	0,00 %	1624	0,000	4	1624	0,000
Internet Protocol Version 4	0,31 %	78	0,02 %	8198	0,000	0	0	0,000
User Datagram Protocol	0,31 %	78	0,02 %	8198	0,000	0	0	0,000
Hypertext Transfer Protocol	0,05 %	12	0,01 %	2100	0,000	12	2100	0,000
Dropbox LAN sync Discovery Protocol	0,03 %	7	0,00 %	1015	0,000	7	1015	0,000
Domain Name Service	0,06 %	15	0,00 %	1035	0,000	15	1035	0,000
NetBIOS Name Service	0,17 %	44	0,01 %	4048	0,000	44	4048	0,000

Buttons: Help, Close

Figura 3.12: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 3.12 se encuentra en la página 103

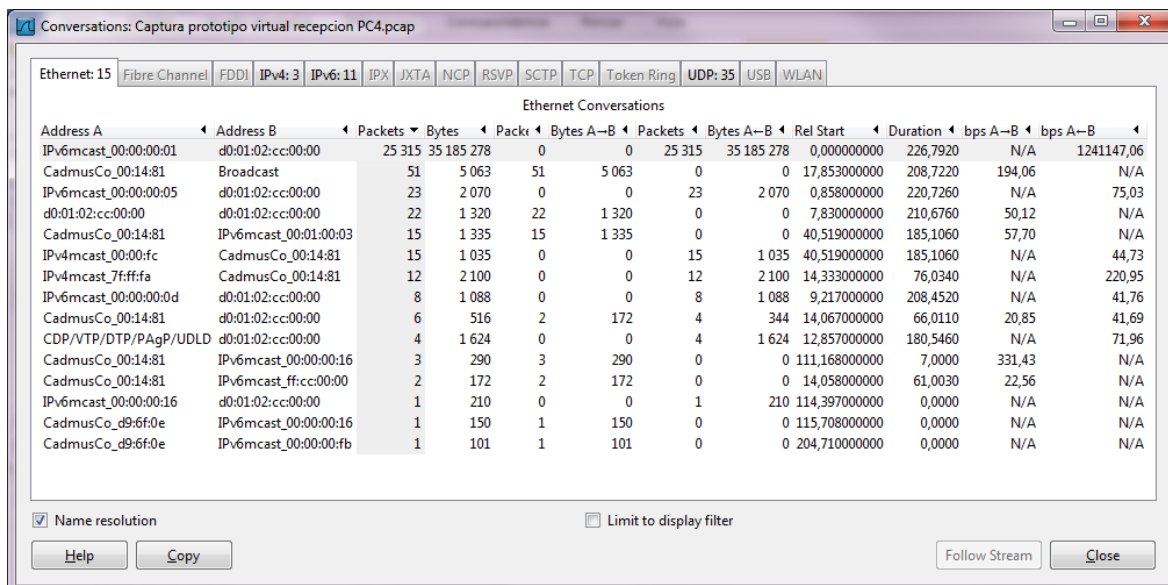


Figura 3.13: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 3.13 se encuentra en la página 104

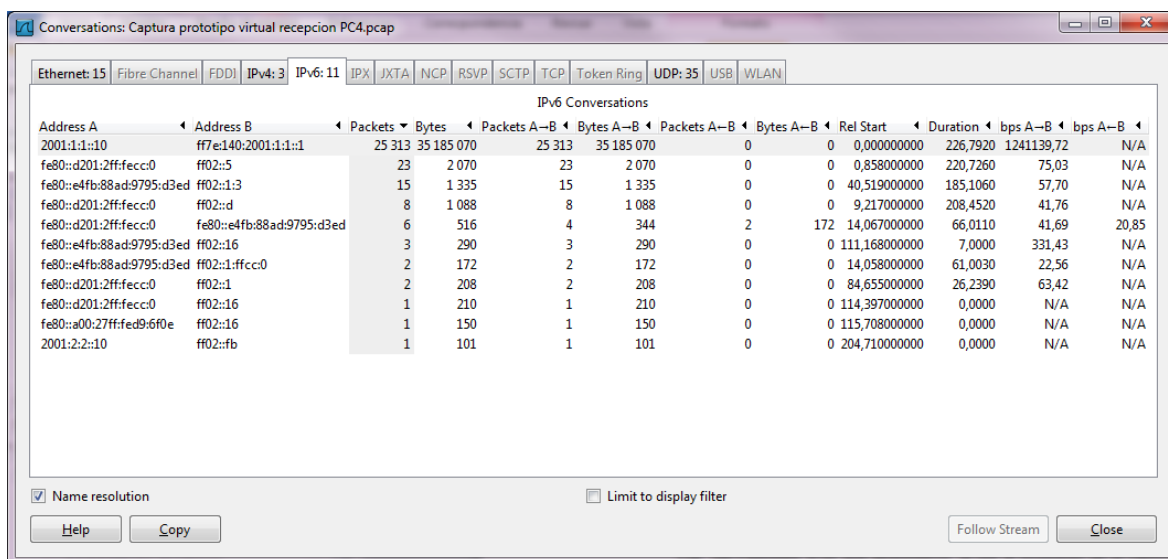


Figura 3.14: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 3.14 se encuentra en la página 105

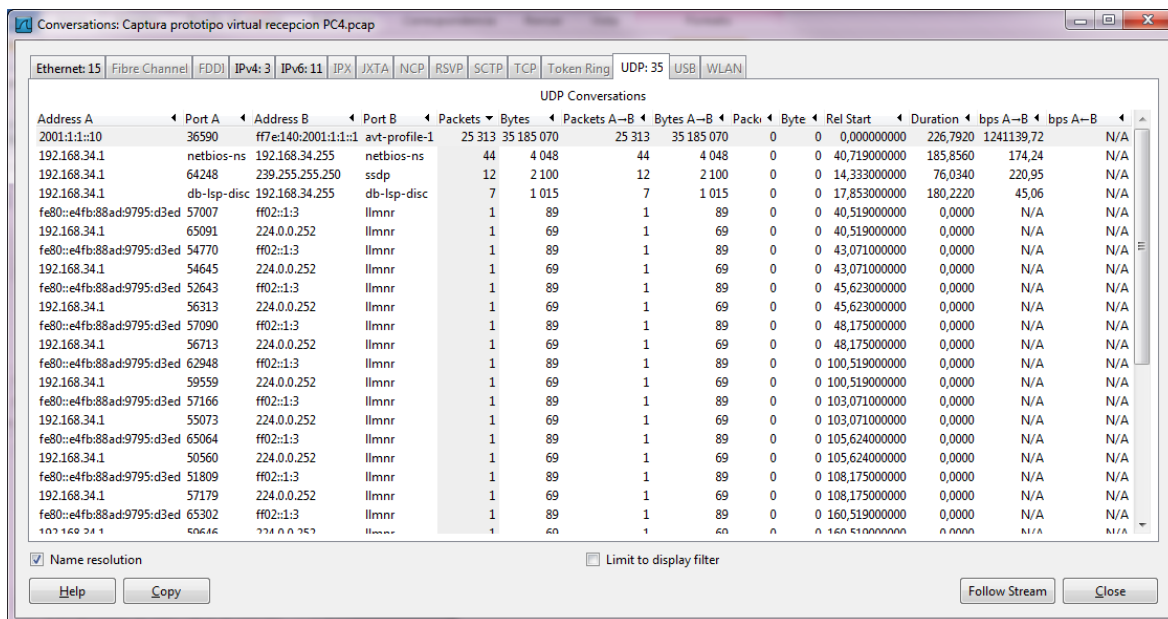


Figura 3.15: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 3.15 se encuentra en la página 105

3.1.1.2 Cálculo de los parámetros de calidad en la red de distribución

3.1.1.2.1 Cálculos de la Velocidad de Transmisión

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	2 ROUTERS PROTOTIPO VIRTUAL			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	35331010,00	35320498,00	35309016,00	227,205
CLIENTE PC1	35202352,00	35191210,00	35179510,00	226,792
TABLA DE VELOCIDADES				
	SERVER VLC		CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	155502,78		155218,67	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	155456,52		155169,54	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	155405,98		155117,95	

Tabla 3.4: Velocidades de transmisión obtenidas en la simulación.

3.1.1.2.2 Cálculos de Latencia

PRUEBA N° 1	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	84,83	85,55
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	45,00	44,00
PAQUETES PERDIDOS	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	0,21	0,27
PAQUETE MAX TIEMPO (mseg)	34,80	28,90
PAQUETE TIEMPO PROMEDIO (mseg)	1,89	1,94

Tabla 3.5: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC1.

PRUEBA N° 2	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	71,20	66,37
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00
PAQUETES PERDIDOS	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,1	11,11
PAQUETE MIN TIEMPO (mseg)	0,29	0,27
PAQUETE MAX TIEMPO (mseg)	10,60	28,90
PAQUETE TIEMPO PROMEDIO (mseg)	1,58	1,47

Tabla 3.6: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC1.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	73,39	68,18
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	44,00	45,00
PAQUETES PERDIDOS	6,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	11,11
PAQUETE MIN TIEMPO (mseg)	0,27	0,24
PAQUETE MAX TIEMPO (mseg)	21,50	18,20
PAQUETE TIEMPO PROMEDIO (mseg)	1,67	1,52

Tabla 3.7: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC1.

A continuación se presenta un cuadro con el resumen de las 3 pruebas realizadas mediante el comando PING.

RESUMEN	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	229,43	220,09
PAQUETES TRANSMITIDOS	150,00	150,00
PAQUETES RECIBIDOS	134,00	134,00
PAQUETES PERDIDOS	16,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,67
PAQUETE MIN TIEMPO (mseg)	0,21	0,24
PAQUETE MAX TIEMPO (mseg)	34,80	28,90
PAQUETE TIEMPO PROMEDIO (mseg)	1,71	1,64

Tabla 3.8: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC1.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING para el cliente PC1, que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 1.71 mseg.
- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 1.64 mseg.

3.1.1.2.3 *Cálculos de Jitter*

CALCULO DE JITTER				
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER
14	0,62	0,02	0,74	0,11
15	0,62	0,00	0,86	-0,12
16	0,73	-0,11	3,41	-2,55
17	1,24	-0,51	3,17	0,24
18	0,92	0,32	0,69	2,48
19	0,61	0,31	3,60	-2,91
20	1,99	-1,38	0,77	2,83
21	0,55	1,44	0,27	0,50
22	0,71	-0,16	3,97	-3,70
23	0,38	0,33	0,67	3,30
24	0,85	-0,47	0,51	0,16
25	0,77	0,08	3,44	-2,93
26	0,64	0,13	0,76	2,68
27	0,50	0,14	0,83	-0,07
28	0,24	0,26	0,65	0,18
29	0,75	-0,51	0,70	-0,05
30	6,30	-5,55	0,93	-0,23
31	0,73	5,57	3,33	-2,40
32	0,21	0,52	0,79	2,54
33	0,49	-0,28	0,70	0,10
34	0,59	-0,10	0,50	0,20
35	0,39	0,20	0,77	-0,27
36	0,76	-0,37	0,37	0,40
37	2,87	-2,11	0,80	-0,43
38	0,57	2,30	0,75	0,05
39	0,68	-0,11	0,37	0,38
40	0,79	-0,11	0,45	-0,08
41	0,79	0,00	0,80	-0,35
42	0,72	0,07	0,87	-0,07
43	0,76	-0,04	0,83	0,04
44	0,73	0,03	0,77	0,06
45	0,64	0,09	0,85	-0,08
46	0,74	-0,10	0,50	0,35
47	5,72	-4,98	0,98	-0,48
48	0,95	4,77	0,85	0,13
49	0,77	0,18	3,35	-2,50
50	0,75	0,02	0,68	2,67
JITTER MIN		-5,55		-3,70
JITTER MAX		5,57		3,30

Tabla 3.9: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1.

3.1.1.2.4 Cálculos de Pérdida de Paquetes

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING		
TOPOLOGIA:	2 ROUTERS PROTOTIPO VIRTUAL	
RESUMEN GENERAL		
PC:	SERVER VLC	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 47 seg.	3 min 46 seg.
TIEMPO EN SEGUNDOS:	227.205 seg.	226.792 seg.
PAQUETES CAPTURADOS:	25605.00	25479.00
PAQUETES MOSTRADOS:	25605.00	25479.00
BYTES TOTALES:	35331010.00	35202352.00
PROMEDIO PAQUETES/SEG:	112696.00	112345.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.379.848	1.381.622
PROMEDIO BYTES/SEG:	155.502.784	155.218.667
PROMEDIO MBITS/SEG:	1244	1242

Tabla 3.10: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la topología tipo malla.

Los paquetes capturados junto con los paquetes mostrados y los bytes totales, tienen una diferencia, que aunque es mínima, existe y por tanto existe pérdida de paquetes.

3.2 IMPLEMENTACIÓN DEL PROTOTIPO EN EL LABORATORIO

Una vez implementado el prototipo en el GNS3, se procederá a realizar el mismo diseño de red con elementos del laboratorio de la facultad, con el fin de comparar los datos obtenidos en la simulación y los datos obtenidos en el laboratorio.

3.2.1 ELEMENTOS A UTILIZAR EN EL LABORATORIO:

Los elementos utilizados en el laboratorio serán los mismos que se utilizó en la simulación, es decir, los elementos tales como Server VLC, Cliente PC1 y Routers R1 y R2, serán prácticamente idénticos. Esto se debe a que en el caso del Server VLC, se va a utilizar el mismo servidor de la simulación, para el caso del cliente PC1, se utilizará un PC del laboratorio de la facultad con las mismas características técnicas de memoria RAM, disco duro, etc., que tiene el Cliente PC1 en el ambiente virtual GNS3.

Para el caso de los routers R1 y R2, se utilizarán dos routers cisco serie c1700 facilitados por el laboratorio de la facultad.



Figura 3.16: Routers c1700 facilitados por el laboratorio de la facultad.

Los Routers R1 y R2 del laboratorio, tenían instalados un IOS versión 2.2, la cual no permite el ingreso de comandos IPv6, por tal razón, fue necesario instalar un IOS versión 2.4. Este nuevo IOS es exactamente el mismo utilizado en la simulación GNS3, es decir, todos los elementos son idénticos al ambiente virtual.



Figura 3.17: Prototipo implementado en el laboratorio de la facultad.

3.2.2 DATOS OBTENIDOS EN EL LABORATORIO

3.2.2.1 Topología a implementar en el laboratorio

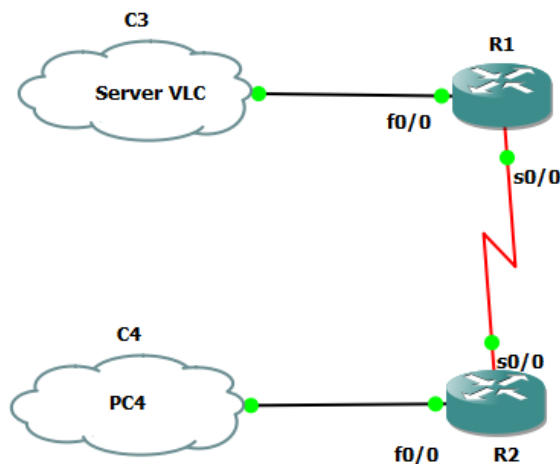


Figura 3.18: Diseño de la red a implementar en el laboratorio.

3.2.2.2 Direccionamiento de la red física a implementar

DISPOSITIVO	DIRECCION IPV6	GATEWAY
Server VLC	2001:1:1::10/64	2001:1:1::1
CLIENTE PC1	2001:2:2::10/64	2001:2:2::2
ROUTER R1		
Fastethernet 0/0	2001:1:1::1/64	
Serial 0/0	2001:1:2::1/64	
ROUTER R2		
Fastethernet 0/0	2001:2:2::2/64	
Serial 0/0	2001:1:2::2/64	
DIRECCION EMBEDDED MULTICAST A UTILIZAR		
Grupo Multicast Embedded	FF07:140:2001:1:1::1	
PROCOLO DE ENRUTAMIENTO UTILIZADO		
PROTOCOLO:	OSPFv6	
GRUPO:	1	
AREA:	0	
ROUTERS IMPLEMENTADOS:	Todos los Routers de la red de distribución	
RP SELECCIONADO		
ROUTER:	R1 (Conectado directamente al Server VLC)	

Tabla 3.11: Direccionamiento de la red física.

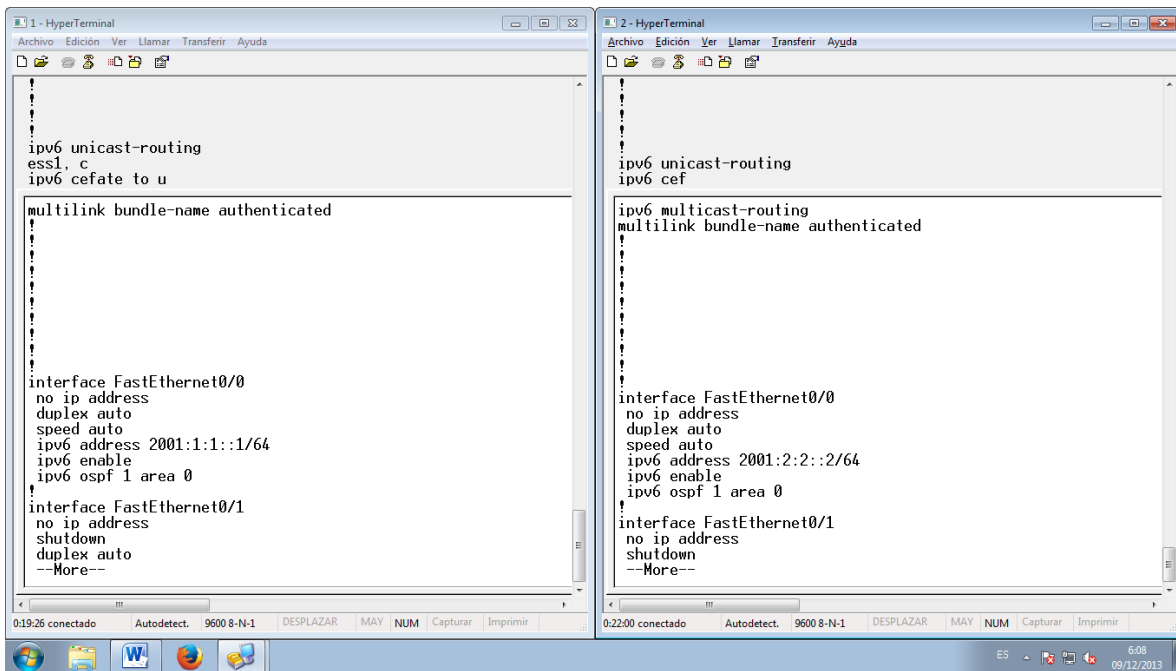


Figura 3.20: Comando “show running config” en los Routers R1 y R2.

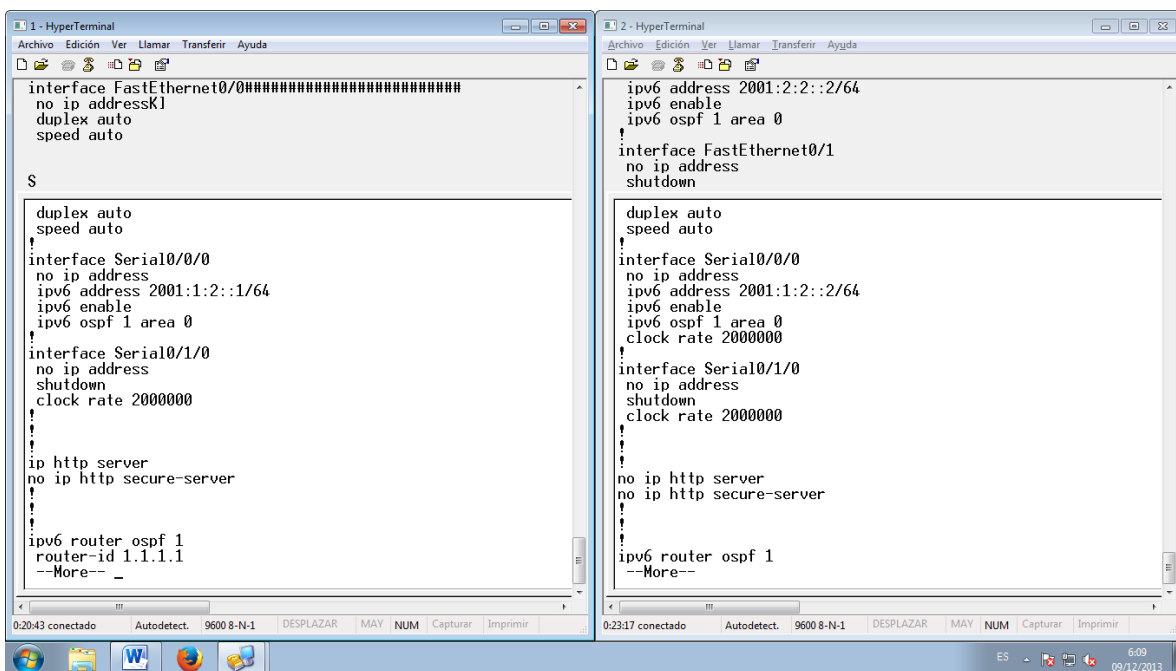


Figura 3.21: Comando “show running config” en los Routers R1 y R2.

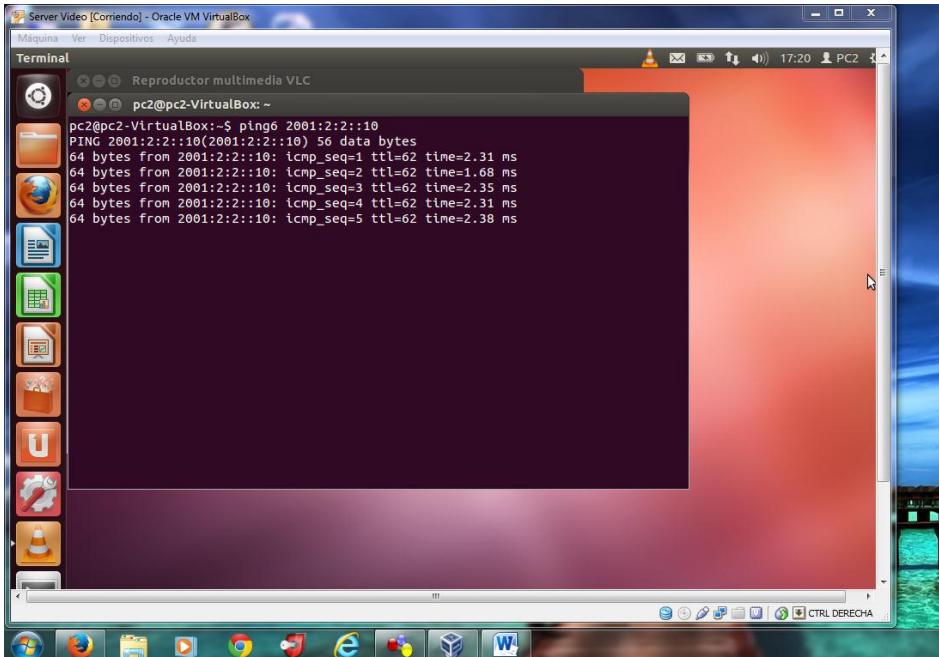

```

ubuntu@ubuntu-pc4: ~
64 bytes from 2001:1:1::10: icmp_seq=21 ttl=62 time=2.01 ms
64 bytes from 2001:1:1::10: icmp_seq=22 ttl=62 time=2.01 ms
64 bytes from 2001:1:1::10: icmp_seq=23 ttl=62 time=2.86 ms
64 bytes from 2001:1:1::10: icmp_seq=24 ttl=62 time=2.18 ms
64 bytes from 2001:1:1::10: icmp_seq=25 ttl=62 time=9.36 ms
64 bytes from 2001:1:1::10: icmp_seq=26 ttl=62 time=2.09 ms
64 bytes from 2001:1:1::10: icmp_seq=27 ttl=62 time=2.10 ms
64 bytes from 2001:1:1::10: icmp_seq=28 ttl=62 time=2.05 ms
64 bytes from 2001:1:1::10: icmp_seq=29 ttl=62 time=9.62 ms
64 bytes from 2001:1:1::10: icmp_seq=30 ttl=62 time=12.5 ms
64 bytes from 2001:1:1::10: icmp_seq=31 ttl=62 time=2.15 ms
^C
--- 2001:1:1::10 ping statistics ---
31 packets transmitted, 31 received, 0% packet loss, time 30037ms
rtt min/avg/max/mdev = 2.010/4.247/13.573/3.764 ms
ubuntu@ubuntu-pc4:~$ ping6 2001:1:1::10
PING 2001:1:1::10(2001:1:1::10) 56 data bytes
64 bytes from 2001:1:1::10: icmp_seq=1 ttl=62 time=2.22 ms
64 bytes from 2001:1:1::10: icmp_seq=2 ttl=62 time=2.11 ms
64 bytes from 2001:1:1::10: icmp_seq=3 ttl=62 time=2.28 ms
64 bytes from 2001:1:1::10: icmp_seq=4 ttl=62 time=2.12 ms
64 bytes from 2001:1:1::10: icmp_seq=5 ttl=62 time=2.18 ms
64 bytes from 2001:1:1::10: icmp_seq=6 ttl=62 time=2.14 ms

```

Figura 3.24: PING desde Cliente PC1 hacia Server VLC.

La figura 3.24 muestra un PING exitoso desde el Cliente PC1 hacia el Server VLC.



```

Server Video [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Terminal
Reproductor multimedia VLC
pc2@pc2-VirtualBox: ~
pc2@pc2-VirtualBox:~$ ping6 2001:2:2::10
PING 2001:2:2::10(2001:2:2::10) 56 data bytes
64 bytes from 2001:2:2::10: icmp_seq=1 ttl=62 time=2.31 ms
64 bytes from 2001:2:2::10: icmp_seq=2 ttl=62 time=1.68 ms
64 bytes from 2001:2:2::10: icmp_seq=3 ttl=62 time=2.35 ms
64 bytes from 2001:2:2::10: icmp_seq=4 ttl=62 time=2.31 ms
64 bytes from 2001:2:2::10: icmp_seq=5 ttl=62 time=2.38 ms

```

Figura 3.25: PING desde el Server VLC hacia el Cliente PC1.

La figura 3.25 muestra un PING exitoso desde el Server VLC hacia el Cliente PC1.

A continuación se envía el video streaming por la red.

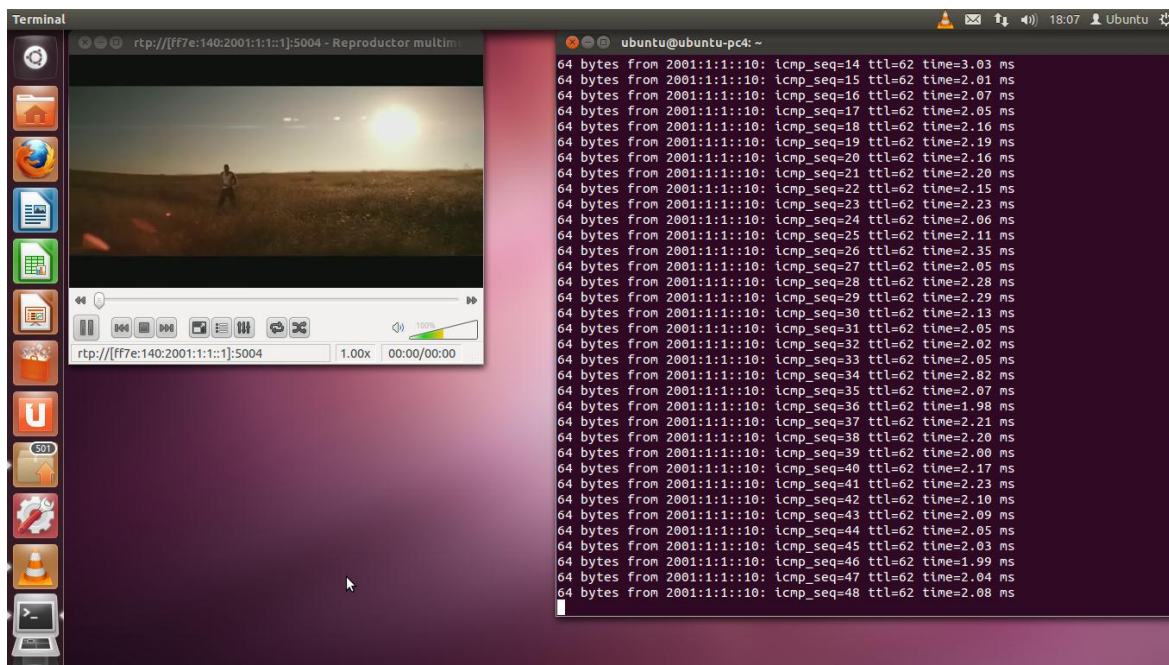


Figura 3.26: Video streaming capturado por Cliente PC1.

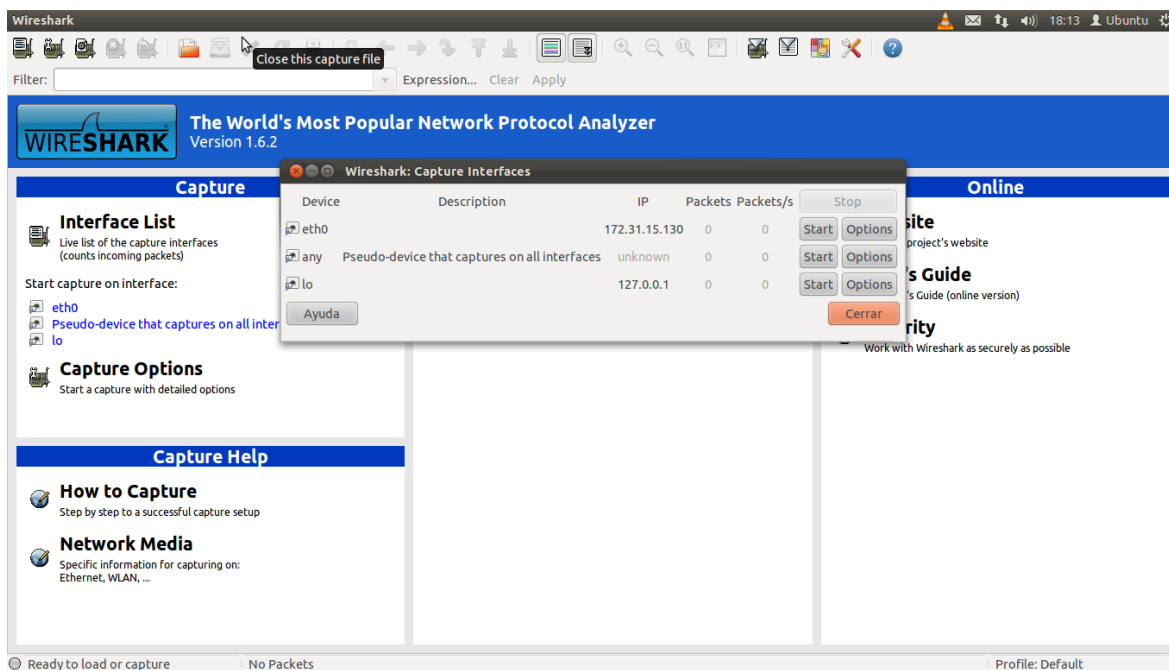


Figura 3.27: Inicio de Wireshark en Cliente PC1 para captura de paquetes.

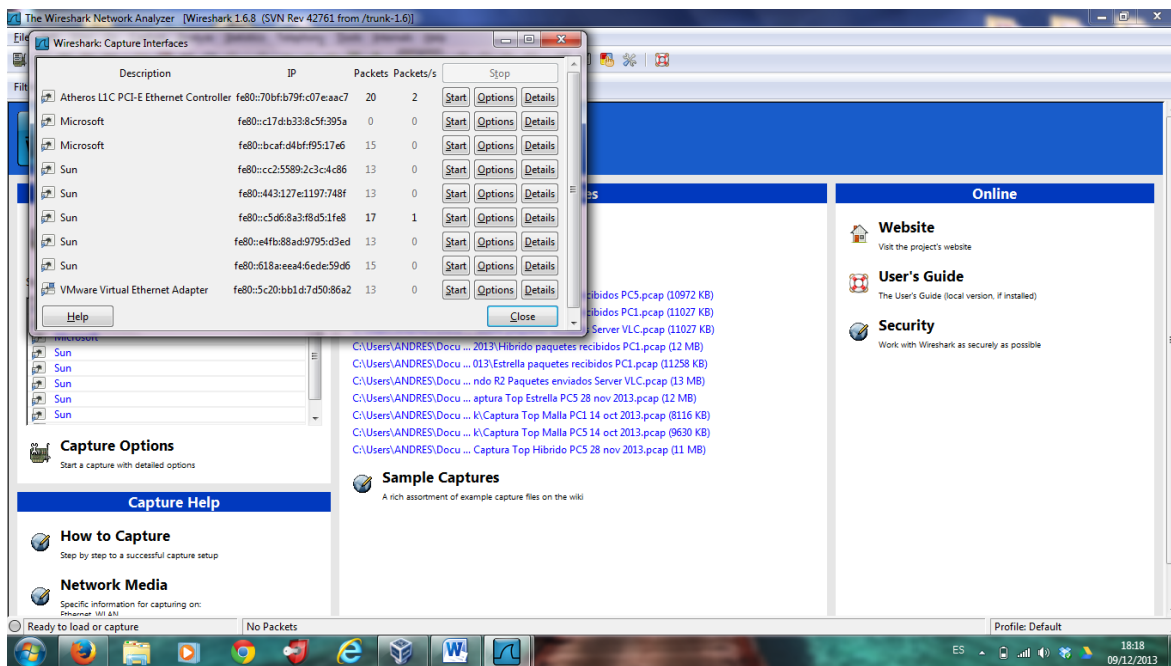


Figura 3.28: Inicio de Wireshark en Server VLC para captura de paquetes.

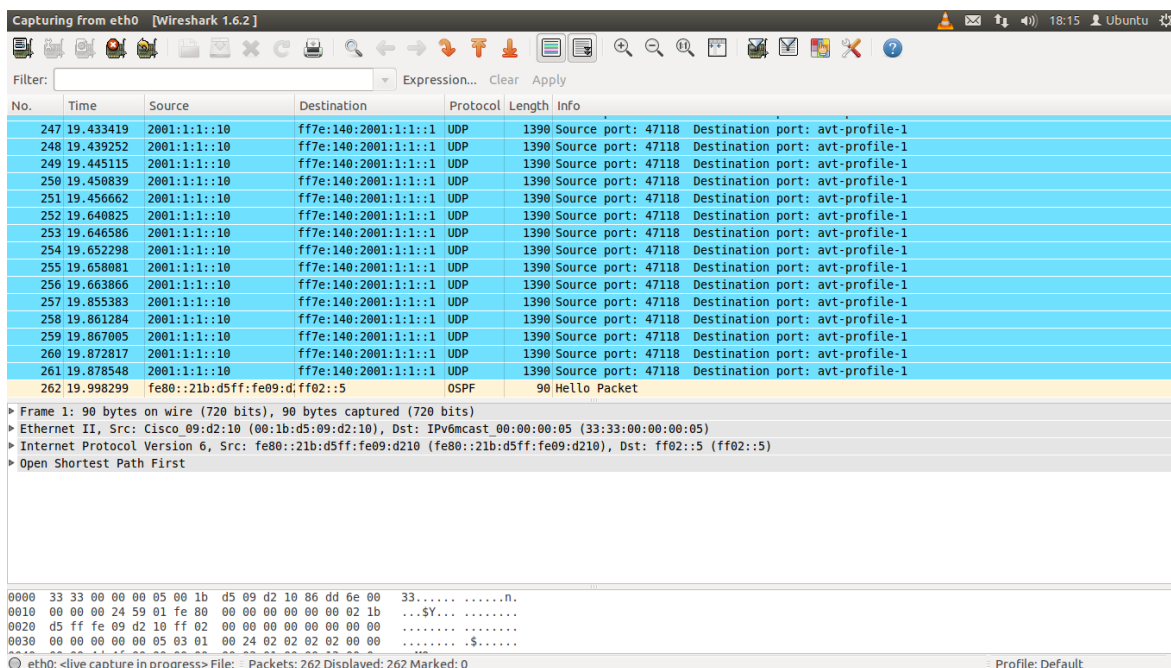


Figura 3.29: Paquetes UDP transmitidos desde el Server VLC hacia el Cliente PC1 capturados con Wireshark en el Cliente PC1

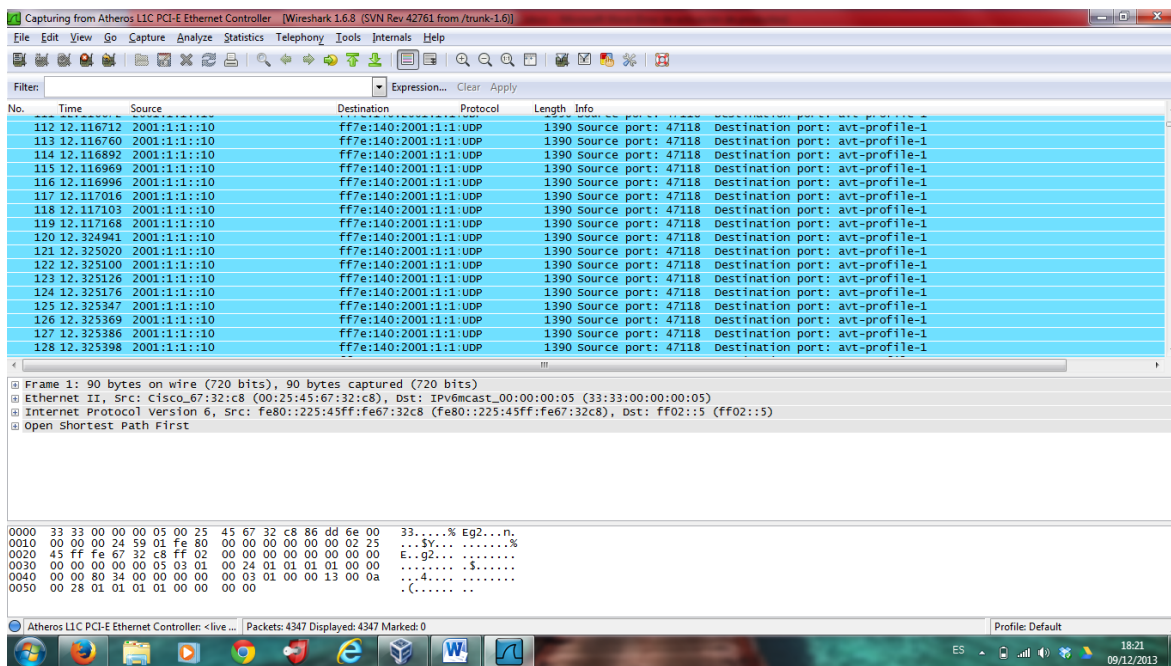


Figura 3.30: Paquetes UDP transmitidos desde el Server VLC hacia el Cliente PC1 capturados con Wireshark en el Server VLC

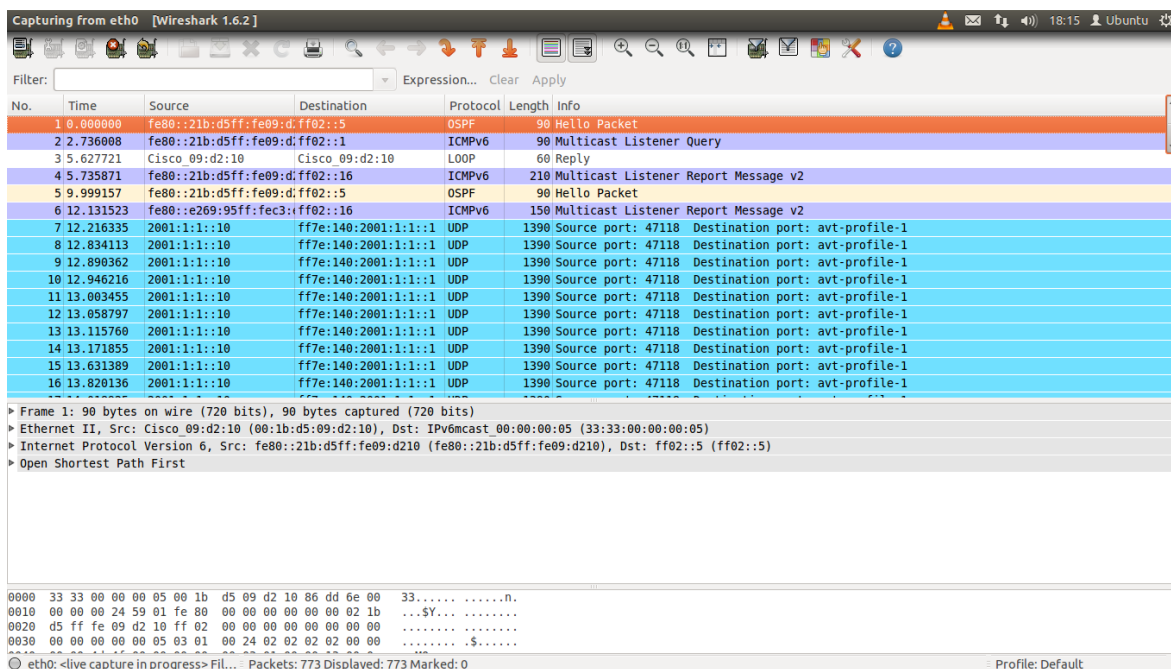


Figura 3.31: Paquetes UDP transmitidos desde el Server VLC hacia el Cliente PC1 capturados con Wireshark

Server VLC

Mediante WIRESHARK se ha capturado los paquetes que se envían a la red desde el Server VLC:

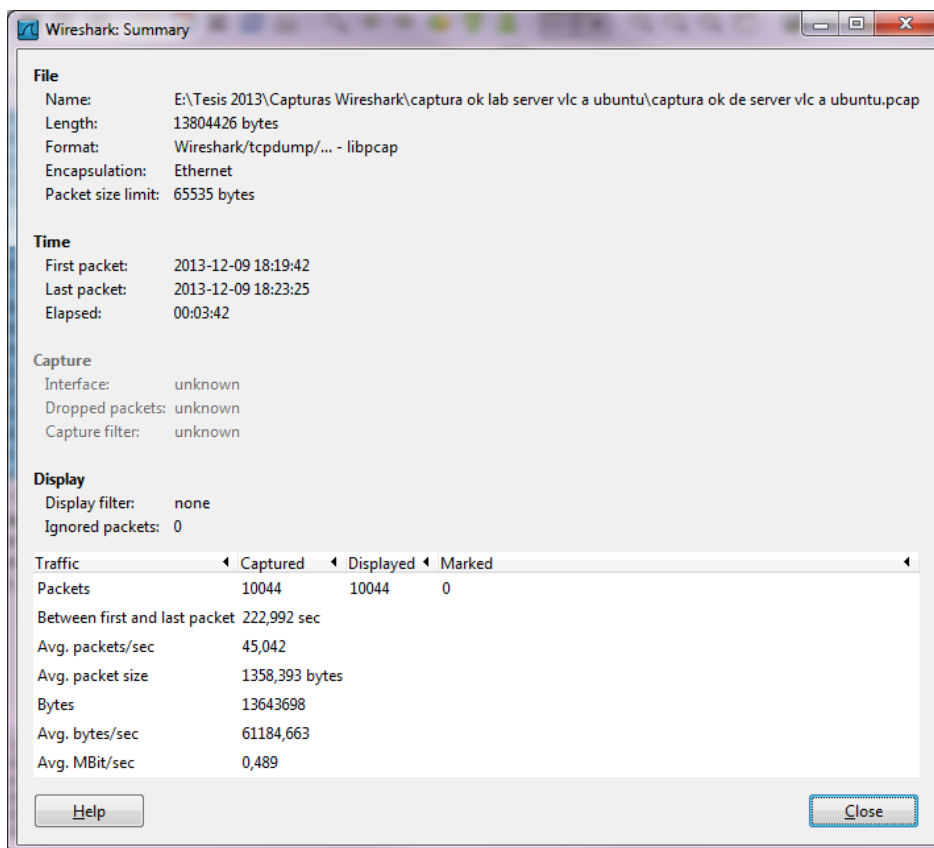


Figura 3.32: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 42 seg.
TIEMPO EN SEGUNDOS:	222.992 seg.
PAQUETES CAPTURADOS:	10044.00
PAQUETES MOSTRADOS:	10044.00
BYTES TOTALES:	13643698.00
PROMEDIO PAQUETES/SEG:	45042.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1358.393
PROMEDIO BYTES/SEG:	61184.663
PROMEDIO MBITS/SEG:	0,489

Tabla 3.12: Resumen de los datos mostrados en Wireshark.

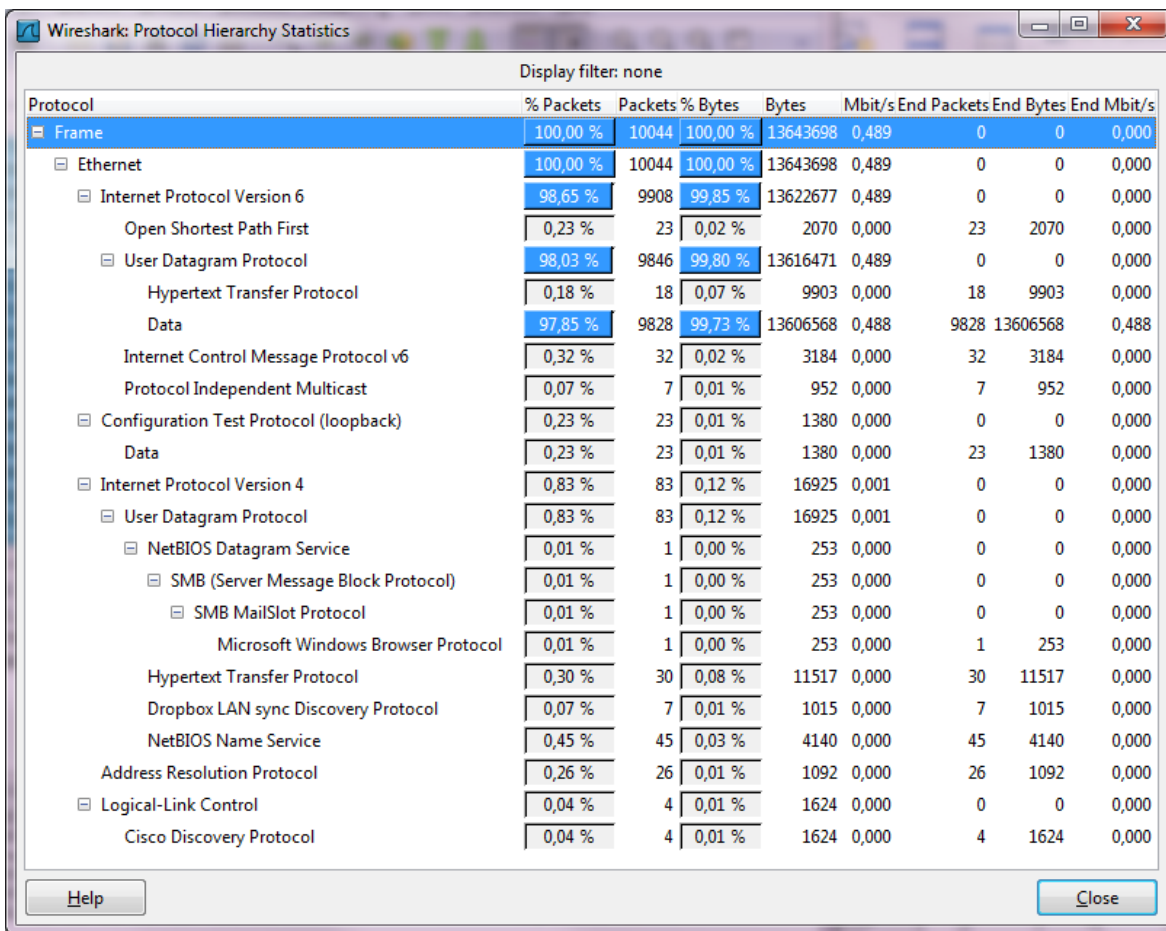


Figura 3.33: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 3.33 se encuentra en la página 103

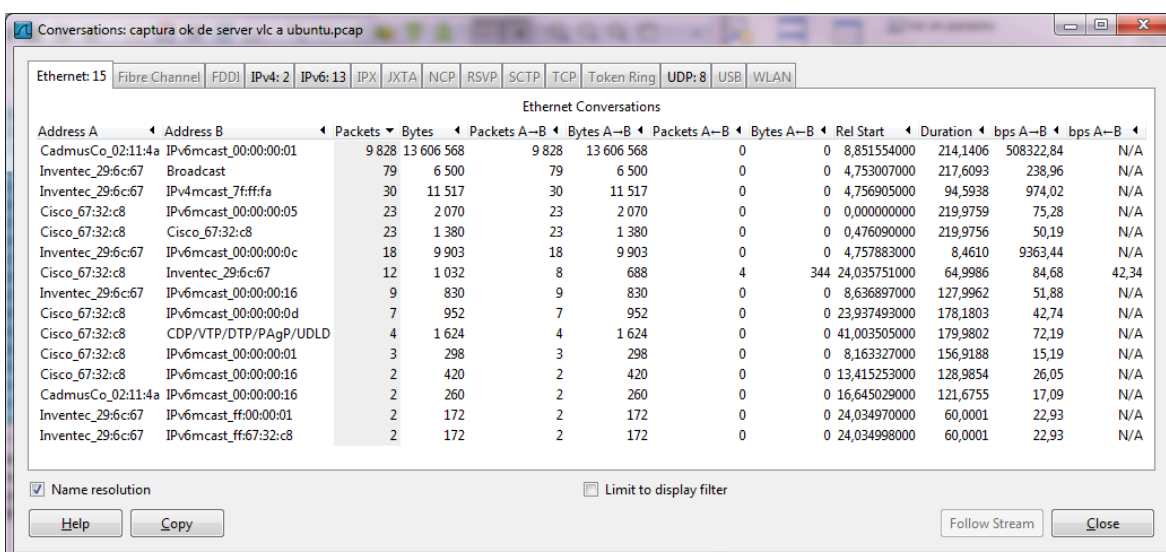


Figura 3.34: Paquetes Ethernet que atravesaron la red al momento de la captura

* La explicación de la figura 3.34 se encuentra en la página 104

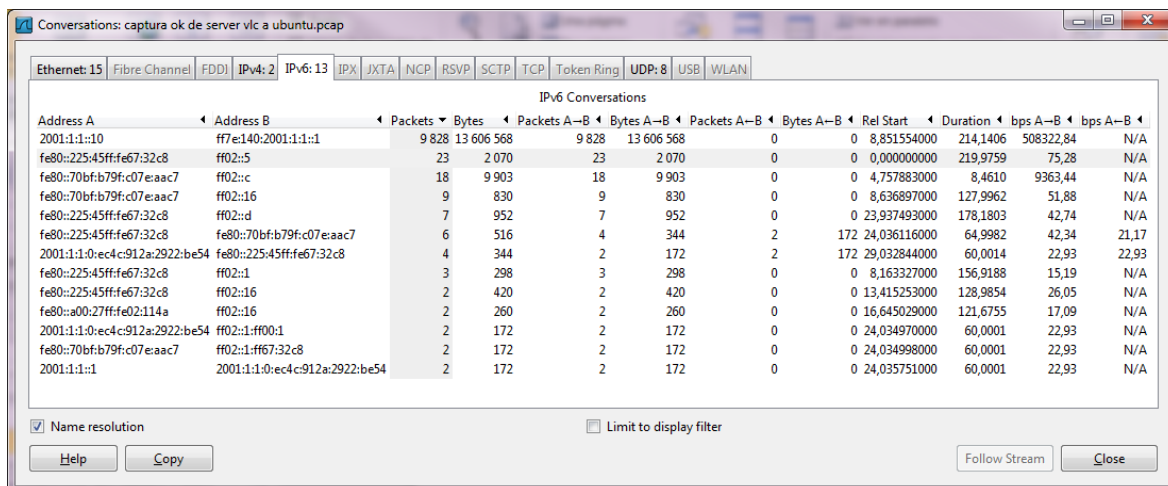


Figura 3.35: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 3.35 se encuentra en la página 105

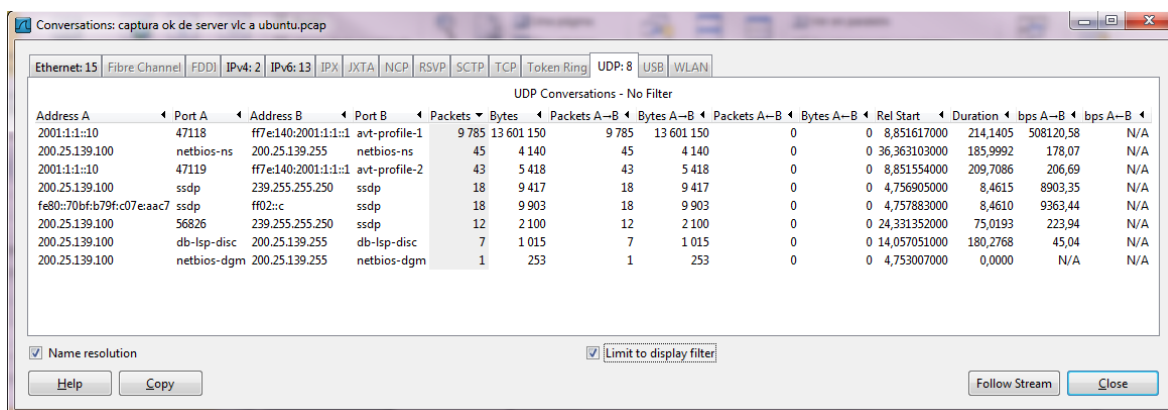


Figura 3.36: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 3.36 se encuentra en la página 105

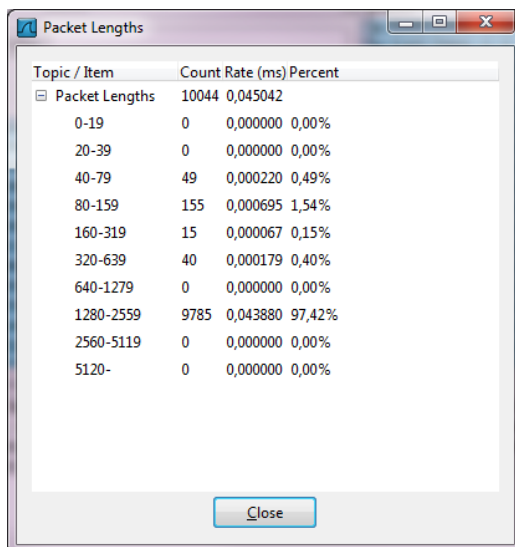


Figura 3.37: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 3.37 se encuentra en la página 106

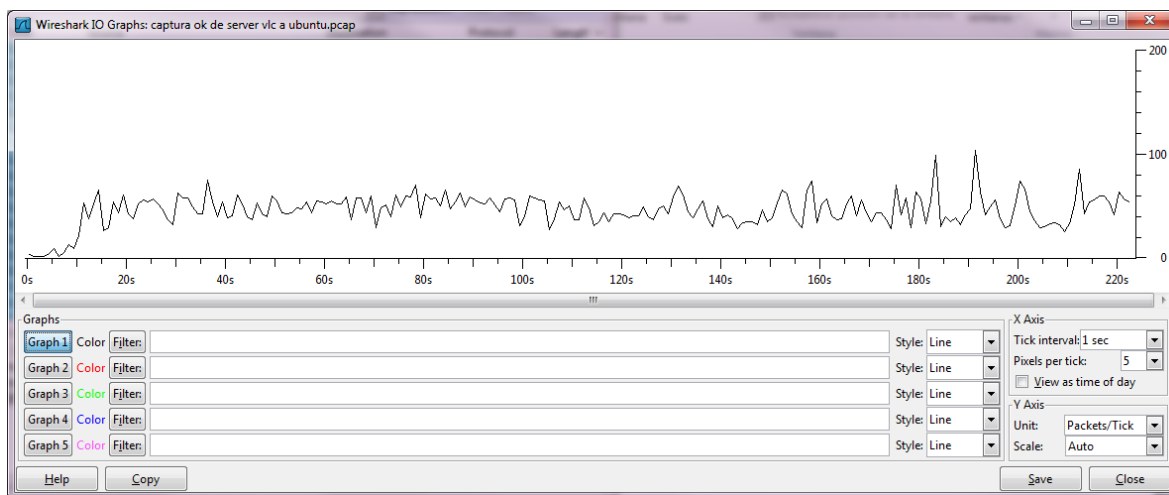


Figura 3.38: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC1

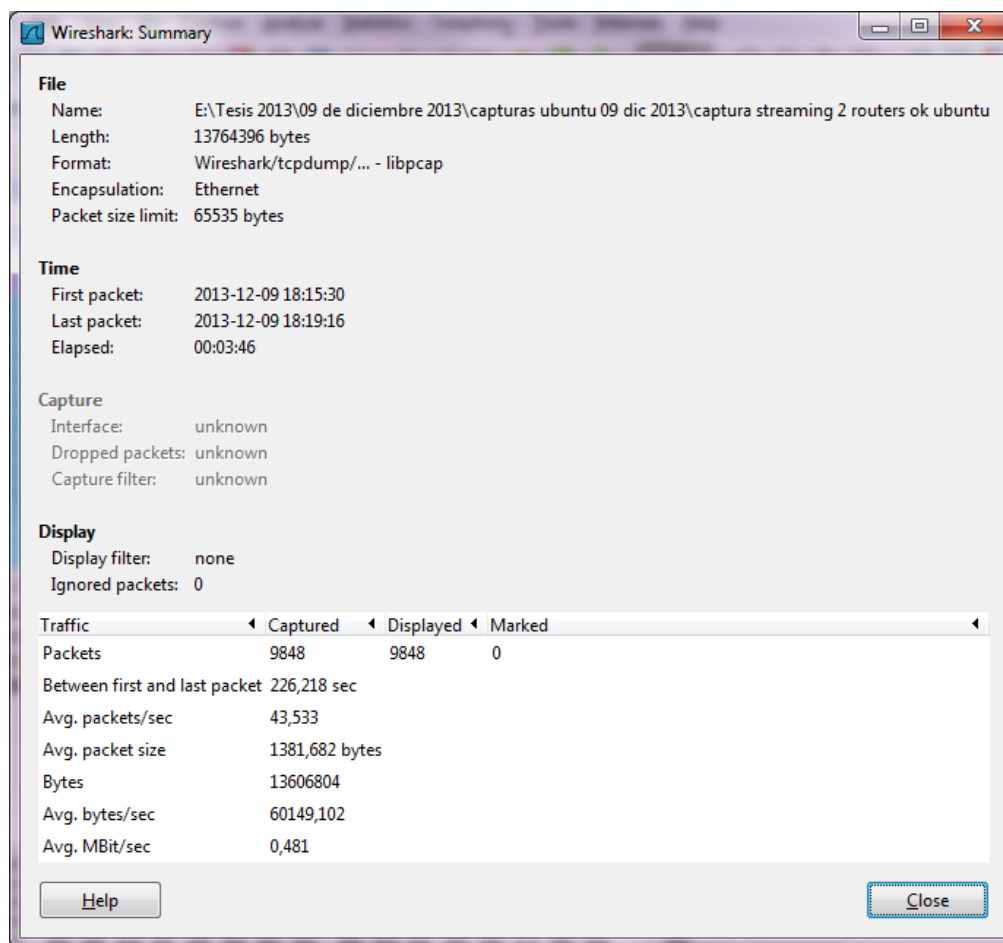


Figura 3.39: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1.

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	3 min 46 seg.
TIEMPO EN SEGUNDOS:	226.218 seg.
PAQUETES CAPTURADOS:	9848.00
PAQUETES MOSTRADOS:	9848.00
BYTES TOTALES:	13606804.00
PROMEDIO PAQUETES/SEG:	43533.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1381.682
PROMEDIO BYTES/SEG:	60149.102
PROMEDIO MBITS/SEG:	0,481

Tabla 3.13: Resumen de los datos mostrados en Wireshark.

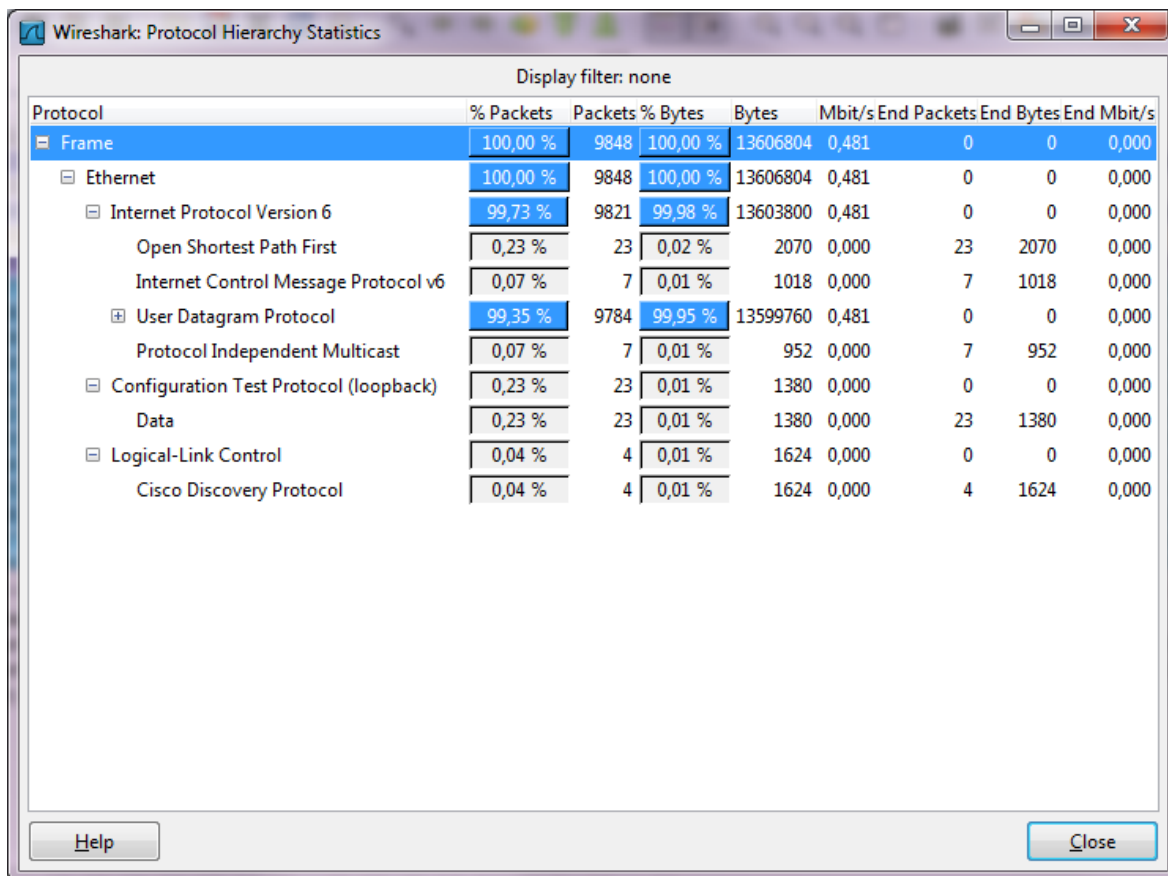


Figura 3.40: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 3.40 se encuentra en la página 103

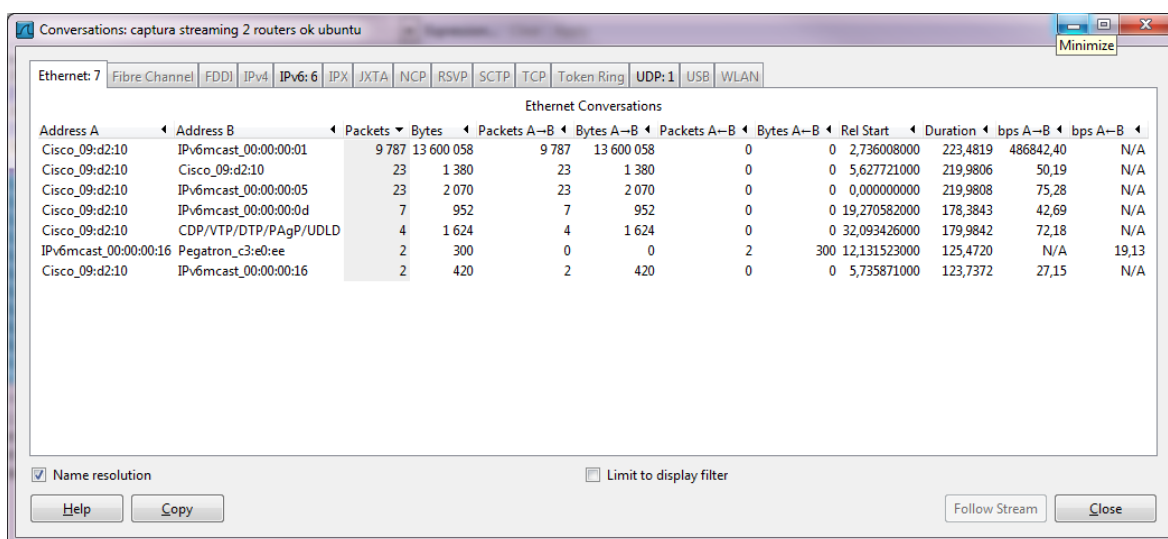


Figura 3.41: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 3.41 se encuentra en la página 104

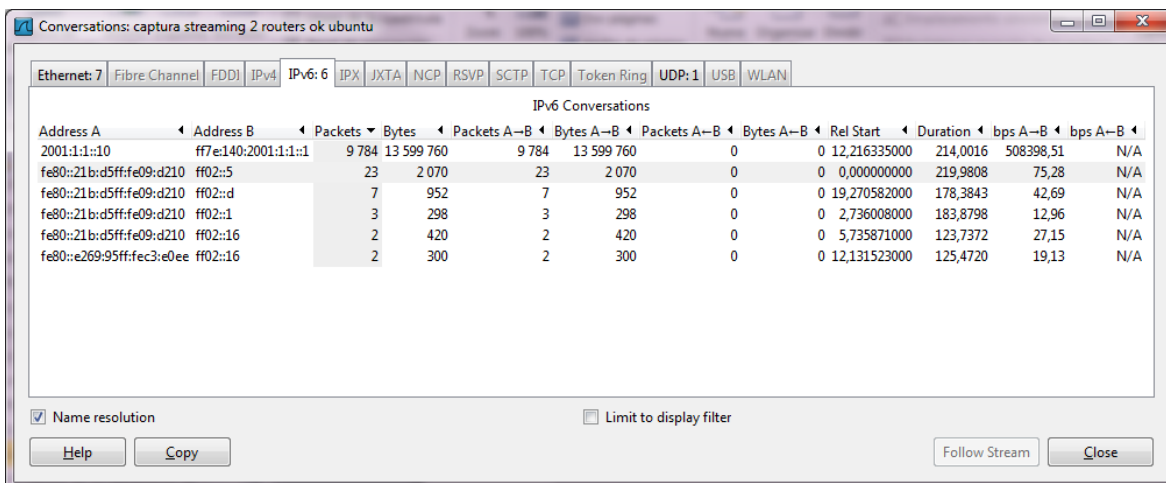


Figura 3.42: Paquetes IPv6 que atravesaron la red al momento de la captura.

* La explicación de la figura 3.42 se encuentra en la página 105

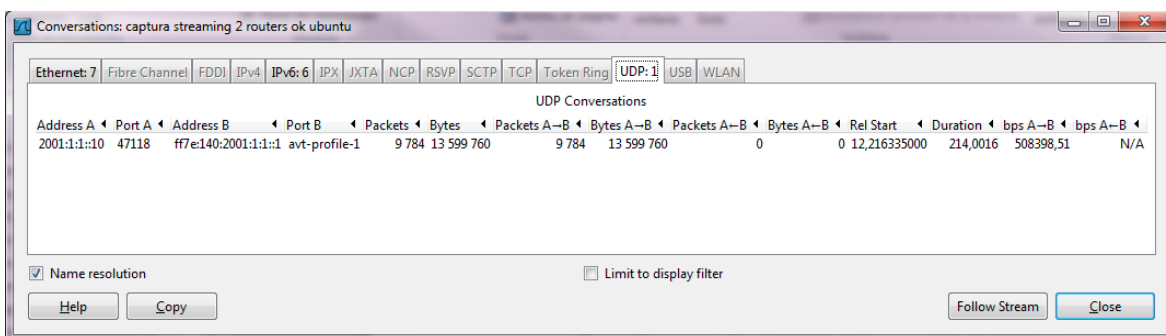


Figura 3.43: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 3.43 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	9848	0,043533	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	23	0,000102	0,23%
80-159	35	0,000155	0,36%
160-319	2	0,000009	0,02%
320-639	4	0,000018	0,04%
640-1279	0	0,000000	0,00%
1280-2559	9784	0,043250	99,35%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 3.44: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 3.44 se encuentra en la página 106

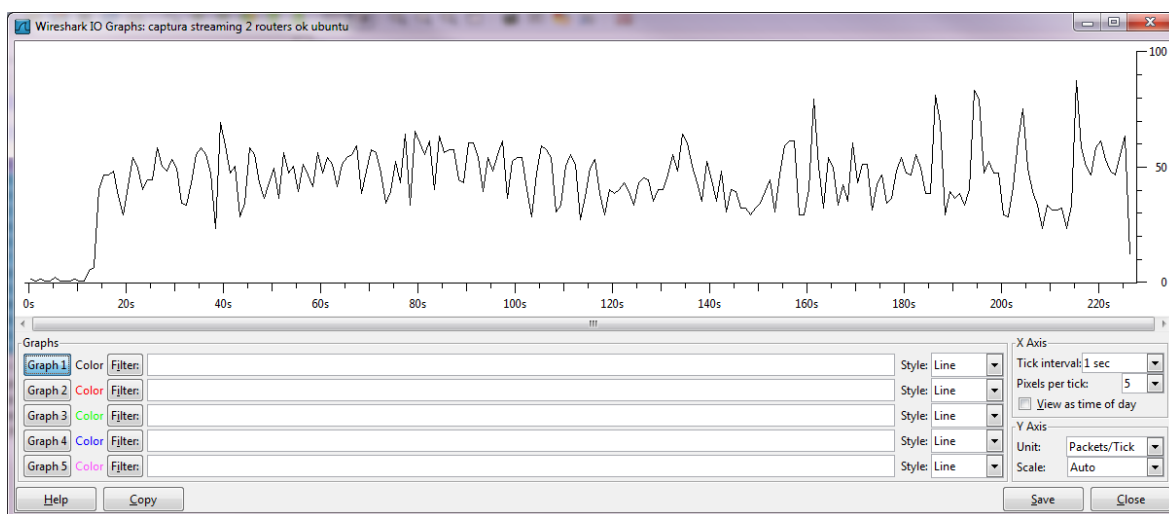


Figura 3.45: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

3.2.2.4 Cálculo de los parámetros de calidad en la red de distribución

3.2.2.4.1 Cálculos de la Velocidad de Transmisión

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	2 ROUTERS PROTOTIPO REAL			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	13643698,00	13622677,00	13606568,00	222,992
CLIENTE PC1	13606804,00	13603800,00	13599760,00	226,218
TABLA DE VELOCIDADES				
	SERVER VLC		CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	61184,70		60149,08	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	61090,43		60135,80	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	61018,19		60117,94	

Tabla 3.13: Velocidades de transmisión obtenidas en el laboratorio.

3.2.2.4.2 Cálculos de Latencia

PRUEBA N° 1	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	97,42	98,04
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	45,00	44,00
PAQUETES PERDIDOS	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	1,98	1,68
PAQUETE MAX TIEMPO (mseg)	3,03	2,76
PAQUETE TIEMPO PROMEDIO (mseg)	2,16	2,23

Tabla 3.14: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 2	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	95,69	101,30
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00
PAQUETES PERDIDOS	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	11,11
PAQUETE MIN TIEMPO (mseg)	1,98	1,68
PAQUETE MAX TIEMPO (mseg)	2,92	2,76
PAQUETE TIEMPO PROMEDIO (mseg)	2,13	2,25

Tabla 3.15: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	97,52	102,81
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	44,00	45,00
PAQUETES PERDIDOS	6,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	11,11
PAQUETE MIN TIEMPO (mseg)	1,95	2,05
PAQUETE MAX TIEMPO (mseg)	2,82	2,90
PAQUETE TIEMPO PROMEDIO (mseg)	2,22	2,28

Tabla 3.16: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

RESUMEN	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	290,63	302,15
PAQUETES TRANSMITIDOS	150,00	150,00
PAQUETES RECIBIDOS	134,00	134,00
PAQUETES PERDIDOS	16,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,67
PAQUETE MIN TIEMPO (mseg)	1,95	1,68
PAQUETE MAX TIEMPO (mseg)	3,03	2,90
PAQUETE TIEMPO PROMEDIO (mseg)	2,17	2,25

Tabla 3.17: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING al cliente PC1, que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 2.17 mseg.

- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 2.25 mseg.

3.2.2.4.3 *Cálculos de Jitter*

CALCULO DE JITTER				
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER
15	2,35	-0,24	2,22	0,06
16	2,05	0,30	2,16	0,06
17	2,28	-0,23	2,21	-0,05
18	2,29	-0,01	2,13	0,08
19	2,13	0,16	2,76	-0,63
20	2,05	0,08	2,19	0,57
21	2,02	0,03	2,26	-0,07
22	2,05	-0,03	2,25	0,01
23	2,02	0,03	2,28	-0,03
24	2,05	-0,03	2,28	0,00
25	2,82	-0,77	2,22	0,06
26	2,07	0,75	2,31	-0,09
27	1,98	0,09	2,30	0,01
28	2,21	-0,23	2,18	0,12
29	2,20	0,01	2,28	-0,10
30	2,00	0,20	2,26	0,02
31	3,03	-1,03	2,23	0,03
32	2,01	1,02	2,12	0,11
33	2,07	-0,06	2,52	-0,40
34	2,05	0,02	2,22	0,30
35	2,16	-0,11	2,04	0,18
36	2,19	-0,03	2,25	-0,21
37	2,16	0,03	2,21	0,04
38	2,20	-0,04	2,34	-0,13
39	2,15	0,05	2,35	-0,01
40	2,23	-0,08	2,06	0,29
41	2,06	0,17	2,26	-0,20
42	2,11	-0,05	2,18	0,08
43	2,35	-0,24	2,25	-0,07
44	2,05	0,30	2,24	0,01
45	2,28	-0,23	2,16	0,08
46	2,29	-0,01	2,29	-0,13
47	2,13	0,16	2,24	0,05
48	2,05	0,08	2,28	-0,04
49	2,02	0,03	1,95	0,33
50	2,05	-0,03	1,97	-0,02
JITTER MIN		-1,03		-0,63
JITTER MAX		1,02		0,57

Tabla 3.18: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1.

3.2.2.4.4 Cálculos de Pérdida de Paquetes

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA		
TRANSMISION DE VIDEO STREAMING		
TOPOLOGIA:	2 ROUTERS PROTOTIPO	
RESUMEN GENERAL		
PC:	SERVER VLC	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	3 min 42 seg.	3 min 46 seg.
TIEMPO EN SEGUNDOS:	222.992 seg.	226.218 seg.
PAQUETES CAPTURADOS:	10044.00	9848.00
PAQUETES MOSTRADOS:	10044.00	9848.00
BYTES TOTALES:	13643698.00	13606804.00
PROMEDIO PAQUETES/SEG:	45042.00	43533.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.358.393	1.381.682
PROMEDIO BYTES/SEG:	61.184.663	60.149.102
PROMEDIO MBITS/SEG:	0,489	0,481

Tabla 3.19: Tabla comparativa de valores obtenidos en la transmisión de video streaming en el laboratorio.

Los paquetes capturados junto con los paquetes mostrados y los bytes totales, tienen una diferencia, que aunque es mínima, existe y por tanto existe pérdida de paquetes.

3.3 DENEGACIÓN DE SERVICIO

3.3.1 STREAMING DE VIDEO Y FLUJO DE PAQUETES SYN

Con el fin de comprobar los efectos de un flujo de datos diferente a la transmisión de un streaming de video en la red de distribución propuesta, se plantea inundar la red con un flujo continuo de datos tipo SYN (datos de sincronización), el cual atravesará la red de principio a fin al mismo tiempo que el streaming de video.

Se ha elegido inundar la red con paquetes tipo SYN, sin ningún motivo en particular, en realidad, cualquier tipo de paquetes sirve para este cometido.

El proceso será, enviar el streaming de video desde el Server VLC hacia el Cliente PC1 e inmediatamente enviar un flujo continuo de paquetes SYN por la misma red y mediante Wireshark, capturar los paquetes salientes y entrantes para los cálculos de los parámetros de calidad para este caso específico.

3.3.2 DENEGACIÓN DE SERVICIO

Este tipo de ataque muy común en la actualidad, provoca la incapacidad/indisponibilidad de un servicio (aplicación específica) o de una máquina. Existen dos tipos de denegación de servicio: el primero, aprovecha un fallo en la aplicación y el segundo, debido a la mala implementación o en la debilidad de un protocolo⁷³.

3.3.2.1 Denegación de servicio de aplicación

Si las vulnerabilidades de una aplicación pueden causar el tomar el control de una máquina (ejemplo del buffer overflow), pueden también causar a la denegación de servicio. La aplicación se volverá indisponible por bloqueo de los recursos de la máquina o por bloqueo completo de la misma⁷⁴.

3.3.2.2 Denegación de servicio de red

Existen diferentes tipos de denegación de servicio utilizando características de la pila TCP/IP.

3.3.2.3 SYN Flooding (inundación de SYNs)

Una conexión TCP se establece en tres etapas (TCP Three Way Handshake). SYN Flooding explota este mecanismo. Las tres etapas son enviar un SYN, recibir un SYN-ACK y enviar un ACK. El objetivo es dejar en la máquina a ser atacada un número elevado de conexiones TCP en espera. Para hacer esto, el cracker envía una gran cantidad de peticiones de conexiones (SYN flag=1), la máquina objetivo envía el SYN-ACK de vuelta para responder al SYN recibido.

⁷³ <http://www.ibiblio.org/pub/Linux/docs/linux-doc-project/linuxfocus/Castellano/March2003/article282.meta.shtml>

⁷⁴ <http://www.zonadeseguridad.net/scapy-inundar-tu-router-de-paquetes-syn/>

El cracker no le responderá con el ACK, así para cada SYN recibido, la máquina objetivo tendrá una conexión abierta, provocando que estas conexiones usen recursos de memoria, después de un corto periodo de tiempo, la máquina se saturará y no podrá aceptar más conexiones. Este tipo de denegación de servicio solo afecta a la máquina objetivo.

El cracker utiliza un inundador de SYNs como el synk4, indicando el puerto TCP destino utilizando una IP de origen aleatoria para impedir que la máquina atacante sea identificada⁷⁵.

3.3.2.4 UDP Flooding (inundación UDP)

Esta denegación utiliza la forma de trabajo que tiene el protocolo UDP (sin conexión). Consiste en crear una tormenta de paquetes UDP sobre una, dos o varias máquinas. Un ataque entre dos máquinas provocaría la congestión de la red sobre la que trabajen estas máquinas y la saturación de los recursos de ambas máquinas. La congestión de la red es más importante ya que el tráfico UDP tiene prioridad sobre el tráfico TCP.

El caso más conocido de inundación UDP es el "*Chargen Denial of Service Attack*" la implementación de este tipo de ataque es muy fácil: Es suficiente con crear una comunicación entre el servicio chargen de una máquina y el servicio echo de otra. El cracker envía paquetes UDP al puerto 19 (chargen) de una de las víctimas dando la dirección IP y el puerto de origen de la otra. En este caso, puerto de origen UDP 7 (echo). La inundación UDP lleva a la saturación del ancho de banda entre ambas máquinas. Una red completa puede ser la víctima de una inundación UDP.

3.3.2.5 Fragmentación de paquetes

La denegación de servicio de la fragmentación de paquetes utiliza las debilidades de algunas pilas TCP/IP respecto a la desfragmentación IP (reensamblado de fragmentos IP).

⁷⁵ <http://samsclass.info/124/proj11/proj7x-scapy-IPv6.html>

Un ataque conocido que usa esto es Teardrop. La fragmentación offset del segundo fragmento es menor que el tamaño del primero y así para el offset añadido al tamaño del segundo. Esto significa que el primer fragmento contiene al segundo (superposición). En el tiempo de desfragmentación, algunos sistemas no gestionan esta excepción y esto les lleva a una denegación de servicio. Hay variantes de este ataque: bonk, boink y newtear por ejemplo. La denegación de servicio "ping de la muerte" explota la mala administración de la desfragmentación de ICMP, enviando más datos que el tamaño máximo de un paquete IP.⁷⁶

3.3.2.6 Denegación de servicio distribuida

La denegación de servicio distribuida tiene como objetivo saturar a la red atacada, mediante el uso de varios orígenes (demonios) para el ataque y masters para controlarlos.

Las herramientas más conocidas para DDoS (*Distributed Denial of Service*) son Tribal Flood Network (TFN), TFN2K, Trinoo y Stacheldraht.

El cracker usa masters para controlar fácilmente los orígenes. Obviamente, necesita conexiones (TCP) a los masters para configurar y preparar el ataque. Los masters sólo envían comandos a los orígenes vía UDP. Sin los masters, el cracker debería conectarse a cada origen. El origen del ataque sería detectado de forma más sencilla y su implementación sería más larga.⁷⁷

3.3.2.7 Scapy

- Es un script escrito en Python
- Genera paquetes de red
- Permite manipular capturas
- Es capaz de realizar ataques
- Funciona con los principales protocolos de comunicación

⁷⁶ <https://code.google.com/p/scapy-gui-IPv6/wiki/Installation>

⁷⁷ <http://www.secdev.org/projects/scapy/doc/installation.html>

Al ser un script, está disponible tanto para Linux como para Windows, ya que Python permite ambos sistemas.

Scapy < 2.X → Python 2.4

Scapy 2.X → Python 2.5 o superior

Para que Scapy funcione, necesita tener instalado Python junto con varias dependencias, según lo que se necesite (dnet, pcap, pyreadline, pywin32, winpcap).

Aparte, puede utilizar varias librerías para servicios avanzados (Plot, mostrar en pdf el paquete...).

PROTOSCOLOS

Scapy es capaz de “diseccionar” la mayoría de protocolos que existen (IP, Ethernet, STP, HSRP...)

Para ver todos los protocolos que soporta, se usa el comando ls().

ARP	HDLC	L2TP	Padding	SNMPget
ASN1_Packet	HSRP	LLC	PrismHeader	SNMPinform
BOOTP	ICMP	MGCP	RIP	SNMPnext
CookedLinux	ICMPError	MobileIP	RIPEntry	SNMPresponse
DHCP	IP	MobileIPRRP	RTP	SNMPset
DNS	IPError	MobileIPRRQ	RadioTap	SNMPtrapv1
DNSQR	IPv6	MobileIPTunnelData	Radius	SNMPtrapv2
DNSRR	ISAKMP	NBNSNodeStatusResponse	Raw	SNMPvarbind
Dot11	ISAKMP_class	NBNSNodeStatusResponseEnd	SMBMailSlot	STP
Dot11ATIM	ISAKMP_payload	NBNSNodeStatusResponseServ	SMBNegotiate_Protocol_Req	SebekHead
Dot11AssoReq	ISAKMP_payload_Hash	ice	uest_Header	SebekV1
Dot11AssoResp	ISAKMP_payload_ID	NBNSQueryRequest	SMBNegotiate_Protocol_Req	SebekV2
Dot11Auth	ISAKMP_payload_KE	NBNSQueryResponse	uest_Tail	SebekV2Sock
Dot11Beacon	ISAKMP_payload_Nonce	NBNSQueryResponseNegative	SMBNegotiate_Protocol_Res	SebekV3
Dot11Deauth	ISAKMP_payload_Proposal	NBNSRequest	ponse_Advanced_Security	SebekV3Sock
Dot11Disas	ISAKMP_payload_SA	NBNSWackResponse	SMBNegotiate_Protocol_Res	Skinny
Dot11Elt	ISAKMP_payload_Transform	NBTDatagram	ponse_No_Security	TCP
Dot11ProbeReq	ISAKMP_payload_VendorID	NBTSession	SMBNegotiate_Protocol_Res	TCPError
Dot11ProbeResp	IrLAPCommand	NTP	ponse_No_Security_No_Key	TFTP
Dot11QoS	IrLAPHead	NetBIOS_DS	SMBNetlogon_Protocol_Res	TFTP_ACK
Dot11ReassoReq	IrLMP	NetflowHeader	onse_Header	TFTP_DATA
Dot11ReassoResp	L2CAP_CmdHdr	NetflowHeaderV1	SMBNetlogon_Protocol_Res	TFTP_ERROR
Dot11WEP	L2CAP_CmdRej	NetflowRecordV1	onse_Tail_LM20	TFTP_OACK
Dot1Q	L2CAP_ConfReq	NoPayload	SMBNetlogon_Protocol_Res	TFTP_Option
Dot3	L2CAP_ConfResp	PPP	onse_Tail_SAM	TFTP_Options
EAP	L2CAP_ConnReq	PPP_ECP	SMBSession_Setup_AndX_R	TFTP_RRQ
EAPOL	L2CAP_ConnResp	PPP_ECP_Option	equest	TFTP_WRRQ
Ether	L2CAP_DisconnReq	PPP_IPCP	SMBSession_Setup_AndX_R	UDP
GPRS	L2CAP_DisconnResp	PPP_IPCP_Option	esponse	UDPError
GRE	L2CAP_Hdr	PPPoE	SNAP	X509Cert
HCI_ACL_Hdr	L2CAP_InfoReq	PPPoED	SNMP	X509RDN
HCI_Hdr	L2CAP_InfoResp	Packet	SNMPbulk	X509v3Ext
				_IPv6OptionHeader

Figura 3.46: Protocolos que soporta Scapy

COMANDOS

Para el control de Scapy, se dispone de varios comandos, que pueden ser listados con el comando `lsc()`.

Hay comandos que no se muestran en la ayuda, como los de gestión de ficheros (`rdpcap`, `wrpcap`) o los de mostrar gráficos (`psdump`, `pdfdump`).

La disponibilidad de muchos de los comandos, depende de si están instaladas las librerías adicionales para dar esa funcionalidad (desencriptación WEP, dibujo, etc.).

Algunas de las extensiones sólo están disponibles para Linux⁷⁸.

GENERACION DE PAQUETES

Para generar paquetes, hay que utilizar los protocolos antes mencionados.

Se pueden generar paquetes tanto de capa 2 (Ethernet) como de capa 3 (IP), necesarios para la comunicación.

Después, se añaden el resto de protocolos que se necesite.

Para generar datos de paquete de capa 2, se utiliza el protocolo Ethernet, abreviado como `Ether()`, indicando MAC de origen (`src`) y de destino (`dst`). Para introducir ambos campos, se separan por una coma (,).

```
capa2=Ether (src="00:00:0c:12:34:56",dst="00:fa:ba:da:00:01")
```

En capa 3, tenemos más campos dentro del comando, aparte de un campo de checksum. Éste campo puede rellenarse o no, ya que se puede generar al momento de enviarse.

```
capa3=IP (src="192.168.0.1",dst="10.200.250.18")
```

APILADO DE CAPAS

Crear un paquete desde cero, puede ser confuso si se introduce demasiados parámetros.

⁷⁸ <http://www.slideshare.net/ositobio/scapy-generacin-y-manipulacin-bsica-de-paquetes-de-red>

```
paquete=Ether(src="00:00:0c:12:34:56",dst="00:fa:ba:da:00:01")/IP(src="192.168.0.1",dst="10.200.250.18").
```

Se puede trabajar con varios "paquetes" de datos, cada uno en un tipo de capa.

Una vez creadas todas las capas, se puede apilarlas, generando un único paquete.

```
paquete=Ether(src="00:00:0c:12:34:56",dst="00:fa:ba:da:00:01")/IP(src="192.168.0.1",dst="10.200.250.18")
```

```
capa2=Ether(src="00:00:0c:12:34:56",dst="00:fa:ba:da:00:01")
```

```
capa3=IP(src="192.168.0.1",dst="10.200.250.18")
```

```
paquete=capa2/capa3
```

VISUALIZACION

Ciertamente ocasionalmente es útil ver cómo está el paquete de datos en memoria y si lo hemos generado de manera correcta.

Para visualizar los paquetes en memoria, se utiliza 3 comandos: `show()`, `show2()` y `hexdump()`.

Sintaxis:

`p.show()`.- Muestra el paquete en memoria

`p.show2()`.- Muestra el paquete rellenando los campos que se deben autogenerar

`hexdump(p)`.- Vuelca el contenido hexadecimal

ENVIO

Una vez generado el paquete de datos, es necesario enviarlo a la red, ya que para ello se lo ha creado.

Es posible enviarlo como paquete de capa 2 o de capa 3, mediante los comandos `sendp()` y `send()` respectivamente.

Estos comandos, generan automáticamente campos como el Checksum. Se le pasa como variable el nombre del paquete de datos⁷⁹.

También podemos enviar varias veces el mismo paquete.

```
sendp(NombreDelPaquete)
```

```
sendp(capa2)
```

```
send(NombreDelPaquete)
```

```
send(capa3)
```

```
send([NombreDelPaquete]*NúmeroDeVeces)
```

```
send([capa3]*10)80
```

3.3.2.8 Paquetes enviados a la red de distribución

En la red de distribución que aquí se propone, se ha empleado el siguiente comando en Scapy:

```
>>> b=Ether(src=None, dst=None)/IPv6(src='2001:1:1::10', dst='2001:2:2::10', hli
m=64)/TCP(dport=80, sport=20, flags=2)/Raw(load='hola mundo')
>>> □
```

Figura 3.47: Comando Scapy para enviar flujo de paquetes SYN

Visto con el comando *show()* tenemos:

⁷⁹ <http://www.secdev.org/projects/scapy/>

⁸⁰ <http://www.seguridadx.com/scapy/#more-135>

```

pc2@pc2-VirtualBox: ~
>>> b.show()
###[ Ethernet ]###
WARNING: Mac address to reach destination not found. Using broadcast.
dst= ff:ff:ff:ff:ff:ff
src= 08:00:27:02:11:4a
type= 0x86dd
###[ IPv6 ]###
version= 6
tc= 0
fl= 0
plen= None
nh= TCP
hlim= 64
src= 2001:1:1::10
dst= 2001:2:2::10
###[ TCP ]###
sport= ftp_data
dport= http
seq= 0
ack= 0
dataofs= None
reserved= 0
flags= S
window= 8192
chksum= None
urgptr= 0
options= {}
###[ Raw ]###
load= 'hola mundo'
>>>

```

Figura 3.48: Paquetes enviados a la red mediante Scapy visto con el comando `show()`

De la última imagen se puede concluir que:

El destino para el protocolo IPv4 no está especificado, por esta razón, se muestra un destino broadcast con la aclaración en la parte superior (**WARNING; Mac address to reach destination not found. Using broadcast**) que el destino no fue encontrado. El origen de los paquetes para el protocolo IPv4 si bien tampoco fue especificado, el programa SCAPY ha tomado la MAC ADDRESS como dirección origen.

Para el caso de IPv6, se puede observar que la versión es la correcta (versión=6), la dirección de origen y destino se encuentran especificadas (src=2001:1:1::10 la cual es la dirección del Servidor VLC de donde se enviará también paquetes desde SCAPY; dst=2001:2:2::10 la cual es dirección del Cliente PC4, es decir, los paquetes enviados por SCAPY atravesaran toda la red desde el Server VLC hacia el Cliente PC4)

3.3.2.9 Prueba de streaming de video enviado a la red de distribución

Cuando ya hemos confirmado el correcto funcionamiento del programa Scapy, podemos enviar el streaming de video junto con paquetes SYN, para comprobar la calidad del video al momento de la recepción en el cliente.

Mediante el programa WIRESHARK se puede capturar los paquetes generados por Scapy, este es el resultado:

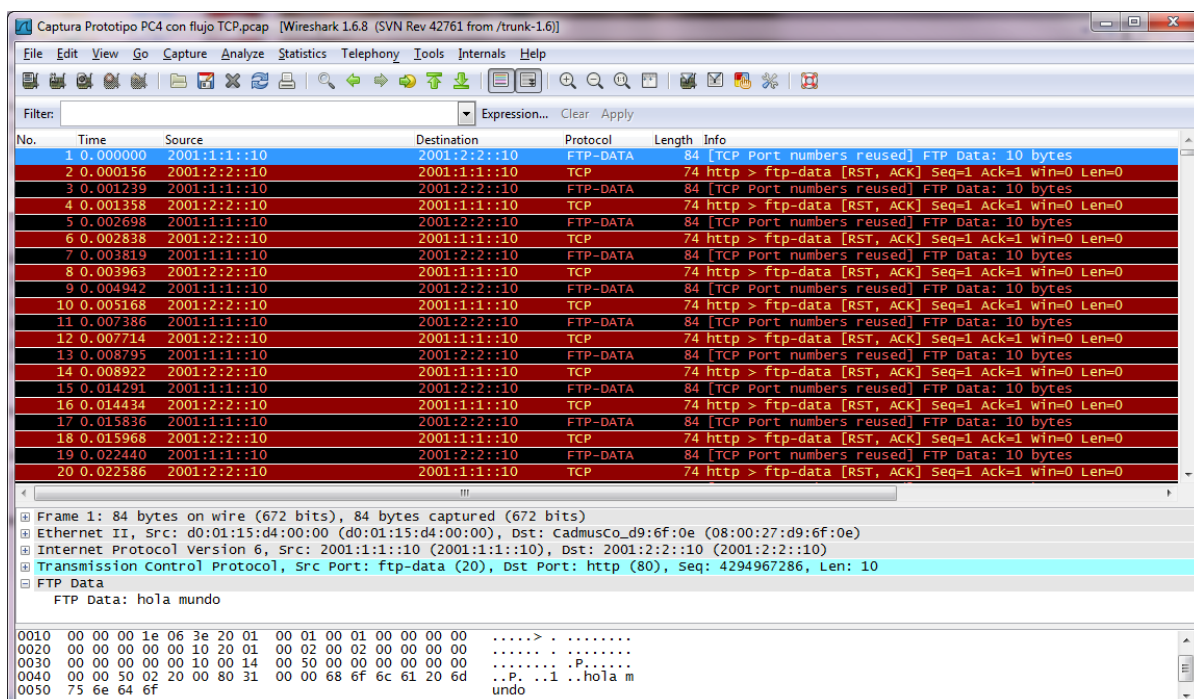


Figura 3.50: Captura de paquetes SYN mediante Wireshark.

Los paquetes han atravesado toda la red, desde el Server VLC hacia el Cliente PC4, claramente se puede observar que los paquetes enviados contienen datos con el texto “hola mundo” y el cliente realiza la contestación de sincronización a cada uno de los paquetes generados.

El siguiente ejercicio muestra el flujo de datos del streaming de video desde el Server VLC hacia el cliente PC1, simultáneamente se genera infinitos paquetes de sincronización desde el mismo origen (Server VLC) hacia el mismo cliente (PC1):

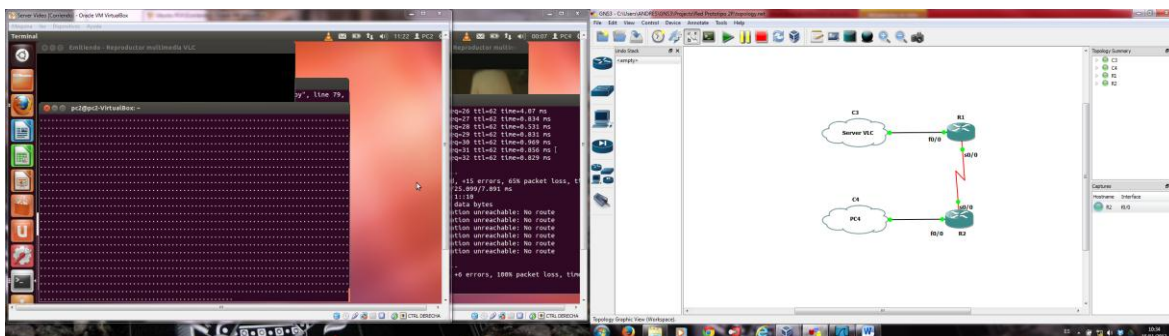


Figura 3.51: Envío de flujo de paquetes a la red.

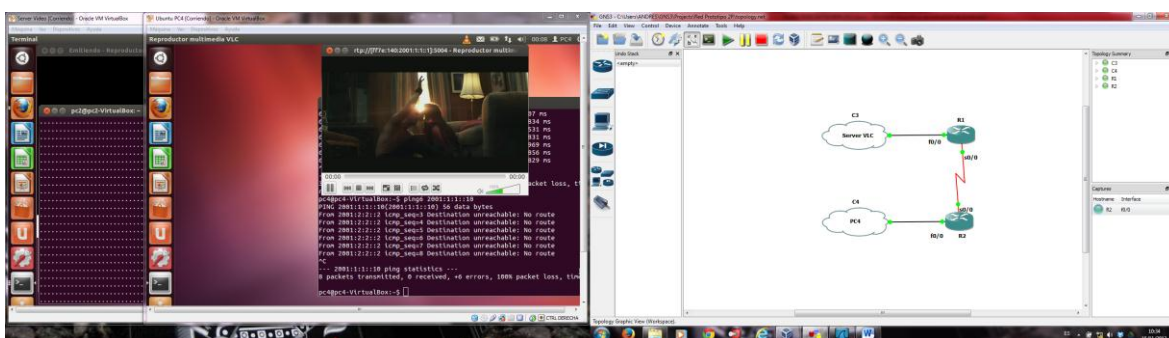


Figura 3.52: Recepción del streaming de video en el cliente PC1.

La captura de paquetes en WIRESHARK a continuación, muestra un flujo de datos UDP (pertenecientes al streaming de video) y TCP (pertenecientes al flujo de paquetes SYNC creados y enviados por Scapy)

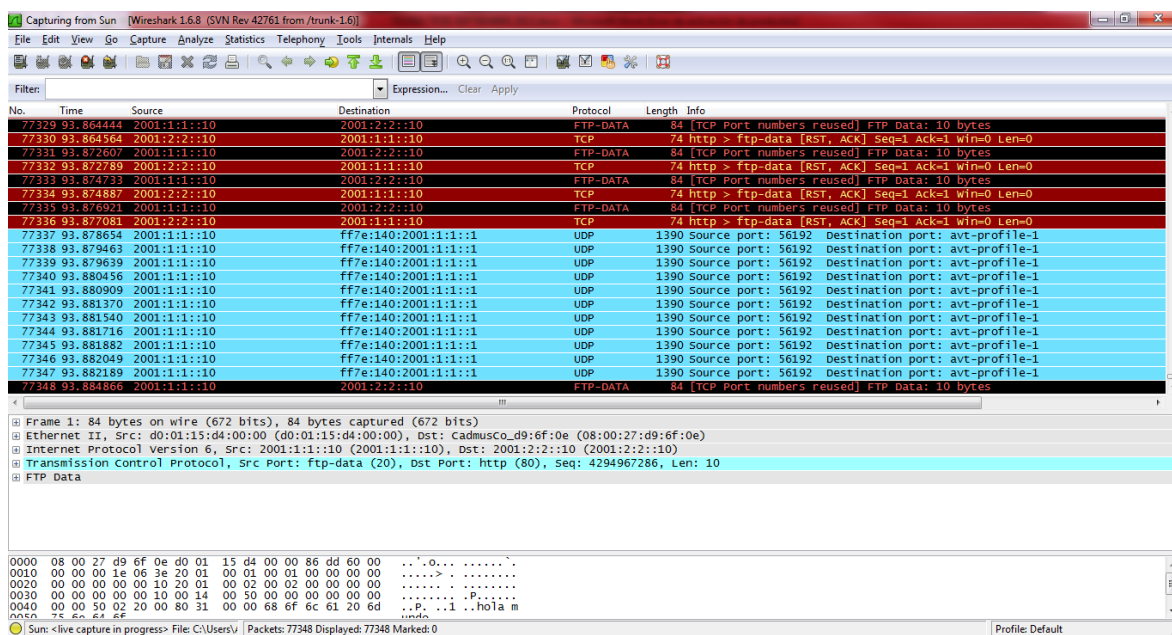


Figura 3.53: Captura de paquetes TCP y UDP al momento del streaming de video.

3.3.2.10 Capturas de pantalla de la red

Server VLC

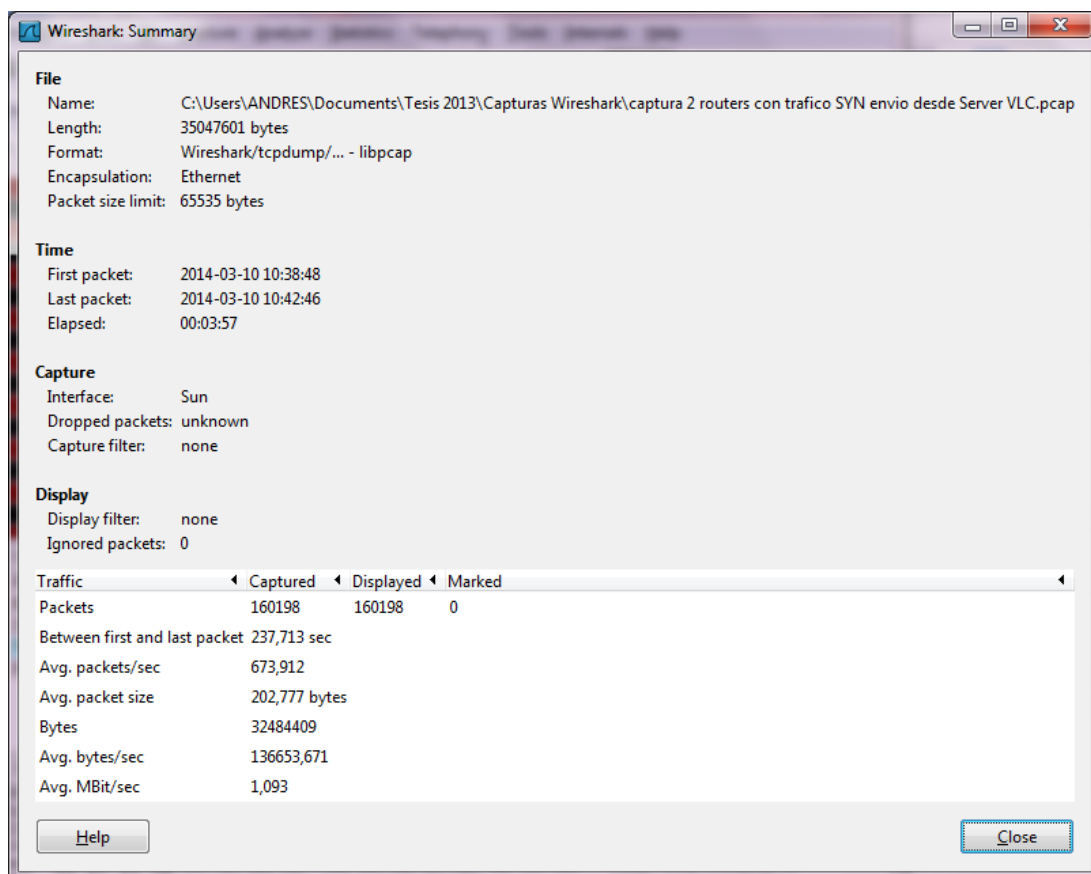


Figura 3.54: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	SERVER VLC
INTERFACE:	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 57 seg.
TIEMPO EN SEGUNDOS:	237.713 seg.
PAQUETES CAPTURADOS:	160198.00
PAQUETES MOSTRADOS:	160198.00
BYTES TOTALES:	32484409.00
PROMEDIO PAQUETES/SEG:	673912.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	202.777
PROMEDIO BYTES/SEG:	136653.671
PROMEDIO MBITS/SEG:	1.093

Tabla 3.20: Resumen de los datos mostrados en Wireshark.

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	160198	100,00 %	32484409	1,093	0	0	0,000
Ethernet	100,00 %	160198	100,00 %	32484409	1,093	0	0	0,000
Internet Protocol Version 6	99,88 %	160011	99,92 %	32457079	1,092	0	0	0,000
Transmission Control Protocol	90,32 %	144689	39,44 %	11512386	0,387	64149	4747026	0,160
FTP Data	50,28 %	80540	20,83 %	6765360	0,228	80540	6765360	0,228
User Datagram Protocol	9,46 %	15157	64,43 %	20929179	0,704	0	0	0,000
Data	9,42 %	15083	64,37 %	20909082	0,704	15083	20909082	0,704
Session Traversal Utilities for NAT	0,00 %	4	0,02 %	5560	0,000	0	0	0,000
Data	0,00 %	4	0,02 %	5560	0,000	4	5560	0,000
Domain Name Service	0,03 %	52	0,01 %	4652	0,000	52	4652	0,000
Hypertext Transfer Protocol	0,01 %	18	0,03 %	9885	0,000	18	9885	0,000
Internet Control Message Protocol v6	0,08 %	133	0,04 %	12266	0,000	133	12266	0,000
Open Shortest Path First	0,01 %	24	0,01 %	2160	0,000	24	2160	0,000
Protocol Independent Multicast	0,00 %	8	0,00 %	1088	0,000	8	1088	0,000
Configuration Test Protocol (loopback)	0,01 %	24	0,00 %	1440	0,000	0	0	0,000
Data	0,01 %	24	0,00 %	1440	0,000	24	1440	0,000
Internet Protocol Version 4	0,10 %	159	0,07 %	24266	0,001	0	0	0,000
User Datagram Protocol	0,10 %	154	0,07 %	23996	0,001	0	0	0,000
Domain Name Service	0,03 %	44	0,01 %	3004	0,000	44	3004	0,000
NetBIOS Name Service	0,05 %	75	0,02 %	6900	0,000	75	6900	0,000
Hypertext Transfer Protocol	0,02 %	33	0,04 %	12024	0,000	33	12024	0,000
Data	0,00 %	2	0,01 %	2068	0,000	2	2068	0,000
Internet Group Management Protocol	0,00 %	5	0,00 %	270	0,000	5	270	0,000
Logical-Link Control	0,00 %	4	0,00 %	1624	0,000	0	0	0,000
Cisco Discovery Protocol	0,00 %	4	0,00 %	1624	0,000	4	1624	0,000

Figura 3.55: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 3.55 se encuentra en la página 103

Ethernet: 22 Fibre Channel FDDI IPv4: 4 IPv6: 24 IPX JXTA NCP RSVP SCTP TCP: 1 Token Ring UDP: 55 USB WLAN

Ethernet Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
CadmusCo_02:11:4a	d0:00:0e4c:00:00	144 725	11 515 346	80 557	6 766 734	64 168	4 748 612	0,000000000	237,7134	227727,47	159809,65
CadmusCo_02:11:4a	IPv6mcast_00:00:00:01	15 085	20 912 534	15 085	20 912 534	0	0	0,068380000	220,3223	759343,28	N/A
CadmusCo_00:20:93	Broadcast	75	6 900	75	6 900	0	0	9,516359000	189,1737	291,80	N/A
CadmusCo_00:20:93	IPv6mcast_ff:20:00:00	56	4 816	56	4 816	0	0	2,011366000	76,3372	504,71	N/A
CadmusCo_00:20:93	IPv6mcast_00:01:00:03	44	3 884	44	3 884	0	0	9,215980000	187,7735	165,48	N/A
IPv4mcast_00:00:fc	CadmusCo_00:20:93	44	3 004	0	0	44	3 004	9,216038000	187,7735	N/A	127,98
IPv4mcast_7f:ffff	CadmusCo_00:20:93	35	14 092	0	0	35	14 092	17,528009000	72,7198	N/A	1550,28
d0:00:0e4c:00:00	d0:00:0e4c:00:00	24	1 440	24	1 440	0	0	0,730990000	232,8397	49,48	N/A
IPv6mcast_00:00:00:05	d0:00:0e4c:00:00	24	2 160	0	0	24	2 160	4,480280000	232,8826	N/A	74,20
CadmusCo_00:20:93	d0:00:0e4c:00:00	22	2 428	11	1 026	11	1 402	64,396883000	8,0555	1018,93	1392,34
CadmusCo_00:20:93	IPv6mcast_00:00:00:0c	20	11 993	20	11 993	0	0	46,680676000	43,5673	2202,20	N/A
CadmusCo_00:20:93	IPv6mcast_00:00:00:16	12	1 120	12	1 120	0	0	16,844204000	135,0128	66,36	N/A
IPv6mcast_00:00:00:0d	d0:00:0e4c:00:00	8	1 088	0	0	8	1 088	14,630814000	211,4216	N/A	41,17
IPv4mcast_00:00:16	CadmusCo_00:20:93	5	270	0	0	5	270	46,622710000	0,2224	N/A	9712,49
IPv6mcast_00:00:00:01	d0:00:0e4c:00:00	4	416	0	0	4	416	15,903438000	217,4409	N/A	15,31
CDP/VTP/DTP/PAGP/UDLD	d0:00:0e4c:00:00	4	1 624	0	0	4	1 624	46,660348000	182,2810	N/A	71,27
IPv6mcast_00:01:00:03	d0:00:0e4c:00:00	3	270	0	0	3	270	46,642746000	1,3411	N/A	1610,61
IPv6mcast_00:00:00:16	d0:00:0e4c:00:00	2	420	0	0	2	420	16,910019000	131,8922	N/A	25,48

Figura 3.56: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 3.56 se encuentra en la página 104

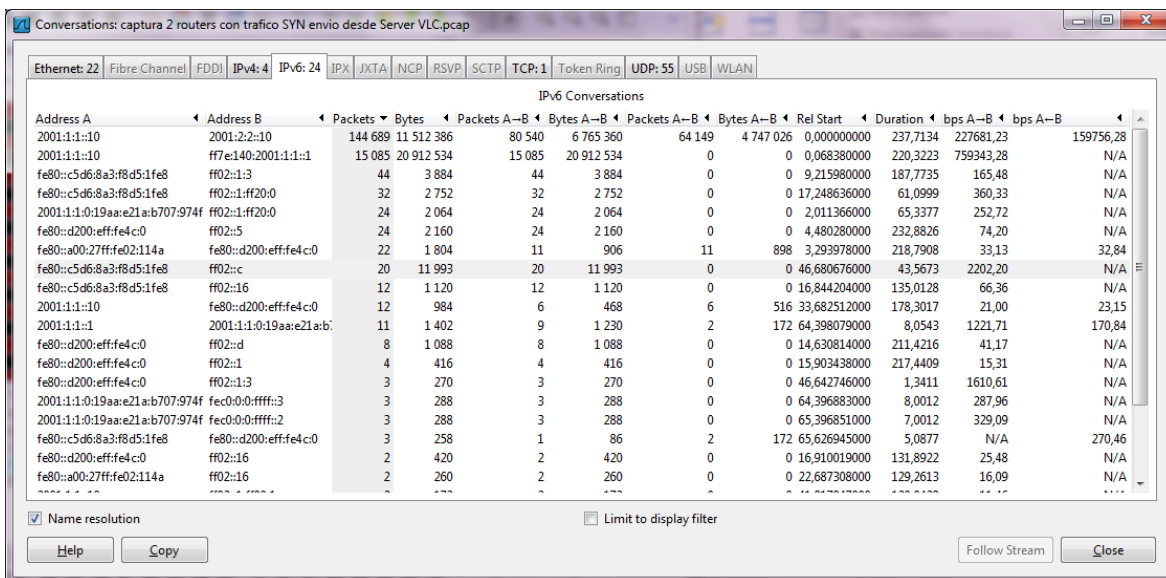


Figura 3.57: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 3.57 se encuentra en la página 105

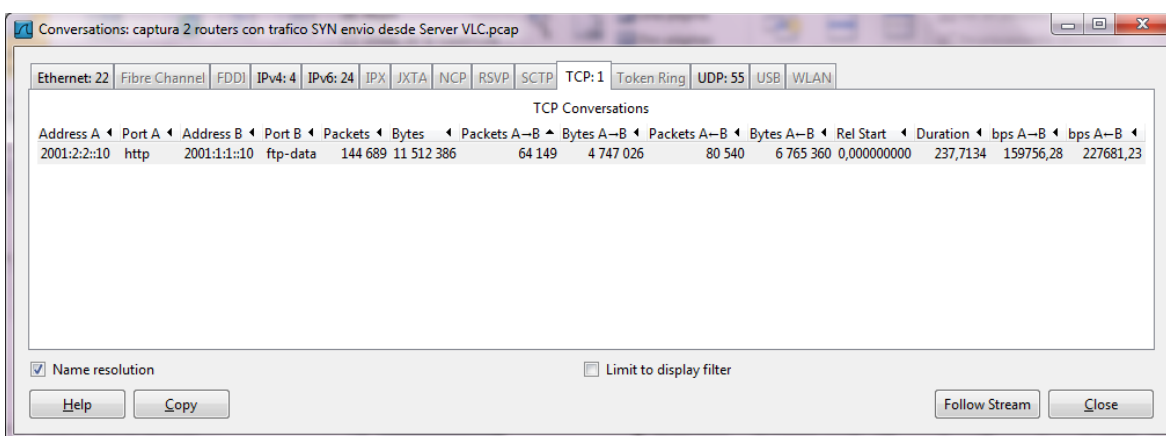


Figura 3.58: Paquetes UDP que atravesaron la red al momento de la captura.

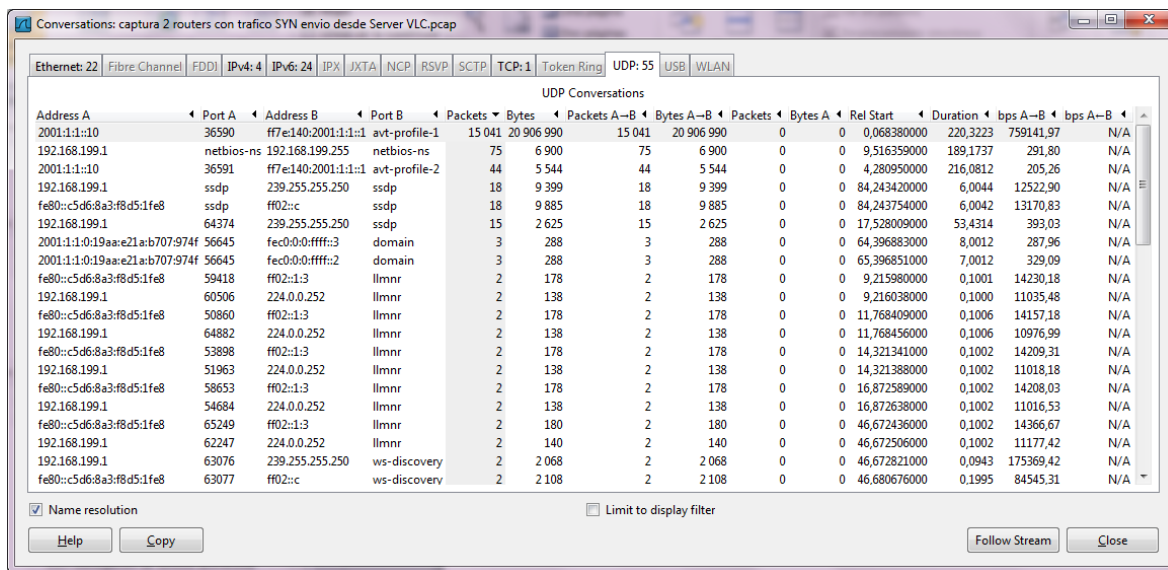


Figura 3.59: Paquetes TCP que atravesaron la red al momento de la captura.

* La explicación de la figura 3.58 se encuentra en la página 105

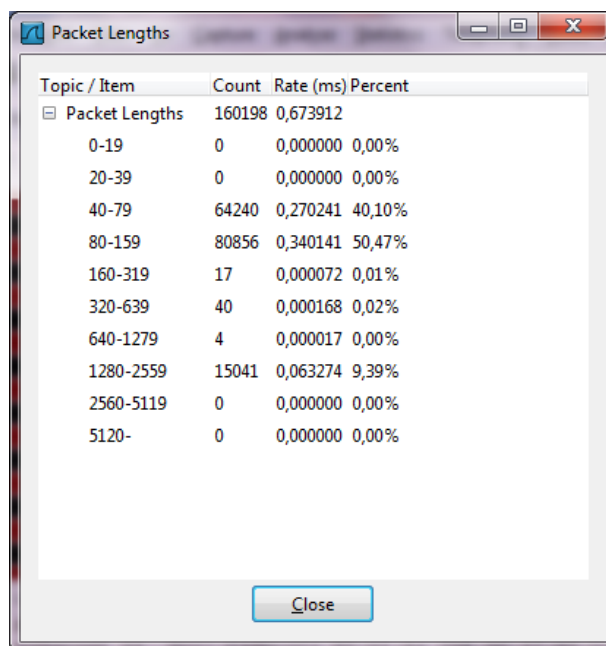


Figura 3.60: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 3.60 se encuentra en la página 106

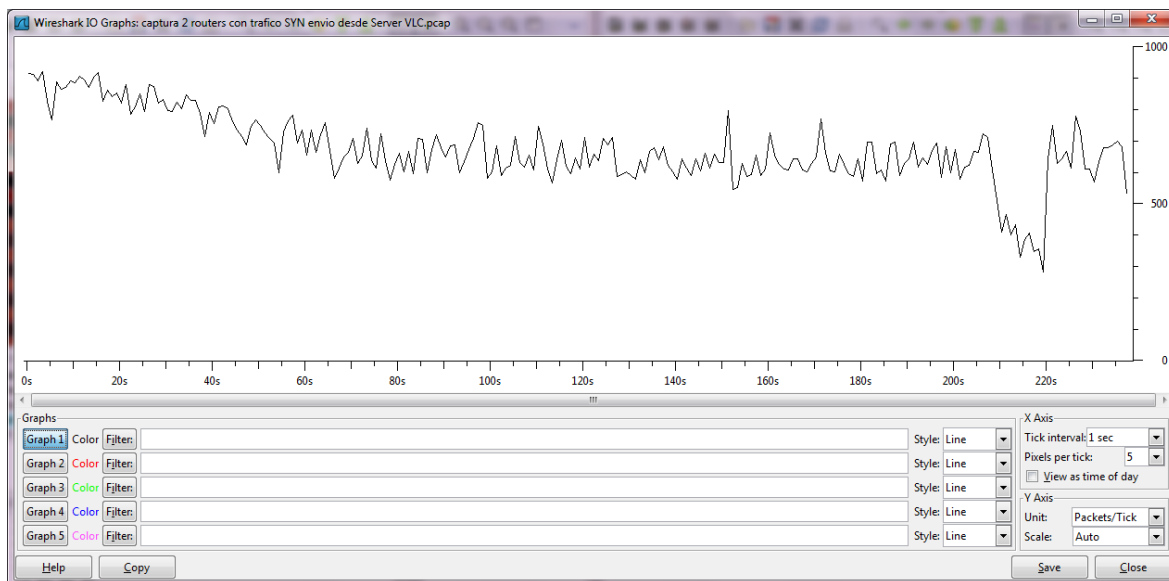


Figura 3.61: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

CLIENTE PC1

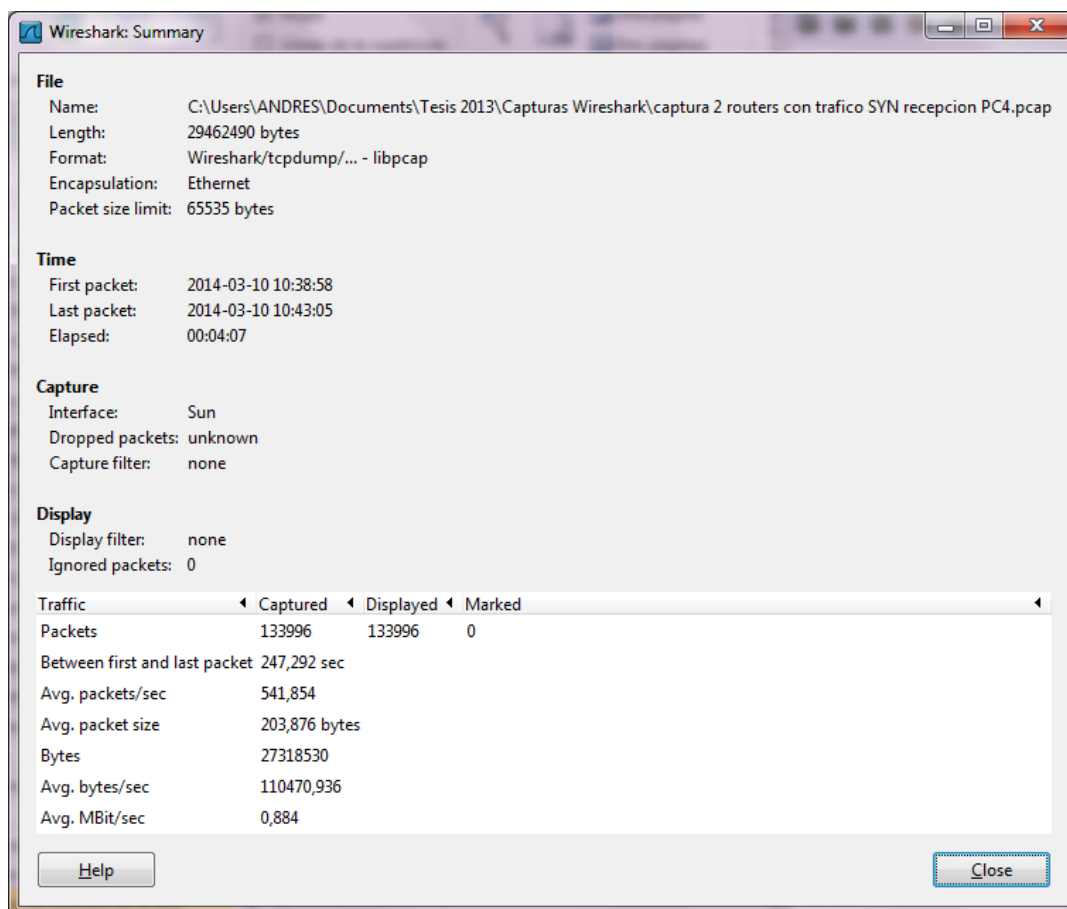


Figura 3.62: Resumen de los paquetes totales capturados por Wireshark, enviados por el Server VLC en el puerto Fastethernet 0/0 del router R1

PC:	CLIENTE PC1
INTERFACE:	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	4 min 07 seg.
TIEMPO EN SEGUNDOS:	247.292 seg.
PAQUETES CAPTURADOS:	133996.00
PAQUETES MOSTRADOS:	133996.00
BYTES TOTALES:	27318530.00
PROMEDIO PAQUETES/SEG:	541.854.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	203.876
PROMEDIO BYTES/SEG:	110470.936
PROMEDIO MBITS/SEG:	0.884

Tabla 3.21: Resumen de los datos mostrados en Wireshark.

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	133996	100,00 %	27318530	0,884	0	0	0,000
Ethernet	100,00 %	133996	100,00 %	27318530	0,884	0	0	0,000
Internet Protocol Version 6	99,85 %	133789	99,89 %	27289387	0,883	0	0	0,000
Transmission Control Protocol	89,99 %	120586	34,87 %	9526294	0,308	60293	4461682	0,144
FTP Data	45,00 %	60293	18,54 %	5064612	0,164	60293	5064612	0,164
User Datagram Protocol	9,65 %	12935	64,91 %	17731802	0,574	0	0	0,000
Data	9,51 %	12738	64,81 %	17705148	0,573	12738	17705148	0,573
Domain Name Service	0,13 %	179	0,06 %	16751	0,001	179	16751	0,001
Hypertext Transfer Protocol	0,01 %	18	0,04 %	9903	0,000	18	9903	0,000
Internet Control Message Protocol v6	0,17 %	234	0,10 %	27817	0,001	234	27817	0,001
Open Shortest Path First	0,02 %	25	0,01 %	2250	0,000	25	2250	0,000
Protocol Independent Multicast	0,01 %	9	0,00 %	1224	0,000	9	1224	0,000
Internet Protocol Version 4	0,13 %	178	0,10 %	26019	0,001	0	0	0,000
Configuration Test Protocol (loopback)	0,02 %	25	0,01 %	1500	0,000	0	0	0,000
Data	0,02 %	25	0,01 %	1500	0,000	25	1500	0,000
Logical-Link Control	0,00 %	4	0,01 %	1624	0,000	0	0	0,000
Cisco Discovery Protocol	0,00 %	4	0,01 %	1624	0,000	4	1624	0,000

Figura 3.63: Resumen detallado de los paquetes capturados por Wireshark.

* La explicación de la figura 3.63 se encuentra en la página 103

Conversations: captura 2 routers con trafico SYN recepcion PC4.pcap

Ethernet: 21 | Fibre Channel | FDDI | IPv4: 4 | IPv6: 25 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 1 | Token Ring | UDP: 88 | USB | WLAN

Ethernet Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
CadmusCo_d9:6f:0e	d0:01:0e:4c:00:00	120 633	9 530 160	60 318	4 463 728	60 315	5 066 432	0,000000000	199,4152	179072,73	203251,59
IPv6mcast_00:00:00:01	d0:01:0e:4c:00:00	12 740	17 703 456	0	0	12 740	17 703 456	0,092235000	218,7492	N/A	647443,14
CadmusCo_00:14:81	d0:01:0e:4c:00:00	280	32 664	139	13 193	141	19 471	36,825376000	127,1817	829,87	1224,77
CadmusCo_00:14:81	Broadcast	88	8 257	88	8 257	0	0	0,362486000	246,9291	267,51	N/A
CadmusCo_00:14:81	IPv6mcast_00:01:00:03	50	4 418	50	4 418	0	0	1,863578000	245,2278	144,13	N/A
IPv4mcast_00:00:fc	CadmusCo_00:14:81	50	3 418	0	0	50	3 418	1,863625000	245,2278	N/A	111,50
IPv4mcast_7f:ff:fa	CadmusCo_00:14:81	35	14 074	0	0	35	14 074	7,623113000	72,7196	N/A	1548,30
d0:01:0e:4c:00:00	d0:01:0e:4c:00:00	25	1 500	25	1 500	0	0	0,765915000	242,1609	49,55	N/A
IPv6mcast_00:00:00:05	d0:01:0e:4c:00:00	25	2 250	0	0	25	2 250	3,724315000	242,1654	N/A	74,33
CadmusCo_00:14:81	IPv6mcast_00:00:00:0c	20	12 011	20	12 011	0	0	36,775805000	43,5670	2205,52	N/A
CadmusCo_00:14:81	IPv6mcast_00:00:00:16	15	1 370	15	1 370	0	0	0,938595000	134,0123	81,78	N/A
IPv6mcast_00:00:00:0d	d0:01:0e:4c:00:00	9	1 224	0	0	9	1 224	3,909069000	239,3384	N/A	40,91
CadmusCo_00:14:81	IPv6mcast_ff:4c:00:00	7	602	7	602	0	0	36,759328000	193,2021	24,93	N/A
IPv4mcast_00:00:16	CadmusCo_00:14:81	5	270	0	0	5	270	36,717730000	0,2223	N/A	9716,38
CDP/VTP/DTP/PAgP/UDLD	d0:01:0e:4c:00:00	4	1 624	0	0	4	1 624	35,865035000	181,6601	N/A	71,52
IPv6mcast_00:01:00:03	d0:01:0e:4c:00:00	3	270	0	0	3	270	36,848369000	1,1635	N/A	1856,42
CadmusCo_d9:6f:0e	IPv6mcast_00:00:00:16	2	300	2	300	0	0	4,153909000	125,8271	19,07	N/A
IPv6mcast_00:00:00:16	d0:01:0e:4c:00:00	2	420	0	0	2	420	5,007235000	129,1474	N/A	26,02
CadmusCo_00:14:81	IPv6mcast_ff:95:d3:ed	1	78	1	78	0	0	36,941277000	0,0000	N/A	N/A
CadmusCo_00:14:81	IPv6mcast_ff:40:76:29	1	78	1	78	0	0	36,941299000	0,0000	N/A	N/A
IPv6mcast_ff:40:76:29	d0:01:0e:4c:00:00	1	86	0	0	1	86	42,170594000	0,0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 3.64: Paquetes Ethernet que atravesaron la red al momento de la captura.

* La explicación de la figura 3.64 se encuentra en la página 104

Conversations: captura 2 routers con trafico SYN recepcion PC4.pcap

Ethernet: 21 | Fibre Channel | FDDI | IPv4: 4 | IPv6: 25 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 1 | Token Ring | UDP: 88 | USB | WLAN

IPv6 Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
2001:1::10	2001:2::10	120 586	9 526 294	60 293	5 064 612	60 293	4 461 682	0,000000000	199,4152	203178,58	178990,65
2001:1::10	ff7e:140:2001:1:1::1	12 736	17 703 040	12 736	17 703 040	0	0	0,092235000	188,2306	752398,09	N/A
2001:2::2	2001:2:2:0:e401:253d:d940:7629	131	18 627	129	18 455	2	172	42,170801000	119,8098	1232,29	11,48
fe80::e4fb:88ad:9795:d3ed	ff02::1:3	50	4 418	50	4 418	0	0	1,863578000	245,2278	144,13	N/A
2001:2:2:0:e401:253d:d940:7629	fec0:0:0:ffff::3	48	4 603	48	4 603	0	0	42,169141000	119,8108	307,35	N/A
2001:2:2:0:e401:253d:d940:7629	fec0:0:0:ffff::1	41	3 911	41	3 911	0	0	42,169213000	119,8107	261,15	N/A
2001:2:2:0:e401:253d:d940:7629	fec0:0:0:ffff::2	40	3 819	40	3 819	0	0	43,169164000	118,8108	257,15	N/A
fe80::d201:eff:fe4c:0	ff02::5	25	2 250	25	2 250	0	0	3,724315000	242,1654	74,33	N/A
fe80::e4fb:88ad:9795:d3ed	ff02::c	20	12 011	20	12 011	0	0	36,775805000	43,5670	2205,52	N/A
fe80::a00:27ff:fed9:6f0e	fe80::d201:eff:fe4c:0	18	1 476	9	734	9	742	13,130445000	152,9357	38,40	38,81
2001:2:2::10	fe80::d201:eff:fe4c:0	16	1 312	8	624	8	688	18,765547000	179,6382	27,79	30,64
fe80::e4fb:88ad:9795:d3ed	ff02::16	15	1 370	15	1 370	0	0	0,938595000	134,0123	81,78	N/A
fe80::d201:eff:fe4c:0	fe80::e4fb:88ad:9795:d3ed	14	1 188	9	758	5	430	36,825376000	127,1817	47,68	27,05
2001:2:2::2	fe80::a00:27ff:fed9:6f0e	13	1 078	5	390	8	688	8,089860000	191,2017	16,32	28,79
fe80::d201:eff:fe4c:0	ff02::d	9	1 224	9	1 224	0	0	3,909069000	239,3384	40,91	N/A
2001:2:2:0:e401:253d:d940:7629	fe80::d201:eff:fe4c:0	6	516	3	258	3	258	79,263318000	79,7596	25,88	25,88
fe80::d201:eff:fe4c:0	ff02::1	4	416	4	416	0	0	0,242340000	218,5991	15,22	N/A
fe80::e4fb:88ad:9795:d3ed	ff02::1:ff4c:0	4	344	4	344	0	0	36,759328000	29,7337	92,55	N/A
fe80::d201:eff:fe4c:0	ff02::1:3	3	270	3	270	0	0	36,848369000	1,1635	1856,42	N/A
2001:2:2:0:e401:253d:d940:7629	ff02::1:ff4c:0	3	258	3	258	0	0	228,242907000	1,7185	1201,05	N/A
fe80::a00:27ff:fed9:6f0e	ff02::16	2	300	2	300	0	0	4,153909000	125,8271	19,07	N/A
fe80::d201:eff:fe4c:0	ff02::16	2	420	2	420	0	0	5,007235000	129,1474	26,02	N/A
::	ff02::1:ff95:d3ed	1	78	1	78	0	0	36,941277000	0,0000	N/A	N/A
::	ff02::1:ff40:7629	1	78	1	78	0	0	36,941299000	0,0000	N/A	N/A
2001:2:2::2	ff02::1:ff40:7629	1	86	1	86	0	0	42,170594000	0,0000	N/A	N/A

Name resolution Limit to display filter

Help Copy Follow Stream Close

Figura 3.65: Paquetes IPv6 que atravesaron la red al momento de la captura

* La explicación de la figura 3.65 se encuentra en la página 105

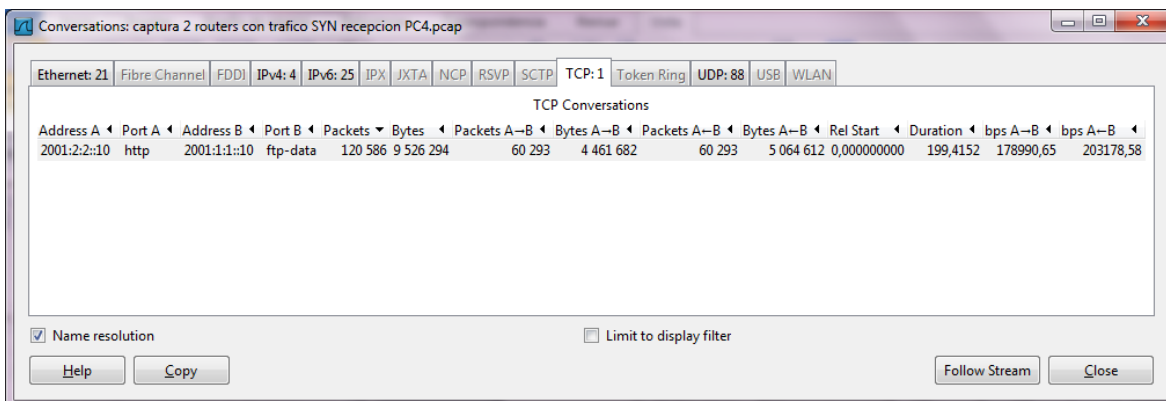


Figura 3.66: Paquetes UDP que atravesaron la red al momento de la captura.

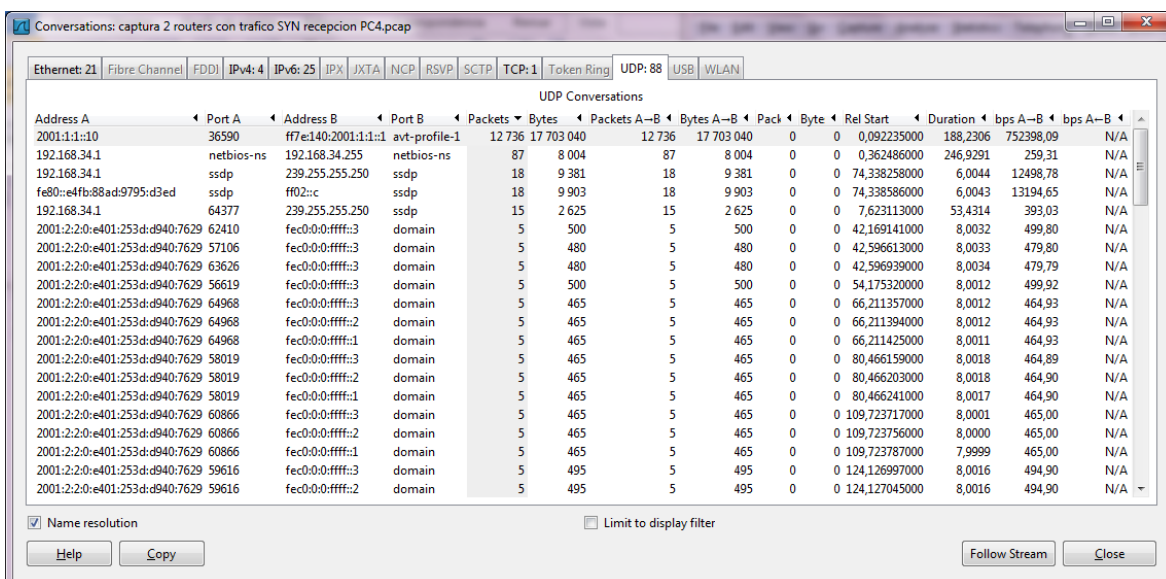


Figura 3.67: Paquetes UDP que atravesaron la red al momento de la captura.

* La explicación de la figura 3.67 se encuentra en la página 105

Topic / Item	Count	Rate (ms)	Percent
Packet Lengths	133996	0,541854	
0-19	0	0,000000	0,00%
20-39	0	0,000000	0,00%
40-79	60400	0,244246	45,08%
80-159	60798	0,245856	45,37%
160-319	18	0,000073	0,01%
320-639	40	0,000162	0,03%
640-1279	4	0,000016	0,00%
1280-2559	12736	0,051502	9,50%
2560-5119	0	0,000000	0,00%
5120-	0	0,000000	0,00%

Figura 3.68: Rangos de las diferentes longitudes de los paquetes capturados.

* La explicación de la figura 3.68 se encuentra en la página 106

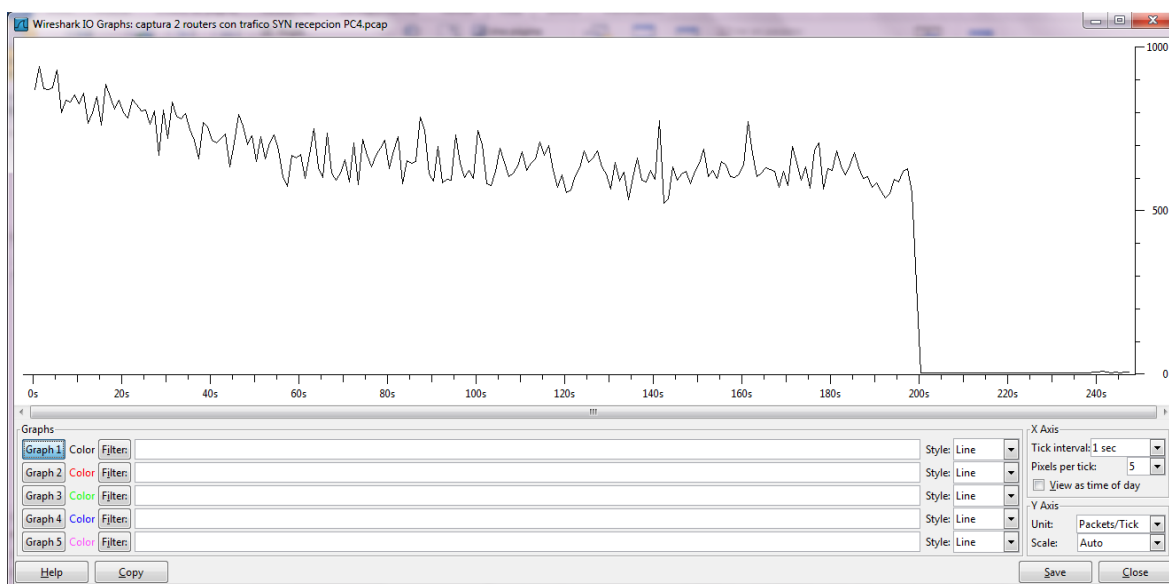


Figura 3.69: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

3.3.2.11 Cálculo de los parámetros de calidad en la red de distribución

3.3.2.11.1 Cálculos de la Velocidad de Transmisión

TABLA DE VALORES CAPTURADOS					
TOPOLOGIA:	2 ROUTERS DENEGACION DE SERVICIO				
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES TCP BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	32484409,00	32457079,00	11512386,00	20929179,00	237,713
CLIENTE PC1	27318530,00	27289387,00	9526294,00	17731802,00	247,292
TABLA DE VELOCIDADES					
		SERVER VLC	CLIENTE PC1		
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)		136653,90	110470,74		
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)		136538,93	110352,89		
VELOCIDAD DE TRANSMISION PURAMENTE DATOS TCP (BYTES/SEG)		48429,77	38522,45		
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)		88043,90	71703,90		

Tabla 3.22: Velocidades de transmisión obtenidas en la simulación.

3.3.2.11.2 Cálculos de Latencia

PRUEBA N° 1	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	69,70	41,18
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	45,00	44,00
PAQUETES PERDIDOS	5,00	6,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	13,64
PAQUETE MIN TIEMPO (mseg)	0,31	0,44
PAQUETE MAX TIEMPO (mseg)	11,60	6,05
PAQUETE TIEMPO PROMEDIO (mseg)	1,55	0,94

Tabla 3.23: Resumen de la tabla de valores de tiempos de retardo, Prueba 1: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 2	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	38,66	49,29
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	45,00	45,00
PAQUETES PERDIDOS	5,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	11,11	11,11
PAQUETE MIN TIEMPO (mseg)	0,29	0,44
PAQUETE MAX TIEMPO (mseg)	7,14	6,05
PAQUETE TIEMPO PROMEDIO (mseg)	0,86	1,10

Tabla 3.24: Resumen de la tabla de valores de tiempos de retardo, Prueba 2: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

PRUEBA N° 3	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	60,10	50,57
PAQUETES TRANSMITIDOS	50,00	50,00
PAQUETES RECIBIDOS	44,00	45,00
PAQUETES PERDIDOS	6,00	5,00
PORCENTAJE DE PAQUETES PERDIDOS %	13,64	11,11
PAQUETE MIN TIEMPO (mseg)	0,50	0,24
PAQUETE MAX TIEMPO (mseg)	9,60	6,05
PAQUETE TIEMPO PROMEDIO (mseg)	1,37	1,12

Tabla 3.25: Resumen de la tabla de valores de tiempos de retardo, Prueba 3: Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

RESUMEN	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	168,46	141,04
PAQUETES TRANSMITIDOS	150,00	150,00
PAQUETES RECIBIDOS	134,00	134,00
PAQUETES PERDIDOS	16,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,67
PAQUETE MIN TIEMPO (mseg)	0,29	0,24
PAQUETE MAX TIEMPO (mseg)	11,60	6,05
PAQUETE TIEMPO PROMEDIO (mseg)	1,26	1,05

Tabla 3.26: Comparación de los valores de tiempos de retardo en las 3 pruebas anteriores, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

El resumen muestra, luego de haber realizado 3 pruebas con el comando PING al cliente PC1, que en promedio el valor del retardo o LATENCIA en la red es:

- Latencia calculada desde el Server VLC a Cliente PC1
Latencia = 1.26 mseg.

- Latencia calculada desde el Cliente PC1 al Server VLC
Latencia = 1.05 mseg.

3.3.2.11.3 Cálculos de Jitter

CALCULO DE JITTER				
N°	SERVER VLC	JITTER	CLIENTE PC1	JITTER
15	0,81	-0,05	0,63	0,25
16	0,86	-0,05	0,78	-0,15
17	0,51	0,35	0,83	-0,05
18	7,14	-6,63	0,73	0,10
19	0,83	6,31	0,70	0,03
20	0,97	-0,14	0,86	-0,16
21	0,88	0,09	0,56	0,30
22	0,93	-0,05	0,65	-0,09
23	9,60	-8,67	0,79	-0,14
24	0,90	8,70	0,69	0,10
25	0,77	0,13	1,42	-0,73
26	0,89	-0,12	0,68	0,74
27	8,78	-7,89	0,82	-0,14
28	0,86	7,92	0,61	0,21
29	0,84	0,02	0,68	-0,07
30	0,74	0,10	0,76	-0,08
31	0,50	0,24	0,66	0,10
32	0,63	-0,13	0,73	-0,07
33	0,74	-0,11	1,00	-0,27
34	0,67	0,07	0,85	0,15
35	0,81	-0,14	0,80	0,05
36	1,06	-0,25	1,26	-0,46
37	0,65	0,41	0,70	0,56
38	0,85	-0,20	0,75	-0,05
39	0,51	0,34	0,71	0,04
40	0,69	-0,18	0,72	-0,01
41	0,39	0,30	6,05	-5,33
42	1,00	-0,61	0,72	5,33
43	0,53	0,47	0,71	0,01
44	0,68	-0,14	1,18	-0,47
45	1,26	-0,59	0,89	0,29
46	1,00	0,26	0,64	0,25
47	0,31	0,69	0,85	-0,21
48	1,11	-0,80	1,00	-0,15
49	0,75	0,36	0,48	0,52
50	1,06	-0,31	0,86	-0,38
JITTER MIN		-8,67		-5,33
JITTER MAX		10,84		5,33

Tabla 3.27: Tabla de valores de la variación de retardo o JITTER, Server VLC ↔ Cliente PC1 y Server VLC ↔ Cliente PC5.

3.3.2.11.4 Cálculos de Pérdida de Paquetes

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING		
TOPOLOGIA:	2 ROUTERS CON DENEGACION DE SERVICIO	
RESUMEN GENERAL		
PC:	SERVER VLC	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	3 min 57 seg.	4 min 07 seg.
TIEMPO EN SEGUNDOS:	237.713 seg.	247.292 seg.
PAQUETES CAPTURADOS:	160198.00	133996.00
PAQUETES MOSTRADOS:	160198.00	133996.00
BYTES TOTALES:	32484409.00	27318530.00
PROMEDIO PAQUETES/SEG:	673912.00	541.854.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	202.777	203.876
PROMEDIO BYTES/SEG:	136.653.671	110.470.936
PROMEDIO MBITS/SEG:	1.093	0.884

Tabla 3.28: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la simulación.

En la tabla comparativa, podemos observar que las velocidades de transmisión del Server VLC y del Cliente PC1 son diferentes, por tanto el número de Bytes recibidos por el cliente PC1 va a ser mucho menor que los Bytes enviados por el Server VLC.

Esto se debe, a que por la red no solo son enviados paquetes de datos de video, sino también, paquetes “basura” los cuales están saturando la red, dando como resultado que varios de los paquetes de datos de video se pierdan durante la transmisión.

Podemos observar también, que a pesar que existe una diferencia de 10 segundos en la captura de paquetes en el Server VLC (tiempo de captura = 3 min y 57 seg) y el Cliente PC1 (tiempo de captura = 4 min y 07 seg), el número de paquetes en el cliente es mucho menor.

En resumen, El Server VLC envió mucha más cantidad de paquetes a la red en el mismo tiempo de transmisión del video streaming, lo cual da como velocidad de transmisión promedio de 1.093 MBits/seg. Para el cliente PC1, si bien el tiempo de recepción de video streaming fue mayor, la cantidad de paquetes fue menor, dando como resultado una velocidad de transmisión promedio de 0.884 MBits/seg.

Es decir, la cantidad de pérdida de paquetes es:

PC:	SERVER VLC	CLIENTE PC1
PAQUETES CAPTURADOS:	160198,00	133996,00
BYTES TOTALES:	32484409,00	27318530,00
BYTES PERDIDOS:	0	5165879,00
PERDIDA DE PAQUETES:	0	26202,00

Tabla 3.29: Paquetes perdidos durante la transmisión.

CAPÍTULO IV

PRUEBAS Y ANÁLISIS DE RESULTADOS

En este proyecto existen varios escenarios posibles que podemos encontrar en las redes de distribución, tales como: diferentes tipos de topologías, routers que de un momento a otro dejan de funcionar y por tanto, la red busca nuevos caminos, ataques a la red mediante flujos de paquetes distintos a paquetes de datos, es decir, denegación de servicio.

En cada uno de estos escenarios se ha capturado la información necesaria para realizar el análisis correspondiente.

Para realizar la comparación de los datos obtenidos, con datos físicamente demostrados en un laboratorio, vamos a ayudarnos del documento llamado “*PROPUESTA PARA LA VALIDACIÓN DE LA CALIDAD DEL VÍDEO EN EL SERVICIO DE IPTV*”, del autor, el Ing. Luís Enrique Conde del Oso, La Habana, Cuba, 2012.⁸¹

Este documento contiene información muy detallada de los parámetros de calidad mínimos necesarios para que una transmisión de video streaming sea exitosa.

A continuación vamos a citar parte del texto que se encuentra en este documento, referente a los parámetros mínimos de calidad para una transmisión de video IPTV:

“Los servicios de IPTV se dividen en dos grandes grupos; el servicio de multidifusión Broadcast TV (BTV), el cual se basa en el flujo (stream) multicast sobre una red IP, y el servicio de unidifusión, por ejemplo el Vídeo en Demanda (VoD), basado en el flujo unicast de vídeo.”

⁸¹ <http://revistas.mes.edu.cu/greenstone/collect/repo/import/repo/20120830/71208073310.pdf>

Tabla 1.1. Tasas de bits mínimas requeridas en función de los codec MPEG2 y MPEG4. (Fuente DSL Forum's WT-126. v0.5 (draft). "Triple Play Service QoE. Requirement and Mechanisms"). [10].

Tipo de Señal	MPG2 (MP@ML)	MPG4 (MP@L3)
Broadcast TV – SD.	2,5 Mbps	1,75 Mbps
Broadcast TV – HD.	15 Mbps	10 Mbps
VoD – SD.	3,18 Mbps	2,1 Mbps

Como se observa en la Tabla 1.1, la selección del codec, la velocidad (bit rate) y los tipos de perfil y nivel de una señal de vídeo transmitida sobre una red IP son aspectos que permiten ofrecer diferentes grados de calidad, QoE.

§1.4 Criterios de dimensionamiento de la red IP con servicios de IPTV

Debido al carácter interactivo de los servicios de IPTV el correcto dimensionamiento de la red IP que los soporta es un factor crítico para su adecuado funcionamiento. [11].

La interactividad comprende diferentes acciones que pueden ser agrupadas en diferentes grupos de acuerdo a su velocidad de respuesta esperada, de esta manera se agrupan como acciones interactivas, de respuestas y acciones temporales.

El estudio de ciertos factores humanos ha demostrado que para que una acción sea percibida por el usuario como instantánea debe recibirse una realimentación como respuesta a esta en un tiempo que se encuentre en el rango entre 50 y 200 mseg.

Por este motivo los disturbios que se presentan en una red IP deben ser controlados de manera que los mismos no afecten la interactividad del usuario con el sistema en las diferentes acciones que este realiza con el mismo. Tabla 1.2.

Tabla 1.2 Clasificación de las acciones más comunes del servicio de IPTV. [11]

Acciones del usuario.	Funcionalidades.	Tipo.	Retardo Máximo.
Interfaz con el sistema.	<ul style="list-style-type: none"> • Navegación en la EPG. • Acción de los controles del VoD (Forward, Rewind y Pausa). Tiempo transcurrido desde que se da la orden en el control remoto hasta que se recibe en la TV la señal o respuesta de que fue ejecutada.	Interactiva.	200 mseg.
Cambio de canal (zapping).	<ul style="list-style-type: none"> • Tiempo desde que se da la orden en el control remoto hasta que se recibe en la TV el canal solicitado en forma estable. 	Respuesta.	2 seg.
Tiempo de inicio.	<ul style="list-style-type: none"> • Tiempo desde que se enciende el STB hasta que se encuentren disponibles los canales. 	Temporal.	10 seg.

En una red IP los disturbios que afectan directamente la QoE de la señal de vídeo del servicio de IPTV, son el retardo (delay), la variación del retardo (jitter) y las pérdidas de paquetes.

El retardo y el jitter máximo soportado en la red IP están directamente relacionados con el tamaño de la memoria de almacenamiento temporal (buffer) del STB. En general los STB comerciales pueden almacenar entre 100 y 500 mseg de vídeo, por lo que teóricamente los parámetros de la red deberían poder variar en ese rango, condición esta que pudiera comprometer otras acciones como el tiempo de cambio de canal (zapping).

Los valores recomendados de retardo y variación del retardo (jitter) de extremo a extremo, [11], (o sea desde el Equipo de Cabecera al STB) son:

- Retardo: menor a 200 ms.
- Jitter: menor a 50 ms.

Respecto a la pérdida de paquetes se puede decir que una señal de vídeo es muy sensible a la pérdida de paquetes, dependiendo además del tipo de información que se pierde, ya que la pérdida de diferentes tipos de imágenes producen diferentes afectaciones, por ejemplo la pérdida de una imagen tipo I (Intra) o una imagen tipo P (Predicted) producen una pérdida de calidad de imagen mayor y durante mayor tiempo que la pérdida de una imagen del tipo B (Bidirectional). [12], [13].

Con el objetivo de minimizar los efectos de las pérdidas de paquetes se recomienda siempre el envío de los paquetes corruptos a la capa de procesamiento de MPEG, siendo esta una mejor condición que descartar paquetes.⁸²

Además en este documento se presenta una tabla de recomendaciones mínimas para satisfacer la calidad de servicio en IPTV estándar.

“La recomendación mínima para satisfacer la QoS del servicio IPTV estándar (SD) con diferentes valores de velocidades (bit rate) se muestran en la Tabla 2.4, y son extraídos de los resultados del documento “Quality of Experience Requirements for IPTV (FG IPTV-DOC-0086).⁸³

Tabla 2.4 Recomendaciones mínimas para satisfacer la QoS del servicio IPTV estándar (SD) para diferentes valores de velocidades (bit rate) según el FG IPTV-DOC-0086. [24].

Transport Stream bit rate(Mbps)	Retardo (mseg)	Jitter (mseg)	Duración máxima de un error. (mseg)	Paquetes IP perdidos	Distancia entre pérdidas	Razón de pérdida de paquetes de vídeo.
3.0	<200	<50	< 16	6 paquetes IP	1 evento de error/hora	< 5.85 E-06
3.75	<200	<50	< 16	7 paquetes IP	1 evento de error/hora	< 5.46 E-06
5.0	<200	<50	< 16	9 paquetes IP	1 evento de error/hora	< 5.26 E-06

⁸² <http://revistas.mes.edu.cu/greenstone/collect/repo/import/repo/20120830/71208073310.pdf>, Capítulo 1. Generalidades del servicio de IPTV y características de las redes que lo soportan.

⁸³ <http://revistas.mes.edu.cu/greenstone/collect/repo/import/repo/20120830/71208073310.pdf>, Capítulo 2. Métricas utilizadas en la validación de la calidad del servicio de IPTV.

ANÁLISIS DE LA TOPOLOGÍA TIPO MALLA:

El primer escenario presentado en este proyecto, es la red de distribución con topología tipo malla:

En esta red se presenta cada una de las configuraciones de los routers al igual que del servidor y de cada uno de los clientes. El objetivo es analizar los cuadros de resultados obtenidos al momento de la difusión del video streaming.

Para el caso de la red de distribución tipo malla tenemos los siguientes resultados:

VELOCIDAD DE TRANSMISIÓN:

TABLA DE VALORES CAPTURADOS				
TOPOLOGÍA:	6 ROUTERS TIPO MALLA			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	11160876,00	11128328,00	11124170,00	162,889
CLIENTE PC5	11105034,00	11072728,00	11068570,00	162,121
CLIENTE PC1	11160876,00	11128328,00	11124170,00	162,889
TABLA DE VELOCIDADES				
	SERVER VLC	CLIENTE PC5	CLIENTE PC1	
VELOCIDAD DE TRANSMISIÓN GENERAL (BYTES/SEG)	68518,29	68498,43	68518,29	
VELOCIDAD DE TRANSMISIÓN PAQUETES IPV6 (BYTES/SEG)	68318,47	68299,16	68318,47	
VELOCIDAD DE TRANSMISIÓN PURAMENTE DATOS UDP (BYTES/SEG)	68292,95	68273,51	68292,95	

Tabla 4.1: Velocidades de transmisión obtenidas en la simulación

Según el documento de respaldo, sugiere que la velocidad mínima de transmisión para un streaming de video en MPG2 debe ser de 2.5 Mbps y en MPG4 debe ser de 1.75 Mbps. En la red tipo malla se tiene una velocidad de 68518.19 Bytes/seg, es decir, 0.548 Mbps

Esto se debe a que para el caso del servidor VLC, se escogió un formato de video H.264 – MP3 (MP4) (como se muestra en la figura 4.1), el cual, el mismo programa implementa una velocidad de transmisión adecuada para que la señal de video sea clara, es decir, el servidor de video VLC proporciona automáticamente la velocidad necesaria para que el paquete de datos llegue a su destino.

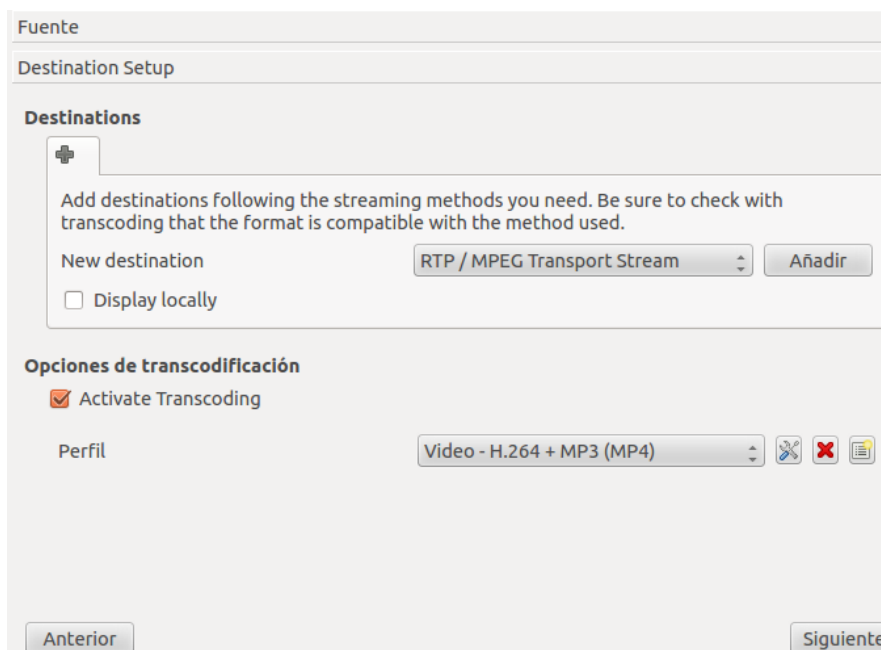


Figura 4.1: Opciones de formato de audio/video en Server VLC.

LATENCIA:

Resumen de los datos obtenidos del retardo o latencia de los paquetes de video enviados a la red, en la topología tipo malla.

RESUMEN	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	443,16	516,23	401,56	499,39
PAQUETES TRANSMITIDOS	150,00	150,00	150,00	150,00
PAQUETES RECIBIDOS	118,00	119,00	121,00	119,00
PAQUETES PERDIDOS	32,00	31,00	29,00	31,00
PORCENTAJE DE PAQUETES PERDIDOS %	21,33	20,67	19,33	20,67
PAQUETE MIN TIEMPO (mseg)	1,08	1,14	1,17	1,34
PAQUETE MAX TIEMPO (mseg)	24,80	33,00	22,60	33,50
PAQUETE TIEMPO PROMEDIO (mseg)	4,04	4,91	3,73	4,35

Tabla 4.2: Resumen del retardo de los paquetes de video enviados a la red.

Los valores recomendados de retardo de extremo a extremo deben ser menores a 200 mseg. En la tabla de resumen de latencias, vemos que el valor de retardo más alto es de 4.91 mseg. Es decir, cumple con los valores recomendados.

Estos valores tan bajos, se deben primeramente a que la red es virtual y no existen elementos externos que afecten al envío de paquetes, es decir, todos los elementos de la red son ideales, por tanto, los valores de retardos son mínimos, ya que todo depende del procesador del host y su velocidad para enviar y recibir los datos.

JITTER

Resumen de los datos obtenidos de la variación del retardo de los paquetes de video enviados a la red, en la topología tipo malla.

	SERVER VLC	CLIENTE PC1	CLIENTE PC5
JITTER MIN (ms)	-22,99	-23,22	-9,98
JITTER MAX (ms)	23,43	23,41	9,9

Tabla 4.3: Resumen de los valores de Jitter.

Los valores recomendados de la variación del retardo (jitter) de extremo a extremo deben ser menores a 50 mseg. En la tabla de resumen de Jitter, vemos que el valor de variación del retardo más alto es de 23.43 mseg. Es decir, cumple con los valores recomendados.

Nuevamente estos valores pequeños de variación del retardo, se deben a las condiciones ideales en las cuales se encuentra esta red de distribución tipo malla en el ambiente GNS3 de simulación.

PÉRDIDA DE PAQUETES:

Resumen de los datos obtenidos de la pérdida de paquetes de video enviados a la red, en la topología tipo malla.

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING			
TOPOLOGIA:	6 ROUTERS TIPO MALLA		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	2 min 42 seg.	2 min 42 seg.	2 min 42 seg.
TIEMPO EN SEGUNDOS:	162.889 seg.	162.121 seg.	162.889 seg.
PAQUETES CAPTURADOS:	8199.00	8156.00	8199.00
PAQUETES MOSTRADOS:	8199.00	8156.00	8199.00
BYTES TOTALES:	11160876.00	11105034.00	11160876.00
PROMEDIO PAQUETES/SEG:	50335.00	50308.00	50335.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.361.248	1.361.578	1.361.248
PROMEDIO BYTES/SEG:	68.518.292	68.498.430	68.518.292
PROMEDIO MBITS/SEG:	0,548	0,548	0,548

Tabla 4.4: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la simulación.

Debido a la red se encuentra en condiciones ideales, se puede observar en la tabla de resumen de la pérdida de paquetes, que la velocidad de transmisión es la misma cuando se envían los paquetes de datos tanto para el Server VLC, cuanto para cada cliente (PC1 y PC5) al momento de la recepción, y además, se observa que la cantidad de paquetes capturados y mostrados son iguales, por tanto, no existe pérdida de paquetes.

En los casos de las redes de distribución tipo Estrella y tipo Híbrido, se obtuvo el mismo resultado que la red tipo malla, es decir:

1. Una velocidad de transmisión promedio similar en los tres casos igual a 0.544 Mbps.
2. Un valor promedio de retardo o latencia menor a 5 mseg. El cual es un valor mucho menor al recomendado.

3. El valor promedio del jitter no supera los 49.62 mseg. El cual está debajo del valor recomendado el cual es 50 mseg. Máximo.
4. No existe pérdida de paquetes, debido a que el ambiente es ideal y no existe condiciones externas que perjudiquen la comunicación.

ANÁLISIS DE CALIDAD DE SERVICIO CUANDO UN ROUTER DE LA RED DEJA DE FUNCIONAR.

En una red de distribución, puede darse el caso que uno de los routers por donde está viajando el streaming de video hacia los diferentes clientes, sufra algún tipo de falla, esta puede ser física o de programación, y por tanto, la transmisión se vea afectada. En este proyecto se contempla este escenario (ver pág. 168), a continuación estos son los resultados.

VELOCIDAD DE TRANSMISIÓN:

TABLA DE VALORES CAPTURADOS				
TOPOLOGIA:	6 ROUTERS TIPO MALLA CON APAGADO DE 1 ROUTER			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	14340945,00	14321952,00	14313826,00	205,626
CLIENTE PC5	11746886,00	11708995,00	11672521,00	205,926
CLIENTE PC1	11751624,00	11729044,00	11720480,00	206,071
TABLA DE VELOCIDADES				
	SERVER VLC	CLIENTE PC5	CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	69742,86	57044,21	57027,06	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	69650,49	56860,21	56917,49	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	69610,97	56683,09	56875,93	

Tabla 4.5: Velocidades de transmisión obtenidas en el laboratorio.

La velocidad de transmisión (a diferencia de los casos anteriores) varía notablemente entre el servidor y cada cliente, el servidor tenemos una velocidad de 69742.86 Bytes/seg. (0.558 Mbps), mientras que en los clientes se tiene una velocidad de 57044.21 Bytes/seg. (0.456 Mbps), esto se debe a que en el momento que dejó de funcionar uno de los routers por donde era enviado el streaming de video, el Server VLC continuó enviando la misma cantidad de paquetes a la misma velocidad sin saber que los receptores no estaban recibiendo los paquetes, es decir la velocidad de transmisión del Servidor VLC siempre fue constante, aun cuando por un momento la red se “cayó”, por otro lado los clientes tuvieron una falla de recepción del video, y debido a la cantidad de paquetes perdidos hasta que la transmisión de video se restablezca por otro camino en la red, dando como resultado una velocidad de transmisión promedio menor en la recepción en comparación al transmisor.

LATENCIA:

Resumen de los datos obtenidos del retardo o latencia de los paquetes de video enviados a la red, en la topología tipo malla cuando un router deja de funcionar:

RESUMEN	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC5
TIEMPO TOTAL (mseg)	7663,44	7222,96	6009,33	6283,63
PAQUETES TRANSMITIDOS	150,00	150,00	150,00	150,00
PAQUETES RECIBIDOS	134,00	135,00	135,00	134,00
PAQUETES PERDIDOS	16,00	15,00	15,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,00	10,00	10,67
PAQUETE MIN TIEMPO (mseg)	0,79	1,05	0,80	0,80
PAQUETE MAX TIEMPO (mseg)	1034,00	1058,00	1035,00	682,00
PAQUETE TIEMPO PROMEDIO (mseg)	56,51	53,50	44,51	46,90

Tabla 4.6: Resumen del retardo de los paquetes de video enviados a la red.

En comparación a los casos anteriores, en esta tabla se puede ver claramente que los retardos son significativamente mayores (10 veces más), esto se debe a la pérdida de paquetes debido al corte de la señal de video, sin embargo, salvo por el momento de corte total de la señal, una vez restablecida la transmisión, la latencia vuelve a ser mucho menor a la recomendada.

JITTER

Resumen de los datos obtenidos de la variación del retardo de los paquetes de video enviados a la red, en la topología tipo malla cuando un router deja de funcionar:

	SERVER VLC	CLIENTE PC1	CLIENTE PC5
JITTER MIN (ms)	-974	-199,3	-287
JITTER MAX (ms)	636	1000,6	305,6

Tabla 4.7: Resumen de los valores de Jitter.

La variación del retardo también se incrementa considerablemente, esto se debe a que al momento del corte de señal, el tiempo entre el último paquete recibido por los clientes y el nuevo paquete recibido después de restablecer la señal, fueron varios segundos (cálculo presentado a continuación en pérdida de paquetes).

Observando únicamente los valores expuestos en la tabla, se podría concluir que la variación del retardo en los paquetes transmitidos, sufre una demora excesivamente grande durante toda la transmisión, sin embargo, en la práctica sabemos, que lo que sucedió, fue que existió un tiempo de corte de la señal, donde no se recibió ningún paquete en el cliente hasta que se encontró un nuevo camino de ruta de la transmisión y luego de ese corte la señal continuó receptándose con normalidad.

Para ilustrar esta explicación tenemos la figura 4.2, donde se observa claramente que los paquetes viajan normalmente hasta un cierto tiempo, luego la transmisión cae totalmente, hasta que la red encuentra otra ruta de transmisión y los paquetes vuelven a ser receptados con normalidad.

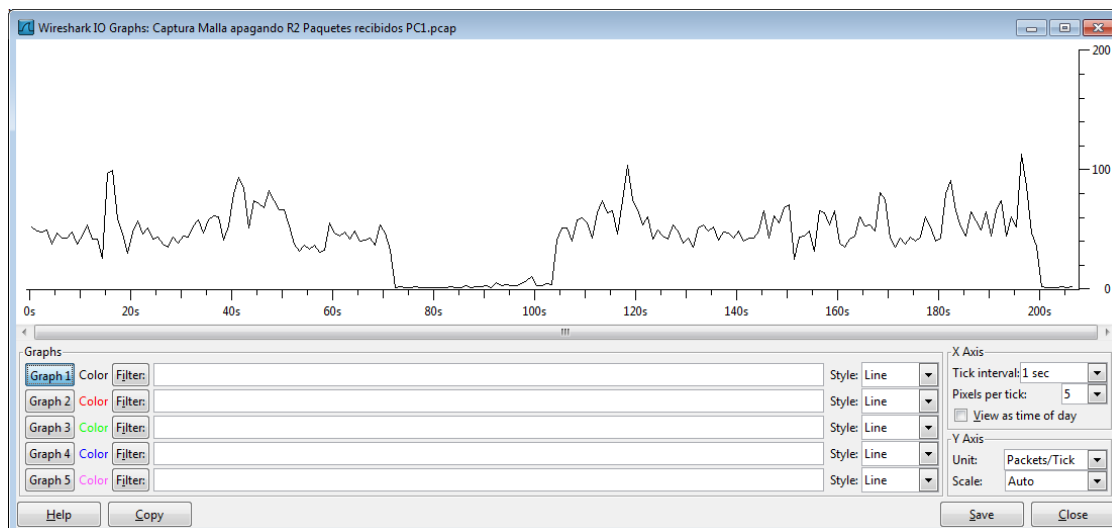


Figura 4.2: Gráfico de los datos obtenidos en la captura de los paquetes durante la transmisión del streaming de video.

PÉRDIDA DE PAQUETES:

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISIÓN DE VIDEO STREAMING			
TOPOLOGÍA:	6 ROUTERS TIPO MALLA CON APAGADO DE 1 ROUTER		
RESUMEN GENERAL			
PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R5	Fastethernet R3
TIEMPO DE CAPTURA DE PAQUETES:	3 min 25 seg.	3 min 26 seg.	3 min 26 seg.
TIEMPO EN SEGUNDOS:	205.626 seg.	205.926 seg.	206.071 seg.
PAQUETES CAPTURADOS:	10602.00	8714.00	8725.00
PAQUETES MOSTRADOS:	10602.00	8714.00	8725.00
BYTES TOTALES:	14340945.00	11746886.00	11751624.00
PROMEDIO PAQUETES/SEG:	51560.00	42350.00	42340.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.352.664	1.347.986	1.346.891
PROMEDIO BYTES/SEG:	69.742.858	57.044.210	57.027.064
PROMEDIO MBITS/SEG:	0,558	0,456	0,456

Tabla 4.8: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la simulación.

En la tabla 4.8, podemos observar, que a diferencia de las tablas de las prácticas anteriores, existen pérdidas de paquetes, debido a la interrupción del camino trazado previamente por los paquetes de streaming de video.

Vemos que entre los Clientes PC1 y PC5, existe prácticamente la misma cantidad de paquetes recibidos en el mismo con una velocidad de transmisión iguales en ambos casos.

Para el caso del Server VLC, podemos observar claramente que éste envió mucho más paquetes de los que los clientes PC1 y PC5 pudieron receptor, esta pérdida de paquetes se produjo al momento de apagar el Router R2, lo cual produjo que la red vuelva a calcular una nueva ruta para el envío de paquetes, mientras tanto los paquetes que el Servidor VLC se encontraba enviando, eran descartados por la red.

En resumen, El Server VLC envió mucha más cantidad de paquetes a la red en el mismo tiempo de transmisión del video streaming, lo cual da como velocidad de transmisión promedio de 0.558 Mbits/seg. Para los clientes PC1 y PC5 si bien el tiempo de recepción de video streaming fue el mismo, la cantidad de paquetes fue menor, dando como resultado una velocidad de transmisión promedio de 0.456 Mbits/seg.

Es decir, la cantidad de pérdida de paquetes es:

PC:	SERVER VLC	CLIENTE PC5	CLIENTE PC1
PAQUETES CAPTURADOS:	10602,00	8714,00	8725,00
BYTES TOTALES:	14340945	11746886	11751624
BYTES PERDIDOS:	0	2594059	2589321
PERDIDA DE PAQUETES:	0	1888,00	1877,00

Tabla 4.9: Valores de paquetes perdidos.

A la vista del Usuario, esta pérdida de paquetes se puede resumir en:

- La señal de video streaming se interrumpe al 1min 1 seg. empezado la trasmisión.
- La pantalla queda congelada con la última imagen captada por el usuario.
- Luego de un tiempo igual a:

$$\text{Velocidad de Transmisión} = \frac{\text{Bytes Totales}}{\text{Tiempo de la Transferencia}}$$

$$\text{Tiempo de la transferencia} = \frac{\text{Bytes Totales}}{\text{Velocidad de Transmisión}}$$

$$\text{Tiempo de la transferencia} = \frac{2594059 \text{ Bytes}}{0.456 \frac{\text{Mbits}}{\text{seg}}}$$

$$\text{Tiempo de restauracion de la señal} = \frac{2594059.00 \text{ Bytes}}{0.456 \frac{\text{Mbits}}{\text{seg}}}$$

$$\text{Tiempo de restauracion de la señal} = \frac{2594059.00 \text{ Bytes}}{57027.064 \frac{\text{Bytes}}{\text{seg}}}$$

$$\text{Tiempo de restauracion de la señal} = \frac{2594059.00 \text{ Bytes}}{57027.064 \frac{\text{Bytes}}{\text{seg}}}$$

$$\text{Tiempo de restauracion de la señal} = 45.49 \text{ seg.}$$

El cliente vuelve a captar la señal del streaming de video, luego de un tiempo aproximado de 45.49 seg.

Los paquetes que se perdieron durante el corte de la señal serían:

TAMAÑO PROMEDIO PAQUETE (BYTES):	1.346,89
BYTES TOTALES PERDIDOS	2.594.059,00
PAQUETES PERDIDOS DURANTE CORTE DE SEÑAL	1.925,96

T

Tabla 4.10: Paquetes perdidos durante el corte de señal.

Por supuesto, para el usuario va a ser bastante molesto el hecho que se haya detenido la señal por tanto tiempo, sin embargo, el sistema una vez superado el inconveniente de crear nuevos caminos durante la transmisión de un video streaming, continúa receptando la señal sin problemas y sin pérdida de paquetes.

COMPARACIÓN ENTRE EL PROTOTIPO Y LA SIMULACIÓN

Para validar los datos aquí presentados, es necesario comparar los datos obtenidos en la simulación con los datos obtenidos en el laboratorio, a continuación se presenta los datos obtenidos:

VELOCIDAD DE TRANSMISIÓN VIRTUAL (SIMULACIÓN):

TABLA DE VALORES CAPTURADOS				
TOPOLOGÍA:	2 ROUTERS PROTOTIPO VIRTUAL			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	35331010,00	35320498,00	35309016,00	227,205
CLIENTE PC1	35202352,00	35191210,00	35179510,00	226,792
TABLA DE VELOCIDADES				
	SERVER VLC		CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	155502,78		155218,67	
VELOCIDAD DE TRANSMISION PAQUETES IPv6 (BYTES/SEG)	155456,52		155169,54	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	155405,98		155117,95	

Tabla 4.11: Velocidades de transmisión obtenidas en la simulación.

VELOCIDAD DE TRANSMISIÓN REAL (PROTOTIPO):

TABLA DE VALORES CAPTURADOS				
TOPOLOGÍA:	2 ROUTERS PROTOTIPO REAL			
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	13643698,00	13622677,00	13606568,00	222,992
CLIENTE PC1	13606804,00	13603800,00	13599760,00	226,218
TABLA DE VELOCIDADES				
	SERVER VLC		CLIENTE PC1	
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	61184,70		60149,08	
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	61090,43		60135,80	
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	61018,19		60117,94	

Tabla 4.12: Velocidades de transmisión obtenidas en el laboratorio.

A continuación una tabla comparativa de las velocidades de transmisión:

TABLA COMPARATIVA DE VELOCIDADES DE TRANSMISION				
	PROTOTIPO VIRTUAL		PROTOTIPO REAL	
	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC1
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)	155502,78	155218,67	61184,7	60149,08
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)	155456,52	155169,54	61090,43	60135,8
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)	155405,98	155117,95	61018,19	60117,94

Tabla 4.13: Velocidades de transmisión en Bytes/seg.

Expresado en Mbps tenemos:

TABLA COMPARATIVA DE VELOCIDADES DE TRANSMISION				
	PROTOTIPO VIRTUAL		PROTOTIPO REAL	
	SERVER VLC	CLIENTE PC1	SERVER VLC	CLIENTE PC1
VELOCIDAD DE TRANSMISION GENERAL (Mbps)	1,244	1,242	0,489	0,481
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (Mbps)	1,244	1,241	0,489	0,481
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (Mbps)	1,243	1,241	0,488	0,481

Tabla 4.14: Velocidades de transmisión en Mbps.

Por tanto, tenemos que para la red virtual, la velocidad de transmisión supera en 2.5 veces a la velocidad de transmisión del prototipo real, esto se debe a que en la red virtual, todos los elementos de la misma son ideales, es decir, las condiciones para la transmisión de datos son excelentes, mientras que en el prototipo real, se debe superar varios factores inherentes a los dispositivos físicos, tales como:

- Estado de los routers (estado de los puertos fastethernet y seriales, conexiones eléctricas, cables de energía en óptimas condiciones, sistema de puesta a tierra adecuados, tiempo de uso del router y estado actual de las tarjetas internas, etc.).
- Estado de las tarjetas de red del servidor y los clientes (velocidades de transmisión, tiempo de uso, configuración, etc.)
- Patch core en buen estado (correctamente ponchados)
- Cables seriales (correctamente armados e instalados)

Todos estos elementos hacen que la velocidad de transmisión disminuya a medida que vaya sobrepasando cada dispositivo de la red.

Por tanto aquí podemos ver, las velocidades en condiciones ideales y en condiciones reales para este tipo de red, esto implica, que si tenemos dispositivos cada vez mejores para nuestra red, la velocidad de transmisión máxima que podríamos alcanzar, sería la misma velocidad que se genera en el ambiente virtual.

LATENCIA:

A continuación la comparación de los retardos para ambos casos:

LATENCIA PROTOTIPO VIRTUAL:

RESUMEN	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	229,43	220,09
PAQUETES TRANSMITIDOS	150,00	150,00
PAQUETES RECIBIDOS	134,00	134,00
PAQUETES PERDIDOS	16,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,67
PAQUETE MIN TIEMPO (mseg)	0,21	0,24
PAQUETE MAX TIEMPO (mseg)	34,80	28,90
PAQUETE TIEMPO PROMEDIO (mseg)	1,71	1,64

Tabla 4.15: Comparación de los valores de tiempos de retardo en la simulación.

LATENCIA PROTOTIPO REAL:

RESUMEN	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	290,63	302,15
PAQUETES TRANSMITIDOS	150,00	150,00
PAQUETES RECIBIDOS	134,00	134,00
PAQUETES PERDIDOS	16,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,67
PAQUETE MIN TIEMPO (mseg)	1,95	1,68
PAQUETE MAX TIEMPO (mseg)	3,03	2,90
PAQUETE TIEMPO PROMEDIO (mseg)	2,17	2,25

Tabla 4.16: Comparación de los valores de tiempos de retardo en el laboratorio.

TABLA COMPARATIVA DE RETARDOS ENTRE LA RED VIRTUAL Y REAL:

RESUMEN	SERVER VLC	CLIENTE PC1
PAQUETE TIEMPO PROMEDIO PROTOTIPO VIRTUAL(mseg)	1,71	1,64
PAQUETE TIEMPO PROMEDIO PROTOTIPO REAL(mseg)	2,17	2,25
TIEMPO DE DIFERENCIA (mseg)	0,46	0,61

Tabla 4.17: Comparación de los valores de tiempos de retardo entre la red virtual y real.

La diferencia de retardo de un paquete entre la red virtual y la real, es la mitad de 1mseg, esta diferencia se debe nuevamente a los factores físicos involucrados en la red.

JITTER

JITTER PROTOTIPO VIRTUAL:

	SERVER VLC	CLIENTE PC1
JITTER MIN (ms)	-5,55	-3,70
JITTER MAX (ms)	5,57	3,30

Tabla 4.17: Valores de Jitter obtenidos en la simulación.

JITTER PROTOTIPO REAL:

	SERVER VLC	CLIENTE PC1
JITTER MIN (ms)	-1,03	-0,63
JITTER MAX (ms)	1,02	0,57

Tabla 4.18: Valores de Jitter obtenidos en el laboratorio.

Si bien, la velocidad de transmisión es mayor en el ambiente virtual y el retardo es menor, cuando comparamos el Jitter, podemos ver que la variación del retardo es menor en el ambiente real, esto se debe a que a menor velocidad de transmisión, los paquetes van a través de la red de una manera más nivelada, por tanto la variación del retardo es mínima.

PÉRDIDA DE PAQUETES:**PÉRDIDA DE PAQUETES PROTOTIPO VIRTUAL:**

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING		
TOPOLOGÍA:	2 ROUTERS PROTOTIPO VIRTUAL	
RESUMEN GENERAL		
PC:	SERVER VLC	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R1
TIEMPO DE CAPTURA DE PAQUETES:	3 min 47 seg.	3 min 46 seg.
TIEMPO EN SEGUNDOS:	227.205 seg.	226.792 seg.
PAQUETES CAPTURADOS:	25605.00	25479.00
PAQUETES MOSTRADOS:	25605.00	25479.00
BYTES TOTALES:	35331010.00	35202352.00
PROMEDIO PAQUETES/SEG:	112696.00	112345.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.379.848	1.381.622
PROMEDIO BYTES/SEG:	155.502.784	155.218.667
PROMEDIO MBITS/SEG:	1.244	1.242

Tabla 4.20: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la simulación.

La pérdida de paquetes que se produce en el transcurso de los paquetes que se envía por la red de extremo a extremo, es mínima, para calcular dicha pérdida tenemos:

Tenemos el número de Bytes totales y la velocidad de transmisión tanto en el emisor como en el receptor, por tanto para calcular los paquetes perdidos, vamos a tomar estos datos pero igualándolos al mismo tiempo , y al final una resta simple nos ayudara a saber el número de paquetea perdidos en el mismo periodo de tiempo.

$$Velocidad\ de\ Transmisión = \frac{Bytes\ Totales}{Tiempo\ de\ la\ Transferencia}$$

*Bytes totales = Tiempo de la Transferencia * Velocidad de Transmisión*

$$\text{Bytes totales} = 226.792 \text{ (seg)} * 1.244 \text{ (Mbps)}$$

$$\text{Bytes totales} = 226.792 \text{ (seg)} * 155500 \text{ (Bytes/seg)}$$

$$\text{Bytes totales} = \mathbf{35266156.00 \text{ Bytes}}$$

La cantidad bytes totales que el servidor VLC transmitió hacia el cliente, en un periodo de tiempo de 3 min 46 seg. (226.792 seg.) es de **35266156 Bytes** y cantidad bytes totales que el Cliente PC1 recibió, en el mismo periodo de tiempo de 3 min 46 seg. (226.792 seg.) es de **35202352 Bytes**.

Por tanto la cantidad de Bytes perdidos son:

$$\text{Bytes perdidos} = \text{Bytes emitidos} - \text{Bytes recibidos}$$

$$\text{Bytes perdidos} = 35266156 \text{ Bytes} - 35202352 \text{ Bytes}$$

$$\text{Bytes perdidos} = \mathbf{63804.00 \text{ Bytes}}$$

Y el número de paquetes perdidos son:

$$\text{Paquetes perdidos} = \frac{\text{Bytes perdidos}}{\text{Tamaño paquetes promedio}}$$

$$\text{Paquetes perdidos} = \frac{63804.00}{1381.622}$$

$$\text{Paquetes perdidos} = \mathbf{46.18 = 47 \text{ Paquetes}}$$

El número de paquetes perdidos es de 47 frente a un flujo total de 25605 paquetes durante toda la transmisión, es decir la tasa de pérdida es 1.83 E-3, lo cual está muy por encima de la recomendación la cual es 5.85 E -6.

PÉRDIDA DE PAQUETES PROTOTIPO REAL:

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA		
TRANSMISION DE VIDEO STREAMING		
TOPOLOGIA:	2 ROUTERS PROTOTIPO	
RESUMEN GENERAL		
PC:	SERVER VLC	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	3 min 42 seg.	3 min 46 seg.
TIEMPO EN SEGUNDOS:	222.992 seg.	226.218 seg.
PAQUETES CAPTURADOS:	10044.00	9848.00
PAQUETES MOSTRADOS:	10044.00	9848.00
BYTES TOTALES:	13643698.00	13606804.00
PROMEDIO PAQUETES/SEG:	45042.00	43533.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	1.358.393	1.381.682
PROMEDIO BYTES/SEG:	61.184.663	60.149.102
PROMEDIO MBITS/SEG:	0,489	0,481

Tabla 4.21: Tabla comparativa de valores obtenidos en la transmisión de video streaming en el laboratorio.

Para el cálculo de la pérdida de paquetes haremos el mismo procedimiento anterior:

$$Velocidad\ de\ Transmisión = \frac{Bytes\ Totales}{Tiempo\ de\ la\ Transferencia}$$

$$Bytes\ totales = Tiempo\ de\ la\ Transferencia * Velocidad\ de\ Transmisión$$

$$Bytes\ totales = 222.992\ (seg) * 0.481\ (Mbps)$$

$$Bytes\ totales = 222.992\ (seg) * 60149.102\ (Bytes/seg)$$

$$Bytes\ totales = 13412769\ Bytes$$

La cantidad bytes totales que el servidor VLC transmitió hacia el cliente, en un periodo de tiempo de 3 min 42 seg. (222.992 seg.) es de **13643698 Bytes** y cantidad bytes totales que el Cliente PC1 recibió, en el mismo periodo de tiempo de 3 min 42 seg. (222.992 seg.) es de **13412769 Bytes**.

Por tanto la cantidad de Bytes perdidos son:

$$\text{Bytes perdidos} = \text{Bytes emitidos} - \text{Bytes receptados}$$

$$\text{Bytes perdidos} = 13643698 \text{ Bytes} - 13412769 \text{ Bytes}$$

$$\text{Bytes perdidos} = \mathbf{230930 \text{ Bytes}}$$

Y el número de paquetes perdidos son:

$$\text{Paquetes perdidos} = \frac{\text{Bytes perdidos}}{\text{Tamaño paquetes promedio}}$$

$$\text{Paquetes perdidos} = \frac{230930.00}{1358.393}$$

$$\text{Paquetes perdidos} = \mathbf{170 \text{ Paquetes}}$$

El número de paquetes perdidos es de 170 frente a un flujo total de 10044 paquetes durante toda la transmisión, es decir la tasa de pérdida es 1.69 E-2, lo cual está muy por encima de la recomendación la cual es 5.85 E -6.

DENEGACIÓN DE SERVICIO:

El objetivo de esta práctica es crear una red con un flujo continuo de paquetes que no son datos del streaming de video, es decir, inundar la red con otro tipo de paquetes y ver el comportamiento de la misma.

Para crear pérdidas de paquetes se implementó un programa de denegación de servicio, el cual, saturaba la red con paquetes diferentes al streaming de video, se eligió el programa SCAPY para este fin y mediante el envío infinitos de paquetes SYN a la red, se observó una muy ligera pérdida de paquetes, a continuación los resultados:

Ambos tipos de paquetes (paquetes UDP del streaming de video y paquetes SYNC para inundar la red), fueron generados desde el Servidor VLC, en este caso no existió corte de la señal de video, sin embargo, para el cliente existieron algunas anomalías presentadas durante la transmisión:

- Retrasos en la recepción del video
- Corte momentáneo de la señal de video.
- Desfase del audio y video.
- Saltos de escenas del video

Para aclarar porque suceden estas anomalías es necesario analizar cada uno de los parámetros de calidad:

VELOCIDAD DE TRANSMISIÓN:

TABLA DE VALORES CAPTURADOS					
TOPOLOGÍA:	2 ROUTERS DENEGACION DE SERVICIO				
	BYTES TOTALES	PAQUETES IPV6 BYTES	PAQUETES TCP BYTES	PAQUETES UDP BYTES	SEGUNDOS
SERVER VLC	32484409,00	32457079,00	11512386,00	20929179,00	237,713
CLIENTE PC1	27318530,00	27289387,00	9526294,00	17731802,00	247,292
TABLA DE VELOCIDADES					
				SERVER VLC	CLIENTE PC1
VELOCIDAD DE TRANSMISION GENERAL (BYTES/SEG)				136653,90	110470,74
VELOCIDAD DE TRANSMISION PAQUETES IPV6 (BYTES/SEG)				136538,93	110352,89
VELOCIDAD DE TRANSMISION PURAMENTE DATOS TCP (BYTES/SEG)				48429,77	38522,45
VELOCIDAD DE TRANSMISION PURAMENTE DATOS UDP (BYTES/SEG)				88043,90	71703,90

Tabla 4.22: Velocidades de transmisión obtenidas en la simulación.

Se debe tomar en cuenta, que el Servidor envía los paquetes TCP y UDP a la red a una velocidad de: 136653.9 Bytes/seg, es decir, 1.093 Mbps, pero únicamente los paquetes UDP que son los paquetes de video streaming, se transmiten a una velocidad de: 88043.90 Bytes/seg, es decir, 0.705 Mbps.

Esta velocidad de transmisión de 0.705 Mbps, es similar a las velocidades presentadas anteriormente en las topologías tipo malla, estrella e híbrido, lo que quiere decir, que la velocidad de transmisión de los paquetes de video streaming es la misma a pesar que por la red pasan otro tipo de paquetes.

LATENCIA:

RESUMEN	SERVER VLC	CLIENTE PC1
TIEMPO TOTAL (mseg)	168,46	141,04
PAQUETES TRANSMITIDOS	150,00	150,00
PAQUETES RECIBIDOS	134,00	134,00
PAQUETES PERDIDOS	16,00	16,00
PORCENTAJE DE PAQUETES PERDIDOS %	10,67	10,67
PAQUETE MIN TIEMPO (mseg)	0,29	0,24
PAQUETE MAX TIEMPO (mseg)	11,60	6,05
PAQUETE TIEMPO PROMEDIO (mseg)	1,26	1,05

Tabla 4.23: Resumen del retardo de los paquetes de video enviados a la red.

Los valores de retardo para todos los paquetes (TCP y UDP) son mínimos, es decir no existe problemas en los tiempos de envío de paquetes.

JITTER:

	SERVER VLC	CLIENTE PC1
JITTER MIN (ms)	-8,67	-5,33
JITTER MAX (ms)	10,84	5,33

Tabla 4.24: Valores de Jitter obtenidos en la simulación.

La variación del retardo o Jitter, tienen valores menores a 10.84 mseg los cuales son valores muy por debajo de los recomendados (valores menores a 50 mseg),

por tanto, no existe ningún problema de tiempo entre la llegada de un paquete y el siguiente.

PÉRDIDA DE PAQUETES:

TABLA COMPARATIVA DE VALORES OBTENIDOS EN LA TRANSMISION DE VIDEO STREAMING		
TOPOLOGIA:	2 ROUTERS CON DENEGACION DE SERVICIO	
RESUMEN GENERAL		
PC:	SERVER VLC	CLIENTE PC1
INTERFACE:	Fastethernet R1	Fastethernet R2
TIEMPO DE CAPTURA DE PAQUETES:	3 min 57 seg.	4 min 07 seg.
TIEMPO EN SEGUNDOS:	237.713 seg.	247.292 seg.
PAQUETES CAPTURADOS:	160198.00	133996.00
PAQUETES MOSTRADOS:	160198.00	133996.00
BYTES TOTALES:	32484409.00	27318530.00
PROMEDIO PAQUETES/SEG:	673912.00	541.854.00
TAMAÑO PROMEDIO PAQUETE (BYTES):	202.777	203.876
PROMEDIO BYTES/SEG:	136.653.671	110.470.936
PROMEDIO MBITS/SEG:	1.093	0.884

Tabla 4.25: Tabla comparativa de valores obtenidos en la transmisión de video streaming en la simulación.

En el cuadro se puede apreciar que existe una cantidad considerable de pérdida de paquetes, a continuación los cálculos:

$$Velocidad\ de\ Transmisión = \frac{Bytes\ Totales}{Tiempo\ de\ la\ Transferencia}$$

$$Bytes\ totales = Tiempo\ de\ la\ Transferencia * Velocidad\ de\ Transmisión$$

$$Bytes\ totales = 237.713(seg) * 0.884 (Mbps)$$

$$Bytes\ totales = 237.713(seg) * 110470.936 (Bytes/seg)$$

$$Bytes\ totales = 26260378 Bytes$$

La cantidad bytes totales que el servidor VLC transmitió hacia el cliente, en un periodo de tiempo de 3 min 57 seg. (237.713 seg.) es de **32484409 Bytes** y cantidad bytes totales que el Cliente PC1 recibió, en el mismo periodo de tiempo de 3 min 57 seg. (222.992 seg.) es de **26260378 Bytes**.

Por tanto la cantidad de Bytes perdidos son:

$$\text{Bytes perdidos} = \text{Bytes emitidos} - \text{Bytes receptados}$$

$$\text{Bytes perdidos} = 32484409 \text{ Bytes} - 26260378 \text{ Bytes}$$

$$\text{Bytes perdidos} = \mathbf{6224032 \text{ Bytes}}$$

Y el número de paquetes perdidos son:

$$\text{Paquetes perdidos} = \frac{\text{Bytes perdidos}}{\text{Tamaño paquetes promedio}}$$

$$\text{Paquetes perdidos} = \frac{6224032.00}{203.876}$$

$$\text{Paquetes perdidos} = \mathbf{30528 \text{ Paquetes}}$$

El número de paquetes perdidos es de 30528 frente a un flujo total de 160198 paquetes durante toda la transmisión, es decir la tasa de pérdida es 1.9 E-1, lo cual está muy por encima de la recomendación la cual es 5.85 E -6.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Para este proyecto se utilizó 2 tipos de sistema operativo, como son WINDOWS y LINUX, con el fin de integrar los dos sistemas operativos más usados a nivel de comunicaciones.

Se utilizó un sistema operativo tipo Windows para alojar al programa GNS3, el cual es la base de este proyecto, por varias razones:

- Según pruebas del Simulador GNS3 realizadas en los sistemas Windows y Linux, Windows proporciona un mejor rendimiento, a pesar que no es muy significativo⁸⁴.
- Facilidad de instalación en comparación con LINUX, ya que existe un paquete completo para sistema Windows, mientras que para Linux es necesario agregar varias librerías extras dependiendo de la distribución que se trabaje.

GNS3 es una herramienta muy valiosa para los ingenieros en redes de comunicaciones, ya que con poco presupuesto y herramientas, se pueden construir redes de cualquier magnitud, limitado únicamente por las capacidades físicas del host donde funciona el programa (memoria RAM, disco duro, puertos Ethernet, etc.).

Wireshark fue el programa analizador de red escogido, es de fácil instalación y manejo, con un ambiente gráfico muy intuitivo. Dentro de su paquete de programación, se encuentran varias herramientas para el análisis de los parámetros de calidad de una red, sean estos de voz, video o datos.

Los cálculos de los parámetros de calidad en cada una de las simulaciones arrojan las siguientes conclusiones:

⁸⁴ <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>

- La simulación en el ambiente virtual GNS3 y el prototipo implementado en el laboratorio de la facultad, muestran que los valores obtenidos finalmente son muy similares, es decir, el simulador GNS3 es una herramienta VÁLIDA COMPROBADA, cuando se desee diseñar e implementar redes de cualquier magnitud, ya que físicamente para muchas personas no sería posible adquirir los equipos físicos, con el GNS3 es posible aumentar la capacidad del host y tener un número ilimitado de dispositivos de red, con la seguridad que al momento de implementarlo físicamente, la variación de los resultados no serán significativos y únicamente se deberán a los parámetros propios del cambio entre ambiente virtual y físico.
- Como este proyecto fue realizado en un ambiente puramente virtual, se puede concluir que no existe pérdida de paquetes al momento de la transmisión del streaming de video en ninguna de las topologías aquí presentadas, por tanto, fue necesario crear las condiciones que permitan pérdida de paquetes intencionalmente.
- El programa de simulación GNS3 es una herramienta muy útil para probar una red de cualquier tipo, limitado únicamente por la capacidad de procesamiento del host donde se encuentra instalado.
- A pesar que se utilizó el programa de denegación de servicio SCAPY para lograr pérdida de paquetes, la red continuó enviando y recibiendo los datos del streaming de video sin mayor inconveniente, es decir, a pesar que la red estaba invadida de paquetes extraños al video, el cliente recibió los datos con normalidad.

Para el ambiente creado con denegación de servicio, se encontraron varios puntos importantes:

- La velocidad de transmisión se duplicó en relación a las velocidades mostradas en las topologías anteriores, esto se debe a que tanto el Servidor como el Cliente, tuvieron que procesar mucha más información en el mismo tiempo.
- Los retardos o latencia en la red, fueron muy similares a las topologías anteriores, es decir, a pesar de la gran cantidad de paquetes circulando

desde el servidor hacia el cliente, los paquetes llegaban a su destino con un retardo no mayor al esperado.

- La variación del retardo también fue lo esperado, no existió una variación mayor a 10.84 mseg lo cual indica que el retardo entre paquetes fue normal.
- A pesar que los parámetros de: velocidad de transmisión, latencia y Jitter, fueron los esperados y permitieron una transmisión exitosa, tenemos un gran problema en el último parámetro, el cual es, la pérdida de paquetes, ya que se puede observar que existe una pérdida significativa de paquetes, esto se debe a que la red estuvo inundada de paquetes “basura” que no tienen nada que ver con el streaming de video y el buffer de los Switchs no fueron suficientes para almacenar tanta información.
- A pesar de la enorme pérdida de paquetes, en la simulación se pudo observar que la señal de video se recibía con normalidad en el cliente PC1, es decir, a pesar de la inundación de paquetes SYN la señal no variaba, lo que significa que los paquetes descartados por los Switchs cuando el buffer excedía su capacidad, eran paquetes SYN, los cuales al ser descartados no influyeron en la calidad de la transmisión de video.

BIBLIOGRAFÍA

- [1] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pag.1-
- [2] <http://www.publicaciones.urbe.edu/index.php/telematique/article/viewFile/766/1843>
- [3] http://www.6sos.org/lista_faqs.php#faq4
- [4] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pag.5-
- [5] <http://www.rau.edu.uy/IPv6/queesIPv6.htm>
- [6] <http://docs.oracle.com/cd/E19957-01/820-2981/IPv6-ref-2/index.html>
- [7] <http://docs.oracle.com/cd/E19957-01/820-2981/IPv6-ref-2/index.html>
- [8] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf>
- [9] <http://ipv4to6.blogspot.com/p/tipos-de-direcciones-IPv6-unicast.html>
- [10] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 15-
- [11] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 16-
- [12] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 16-
- [13] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 17-
- [14] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 17-
- [15] <http://ipv4to6.blogspot.com/p/tipos-de-direcciones-IPv6-multicast.html>
- [16] http://lacnic.net/documentos/lacnicx/introduccion_IPv6_v11.pdf -pág. 29-
- [17] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 18-
- [18] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> –pág. 19-
- [19] <http://www.rau.edu.uy/IPv6/queesIPv6.htm>

- [20] http://lacnic.net/documentos/lacnicx/introduccion_IPv6_v11.pdf -pág. 30-
- [21] http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/Walc2011-Consulintel_IPv6_ES_ROUTING_CHOF.pdf -pág. 7-
- [22] <http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf> -pág. 38-
- [23] http://cs.mty.itesm.mx/lab/redes2/IPv6/P6_IPv6_RIPng.pdf
- [24] http://cs.mty.itesm.mx/lab/redes2/IPv6/P7_IPv6_EIGRP.pdf
- [25] http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/Walc2011-Consulintel_IPv6_ES_ROUTING_CHOF.pdf -pág. 13-
- [26] <http://www.simulationexams.com/tutorials/ccna/ospf-routing-fundamentals.htm>
- [27] http://www.6deploy.org/workshops2/20111010_guayaquil_ecuador/Walc2011-Consulintel_IPv6_ES_ROUTING_CHOF.pdf -pág. 15-
- [28] <http://www.labs.lacnic.net/drupal/sites/default/files/ospf-isis-IPv6.pdf>
- [29] http://www.6deploy.eu/workshops2/20121015_panama_panama/DIA2-1-Consulintel_Curso-IPv6_WALC2012.pdf
- [30] http://www.net130.com/CMS/Pub/network/network_protocol/2005_08_21_36977_3.htm
- [31] http://eprints.ucm.es/10051/1/PROYECTO_MII_TREJO.pdf -pág. 28-
- [32] http://www.6deploy.org/workshops/20101011_santa_cruz_bolivia/multicast-IPv6-walc.pdf -pág. 28-
- [33] http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf -pág. 34-
- [34] http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA5-1-6-Consulintel_Curso-IPv6_WALC2011.pdf
- [35] http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf -pág. 38-
- [36] http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf -pág. 39-
- [37] http://lacnic.net/documentos/lacnicxii/presentaciones/flip6/05_Jordi.pdf
- [38] http://translate.google.com.ec/translate?hl=es&sl=en&u=http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/whitepaper_c11-

- 508498.html&prev=/search%3Fq%3DEmbedded-RP%26sa%3DX%26tbas%3D0%26biw%3D1360%26bih%3D678
- [39] http://www.6deploy.org/workshops/20101011_santa_cruz_bolivia/multicast-IPv6-walc.pdf
- [40] http://www.cs.buap.mx/~iolmos/redes/3_Rendimiento.pdf -pág. 1-
- [41] http://www.cs.buap.mx/~iolmos/redes/3_Rendimiento.pdf -pág. 2-
- [42] http://www.cs.buap.mx/~iolmos/redes/3_Rendimiento.pdf -pág. 4-
- [43] http://www.eetimes.com/document.asp?doc_id=1277196
- [44] <http://primeraunidad-multimedia.blogspot.com/2009/09/retardo-jitter-latencia.html>
- [45] http://noisecom.com/~media/Noisecom/Manuals%20and%20Software/WTG_Intro_to_%20Jitter_SP.ashx
- [46] <http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones3.shtml#ixzz2fHLRWaKk>
- [47] <http://www.monografias.com/trabajos33/telecomunicaciones/telecomunicaciones3.shtml#ixzz2fHLRWaKk>
- [48] <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>
- [49] <http://www.ecured.cu/index.php/IPTV>
- [50] http://www.scielo.org.co/scielo.php?pid=S0123-921X2011000100010&script=sci_arttext
- [51] http://aat.inictel-uni.edu.pe/files/AAT-03_Sistema_IPTV_para_Investigacion.pdf
- [52] <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>
- [53] <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>
- [54] <http://www.idolamedia.com/documentos/estudio-IPTV.pdf>
- [55] <http://www.idolamedia.com/documentos/estudio-IPTV.pdf>
- [56] http://www.scielo.org.co/scielo.php?pid=S0123-921X2011000100010&script=sci_arttext
- [57] <http://www.tmbroadcast.es/index.php/conceptos-generales-de-IPTV/>
- [58] http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf
- [59] <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>

- [60] http://upcommons.upc.edu/pfc/bitstream/2099.1/9989/1/PFC_Lisset_D%C3%ADaz.pdf
- [61] <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>
- [62] http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf
- [63] http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf
- [64] <http://jorgedenovasri.files.wordpress.com/2012/09/gns3.pdf>
- [65] http://dymyt.files.wordpress.com/2012/01/gns3-0-4-1_documentation_spanish.pdf
- [66] <http://seguridadyredes.wordpress.com/2008/02/14/analisis-de-red-con-wireshark-interpretando-los-datos/>
- [67] www.inteco.es/file/5j9r8LaoJvwuB2ZrJ-XI7g
- [68] http://es.wikipedia.org/wiki/Paquete_de_datos
- [69] http://es.wikipedia.org/wiki/Red_de_computadoras
- [70] <http://186.42.96.211:8080/jspui/bitstream/123456789/473/1/An%C3%A1lisis%20%26%20Captura%20de%20Paquetes%20de%20Datos%20-%20Wireshark.pdf>
- <http://ftp.gul.es/pub/gul/cursos/2009/marzo/Análisis%20de%20redes%20con%20WireShark/wireshark.pdf>
- [71] <http://www.visualbeta.es/3009/software-libre/vlc-el-mejor-reproductor-multimedia/>
- [72] <http://www.slideshare.net/manuelfloresv/analisis-de-los-protocolos-de-tiempo-real-rtp-rtcp-y-rtsp>
- [73] <http://www.ibiblio.org/pub/Linux/docs/linux-doc-project/linuxfocus/Castellano/March2003/article282.meta.shtml>
- [74] <http://www.zonadeseguridad.net/scapy-inundar-tu-router-de-paquetes-syn/>
- [75] <http://samsclass.info/124/proj11/proj7x-scapy-IPv6.html>
- [76] <https://code.google.com/p/scapy-gui-IPv6/wiki/Installation>
- [77] <http://www.secdev.org/projects/scapy/doc/installation.html>
- [78] <http://www.slideshare.net/ositobio/scapy-generacin-y-manipulacin-bsica-de-paquetes-de-red>

- [79] <http://www.secdev.org/projects/scapy/>
- [80] <http://www.seguridadx.com/scapy/#more-135>
- [81] <http://revistas.mes.edu.cu/greenstone/collect/repo/import/repo/20120830/71208073310.pdf>
- [82] <http://revistas.mes.edu.cu/greenstone/collect/repo/import/repo/20120830/71208073310.pdf>, Capítulo 1. Generalidades del servicio de IPTV y características de las redes que lo soportan.
- [83] <http://revistas.mes.edu.cu/greenstone/collect/repo/import/repo/20120830/71208073310.pdf>, Capítulo 2. Métricas utilizadas en la validación de la calidad del servicio de IPTV.