Análisis de la calidad de experiencia Q&E y Seguridad en la red en el Tráfico de Streaming Multimedia entre IPv6 & IPv4

Ricardo Andrés Medina Puentes

Trabajo de grado para optar el título de Magister en Redes y Sistemas de Comunicación

Director

Tito Raúl Vargas Hernández

Maestría en Redes, Tecnologías y Redes de Comunicaciones

Universidad Santo Tomás, Bucaramanga

División de Ingenierías y Arquitectura

Facultad de Ingeniería en Telecomunicaciones

2022

Dedicatoria

La dedicatoria de este trabajo va dirigida de manera muy especial a mis padres, quienes han fundado los cimientos para el desarrollo integral de sus hijos y nos han formado con las bases de la honestidad, el amor, el trabajo y la humildad. Para ellos, una dedicatoria muy especial como mínima retribución a todo el sacrificio que han realizado a lo largo de su vida para llevar adelante a sus hijos.

A mis hermanos, quienes me han apoyado en múltiples situaciones y en diferentes aspectos, especialmente, con el ánimo de continuar con aquello que se inicia y no darse por vencido.

Al Ingeniero Tito Raúl Vargas por su constante apoyo en el desarrollo de este trabajo final de maestría y ha mostrado toda su dedicación y tutoría en la orientación de las diferentes problemáticas que se presentaron y a las cuales dio diligencia desde su experticia y liderazgo.

Así mismo, a todas aquellas personas y amigos muy especiales que me han apoyado y exhortado a seguir adelante y superarme personal y laboralmente, también dedico este trabajo.

Agradecimientos

El agradecimiento de este trabajo final de maestría va dirigido inicialmente a mi director Tito Raúl Vargas Hernández, a quién debo el honor de ser participe del programa de posgrado y de quién recibí la invitación y todo el apoyo para postularme y continuar con el proceso. Esto ha significado, de manera personal, una enorme oportunidad de crecimiento personal y profesional y la maravillosa oportunidad de hacer parte del área académica.

A mis amigos, familia, compañeros presentes y pasados, quienes de una u otra forma, han aportado desde su experiencia, apoyo, conocimiento, alegrías y tristezas, a lo largo de este camino que ha dejado toda la experiencia y saberes para la construcción de mi desarrollo profesional y personal.

Contenido

Lista de tablas

Lista de figuras

Resumen

Los constantes cambios en términos tecnológicos a los que la Universidad Santo Tomás Seccional Bucaramanga se ve enfrentada como institución educativa y que repercuten en desarrollar, crear y mejorar los medios tecnológicos que brinda la institución en pro de ofrecer los mejores estándares de educación de calidad mediante el incremento en la apropiación de las TIC por parte de la comunidad académica, innovación y uso de tecnologías que implican una problemática en infraestructura y actualización de equipos que permitan una escalabilidad adecuada. En este proceso se incorpora la implementación del protocolo de internet versión 6, IPv6, como parte de la actualización del sistema de carteleras digitales existente en los campus de Bucaramanga y Floridablanca y que permite un trabajo de investigación en torno a esta temática. Este trabajo de investigación busca realizar la comparativa de tráfico multimedia entre los protocolos IPv4 e Ipv6, por medio de un entorno controlado de laboratorio, incorporando mecanismos de compresión de video H.264 y H.265 a diferentes formatos de calidad de video bajo tres tasas de bit propuestas a partir del encolamiento de paquetes configurado en el router a fin de analizar la adaptación del contenido de manera dinámica mediante el protocolo DASH e identificar vulnerabilidades al tráfico Ipv6 mediante la aplicación de ataques a la red de manera controlada. Finalmente, resolver estas variables se traduce en una calidad de experiencia positiva para los usuarios que consumen el contenido de las cartelas digitales y favorecen el desempeño de la red. Se presenta el análisis de los resultados obtenidos para la comparativa de tráfico multimedia entre los protocolos de internet mencionados, el análisis de seguridad de IPv6 y los parámetros de calidad de servicio y las técnicas de calidad de la experiencia utilizados para el desarrollo de la investigación.

Abstract

The ongoing technological changes that University Bucaramanga´s Campus constantly faces as a higher education institution affects directly its development, therefore, it requires developing, creating and improving its technological tools in order to get a higher quality and education standards; this can be done by increasing the ICT appropriation by the academic community, along with the innovation and use of technology, which demands a better infrastructure and upgraded devices that allow a suitable scalability.

The aforementioned process includes the implementation of IPv6 protocol as part of the actualization of the existing digital posters system in Bucaramanga and Floridablanca University Campus and which at the same time, enables to conduct a research study around the issue.

This research study seeks to carry out a multimedia internet traffic comparative between IPv4 and IPv6 protocols, through a laboratory-controlled environment, including video compression mechanisms H.264 and H.265 at different video quality formats under three proposed bitrates from queuing packets configured on the router in order to analyze content adaptation in a dynamic way by means of a DASH protocol and identify IPv6 traffic vulnerabilities with controlled network attacks applications.

Finally, to solve these variables results in a positive experience for the users who consume multimedia content from digital posters and support the network performance. The analysis of the results obtained is presented along with the multimedia traffic comparative between internet protocols previously mentioned, IPv6 security analysis and quality service parameters, just as quality experience techniques used for this research study.

Introducción

El presente proyecto, busca simular una actualización tecnológica en la Universidad Santo Tomás seccional Bucaramanga utilizando el protocolo de internet versión 6, IPv6, sobre su sistema de configuración de red. El desarrollo de este proyecto de actualización tecnológica se basa en el análisis previo de cuatro temáticas clave.

La primera es el análisis de la plataforma de *Video Streaming* ya existente para difundir información institucional mediante carteleras digitales en los campus de Bucaramanga y Floridablanca. Esta plataforma se despliega por los campus conectada por medio de la red IP administrativa; está configurada con el protocolo IPv4 y utiliza dispositivos Raspberry Pi [1] y monitores Samsung para Digital Signage[1]. Dentro del contenido publicado en estas carteleras digitales, se encuentran videos institucionales acerca de los procesos de Acreditación de Alta Calidad, Plan Integral Multicampus y contenido institucional correspondiente a oferta de programas académicos de pregrado y posgrado, así como de educación continua. Por otra parte, se publicitan eventos académicos que tienen lugar dentro y/o fuera de los diferentes campus universitarios.

Esta *plataforma streaming* marca un punto de referencia para abordar la segunda temática y posiblemente también sea referencia para trabajos futuros, ya que por ejemplo abre una puerta para incorporar protocolos de video adaptativo y video sobre demanda en la plataforma existente. Esta segunda temática se trata del protocolo IPv6 y su adopción para soportar los servicios de streaming multimedia bajo determinados parámetros de seguridad y analizar su desempeño en comparación con el protocolo IPv4.

[1] Digital Signage Colombia S.A, compañía de señalización digital multimedia.

Para plantear cualquier trabajo sobre una plataforma de video streaming en una base *dual stacking*, donde coexisten los protocolos de internet IPv4 e IPv6, es imprescindible abordar otras dos temáticas clave: Calidad de experiencia y Seguridad en redes IPv6, las cuales representan la tercera y cuarta temáticas del proyecto, respectivamente.

Por su parte, la Calidad de experiencia demanda un análisis de tráfico IPv4 versus IPv6, con el cual se pretende estudiar el comportamiento de la cabecera IP [2] en servicios de *video streaming*. Las diferencias representativas y significantes que se encuentren serán la base fundamental para el presente estudio, pues a partir de ahí se entrará al campo práctico en forma de aplicación tecnológica. Inicialmente, este análisis se realiza dentro de un entorno controlado de laboratorio con equipos de red que, por tratarse de un entorno académico, probablemente no manejan grandes cantidades de tráfico. Esto conlleva a pasar a un plano práctico experimental ya propiamente dentro de las redes IP, sobre las cuales se despliega actualmente el servicio de carteleras digitales.

Entonces, se pasa a realizar una segunda fase del análisis del comportamiento de las redes. En este punto es necesario tocar temas de seguridad en las redes, ya que los niveles de seguridad de red a nivel general en la Universidad se encuentran aplicados a las redes IPv4 y en una forma básica a Ipv6. Esto da espacio a posibles vulnerabilidades [3] de la red sobre IPv6 ya que, tratándose de un campo experimental, no se conoce de primera mano cómo pueda verse afectada la red de la Universidad, en sus diferentes ámbitos. Asimismo, se encuentra que es imperativo realizar los análisis correspondientes por medio de ataques controlados a la red, tales como MITM[2] (*Man In The Middle*) sobre redes IPv6 con *Neighbor Advertisement Spoofing*,

[2] Man In The Middle: Es un ataque de un intermediario en un enlace de comunicaciones el cual intercepta, modifica o se apropia de la comunicación.

ataque SLAAC[3] (*Sateless Address Autoconfiguration*) [4], *Fake* DHCPv6[4] (*Dynamic Host Configuration Protocol versión 6*) [5], DoS[5] (*Denial of Service*) [6] sobre redes IPv6 con *SLAAC DoS*, con el fin de estudiar los posibles baches de seguridad que se puedan detectar y evitar inconvenientes desde el punto de vista de la seguridad de red.

Finalmente, en vista del apoyo al cumplimiento de los objetivos de los Planes de Desarrollo de la Universidad Santo Tomás seccional Bucaramanga, correspondientes a focalizar y articular la investigación y la proyección social de la USTA con visibilidad e impacto nacional y global, el presente proyecto aporta a la producción investigativa de impacto en la población universitaria, mejorando la clasificación de los grupos de investigación.

Palabras Clave: Streaming Media, Quality of Experience, IP networks, Firewalls (computing), DASH Protocol

[3] SLAAC: *Stateless Address Autoconfiguration.* Mecanismo que utiliza IPv6 para la autoconfiguración de direcciones.

[4] DHCPv6: *Dynamic Host Configuration Protocol Version 6.* Protocolo de configuración automática de direcciones IPv6.

[5] DoS: *Denial of Service.* Ataque a un sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Hnadley, M., Rescrola, E.

1. Análisis de la calidad de experiencia Q&E y Seguridad en la red en el Tráfico de Streaming Multimedia entre IPv6 & IPv4

1.1 Planteamiento del problema

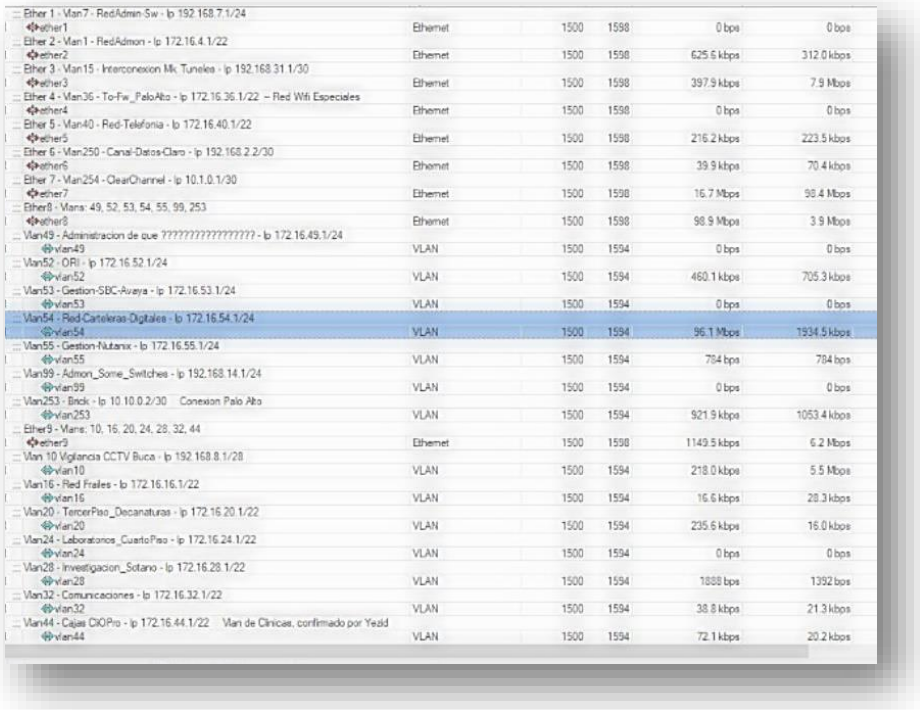
Inicialmente, la presente investigación se enfoca en simular la integración de servicios multimedia en el sistema de carteleras digitales del campus Floridablanca de la Universidad Santo Tomás, seccional Bucaramanga. Estos servicios se incorporan con el fin de actualizar el sistema de carteleras digitales existente, como base importante para establecer servicios de video streaming, además de video sobre demanda. De esta manera, se hace posible estudiar la viabilidad de albergar no sólo contenido institucional, como se hace actualmente, sino contenido de la población académica en sus diversas actividades, tanto académicas como de bienestar universitario, así como tutorías disponibles para los estudiantes, por citar algunos ejemplos.

Esto sería el abordaje del problema desde el punto de vista del aprovechamiento de un servicio existente para actualizarlo implementando desarrollo tecnológico de plataformas de video streaming. Sin embargo, para la puesta en marcha de estos servicios se deben contemplar diversos parámetros que representan potenciales inconvenientes, tales como: la calidad de servicio de la red, el procesamiento del servidor además del tratamiento y análisis de paquetes, entre otros. Este último parámetro, tratamiento y análisis de paquetes IP, corresponde a la raíz del problema de investigación, ya que con la implementación del servicio de *video streaming*, también se busca estudiar el comportamiento de la paquetización de *video streaming.*

Una de las principales problemáticas que actualmente se presentan a nivel de red es la utilización del ancho de banda por parte de estos servicios. Para poner el escenario en contexto, existe un canal de datos que comunica las sedes de Floridablanca y Bucaramanga de la USTA

con una capacidad contratada con el ISP de 100 Mbps. A través de este canal de datos se establece comunicación entre los diferentes servicios institucionales alojados en diferentes servidores ubicados en la sede de Bucaramanga, de manera que, los equipos en el campus Floridablanca de Universidad, establecen comunicación por medio de este canal (*clear channel*)[6] de fibra oscura con los servidores en Bucaramanga. Para el caso del sistema de carteleras digitales, el servidor se encuentra en el campus de florida, de manera que los dispositivos que se encuentran en Bucaramanga deben establecer comunicación con el servidor de Floridablanca. Esta comunicación implica difusión Unicast entre el servidor y los dispositivos, lo cual conlleva a una ocupación del canal de datos de más del 90% como se puede observar en las siguientes imágenes:

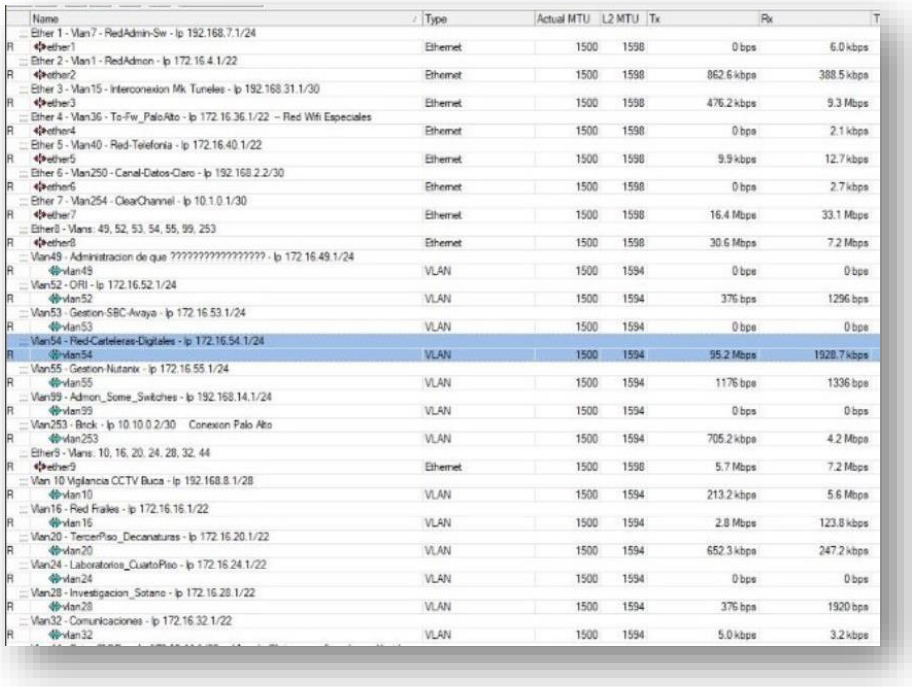
Figura 1. *Lectura de tráfico VLAN de video.*



[6] *Clear Channel:* Servicio que permite la transmisión de datos de un lugar remoto a uno central. Es un enlace dedicado de datos punto a punto.

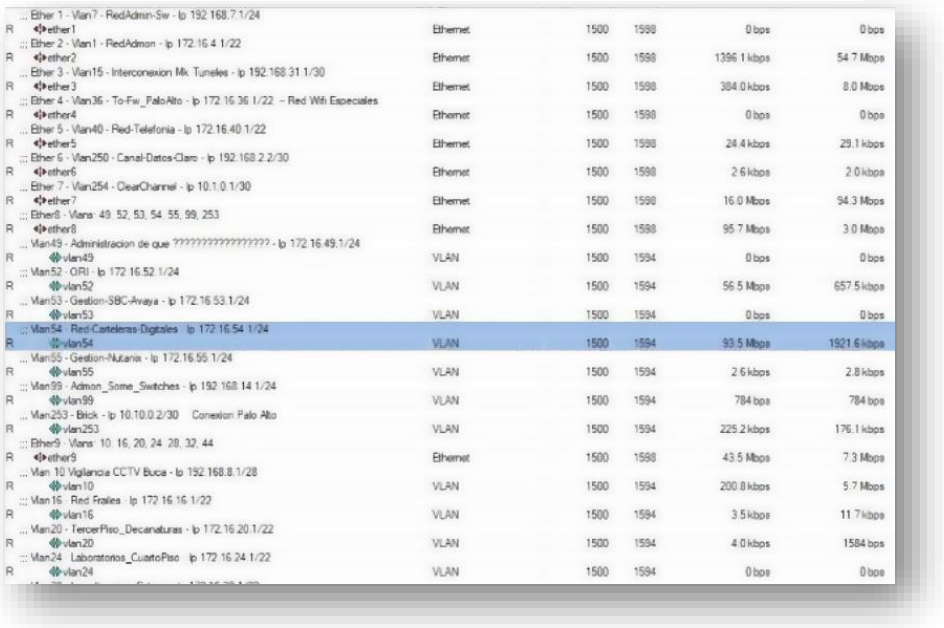
Si bien, esta ocupación de canal no es constante, ya que se presenta cuando se realiza la transmisión de videos institucionales, y estos a su vez son transmitidos en ciertas franjas horarias mientras que el resto de tiempo se transmiten sólo imágenes, la franja horaria en la que se transmite el contenido de video, llega a ocupar casi la totalidad del canal al punto que se crea lo que se denomina “cuello de botella” lo cual ha afectado mayormente la transmisión de voz sobre IP para la plataforma de telefonía de la Universidad, pues el servidor de telefonía se encuentra en Bucaramanga y en florida se encuentran más de 250 extensiones telefónicas, lo cual significa que en un momento dado se satura el canal, tal y como se evidencia en las Figuras 2 y 3, en donde se muestra el tráfico por VLAN´s y se resalta la VLAN número 54, a través de la cual se transmite el contenido multimedia por medio de la red 172.16.54.0/24 a un bitrate de interfaz de aproximadamente 95.2 Mbps en transmisión.

Figura 2. *Lectura de tráfico de VLAN de video*



	Name	Type	Actual MTU	L2 MTU	Tx	Rx	T
	Ether 1 - Vlan7 - RedAdmin-Sw - Ip 192.168.7.1/24						
R	ether1	Ethernet	1500	1598	0 bps	6.0 kbps	
	Ether 2 - Vlan1 - RedAdmon - Ip 172.16.4.1/22						
R	ether2	Ethernet	1500	1598	862.6 kbps	388.5 kbps	
	Ether 3 - Vlan15 - Interconexion Mk Tuneles - Ip 192.168.31.1/30						
R	ether3	Ethernet	1500	1598	476.2 kbps	9.3 Mbps	
	Ether 4 - Vlan36 - To-Fw_PaloAlto - Ip 172.16.36.1/22 -- Red Wifi Especiales						
R	ether4	Ethernet	1500	1598	0 bps	2.1 kbps	
	Ether 5 - Vlan40 - Red-Telefonia - Ip 172.16.40.1/22						
R	ether5	Ethernet	1500	1598	9.9 kbps	12.7 kbps	
	Ether 6 - Vlan250 - Canal-Datos-Claro - Ip 192.168.2.2/30						
R	ether6	Ethernet	1500	1598	0 bps	2.7 kbps	
	Ether 7 - Vlan254 - ClearChannel - Ip 10.1.0.1/30						
R	ether7	Ethernet	1500	1598	16.4 Mbps	33.1 Mbps	
	Ether8 - Vlans: 49, 52, 53, 54, 55, 99, 253						
R	ether8	Ethernet	1500	1598	30.6 Mbps	7.2 Mbps	
	Vlan49 - Administracion de que ???????????????? - Ip 172.16.49.1/24						
R	vlan49	VLAN	1500	1594	0 bps	0 bps	
	Vlan52 - ORI - Ip 172.16.52.1/24						
R	vlan52	VLAN	1500	1594	376 bps	1296 bps	
	Vlan53 - Gestion-SBC-Avaya - Ip 172.16.53.1/24						
R	vlan53	VLAN	1500	1594	0 bps	0 bps	
	Vlan54 - Red-Carteleras-Digitales - Ip 172.16.54.1/24						
R	vlan54	VLAN	1500	1594	95.2 Mbps	1928.7 kbps	
	Vlan55 - Gestion-Nutanix - Ip 172.16.55.1/24						
R	vlan55	VLAN	1500	1594	1176 bps	1336 bps	
	Vlan99 - Admon_Some_Switches - Ip 192.168.14.1/24						
R	vlan99	VLAN	1500	1594	0 bps	0 bps	
	Vlan253 - Brick - Ip 10.10.0.2/30 Conexion Palo Alto						
R	vlan253	VLAN	1500	1594	705.2 kbps	4.2 Mbps	
	Ether9 - Vlans: 10, 16, 20, 24, 28, 32, 44						
R	ether9	Ethernet	1500	1598	5.7 Mbps	7.2 Mbps	
	Vlan 10 Vigilancia CCTV Buca - Ip 192.168.8.1/28						
R	vlan10	VLAN	1500	1594	213.2 kbps	5.6 Mbps	
	Vlan16 - Red Frailes - Ip 172.16.16.1/22						
R	vlan16	VLAN	1500	1594	2.8 Mbps	123.8 kbps	
	Vlan20 - TercerPiso_Decanaturas - Ip 172.16.20.1/22						
R	vlan20	VLAN	1500	1594	652.3 kbps	247.2 kbps	
	Vlan24 - Laboratorios_CuartoPiso - Ip 172.16.24.1/22						
R	vlan24	VLAN	1500	1594	0 bps	0 bps	
	Vlan28 - Investigacion_Sotano - Ip 172.16.28.1/22						
R	vlan28	VLAN	1500	1594	376 bps	1920 bps	
	Vlan32 - Comunicaciones - Ip 172.16.32.1/22						
R	vlan32	VLAN	1500	1594	5.0 kbps	3.2 kbps	

Figura 3. *Lectura de tráfico de VLAN de video, elaborada por el autor.*



Inicialmente, la comparación entre el protocolo IPv4 y el protocolo IPv6 se realiza desde un entorno de red controlado a fin de poder estudiar estos resultados. Al analizar el comportamiento de la transmisión de paquetes mediante la red de la Universidad, se busca evaluar si realmente la utilización del protocolo de red IPv6 aporta una mejora considerable en términos de calidad, teniendo en cuenta aspectos de resolución de video, utilización del ancho de banda, enrutamiento de paquetes, fragmentación de paquetes, tasa de transmisión, jitter, etc. En el caso de que las mejoras resulten significativas tanto en la calidad de servicio como en la calidad de experiencia QoE se implementaría por primera vez este protocolo para un servicio en el Campus de la universidad.

Por otra parte, al implementar servicios sobre IPv6, necesariamente se deben ajustar temas de seguridad, porque generalmente, a niveles de las diferentes capas del modelo TCP/IP[7]

[7] TCP/IP: Siglas del protocolo de control de transmisión/ protocolo de internet.

(RFC1180) [7], la seguridad se da en función de proteger la red a partir de cualquier incidencia sobre IPv4 [8]; y en vista de que el campus de la Universidad Santo Tomás tiene un robusto sistema de Firewall, se debe estudiar, analizar y eventualmente su sistema de seguridad tendrá que mejorar o adecuarse en las redes para garantizar una transmisión segura del contenido sobre IPv6 en función de las diferentes incidencias en la seguridad de las redes IPv6 y las tecnologías de transición con tunelización de tráfico IPv6 sobre IPv4, que representan un riesgo para técnicas de ataques no anticipados sobre el protocolo IPv6 [9].

Pregunta de investigación

¿Cómo se comporta el protocolo IPv6 en la transmisión de contenido multimedia en comparación con IPv4, al ser implementado en servicios de video streaming como actualización tecnológica del sistema de carteleras digitales de la Universidad Santo Tomás seccional Bucaramanga?

1.2. Objetivos

1.2.1 Objetivo General

Evaluar la calidad de experiencia QoE de *video streaming* sobre IPv6 con respecto a IPv4 mediante el estudio de tráfico en la transmisión de contenido multimedia, la medición de la calidad de servicio QoS y análisis de seguridad en la red para una actualización tecnológica del sistema de carteleras digitales de la Universidad Santo Tomás seccional Bucaramanga.

1.2.2 Objetivos Específicos

- Elaborar un diagnóstico sobre el comportamiento de tráfico de *streaming* multimedia adaptativo IPv4 e Ipv6 por medio de topología tipo cliente -servidor dentro de un entorno controlado de red, a partir de la cual se evaluarán los resultados.
- Analizar parámetros de seguridad en IPv6 a partir de la topología tipo cliente – servidor mediante ataques en la red en un escenario simulado e identificar posibles incidencias de seguridad dentro de la red privada de la U. Santo Tomás.
- Evaluar la calidad de experiencia y la calidad de servicio de video streaming sobre IPv6 por medio del sistema de carteleras digitales utilizando un modelo comparativo que permitirá analizar las características del tráfico de red con respecto a IPv4.

2. Marco Referencial

2.1 Marco Conceptual

IPv6*: (RFC 8200) (2017) "IP version 6 (IPv6) is a new version of the Internet Protocol (IP), designed as the successor to IP version 4 (IPv4) [RFC791]".* [10]

IPv4: (RFC 791) (1981) "*Internet Protocol versión 4*". [11]

QoS: ITU-T Rec. E.800; "Totalidad de características de un servicio de telecomunicaciones que soporta en su habilidad de satisfacer necesidades implicadas y establecidas de los usuarios del servicio". [12]

QoE: De acuerdo con la recomendación ITU-T P.10/G100: "la calidad de experiencia (QoE) fue inicialmente definida como la aceptabilidad general de una aplicación o un servicio, percibido subjetivamente por el usuario final". [13]

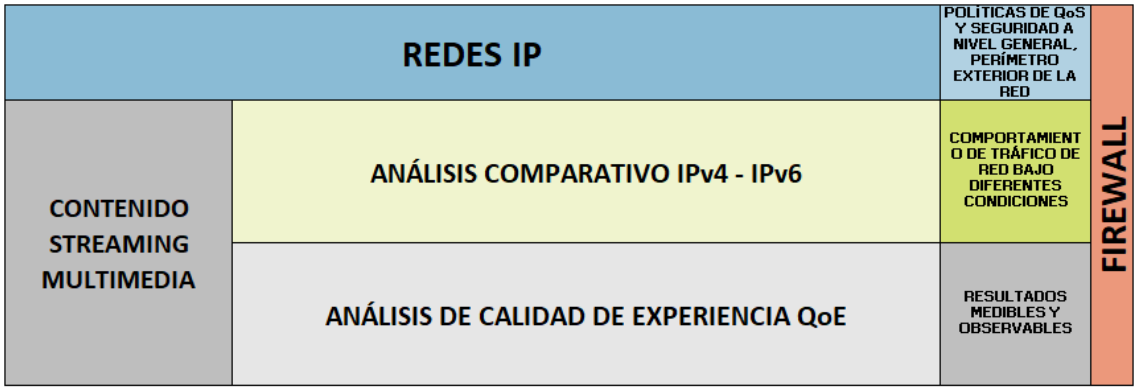
Firewall: (b-ISO/IEC 27030-1) (2019):" Tipo de barrera de seguridad ubicada entre ambientes de red, consistente de un sistema de detección de intrusos, así como de tratamiento de tráfico de red". [14]

Protocolo DASH: Protocolo dinámico adaptativo sobre HTTP.

Streaming Adaptativo: Definido por el estándar IEEE 1857.7-2018 - IEEE *Standard for Adaptive Streaming*; "especifica el formato de descripción de presentación del contenido (MPD) y el formato de segmento del contenido para streaming adaptativo y dinámico sobre redes tales como Hypertext Transfer Protocol (HTTP). [15]

Codificación Avanzada de Video y Audio: Según el estándar 1857-2013 de la IEEE, se define como: "un conjunto de herramientas para codificación de video eficiente, incluyendo un contexto de codificación aritmética binaria adaptativa, así como el método de codificación correspondiente". [16]

Figura 4. *Contexto de la Investigación.*



2.2 Marco Teórico

En el contexto de la infraestructura mundial de redes IP, en los últimos años múltiples autores han anticipado el agotamiento de direcciones IPv4 a nivel mundial. Sin embargo, a principios de los noventa esto fue previsto por la IANA (*Internet Assigned Numbers Authority*), y este fenómeno empieza a ocurrir inicialmente en Asia, continente en el cual se despliega actualmente el mayor avance en protocolo IPv6. En el continente africano aún se conservan gran parte del direccionamiento asignado a esta región. En vista de este agotamiento, diversas fuentes han empleado estrategias para la perdurabilidad de la versión 4 de internet mediante técnicas de optimización de recursos de asignación de direccionamiento. No obstante, el direccionamiento IPv6 ha empezado a tomar lugar dentro de este escenario, en el cual la presencia de esta nueva versión del protocolo de internet ya es inminente y gradualmente viene tomando lugar. Sin embargo, existen aún diferentes inquietudes dentro del gremio del networking a nivel local sobre la entrada en marcha de este protocolo, bien sea por desconocimiento de su estructura o simplemente por desinterés en el asunto.

Al considerar la problemática planteada, desde el punto de vista de la infraestructura de la red y de los constantes avances que surgen continuamente en el mundo de los sistemas de comunicaciones, las políticas de calidad de servicio son imprescindibles en redes de datos que

incorporen contenido de video, voz y datos. Las políticas de calidad de servicio implican en sí mismas múltiples parámetros que van desde un adecuado diseño y planeación de la red que permita redundancia y disponibilidad, manejo moderado de presupuesto con el cual se logren adquirir equipos ideales para las funciones requeridas sin acarrear costos extras que no sean necesarios debido a una mala planeación, tratamiento de los diferentes servicios de la red a partir del análisis y priorización de estos, manejo de encolamiento de paquetes en las interfaces troncales de los equipos de distribución, protocolos de enrutamiento, control de acceso al medio a través políticas de seguridad en la red de primer nivel como autenticación y certificación de usuarios, asignación de zonas desmilitarizadas, filtrado de contenido, prevención y detección de intrusos, análisis profundo de paquetes, reglas de control de acceso, prevención de diferentes tipos de ataques a la red, entre otros aspectos relacionados con diseño y planeación de redes IP [17].

En consecuencia, la calidad de servicio impuesta en una red se traduce finalmente en la calidad de experiencia QoE, parámetro subjetivamente medible desde el punto de vista del usuario [18]. Entra en escena entonces el protocolo IPv6, que viene a coexistir dentro de las redes IPv4 y cuyo objeto de la presente investigación es realizar un análisis comparativo de la transmisión de contenido streaming multimedia sobre ambos protocolos para determinar su viabilidad para una actualización tecnológica, aplicando los parámetros anteriormente mencionados.

Con esto se pretende entonces plantear un modelo que integre las diferentes características planteadas en la presente investigación como se muestra en la Figura 6.

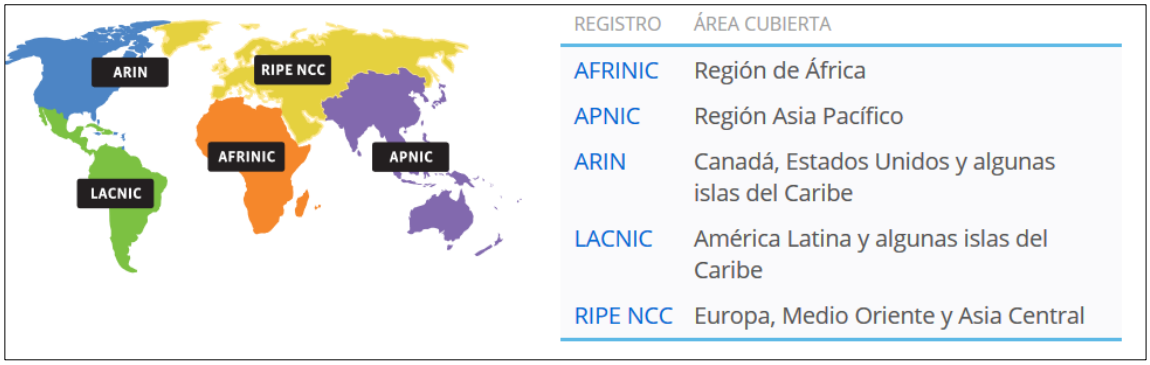
- IPv4: El protocolo de internet IPv4 consta de una serie de numeración regulada, asignada y reglamentada por la IANA [19], entidad encargada de asignar y regular las

direcciones IP. Las direcciones IP, correspondientes a la capa de red del protocolo de red TCP/IP, son asignadas de acuerdo con la ubicación geográfica de los usuarios llamadas regiones. Existen cinco regiones a nivel mundial:

1. Latin American and Caribbean Internet Address Registry. [20]
2. American Registry for Internet Numbers. [21]
3. RIPE Network Coordination Center. [22]
4. Asia-Pacific Network Coordination Center. [23]
5. African Network Information Center. [24]

A cada región le es asignado una sección de direcciones IP disponibles. Estas direcciones son conocidas como direcciones IP públicas, en este sentido existen dos tipos de direcciones IP; públicas y privadas. Las direcciones públicas son utilizadas para viajar a través de la red de internet, ya que estas son asignadas y autorizadas por la IANA a través de las diferentes organizaciones regionales. Estas direcciones están autorizadas para ser enrutadas a través de las redes mundiales de internet por medio de los proveedores de servicio de internet ISP (*Internet Provider Services*). Las direcciones IP privadas son clasificadas y agrupadas en tres grupos A, B y C. Cada uno de estos grupos designa las dimensiones que van a tomar las redes de acuerdo con la cantidad de bits que se tomen para subred y para asignación de hosts.

Figura 5. *Asignación Regional de Direcciones IP por Áreas Continentales.*



Tomado de [20].

La clase A (0.0.0.0 – 127.0.0.0) utiliza el primer octeto para designar la cantidad de subredes (128) y los otros tres octetos para terminales (más de 16 millones), esto se hace con el fin de tener disponibilidad de direccionamiento para redes con decenas de miles de usuarios. La clase B (128.0.0.0 – 195.255.0.0) utiliza los dos primeros octetos para la asignación de subredes (16384) y los dos restantes para la asignación de hosts (65.534), esta clase se usa para redes "medianas", sin embargo, su disponibilidad de direccionamiento es considerablemente amplia. Por último, está la clase C (192.0.0.0 – 239.255.255.0). Existen por otra parte, dos clases más, D y E. la clase D es utilizada para tráfico multicast y la clase E es utilizada para fines experimentales. Por otra parte, existen direcciones aisladas que son de uso exclusivo, como la dirección Ip 127.0.0.1 correspondiente a la dirección Loopback, asignada automáticamente por los dispositivos de red para enviar paquetes *request-response* a sí mismo con el fin de realizar pruebas de conectividad [25].

Una de las características principales de Ipv4 es el uso de la máscara de subred, la cual define el alcance de la cantidad de bits de red y de hosts, y delimita el ámbito de red, es decir el punto desde donde inicia y termina el dominio de una red, con el fin de segmentarla y definir qué cantidad de direcciones IP van a hacer parte de este grupo o dominio de red.

- IPv6: De la misma forma en que se regulan y asignan las direcciones IPv4, la IANA realiza la asignación y clasificación de direccionamiento IPv6 a nivel mundial. El direccionamiento IPv6 utiliza 128 bites de información en lugar de los 32 que usa IPv4. Dentro de la clasificación de direccionamiento IPv6 encontramos direcciones *Anycast, Global Unicast* y *Multicast*. Las direcciones IPv6 a pesar de ocupar un espacio mayor que IPv4, están diseñadas no sólo para mitigar el agotamiento del direccionamiento

IPv4, sino para implementar un modelo en el que se buscar acortar los saltos de red que se hacen en IPv4, por una parte, y por otra eliminar el concepto de NAT10 (*Network Address Translation*), lo cual, en teoría, ahorraría recursos de procesamiento en el tratamiento de paquetes desde los enrutadores. Otra característica de IPv6, es que este protocolo permite crear trillones de direcciones debido a que dado la cantidad de bites de su cabecera, existe un gran número de posibilidades de combinación que permitiría crear nuevas direcciones.

10 NAT: *Network Address Translation.* Mecanismo usado para traducir direcciones IP de un ámbito privado a direcciones IP públicas. Adicionalmente, ipv6 tiene la particularidad de que no utiliza máscara de subred como lo hace Ipv4, la versión 6 no utiliza la denotación de la máscara de subred, sino que lo hace con la denotación de prefijos. De esta manera, con los prefijos es posible crear subredes en IPv6. IPv6 implementa nuevas características dentro del modelo de encapsulación de paquetes en la cabecera IP, elimina ciertos campos que vienen incluidos en IPv4 con el fin de quitar peso a la transmisión y optimiza campos como el *payload* y *cheksum* dentro de la cabecera IP. Ver Figura 8.

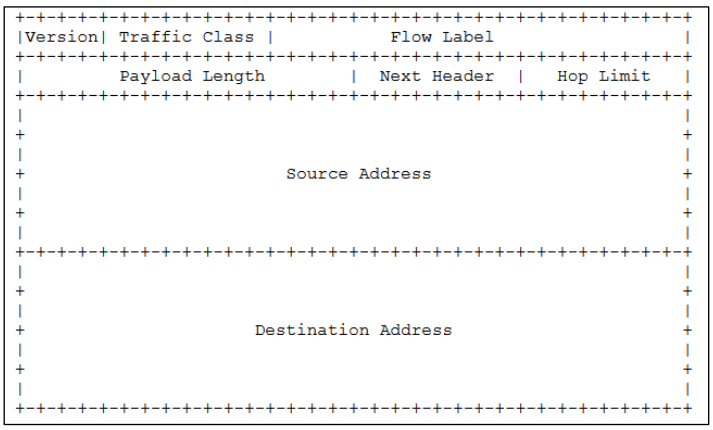
Tabla 1. *Identificación de los tipos de direccionamiento IPv6.*

Tipo de Direccion	Prefijo Binario	Notación Ipv6
No especificada	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

Adaptado de [26].

Finalmente, IPv6 se caracteriza porque sus direcciones son únicas en el mundo, es decir, se elimina el concepto de direcciones privadas y públicas, pues IPv6 permite la comunicación usando las direcciones de los hosts directamente a través de la red (*global unicast*).

Figura 6. *Formato de Cabecera IPv6*



Tomado de [27].

- Firewall: Los Firewall son dispositivos creados para blindar las redes privadas de una organización o de una compañía. Existen dentro de los firewalls, diferentes niveles de protección de acuerdo con la capa de operación. Por ejemplo, para la capa de enlace, técnicas que emplean firewall para suprimir ataques a nivel de tablas ARP, como *ARP Flooding* o *ARP Spoofing*. En la capa de red se encuentran diversos métodos de protección como detección profunda de paquetes, que des encapsula y procesa los paquetes de acuerdo con su origen destino con el fin de certificar la autenticidad de la información dentro de la organización.

Además de crear este tipo de políticas, los firewalls, en especial los más robustos permiten crear tareas de networking a nivel de capa 3 (red), asignando ámbitos de direccionamiento IP, así como asignación de objetos dinámicos y estáticos. Por otra parte, los Firewalls, blindan la red interna de ataques externos aplicando estrategias de detección de intrusos por zonas

geográficas bloqueando eventualmente direcciones IP públicas asignadas a ciertos países, por las respectivas regiones, filtrado de contenido HTTP, consistente en el filtrado de páginas web fraudulentas o que utilicen contenido no permitido dentro de una organización como contenido para adultos, ventas de armas, drogas, entre otras. Por otra parte, desde el nivel de acceso, también permite crear reglas de control de acceso (ACL). Los firewalls más robustos tienen la capacidad de procesar gran cantidad de información bajo condiciones de red densas o que demanden fluidez, igualmente, tanto para IPv4 como para IPv6. Dentro de la Universidad Santo Tomás, el sistema de Firewalls opera bajo el modelo dual-stacking, es decir, soporta ambos protocolos. El modelo para Ipv6 permite detectar ataques tales como IPv6 Spoofing o DHCP SLAAC.

Existen algunas herramientas desarrolladas para detectar falencias en la red y que igualmente soportan ambos protocolos. Una de estas es EvilFoca [28],con la cual se pueden perpetrar ataques controlados con MITM (Man In The Middle) para IPv4 e IPv6, ataques de denegación de servicios para IPv4 sobre ARP Spoofing y ARP Flooding, y para IPv6 con SLAAC DoS entre otros.

Es importante mencionar el uso de gestores de tráfico IP a través de simuladores de red tales como Cisco Packet Tracer, Riverbed Modeler o GNS, así como de herramientas de análisis y visualización de tráfico como Wireshark, el cual permite una gran cantidad de funciones que van desde el escaneo de un dominio de broadcast hasta el análisis de puertos de las capas de transporte. Esta herramienta es indispensable para la recolección de información en términos de realizar estudios estadísticos de la red o de detección de problemáticas presentadas en la red.

- DASH Protocol: Consiste en un mecanismo creado para sobrellevar la ocupación del ancho de banda de parte de contenidos que demandan gran espacio para su transmisión como es el caso de video streaming y/ multimedia. Este protocolo adapta la tasa de transmisión a la calidad de video transmitido. Podemos observar que plataformas como HBO, YouTube o Netflix utilizan este protocolo para adaptar la calidad del video al bitrate de transmisión, con la finalidad de no presentar pérdidas en la difusión del contenido. Sin embargo, aquí surge una pregunta importante, ¿Cómo puede afectar la calidad de experiencia para el usuario, utilizar esta estrategia de calidad de servicio que desmejora la calidad de video para evitar interrupciones? Nos encontramos entonces en un escenario en el cual por una parte se encuentra la limitante de la infraestructura de red dada por el canal de ancho de banda y por otra, la forma de mitigar este impacto, implementado políticas de calidad de servicio que irónicamente afectan la percepción del usuario, ¿es preferible tener interrupciones y conservar la calidad de video, o tener una transmisión constante, pero a una baja calidad? No obstante, diferentes mecanismos como el Buffering logran reducir esta problemática, al menos gradualmente.

2.3 Marco Legal

El presente trabajo de investigación está enmarcado dentro de los lineamientos de plan integral multi campus que buscan, entre otras líneas de acción, la proyección social y la investigación, así como el enriquecimiento regional de los programas bajo estándares comunes con miras a la transformación social. [29].

- ITU-R BT.1833-3: *"Acerca de componentes satelitales que combinan sistemas multimedia (no dedicados o explícitamente dedicados a la difusión) y componentes de difusión terrestre*

dedicados integrados dentro de los planes de frecuencia nacional que cumplan los requerimientos para una amplia cobertura con buena calidad de servicio." **[30]**.

- ITU-R F.1399-1: *"Quality of Service (4.2.20): el efecto colectivo del desempeño del servicio el cual determina el grado de satisfacción de un usuario o de un servicio."* **[31]**
- IANA (Autoridad de números asignados de internet).

Como responsable de la coordinación global de para los sistemas de direccionamiento del protocolo de internet y de los números de sistemas autónomos usados para enrutar el tráfico de internet, la IANA es la organización encargada de administrar y asignar los números de direccionamientos tanto en la versión 4 como en la versión 6 del protocolo de internet, en bloques para las diferentes regiones a nivel mundial. Para Latinoamérica y caribe, la IANA asigna un segmento de direccionamiento el cual es gestionado por la LACNIC (*LatinAmerica and Caribbean Network Information Center*). [32]

En este orden de ideas, y de acuerdo a las clases de direccionamiento IP, la investigación se fundamenta en las bases establecidas por los entes generadores y administradores de direccionamiento de números para el protocolo IP para la asignación de direcciones IP, en este caso de carácter privado por tratarse de direcciones sin clase que utilizan VLSM[8] para IPv4 y de direcciones globales unicast para Ipv6.

2.4 Estado del Arte

2.4.1 Direccionamiento IP y calidad de servicio QoS en IPv6

En el ámbito de la exploración del protocolo de internet se encuentran varios autores que han realizado diferentes investigaciones paralelamente en diversos campos, como

[8] VLSM: *Variable Length Subnet Mask;* Máscara de subred de longitud variable.

comunicaciones *dual-stacking,* IPv6 para redes móviles, implementaciones en seguridad, etc. Huang Chung-Ming et al., plantean un antecedente relevante para el desarrollo de la presente investigación, con el estudio de un mecanismo de reenvío de video por capas aplicado a IPv6 para clientes móviles [33]. Dell P. plantea un escenario en el cual analiza a fondo la situación actual (2018) de la transición dual-stacking sobre dispositivos de red y cuestiona si el escenario a futuro podría ser desalentador desde el punto de vista operativo y económico para las compañías [34]. Hassan & Jabbar (2017) realizan un estudio de calidad de servicio QoS [35] en el cual abordan la creciente demanda de aplicaciones en tiempo real y el consumo de estas a través de los diferentes tipos de terminales que se conectan a la red de internet. Este estudio se enfoca en proponer mecanismos confiables de calidad de servicio dada la alta demanda de tráfico en tiempo real en la red y cómo la demanda de video streaming en tiempo real requiere incrementar los esfuerzos para encontrar los requerimientos de los usuarios finales. Sin embargo, se realiza en dos fases en las cuales se aplican parámetros de QoS desde la fuente del tráfico hasta los dispositivos finales. Esta política se basa en añadir una cabecera de capa de flujo en la trama IPv6 la cual es leída por los enrutadores para interpretar los requerimientos de tráfico. Así mismo, estas políticas de calidad de servicio finalmente se traducen en la calidad de experiencia QoE para los usuarios que consumen contenido. No obstante, el análisis de resultados arroja como resultado que es necesaria una estrategia de calidad de servicio que pueda mantener finalmente una calidad de experiencia positiva para el usuario, sugiere un trabajo orientado a servicios diferenciados *DiffServ.*

2.4.2 Contenido multimedia adaptativo

Si bien esta investigación sugiere un tipo de solución diferente a una de las temáticas planteadas en el presente documento enfocada al tráfico adaptativo, marca una referencia útil para establecer una idea del comportamiento del tráfico de transmisión de video en función de la tasa de transmisión o *bitrate*, incorporando variables presentadas en este tipo de transmisiones, tales como jitter, ancho de banda, entre otras. Savvas Papagiannidis et al., examinan como IPv6 podría afectar positiva o negativamente las aplicaciones, una de ellas: IPTv, y los posibles impactos e implicaciones de la difusión de televisión en [36]. Dujuan Gu et al., propone una arquitectura de red virtual VNET6 [37] con una evolución de red incremental. El objetivo de VNET6 es adaptar un gran espectro de aplicaciones y requerimientos. Como tendencia actual a investigar se encuentra que Yashuang Guo et al., proponen un esquema de caché dinámico escalable en el tiempo para streaming en redes vehiculares en la cual la adaptación de calidad de video en la capa de aplicación es desempeñada en una gran escala de tiempo mientras la tasa de transmisión sobre la capa física es desempeñada sobre una escala de tiempo mucho más pequeña en [38]. Lencse & Kadobayashi [39] plantean un modelo jerárquico descendente en el cual se indican categorías genéricas, analiza tecnologías de transición IPv6 y las implementaciones de estas tecnologías de transición. Elsa Macías y Álvaro Suárez [40] identifican y analizan diferentes protocolos utilizados para la transmisión de video streaming a través de redes *ad-hoc*, en donde proponen métodos de ahorro de batería y optimización de ancho de banda, así como la previsión de pérdida de paquetes utilizando el protocolo OLSR *(Optimazed Link State Routing)* mediante el análisis de paquetes con la herramienta Wireshark en la plataforma video player VLC[9] .

[9] VLC: *VideoLan Client.* Software de reproducción de contenido de fuente abierta, como parte de un proyecto académico que comenzó en Paris a mediados de los 90´s.

De acuerdo con un reporte publicado por Cisco [41], para el año 2020 el contenido que dominará internet será el de video, copando por hasta un 85% el tráfico total de internet. Para sobrellevar el creciente y acelerado crecimiento de este tipo de contenido en la red, aparecen las redes de distribución de contenido CDN, cuya infraestructura ha sido fortalecido en la última década. Según Y. Tian et al., las CDN´s *"son redes superpuestas de servidores que son desplegados en diferentes ubicaciones geográficas. En lugar de descargar contenidos directamente desde el servidor original, los usuarios finales acceden a este contenido por medio del servidor más próximo"* (2017). Esta referencia aporta una idea valiosa a la presente investigación como una posible solución presentada en la problemática del proyecto consistente en la ocupación del ancho de banda entre las dos sedes de la Universidad Santo Tomás que alojan los monitores que despliegan el contenido. Como se evidencia en las Figuras 1, 2 y 3, este sobreuso del canal de datos entre ambas sedes se da en gran parte por la transmisión de video streaming en las carteleras digitales ubicadas en la sede de Bucaramanga y que se interconectan con el servidor ubicado en el Campus Floridablanca. De acuerdo con [42], si todos los usuarios solicitaran contenido directamente a un único servidor, evidentemente en un momento dado se presentaría una congestión de la red, tal que los paquetes *request – reply* empezarían a perderse, lo que se resumiría en un inevitable colapso del servicio.

Esto no sólo aplica para las grandes plataformas de video streaming o video sobre demanda, tal y como se evidencia en las anteriores figuras, en una red a pequeña escala como la de la red de carteleras digitales de la Universidad Santo Tomás, también se evidencia este tipo de inconveniente si no se implementan políticas de calidad de servicio para que finalmente se traduzca en una óptima calidad de experiencia para el usuario. En este orden de ideas, se sugiere que una posible solución a esta problemática, al menos en primera instancia, sería la ubicación

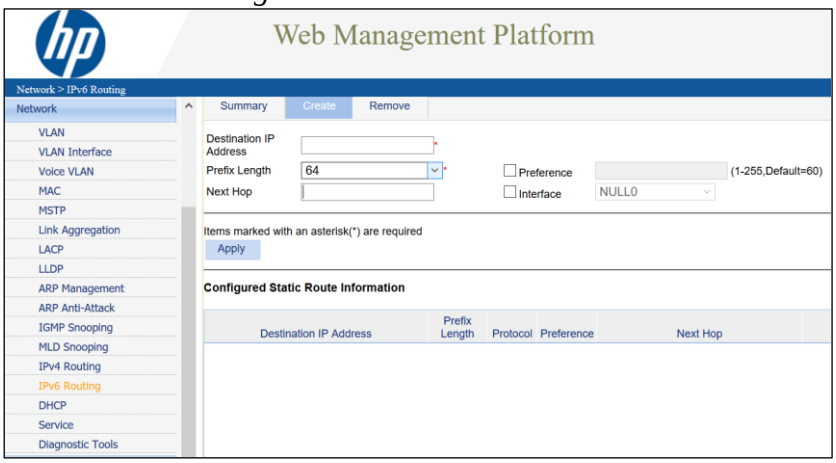
de un servidor de difusión de contenido en la sede de Bucaramanga. Con esto, teóricamente se evitaría la ocupación de ancho de banda que se viene presentando en el canal de datos pues ya no se estaría transmitiendo difusión Unicast entre el servidor y cada dispositivo, sino que existiría una sincronización únicamente entre ambos servidores.

2.4.3 Seguridad en la red

En el ámbito de la seguridad en la red, es necesario enfocar la atención en las vulnerabilidades que pueden llegar a presentarse en una red no sólo IPv6 sino también IPv4. La función de los Firewalls radica en brindar una protección desde el tratamiento y filtrado de paquetes, así como en la detección de diversos tipos de ataques a la red o amenazas como virus por medio de certificación de usuarios en tráfico entrante o saliente. De aquí que una falla en la seguridad de la red podría desencadenar en resultados adversos con efectos dramáticos en toda la red de una organización [43]. Diferentes técnicas son adaptadas a las condiciones del tráfico aplicando datos estadísticos calculados activamente para optimizar dinámicamente el orden de las reglas de filtrado de paquetes, dando explicación al orden de las reglas de firewall, así como del peso o prioridad de cada una dentro de las configuraciones. Al-Shaer E. (2014) [44] describe y compara las técnicas existentes de configuración de políticas de firewalls dinámicos basados en análisis de tráfico *on-line* y *off-line,* a través de un escenario real e igualmente dentro de un escenario simulado.

Dentro del contexto de la seguridad en la red interna del campus Floridablanca de la Universidad, se puede encontrar que la mayoría de los equipos de conmutación encargados de distribuir paquetes en la red a nivel de capa 3 del modelo TCP/IP, soportan IPv6 como se puede observar en las figuras 7 y 8.

Figura 7. *Herramienta IPv6 Routing en Switche Hewlett Packard.*



Sin embargo, si bien no tienen interfaces configuradas en IPv6, estas funciones están habilitadas, por lo menos para un 60% de los dispositivos de red en el campus que las soportan, el tráfico IPv6 puede pasar transparente en flujos 802.1Q9 por capa 2 o capa de enlace, viajando entre las VLAN´s distribuidas a lo largo del campus por los conmutadores. 9 IEEE 802.1Q; Estándar que define una arquitectura para Virtual Bridged LAN´s.

Figura 8. *Resumen de Interfaz IPv6 en Switche 3Com 4500*

```
[SW4_P1_SANTANDER]disp ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                          Physical   Protocol   IPv6 Address
Vlan-interface1                      down       down     Unassigned
Vlan-interface64                     up         down     Unassigned
Vlan-interface120                    up         down     Unassigned
[SW4_P1_SANTANDER]
```

Dado que las implementaciones en IPv6 son relativamente recientes, así mismo, quizá se encuentren vulnerabilidades en este protocolo, espacios donde un posible atacante encuentre la forma de evadir controles de seguridad IPv4 para atacar una red a través de IPv6 [45]. Los dispositivos con protocolo IPv6 activo o habilitado en alguna de sus interfaces utilizan protocolos de reconocimiento de su entorno de red mediante el descubrimiento de vecinos, así lo describe el protocolo sin estado NDP [4]. Este protocolo es usado entre otras cosas, para

facilitar la comunicación entre enlaces locales IPv6 y ubicar otros dispositivos o interfaces de equipos de comunicación sobre IPv6, detectar direcciones duplicadas y brindar confiabilidad acerca del estado de las interfaces o los hosts en la red. Sin embargo, los enlaces que utilizan este protocolo son susceptibles a ataques de red que deben ser tenidos en cuenta o de lo contrario dejarían vulnerable la red. De esta manera, la RFC 3971 [46], aboga por emplear una nueva versión de este protocolo, llamada SeND, la cual hace inviolable el proceso de descubrimiento de vecinos en la red IPv6. J. L. Shah (2019) [47] visita nuevamente este protocolo y revisa los retos de desempeño, así como también algunas propuestas factibles y recomendaciones para facilitar un despliegue práctico de SeND en redes IPv6 incluyendo también una mención grosso modo del protocolo en dispositivos móviles. De acuerdo con la investigación de Caiza et al., (año) los atacantes utilizan estrategias de escaneo por medio de la asignación de direcciones IPv6. En este sentido, es imperativo implementar planes de detección de intrusos en la red, en este caso (autores) año implementaron un sistema de seguridad perimetral dentro de una red local para asegurar anomalías a causas del protocolo IPv6 [48].

Tomando puntos de referencia en investigaciones acerca de sistemas de video streaming y protocolos de video adaptativo como DASH Protocol (*Dynamic Adaptive Streaming over HTTP*), M. Ki, J. Seok, and H. Y. Kim (2017) [49] plantea un antecedente relacionado con plataformas de video, en este caso para televisión digital terrestre en la República de Corea, cuyo escenario se espera soporte no sólo contenido multimedia a través de redes de banda ancha sino también para transmisión de sistemas de difusión bajo el estándar ATSC 3.0. Entrando un poco más a fondo sobre sistemas adaptativos de video, (M. Zhao *et al*) (2017) [50] propone un innovador sistema interactivo que permite que los usuarios cambien periódicamente los puntos de vista en la imagen de video. Si la nueva perspectiva no se encuentra disponible, se plantean

técnicas para que códecs vecinos suplan información temporalmente a sus vecinos desde su caché usando además el servicio DASH, el cual es un estándar de video adaptativo que permite ajustar la calidad de la transmisión de video de acuerdo con las condiciones de la red.

3. Metodología

Para el desarrollo de la presente investigación, y en función de las temáticas sobre las cuales se basa (análisis de calidad de experiencia de contenido multimedia, protocolo dinámico adaptativo, seguridad en redes y protocolos de internet IPv4 e IPv6), se acude a una metodología investigativa mixta que combina caso de estudio (*carteleras digitales*) e investigación experimental mediante pruebas guiadas en entorno controlado de laboratorio.

El método de análisis de información se lleva a cabo desde lo cuantitativo a través de edición y modificación del contenido multimedia a tratar, el establecimiento de los escenarios de red provistos para la implementación de los protocolos de internet (*dual stack*), entornos de ataques controlados a la red IPv6, así como también, los métodos de prueba provistos para el análisis de la calidad de experiencia. Por otra parte, desde el enfoque cualitativo, se aplicará una metodología de encuesta para colectar información mediante técnica de puntuación de opinión media y en análisis requerido aplicado a los resultados obtenidos con base en la comparativa del tráfico multimedia IPv4 versus IPv6.

Con base en la metodología de investigación y del método de análisis de la información propuestas, la metodología de obtención de la información resulta de carácter mixto, tomado del caso de estudio, encuesta y resultados experimentales.

Se presentan a continuación, cinco fases que permiten llevar a cabo el cumplimiento de los objetivos propuestos, lo cual se sintetiza en la siguiente tabla:

Tabla 2. Correlación de fases de la metodología con los respectivos objetivos específicos a cumplir.

Número	Fase	Objetivo Específico
3.1	Caracterización del tráfico multimedia	Elaborar un diagnóstico sobre el comportamiento de tráfico de streaming multimedia adaptativo IPv4 e IPv6
3.2	Implementación de protocolo dinámico adaptativo DASH	
3.3	Análisis de tráfico de contenido multimedia IPv4 e IPv6	
3.4	Análisis de seguridad de red en la transmisión de contenido multimedia en redes IPv6	Analizar parámetros de seguridad en IPv6
3.5	Evaluación de la calidad de experiencia QoE del servicio de streaming sobre IPv6	Evaluar calidad de experiencia de video streaming sobre IPv6

3.1 Fase 1. Caracterización del tráfico multimedia

- *Actividad 3.1.1* Adquisición de los contenidos multimedia desde plataformas web de código abierto.
- *Actividad 3.1.1* Conocimiento de la plataforma FFMPEG, a partir de la cual se generarán los códigos necesarios para la edición de los contenidos adquiridos.
- *Actividad 3.1.2* Edición del contenido multimedia. En esta actividad se generan los segmentos (recortes) en diferentes calidades (bitrate) a partir del video a utilizar en el laboratorio. Así mismo, se extrae el fichero de audio del archivo original (formato .mp3) antes de generar los segmentos de video.
- *Actividad 3.1.3* Compresión de los segmentos de video mediante la utilización de métodos de codificación en FFMEPG. Se aplican cambios a los formatos H.265 y H.264 para los diferentes segmentos de video generados.

3.2 Fase 2. Implementación de protocolo dinámico adaptativo DASH

- *Actividad 3.2.1* Identificación de herramienta DASH Player sobre la cual se ejecutarán los segmentos multimedia generados anteriormente.
- *Actividad 3.2.2* Generación de los formatos de descripción de presentación del contenido (MPD) desde FFMPEG, los cuales permitirán ejecutar los segmentos de contenido para el streaming adaptativo y dinámico [15].
- *Actividad 3.2.3* Implementación de protocolo DASH a través de la herramienta DASH Player mediante la incorporación de los ficheros MPD generados previamente.

3.3 Fase 3. Análisis de tráfico de contenido multimedia IPv4 e IPv6

- *Actividad 3.3.1* Adaptación de entorno de red *dual stack* (IPv4 e IPv6) en el cual se genera un escenario cliente – servidor que permita analizar el tráfico de red dentro del mismo.
- *Actividad 3.3.2* Análisis comparativo del tráfico de red mediante aplicación de métricas objetivas: retardo, Jitter y PSNR (*Peak Signal-to-Noise Ratio*).
- *Actividad 3.3.3* Documentación de los resultados observados a partir de las actividades planteadas en las fases 1, 2 y 3.

3.4 Fase 4. Análisis de seguridad de red en la transmisión de contenido multimedia en redes IPv6.

- *Actividad 3.4.1.* Identificación de los parámetros de configuración de red y de calidad de servicio utilizados en la fase 3 dentro del entorno cliente – servidor, que permitirán caracterizar los aspectos de seguridad.

- *Actividad 3.4.2.* Caracterización de vulnerabilidades de red en el marco de la seguridad en la red IPv6.
    - Actividad 3.4.2.1. Implementación de ataque *Neighbor Advertisement Spoofing.*
    - Actividad 3.4.2.2. Implementación de ataque mediante SLAAC.
    - Actividad 3.4.2.3. Implementación de ataque de seguridad mediante DHCPv6.
    - Actividad 3.4.2.5. Implementación de ataque de seguridad mediante WPADv6.
- *Actividad 3.4.3*. Documentación de los resultados obtenidos durante la fase 4.

3.5 Fase 5. Evaluación de la calidad de experiencia QoE del servicio de streaming sobre IPv6 bajo el modelo comparativo DSIS[10] [51]

- *Actividad 3.5.1*. Selección de dos contenidos de video diferentes en su formato original reproducidos desde la fuente.
    - Actividad 3.5.1.2. Selección de pruebas del sistema que deberían ser aplicadas: las pruebas a realizar serán análisis de percepción del espectador al contenido fuente (SRC) y posteriormente en comparativa a los segmentos de video procesados (PVS)

[10] DSIS: *(Double Stimulus Impairment Scale*). Procedimiento que permite realizar un método comparativo entre un contenido multimedia fuente (*perfecto*) y el mismo contenido, pero con imperfecciones propias del resultado de la transmisión o presentación del contenido.

- Actividad 3.5.1.3. Aplicación de configuraciones al contenido fuente, lo cual resultará en las secuencias de video procesadas de prueba. Estas configuraciones hacen referencia a la modificación del bitrate para tres diferentes calidades de imagen.
- Actividad 3.5.1.4. Implementación de pruebas basadas en utilización de software orientado a emular parámetros subjetivos con base en consideraciones perceptuales de la vista humana y elementos del entorno.
- Actividad 3.5.1.5. Comparativa de los resultados a partir del análisis de los parámetros VQM, PSNR y SSIM, entre el contenido original y el contenido procesado.
    a) *Se presentará el contenido original del primer video y posteriormente, los segmentos de video procesados del mismo. Seguidamente, se presentarán de la misma manera, el contenido subsiguiente.*
- *Actividad 3.5.2*. Documentación de resultados de la fase cinco.
- *Actividad 3.5.3*. Redacción de las conclusiones del trabajo de investigación y del trabajo a futuro.

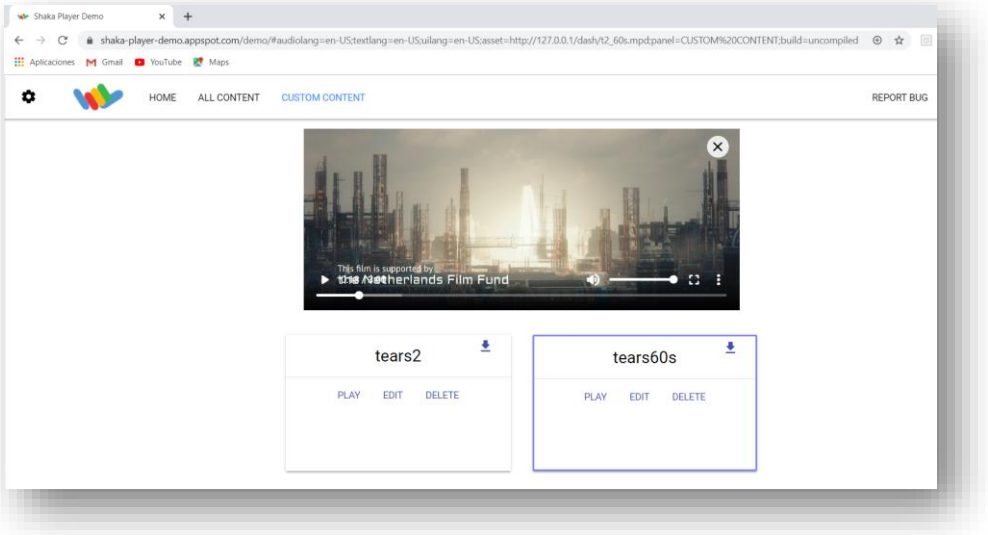
4. Resultados

En el siguiente capítulo se presentan los resultados obtenidos en cada etapa del desarrollo de la investigación a partir de la metodología propuesta en el apartado anterior. Una vez finalizada cada fase, se muestran los aportes más representativos a la investigación y que, en general, vertebran la integración de los obtenidos, con los cuales se dará paso al análisis de estos y sus respectivas conclusiones.

Para un primer ejercicio, se genera un archivo manifiesto con dos segmentos de video producidos a partir de un archivo original ("*Tears of Steel*"), cada uno de 30 segundos y cada

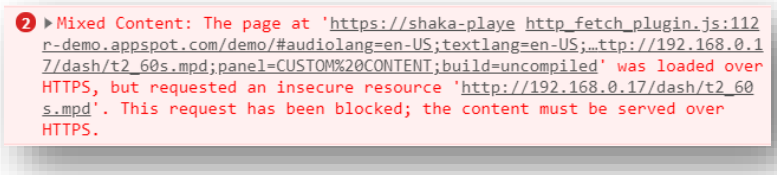
uno de estos con tres calidades diferentes (360p, 720p y 1080p). El cliente crea una nueva solicitud en el reproductor Shaka Player:

Figura 9 *Configuración cliente DashPlayer. Llamado al archivo MPD.*



Para lograr alcanzar el servidor a través del reproductor Shaka Player, la solicitud debe ser realizada a través del protocolo HTTP seguro (HTTPS), ya que esta herramienta web es cargada a través de este último y al solicitar los recursos al servidor, si este los sirve con HTTP, se presentará un error de contenido mixto desde el navegador en el lado del cliente, a quién se bloqueará el contenido solicitado (*request),* y se informará que este contenido debe ser servido con HTTPS mediante certificado SSL[11] como se muestra en la siguiente figura:

Figura 10. *Mensaje de error de contenido mixto. El request es bloqueado para el cliente hasta tanto el contenido no sea servido con HTTPS.*



[11] SSL: Secure Socket Layer. Protocolo que permite la encriptación y cifrado de la información entre cliente y servidor. [42]

En este primer ejercicio no se configuran parámetros de calidad de servicio ya que, en este escenario, se pretende transmitir el contenido multimedia como si se tratara de tráfico *best effort* con la finalidad de analizarlo bajo estas condiciones. Igualmente, cabe recalcar que, al tratarse de una red local dentro de un entorno controlado de laboratorio, no existen múltiples afectaciones en la transmisión que sí se pueden presentar en un entorno de red real como el de la Universidad.

Estos factores, como se ha mencionado en la introducción y la descripción del marco problémico del presente documento, están determinados entre otros, por las condiciones del medio de transmisión, el cual determina igualmente la forma de acceso al medio para la información, el tipo de tecnología que se utilice para la codificación de la información, el ancho de banda disponible en el canal de comunicaciones en un momento determinado, la capacidad máxima de transmisión del canal de comunicaciones determinada por las interfaces de los equipos de comunicaciones, los valores de ancho de banda asignados a diferentes servicios, la segmentación de la red, tunelización, parámetros de seguridad y capacidad de procesamiento de los equipos de red.

No obstante, algunos de los parámetros mencionados anteriormente podrán ser analizados a pesar de tratarse de un entorno controlado de laboratorio, en donde las condiciones se aproximan más a un entorno “ideal”.

4.1 Caracterización del tráfico y adquisición del contenido multimedia.

El tratamiento de contenido se lleva a cabo utilizando plataformas de código abierto que permiten la descarga de archivos de video en diferentes calidades y en diferentes contenedores

(mov, mp4, yuv, etc.). Con estos archivos es posible realizar la generación del contenido multimedia.

La preparación del contenido se consigue diferenciando y manipulando el bitrate de los archivos. Los archivos de video se cambian de contenedor para analizar si existe alguna diferencia en términos de calidad o más puntualmente, de tamaño del archivo.

Por otra parte, los archivos descargados originalmente vienen codificados con H.264 pero se cambia el códec a H.265 para posteriores análisis, pues en teoría, presentará una mejora significativa en el tamaño del archivo sin alterar la calidad de reproducción [52]. De ser posible, sería una alternativa viable para disponer de la mejor calidad de contenido posible a un menor bitrate.

Los ficheros obtenidos de contenido multimedia para las pruebas realizadas son los siguientes:

a) Tears of Steel (Trailer en formato HD (720p) y contenedor .mp4). Tomado Proyecto Mongo [53], presenta la herramienta *Open Movie*, la cual permite descargar, editar y compartir libremente el contenido. Este video tiene una duración de 12 minutos.

Figura 11. *Póster de Tear of Steel (2013)*

Tomado de [53].

b) Sintel (Trailer en formato HD (720p) y contenedor .mkv). Tomado de la plataforma *durian.blender.org*, con duración de 14 minutos.

Figura 12. *Póster de Sintel (2013).*

Tomado de [54].

Conocimiento de la Plataforma FFMPEG:

La herramienta utilizada para la compresión y codificación de video fue FFMPEG, software de código abierto desarrollado en GNU/LINUX [55], pero se puede compilar en otros sistemas operativos. Este software permite modificar o manipular el contenido, realizar recortes en diferentes puntos de un video o cambiar el tipo de contenedor.

El objetivo de la codificación y compresión del contenido es obtener segmentos de video que conserven su calidad de video a la menor tasa de bit posible. En esta actividad, se debe tomar como parámetro objetivo el bitrate del video para generar diferentes calidades, ya que se ha obtenido un video en calidad 720p (1280*720p).

Edición del Contenido Multimedia y Compresión de los Segmentos de Video:

El archivo original original *tears_of_steel_1080p.mov*, tomado de [53], y su contendor es .MOV. Se procede a cambiar el contenedor a .MP4 mediante la sentencia *ffmpeg -i [archivo de entrada .MOV] -report [archivo de salida .MP4].* El siguiente paso será analizar si aparte del cambio del contenedor, existen otros parámetros que se han podido modificar con el procedimiento, como los cuadros por segundo o tamaño del archivo, con *ffprobe [nombre del archivo de salida .MP4].* Una vez el archivo MP4 sea generado, se debe generar un recorte de tres minutos del video original, cabe aclarar que el archivo original tiene una duración de doce minutos y catorce segundos, lo cual significa que el archivo es muy extenso para ser procesado.

La generación del recorte se da por medio de la método *ffmpeg -i* [archivo a recortar] -ss [inicio en hrs:min:seg] -t [duración en segundos] -c:v copy -c:a copy [archivo de salida .MP4].

Antes de modificar el archivo correspondiente al recorte de tres minutos, se analiza con el método *ffprobe* para verificar las características del video. Se debe extraer el audio del video usando el método *ffmpeg -i* [archivo de entrada]-c:a copy -vn [archivo de salida MP4]. Con esto, se pueden generar ahora los segmentos de diferentes calidades modificando el bitrate para cada caso. Se pretende generar tres calidades diferentes para el archivo original. Con la siguiente sentencia se procederá a realizar los segmentos:

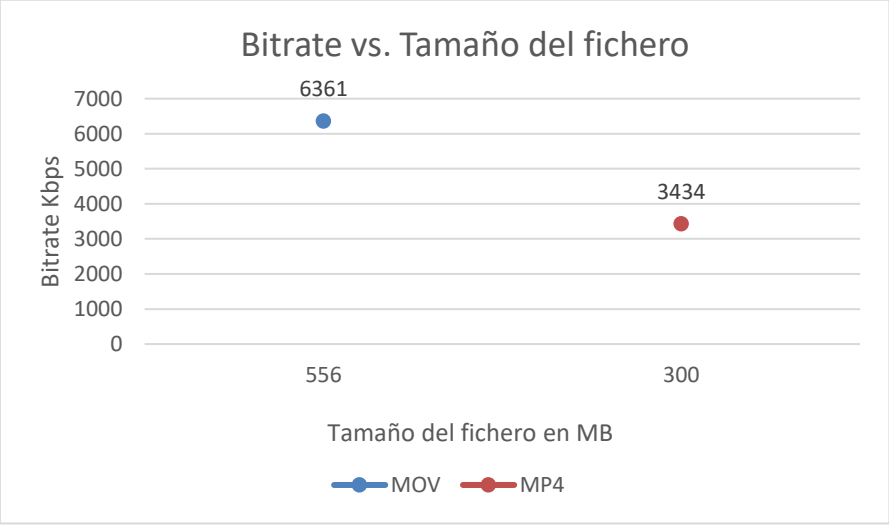
ffmpeg -i [archive de entrada] -an -c:v libx264 -x264opts keyint=24:min-keyint=24:no-scenecut -b:v [tasa de bit] -maxrate [máxima tasa de bits] -bufsize [tamaño del búfer] -vf scale=-1:[escala del video] [nombrar archivo de salida].

Paralelamente, como práctica adicional se codificó cada archivo en HVEC (H.265), desde el original hasta los segmentos generados a partir de la modificación del bitrate, para analizar lo que sucede al cambiar de códec y cómo afectaría esto en la reproducción del contenido cuando ya se encuentre en servicio.

A partir de la edición de la codificación y edición del contenido dispuesto, se logra obtener información que permite realizar una comparación en términos de rendimiento versus calidad. Algunos de los parámetros objetivos para tener en cuenta son *bitrate*, resolución, tamaño del fichero, tiempo de codificación, QP[12] y CRF[13].

En primera instancia, se comparan ciertas características del archivo original descargado en formato .mov con respecto al mismo archivo comprimido en contenedor .mp4 y se observa lo siguiente:

Figura 13. *Bitrate versus Tamaño del Fichero para los Contenedores .mov y .mp4.*

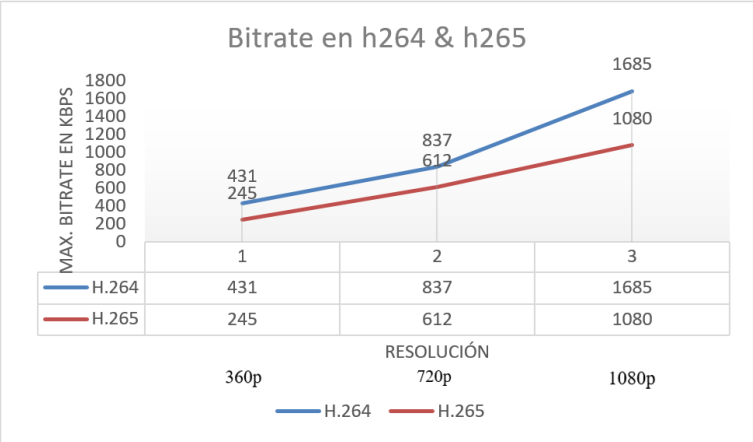


Luego de cambiar el contenedor del archivo a MP4, se observa que su tasa de bit disminuye y por tanto su tamaño a casi el 50%.

En el proceso de codificación y compresión de video se tomó como muestra el fichero anterior en formato MP4 y se recortó a una duración de 3 tres minutos. Con este recorte, se generaron tres ficheros h.264 y tres h.265 los cuales fueron comprimidos a diferentes calidades para cada códec. Se obtuvieron los siguientes resultados:

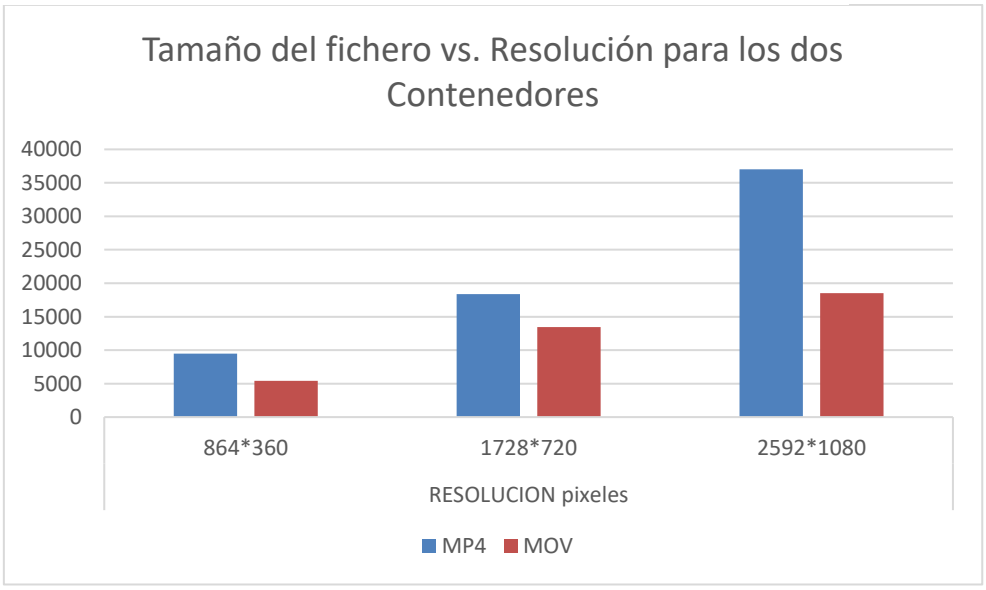
Figura 14. *Desempeño del bitrate en los códecs h.264 y h.265.*

[12] QP (*Quantization Parameter*), parámetro que configura la cantidad de bits que deberían alojarse para codificar cada bloque de imágenes
[13] *Constant Rate Factor*. Factor de tasa constante. Es la calidad por defecto o control de tasa, configurada para los códecs H.264 y H.265.



Otra forma de representar los resultados obtenidos hasta aquí es sintetizar el tamaño del fichero versus el formato de compresión de video. En la siguiente gráfica se puede observar la relación entre los formatos de compresión de video y el tamaño del fichero en función del contenedor a utilizar.

Figura 15. *Relación entre tamaño del fichero, resolución y contenedor de video.*

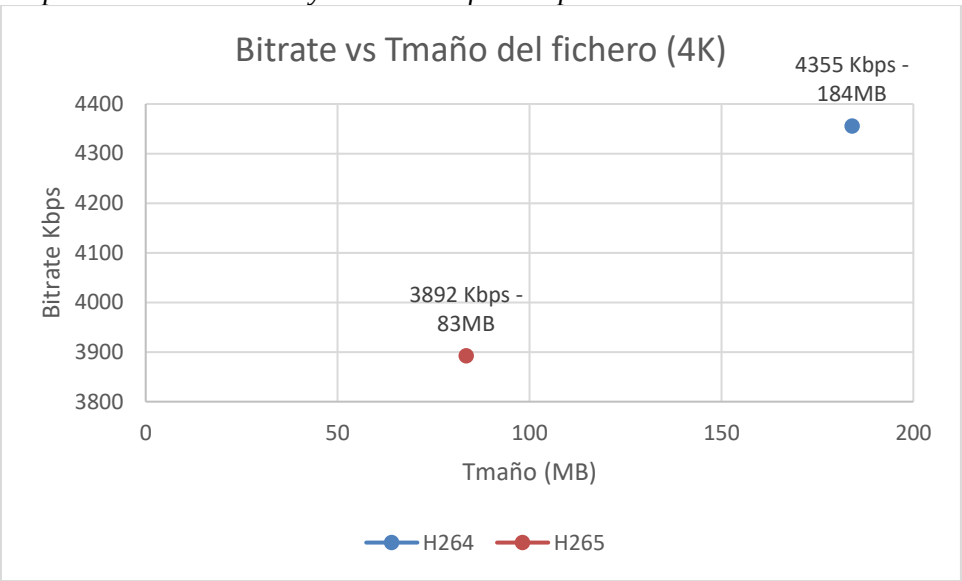


Se comprueba que el códec h.264 utiliza una mayor tasa de transmisión con respecto a h.265 y con una aparente tendencia a aumentar la diferencia de bitrate versus calidad, lo cual conlleva a la siguiente prueba que consiste en obtener información a partir de la comparación del

rendimiento de ambos códecs aplicada a un fichero con resolución 4k (4096*1744p), la cual se aplica como aporte adicional a las actividades propuestas en la Fase 1, igualmente con enfoque completamente experimental y con acotamiento estrictamente a esta fase, ya que el reproductor DASH no soporta contenidos en esta calidad.

En el siguiente gráfico se muestra la comparativa entre la tasa de bits y los códecs utilizados para el experimento en 4K, lo que arroja como resultado dos valores de tamaño de fichero:

Figura 16. *Comparación entre bitrate y tamaño del fichero para 4K.*



Esta vez se ha toma como muestra un video en 4K el cual fue recortado igualmente a 3 minutos. Al codificar el video, la diferencia en tamaño reduce notablemente en la medida que su bitrate también lo hace. Sin embargo, para percibir la diferencia real en la transmisión del video, es necesario contar con una pantalla que soporte tal resolución, pues si bien el tamaño del fichero disminuye, también lo ha hecho su tasa de bit y esto puede afectar ciertamente la calidad de experiencia.

En conclusión, se ha conseguido evidenciar que a partir de la codificación del contenido multimedia en H265, se reduce los parámetros expuestos en este apartado (tasa de bits y

tamaño) para las diferentes resoluciones, manteniendo la misma calidad del formato propuesto para cada uno de los escenarios, en comparación con el códec H264.

4.2 Implementación Protocolo Adaptativo DASH (Dynamic Adaptive Streaming over HTTP) e identificación de herramienta DASH PLAYER y generación de archivo MPD.

La siguiente actividad consiste en servir el contenido utilizando un reproductor DASH, por medio de Shaka Player, diseñado para Google Chrome. Este reproductor interpreta un archivo MPD generado mediante la herramienta MP4BOX, el cual genera un script de cada uno de los segmentos generados, en el que se compila las características de cada uno de los archivos de video y del archivo de audio. Shaka Player reproduce el contenido de lado del cliente, el cual es servido desde el archivo *manifest.mpd* por el servidor, en este caso *Apache.*

Los ficheros generados en diferentes calidades para cada códec ahora serán compilados en un archivo MPD (*Media Presentation Description*), el cual organiza los segmentos creados e incorpora el archivo de audio para ser reproducidos en el explorador, utilizando como reproductor DASH a *ShakaPlayer*. Este reproductor basado en *Google Chrome* reproduce los segmentos DASH, a partir del archivo MPD generado.

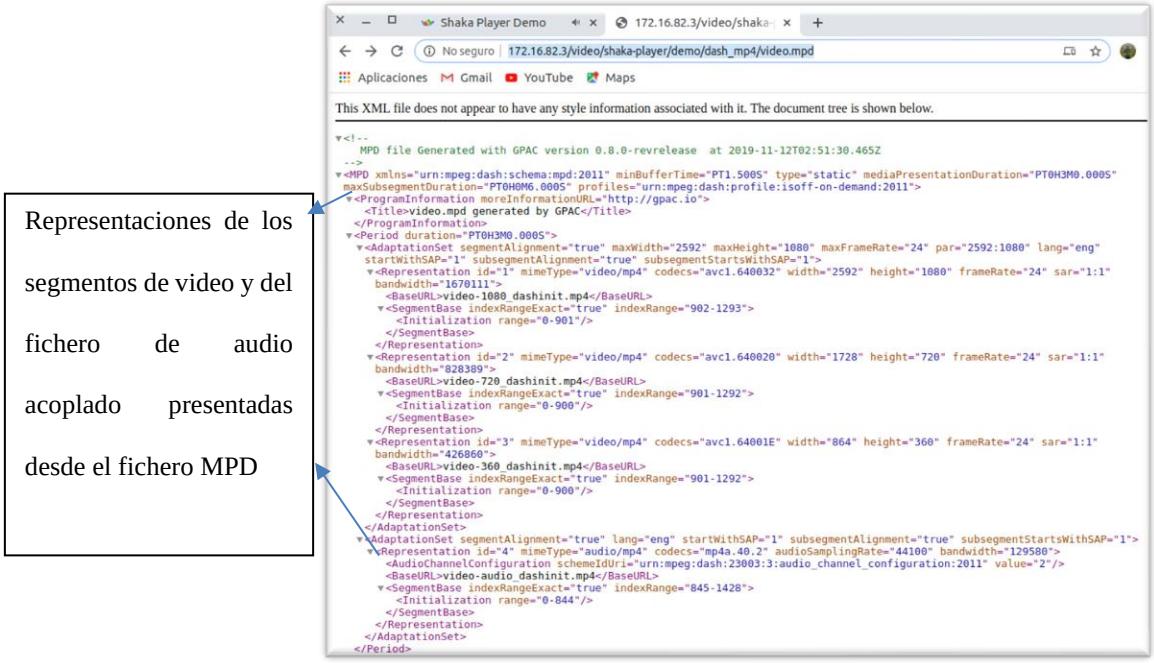
La generación del archivo MPD se produce desde FFMPEG mediante la siguiente sentencia:

MP4Box -dash 4000 -rap -frag-rap -profile onDemand -out *video_out.mpd video_in360p.mp4 video_in720p.mp4 video_in1080p.mp4 audio_in.mp4,* en la cual se determina el archivo de salida .mpd cn base en la compilación de los tres segmentos de video generados .mp4, así como también del fichero de audio .mp4.

Con esto, se tiene una primera aproximación a la creación de una topología tipo cliente – servidor y se puede pasar al análisis y comparación del comportamiento del tráfico multimedia adaptativo DASH entre IPv4 e IPV6.

Como apartado adicional, se debe agregar que el equipo cliente solicitará los ficheros necesarios al servidor a través del navegador, el protocolo DASH se encargará de analizar la capacidad de flujo de datos con base en la cual servirá la calidad de video soportada. Esto se lleva a cabo implementando, en etapa experimental, un servicio Apache en XAMPP desde el server (*equipo con S.O Windows 10*), desde el cual será llamado el archivo MPD como se muestra en la sigueinte ilustración:

Figura 17. *Lectura de la ruta del archivo MPD desde el navegador.*

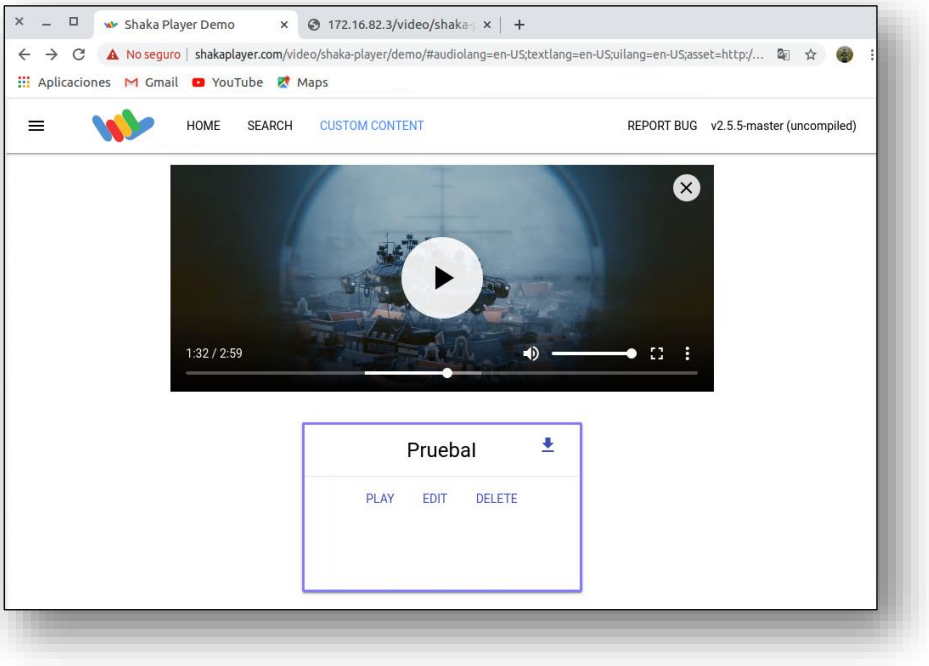


En un primer momento de la implementación del protocolo adaptativo, se descarga e instala la herramienta XAMPP compatible con Windows (*entorno de operación*), Linux y

MacOS, sobre la cual se alojará una carpeta con el manifiesto MPD y los respectivos *dash_init* que corresponden a los segmentos de video y de audio que se concatenarán desde el navegador.

Luego de aplicar la respectiva configuración del servidor Shaka Player (*Xampp*), se crea la compilación de los archivos correspondientes al MPD, es decir, aquellos ficheros que serán llamados por el MPD desde la ruta que se muestra en la imagen anterior.

Figura 18. *Reproducción DASH para Tears of Steel desde Shaka Player.*

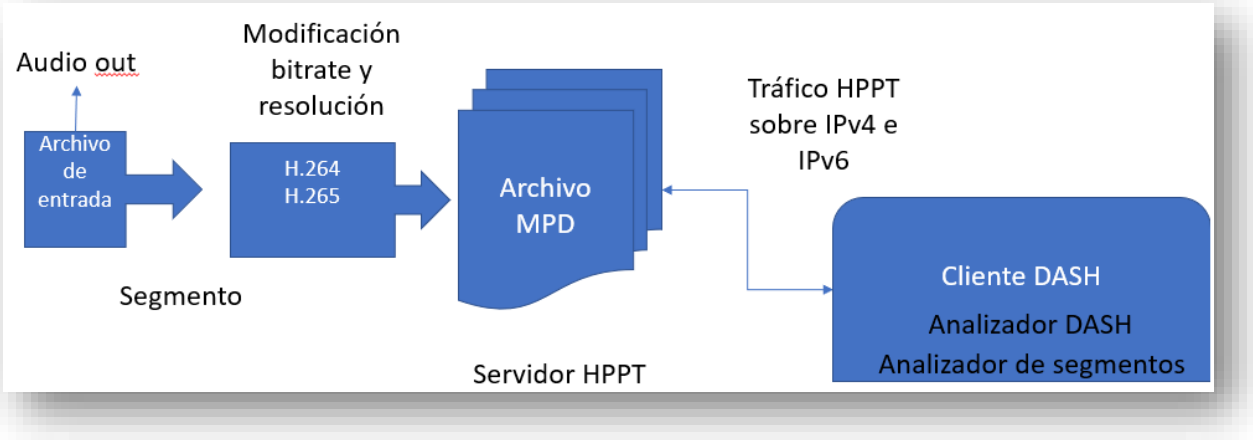


El archivo manifiesto MPD es un XML que describe los segmentos de las representaciones de los archivos de audio y video, además para lograr la reproducción DASH, es necesario un archivo de inicialización y uno de segmento, ambos contienen las cabeceras necesarias para decodificar los bytes en segmentos y a su vez, los archivos reproducibles que incluyen tantos *tracks* de audio y video como sean necesarios. Sin embargo, para la demostración práctica, se ha empleado un único fichero de audio que se concatena con todos los segmentos de video generados de manera ordenada.

Este procedimiento se realiza igualmente para el segundo fichero de contenido propuesto, Sintel.

Finalmente, en la figura **17** se aprecia la arquitectura del protocolo DASH implementada. Se ha configurado el servidor HTTP mediante el servicio XAMPP, adaptando el contenido multimedia a DASH y generando los segmentos y el archivo MPD a fin de analizar la comparativa de tráfico de los protocolos Ipv4 e Ipv6 para los diferentes códecs por medio de la transmisión en un entorno local de red.

Figura 19. *Esquema general de la arquitectura DASH aplicada al proyecto.*



4.3 Comparación de tráfico de streaming multimedia adaptativo entre IPv4 e IPv6.

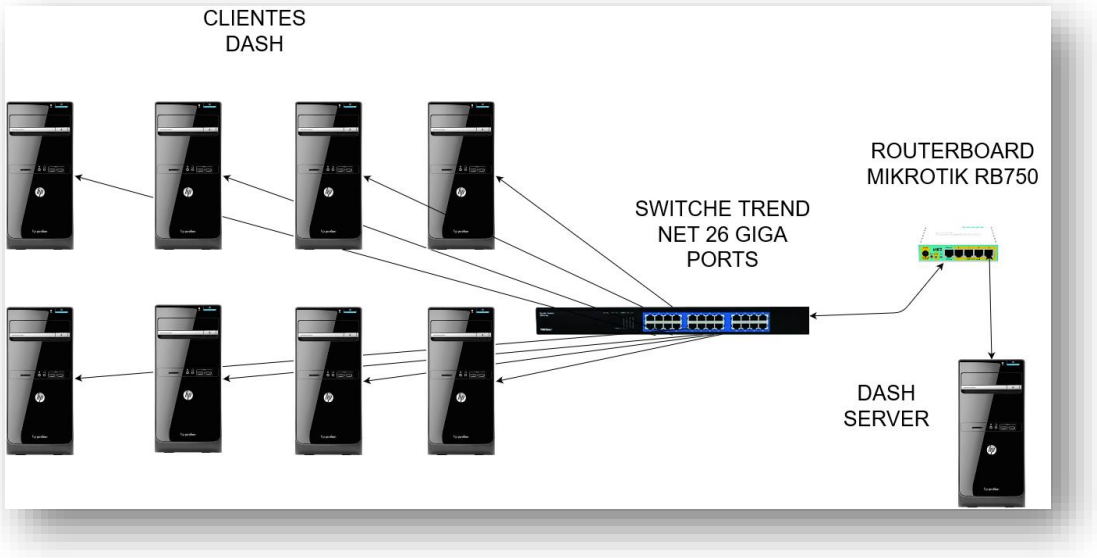
Con el contenido listo para ser solicitado al servidor Apache, se procede a configurar un entorno de red *dual stack* en la que coexistan los protocolos de internet IPv4 e IPv6 para realizar la comparación y análisis del comportamiento del tráfico de streaming en cada uno de ellos, midiendo como parámetros objetivos el retardo (*delay*), Jitter y el PSNR.

El entorno de red se genera a partir de un RouterBoard Mikrotik 750GL, el cual permite la conectividad a través de ambos protocolos, IPv4 e Ipv6. Con el servicio en marcha dispuesto desde un escenario de laboratorio, específicamente en el laboratorio de Telecomunicaciones de la Universidad Santo Tomás, se han configurado 8 equipos dentro de un dominio de red para

IPv4 y para Ipv6 gestionados desde el router mencionado anteriormente. Estos clientes solicitan contenido al servidor inicialmente en IPv4 y posteriormente en Ipv6 para realizar la lectura del tráfico mediante las herramientas Wireshark y Analizador de Tráfico de MikroTik.

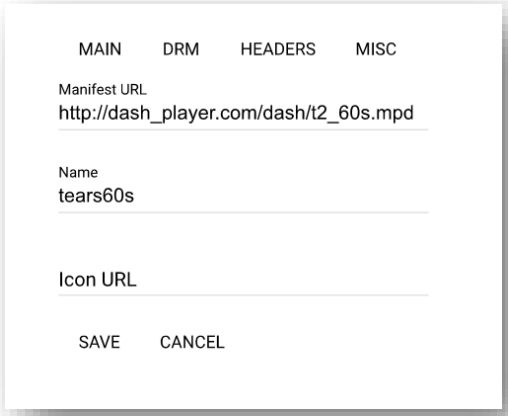
A continuación, se presenta la topología de red implementada en el entorno de laboratorio:

Figura 20. *Entorno de laboratorio. Topología de red*



Cada cliente realiza la solicitud al servidor a través de *Shaka Player,* una herramienta web con la que, además, se cuenta con aplicativo de escritorio. Es preciso conocer la ruta del archivo manifiesto MPD en el servidor para que se genere un socket ordenado desde el servidor.

Figura 21. *Configuración del Cliente Dash Player. Llamado al archivo MPD.*



La validación de la adaptación dinámica del tráfico se realiza por medio de la limitación de la capacidad máxima de transferencia de datos del canal, la cual se configura en el enrutador que gestiona la red local y se logra por medio de la herramienta *queues* o colas de tráfico. Este parámetro de configuración permite establecer tres valores diferentes del ancho de banda para la subred IP establecida para el laboratorio. Con estas variantes de ancho de banda es posible entonces emular un entorno real de tráfico IP en el que, debido a condiciones de los medios de transmisión, equipos de comunicación o conmutación de paquetes, topologías de red, saltos a través de la red, cantidad de usuarios conectados a la red, entre otros, el flujo de transmisión de bits por segundo se ve afectado negativamente presentando retardos en la transmisión misma que se puede traducir en la disminución de la calidad de la presentación del contenido.

Con base en esta configuración, se propone la siguiente estructura para el análisis de tráfico IPv4 e IPv6 en función de la calidad de contenido multimedia servido[14]. El análisis se presenta en la tabla 3, la cual presenta la relación del Jitter para la transmisión de los segmentos en diferentes formatos de calidad, bajo las tasas de transmisión propuestas y mediante la

14 Calidad del contenido multimedia. En la tabla se incluyen segmentos en calidad 3840 * 2160 píxeles como valor agregado al análisis del comportamiento del tráfico.

utilización de los códecs H.264 y H.265, así mismo, realizando la comparativa entre IPv4 e IPv6. Por otra parte, se presenta en la tabla 4, la relación PSNR bajo los mismos parámetros, exceptuando la transmisión de datos (IPv4/IPv6), con base en el estudio analítico de la conmutación de paquetes de tamaño fijo. Estos valores son obtenidos mediante la herramienta FFMPEG a partir de la comparación entre el fichero de entrada (segmento del video original recortado a 30 segundos) y el fichero de salida (segmento de video comprimido a diferentes tasas de bit y resolución) tanto para el protocolo IPv4 e IPv6.

Tabla 3. *Relación del Jitter (variación del retardo en milisegundos) en la transmisión del tráfico multimedia IPv4 e IPv6 con parámetros QoS (Colas de tráfico aplicadas a diferentes formatos de resolución) preconfigurados.*

Calidad / **Colas de Tráfico**	**360P**		**720P**		**1080P**		**2160P**		**Protocolo de Internet**
Q1 (256Kbps)	3,0651	2,3491	3,7133	3,4089	8,8080	6,5722	8,1082	7,8812	**IPv4**
	3,1227	2,1598	3,6956	3,3578	8,9758	6,8521	7,7512	7,6250	**IPv6**
Q2 (512Kbps)	2,4470	1,8723	5,4771	3,0441	7,4002	4,6881	6,2966	5,3565	**IPv4**
	2,3459	1,9875	5,3155	2,9120	6,9856	4,7852	6,3120	5,1549	**IPv6**
Q3 (1000Kbps)	1,6487	1,6053	4,9067	3,3884	7,3398	4,5395	7,9800	5,6799	**IPv4**
	1,5985	1,8512	4,5695	3,2458	7,3115	4,5060	7,8564	5,6145	**IPv6**
Compresión	**H-264**	**H-265**	**H-264**	**H-265**	**H-264**	**H-265**	**H-264**	**H-265**	

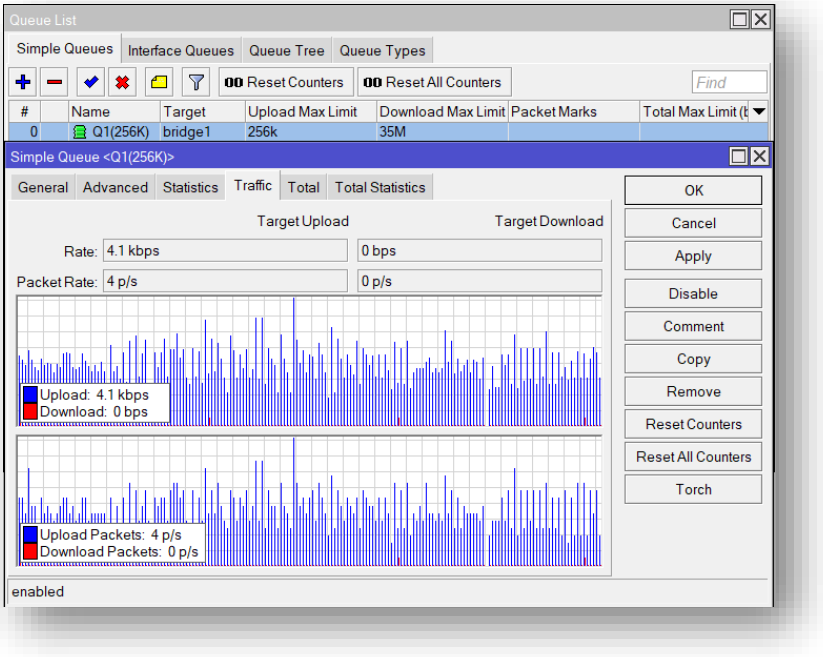
Nota: se permite apreciar la variación del tiempo de transmisión para las calidades de video utilizadas con respecto a la aplicación de un códec específico, con lo cual puede observarse que:
a. Disminución del bitrate para cada una de las colas en H.265 frente a H.264
b. Disminución del bitrate mediante la transmisión de IPv6 frente a IPv4

Tabla 4. *Relación del PSNR (Relación Señal a Ruido - Pico) en la compresión del contenido multimedia entre los ficheros de entrada segmentados a 30s y los respectivos ficheros de salida comprimidos en H264 y H265.*

Calidad	**360P**		**720P**		**1080P**		**2160P**	
Bitrate								
1024k	46.1384	45.2103	48.1620	47.2033	48.5164	46.2660	50.2561	48.9897
512k	40.1258	40.0215	43.3784	44.6001	43.7328	43.6690	45.8459	45.8901
256K	38.4381	35.1984	39.1503	38.6881	39.6102	37.7590	41.9521	41.1521
Compresión	**H-264**	**H-265**	**H-264**	**H-265**	**H-264**	**H-265**	**H-264**	**H-265**

Nota: La tabla presentada muestra la comparativa PSNR existente entre los ficheros de entrada y salida antes y después de ser comprimidos con un códec específico. Se aprecia que el PSNR disminuye con H.265 con respecto al fichero de entrada en comparación con H-264. Este resultado se obtiene localmente, es decir, antes de ser transmitido mediante IPv4 e IPv6.

Figura 22. *Cola de tráfico IPv4 en producción.*



En conclusión, se ha propuesto un entorno controlado de laboratorio bajo la arquitectura cliente servidor mediante protocolos de transmisión de capa de red IPv4 e IPv6 a fin de lograr la comparativa de la eficiencia de estos. La figura 22 muestra la cola de tráfico Q1 a 256Kbps en IPv4 para la transmisión de contenido en la red mostrada en la figura 20. En este entorno se configuró un fichero de entrada a partir de segmentos (recortes) de video bajo la utilización de los códecs H.264 y H.265. Así mismo, se utilizaron tres tasas de bit distintas que permitieran diferenciar la capacidad de las interfaces de red a partir de encolamiento de tráfico para las calidades propuestas en el ejercicio.

Con lo anterior, se pudo evidenciar la disminución del jitter en la transmisión de contenido multimedia a través del protocolo IPv6 en comparación con IPv4 para cada formato de calidad configurado en cada una de las colas de tráfico propuestas, tanto para H.264 como para H.265.

Adicionalmente, se permite apreciar mejoría en la relación PSNR para los parámetros mencionados anteriormente y observados en la tabla 4, con la salvedad de que estos valores se obtuvieron a partir de la comparación del fichero de entrada frente a los formatos generados a la salida desde el mismo hardware, es decir, sin ser transmitidos a través de la red.

4.4 Análisis de seguridad de red en transmisión de contenido multimedia en redes IPv6

4.4.1 Identificación de los parámetros de configuración de red y de calidad de servicio

La implementación de una red IPv6 incorpora nuevas preocupaciones en términos de seguridad de la red. A pesar que la seguridad para el protocolo IPv6 es implementada a través de políticas por defecto que están configuradas de fábrica en los dispositivos perimetrales, la seguridad de la red perimetral e interna está basada en el protocolo IPv4 y sus políticas son

prioritarias, por lo cual, se hace necesario un diagnóstico de la seguridad de la red llevando a cabo un ataque simulado en un entorno controlado de laboratorio utilizando la herramienta EvilFoca de ElevenPaths[15], el cual afectaría las capas 2 y 3 del modelo TCP/IP, aplicado al escenario cliente – servidor dispuesto en la actividad anterior. La importancia de esta simulación radica en qué medidas de seguridad de red se pueden aplicar en la infraestructura de red actual de la Universidad con el fin de prevenir algún tipo de ataque basado en IPv6.

4.4.2 Caracterización de vulnerabilidades de red en el marco de la seguridad en la red IPv6

Para llevar a cabo el ataque a la red IPv6 en el entorno de laboratorio controlado, e emplean cuatro variantes del método MIT (*Man In the Middle)*:

4.4.2.1 Neighbor Advertisement Spoofing

En esta modalidad de ataque, el atacante envía a sus víctimas información ICMPv6 falsa con el fin de conducir cualquier tráfico hacía la dirección IP de la víctima como se muestra en la figura 23 y se lleva a cabo por medio de la herramienta Evil Foca en el panel de administración de la figura 24.

Figura 23. *Captura de tráfico Neighbor Advertisement ICMPv6 falso desde el equipo atacante hacía el equipo objetivo.*

[15] Equipo de Ciber Seguridad Tech de Telefónica.

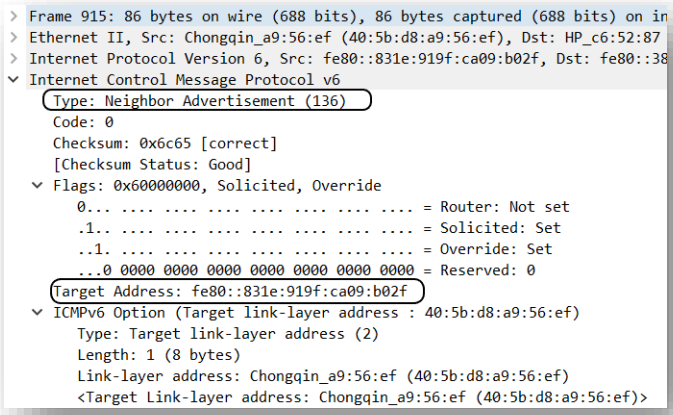
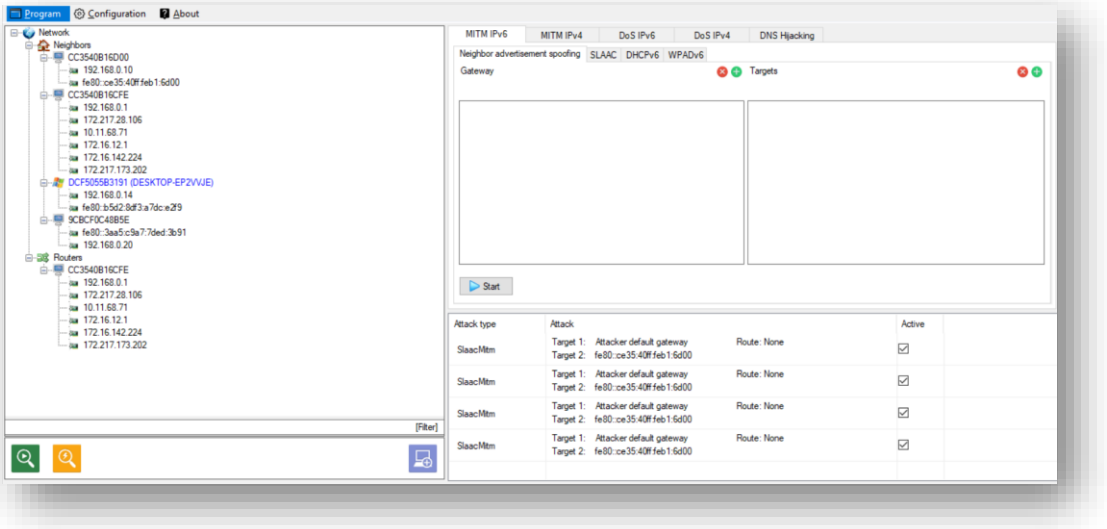
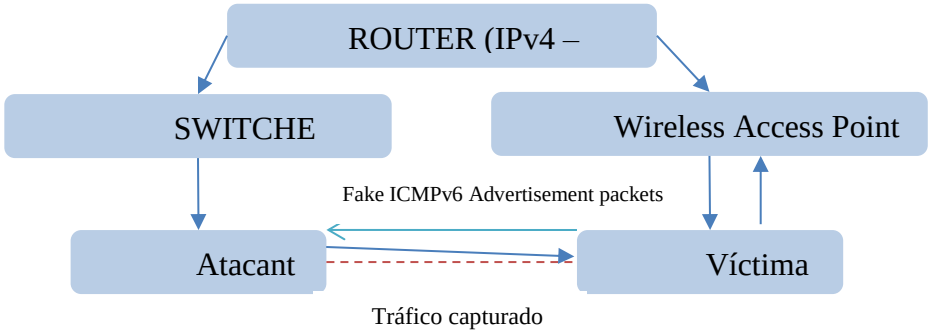


Figura 24. *Tablero de Configuración Neighbor Advertisement Spoofing*



Para la ejecución del Neighbor Advertisement Spoofing, se crea la topología de red mostrada en la figura 25 mediante la cual los equipos de red tengan conectividad entre sí:

Figura 25. *Diagrama simplificado de red dispuesto para la ejecución del ataque Neighbor Advertisement Spoofing.*



Mediante el software Evil Foca, el atacante escanea la red en busca de vecinos de red IPv6 con el fin de escoger una víctima. Se genera entonces el ataque mediante la configuración del equipo atacante como falsa puerta de enlace de la red (Gateway) y el equipo objetivo, y se ejecuta el ataque.

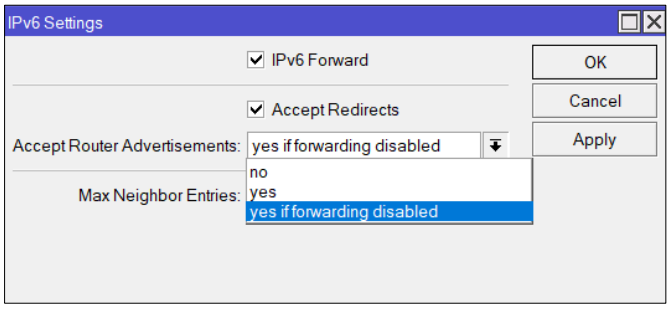
Este ataque tiene como resultado que el dispositivo víctima de ataque recibe las respuestas NDP no desde el router sino desde el equipo atacante, lo cual implica que no establecerá comunicación con el servidor original y obtendrá respuestas falsas desde el atacante. Se deniega el servicio que está siendo requerido por el usuario víctima.

Parámetros de Seguridad para evitar el ataque de red:

Por medio del protocolo seguro Secure Neighbor Discovery (SEND) RFC 3971, es posible establecer parámetros que permitan asegurar la comunicación entre dos o más dispositivos en una red local por medio de IPv6, evitando un ataque de hombre en el medio MITM. Este protocolo establece los mecanismos de seguridad para proteger los mensajes NDP (*Neighbor Discovery Protocol*), mediante la certificación de caminos (*certificaction paths*), la cual se habilita en las partes de una comunicación, router y usuario, a través la función de dispositivos de confianza de manera que un dispositivo host tenga un anclaje de confianza con

el cual el router debe establecer un certificado de confianza antes de que el host los adopte con el router por defecto. [56].

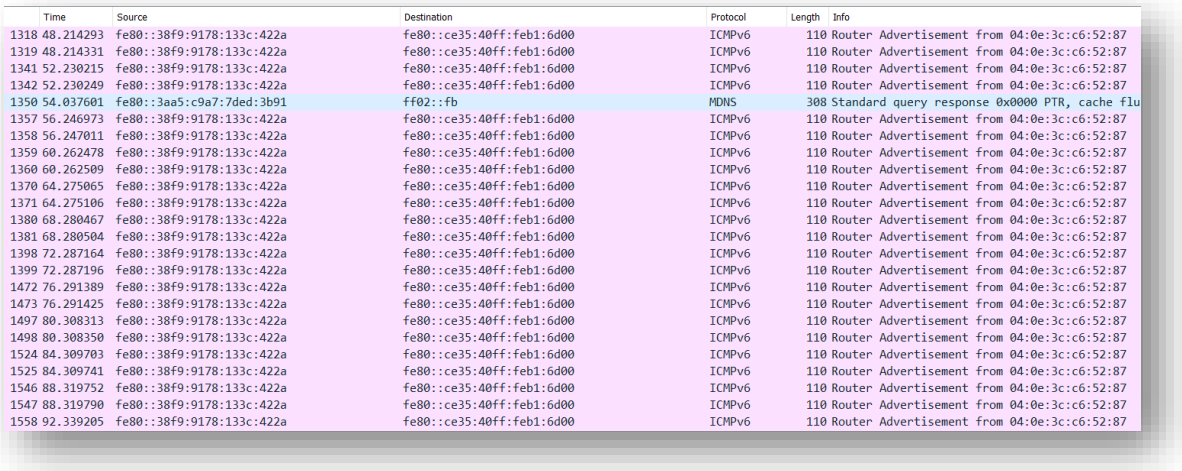
Figura 26. *Configuración de seguridad IPv6 para evitar NDP/NA de otros enrutadores*



4.4.2.2 SLAAC16

En este tipo de ataque, el atacante envía nuevamente información ICMPv6, pero esta vez correspondiente a los anuncios ICMPv6 del router, con el fin de dirigir el tráfico hacía la dirección IP de la víctima.

Figura 27. *Captura de datos ICMPv6. Generación de anuncios falsos de paquetes de anunciamiento IPv6 del router, originados por el equipo atacante y enviados a la Ipv6 de la víctima*



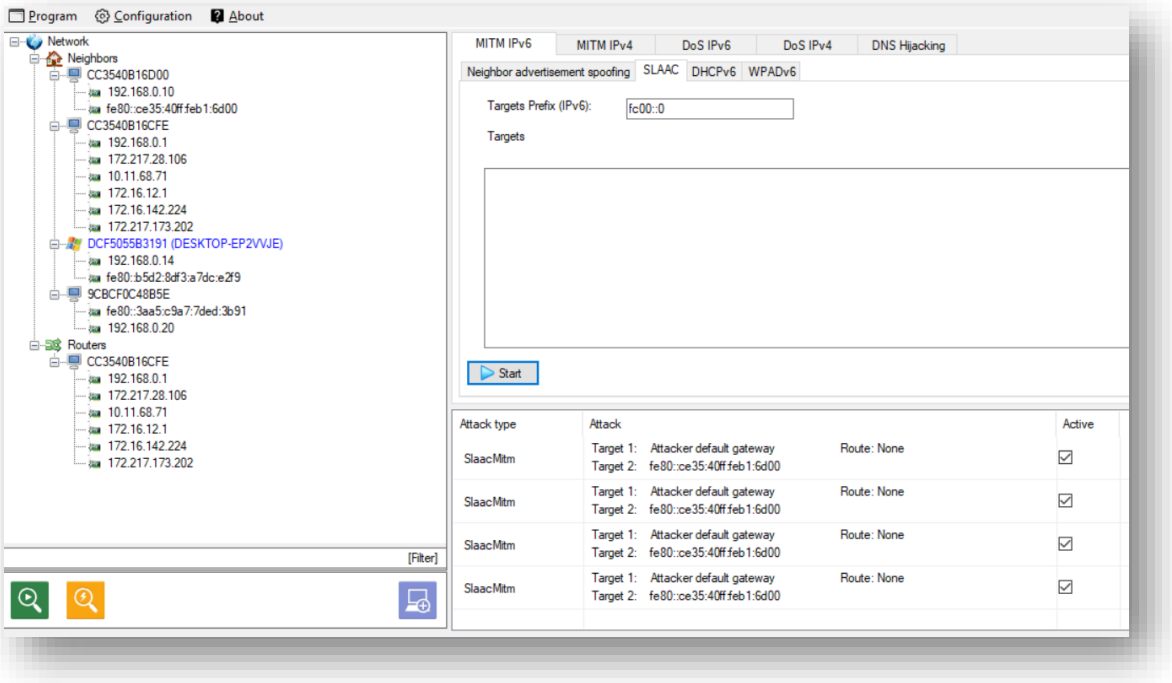
	Time	Source	Destination	Protocol	Length	Info
1318	48.214293	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1319	48.214331	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1341	52.230215	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1342	52.230249	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1350	54.037601	fe80::3aa5:c9a7:7ded:3b91	ff02::fb	MDNS	308	Standard query response 0x0000 PTR, cache flu
1357	56.246973	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1358	56.247011	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1359	60.262478	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1360	60.262509	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1370	64.275065	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1371	64.275106	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1380	68.280467	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1381	68.280504	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1398	72.287164	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1399	72.287196	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1472	76.291389	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1473	76.291425	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1497	80.308313	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1498	80.308350	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1524	84.309703	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1525	84.309741	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1546	88.319752	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1547	88.319790	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87
1558	92.339205	fe80::38f9:9178:133c:422a	fe80::ce35:40ff:feb1:6d00	ICMPv6	110	Router Advertisement from 04:0e:3c:c6:52:87

La captura de datos se realiza mediante la herramienta Wireshark, desde la cual, se evidencia el envío de los paquetes de anunciamiento del router (Router Advertisement) desde

[16] Stateless Address Autoconfiguration. [67]

el equipo que genera el ataque con dirección IPv6 fe80::38f9:9178:133c:422a hacia la dirección IPv6 del equipo objetivo fe80::ce35:40ff:feb1:6d00.

Figura 28. *Panel de configuración de herramienta Evil Foca. Ataque a la red MITM IPv6 mediante SLAAC.*

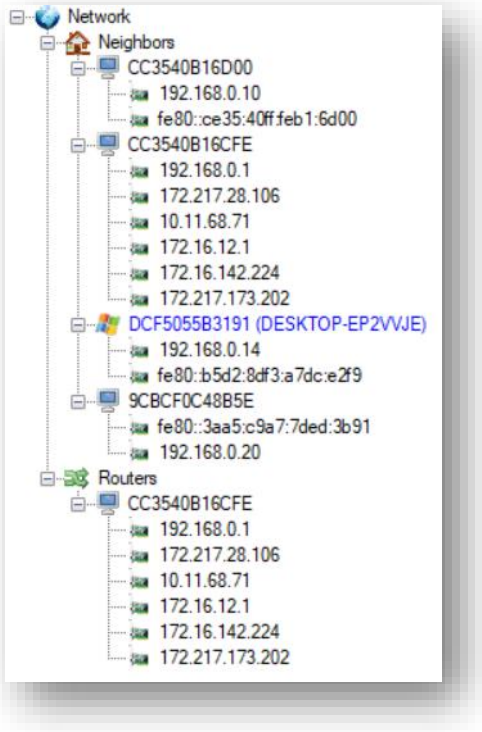


Desde la herramienta Evil Foca, se emula el ataque a la red mediante la opción MITM – SLAAC, a través de la cual, se genera un prefijo IPv6 por defecto, que permita escanear la red de manera que pueda encontrar cualquier dirección IPv6, bien sea local o global Unicast.

Se encuentra un listado de direcciones IPv6 de enlace local (fe80::), así como también IPv4 clase A, clase B, clase C y sin clase, que identifican a los equipos conectados a las redes locales a las cuales se tiene alcance a través de la herramienta Evil Foca.

Si bien esta prueba no logra generar problemas en la intercomunicación de los equipos clientes con el servidor, permite detectar vulnerabilidades a través de DHCPv6 y establecer políticas de seguridad que permitan evitarlas.

Figura 29. *Lista de escaneo de direcciones IPv4 e IPv6 alcanzables a través de la red de despliegue para los escenarios de ataque simulado.*



Parámetros de Seguridad para evitar el ataque de red:

Existen herramientas recursivas, versátiles e intuitivas que pueden evitar ataques a través de la autoconfiguración de direcciones sin clase SLAAC, el cual corresponde a uno de los mecanismos de descubrimiento de vecinos (NDP) en IPv6.

Para el desarrollo de esta práctica, se han utilizado dos parámetros de configuración desde la herramienta Mikrotik, que evitan la transmisión o reenvío de paquetes desde dispositivos no confiables o certificados. De entrada, es posible evitar la transmisión de paquetes ICMPv6 desde el router, simplemente generando una política que límite o corte la transmisión de echo *requests* o echo *replies* desde alguno de los hosts.

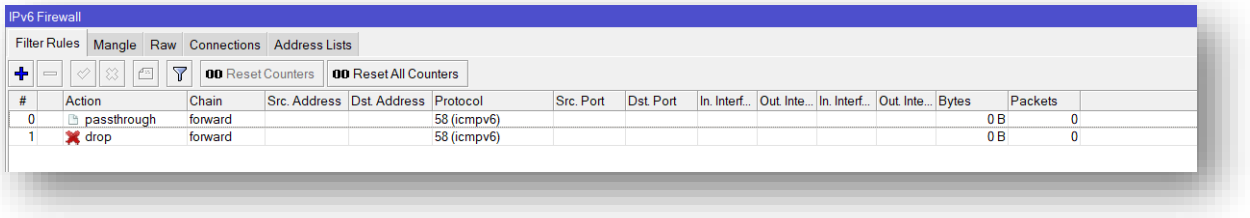
Uno de los mecanismos utilizados para evitar a toda costa este ataque se puede prevenir mediante la siguiente línea en mikrotik: (*add chain=forward protocol=icmpv6 icmp-*

options=0:0 action=drop comment="host unrechable"). Sin embargo, es preciso aclarar que esta regla evitará que se realice comunicación vía ICMPv6 entre dispositivos, lo cual puede resultar contraproducente si se necesita validar pruebas de conectividad.

Se requiere entonces de reglas definidas para el tipo de conexiones que establecen mediante la configuración de SLAAC, al tener en cuenta que, para que esta configuración surja efecto, es preciso anotar que el enrutador o cortafuegos, tenga habilitada la opción *router Discovery* de manera que permita identificar automáticamente a los hosts que solicitan direccionamiento o realizan NDP/NS (*Neighbor Discovery Protocol / Neighbor Solicitation*).

Ya que mediante SLAAC el atacante simula ser un router falso, los anunciamientos que este genere deben pasar por la puerta de enlace de la red, el router genuino debe poder evitar entonces estos paquetes de solicitud falsos.

Figura 30. *Política de seguridad en IPv6 Firewall del enrutador Mikrotik*

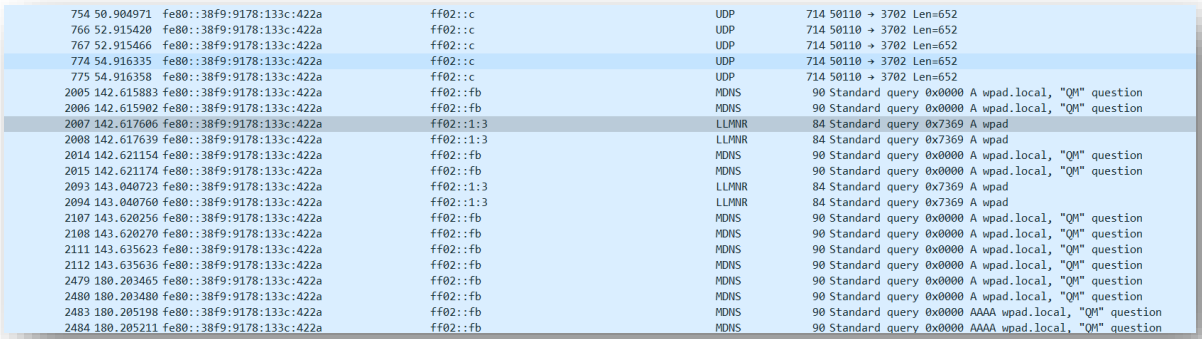


Nota*:* Permite identificar la conexión ICMPv6 mediante el marcado de paquete cuando se trate de un paquete erróneo (bad packet) y posteriormente eliminarlo.

4.4.2.3 DHCPv6

En este ataque, el computador atacante actúa como un servidor DHCPv6 solitario, configurando direcciones IP y servidor DNS en los equipos de los clientes.

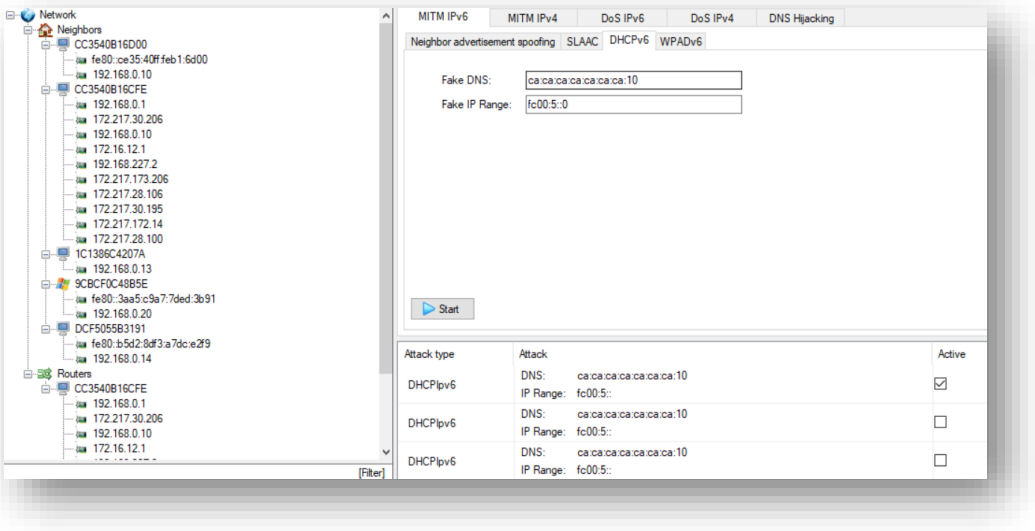
Figura 31. *Escaneo de tráfico IPv6 durante el ataque DHCPv6 mediante los protocolos UDP, LLMNR y MDNS*



754	50.904971	fe80::38f9:9178:133c:422a	ff02::c	UDP	714	50110 → 3702 Len=652
766	52.915420	fe80::38f9:9178:133c:422a	ff02::c	UDP	714	50110 → 3702 Len=652
767	52.915466	fe80::38f9:9178:133c:422a	ff02::c	UDP	714	50110 → 3702 Len=652
774	54.916335	fe80::38f9:9178:133c:422a	ff02::c	UDP	714	50110 → 3702 Len=652
775	54.916358	fe80::38f9:9178:133c:422a	ff02::c	UDP	714	50110 → 3702 Len=652
2005	142.615883	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2006	142.615902	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2007	142.617606	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84	Standard query 0x7369 A wpad
2008	142.617639	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84	Standard query 0x7369 A wpad
2014	142.621154	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2015	142.621174	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2093	143.040723	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84	Standard query 0x7369 A wpad
2094	143.040760	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84	Standard query 0x7369 A wpad
2107	143.620256	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2108	143.620270	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2111	143.635623	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2112	143.635636	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2479	180.203465	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2480	180.203480	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
2483	180.205198	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 AAAA wpad.local, "QM" question
2484	180.205211	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90	Standard query 0x0000 AAAA wpad.local, "QM" question

Este ataque permite que los demás dispositivos que son alcanzables a través de la red IPv6, puedan responder a una consulta (*query*) multicas DNS generada desde el equipo atacante mediante la utilización de los protocolos mencionados en la Figura 20, los cuales se encargan de crear una resolución de nombres dentro de una red local a partir de un oferente de este tipo de consultas y respuestas para nombres de dominio. Así mismo, el LLMNR genera una configuración automática de DNS lo cual permite que los hosts en el mismo enlace continúen comunicándose mientras la comunicación global Unicast se encuentre establecida. Esto puede llegar a irrumpir en la comunicación entre el dispositivo víctima e internet.

Figura 32. *Implementación de ataque DHCPv6 sobre la red local*



Parámetros de Seguridad Para Evitar el Ataque de Red:

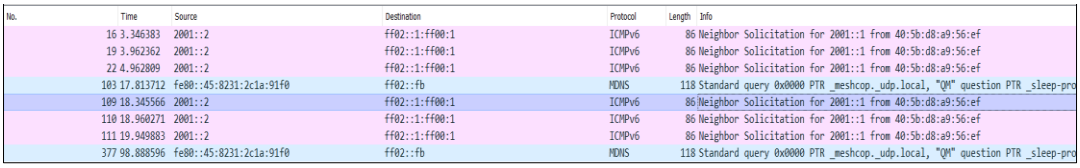
La utilización de un mecanismo que permita autenticar y autorizar las conexiones a la red a través de la interfaz física del enrutador se hace necesario para evitar este ataque. Se cuenta con el protocolo RADIUS[17], el cual permite identificar mediante los campos del paquete, la longitud del paquete, el campo autenticador, solicitud y respuesta de autenticación y los atributos, mediante la identificación del tipo de paquete a través del campo de código en el primer octeto del paquete. Ya que este ataque está basado en solicitudes DHCPv6, es preciso evitar este tipo de ataque en primer lugar, mediante el bloqueo de este tipo de paquetes, lo cual se puede conseguir a través de la configuración de políticas de firewall desde el dispositivo que gestiona la red, comúnmente, el dispositivo de cabecera de red.

Una forma de identificar este tipo de incidencia es mediante el monitoreo de paquetes a través de la utilización de la herramienta Wireshark. Así, se puede observar que para una subred

[17] RADIUS: Remote authentication Dial-In User Service. Protocolo de autorización y autenticación para servicios de movilidad y/o acceso a la red. RFC 2139.

IPv6, los hosts realizan *requests* hacia la subred, solicitando configuración DHCPv6 a cuál es recibida por los demás dispositivos de la subred, esto puede significar, que a pesar de que los dispositivos adyacentes de la red también realicen solicitud DHCP, estos pueden procesar transparentemente solicitudes DHPCv6 abriendo las puertas a un ataque orientado a la red en lugar de un ataque orienta a la adyacencia de los demás dispositivos en la red.

Figura 33. *Monitoreo de red IPv6. Solicitud Neighbor Advertisement NA/NS desde un host de una red local preestablecida, enviado a los demás dispositivos de la red local.*



No.	Time	Source	Destination	Protocol	Length	Info
16	3.346383	2001::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001::1 from 40:5b:d8:a9:56:ef
19	3.962362	2001::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001::1 from 40:5b:d8:a9:56:ef
22	4.962809	2001::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001::1 from 40:5b:d8:a9:56:ef
103	17.813712	fe80::45:8231:2c1a:91f0	ff02::fb	MDNS	118	Standard query 0x0000 PTR _meshcop._udp.local, "QM" question PTR _sleep-pro
109	18.345566	2001::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001::1 from 40:5b:d8:a9:56:ef
110	18.960271	2001::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001::1 from 40:5b:d8:a9:56:ef
111	19.949883	2001::2	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001::1 from 40:5b:d8:a9:56:ef
377	98.888596	fe80::45:8231:2c1a:91f0	ff02::fb	MDNS	118	Standard query 0x0000 PTR _meshcop._udp.local, "QM" question PTR _sleep-pro

Como se observa en la figura 32, los dispositivos que realizan solicitudes orientadas en adyacencias pueden representar un vector de ataque definido, orientado a la red o a la adyacencia. Para el caso de ataques de denegación de servicio direccionados mediante DHCPv6, es necesario establecer políticas de autenticación de hosts frente al router o firewall, dispositivo que validará esta comunicación mediante la certificación de los mensajes entre host y router.

4.4.2.4 WPADv6[18]

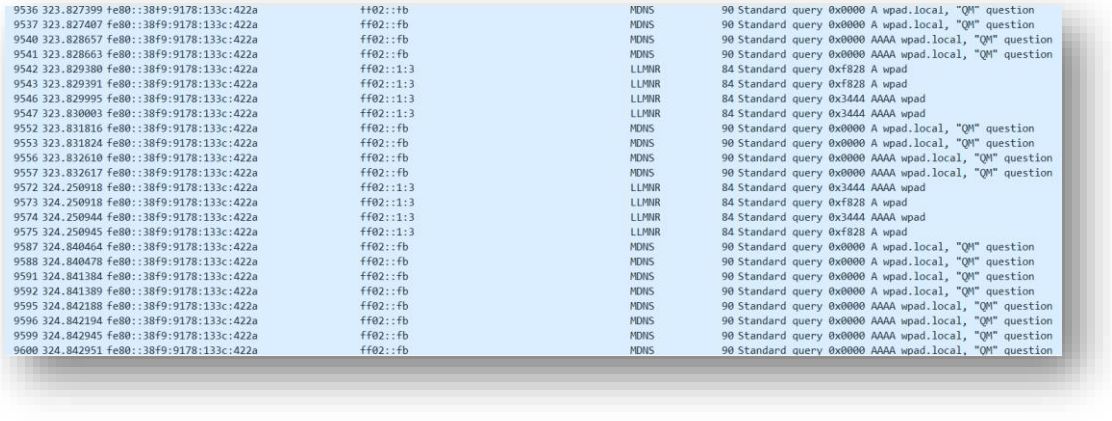
El atacante envía información de respuestas falsas de paquetes WPADv6 LLMNR de descubrimiento de dispositivos que funcionan como servidores proxy para enviar tráfico HTTP(S), mediante el protocolo de resolución de nombres de enlace local para multicast (Link

[18] Web Proxy Autodiscovery Protocol para IPv6. Método utilizado por el sistema operativo Windows para detectar qué máquinas son utilizadas como un proxy para enviar tráfico HTTP(S).

Local Multicast Name Resolution LLMNR), causando que cualquier tráfico IPv6 que vaya hacia la red de la víctima, use su máquina como un servidor proxy.

En la figura 34 se aprecia la captura de tráfico IPv6 por medio de la herramienta Wireshark a fin de identificar el protocolo LLMNR utilizado en esta modalidad de ataque a la red IPv6.

Figura 34. *Captura de tráfico IPv6 por medio de la modalidad de ataque WPADv6.*



9536	323.827399	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9537	323.827407	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9540	323.828657	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9541	323.828663	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9542	323.829380	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0xf828 A wpad
9543	323.829391	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0xf828 A wpad
9546	323.829995	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0x3444 AAAA wpad
9547	323.830003	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0x3444 AAAA wpad
9552	323.831816	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9553	323.831824	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9556	323.832610	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9557	323.832617	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9572	324.250918	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0x3444 AAAA wpad
9573	324.250918	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0xf828 A wpad
9574	324.250944	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0x3444 AAAA wpad
9575	324.250945	fe80::38f9:9178:133c:422a	ff02::1:3	LLMNR	84 Standard query 0xf828 A wpad
9587	324.840464	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9588	324.840478	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9591	324.841384	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9592	324.841389	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
9595	324.842188	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9596	324.842194	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9599	324.842945	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question
9600	324.842951	fe80::38f9:9178:133c:422a	ff02::fb	MDNS	90 Standard query 0x0000 AAAA wpad.local, "QM" question

Parámetros de Seguridad para evitar el ataque de red:

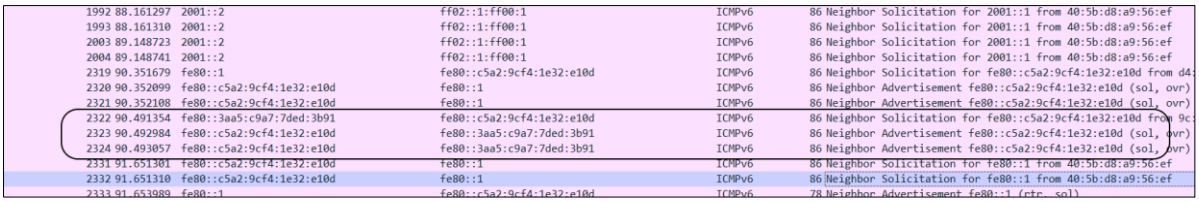
Similar a los ataques que se han mencionado anteriormente, este ataque también hace parte del grupo de ataques basados en MITM, y que busca bien sea corromper la información de los hosts adyacentes o generar denegación de servicio.

Sin embargo, aquí es el dispositivo víctima el que abre las puertas del ataque directamente a los atacantes mediante solicitudes DNS a la red, en caso tal de que el servidor DNS no responda o no tenga la respuesta que el usuario está consultando, el host reenviará la información nuevamente a la red en busca nuevamente de la respuesta preguntando a los demás nodos si alguno conoce la respuesta de la información que se está consultando. He aquí la oportunidad para que el dispositivo atacante genere una respuesta ilegítima, enmascarada en

una respuesta válida para la víctima, logrando desviar el tráfico de la víctima hacía el dispositivo atacante.

No obstante, se han generado diversos mecanismos de defensa que evitan este tipo de ataque. Dado que este tipo de ataque guarda similitudes con DHCPv6, igualmente, técnicas de certificación de mensajes y autenticación de usuarios ante el servidor DNS pueden mitigar esta incidencia de manera significativa. En la figura 35 se muestran algunos paquetes capturados que utilizan la solicitud y anunciamiento de los vecinos para las direcciones MAC e IPv6 de origen y destino de los equipos de la red. Esta captura se realiza desde el equipo atacante (MITM).

Figura 35. *Identificación de Neighbor Advertisement y Neighbor Solicitation.*



Firewalls robustos como Sonicwall NSA 5650, Sonicwall Supermassive 9200, Sophos XGS Series, Palo Alto PA Series, entre otros, ofrecen políticas de seguridad por defecto que bloquean el tráfico IPv6 tanto en pre enrutamiento como post enrutamiento para capa 3, limitaciones de solicitudes a nivel de ICMPv6 en red local y evitación de anunciamientos de direcciones, así como también, inspección profunda de paquetes tanto para el tráfico entrante como para el tráfico saliente, lo cual ofrece de entrada una solución preventiva ante incidentes de red y presenta una capa de seguridad robusta bien sea para enfrentar a los ataques de red, así como para mostrar políticas robustas de seguridad ante auditorías de seguridad.

4.4.2.5 Políticas QoS en la seguridad de la información.

De acuerdo con los parámetros de calidad de servicio que permitan la integridad de la información, es decir, que esta no pueda ser alterada por entidades no autorizadas, se caracterizaron las políticas de seguridad pertinentes al proyecto con base en los ataques propuestos en la tabla 5:

Tabla 5. *Relación de las políticas de seguridad utilizadas para los ataques propuestos:*

Política de seguridad	**Ataque propuesto**
Secure Neighbor Discovery (SEND) RFC 3971	Neighbor Advertisement Spoofing
RADIUS	DHCPv6
Denegación ICMPv6	SLAAC
Certificación y autenticación de usuarios	WPADv6

Nota: la tabla 5 relaciona los ataques propuestos con las políticas de seguridad utilizadas para evitar ataques a la red mediante IPv6. No obstante, es posible contar con otro tipo de defensa ante los ataques vía IPv6 como servicios de filtrado de contenido a través de este protocolo pero que, sin embargo, denegarían el tráfico IPv6.

4.5 Análisis de resultados

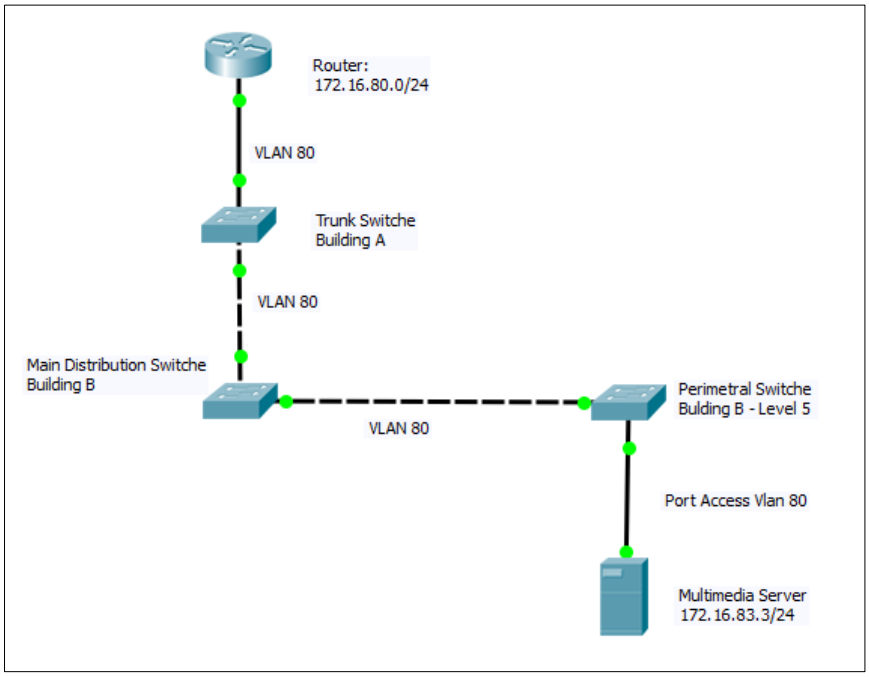
La realización del laboratorio se presenta como sigue, mediante la topología de red propuesta en el escenario de las prácticas controladas de laboratorio y el análisis del tráfico multimedia.

4.5.1 Topología de red

La topología de red juega un papel importante en el desempeño de la transmisión del contenido multimedia ya que a partir del diseño de ésta se definen políticas de calidad de servicio que permiten priorizar y diferenciar servicios dentro de la red de la universidad.

Dado que en la actualidad se cuenta con el servicio de carteleras digitales desplegado en los campus de Bucaramanga y Floridablanca de la Universidad Santo Tomás, existe un servidor de contenido multimedia dispuesto en el campus de Floridablanca. Este servidor cuenta con la distribución Ubuntu de Linux cuya configuración de red hace parte de la topología de red interna IPv4 de la Universidad de la siguiente manera:

Figura 36. *Topología de red IPv4 para servidor de contenido multimedia de la Universidad Santo Tomás.*



Sobre esta topología se plantea la siguiente implementación que incorpora el protocolo de internet IPv6:

Tabla 6. *Configuración IPv4 – Ipv6 en topología cliente servidor.*

IPv4		
VLAN 80 IPv4	**SERVER**	**CLIENT**
ether 1	ether 2	ether 3
IPV6 - BRIDGE 1		
ether 1	ether 2	ether 3

Nota: la VLAN 80 permite el tráfico IPv4 a través de la interfaz eth1 y comunicación con el servidor a través de la interfaz eth2 y el cliente eth3. Por otra parte, el tráfico IPv6 se segmenta a través de un puente para las tres interfaces.

Debido a que tanto la routerboard implementada como las interfaces de red del servidor y del cliente soportan la configuración IPv4 e IPv6 simultáneamente (figuras 37 y 38), es posible implementar ambos protocolos paralelamente en una misma interfaz, de esta manera, la routerboard actúa como un *bridge* para la red IPv4 ya existente, es decir, pasa transparente a través de la routerboard, y a esta misma interfaz *bridge* se asigna un pool de direccionamiento IPv6 de manera que los equipos finales sean visibles a través de la red con ambos protocolos.

Figura 37. *Ejemplo de asignación de direccionamiento IPv6 a las diferentes interfaces de la routerboard.*

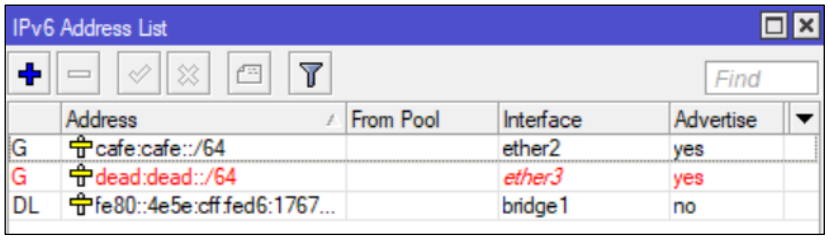
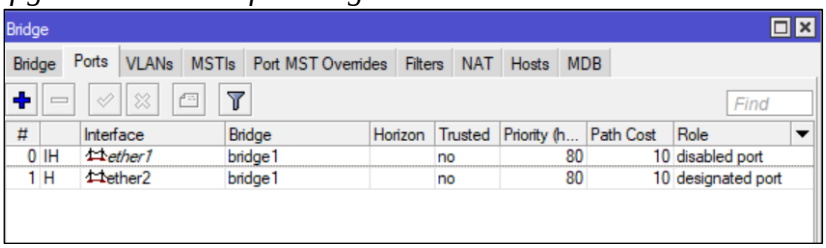


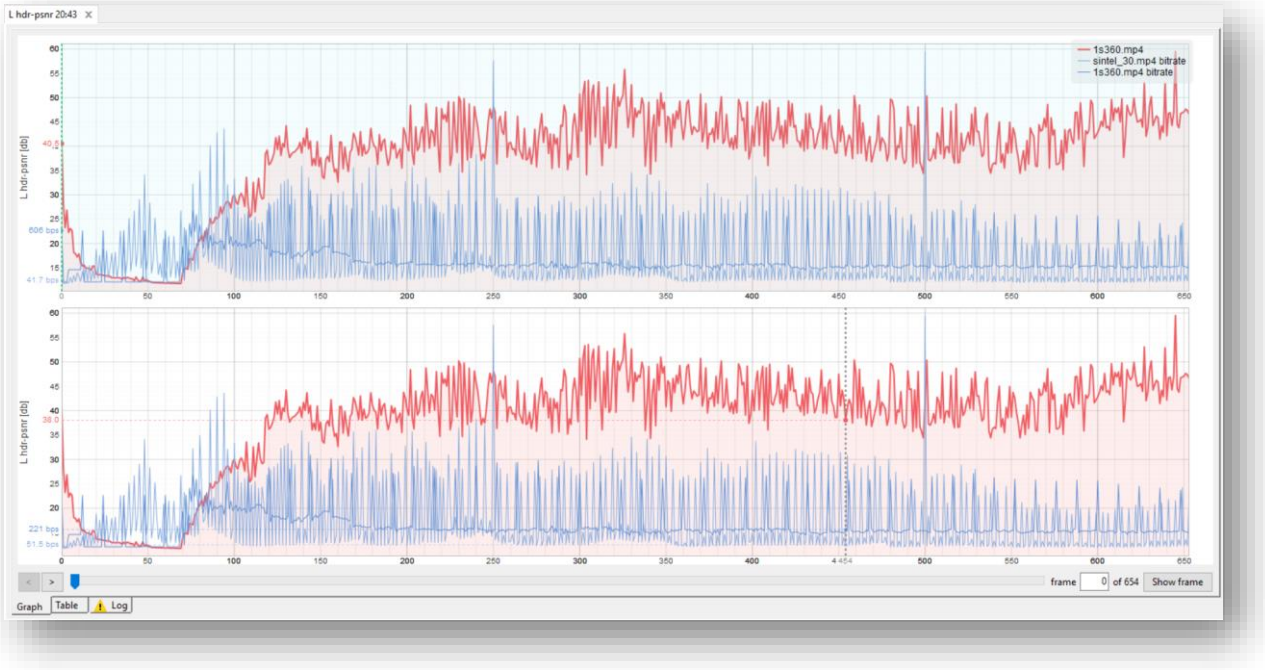
Figura 38. *Configuración de interfaz bridge en la routerboard.*



Para la realización del banco de pruebas, se proponen dos escenarios derivados del entorno controlado de laboratorio. El primero se basa en la presentación del contenido sin la utilización de parámetros de calidad de servicio mediante la transmisión de tráfico de mejor esfuerzo (*best effort*), en donde los primeros paquetes en entrar a las interfaces serán los primeros en salir (*First In – First Out: FiFo*). El segundo escenario es una red con calidad de servicio incorporada, dentro de la cual se han implementado tres colas de tráfico mencionadas al inicio de la sección y que aplican a las diferentes calidades de los servicios presentados, en los dos estándares de compresión de video utilizados, H264 y H265.

Para la medición subjetiva de la calidad de experiencia, se utilizan tres componentes conceptuales que serán el eje de esta sección: *Video Quality Metric* (VQM), *Peak Signal Ratio Noise* (PSNR) y *Structural Similarity Index Measure* (SSIM). Estas métricas subjetivas presentan ventajas para establecer las métricas de calidad de servicio, orientadas a la calidad del contenido multimedia adaptativo, y se asocian adecuadamente a los parámetros de red, asociados a la calidad de servicio QoS preestablecida para el desarrollo de la investigación, así como también, a los protocolos IPv4 e IPv6, a los cuales se aplica la comparativa.

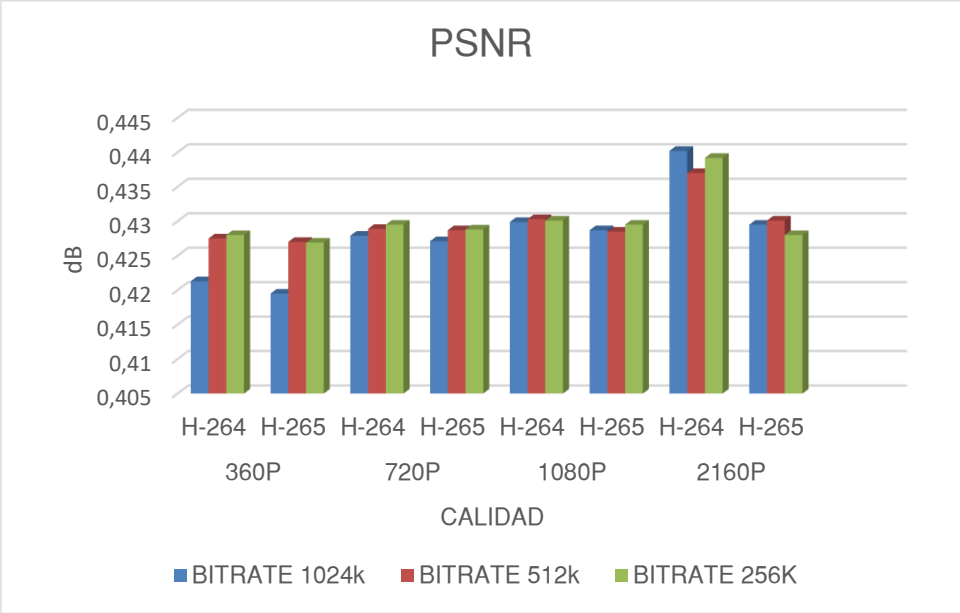
Figura 39. *Análisis de PSNR para el segmento 360p de 30 segundos mediante la herramienta MSU Video Quality Measurement Tool (VMQT).*



4.5.2 Comparativa de PSNR para el tráfico IPv6 e IPv4.

Como se muestra en la Tabla 4, se establece la relación del PSNR (Relación Señal a Ruido - Pico) en la compresión del contenido multimedia entre los ficheros de entrada segmentados a 30s y los respectivos ficheros de salida comprimidos en H264 y H265 antes de ser transmitidos por la red. Esto permite identificar la relación señal a ruido promedio a partir del análisis de los frames para cada segmento de video como se muestra en la Figura 38 para el fichero de entrada ‘sintel_30.mp4’ versus el fichero de salida comprimido en H.264, a 256kbps en formato 360p. Así mismo, se presentan los resultados de la relación señal a ruido entre el contenido original y después de ser comprimido a H.264 y H.265 para las 3 tasas de bit propuestas y para las calidades de video establecidas.

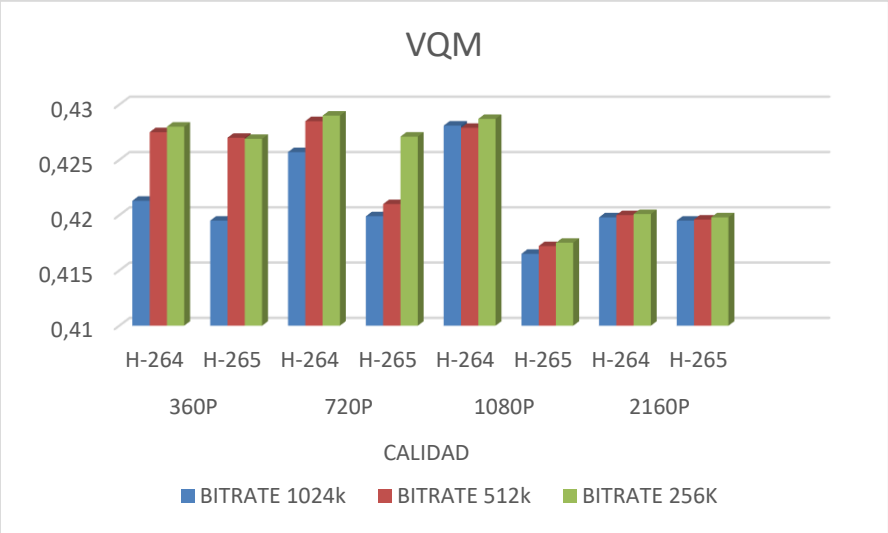
Figura 40. *Comparativa de PSNR para los Bitrate y las Calidades establecidas.*



Como segunda métrica utilizada para esta sección, se utiliza la métrica de calidad de video VQM, la cual aplica una comparativa entre el contenido original y el video luego de ser procesado [57]. Con esto, se logra evidenciar el nivel de calidad del contenido procesado con base en la percepción subjetiva del ojo humano mediante la división de la imagen en secuencias de bloques temporales – espaciales, con lo cual se miden parámetros como el *blurring*[19] [58], distorsión de bloques[20] y la distorsión de color. Los valores posibles para VQM toman lugar entre 0 y 1, en donde 0 indica un mejor valor de VQM.

Figura 41. *Comparativa del parámetro VQM para los Bitrate y las Calidades establecidas.*

[19] Blurring o difuminación, consiste en aplicar una transición suave de color de un lado del límite de una imagen a otro de forma delicada en lugar de repentina.
[20] La distorsión de bloques consiste en errores que se repiten en bloques de frames para una secuencia de contenido de video.



Para el parámetro VQM, así como para el PSNR y el SSIM, se han considerado los contenidos en 4 formatos de calidad distintos y 3 tasa de bit particulares configuradas en los parámetros de calidad de servicio, como se mencionó en la fase 3 de la metodología, comparación de tráfico de streaming multimedia adaptativo entre IPv4 e IPv6.

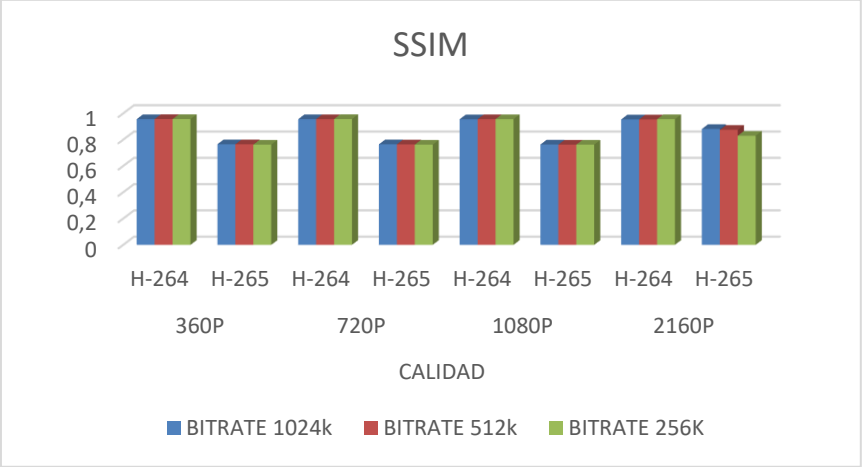
Por último, para las métricas VQM, se identifica que los valores más altos se evidencian en los formatos de calidad más bajos, guardando el patrón característico que define el aumento del VQM mientras disminuye el bitrate.

Como última métrica subjetiva analizada mediante software, se analiza el índice de similaridad estructural SSIM (*Structural Similarity Index*), el cual se define de acuerdo con [59] como un método de medición de la calidad basado en la degradación estructural de la información y es un valor agregado a los métodos conocidos de evaluación y medición de la calidad de imagen basados en la diferencia entre una imagen distorsionada y una imagen de referencia. Este principio, ha sido introducido al laboratorio con el fin de realizar la comparativa entre el contenido original referencia y los segmentos de video resultantes del procesamiento de cambio de compresión, bitrate y calidad de video, con el fin de analizar la calidad de

experiencia del usuario realizando inicialmente la comparación a partir de la utilización del software *MSU Video Quality Measurement Tool (VMQT)* que permite emular la percepción humana para finalmente contrastarlo con las calificaciones dadas por los espectadores.

Esta métrica en particular permite evidenciar un contraste notable entre los dos códecs de compresión de video, ya que para las 4 calidades propuestas bajo el estándar de compresión H.265 en la Figura 31, se muestra que este códec presenta un valor menor de SSIM frente a H.264. En contraste, el contenido bajo el estándar H.264 presenta un valor más ato con valores aproximadamente similares, aunque presentan una leve disminución mientras aumenta la calidad del contenido, es decir, el códec H.264 en 512k tiene un valor menor de SSIM para el formato 2160p que el formato 360p con el mismo códec y bitrate.

Figura 42. *Comparativa del parámetro SSIM para los Bitrate y las Calidades establecidas.*



A partir de la implementación de la calidad de servicio para redes multimedia, el camino lleva finalmente a evaluar la calidad de experiencia, ya que son dos aspectos que se encuentran íntimamente relacionados.

En cuanto a la calidad de servicio implementada, se crearon 3 colas de tráfico con limitación de descarga y subida de paquetes. Estas colas de tráfico se configuraron a partir de 256, 512 y 1000Kbps.

4.5.3 Calidad de experiencia y la calidad de servicio de video streaming sobre IPv6

Para realizar la medición de la calidad de servicio, es necesario retomar los resultados obtenidos en el desarrollo del primer objetivo, en donde se evidencia si existe una diferencia real en el comportamiento del tráfico multimedia streaming bajo condiciones controladas de red, así como en el escenario real de la red. Así mismo, aplicar nuevas variables a la actividad tales como incluir contenido con resolución 4K (2160p) (3840*2160) codificados tanto en H.264 como en H.265, que permitan llevar el sistema a un punto de estrés tal, que sea posible observar cuales serían los nuevos retos en términos de infraestructura de hardware y de software que permitan la escalabilidad de las emergentes tecnologías de streaming que incorporan mejoras en la calidad de la imagen.

Finalmente, la aceptabilidad del servicio de video streaming soportado en IPv6, percibido subjetivamente por el usuario final [13], evaluará la calidad de experiencia QoE, objeto de la investigación. Los resultados obtenidos en las anteriores actividades, en la calidad de servicio QoS serán los resultados medibles para esta actividad.

Los experimentos llevados a cabo se desarrollaron en una red local dual stack IPv4/IPv6 con un servidor de contenido multimedia adaptativo ante diferentes colas de tráfico que, intencionalmente, limitan la tasa de tráfico de la red y permiten observar mejoras o

desmejoramientos en la red, de acuerdo con los límites de tráfico de subida y descarga establecidos.

Dentro de los parámetros de calidad de servicio establecidos para las prácticas, se han generado en esencia tres colas de tráfico de 250, 512 y 1000 kilobits por segundo (kbps) sobre la red dual stack (IPv4/IPv6), en la cual, al menos tres dispositivos clientes realizan las solicitudes de contenido multimedia al servidor DASH. En la capa de enlace se caracteriza la extensión de os paquetes de datos a través de un dispositivo de conmutación de paquetes no administrable y con interfaces BASE 10/100/1000 auto negociable, de manera que la transmisión de datos estará supeditada a la tasa máxima de transmisión que permitan las interfaces de red de los equipos conectados, en particular se conoce que las interfaces de los dispositivos operan a 1000 Mbps al igual que las interfaces del dispositivo de distribución o conmutación.

Para la transmisión del contenido bajo estas tasas de transmisión, se han considerado diferentes calidades del material, en particular, 360p, 720, 1080p y una adicional que se contempló como actividad adicional, 2160p. Estas calidades transmitidas bajo las diferentes colas de tráfico, 250, 512 y 1000Kbps, fueron adicionalmente comprimidas utilizando dos formatos de compresión, H264 y H265, y adicionalmente, los parámetros de seguridad necesarios para prevenir un ataque de red bajo el protocolo IPv6, como agregado a las políticas IPv4 ya conocidas y que se permiten coexistir en un ambiente de seguridad perimetral de la red. Con esto, se plantean entonces 5 parámetros variables para el desarrollo del trabajo de investigación y que permite establecer las bases para realizar mediciones basadas en calidad de la experiencia QoE entendidas como las mediciones subjetivas, luego de realizar las mediciones objetivas basadas en calidad de la experiencia.

La medición de la calidad del contenido multimedia, desde el punto de vista del espectador, es extrínsecamente subjetiva, ya que existen factores que pueden generar diferencias significativas entre las diferentes percepciones de los usuarios y que están relacionados con el estado visual de la persona, la cantidad de iluminación del entorno, el tamaño de la pantalla en la que se está proyectando el contenido, agotamiento visual, entre otros.

Estas mediciones se realizan, en el marco de la presente investigación, basadas en el sistema de visión humano (SVH) [60], e incorporan aspectos relacionados, por una parte, con la calidad del servicio impuesta a la red, y por otra a las condiciones visuales del espectador mencionadas anteriormente.

5. Conclusiones

El presente trabajo de investigación ha planteado cuatro ejes temáticos principales que se integran a lo largo del documento de manera progresiva a través de la implementación de los laboratorios, y de los cuales se presentan las conclusiones para cada uno de los resultados obtenidos en cada fase.

Esta investigación ha tenido como objetivo evaluar la calidad de experiencia QoE de *video streaming* sobre IPv6 con respecto a IPv4 mediante el estudio de tráfico en la transmisión de contenido multimedia, la medición de la calidad de servicio QoS y análisis de seguridad en la red para una actualización tecnológica del sistema de carteleras digitales de la Universidad Santo Tomás seccional Bucaramanga. Sin embargo, en el marco de la pandemia del Covid-19, se presentaron dificultades en términos de la implementación de los laboratorios, con lo cual fue necesario replantear los escenarios de instalación de aplicativos y el entorno de laboratorio.

Dos de las principales justificaciones que se presentan en el presente trabajo de investigación, se cohesionan en dos campos de estudio; la ocupación de ancho de banda del contenido multimedia y la adopción del protocolo de internet IPv6. Estos dos aspectos conllevan a analizar otros elementos colaterales que no se deben pasar por alto en las infraestructuras de red.

Desde el punto de vista del contenido multimedia, es imprescindible hablar de la calidad de servicio de la infraestructura que permite servir este tipo de contenido, especialmente si los usuarios se ubican dentro de la misma infraestructura de red, ya que lo anterior supone una serie de parámetros de configuración en términos de priorización de tráfico, incorporación de equipos de red que soporten la demanda de tráfico, infraestructura física y segmentación de red para video con políticas de diferenciación de tráfico mediante segmentación de dominios de broadcast a través de VLAN, marcado de tráfico, paquetes, configuración de colas de tráfico, entre otros.

Por otra parte, la incorporación de protocolo IPv6 conlleva directamente a analizar las políticas de seguridad implementadas para este protocolo que permitan mitigar las diferentes amenazas presentes en la red y a través de las cuales se pueden presentar incidentes de seguridad tal y como se mostró en los apartados de la fase 4, correspondientes a la seguridad en el tráfico IPv6.

A nivel de laboratorio, se logró desarrollar la segmentación de video por bloques de 30 segundos, de manera que fuese posible segmentar[21] el contenido de manera dinámica. Se extrajo la pista de audio de cada recorte de video para finalmente compilarla con el manifiesto MPD por medio de los *dash_init* generados desde la configuración en FFMPEG.

[21] Disposición del contenido durante un periodo de tiempo específico y que presenta los bloques progresivamente en función de la capacidad de la red.

A través de este último, se logró generar 3 calidades distintas (360p, 720p y 1080p) para cada recorte de video utilizado, así mismo, cada una de estas calidades se generó con 3 tasas de bit (256k, 512k y 1024k) características, con la finalidad de realizar la comparación por medio de parámetros objetivos y subjetivos para los protocolos IPv4 e IPv6.

Las pruebas se llevaron a cabo en equipos con características de hardware similares, especialmente a nivel de la pantalla de visualización (FHD[22]) por medio de un reproductor Dash Player instalado en Google Chrome para cada equipo. Las pruebas fueron posibles a través de este navegador e igualmente por medio del navegador Brave, desarrollado igualmente por Google, mientras que en el navegador Mozilla Firefox, se presentaron limitantes de compatibilidad a la hora de realizar las pruebas, especialmente con los códecs utilizados para HEVC (H.265), por lo cual, finalmente se utilizó el navegador Chrome.

Se aplicaron dos formatos de compresión como objeto de estudio para las prácticas realizadas (H.264 y H.265), con base en los cuales se analizaría más adelante la calidad de experiencia en ambos protocolos de internet. Con esto, se presentó en el desarrollo de cada sección, la incorporación y análisis de cada una de las 4 variables mencionadas hasta este punto; calidad de contenido (360p, 720p y 1080p), tasa de bit (*bitrate*), códec (H.264 y H.265) y los protocolos de internet IPv4 e Ipv6.

Por otra parte, de acuerdo con la Figura 11, se observó una disminución del bitrate para el formato de video original cuando este se cambia de contenedor .mov a .mp4, es decir, antes de ser procesado en los códecs h.254 o h.265, lo cual representaría menor capacidad de procesamiento para el medio que reproduzca el contenido multimedio. En la Figura 12 se pudo

[22] Formato Full High Definition (1920*1080p).

observar que, una vez los segmentos de video de 3 minutos se cambiaron a contenedor .mp4, el bitrate aumentó en función del aumento de la calidad del video (resolución).

Otro parámetro objetivo que presentó una diferencia notable es la relación entre tamaño del fichero con el tipo de contenedor (ver figura 11), a partir del cual se pudo observar que el tamaño del fichero disminuye cuando se convierte de .mov a .mp4, estas transformaciones se realizan a partir del archivo original descargado. Lo anterior supone una ventaja en términos de capacidad de procesamiento de contenido multimedia.

Por otra parte, se evidenció que la tasa de bit aumenta en proporción a la calidad o resolución del contenido de video (ver figura 12), ya que para el contenido en formato FHD se pudo observar que el bitrate aumenta más del 200% del formato 360p al formato 1080p. Sin embargo, a partir de la comparativa entre los códecs, h.265 mantiene un bitrate menor que h.265 para los formatos respectivos.

Se presenta la topología de red utilizada en entorno controlado de laboratorio en la Figura 14, por medio de la cual se incorpora la configuración Dual Stack para IPv4 e Ipv6. La configuración finalmente realizada presentó dificultades al acceder, a través de la red local, al servidor mediante la red IPv6. Para este último, se aplicó configuración dinámica de direccionamiento IPv6 por medio de DHCPv6 y un Pool de direcciones IPv6 adoptado por el servido r IPv6. La interfaz del router anuncia de esta manera las direcciones IPv6 en la interfaz con base en un prefijo de longitud de 64 bits, de manera que, se genera un ID de interfaz para cada host conectado a la red. Sin embargo, al aplicar esta configuración, no era posible generar reconocimiento a través de la red para las direcciones Ipv6 configuradas de manera automática para equipo, con lo cual, estos no lograban acceder al servidor a través de IPv6.

Se aplicó una segunda estrategia que consistió en descartar el Pool IPv6 y configurar el prefijo de longitud 64 bits mediante la herramienta SLAAC, de manera que no fuese posible generar el prefijo y sus respectivos parámetros de configuración a través del router sin la necesidad de un servidor DHCPv6. Sin embargo, la problemática de accesibilidad a través de la red IPv6 persistió.

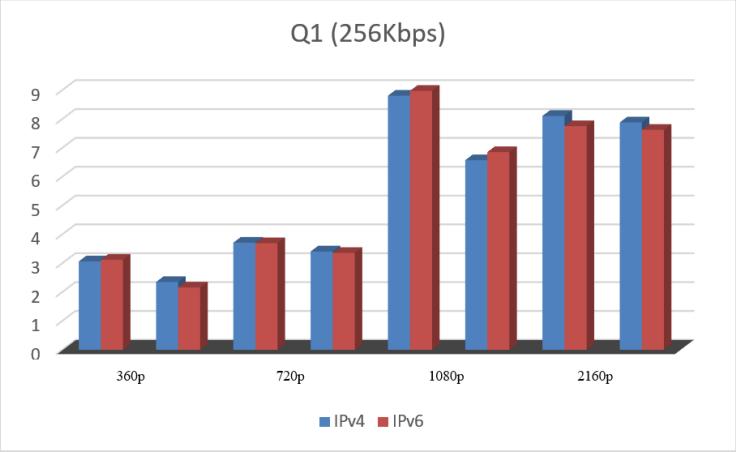
En contraste, se pudo observar que en cuanto al diferencial de retardo (*jitter*) generado en el entorno de laboratorio controlado, existe una diferencia, aunque mínima, que da ventaja al protocolo IPv6, el cual tiende a presentar una diferencia de retardo de transmisión de paquetes menor a IPv4 para el entorno de red propuesto. Sin embargo, algunas variaciones aleatorias de los tiempos arrojan excepciones, como la que se puede observar en la siguiente figura, particularmente para el formato 1080p en H.265, en donde la transmisión de contenido para IPv6 presentó el mayor retardo de esta muestra.

Por último, se asignó la configuración de direccionamiento de manera estática en la interfaz del router, de manera que esta actuaría como puerta de enlace para los equipos de la subred que tuviesen una configuración de red estática para IPv6 y se tuviese respuesta de ping hacía la puerta de enlace y finalmente al servidor. De esta forma fue posible solucionar el problema de accesibilidad IPv6 para el servidor del laboratorio.

El desarrollo de este laboratorio fue posible en medio de las políticas de bioseguridad y aislamiento durante la pandemia ya que, durante el periodo de aislamiento total, se limitó a un entorno de laboratorio con hasta máximo 4 equipos en red, con lo cual, si bien fue posible realizar algunas pruebas de conectividad, aún carecía de un entorno masivo que permitiera una observación de mediciones más acercada a la realidad.

A través de la observación de la transmisión de tráfico de contenido multimedia en redes IPv4 e IPv6, se pudo apreciar, con base en los parámetros de configuración del contenido, que existe una diferencia de mejora cuando se logra realizar la transmisión en contenido IPv6 frente IPv4 en términos del retardo introducido a la red en un entorno de laboratorio bajo las mismas condiciones para ambos protocolos. Esta mejora, sin embargo, es observable por medio de mediciones basadas en análisis de tráfico por medio de la utilización de software especializado para este ejercicio, como Wireshark o Colasoft de Camtasia y no se presenta hasta este punto una diferencia notable a nivel de percepción, no obstante, esto último se analiza en la sección del análisis de la calidad de experiencia.

Figura 43. *Comparativa del Jitter (ms) entre IPv4 e IPv6 para la cola de tráfico Q1 (256kbps).*



Nota*:* el primer par de columnas de cada segmento de calidad (resolución) en la figura 42, representa los valores de jitter para h.264, mientras que los valores de las dos últimas columnas para cada valor de resolución representan el retardo para h.265.

Si bien el entorno de laboratorio se ha planteado para formatos de resolución 360p, 720p y 1080p como formatos mayormente utilizados para la transmisión de contenido multimedia adaptativo a las variaciones de la capacidad de descarga y ajustables a los parámetros de *Buffering* en la presentación del contenido, se ha agregado un ejercicio adicional como valor

agregado al desarrollo de la investigación y que será mencionado igualmente en la sección de trabajos a futuro.

5.2.1 Prospecto de transmisión mediante los parámetros más favorables.

Con base en los resultados obtenido en las practicas realizadas, se abre la posibilidad de aplicar una combinación de los parámetros más favorables en la transmisión de contenido multimedia bajo el formato 2160p de manera que sea escalable y adaptativo en la red. Esto es posible a partir de la transmisión de contenido multimedia en formato 2160p (o similares a 4K o UHD) mediante la utilización del protocolo de internet IPv6 aplicando el códec HEVC (H.265), marcado de tráfico que permita etiquetar las conexiones y los paquetes para el este contenido multimedia, con lo cual es posible aplicar políticas de calidad de servicio, dando prioridad de tasa de transmisión, como se pudo observar en la Tabla 3, en donde se muestra que para el contenido con el mayor formato de calidad (2160p) utilizado, el Jitter disminuye cuando se encuentra ante un encolamiento de tráfico de 1000Kbps (1Mbps).

Es importante agregar, que para un mejor desempeño de una red de datos en general, es necesario aplicar políticas de calidad de servicio que permitan clasificar los tipos de tráfico mediante el marcado de los paquetes y la segmentación de la red a través de diferentes VLAN´s a través de las cuales sea posible aplicar dichas políticas. Sin embargo, se evidencia que para la segmentación de los dominios de red a través de las VLAN´s per se, no es suficiente para mejorar la ocupación del ancho de banda cuando se está transmitiendo contenido multimedia (véase Figuras 1 y 2), sino que este tipo de servicio demanda la utilización del códec HEVC o H.265 que permita la disminución de los tamaños de los ficheros, así como también, la conversión de los ficheros a un contenedor que lo haga más liviano, como se pudo observar en

la Figura 11 (Bitrate versus Tamaño del Fichero para los Contenedores .mov y .mp4), y finalmente, la adopción del protocolo IPv6 de manera nativa, ya que, de acuerdo con los resultados obtenidos, evidencia una mejora de aproximadamente 2% (0.5 ms) bajo colas de tráfico de por lo menos 1Mbps.

Una de las principales preocupaciones mencionadas en el marco problémico gira en torno a las amenazas de seguridad presentes en las redes de datos y especialmente, en las infraestructuras físicas que incorporan el protocolo IPv6. No obstante, aunque no se despliegue el protocolo IPv6 como tal en la red, este se utiliza en background mediante la comunicación entre dispositivos, especialmente por medio de las direcciones fe80:: de ipv6, especialmente asignadas como direcciones IPv6 de enlace local, y usadas para el establecimiento de comunicación a nivel local entre máquinas y representa un vector de ataque para las redes de datos, como se evidencia en las fase 4; parámetros de seguridad IPv6.

Y es precisamente a través de este vector de ataque, que se logró evidenciar que los ataques propuestos para el entorno controlado de laboratorio incorporan este direccionamiento y fue posible validarlo por medio de la herramienta Wireshark mediante *Sniffing* de tráfico.

Como se pudo observar para cada una de las secciones de la fase 4 relacionada con los parámetros de seguridad, se realizaron cuatro tipos de ataques de seguridad orientados a IPv6 a fin de analizar su incidencia en el tráfico multimedia que se transmitía a través de la red por medio de este protocolo y se propuso para cada uno de los ataques, una política de seguridad a nivel perimetral de la red que evita se lleve a cabo el despliegue de cada uno de los ataques propuestos.

Con base en lo anterior, se concluye que es imprescindible la incorporación de políticas de seguridad a nivel, no solamente de enlace y de red, sino de aplicación, para el protocolo Ipv6

y que las políticas de seguridad implementadas para las redes de datos generalmente se implementan específicamente el protocolo IPv4 y se crean reglas de manera general para Ipv6 pero que no son lo suficientemente robustas para detener o evitar los ataques propuestos en el laboratorio. Existen otros métodos para evitar estas incidencias en la red, dependiendo del nivel (OSI[23]) que se esté utilizando, como por ejemplo a nivel de la capa de enlace, evitar los ataques de MITM mediante la aplicación de seguridad en los puertos de los equipos de distribución de manera que permita únicamente una dirección MAC por puerto asociada al direccionamiento IPv6. A nivel de red, políticas de firewall que se integren con la capa de transporte igualmente, como se ha mencionado anteriormente, por medio del marcado de conexiones y paquetes en la transmisión de diferentes tipos de contenido.

Se pudo observar que el desempeño de los dos protocolos de internet IPv4 e IPv6 fue similar en las dos primeras colas de tráfico, cuando este se transmitió codificado en H.264 y H.265. sin embargo, se pudo observar una mejora en la diferencia del retardo en la transmisión de paquetes cuando se aplicó la cola de 1000Kbps (1Mbps) a través del protocolo IPv6, particularmente cuando este se transmitió codificado en H.265.

La calidad perceptual del contenido se reflejó mediante la emulación de los parámetros subjetivos de evaluación de la calidad de la experiencia del contenido a través de la aplicación de las pruebas que permitieron comparar el contenido original versus el contenido procesado para los 3 formatos de calidad propuestos, codificados tanto en H.264 como en H.265.

De acuerdo con la fase, se observa en primera instancia que, para el análisis de todos los formatos conseguidos en las comparativas de los formatos de contenido original versus el contenido procesado, se obtuvieron métricas por debajo de 0,5 para el entorno de transmisión,

[23] (Open Systems Interconnected). Arquitectura estandarizada desarrollada por la ISO que divide los niveles de comunicación de datos en 7 capas, desde la física hasta la capa de aplicación.

lo que significa que, para la escala de VQM, se obtienen valores como mínimo aceptables para esta consideración. Por otra parte, se evidencia que los valores de VQM obtenidos para todos los formatos bajo el estándar de compresión H.265 muestran una mejora en la medida en la que se aumenta el formato de calidad del contenido multimedia, adicionalmente, para cada formato de calidad, es notable la diferencia entre las métricas obtenidas para cada bitrate. Si se toma como referencia el formato 2160p, se puede observar que, por una parte, el valor disminuye cuando se compara H.264 con H.265, siendo este último, el que muestra un mejor desempeño, y por otra, que el valor VQM también disminuye mientras que la tasa de bit aumenta, es decir, para el formato de referencia, se obtiene que el mejor valor posible obtenido, corresponde a la tasa de bit de 1024kbps en H.265.

Sin embargo, las métricas también muestran una característica que se puede describir al comparar el formato 720p con el formato 2160p, ya que, este último si bien corresponde al formato de mejor calidad perceptual, muestra valores de VQM más altos que el formato de 720p. Para lograr identificar la razón de esta diferencia, es necesario establecer en primer lugar que todos los formatos utilizados para el laboratorio están configurados previamente en 24 fps (frames por segundo) ya que, de no ser así, esto podría concurrir a un error significativo en la toma de resultados. En segundo lugar, cabe aclarar que el software utilizado para la realización de la comparativa, MSU VQMT Demo 13.1[24], tiene características de funcionamiento que permiten un mejor desempeño hasta el formato FHD (1920*1080p), es por esto, que al procesar un segmento con un formato mayor, encuentre se cuente con errores de distorsión de bloques debido a la capacidad de procesamiento de los frames para este contenido, esta diferencia se puede traducir en un desmejoramiento del VQM en 2160p frente a 720p.

[24] Software de escritorio especializado para el análisis de contenido multimedia procesado.

Para el ejercicio adicional realizado con base en el formato de 2160p, se hace la precisión de que los parámetros objetivos observables a partir de las gráficas y métricas obtenidas, se realizaron únicamente para efectos de seguimiento de tráfico y no a partir de la visualización del contenido, ya que no se cuenta con una interfaz de visualización que soporte este formato de calidad, como máximo.

6. Trabajo futuro

Existen varios puntos de vista al analizar el trabajo a futuro en las áreas de comunicaciones aplicadas objeto de investigación del presente documento, y las cuales se cohesionan al aplicarse en la transmisión de contenido multimedia.

Una de las principales áreas a explotar se presenta como la adopción del protocolo IPv6, ya que, como se ha mencionado en el desarrollo del trabajo de investigación, existe aún falta de implementación de este protocolo en Colombia, particularmente para los usuarios residenciales. Sin embargo, algunos proveedores de servicios de internet ya están incorporando este protocolo en algunos planes, especialmente empresariales, pero la brecha es aún larga para dar cobertura total a nivel nacional de IPv6. Por otra parte, la iniciativa debe nacer desde la academia como centro de investigación e impulso para este tipo de tecnologías disruptivas.

Este protocolo presenta una mejora considerable en la transmisión de contenido multimedia en formato FHD o superior (UHD) codificado en h.265, ya que dadas las condiciones de redes de difusión de contenido, la masificación de la difusión de streaming multimedia adaptativo en alta calidad a través de las redes convergentes y el aumento exponencial de usuarios a nivel mundial, crean la necesidad de incorporar este protocolo que, a través del documento, se ha evidenciado que presenta una mejora para este tipo de tráfico.

En cuanto a los códecs de video, existen iniciativas como la codificación de video versátil VVC/H.266, AV1 y VP9 y que es llamada a mejorar lo logrado hasta entonces con H.265. Esta tecnología ha presentado igualmente retrasos en su lanzamiento en el marco de la pandemia mundial impuesta por el Covid-19, ya que se esperaba que para el 2021 estuviese operativa a nivel mundial y, sin embargo, aún está como prototipo de laboratorio. VVC supone la capacidad de realizar transmisiones de contenido en formato 8K (7680*4320), y que se espera este formato tenga presencia gradualmente en la próxima década a nivel mundial.

Y es precisamente esto último, lo que representa el mayor reto a superar en términos de transmisión de contenido multimedia a nivel global, ya que justo ahí se incorporan las diferentes tecnologías utilizadas en el presente proyecto de investigación; protocolo IPv6, calidad de servicio y calidad de experiencia, transmisión de contenido multimedia por medio de herramientas adaptativas para streaming a través de las redes de datos que se acoplen a la capacidad de la red y de los equipos a través de los cuales se presenta el contenido.

Por otra parte, se espera la incorporación de contenido multimedia tenga este gran salto a nivel mundial en los próximos años y, con esta investigación, se dejen puertas abiertas que permitan analizar los diferentes campos de estudio para hacer posible la adopción de estas nuevas tecnologías de forma masiva.

Se logró obtener adicionalmente, resultados preliminares que permiten abrir las puertas a futuros trabajos en áreas de transmisión de contenido multimedia adaptativo para redes convergentes que permitan acarrear contenido en formato UHD o similar. Se obtuvo entonces como primer resultado de este experimento adicional, que existe una diferencia notable en el tamaño del fichero para el formato 2160p cuando este se codifica en h.265 frente al mismo fichero codificado en h.264 (véase Figura 14).

Finalmente, con respecto al contenido configurado en formato 2160p, se concluye que la generación de contenido multimedia en formatos UHD o similares, y el procesamiento de este tipo de contenido, demanda la utilización de hardware de determinada capacidad para lograr agilidad en este proceso, por lo cual, contado con el hardware disponible para la realización de las prácticas requeridas, iniciando con la compresión del contenido original en los códecs h.264 y h.265 bajo el formato 2160p y la aplicación de pruebas y mediciones de parámetros objetivos como el Jitter y el PSNR, conlleva a un tiempo de espera de alrededor de 3 minutos para generar un archivo de salida en el formato esperado, por lo cual se recomienda la utilización de tarjeta de video dedicada para esta función específica

Referencias

[1] A. J. a. M. Riveros, «Carteleras DIgitales, P. La, U. Santo.,» 2015.

[2] V. E. Rodr, «Design, Implementation and Evaluation of IPv4/IPv6 Longest Prefix Match support in Multi-Architecture Programmable Dataplanes,» 2018, pp. 6 - 11.

[3] R. A. M. Puentes, R-DC-96 Plantilla de Informe Final Monografía, Seminario Emprendimiento, Bucaramanga, 2017.

[4] E. N. W. S. T. Narten, Neighbor Discovery for IP Version 6 (IPv6), 2009.

[5] O. D. R. Troan, «IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6,» RFC 3633, 2003.

[6] M. R. E. Handley, «Internet Denial-of-Service Considerations,» RFC 4732, 2006.

[7] T. K. C. Socolofsky, «A TCP/IP Tutorial,» Spider Systems Limited, 1991.

[8] A. S. C. B. P. M. M. N. H. M. V. Y. D. G. Caiza, Implementacion de un prototipo como sistema detecetor de intrusos para ataques dirigidos al protocolo IPv6, Cumbres, Vol. 3, no. 2, pp. 9-16, 2017, 2017.

[9] G. J. D. O. A. Borowka, No Titlee, vol. 2, Conference Proceedings, 2013.

[10] R. H. S. Deering, «rfc 8200,» July 2017. [En línea]. Available: https://tools.ietf.org/html/rfc8200.

[11] D. A. R. P. Agency, «rfc 791,» September 1981. [En línea]. Available: https://tools.ietf.org/html/rfc791.

[12] T. S. a. S. Operation, «ITU-T E.800,» 2008. [En línea]. Available: https://www.itu.int/rec/T-REC-E.800-200809-I.

[13] I. T. Union, «Vocabulario sobre calidad de funcionamiento, calidad de servicio y calidad de experiencia,» 19 December 2007. [En línea]. Available: https://www.itu.int/rec/T-REC-P.10-201711-I/es.

[14] T. Committee, «Information Technology, Security Techniques, Guidelines for privacy and security in Internet of Things,» 2019. [En línea]. Available: https://www.iso.org/standard/44373.html.

[15] C. -. S. A. Board, «1857.7-2018 - IEEE Standard for Adaptive Streaming,» 10 December 2014. [En línea]. Available: https://standards.ieee.org/standard/1857_7-2018.html.

[16] C. -. S. A. Board, «1857-2013 - IEEE Standard for Advanced Audio and Video Coding,» 29 March 2012. [En línea]. Available: https://standards.ieee.org/standard/1857-2013.html.

[17] A. C. a. G. B. K. Dadheech, «De-Militarized Zone: A Next Level to Network Security,» de *2018 Second International COnference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, 2018, pp. 595-600.

[18] C. P. F. D. T. &. A. L. Maria Torres Vega, «A Review of Predictive Quality of Experience Management in Video Streaming Services,» de *IEEE Transactions on Broadcasting*, 2018, pp. 64(2), 1-14.

[19] I. -P. Registries, «Internet Assigned Numbers Authority,» IANA, 2019. [En línea]. Available: www.iana.org/protocols.

[20] LACNIC, «LACNIC - Inicio,» Lacnic, 2019. [En línea]. Available: www.lacnic.net/.

[21] ARIN, «American Registry for Internet Numbers,» 2019. [En línea]. Available: https://www.arin.net/.

[22] RIPE, «Network Coordination Centre, RIPE,» 2019. [En línea]. Available: https://www.ripe.net.

[23] APNIC, «APNIC,» 2019. [En línea]. Available: https://www.afrinic.net/.

[24] AFRINIC, «AFRINIC,» 2019. [En línea]. Available: https://www.afrinic.net/.

[25] E. A. a. A. G. Tome, Redes Cisco. Guía de Estudio Para la Certificación CCNA Routing y Switching, 2014, p. 510.

[26] S. D. R. Hinden, «Arquitectura de Direccionamiento IP version 6, RFC4291,» 2006.

[27] S. D. S. Hinden, «Internet Protocol, Version 6 (IPv6) Specification,» RFC 2460, 1998.

[28] C. Alonso, «EvilFOCA, elevenpaths-labstool,» 2019. [En línea]. Available: http://www.elevenpaths.com.

[29] S. U. Tomás, «Plan General de Desarrollo,» 2019. [En línea]. Available: http://fliphtml5.com/xben/kmwb.

[30] T. U. Union, «ITU - International Telecommunication Union,» 2007. [En línea]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/bt/R-REC-BT.1833-3-201402-I!!PDF-E.pdf.

[31] T. I. Union, «ITU - International Telecommunication Union,» 2001. [En línea]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/f/R-REC-F.1399-1-200105-I!!PDF-E.pdf. [Último acceso: 02 2020].

[32] I. «IANA - Internet Assigned Number Authority,» 2020. [En línea]. Available: https://www.iana.org/numbers. [Último acceso: 03 02 2020].

[33] M. L. C. H. &. T. M. D. C. Huang, «Scalable MPEG-4 Streaming over the IPv6 mobile network environment.,» *Computer Communications,* p. 29(16), 2005.

[34] P. Dell., «On the dual-stacking transition to IPv6: A forlorn hope?,» *Telecommunications Policy,* pp. 42(7) 575-581, 2018.

[35] R. H. &. R. Jabbar, «End-to-End (e2e) Quality of Service (QoS) for IPv6 video streaming.,» *19th International Conference on Advanced Communication Technology (ICACT),* pp. 67(6), 1-1, 2017.

[36] S. B. &. L. F. Savvas Papagiannidis, «Well beyond streaming video:; IPv6 and the next generation television.,» *Technological Forecasting and Social Change,* pp. 73(5), 510-523, 2006.

[37] X. L. G. Q. S. Y. Z. L. &. B. Y. D. Gu, «VNET:6 IPV6 virtual network for the collaboration between applications and networks.,» *Journal of Network and Computer Applications,* pp. 36(6), 1579-1588, 2013.

[38] Q. Y. F. R. Y. &. V. L. Y. Guo, «Cache-Enabled Adaptive Video Streaming over Vehicular Networks: A Dynamic Approach.,» *IEEE Transactions on Vehicular Technology,* pp. 67(6), 1-1, 2018.

[39] Y. K. &. G. Lence, «Methodology for the indentification of potencial issues of diferrent IPv6 transition technologies: Threat analysis of DNS64 nad satetful NAT64.,» *Computers and Security,* vol. 77, pp. 397-411, 2018.

[40] Á. S. &. J. M. Elsa Macías, «Using OSLR for Streaming Video in 802.11 Ad-Hoc Networksto save Bandwith,» February 2018.

[41] I. Cisco & Cisco Systems, «Forecast and Methodology, 2010 - 2015, 2017-2022,» *Cisco Visual Networking Index,* 2011.

[42] M. Z. &. X. Z. Y. Tian, «Internet Video Data Streaming,» 2017.

[43] P. D. R. F. L. G. M. T. a. L. V. C. Bodei, Firewall Management with FireWall Synthesizer, vol. 2058, C. W. Proc., Ed., 2018, pp. 1-7.

[44] E. Al-Shaer, Dynamic Firewall Configuration Optimization in: Automated Firewall Analytics., e. P. C. Science, Ed., Springer, Cham, 2014 .

[45] A. T. &. A. Castillo, «Projecting the Growth and Economic Impact of the Internet of Things,» *Economic Perspectives,* p. 10, 2015.

[46] J. K. B. Z. P. N. J. Arkko, «RFC 3971 "Secure Neighbor Discovery (SEND)",» RFC 3971, Marzo 2005. [En línea]. Available: https://tool.ietf.org/html/rfc3971.

[47] J. L. .. Shah, Secure neighbor discovery protocol: Review and Recommendations, Srinagar: Cluster University Srinagar, January - June 2019.

[48] G. Y. a. J. Bi, «A CGA based IP source address authentication methon un IPv6 access network,» de *33rd IEEE Conference on Local Computer Network (LCN)*, Montreal - Que., 2008, pp. 534-535.

[49] J. S. a. H. Y. K. M. Ki, «ROUTE/DASH Server system development for real-time UHD broadcasting,» de *Int. Conf. Adv. Communication Technology.*, 2017.

[50] M. Z. e. al., «QoE-driven optimizarion dor cloud-assisted DASH-based scalable interactive multiview video streaming over wireless network,» de *Signal Process Commun*, 2017, pp. 157-172.

[51] U. «Metodologías para la evaluación subjetiva de la calidad de las imágenes de televisión,» *Recomendación UIT-R BT.500*, p. 110, 10 2019.

[52] Y. L. P. Rafael Alejandro Olivera Solis, «scieo.sld.cu,» agosto 2019. [En línea]. Available: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282019000200022&lng=es&nrm=iso. [Último acceso: 03 enero 2020].

[53] Blender Foundation, «mango.blender.org/,» 2012. [En línea]. Available: https://mango.blender.org/.

[54] D. B. O. M. P. «Sintel,» Durian Blender, 2013. [En línea]. Available: www.sintel.org. [Último acceso: 31 10 2020].

[55] «FFMPEG,» Telepoing.bg, 2020. [En línea]. Available: https://ffmpeg.org.

[56] B. Zill y P. Nikander, «Secure Neighbor Discovery (SEND),» marzo 2005. [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc3971. [Último acceso: 15 09 2021].

[57] P. Margarte H, «A new standardized method for objectively measuring video quality,» *IEEE Transactions on broadcasting50.3,* 2004.

[58] K. Romer, «Objective and Subjective Measurements,» de *Objective and Subjective Measurements*, 2012.

[59] S. Akramullah, Digital Video Concepts, Methods and Metrics, New York: Springer Science+Business Media New York, 2014.

[60] S. Winkler , Digital Video Quality: Vision Models and Metrics, 1997.

[61] M. d. E. Nacional, «Concejo Nacional de Acreditación,» 29 01 2016. [En línea]. Available: https://saces.mineducacion.gov.co/cna/Buscador/Fortalezas.php.

[62] Q. Q. S. Limited, «QS Stars Explained,» 2019. [En línea]. Available: https://www.qs.com/qs-stars-explained/.

[63] I. I. p. e. A. d. l. Calidad, «Cinda,» 07 2019. [En línea]. Available: https://cinda.cl/wp-content/uploads.

[64] E. Lee y V. Chan, «Part 1: optical communication over the clear turbulent atmospheric channel using diversity,» *IEEE Journal on Selected Areas in Communications,* vol. 22, 15 November 2004.

[65] W. Robitza, «CRF Guide (Constant Rate Factor in x264, x265 and libvpx),» 24 February 2017. [En línea]. Available:

https://slhck.info/video/2017/02/24/crf-guide.html. [Último acceso: 27 January 2020].

[66] V. Thirumalai , H. N. Jacobson y L. R. Joshi, «Quantization parameter (QP) calculation for display stream compression (DSC) based on complexity measure,» 2016. [En línea]. Available: https://patents.google.com/patent/US10284849B2/en.

[67] S. Thompson, T. Narten y Jinmei, «IPv6 Stateless Address Autoconfiguration,» *IETF RFC 4862 Cisco, IBM, Toshiba,* 2007.

[68] Telefónica Cybersecurity & Cloud Tech, S.L.U., «Telefonica Tech Ciber Security,» Telefonica Tech, 08 2021. [En línea]. Available: https://www.elevenpaths.com/. [Último acceso: 31 08 2021].

[69] E. Hjelmvik, «Netresec,» 17 07 2015. [En línea]. Available: https://www.netresec.com/?page=Blog&month=2012-07&post=WPAD-Man-in-the-Middle. [Último acceso: 02 09 2021].

[70] Rigney, C., «RADIUS Accounting,» abril 1997. [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc2139. [Último acceso: 22 09 2021].

[71] G. H. Tolosa, «Protocolos y Modelos OSI,» *Laboratorio de Redes,* 2014.