ANÁLISIS DE DESEMPEÑO PARA UNA RED IP CON TRÁFICO GENERADO POR UN SERVIDOR DE VIDEO STREAMING UTILIZANDO PROTOCOLOS DE ENRUTAMIENTO TIPO IGP, MULTICAST Y UNICAST PARA IPv4 E IPv6.

Autor:
ANDRÉS FELIPE MACÍAS DÍAZ
Estudiante Ingeniería de Telecomunicaciones

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
2013

ANÁLISIS DE DESEMPEÑO PARA UNA RED IP CON TRÁFICO GENERADO POR UN SERVIDOR DE VIDEO STREAMING UTILIZANDO PROTOCOLOS DE ENRUTAMIENTO TIPO IGP, MULTICAST Y UNICAST PARA IPv4 E IPv6.

Autor:

ANDRÉS FELIPE MACÍAS DÍAZ

Estudiante de Ingeniería de Telecomunicaciones

Directora:

MAYRA LILIANA SALCEDO GONZÁLEZ

Ingeniera de telecomunicaciones

Master oficial en tecnologías redes y sistemas de comunicaciones

Asesor:

JULIO ERNESTO SUAREZ PÁEZ

Ingeniero de telecomunicaciones

Magister en Ingeniería de Telecomunicaciones

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERIA DE TELECOMUNICACIONES

BOGOTÁ D.C.

2013

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C, Octubre XXXX de 2013

Agradecimientos

La realización de este proyecto fue posible gracias a la constante ayuda y asesoría del ingeniero Julio Suarez y la ingeniera Mayra Salcedo, los cuales compartieron sus conocimientos y dieron su apoyo total para lograr los objetivos establecidos en este proyecto.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

El servicio de IPTV ha despertado el interés en el mundo de las telecomunicaciones, al ser visto como la nueva tendencia en la televisión por suscripción, con el fin de ofrecer al usuario televisión de alta calidad (HD) en una red de telecomunicaciones, a través del protocolo IP. Sin embargo, el despliegue de este servicio hará exigencias a la red por la cual sea desplegado; estas exigencias serán diferentes según los parámetros técnicos y protocolos desplegados en cada red, entre los cuales se destacan la versión del protocolo IP (IPv4 o IPv6) y el tipo de tráfico (Unicast o Multicast). Por ello, es necesario para un operador de telecomunicaciones conocer cómo será el rendimiento de su red al ofrecer este tipo de servicio. Esta investigación surge también a la necesidad social que se encuentra adherida al servicio que se pretende ofrecer en la red, pues el contenido visual que se transmite puede ser con fines educativos o culturales, para así brindar oportunidades de educación a las personas que habitan en los sectores más alejados de las ciudades.

En este proyecto de grado se implementó una red que soporte el tráfico requerido por un servidor de Streaming, simulando el tráfico de televisión con un video de alta calidad, usando herramientas de software libre. Para ello se utilizaron los equipos Huawei adquiridos por la Universidad para el desarrollo del proyecto de investigación principal, aprobado por el FODEIN y liderado por los Ingenieros Mayra Salcedo y Julio Suárez. Con el fin de realizar este proyecto se implementó el montaje del servidor de tal forma que sea compatible con un IMS CORE (IP Multimedia Subsystem), el cual controla los servicios prestados por una red NGN (Next Generation Network); finalmente se envió el tráfico de Video en IPv4 Unicast y Multicast e IPv6 Unicast y Multicas, acto seguido se realizaron comparaciones de desempeño en los equipos activos de la red. Adicionalmente se presenta la implementación y uso del servidor de IPTV UCT (1) con el cual se complementa el trabajo realizado para verificar la compatibilidad del servidor de streaming con el

IMS CORE.

En este documento se presenta la monografía del proyecto, donde se realiza la documentación del trabajo desarrollado, dividiéndolo en marco teórico, mostrando el desarrollo del proyecto, la forma como se hizo, los resultados obtenidos, el análisis de estos resultados y finalmente las conclusiones.

1. OBJETIVOS

1.1 Objetivo general

- Analizar el desempeño de una red IP usando el tráfico generado por un servidor de Video Streaming teniendo en cuenta los parámetros de desempeño, específicamente: uso de interfaz, uso de procesador y ocupación de memoria, con protocolos IPv4 e IPv6, determinando las diferencias entre estos dos protocolos.

1.2 Objetivos específicos

- Implementar una plataforma de Video Streaming usando herramientas de software libre.
- Configurar en los equipos Huawei de la Universidad, el protocolo de enrutamiento tipo IGP para IPv4 e IPv6.
- Configurar sobre equipos IP, protocolos de enrutamiento de Multicast como PIM-SM o PIM-DM.
- Implementar un servidor de monitoreo de red SNMP utilizando herramientas de software libre.
- Realizar pruebas de uso de interfaz, uso de CPU y ocupación de memoria en los equipos IP a través del servidor SNMP y la consola de los equipos activos.

2. PROYECCION SOCIAL DEL PROYECTO

El estudio de las humanidades en la universidad Santo Tomas brinda al estudiante las herramientas necesarias para lograr llevar a cabo un desarrollo integral en la formación que debe adquirir para el ámbito laboral, social y cultural del país. Lograr fortalecer estos conocimientos en la mente de un estudiante le brinda criterio a la hora de llevar a cabo una vida profesional eficiente, en la que no solo realice una labor individual en beneficio propio, sino que mejore su calidad de persona llevando a cabo labores sociales en las cuales beneficie con sus conocimientos y trabajo a la comunidad en general o en particular. Por lo tanto es necesario fortalecer el componente humanístico con el fin de imponer en el profesional un pensamiento crítico acerca de las necesidades de su entorno y su cultura, con el fin de dar una característica social relevante. Es por ello que en este escrito se da el énfasis humanístico y social observado durante el desarrollo del proyecto de grado. Para un país es muy importante la educación de todos los sectores con el fin de lograr un desarrollo en sus ámbitos político, cultural, deportivo, tecnológico, económico, etc. Colombia es un país donde este tipo de desarrollo se encuentra aglomerado en las grandes ciudades como Bogotá, Medellín y Cali. Sin embargo, no toda la población se encuentra concentrada en estas urbes, sino que se encuentran en zonas apartadas del campo y no tienen la capacidad de acceder al sistema educativo que ofrece el gobierno, ya sea por falta de conocimiento sobre ese sistema o por falta de recursos para acceder a él. Que estas personas se adhieran al sistema, es muy importante para el desarrollo del país, ya que son ellos, los que trabajan el sector agrícola, minero, agropecuario y ganadero, es decir, son una parte importante para la economía del país por lo tanto, que tengan conocimiento acerca de métodos con los cuales mejorar su productividad, de la mano de expertos en el tema es crucial a la hora de posicionar a Colombia como un país desarrollado.

Para lograr este objetivo es muy importante que en Colombia se tenga en cuenta el desarrollo tecnológico, pues es a través de sistemas de telecomunicación y de informática que una persona campesina pueda acceder a una educación virtual o plan educativo del gobierno de manera gratuita. Sin embargo, hasta ahora, se está comenzando a realizar este tipo de desarrollos en nuestro país y es por ello que es de suma importancia la investigación y el estudio de redes que lleven los contenidos educativos, los cuales en su mayoría se muestran a través de videos y teleconferencias, generados por medios audiovisuales, transportados desde su origen en la ciudad, hasta el destino en un pueblo rural alejado de la urbe. Lograr este transporte es un objetivo fundamental de los operadores de telecomunicaciones, los cuales tienen desplegadas redes de datos y redes de transporte a través de fibra óptica. Sin embargo, las redes de datos necesitan de constante monitoreo y gestión para que el video que se está transportando o el streaming que se esté realizando llegue a su destino con buena calidad y sin retardos. Para ello es necesario realizar un estudio en la red en el cual se

especifique cuales equipos se requieren para soportar este tipo de tráfico, cuantos clientes pueden estar utilizando la red al mismo tiempo sin que esta colapse.

Es por ello que en este proyecto de grado se implementó un servidor de streaming en una red la cual simula a red de datos de un operador telecomunicaciones, para así realizar un estudio de investigación que ayude al operador a establecer su plan a la hora de ofrecer estos servicios comunitarios. A su vez se puede evidenciar el uso de los conocimientos adquiridos en la carrera en el ámbito técnico de las redes de datos. Es un trabajo técnico el cual ayuda a un operador a conocer sus limitaciones y sus ventajas a la hora de transportar tráfico de video, el cual es usado por los usuarios para videoconferencias y streaming de video. Contar con una red capaz de cumplir con los requisitos exigidos para no presentar un fallo en los servicios que se brindan es vital para la credibilidad del operador, y a su vez se está brindando un beneficio a la comunidad en general, es decir, los usuarios que utilizarán el servicio en un futuro.

Por lo tanto este trabajo de investigación puede ayudar a un ingeniero encargado de desplegar la red del operador, a conocer los aspectos técnicos que debe tener en cuenta para que el servicio de video no se vea interrumpido a la hora de tener un cliente o varios clientes conectados. Los beneficios de desplegar este tipo de servicios en un país como Colombia son variados. Por ejemplo: un operador también necesita dar cobertura en su red a zonas apartadas en donde planes del gobierno como “Vive Digital” pretende dar educación digital a la población de estas zonas y a través de un streaming de video se puede ofrecer este servicio. La televisión es el medio de comunicación que más impacto tiene en la sociedad., por lo tanto, el objetivo de enviar contenido de televisión a través de computadores beneficia a los usuarios, ya que este contenido llega instantáneo, cuando el usuario lo requiera y es además de alta calidad. También abre las puertas a los creadores de contenidos digitales, tales como comunicadores sociales, cineastas o cualquier persona que quiera realizar contenido audiovisual, esto lo lleva a que desarrolle sus productos sin necesidad de crear su propio canal de televisión. Esto beneficia a la comunidad en general e incentiva el uso de la tecnología para mejorar el desarrollo del país.

Una inclusión social de este trabajo no solo sirve para lograr dar un enfoque humanístico sino también para lograr el desarrollo social expuesto anteriormente, lo que beneficia a la comunidad y logra un desarrollo del sector tecnológico del país. En conclusión, el enfoque de este proyecto de grado no solo se realiza como un trabajo técnico sino que también se constituye en un objeto social, logrando llevar a cabo una investigación que concierne al sector tecnológico, beneficiando a la población rural aislada que no tiene acceso a los sistemas educativos, al brindar estudios sobre métodos que permiten a las empresas de telecomunicaciones mejorar sus redes para brindar servicios educativos virtuales de alta calidad.

3. MARCO TEÓRICO

Para realizar este proyecto es necesario tener conocimiento de los protocolos y tipos de tráfico usados. Es por ello que dar una descripción del funcionamiento de estos conceptos ayuda a mejorar el entendimiento del proyecto. A continuación se presenta el marco teórico, donde se describirán teóricamente los protocolos y tipos de tráficos usados en este proyecto.

3.1 PROTOCOLO DE INTERNET (IP)

3.1.1 IPv4

IPv4 es la versión 4 del protocolo IP (Internet Protcol), el cual ofrece los mecanismos necesarios para transportar datagramas a través de una red. Este datagrama se encuentra formado por una cabecera IP y los datos que se quieren transportar (2). Sin embargo, IP no garantiza que el datagrama se entregue a su destino y por lo tanto para obtener mayor fiabilidad IP se ha concentrado en la capa TCP (Transport Control Protocol). En IPv4 las direcciones IP están conformadas por cuatro octetos de 8 bits cada uno, para formar 32 bits y cada máquina a la que se le quiere enviar la información tiene una dirección única, por ejemplo: 192.18.30.52. Cada máquina tiene también aparte de una dirección IP una máscara de subred, la cual tiene como función identificar la parte de red o de subred de una dirección (2). Las direcciones IPv4 se encuentran clasificadas en cinco grandes grupos: A, B, C, D, E.

Clase	Rango	Máscara de Red	Broadcast
A	1.0.0.0 - 126.255.255.255	255.0.0.0	x.255.255.255
B	128.0.0.0 - 191.255.255.255	255.255.0.0	x.x.255.255
C	192.0.0.0 - 223.255.255.255	255.255.255.0	x.x.x.255
D	224.0.0.0 - 239.255.255.255		
E	240.0.0.0 - 255.255.255.255		

Tabla 1: Clasificación direcciones IPv4. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

En la tabla 1 se puede observar los rangos de direcciones que pertenecen a cada clase, la máscara de red de cada rango y su dirección de broadcast. En el direccionamiento IPv4 se usan los rangos de direcciones dependiendo del número de host y el número de redes que se necesita. Para ello se utiliza la técnica VLSM(Variable Lenght Subnet Mask) (2).

Las direcciones 127.x.x.x son las de loopback, las cuales se reservan para lograr la identificación de la misma máquina.Las direcciones terminadas en 255 son las de broadcast, las cuales se usan para enviar información a todo un grupo de máquinas conectadas a la misma red. Las direcciones clase D son las denominadas multicast, las cuales representan un grupo de máquinas específico, mientras que el resto de direcciones son unicast. Las clase E están reservadas para investigación y academia, por lo tanto no se asignan a ninguna máquina.

3.1.2 IPv6

IPv6 es la versión mejorada del protocolo IP, con el cual se complementa IPv4 a la hora de hablar de las siguientes características:

- Las direcciones son de 128 bits divididas en 16 octetos.
- Simplifica la cabecera de IP pero posee cabeceras de extensión, en las cuales se pueden agregar nuevas funciones de intercomunicación cuando se necesiten.
- Dispone de más seguridad en la comunicación que IPv4
- Introduce flujos, los cuales se usan para especificar requisitos de transmisión, como en el video en tiempo real.

Como las direcciones IP son tan largas al tener tantos bits, se representan como ocho números hexadecimales separados por dos puntos, donde cada número hexadecimal representa 16 bits. Por ejemplo: 41BC:0:0:5:DDE1:8006:2334. Esta dirección se puede comprimir eliminando la serie de 0 por "::". Así la dirección anterior quedaría de la siguiente forma: 41BC::5:DDE1:8006:2334. La clasificación de las direcciones IPv6 es muy distinta a la de IPv4, teniendo en cuenta el hecho de la reasignación de las direcciones al conectarse a Internet (2) (3). La clasificación es la siguiente:

- **Direcciones locales (ULA)** (4)**:** son las direcciones que se encuentran en el bloque de red FC00:: y simbolizan las redes IPv4 privadas. Están permitidas para el uso en redes privadas y no pueden ser usadas en la Internet IPv6 (4). Este grupo también pertenece a las direcciones tipo unicast de IPv6.
- **Direcciones anycast:** estas direcciones son asignadas a un grupo de interfaces especifico y se encuentran presentes en varios puntos de la red. Cualquier dirección de unicast puede ser anycast.
- **Direcciones multicast:** tienen el mismo uso que las direcciones multicast IPv4.

IPv6 no implementa direcciones de broadcast.

3.2 TIPOS DE TRÁFICO EN IPv4

Al interconectarse las redes en IPv4, existen formas de envío de tráfico. Esto depende del destino hacia el cual se quiere enviar, ya que puede ser a un host en particular, a un grupo de máquinas en una misma subred, o de multienvío. Es por ello que el tráfico en IPv4 se ha dividido en la siguiente forma:

- **Unicast:** Es el tipo de tráfico más común en red, en el cual se envía a cada host de destino el tráfico proveniente del host de partida. Para ello se asignan a los host direcciones IPv4 de clase A, B o C, siendo cualquiera de estas direcciones de tipo unicast. El tráfico puede ser de cualquier tipo: video, audio, hipertexto, mensajes de control de la red, etc. Unicast es muy eficiente a la hora del envío de punto a punto en la red.
- **Broadcast:** Con IPv4 se pueden enviar datagramas a todos los host de una misma red. Esto se hace enviando dicho datagrama a una dirección de red específica dentro de la red. Por ejemplo: se tiene la red Ethernet 192.168.1.0 la cual posee cierta cantidad de host. Para enviar este datagrama a todos los host de la red se envía a la dirección 192.168.1.255 y todos los host recibirán el datagrama. Los routers y switches reconocen el formato de la dirección IP de broadcast para realizar la difusión de este tipo de tráfico, por lo tanto ningún host puede ser asignado con esta dirección. Esta dirección varía dependiendo del subnetting que se haya hecho en la red.
- **Multicast:** Este tráfico es una forma de envío múltiple, en el cual el datagrama que se requiere enviar en la red, duplica el número de veces que es solicitado, en vez de ser enviado como un tráfico de unicast a cada uno de los host que lo solicite. Para identificar este tipo de tráfico en la red se usan las direcciones de clase D (5), sin embargo estas direcciones no se asignan físicamente a las interfaces sino que se asignan como grupos de multicast. Un grupo de multicast es un conjunto de sistemas a los que se les ha asignado una dirección IP de multicast , tienen la capacidad de recoger los datos enviados a su dirección multicast, pero siguen manteniendo su propia dirección unicast.

3.3 TIPOS DE TRÁFICO EN IPv6

De la misma manera que IPv4, IPv6 implementa diferentes tipos de tráfico en sus direcciones. Las direcciones IPv6 de 128 bits identifican interfaces individuales o grupos de interfaces, y es así como una única interfaz puede tener múltiples tipos de direcciones IPv6 (2) (6). Estas direcciones pueden ser:

- **Unicast:** Del mismo modo que IPv4, este tipo de direcciones identifican a una única interfaz, y un paquete enviado a esta dirección será entregado sólo a la interfaz identificada con dicha dirección.
- **Anycast:** Las direcciones anycast identifican a un grupo de interfaces de forma que un paquete enviado a una dirección anycast será entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano según la distancia asignada en el protocolo de enrutamiento configurado (7). Estas direcciones utilizan cualquier formato de dirección unicast.
- **Multicast:** Al igual que las direcciones anycast, y al igual que las direcciones multicast en IPv4, este tráfico envía el paquete a un grupo de multicast formado por varios hosts en la red. Este tráfico suplanta al tráfico broadcast en IPv4, por lo tanto IPv6 no implementa direcciones broadcast (2).

3.4 ENRUTAMIENTO UNICAST

En esta sección se hace referencia a un gran número de protocolos usados para el enrutamiento de la información unicast. Varios de estos protocolos, como el OSPF usan una versión para IPv6, como es el caso de OSPFv3 (8), que tiene el mismo funcionamiento de OSPF.

3.4.1 OSPF

OSPF (Open Shortest Path First) es un protocolo de enrutamiento usado dentro de un SA (Sistema Autónomo) que incorpora métricas de estado de enlace y de distancia para construir un mapa de la red y así construir el camino que va a recorrer el paquete en la red. Además, el protocolo dispone de:

- Detección de los cambios en la topología de red y restablecimiento de la ruta sin bucles.
- Baja sobrecarga, usando actualizaciones que informan de los cambios en lugar de todas las rutas.
- División de tráfico por múltiples rutas
- Encaminamiento según el tipo de servicio
- Uso de multienvio en LAN

OSPF usa el enrutamiento por áreas para generar un mapa completo del enlace en esa área, por lo tanto cuando un router pide información de la red OSPF solo da información acerca del área a la cual el router pertenece (2) (7) (9). Todos los routers con OSPF en un área mantienen una base de datos de enrutamiento que describe la topología y estado de todos los elementos en esa área. Siempre que ocurre un cambio, la información se propaga por toda el área y de esta forma el

router da respuesta al problema. Un router que este iniciándose obtiene una copia de la base de datos actual de su vecino. Tras esto solo se comunican los cambios, que se llegan a conocer rápidamente pues OSPF usa un algoritmo de distribución eficiente para expandir la información de actualización por el área.

3.4.2 EGP

El protocolo EGP (Exterior Gateway Protocol) es el protocolo básico usado en la Internet para que los sistemas autónomos envíen información a redes externas, diciéndole a los routers con EGP cuales redes pueden llegar. Un router de EGP se configura con las direcciones IP de uno o más routers EGP vecinos exteriores, estando conectados a una red común multiacceso o unidos por enlaces punto a punto y así permitiendo al router descubrir que redes se pueden alcanzar a través de sus vecinos exteriores (2) (9). Sin embargo, no indica las rutas que siguen los datagramas hacia lugares externos, y oculta los sistemas autónomos que se atraviesan por el camino. Es por ello que se ha demostrado que este protocolo es inadecuado para el entorno actual y su uso ha disminuido (10).

3.4.3 RIP

RIP es un protocolo de enrutamiento de vector distancia que usa un algoritmo para establecer las rutas. En RIP a cada salto en la red se le asigna un “coste”, que normalmente es 1, y la métrica total de un salto es la suma de los costes de salto. Mientras tanto RIP elige el siguiente salto con el fin de que los datagramas sigan un camino de coste mínimo. La métrica máxima que tiene este protocolo para cualquier camino es de 15, cuando llega a 16 envía un mensaje de “no puedo llegar hasta allí” y al realizar un corte en la red RIP es muy lento para restablecer rutas optimas, y en forma similar no responde a los cambios en retrasos o carga en los enlaces. Por estas razones RIP es muy usado a nivel mundial en redes pequeñas o con topología simple.
Al empezar RIP, cada router necesita conocer solamente las redes a las que éste se encuentra conectado, por lo tanto difunde esta información solamente a todos los routers vecinos en la LAN. Así, la información se va divulgando en la red y un router puede saber a cuantos saltos esta de cada subred que compone la red, realizando así tablas de enrutamiento. Los pasos que realiza RIP para realizar el enrutamiento son las siguientes:

- Se asigna un coste de atravesar una subred conectada, este coste es 1 normalmente.
- El router envía su tabla de enrutamiento actual a sus vecinos cada 30 segundos.
- Cuando el router recibe la tabla del vecino comprueba cada entrada. Se añade a cada métrica el coste asignado a la subred por la que llegó la tabla.

- Si hay un destino nuevo, se añade a la tabla de enrutamiento local.
- Si algún destino ya existe en la tabla, pero la actualización ofrece una ruta más corta, se sustituye la entrada.

Con la versión 2 de RIP las tablas se envían a través del multienvío en vez de la difusión, por lo tanto se empaqueta más información en los mensajes de actualización (2).

3.4.4 IS-IS

Este protocolo se definió inicialmente para enrutadores que usaran el modelo OSI, pero se ha extendido para IP. IS-IS es un protocolo de estado de enlace que dispone de enrutamiento jerárquico, enrutamiento por tipo de servicio, división del tráfico por varias rutas y autenticación. Tiene dos tipos de rutas: el enrutamiento de nivel 1 dentro de un área y el enrutamiento nivel 2 para destinos fuera del área (2). Los routers de nivel 1 se pueden ver de forma análoga a enrutadores de una red troncal en OSPF. Se encargan de reenviar el tráfico a destinos fuera del área al router de nivel 2 más cercano. El tráfico se encamina a un router de nivel 2 conectado al área de destino. IS-IS usa avisos de estado de enlace, difusión y numero de secuencia, de manera similar a como lo hace OSPF.

3.5 ENRUTAMIENTO MULTICAST

En esta parte se describirán los protocolos más comunes usados por los routers para enviar tráfico multicast a través de la red. Estos protocolos se usan para IPv4 e IPv6 (6) (11).

3.5.1 PIM-SM

PIM (Protocol Independent Multicast) es el protocolo de enrutamiento que crea la estructura jerárquica de “árbol” con el fin de crear los grupos multicast entre los host. En la forma SM (Sparse Mode) es necesario configurar el RP (Rendezvous Point) o también llamado punto de encuentro, ya que en PIM-SM el RP es el encargado de enviar la información multicast a todos los routers PIM-SM conectados en la red (11). Cuando un receptor requiere datos de un grupo multicast especifico, el router conectado a dicho receptor envía un mensaje Join al RP asociado al grupo multicast. Las rutas de transmisión del mensaje hacia el RP forman las rapas del “árbol” RPT (RP-rooted tree). Cuando la fuente de emisión multicast intenta enviar datos al grupo multicast la interfaz conectada con la fuente se registra con el RP. Al llegar al RP, el paquete multicast se replica y se transmite a los receptores a los largo del RPT. Este tipo de configuración del RP es estática pues se asigna a una interfaz de un router PIM (6).
Otro aspecto importante de configuración de PIM-SM es el bootstrap router (BSR), el cual es el núcleo de gestión de la red PIM-SM. El BSR recoge información de

los Candidate-RPs (C-RPs) y escoge el C-RP apropiado para formar un RP-Set de cada grupo multicast. El RP-Set es una base de datos del mapeo entre los grupos y los RP. El BSR advierte entonces el RP-Set a la red PIM-SM, y así todos los routers saben dónde se encuentra el RP.

3.5.2 PIM-DM

PIM-DM (Dense Mode) usa el mismo método de árbol jerárquico que usa PIM-SM para enviar el tráfico multicast, sin embargo como lo hace es distinto, ya que al final, los nodos conectados a la red se suscribirán para recibir los paquetes multicast. El proceso de establecimiento del SPT (Source Pathed Tree) es un proceso de flooding and pruning (11). PIM-DM asume que todos los hosts de la red están listos para recibir el tráfico multicast. Cuando una fuente multicast empieza a enviar el tráfico a un determinado grupo, el router después de recibir el flujo, realiza un chequeo del RPF (Reverse Path Forwarding) basado en la tabla de routing unicast. RPF es una técnica usada por los routers para garantizar reenvío de los paquetes multicast y previene la suplantación de direcciones IP en enrutamiento unicast. Si el RPF no presenta errores, el router crea una entrada multicast y envía el tráfico a todos los nodos PIM-DM de la red. Si el RPF presenta fallos, el router descarta los paquetes, y la entrada es creada en cada router en el dominio multicast PIM-DM (11).
Cuando una interfaz de un router está conectada a un receptor multicast, esta interfaz se vuelve downstreams. Por defecto todas las interfaces de PIM-DM tiene receptores multicast virtuales, por lo tanto el tráfico es enviado por todas las interfaces. Sin embargo, si no hay interfaces downstream el router envía un mensaje prune a los nodos upstream indicándoles que no envíe más tráfico a los nodos downstream. Después de recibir este mensaje los nodos upstream eliminan la entrada multicast de la interfaz downstream de la tabla de routing multicast, siendo así el “árbol” SPT es construido (5) (6). De esta forma funciona el proceso flooding and pruning, el cual es ejecutado periódicamente.

3.6 PROTOCOLOS DE TRANSPORTE MULTIMEDIA

Existen protocolos de la capa de sesión usados en una red para transmisión de datos en tiempo real, así como audio y video. Entre ellos se encuentran los protocolos RTP y RTSP (12), ampliamente usados para videostreaming unicast y multicast. A continuación se hace una breve descripción de estos protocolos:

3.6.1 RTP

El protocolo RTP (Real Transport Protocol) nació ante la necesidad de establecer un protocolo específico para el transporte de datos en tiempo real. RTP se establece en el usuario y se ejecuta por lo general sobre UDP, que ofrece menor retardo que TCP, con lo cual se gana velocidad a cambio de confiabilidad. Es por ello que RTP (12) (13) no garantiza la llegada de los paquetes en el tiempo

adecuado. La función básica de este protocolo es multiplexar varios flujos de datos en tiempo real en un solo flujo de paquetes UDP (12), con el fin de enviar a un solo destino (unicast) o a múltiples destinos (multicast).

3.6.2 RTSP

El protocolo RTSP (Real-Time Streaming Protocol) es un protocolo basado en texto e independiente del protocolo de transporte, el cual permite realizar un control remoto de sesión de una transmisión multimedia, el cual permite: recuperar un determinado medio de un servidor, invitar a un servidor a unirse a un streaming, grabar el streaming. RTSP utiliza en parte el protocolo HTTP (12) (14) (Hyper Transfer Text Protocol) ya que emplea el uso de URL's para transmisión. De esta manera RTSP guarda el video a transmitir en un buffer del servidor, lo que permite el uso de VoD (Video on Demand), con el fin de que el usuario acceda al video cuando lo solicite y tenga libre reproducción del mismo.

3.7 PROTOCOLO SIMPLE DE GESTION Y MONITOREO DE RED

SNMP (Simple Network Management Protocol) es un protocolo creado para realizar la administración y gestión de una red TCP/IP de una manera rápida y sencilla. SNMP sigue el modelo de una base de datos lógica almacenada en el sistema donde se guarda información de configuración, estado, error y rendimiento de todos los componentes que conforman la red. Para tener acceso a esta información, el sistema administrado debe contener un componente de software denominado agente, el cual responde las peticiones, realiza actualizaciones e informa de los problemas (15) (2). Por lo tanto también existe un software de administrador o servidor, el cual envía y recibe los mensajes SNMP y se comunica con el agente para pedirle información del componente y guardarla en su base de datos. A su vez, existe la información, la cual se modela lógicamente en MIB's (Management Information Base), y contiene todos los datos de administración de la red en forma de variables, donde usualmente se guardan: información de estado y del sistema, estadísticas de rendimiento y parámetros de configuración. Por lo tanto, el administrador supervisa el sistema solicitando al agente del mismo que envía de vuelta los valores de los datos de su base de datos de la MIB y controla un sistema solicitando a sus agentes que actualicen el estado de las MIB's o los parámetros de configuración.

3.8 PARÁMETROS A MEDIR

En una red se tienen ciertos parámetros los cuales pueden ser medidos para determinar las características que la red presenta a la hora de enviar cierto tipo de tráfico y así analizar el comportamiento de la misma. Los parámetros usados en este proyecto fueron los siguientes:

- **Uso de interfaz:** Este parámetro muestra la velocidad de transmisión de una determinada interfaz de red, en un instante de tiempo específico. La unidad de medida más usada es Mb/s.
- **Uso de CPU:** determina el porcentaje de uso del procesador que un equipo está utilizando para su funcionamiento.
- **Uso de memoria:** determina el porcentaje de uso de memoria que un equipo está utilizando para su funcionamiento.

4. DESARROLLO DEL PROYECTO

Para la ejecución de este proyecto, se diseñó un ambiente de pruebas configurando una red WAN física. Para ello se tuvieron en cuenta los siguientes aspectos: topología de la red, equipos a utilizar y esquema de direccionamiento de red. Además, se hizo una justificación del software, protocolos de enrutamiento y sistema de gestión utilizados. Es por ello que en esta sección se explicará todo lo concerniente a como se llevó a cabo el desarrollo del proyecto.

4.1 AMBIENTE DE PRUEBAS DE RED

En el ambiente de pruebas de red se tuvo en cuenta la parte física, a la cual pertenecen los equipos que se tienen y como fueron conectados. También fué necesario tener en cuenta la parte lógica, la cual hace referencia al direccionamiento en IPv4 e IPv6 que se desarrolló para lograr el propósito de este proyecto. A continuación se muestra este desarrollo. Respecto al anteproyecto se realizó un cambio en cuanto al parámetro “throughput”, ya que se evidenció que lo que se iba a medir en el ambiente de pruebas era el uso de interfaz, el cual se especificó en el marco teórico, y se evidencia en las muestras tomadas con la herramienta de monitoreo de red.

4.1.1 Diseño físico

Para realizar las pruebas en los routers, se configuró una red WAN la cual involucró equipos, con las siguientes especificaciones:

- Servidor de Streaming: Computador con sistema operativo Ubuntu Server 12.04.
- Dos routers: Marca Huawei número de serie AR2220.
- Clientes: cinco computadores, 3 con sistema operativo Ubuntu Server 12.04 y dos con sistema operativo Windows 7.
- Switch: Marca Huawei S1700 Managed Series

Al tener estos equipos los conectamos en la siguiente red:

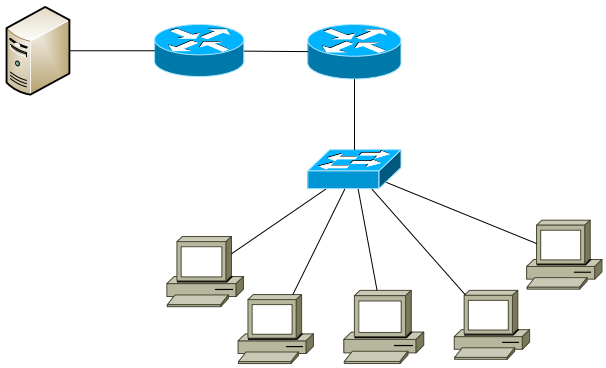

Figura 1: Interconexión de equipos en el ambiente de pruebas de red. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Este esquema de red es útil ya que proporciona los elementos de análisis necesarios a la hora de realizar las pruebas. El tráfico enviado pasó a través de los routers, los cuales se encargaron de transportarlo a cada cliente, dependiendo del tipo de prueba que se estaba realizando. Tener dos routers es necesario, ya que simula la red de un pequeño operador de telecomunicaciones. El switch es utilizado dependiendo del tipo de prueba, sin embargo es necesario para poder conectar más de un cliente a la red.

4.1.2 Diseño lógico

En esta parte se tuvo en cuenta el direccionamiento de red en IPv4 e IPv6. Es muy importante tener en cuenta que se simula que la red pertenece a una empresa carrier, por lo tanto se tienen muchas direcciones para host y algunas para red. Además las direcciones que se tuvieron en cuenta tienen que ser de tipo privado en la nube WAN y de tipo público en las interfaces conectadas al servidor y los clientes.

4.1.2.1 Direccionamiento de red en IPv4

En IPv4 se utilizó el siguiente esquema de direccionamiento de red:

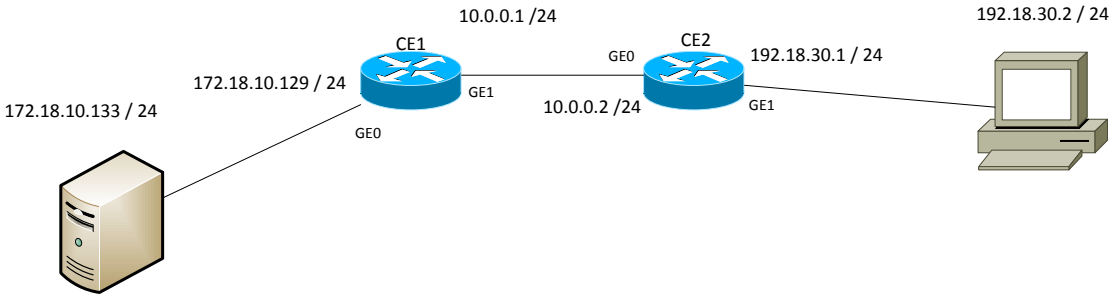

Figura 2: Esquema direccionamiento de red IPv4. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Este esquema es usado en unicast, con una máscara de red de 24 bits, lo que permite una conexión de 254 hosts por red. Se usó este tipo de direccionamiento para simular el direccionamiento usado por un operador de telecomunicaciones donde usa en su red WAN direcciones privadas, mientras que en sus interfaces de host usa direcciones públicas. Para conectar más de un host cliente a la red, simplemente se le configuró una dirección IP que se encuentra dentro de la red 192.18.30.0

Para multicast se utilizaron tres direcciones de red: 224.255.0.1, 224.255.0.2, 224.255.0.3. En cada dirección se envió el flujo de video correspondiente a cada canal configurado en el servidor de streaming, el cual se explica en la siguiente sección.

4.1.2.2 Direccionamiento de red en IPv6

Para IPv6 se utilizó el siguiente esquema de direccionamiento de red:

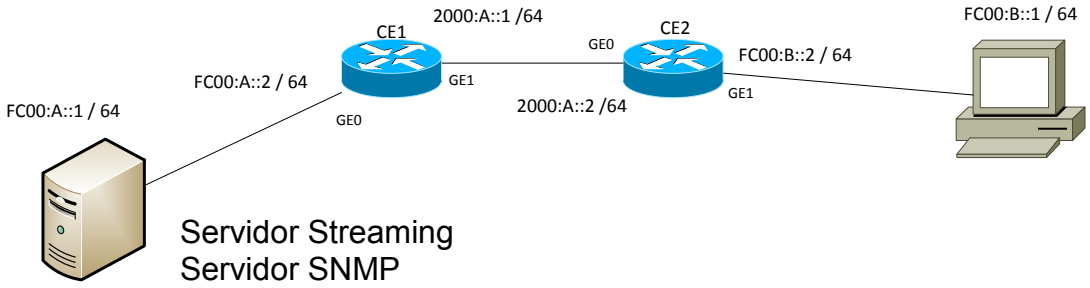

Figura 3: Esquema de direccionamiento de red IPv6. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Las direcciones usadas en este direccionamiento son de tipo ULA en las interfaces conectadas a los hosts y de tipo global en la red WAN. Se utilizó este direccionamiento para simular el caso en el que el operador usa en sus interfaces de red WAN direcciones públicas usadas para Internet, y en sus interfaces de host direcciones privadas. Este caso ocurre cuando el operador es contratado por una empresa que necesita sus direcciones LAN privada por cuestiones de seguridad (2) (3). Para conectar más hosts clientes a la red, se configura su dirección IPv6 dentro de la red FC00:B::

Para ambos casos se utilizó esta arquitectura de red ya que es similar a la topología de la red con la que cuenta la universidad en el laboratorio ETM 11, mostrada en la siguiente figura:

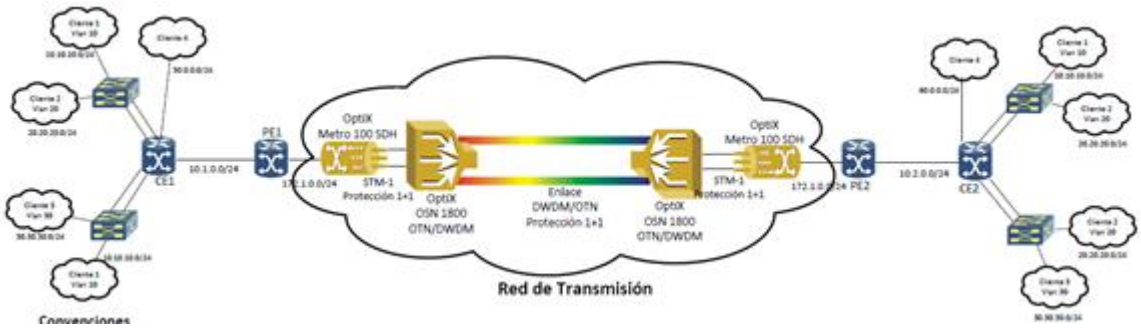

Figura 3.1: Arquitectura de red laboratorio USTA. Fuente: **Julio Ernesto Suárez Páez.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Como se puede observar, esta red cuenta con cuatro routers, dos interconectados a través de una red SDH/DWDM. En un principio se intentó utilizar esta red para realizar los objetivos de este proyecto, sin embargo se tuvieron limitaciones tecnológicas con los sistemas operativos de los routers, ya que no poseían la capacidad de transporte multicast en IPv6.

Para solucionar este problema se utilizaron dos routers Huawei AR2220 que fueron adquiridos en el proyecto de investigación liderado por el Ingeniero Julio Suárez tiutlado “Interconexión e interoperabilidad del laboratorio de comunicaciones unificadas en Bogotá y Bucaramanga sobre las Redes Academias Avanzadas RUMBO, UNIRED y RENATA” dentro del cual se desarrolló este trabajo de grado. Sin embargo, con soporte del fabricante fue necesario actualizar el sistema operativo de los equipos para que soportaran Multicast IPv6.

4.2 SOFTWARE UTILIZADO

Como el servidor de streaming se montó en una máquina Ubuntu Server se utilizó el software de video VideoLan, el cual es gratuito y sin licencia, por lo que se pudo adquirir libremente. Este programa es usado para la transmisión de video de cualquier formato con gran capacidad de ancho de banda (16). La solución de VideoLan se muestra en la siguiente figura:

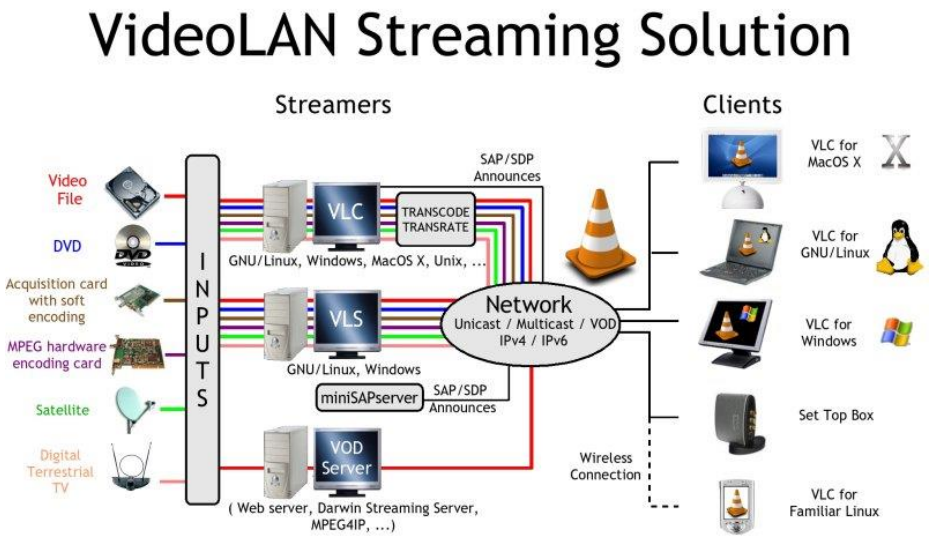

Figura 4: Solución de streaming de VideoLAN (16)

Este software se puede ejecutar como servidor (VLS), el cual puede transmitir archivos MPEG, DVD, canales digitales de satélite, de televisión, video en vivo sobre una red en unicast y multicast, o como cliente (VLC) usado para recibir, decodificar y visualizar los flujos MPEG en cualquier sistema operativo (16).
El por qué se eligió este software se debe a múltiples razones. VideoLAN es muy sencillo de manejar, puede ser controlado a través de la consola de UNIX, interfaz web o vía telnet, lo que hace que se pueda monitorear en cualquier momento. Es capaz de realizar el streaming de videos muy pesados utilizando flujo unicast y

multicast en IPv4, y lo más importante, en IPv6. Además permite realizar una plataforma de VoD (Video on Demand) o anuncio de canales via SAP (16), lo que lo hace una herramienta muy eficaz para trabajar con servidores IPTV e IMS (1) (17).

4.3 SISTEMA DE GESTIÓN UTILIZADO

Con la ayuda del protocolo SNMP se usó la herramienta web MRTG (Multi Routing Traffic Grapher) en el servidor, con la cual se generaron gráficas del tráfico de las interfaces de los routers de la red. Estas gráficas se generaron en HTML dando a conocer la evolución del tráfico a través del tiempo. Esta herramienta utiliza SNMP para obtener la información del router, y para ello este tiene que ser configurado como un agente de SNMP. MRTG funciona como un demonio y se ejecuta a través de una tarea programada usando la función cron, lo que permite que por defecto se actualicen los datos sacados del router cada 5 minutos. MRTG también genera gráficos de otro tipo de variables, tales como el uso del CPU y de la memoria en los routers.

Se escogió esta herramienta como la adecuada para generar las gráficas ya que es de fácil acceso y de fácil configuración. Utiliza SNMP, el cual es de fácil instalación en el servidor, y optimiza el rendimiento del computador, pues no necesita de mucho procesamiento, al ser una herramienta web.

5. IMPLEMENTACIÓN

Para describir el desarrollo de este proyecto se realiza este manual técnico, en el cual se mostrará paso por paso la configuración realizada en cada equipo. En primer lugar se realizó el montaje del servidor de streaming usando la herramienta de software libre VLC. En segundo lugar se configuró los routers con protocolos de enrutamiento en IPv4 e IPv6, mostrando en los anexos los archivos de configuración pertinentes a los routers, en el escenario de red propuesto. Acto seguido se implementó el servidor de gestión y administración de la red usando la herramienta MRTG. Por último se describe la configuración del servidor UCT IPTV, para probar la compatibilidad con NGN. Es por ello que el fin de este manual es servir como guía para aprender cómo se realizó este proyecto.

5.1 CONFIGURACIÓN DE LA INTERFAZ DE RED ETH0

Para configurar la interfaz de red del servidor se requirió el uso de los siguientes comandos:

- *sudo gedit /etc/network/interfaces:* con este comando editamos el archivo de red que indica al servidor la configuración de red:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 172.18.10.133
netmask 255.255.255.0
network 172.18.10.0
broadcast 172.18.10.255
gateway 172.18.10.129
iface eth0 inet6 static
address FC00:A::1
netmask 64
network FC00:A::
gateway FC00:A::2
dns-nameservers 172.16.1.3
```

- A continuación fue necesario reiniciar el servicio de networking usando el comando: *sudo /etc/init.d/networking restart.*

5.2 CONFIGURACIÓN SERVIDOR DE VIDEO STREAMING

Pasos a seguir para IPv4:

- Instalar VLC y sus plugins con los comandos: *sudo apt-get install vlc mozilla-plugin-vlc videolan-doc* (16)

- Poseer un archivo de video específico.

- Realizar un archivo de configuración, con el cuál se establecerá la configuración del servidor de streaming. En el anexo 1 se podrá observar este archivo con la explicación pertinente.

- Ejecutar VLC como un servidor de streaming, a través del siguiente comando:

  vlc --ttl 12 -vvv -I telnet --telnet-password videolan --rtsp-host 172.18.10.133 --rtsp-port 8000 –vlm-conf=/home/vlm.conf (16)

Dónde:

--ttl: es el valor del tiempo de vida de los paquetes IP.
--vvv: es el comando para acceder a VLC como servidor de streaming
-I: es la interfaz por la cual se accede a VLC, puede ser: telnet, web o consola
--telnet-password: es una contraseña que se le asigna al acceso via telnet
--rtsp-host: especifica la dirección IP del servidor de streaming
--rtsp-port: especifica el puerto usado por el servidor
-vlm-conf: especifica la ruta donde se encuentra guardado el archivo de configuración (16)

- Acceder a VLC en un host a través de Medio/Abrir volcado de red. Ingresar en la URL la dirección del servidor, el puerto y el nombre del canal donde se tiene el video. En la siguiente figura se muestra la URL para acceder al flujo unicast:

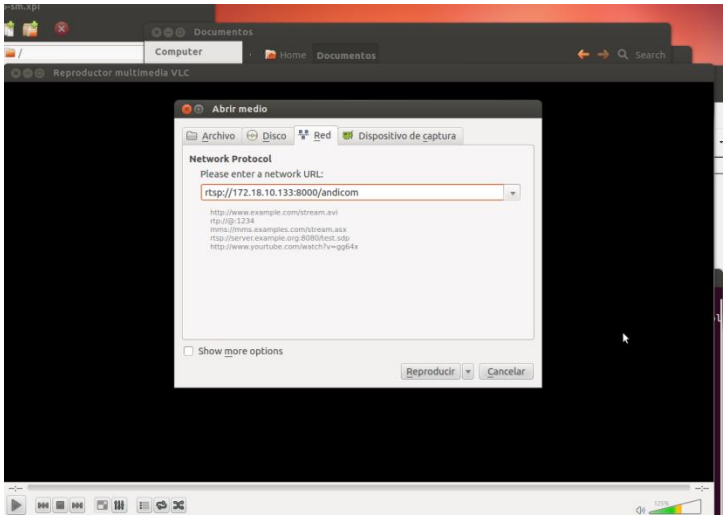

Figura 5 : Acceso del cliente al flujo unicast. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

- Para acceder a los canales multicast se dirige a Ver/Lista de reproducción/Red Local/Emisiones de red (SAP) (18), donde se podrán encontrar los tres canales multicast creados en el archivo de configuración. En la siguiente figura se muestran los canales en el VLC:

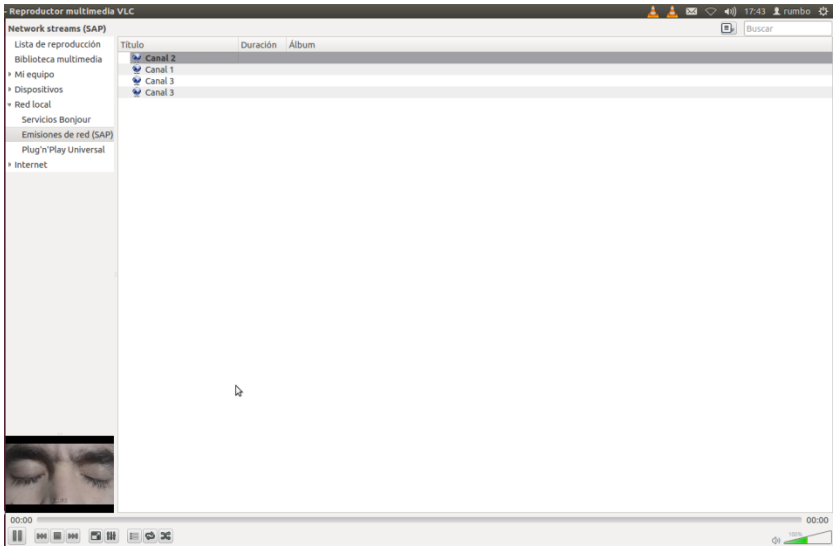

Figura 6: Canales multicast en el cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Pasos a seguir para IPv6:

VLC no soporta el protocolo RTSP para IPv6, por lo tanto usa RTP para los streamings en unicast y multicast. En el caso de IPv6 es más eficiente realizar el streaming a traves de la interfaz gráfica de VideoLAN. Para ello se siguen los siguientes pasos:

- En VLC ir a Medio>Emitir, a continuación aparece la siguiente pantalla, donde se añade el video a emitir:

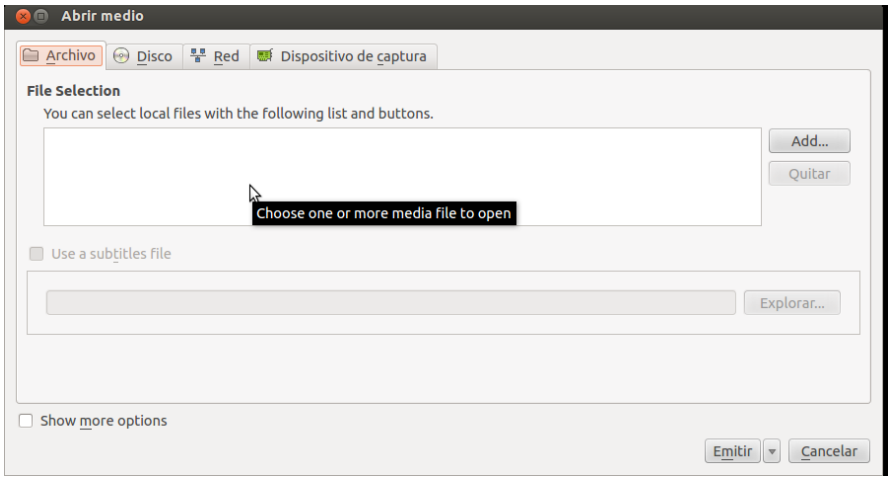

Figura 7: Pantalla interfaz de configuración de emisión en VLC. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

- Una vez agregada la entrada, es hora de agregar la salida, en donde se agregó el protocolo RTP como protocolo de salida de la transmisión, la dirección IP a la cual transmitió el flujo unicast. Es necesario emitir un flujo distinto para cada una de los clientes a los que se quiere transmitir. En VLC las direcciones IPv6 se escribren entre corchetes. Ej: [fc00:b::2]. El puerto por defecto de RTP es el 5004 y no hay necesidad de cambiarlo. La transcodificacion del video será MPEG-2 aunque tampoco es necesario transcodificarlo. En la siguiente figura se muestra este procedimiento:
-

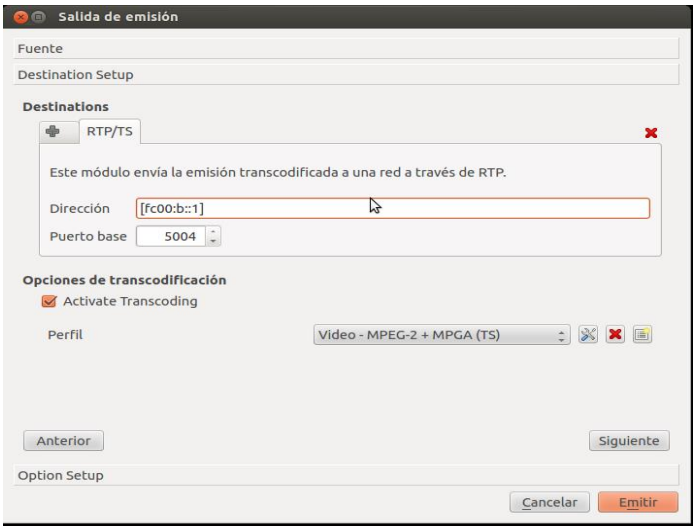

Figura 8: Configuración protocolo de emisión VLC. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

- Dar en siguiente y a continuación cambiar el TTL de la transmisión. Puede ser cualquiera, sin embargo tiene que ser mayor a 1:

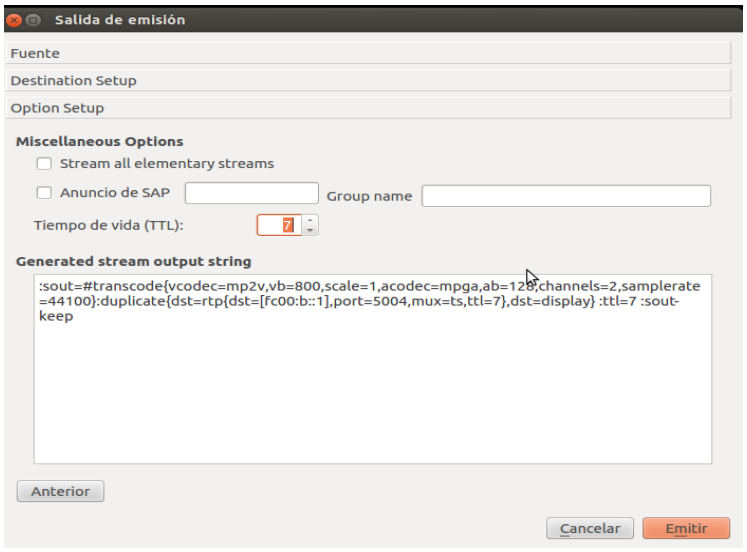

Figura 9: Opciones secundarias de emisión en VLC. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

- Ya se tiene configurada la transmisión. Para acceder como cliente se usa la opción Abrir volcado de red y se añade la ruta "*rtp://[fc00:b::1]*", como se muestra en la figura:

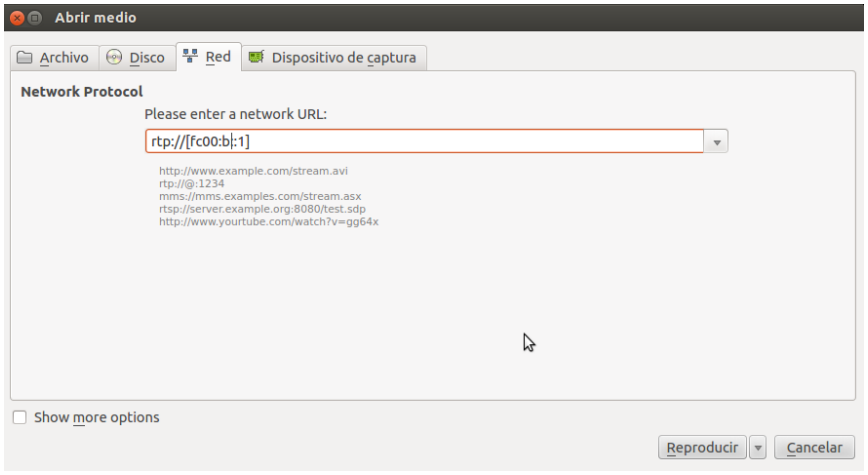

Figura 10:Acceso al servidor del cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

- Para transmitir en multicast IPv6 se realizó en VLC los pasos anteriormente mencionados. Sin embargo, en multicast no es necesario realizar una emisión diferente para transmitir a cada host. Basta simplemente con realizar una emisión RTP usando una dirección multicast en IPv6, la cual es del tipo [FF0X::] (2).

5.3 CONFIGURACIÓN DE ENRUTAMIENTO

Para la configuración del enrutamiento fue necesario tener en cuenta el diseño lógico de la red pues este muestra el direccionamiento usado, el cual se tiene que configurar en los routers :

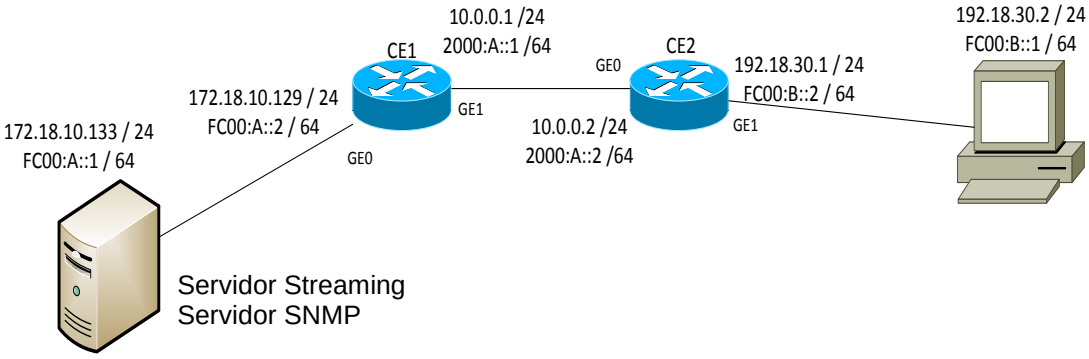

Figura 11: Arquitectura de red para realizar pruebas. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Los pasos seguidos para configurar todos los protocolos de enrutamiento fueron:

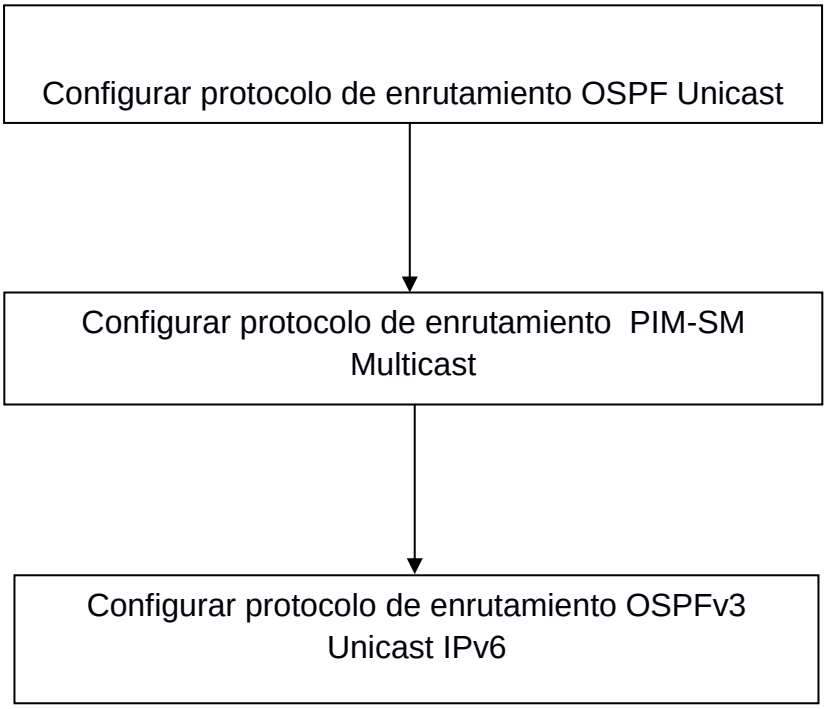

Figura 12: Pasos a seguir para configuración de enrutamiento del proyecto. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

5.3.1 Configuración OSPF

- Entrar en modo habilitado usando el comando *system-view* (11)
- Configurar las interfaces de red y la interfaz de loopback para el router CE1 (11)

```
[CE1] interface LoopBack0
[CE1] ip address 3.3.3.3 255.255.255.255
[CE1] interface GigabitEthernet0/0/0
[CE1] ip address 172.18.10.129 255.255.255.0
[CE1] interface GigabitEthernet0/0/1
[CE1] ip address 10.0.0.1 255.255.255.0
```

- Configurar las interfaces de red y la interfaz de loopback para el router CE2 (11)

```
[CE2] interface GigabitEthernet0/0/0
[CE2] ip address 10.0.0.2 255.255.255.0
[CE2] interface GigabitEthernet0/0/1
```

```
[CE2] ip address 192.18.30.1 255.255.255.0
[CE2] interface LoopBack0
[CE2] ip address 6.6.6.6 255.255.255.255
```

- Configurar ID del router y OSPF para CE1 (11)

```
[CE1] router id 3.3.3.3
[CE1] ospf
[CE1] area 1
[CE1] network 3.3.3.3 0.0.0.0
[CE1] network 10.0.0.0 0.0.0.255
[CE1] network 172.18.10.0 0.0.0.255
```

- Configurar ID del router y OSPF para CE2 (11)

```
[CE2] router id 6.6.6.6
[CE2] ospf
[CE2] area 1
[CE2] network 6.6.6.60.0.0.0
[CE2] network 10.0.0.0 0.0.0.255
[CE2] network 198.18.30.0 0.0.0.255
```

- Inmediatamente deberían actualizarse los *neighbors* o vecinos del router. Las tablas de enrutamiento se pueden observar con el comando *display ip routing-table.* En los anexos 2, 3, se muestran las tablas de enrutamiento de CE1 y CE2 respectivamente.

5.3.2 Configuración PIM-SM

- En modo habilitado, configurar el router para aceptar tráfico multicast con el comando:

multicast routing-enable (11)

- En cada interfaz configurar el protocolo pim-sm. Se repite este paso para el router CE2 (11)

```
[CE1] interface LoopBack0
[CE1] pim-sm
[CE1] interface GigabitEthernet0/0/0
[CE1] pim-sm
[CE1] interface GigabitEthernet0/0/1
[CE1] pim-sm
```

- Establecer el punto de encuentro (*Rendevousz Point)* en uno de los routers, en este caso escogí este punto en el router CE2 en la interfaz GigabitEthernet0/0/0. (11)

  ```
  [CE2] c-bsr GigabitEthernet0/0/0
  [CE2] c-rp GigabitEthernet0/0/0
  ```

- Se configura el protocolo IGMP (Internet Group Management Protocol) (11) en la interfaz conectada al cliente con los siguientes comandos:

  ```
  [CE2] igmp enable
  [CE2] igmp version 3
  ```

- Para mirar la onfiguración del punto de acceso se usa el comando *display pim bsr-info.* En el anexo 4 se observa el resultado de este comando en el router CE2.

- En seguida, es necesario ejecutar el servidor de streaming para comenzar a enviar tráfico multicast, y así mirar las tablas de enrutamiento PIM. Para ello se usa el comando *display pim routing-table.* En el anexo 5 y 6 se observan estas tablas en los routers CE1 y CE2 respectivamente.

- Para la configuración de PIM en IPv6 se ejecutan los siguientes comandos en cada router:

  ```
  [CE2] multicast IPv6 routing-enable
  [CE2] interface GigabitEthernet 0/0/0
  [CE2] pim ipv6 sm
  [CE2] interface GigabitEthernet 0/0/1
  [CE2] pim ipv6 sm
  [CE2] interface Loopback 0
  [CE2] pim ipv6 sm
  ```

- De la misma manera que en PIM IPv4 se configura IGMP en IPv6 se configura MLD (Multicast Listener Discovery) (6) en el router conectado a los hosts:

  ```
  [CE2] mld enable
  [CE2] mld version 2
  ```

Para habilitar el uso del comando *multicast IPv6 routing-enable* es necesario actualizar el software del router. Para ello se pidió a Huawei que diera la versión de software que si permitiera el uso del comando.

5.3.3 Configuración OSPFv3

- Entrar en modo habilitado usando el comando *system-view*

- Configurar las interfaces de red y la interfaz de loopback para el router CE1 (11)

```
[CE1] interface LoopBack0
[CE1] ipv6 enable
[CE1] ipv6 address 3333::3/128
[CE1] ospfv3 1 area 2
[CE1] interface GigabitEthernet0/0/0
[CE1] ipv6 enable
[CE1] ipv6 address FC00:A::2/64
[CE1] ospfv3 1 area 2
[CE1] interface GigabitEthernet0/0/1
[CE1] ipv6 enable
[CE1] ipv6 address 2000:A::1/64
[CE1] ospfv3 1 area 2
```

- Configurar las interfaces de red y la interfaz de loopback para el router CE2 (11)

```
[CE2] interface GigabitEthernet0/0/0
[CE2] ipv6 enable
[CE2] ipv6 address 2000:A::2/64
[[CE2] interface GigabitEthernet0/0/1
[CE2] ipv6 enable
[CE2] ipv6 address FC00:B::2/64
[CE2] ospfv3 1 area 2
[CE2] interface LoopBack0
[CE2] ipv6 enable
[CE2] ipv6 address 6666::6/128
[CE2] ospfv3 1 area 2
```

- Inmediatamente deberían actualizarse los *neighbors* o vecinos del router. Las tablas de enrutamiento se pueden observar con el comando *display ospfv3 routing.* En los anexos 7 y 8, se muestran las tablas de CE1 y CE2 respectivamente.

5.3.4 Configuración de los routers como agentes SNMP

- Para habilitar el uso de SNMP en los routers se usa el comando: *snmp-agent* (15)
- Luego se añade la comunidad, el cual es un grupo que se asigna para que el servidor pueda comunicarse mejor con los routers, usando el comando: *snmp-agent community write routers.* (15)

Luego de terminar toda esta configuración se tienen los routers listos para el trabajo que se quiere hacer. En el anexo 9 y 10 se pueden ver los archivos de configuración de los routers CE1 y CE2 respectivamente.

5.4 CONFIGURACIÓN SERVIDOR SNMP

Servidor SNMP – MRTG

- Instalar el servicio snmp usando el comando *sudo apt-get install snmp snmpd*
- Instalar mrgt con el comando *sudo apt-get install mrtg*
- Crear una carpeta */etc/mrtg* y añadir en esa carpeta el archivo de configuración */etc/mrtg.cfg* creado por la instalación, através de los comandos *sudo mkdir /etc/mrtg && sudo mv /etc/mrtg.cfg /etc/mrtg*
- Modificar el archivo de configuración para que acceda a los routers, através del comando:

  sudo cfgmaker --output /etc/mrtg/mrtg.cfg public@the-first-router's-IP-address public@the-second-router's-IP-address

En este comando se cambia el *public* por el nombre de la comunidad que se configuró en los routers y se agrega la IP de alguna interfaz del router.

- Luego de ejecutar este paso se crea el archivo de configuración *mrtg.cfg*, el cual se va a modificar añadiendo las siguientes características:

  WorkDir: /var/www/mrtg: se añade la carpeta donde se guardarán los archivos .log y .png, es decir las gráficas que saca el programa

Interval: 5: es el intervalo de tiempo en el cual el programa toma una muestra, el cual no puede ser inferior a 5 minutos.

RunAsDaemon: Yes: con esta opción le decimos a MRTG que corra como un demonio, es decir que se inicie al iniciar el sistema operativo.

EnableIPv6: yes: se habilita el uso de IPv6 en MRTG

- En seguida se usa los siguientes comandos:

sudo indexmaker --output=/var/www/mrtg/index.html /etc/mrtg/mrtg.cfgsudo env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg

Con estos comandos MRTG que indexa el archivo de configuración en una página web con el fin de observar los gráficos en la web. En la figura se observa el resultado de la página a la cual se accesa ingresando en el browser la dirección *localhost/mrtg:*

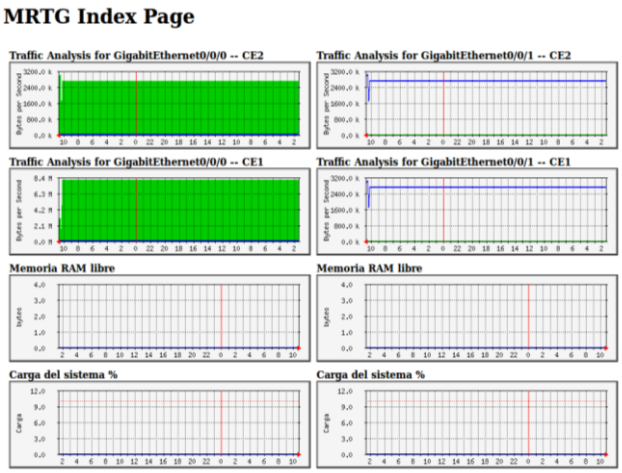

Figura 13: Página de inicio de MRTG. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Al hacer click en alguna imagen MRTG muestra graficadas las muestras que toma cada 5 minutos, y las reparte en gráficas diarias, semanales, mensuales y anuales, como lo muestra la figura:

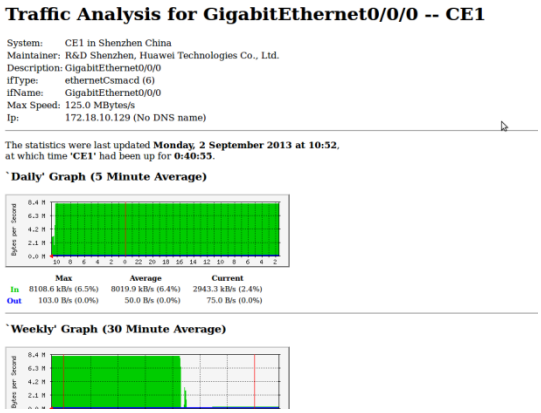

Figura 14: Página con gráficas detalladas de la interfaz GE0 del router CE1. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

5.5 IMPLEMENTACIÓN Y CONFIGURACIÓN DEL SERVIDOR UCT IPTV

Este servidor se implementó con el fin de probar la compatibilidad del servidor de streaming con IPTV y con NGN

- Descargar el software y paquetes correspondientes al servidor UCT IPTV Advanced de la página web del fabricante. El servidor solo funciona para el sistema operativo LINUX.

- Crear y configurar un archivo XML el cual servirá para añadir los canales que se pueden ver por IPTV y sus respectivos streams. En el anexo 11 se muestra este archivo.

- Ejecutar el servidor de IPTV a través del siguiente comando:

  Uctiptv_as ruta_del archivo_XML

- Configurar el streaming de video tal como se explicó en la sección 4.1

- Poseer un servidor IMS CORE, previamente configurado para aceptar el uso del servicio IPTV, esto con el fin de autenticar un usuario que necesite el servicio

- Descargar el cliente UCT IMS CLIENT con el fin de realizar las pruebas.

6. REALIZACIÓN DE PRUEBAS

En esta sección se hará la descripción de las pruebas ejecutadas una vez realizada la configuración del servidor de streaming y de la red planteada. Se describirá cuales pruebas se tomaron y como se hizo el ambiente de pruebas.

6.1 DESCRIPCIÓN DEL AMBIENTE DE PRUEBAS

Para realizar el ambiente de pruebas fue necesario tener en cuenta los equipos en los que se tomaron las pruebas y los tres factores a los que se le tomaron las medidas. Los equipos en los que se realizaron las medidas fueron los dos routers y el servidor, mientras que las variables fueron: uso de las interfaces de los equipos, uso de CPU y uso de memoria. Para realizar estas medidas se tuvieron en cuenta los siguientes aspectos:

- Con la herramienta MRTG se obtuvieron los datos del uso de interfaz de las interfaces de GE0 y GE1 de los routers.
- Con el comando *display cpu-usage* se obtuvo el uso de CPU de los routers.
- Con el comando *display memory-usage* se obtuvo el uso de memoria en los routers.
- Con la herramienta *system monitor* de Ubuntu se obtuvo las medidas de uso de CPU, uso de interfaz y uso de memoria del servidor.

La frecuencia de adquisición de estos datos fue de 5 minutos, con el fin de ajustarse a la frecuencia de MRTG. Luego, los datos fueron introducidos en tablas de Excel. Estas pruebas se realizaron con el streaming de un video el cual posee las siguientes características:

- **Tamaño:** 17.4 GB
- **Formato:** MPG
- **Duración:** 1:45:09

A su vez los equipos poseen las siguientes características:

Equipo	Memoria RAM	Procesador	Sistema operativo	Velocidad interfaces
Servidor	512Mb	Intel atom	Ubuntu Server	400Mbps
Router CE1	2048Mb	AR01BAK2A	VRP software	75Mbps
Router CE2	2048Mb	AR01BAK2A	VRP software	75Mbps

Tabla 2: Especificaciones técnicas de los equipos usados en el proyecto. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

6.2 DESCRIPCIÓN DE LAS PRUEBAS

Para lograr un verdadero análisis del comportamiento de los routers y del servidor ante el streaming de un video de tanto tamaño y duración, fue necesario realizar las pruebas para un cliente que accede al servidor y para cinco clientes accediendo al mismo tiempo. En la siguiente tabla se muestra el tipo de pruebas que se realizaron:

Prueba	Un cliente	Cinco clientes
Unicast IPv4	X	X
Multicast IPv4	X	X
Unicast IPv6	X	X
Multicast IPv6	X	X

Tabla 3: Pruebas realizadas. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Luego de organizar las muestras en Excel, se realizaron las gráficas de los mismos obteniendo los siguientes resultados:

6.2.1 Unicast IPv4 un cliente

Uso de CPU

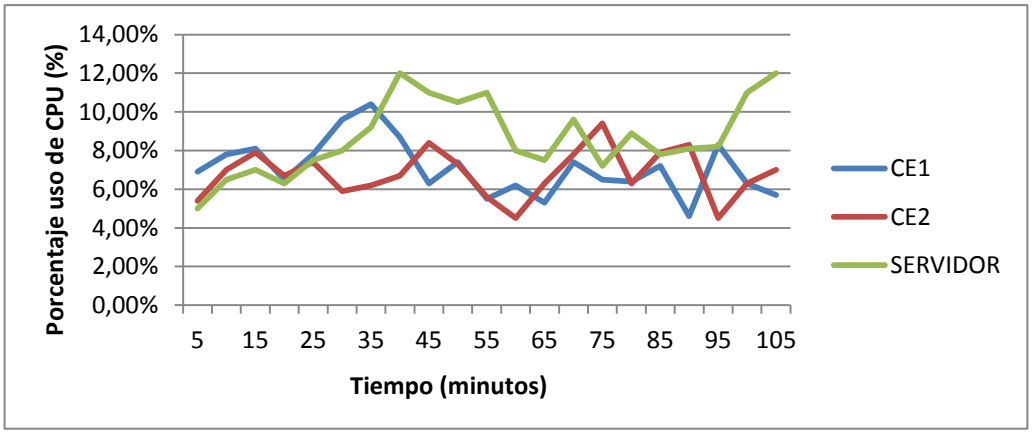

Figura 15: Gráfica con pruebas uso CPU unicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de memoria

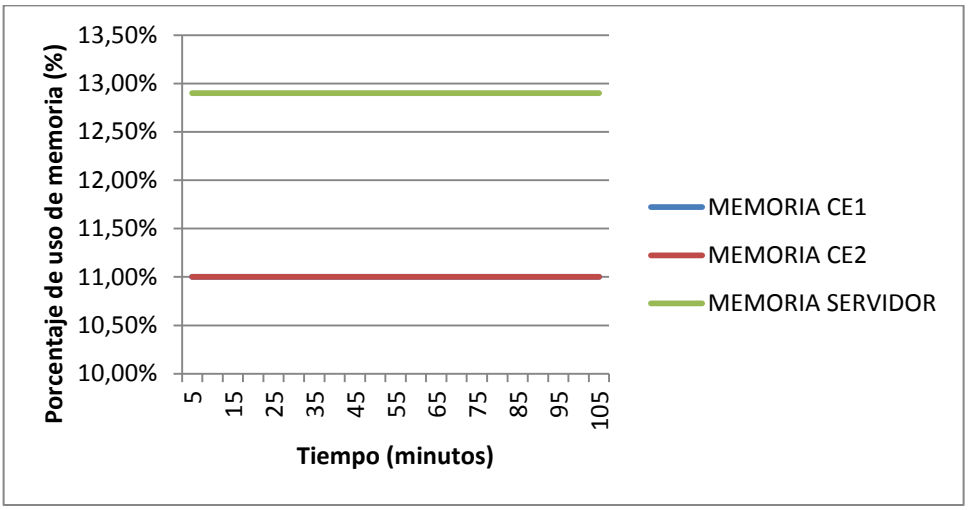

Figura 16: Gráfica con pruebas uso memoria unicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE1

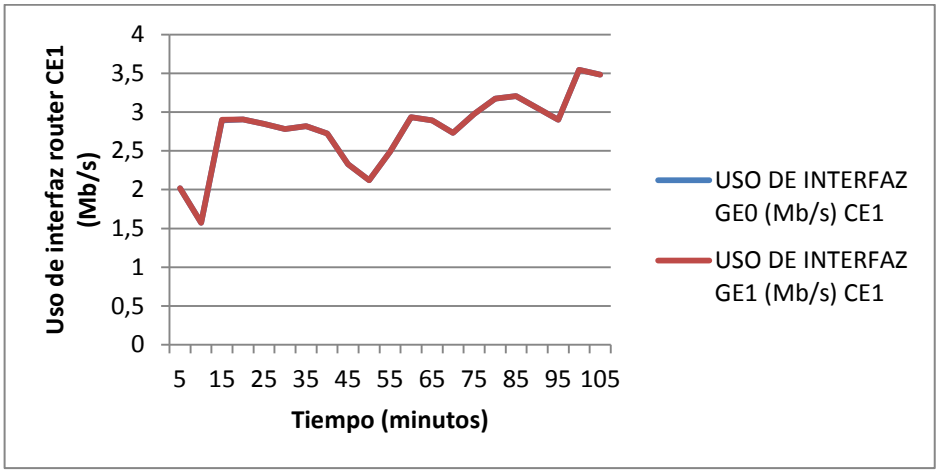

Figura 17: Gráfica con pruebas uso de interfaz router CE1 unicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE2

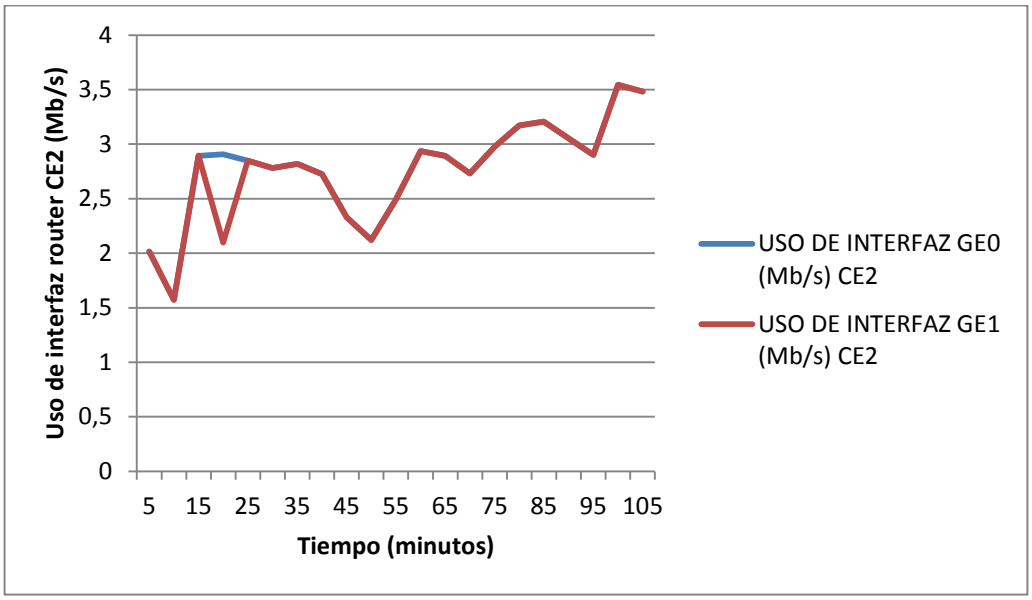

Figura 18: Gráfica con pruebas uso de interfaz router CE2 unicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz eth0

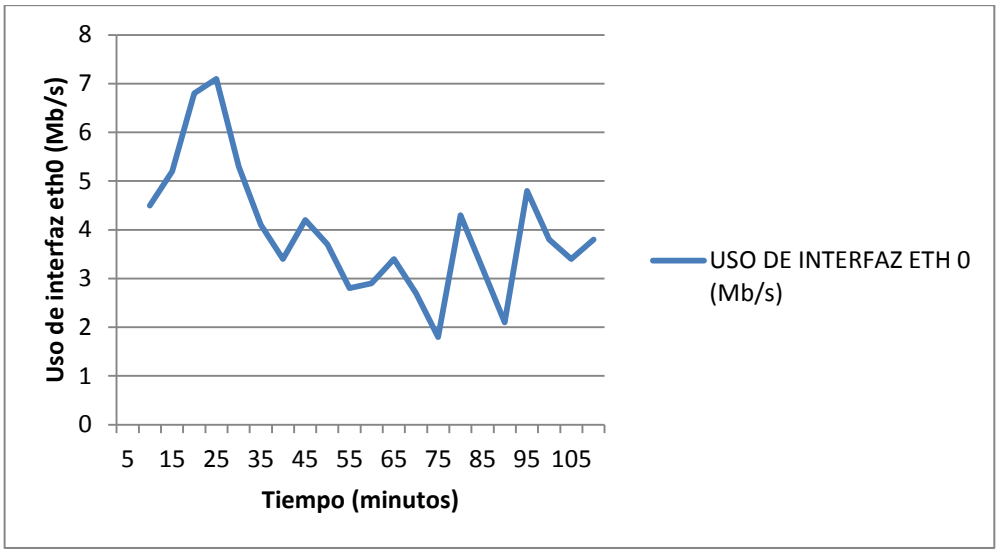

Figura 19: Gráfica con pruebas uso de interfaz eth0 unicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

6.2.2 Multicast IPv4 un cliente

Uso de CPU

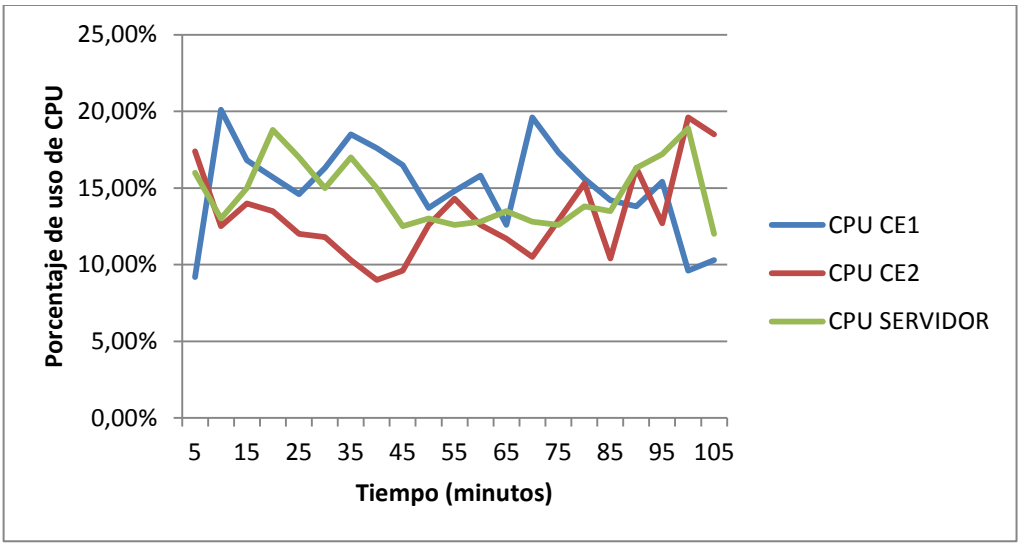

Figura 20: Gráfica con pruebas uso CPU multicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de memoria

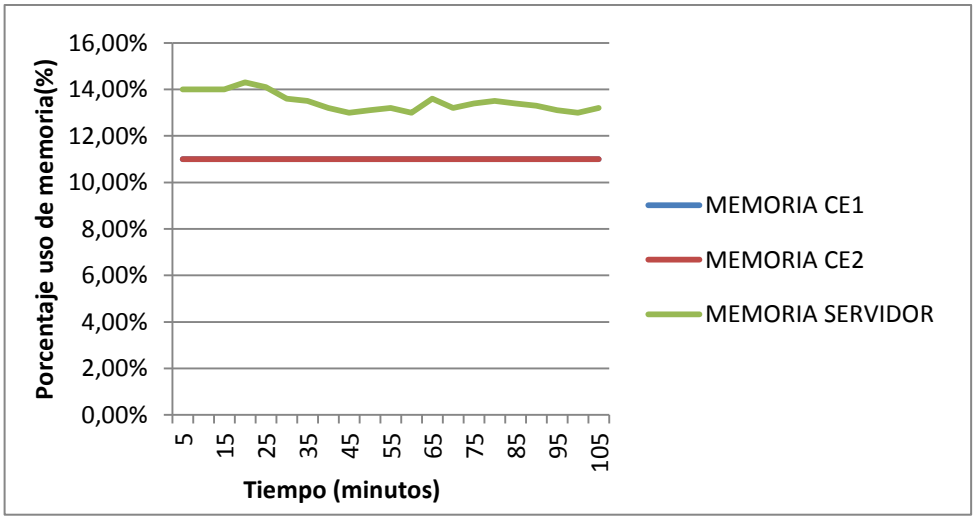

Figura 21: Gráfica con pruebas uso memoria multicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE1

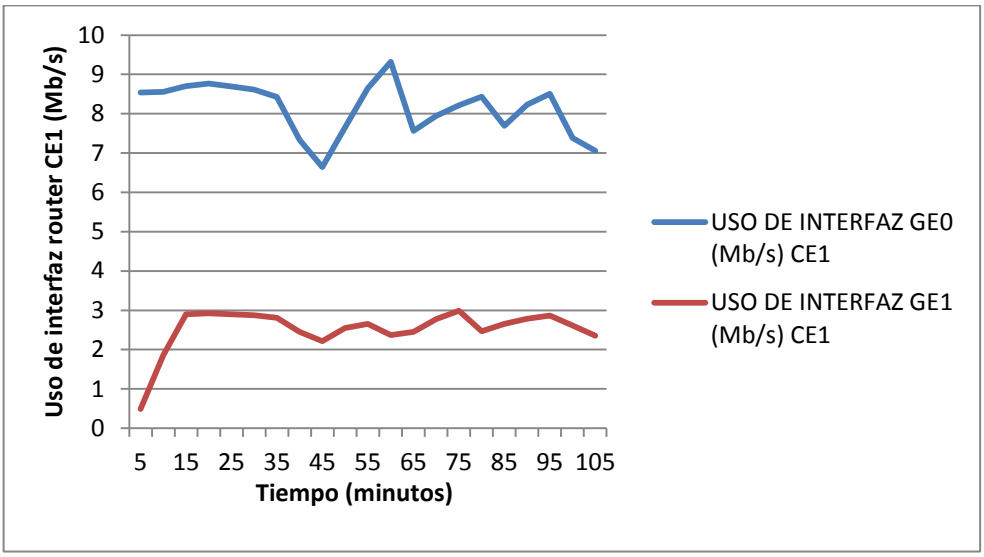

Figura 22: Gráfica con pruebas uso de interfaz router CE1 multicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE2

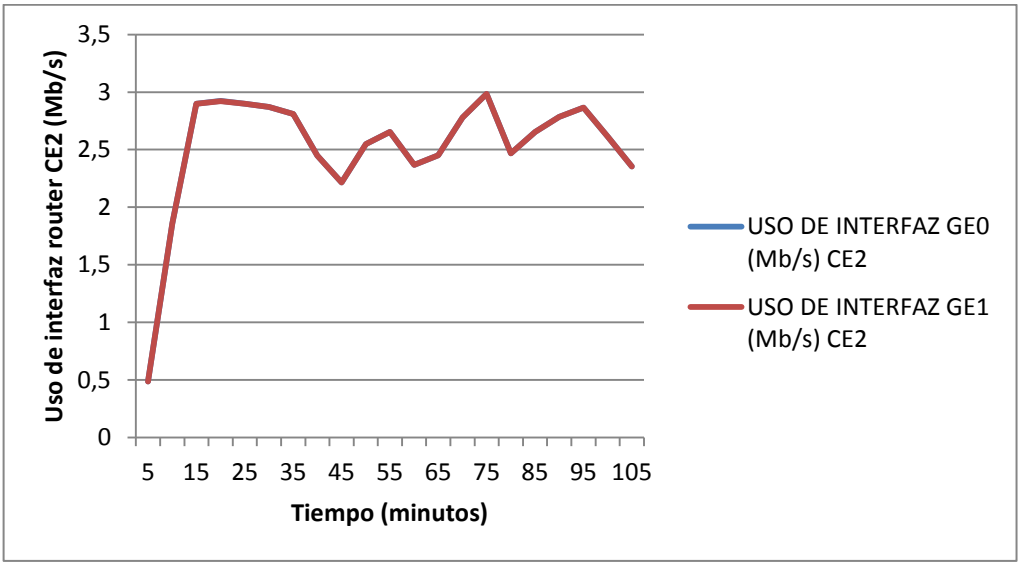

Figura 23: Gráfica con pruebas uso de interfaz router CE2 multicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz eth0

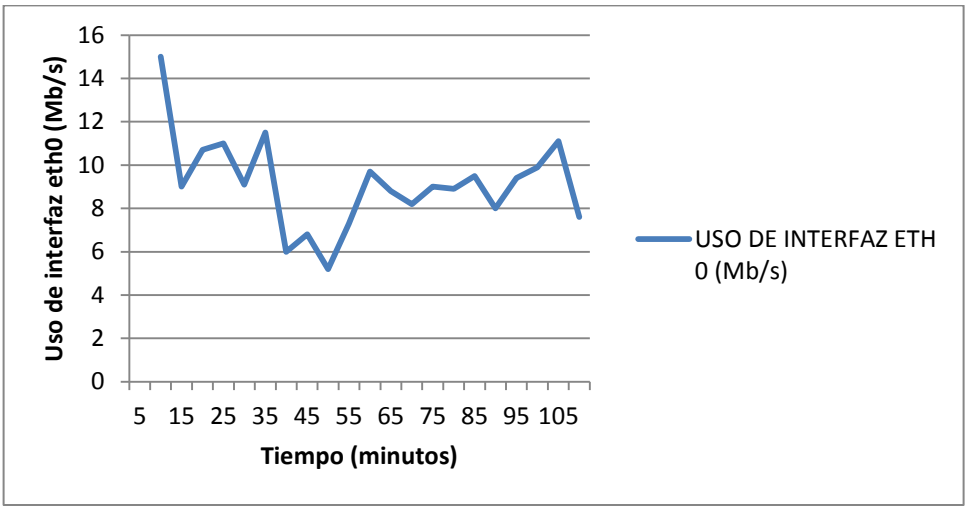

Figura 24: Gráfica con pruebas uso de interfaz eth0 multicast IPv4 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

6.2.3 Unicast IPv6 un cliente

Uso de CPU

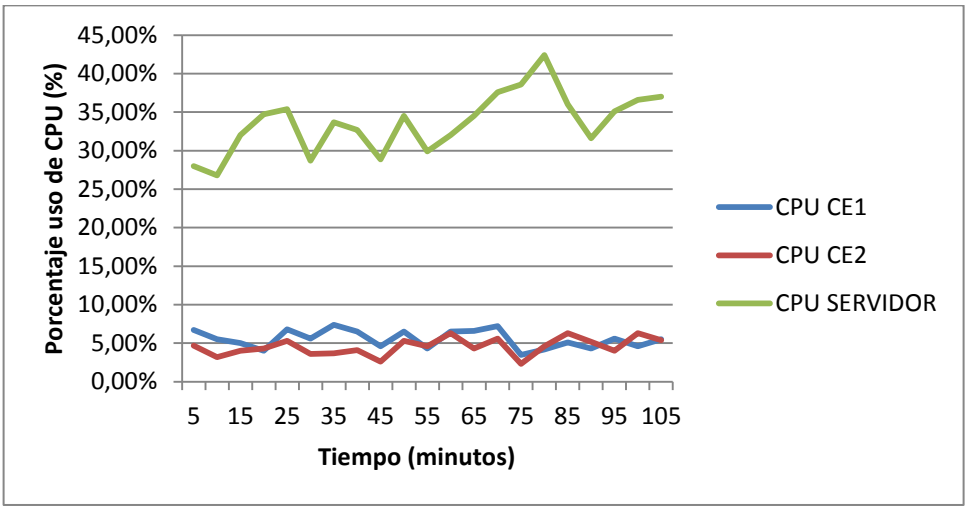

Figura 25: Gráfica con pruebas uso CPU unicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de memoria

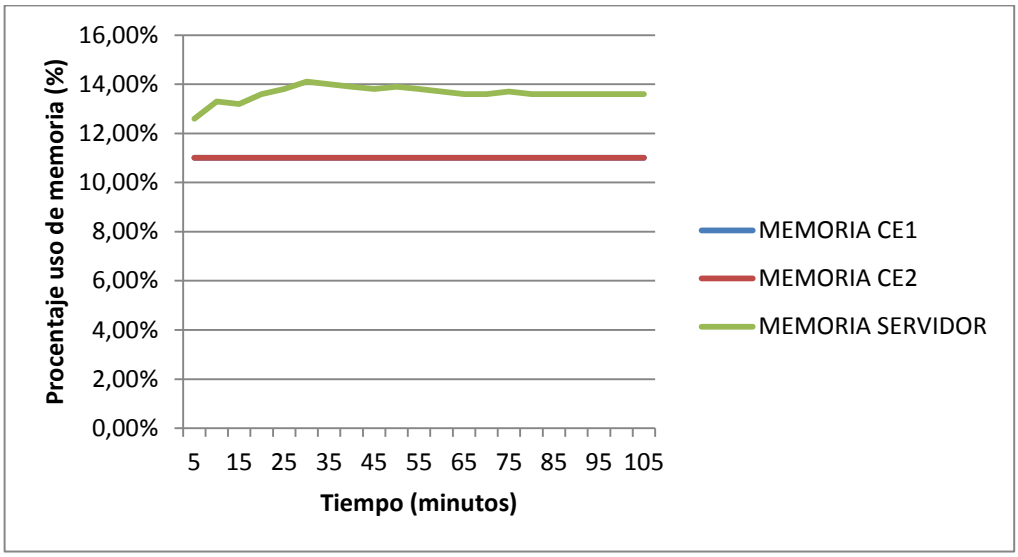

Figura 26: Gráfica con pruebas uso memoria unicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE1

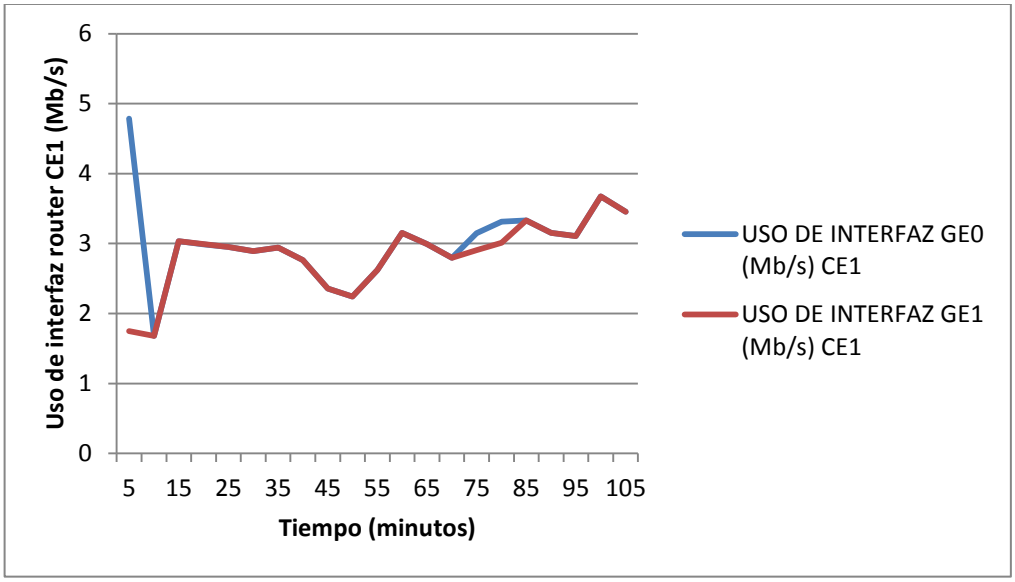

Figura 27: Gráfica con pruebas uso de interfaz router CE1 unicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE2

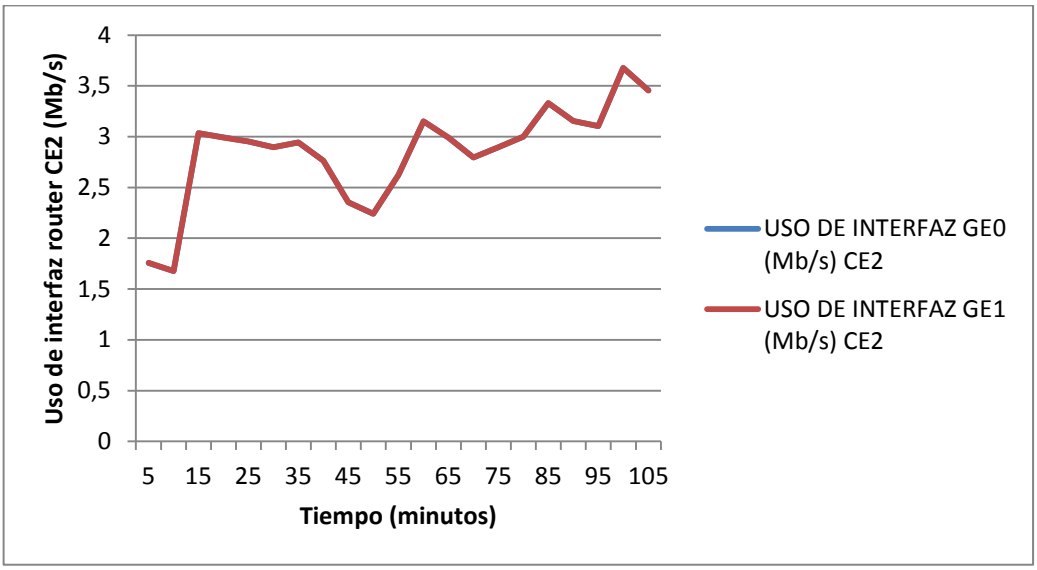

Figura 28: Gráfica con pruebas uso de interfaz router CE2 unicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz interfaz eth0

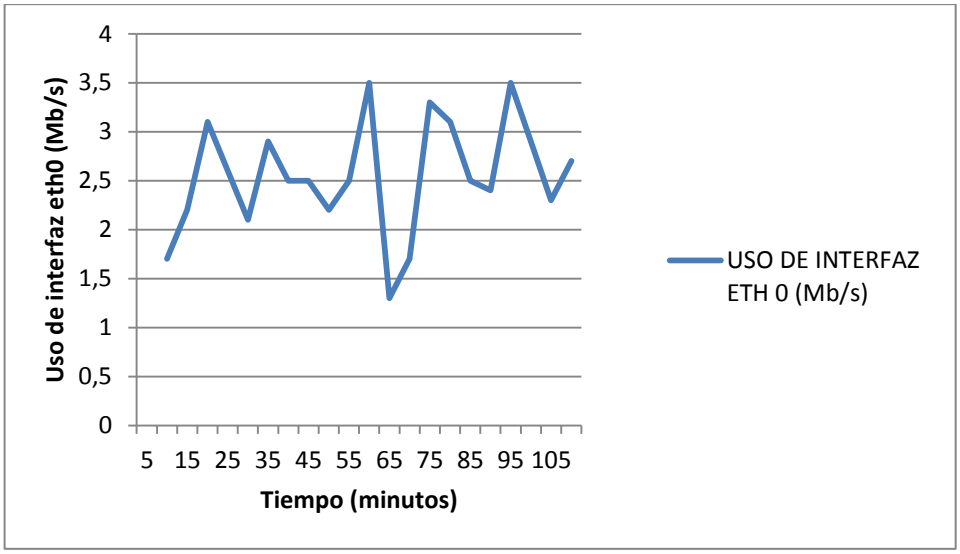

Figura 29: Gráfica con pruebas uso de interfaz eth0 unicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

6.2.4 Multicast IPv6 un cliente

Uso de CPU

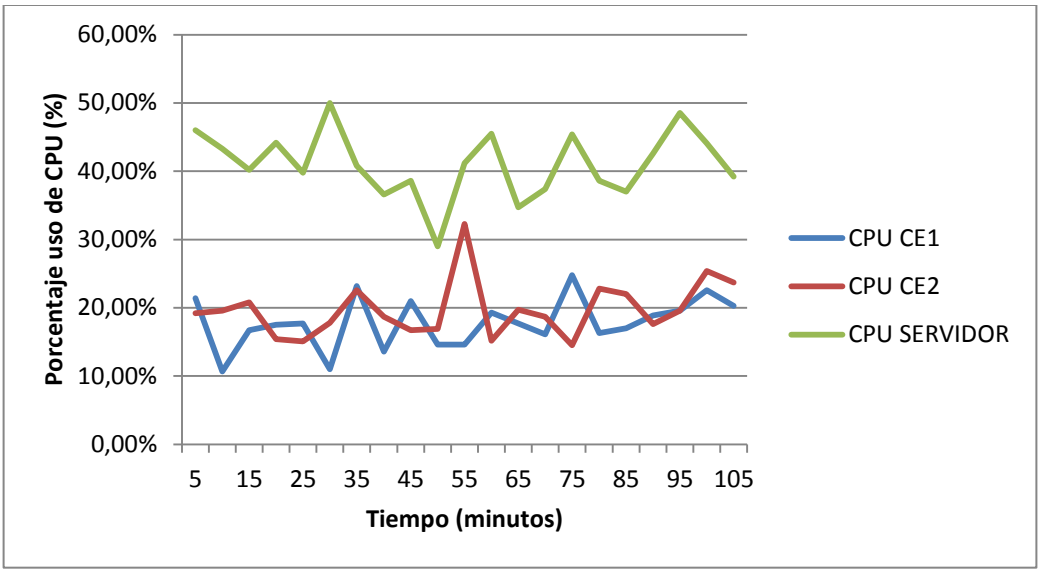

Figura 30: Gráfica con pruebas uso CPU multicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de memoria

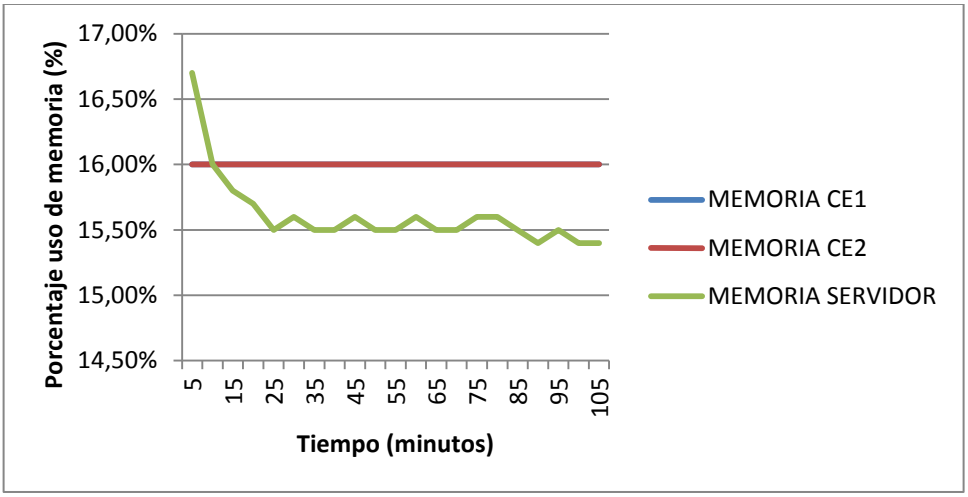

Figura 31: Gráfica con pruebas uso memoria multicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE1

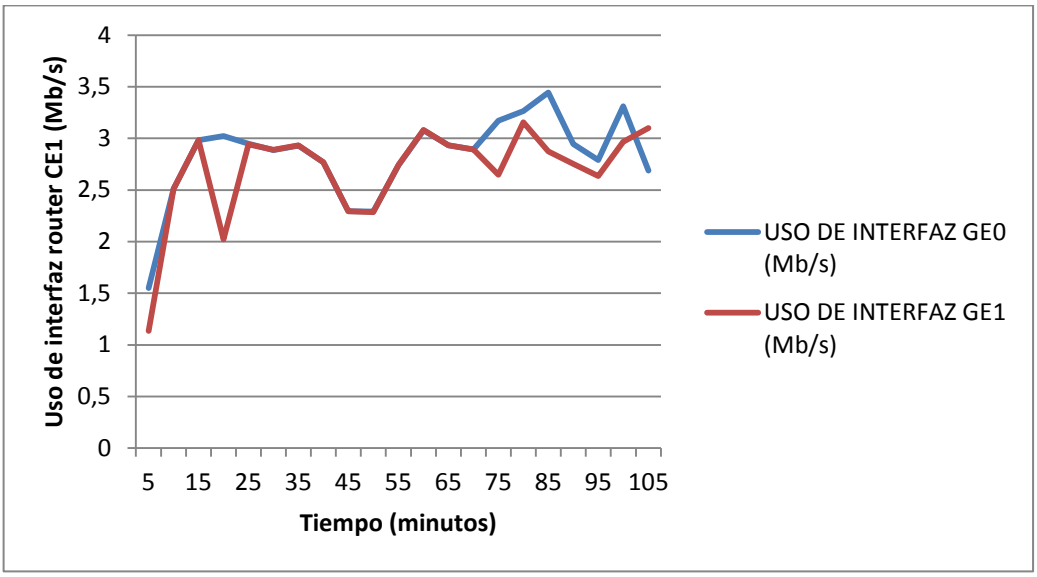

Figura 32: Gráfica con pruebas uso de interfaz router CE1 multicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE1

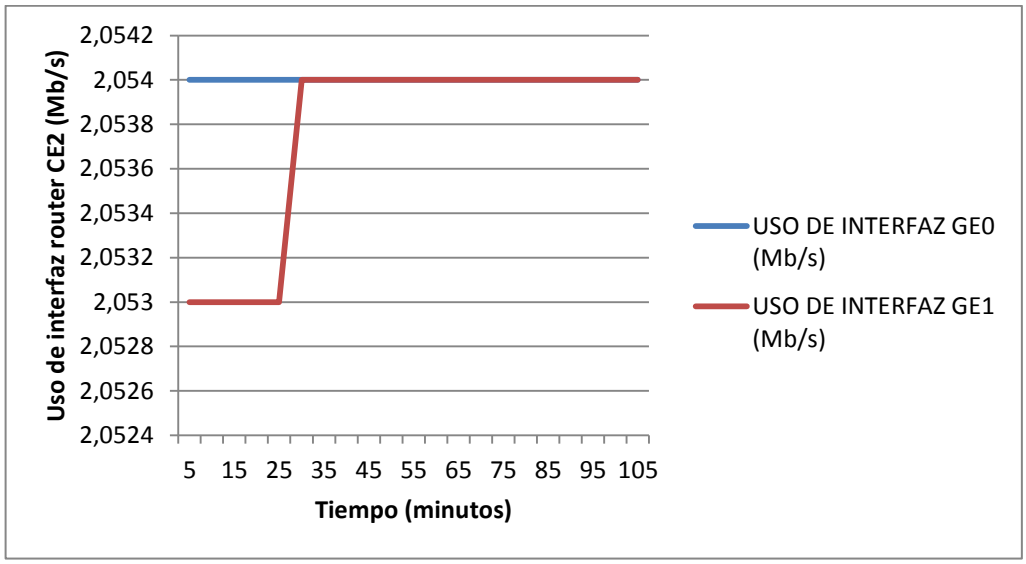

Figura 33: Gráfica con pruebas uso de interfaz router CE2 multicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz eth0

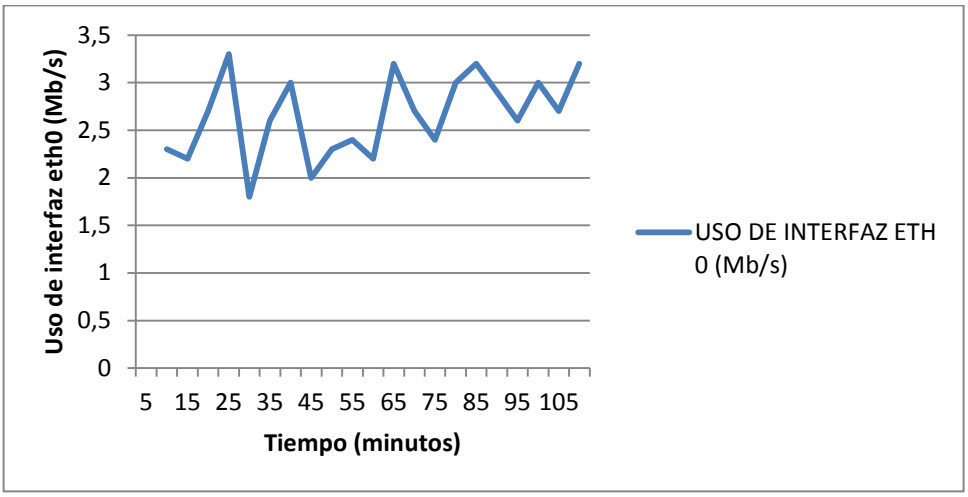

Figura 34: Gráfica con pruebas uso de interfaz eth0 multicast IPv6 un cliente. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

6.2.5 Unicast IPv4 cinco clientes

Uso de CPU

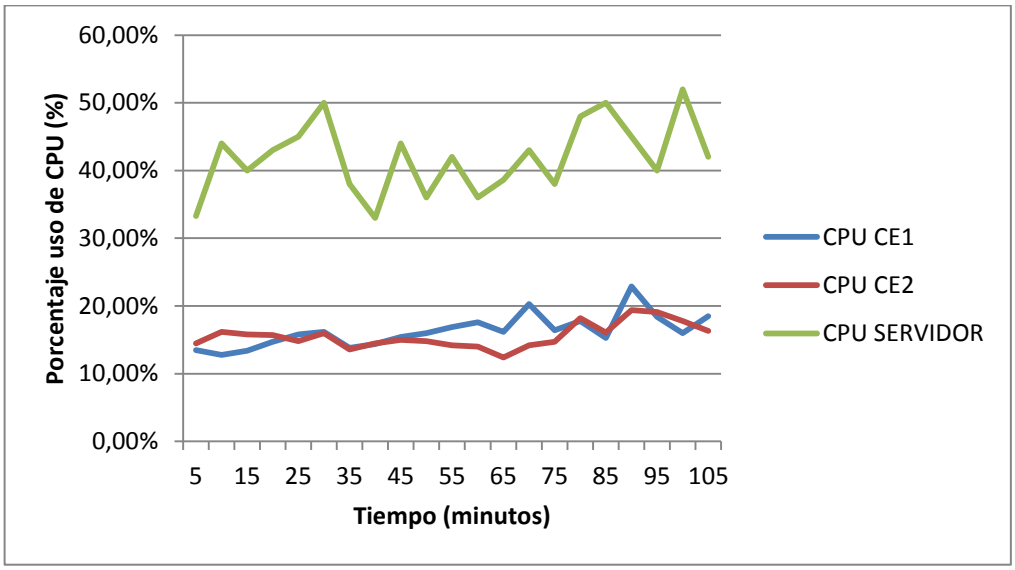

Figura 35: Gráfica con pruebas uso CPU unicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de memoria

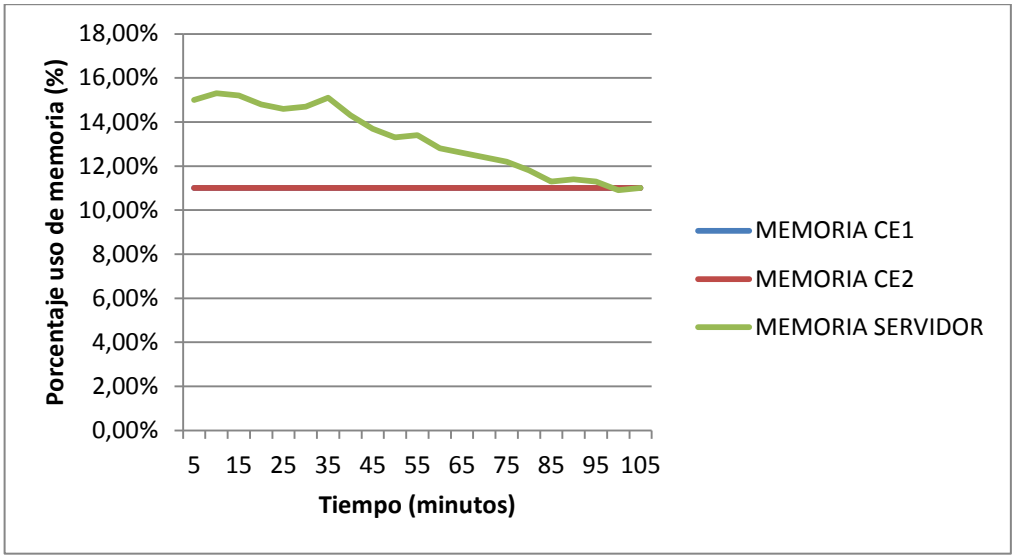

Figura 36: Gráfica con pruebas uso memoria unicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE1

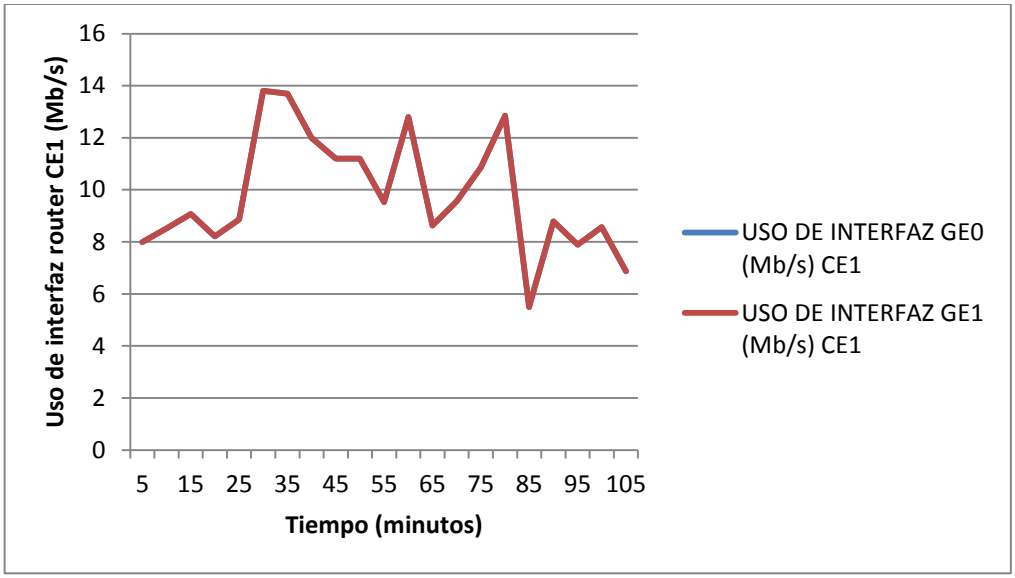

Figura 37: Gráfica con pruebas uso de interfaz router CE1 unicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Uso de interfaz router CE2

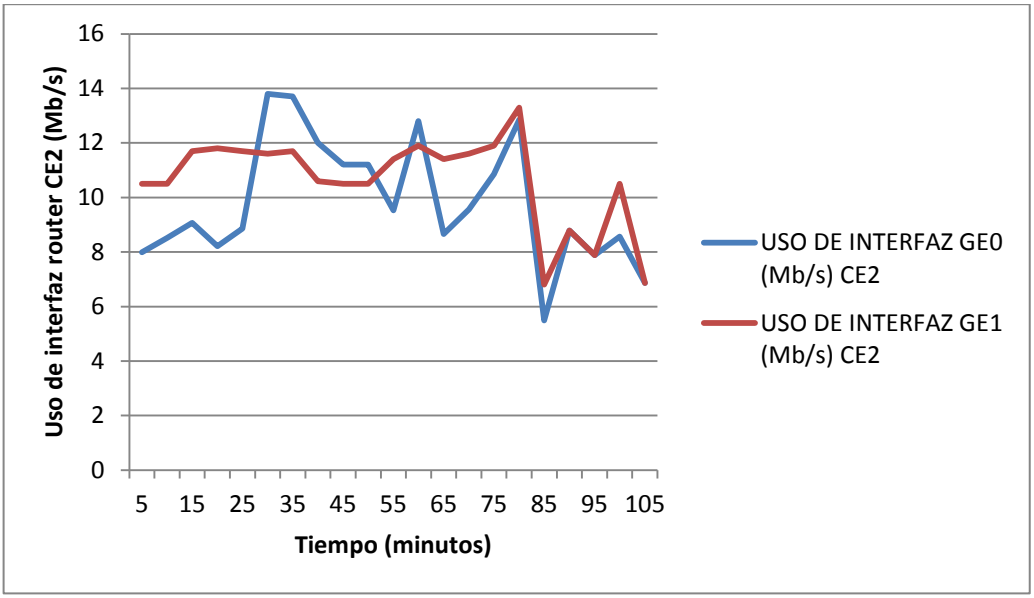

Figura 38: Gráfica con pruebas uso de interfaz router CE2 unicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz eth0

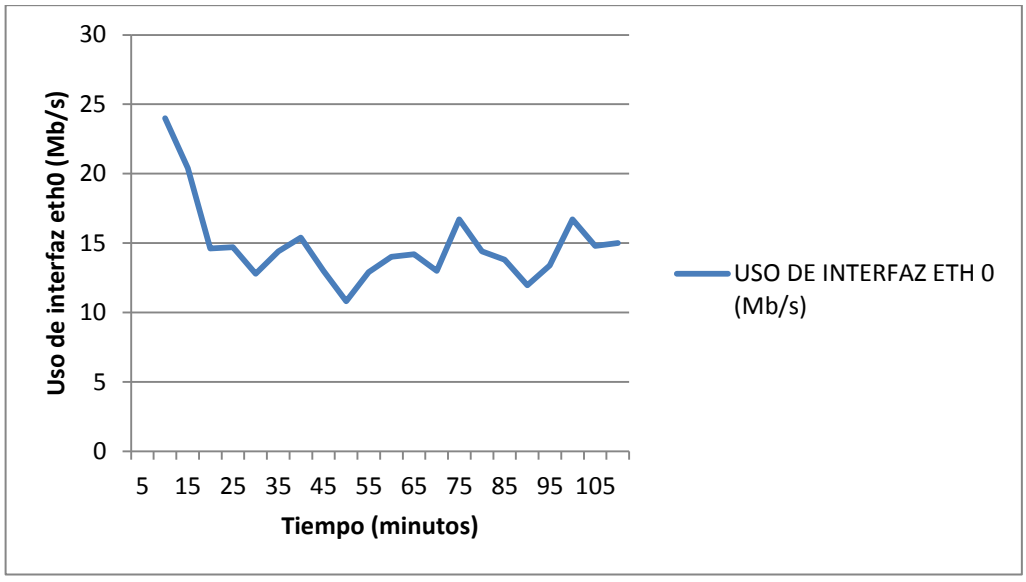

Figura 39: Gráfica con pruebas uso de interfaz eth0 unicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

6.2.6 Multicast IPv4 cinco clientes

Uso de CPU

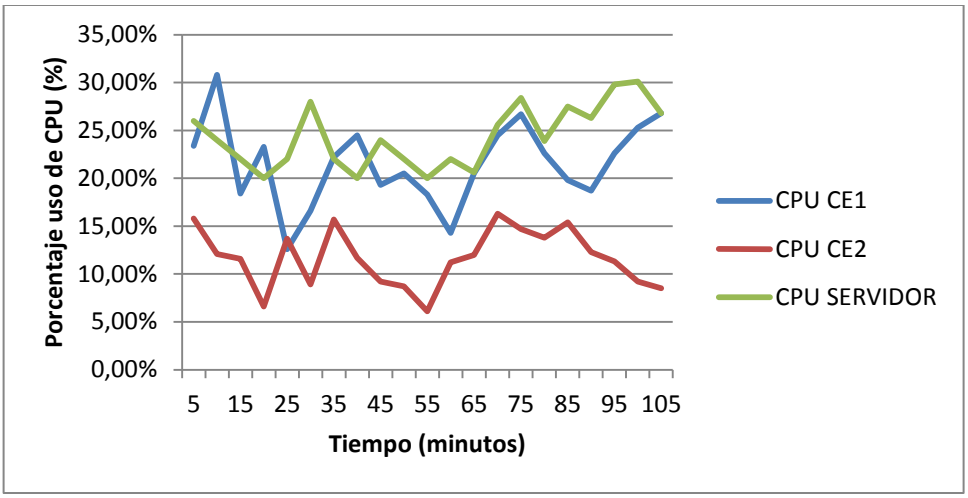

Figura 40: Gráfica con pruebas uso CPU multicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de memoria

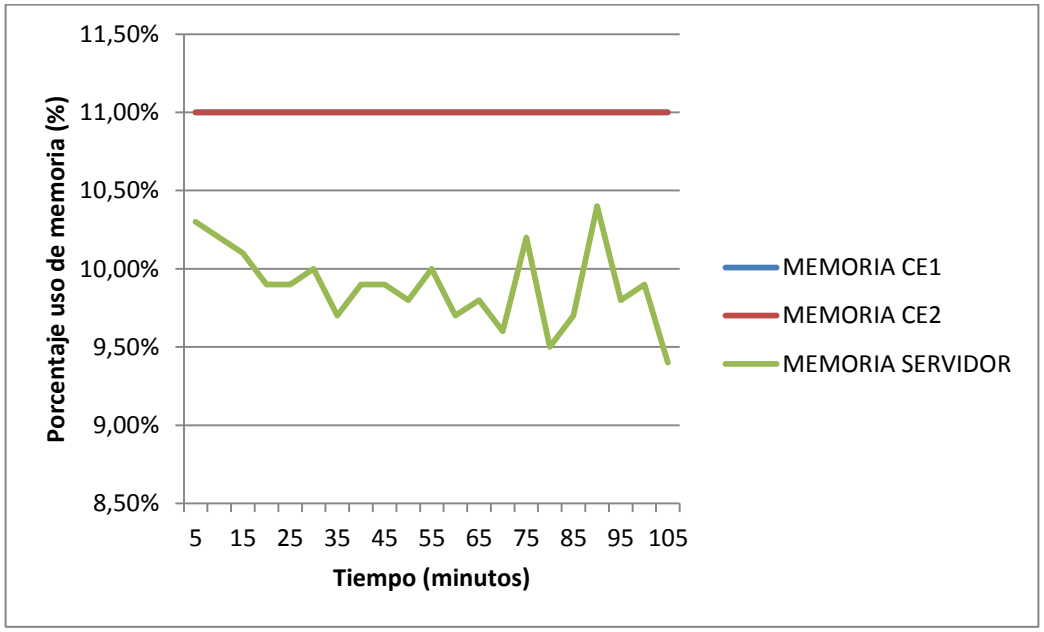

Figura 41: Gráfica con pruebas uso memoria multicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz router CE1

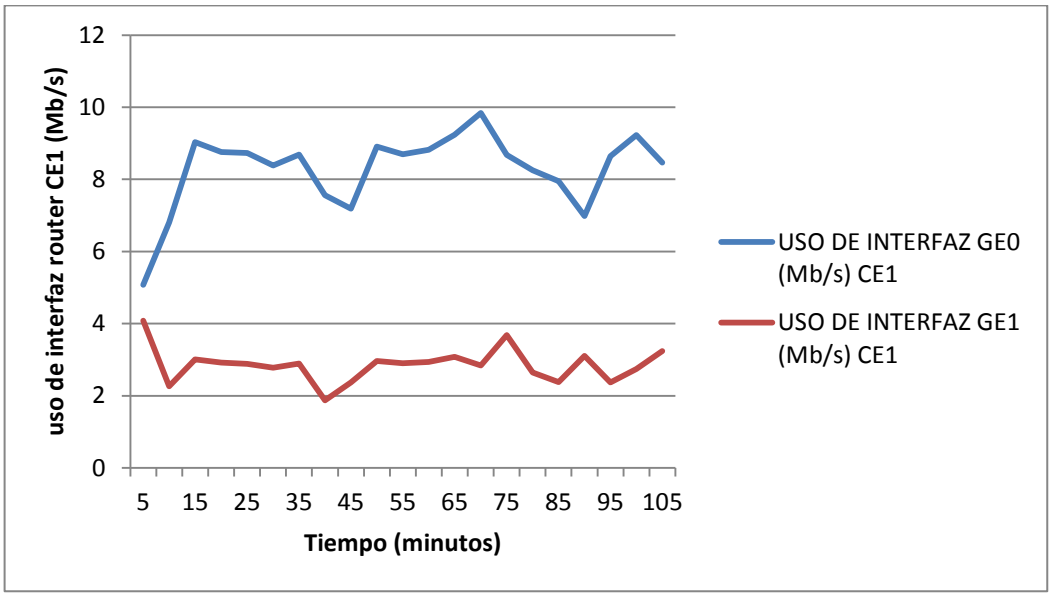

Figura 42: Gráfica con pruebas uso de interfaz router CE1 multicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz router CE2

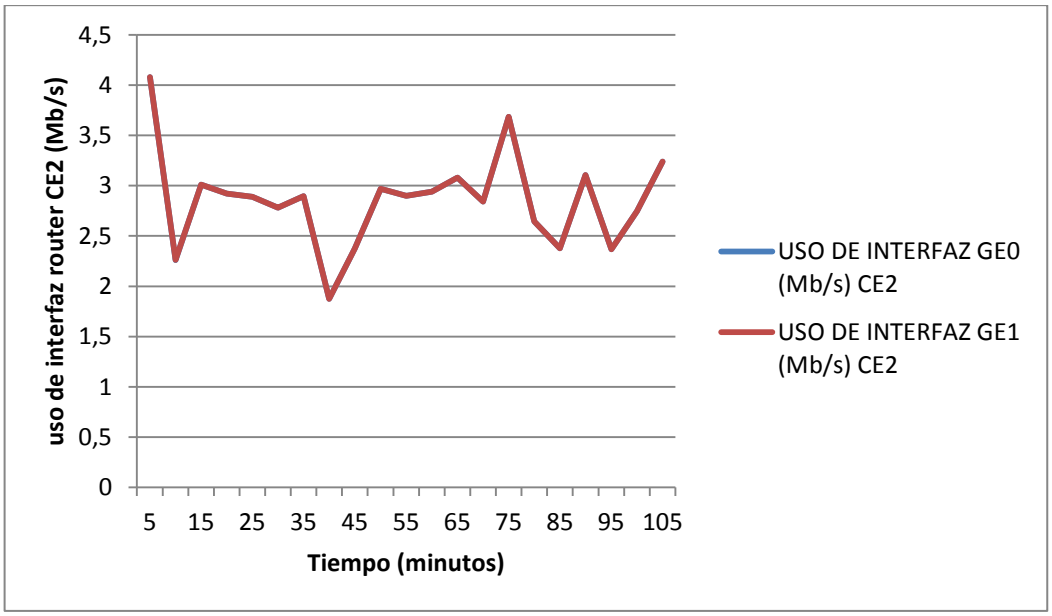

Figura 43: Gráfica con pruebas uso de interfaz router CE2 multicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz eth0

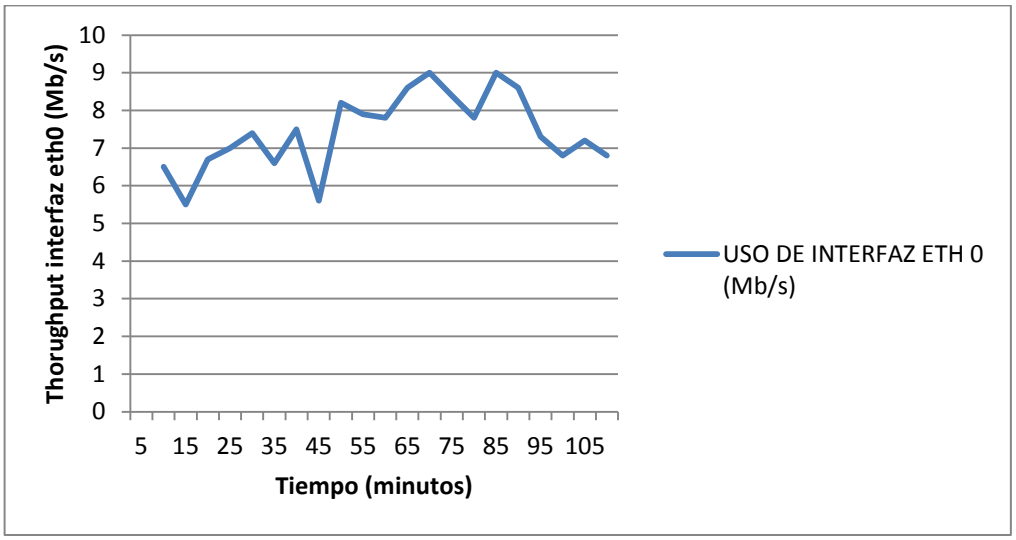

Figura 44: Gráfica con pruebas uso de interfaz eth0 multicast IPv4 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

6.2.7 Unicast IPv6 cinco clientes

Uso de CPU

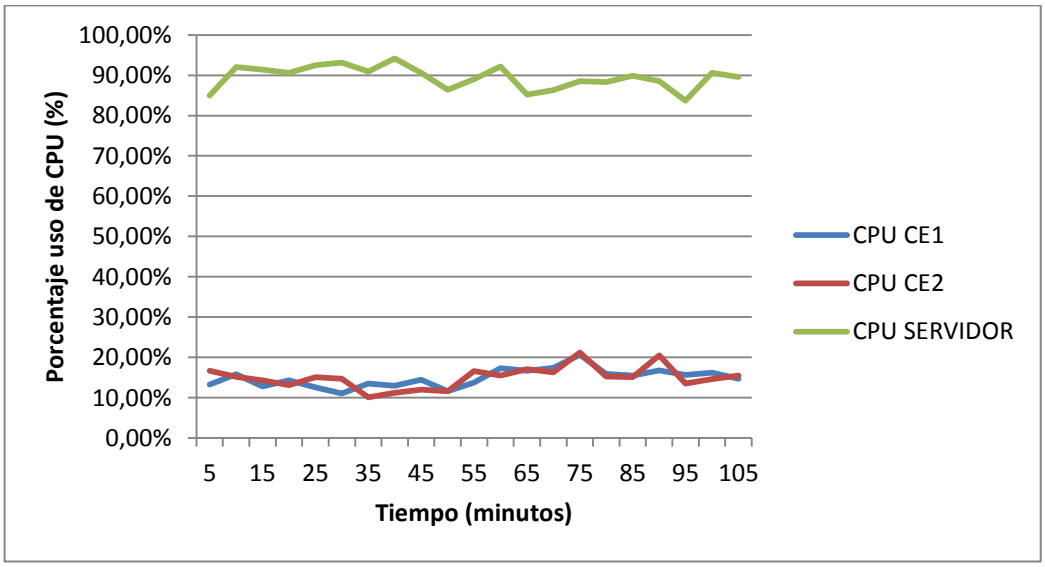

Figura 45: Gráfica con pruebas uso CPU unicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de memoria

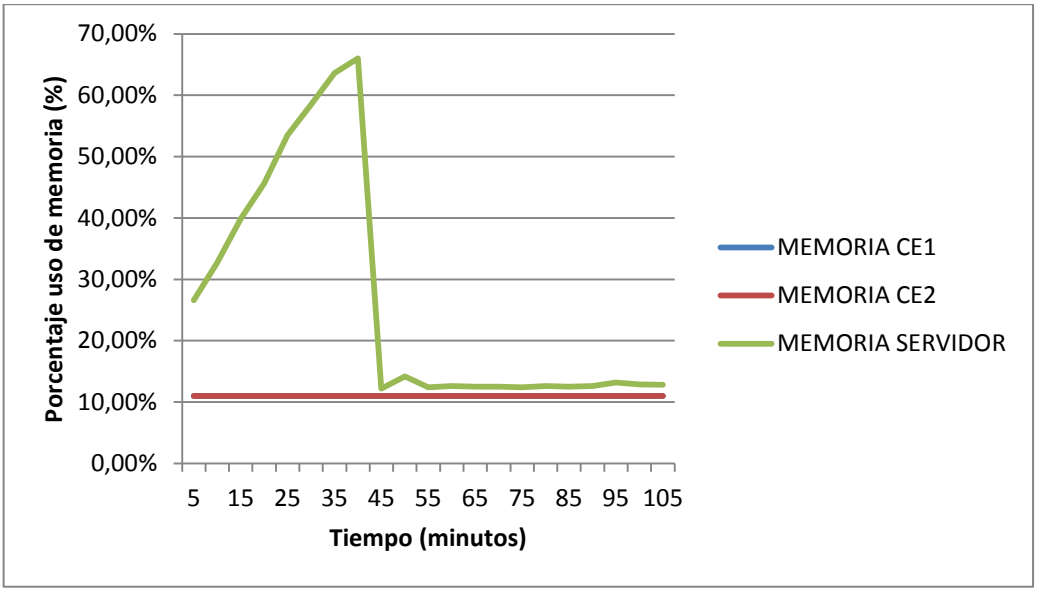

Figura 46: Gráfica con pruebas uso memoria unicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz router CE1

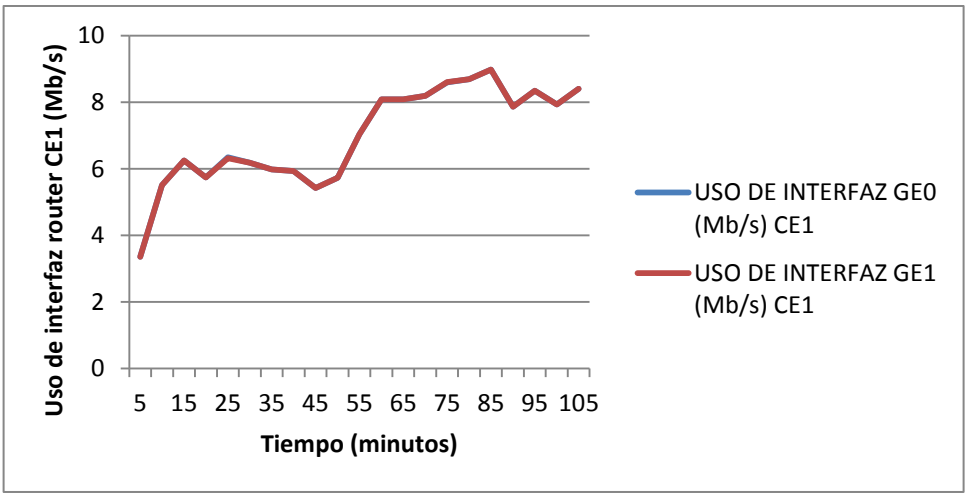

Figura 47: Gráfica con pruebas uso de interfaz router CE1 unicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz router CE2

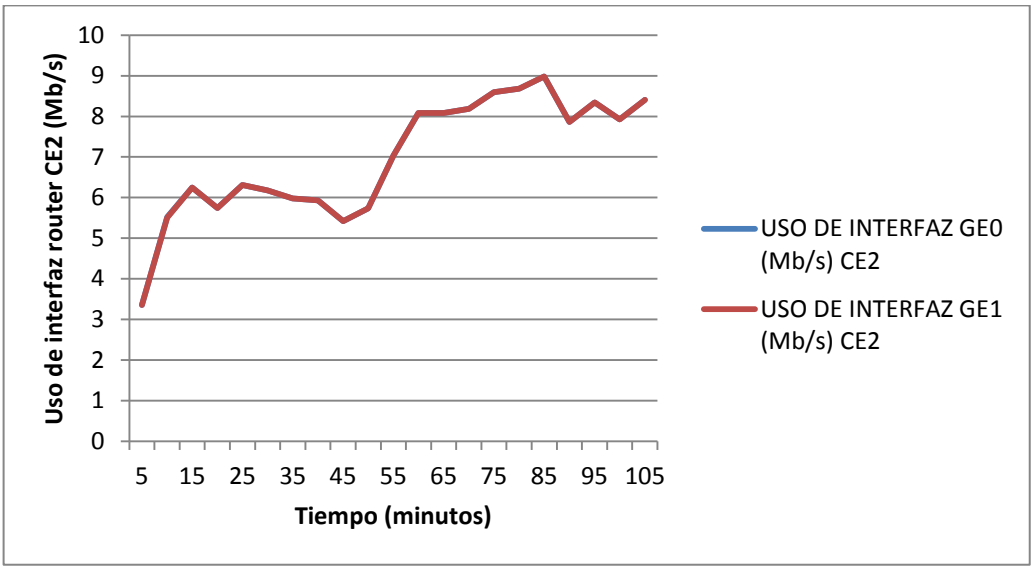

Figura 48: Gráfica con pruebas uso de interfaz router CE2 unicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz eth0

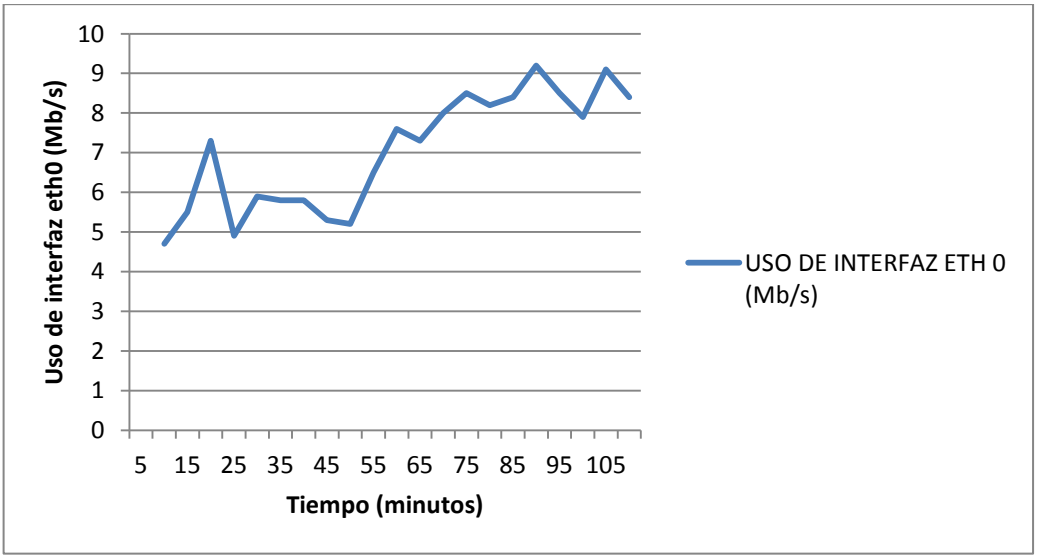

Figura 49: Gráfica con pruebas uso de interfaz eth0 unicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

6.2.8 Multicast IPv6 cinco clientes

Uso de CPU

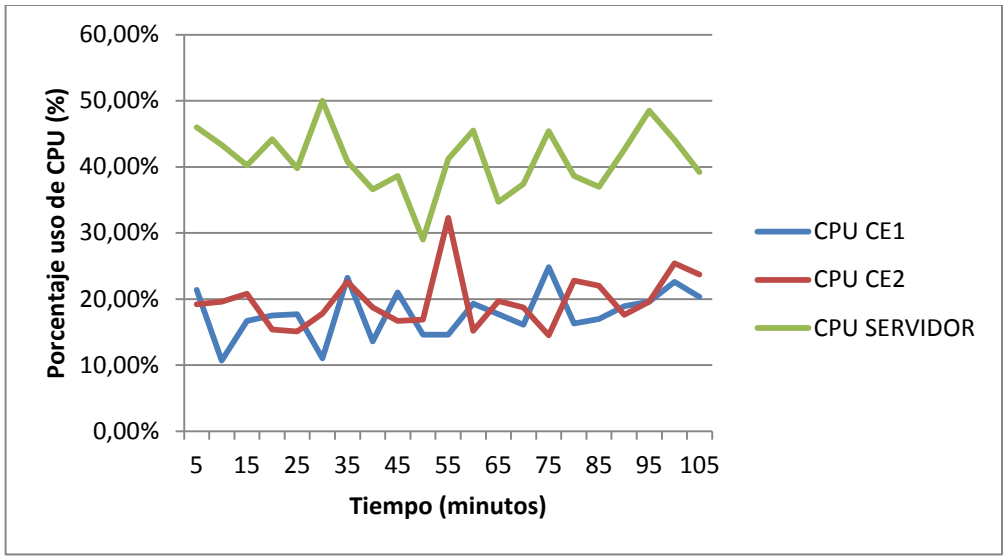

Figura 50: Gráfica con pruebas CPU multicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de memoria

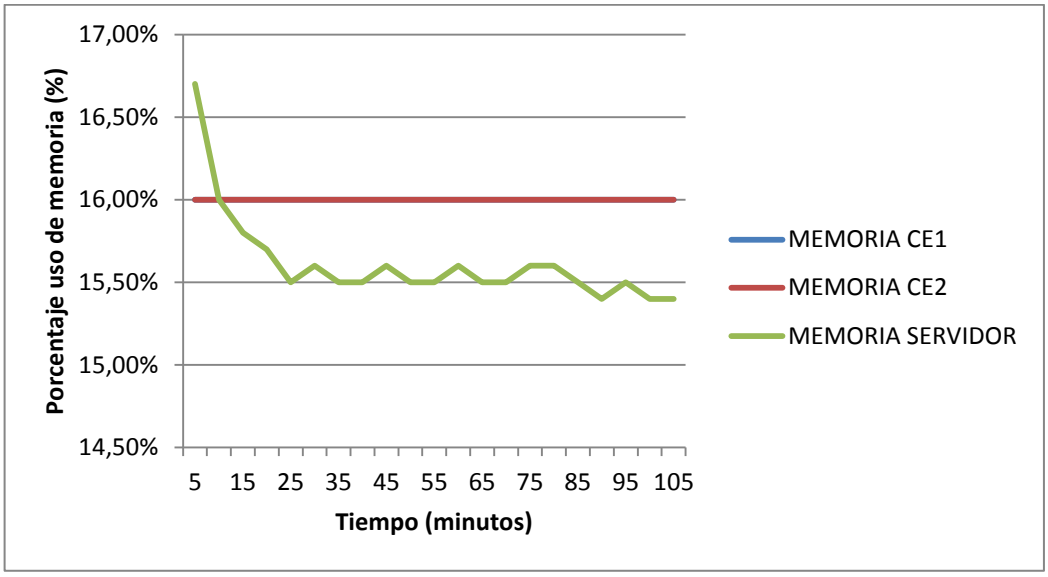

Figura 51: Gráfica con pruebas memoria multicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz router CE1

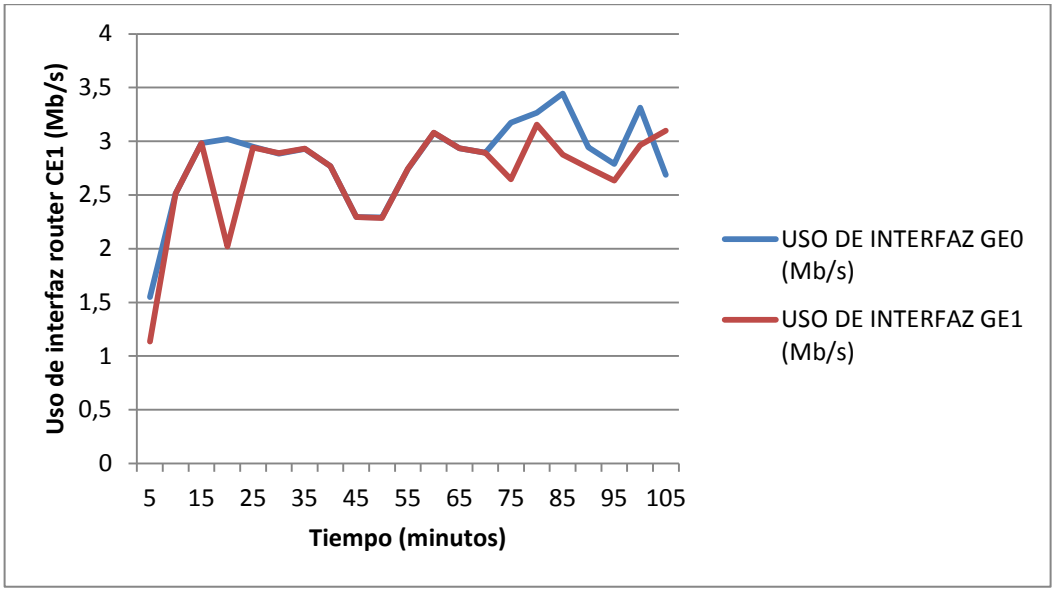

Figura 52: Gráfica con pruebas uso de interfaz router CE1 multicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz router CE2

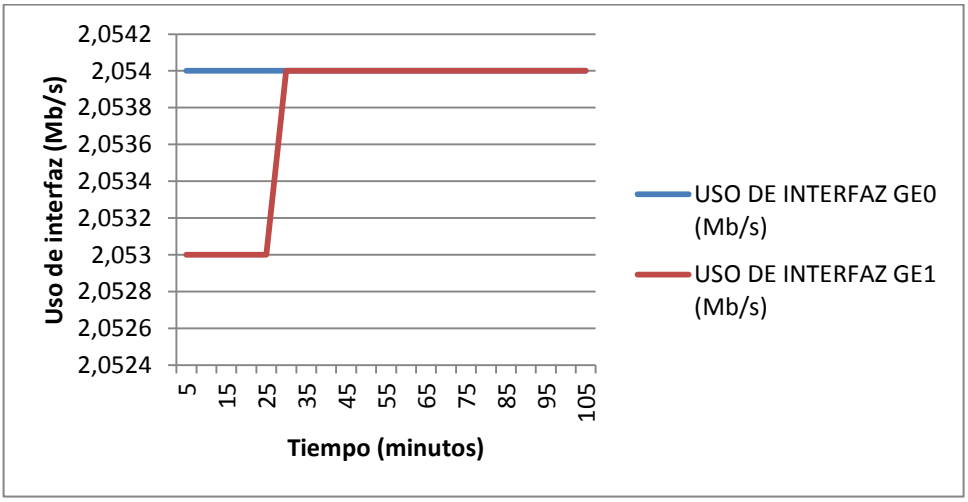

Figura 53: Gráfica con pruebas uso de interfaz router CE2 multicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Uso de interfaz interfaz eth0

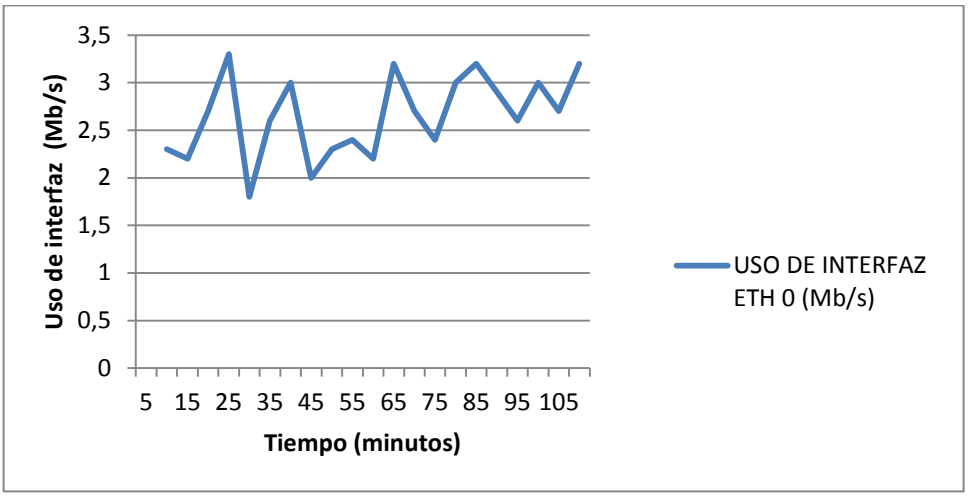

Figura 54: Gráfica con pruebas uso de interfaz eth0 multicast IPv6 cinco clientes. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

7. ANÁLISIS DE RESULTADOS

Luego de obtener las pruebas y graficar los resultados se realizó el análisis de éstos, para lo cual se presenta en la siguiente tabla el valor promedio de cada variable.

		CPU			MEMORIA		
PRUEBA		**CE1**	**CE2**	**SERVIDOR**	**CE1**	**CE2**	**SERVIDOR**
Un cliente	Unicast IPv4	7,09%	6,80%	8,60%	11%	11%	12.9%
	Multicast IPv4	15,14%	13,21%	14,68%	11%	11%	14,68%
	Unicast IPv6	5,52%	4,56%	33,65%	11%	11%	13,63%
	Multicast IPv6	17,84%	19.73%	41.08%	16%	16%	16.70%
Cinco clientes	Unicast IPv4	16,30%	15,59%	41,95%	11%	11%	13,20%
	Multicast IPv4	21,51%	11,66%	24,33%	11%	11%	9,89%
	Unicast IPv6	14,91%	14,01%	89,45%	11%	11%	26,28%
	Multicast IPv6	17,7%	18,20%	35,40%	16%	16%	16,21%

Tabla 4: Valor promedio de uso de CPU y memoria medidos en el proyecto. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Como las mediciones del uso de interfaz se realizaron cada cinco minutos, este parámetro será analizado en MB/min, con el fin de tener una medida acertada del uso de la interfaz cada minuto que se transmitió el video.

		USO DE INTERFAZ ROUTER CE1		**USO DE INTERFAZ ROUTER CE2**		**THROUGH PUT ETH 0 (Mb/min)**
PRUEBA		**GE0 (MB/min)**	**GE1 (MB/min)**	**GE0 (MB/min)**	**GE1 (MB/min)**	
Un cliente	Unicast IPv4	166,8	166,86	166,8	164,52	237,6
	Multicast IPv4	488,34	151,26	151,26	151,74	547,68
	Unicast IPv6	181,08	170,82	170,82	170,82	152,82
	Multicast IPv6	169,8	161,52	123,24	123,24	159
Cinco clientes	Unicast IPv4	589,56	589,56	589,62	638,4	888,42
	Multicast IPv4	496,98	171,36	171,36	171,36	445,8
	Unicast IPv6	418,8	418,8	418,86	418,86	422,82
	Multicast IPv6	170,16	170,7	123,24	123,24	173,4

Tabla 5: Valor promedio de uso de interfaz medido en el proyecto. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Observando las tablas se pueden realizar los siguientes análisis:

- El uso de CPU en los routers varía según el tipo de tráfico que se envía en la red, siendo para multicast mayor que para unicast. El router CE1 usa más su CPU que el router CE2 en todos los casos, excepto en la prueba de multicast IPv6. En cuanto al servidor, tiene un uso de CPU bajo para las pruebas IPv4 con un cliente, un uso medio con cinco clientes, y un uso muy elevado con cinco clientes en unicast IPv6. Aunque el procesamiento que realiza el router es mayor en multicast, este presenta un mejor rendimiento cuando maneja tráfico multicast, ya que el uso de interfaz es más bajo que en unicast.

- La memoria presenta un caso particular, ya que en ninguna de las pruebas realizadas el uso de memoria en los routers aumenta o disminuye, lo que mantiene a los routers siempre con un uso de memoria del 11%. Para multicast IPv6 el uso de memoria aumenta en un 5% ya que es necesario configurar PIM-SM para IPv6 con el fin de realizar estas pruebas. El servidor presenta un uso bajo de memoria para todos los casos, excepto para unicast IPv6, donde presenta un uso medio. La memoria de un router no se ve alterada por el tipo de tráfico que pasa por sus interfaces, por lo tanto el router no guarda la información que se transmite por él.

- El uso de la interfaz en el router CE1 es muy variado. Se puede observar que el uso más alto se presenta en la prueba de unicast IPv4 con cinco clientes llegando a un uso de interfaz de 10Mb/s en los routers y de 14Mb/s en el servidor. En multicast IPv4 se tiene un uso aproximado de 8Mb/s en la interfaz GE0 del router CE1, mientras que en las otras interfaces se tiene un uso de interfaz menor. Esto se debe a que esta interfaz es la que se encuentra conectada a la fuente multicast, es decir, el servidor, y mientras canales se tengan en emisión, mayor es la cantidad de información que envía. Para multicast IPv6 se emitió solo un canal y por ello el uso en la interfaz GE0 del router CE1 no es elevado. El uso de las demás interfaces fue constante a lo largo de la prueba. Mientras tanto la interfaz eth0 del servidor, tiene un uso similar al de la interfaz GE0 del router CE1, pues está enviando los distintos tipos de tráfico a esta interfaz. Mientras más canales se emitan en un flujo multicast, mas aumenta el uso de la interfaz conectada al servidor, sin embargo las otras interfaces del router mantienen un uso bajo.

- Realizando una comparación entre el uso del protocolo IPv4 e IPv6 en unicast se puede evidenciar lo siguiente: los routers usan una cantidad de CPU similar para IPv4 e IPv6, por lo que el uso de un protocolo u otro no afecta esta variable en los routers, sin embargo en el servidor si hay una diferencia del uso, siendo mayor para IPv6 que para IPv4. En el uso de las interfaces de los routers, tampoco se evidencia mucha diferencia para un protocolo o para otro. El servidor de streaming con IPv6 Unicast es el menos eficiente ya que consume una gran cantidad de CPU de la máquina, además de presentar un uso elevado en las interfaces del router.

- Se evidencian muchas diferencias cuando se realizaron las pruebas con un cliente y con cinco clientes, y el tipo de tráfico que se envía también genera diferente desempeño en la red. Al recibir cinco clientes multicast IPv4, se puede observar que el uso de las interfaces del router no varía en comparación con un cliente, mientras que en unicast las interfaces necesitan enviar más tráfico y están más llenas. Evidentemente el procesamiento aumenta en los routers y en el servidor. En multicast el router CE1 realiza más procesamiento que el router CE2.

- IPv6 unicast presenta un caso particular y es el gran uso de CPU que utiliza el servidor. Esto se debe al uso del protocolo RTP, en el cual se necesita realizar un streaming distinto para cada cliente conectado a la red.

En resumen se evidenciaron las siguientes características a la hora de realizar las pruebas:

- El uso de multicast es más beneficioso a la hora de realizar el streaming, ya que no consume muchos recursos de los routers y el uso en las interfaces es bajo, al ser una tecnología que duplica la información desde un punto de la red. A la hora de conectar más de un cliente a la red, unicast trae consigo una saturación de uso en las interfaces lo que conlleva a que la calidad del servicio brindado se deteriore y el video empieza a verse borroso y pausado a medida que una mayor cantidad de clientes se conecten a la red.
- Un servidor de video streaming demanda un uso de CPU considerado por parte del equipo donde se emite el flujo de video. Es por ello que tener un equipo el cual funcione correctamente a la hora de enviar un tráfico muy pesado es necesario para que no colapse la transmisión.
- El uso de IPv6 para este tipo de servicios es beneficioso en multicast, ya que presenta características de uso de interfaz similares a IPv4 y en los routers como en el servidor el uso de CPU no aumenta considerablemente. Usando VideoLAN se puede realizar una lista de canales multicast para realizar distintos streaming a la vez. Complementando esta característica con un servidor de IPTV se obtiene una plataforma completa de video muy eficaz para darle un servicio óptimo al usuario.
- El uso de memoria no es un parámetro al cual haya que darle mayor consideración a la hora de tratar con tráfico de video, ya que la información que pasa a través de la interfaz de un router no afecta el uso de memoria del mismo.

Una vez obtenidos estos resultados y luego de realizar este análisis profundo se realizaron gráficas comparativas donde se evidencia las diferencias del tipo de tráfico y protocolos usados. En la figura 55 se muestra la comparación usando como factor de medida el uso en la interfaz GE0 del router CE2 con cinco clientes

y en la figura 56 se muestra la comparación usando como factor de medida el uso de CPU en el router CE1 con cinco clientes también.

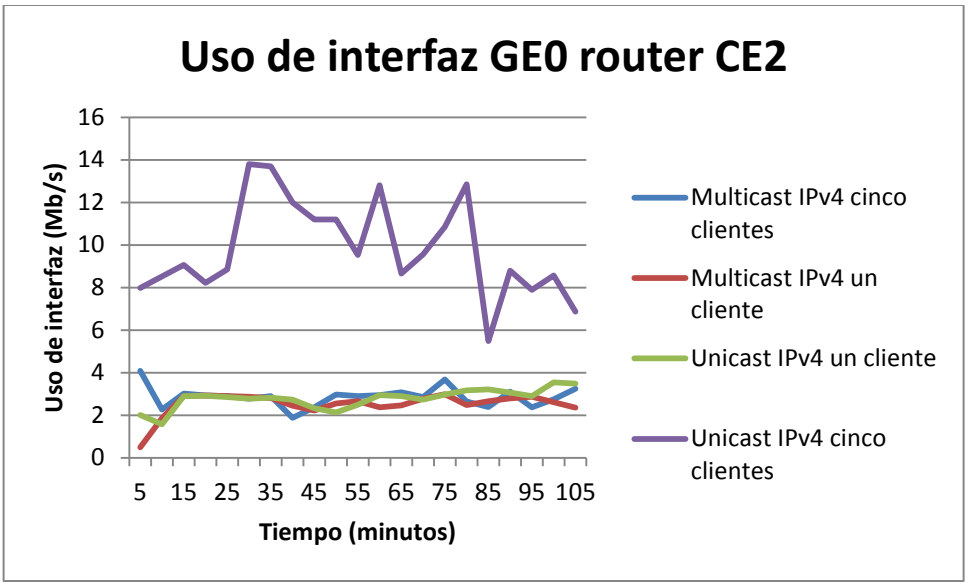

Figura 55: Gráfica comparativa entre uso de multicast y unicast. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

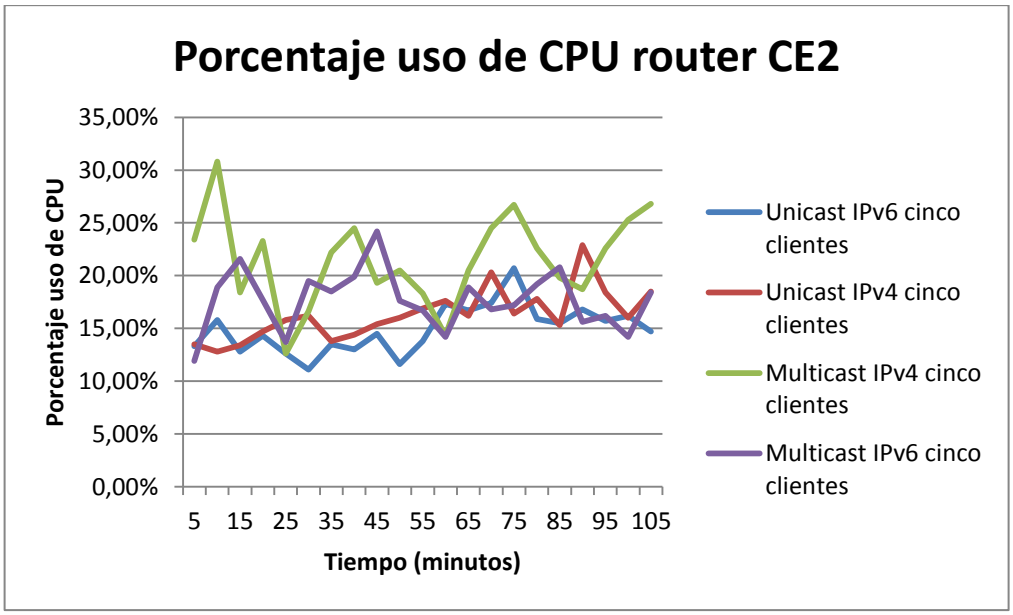

Figura 56: Gráfica comparativa entre uso de IPv4 e IPv6. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013

Observando la gráfica 55 se puede evidenciar el aumento del uso de interfaz en unicast al conectar cinco clientes y en la gráfica 56 existe un uso similar de CPU entre IPv4 e IPv6.

Como el uso de interfaz se midió cada cinco minutos, y la media está dada en MB/s, se realizó la conversión de los valores a MB/min, con el fin de tener un valor acorde a la escala de tiempo en la que se hizo la medición. En las siguientes tablas se observa el promedio de los resultados obtenidos para cada parámetro:

		RENDIMIENTO GENERAL EN ROUTERS		
PRUEBA		**USO DE CPU**	**USO DE MEMORIA**	**USO DE INTERFAZ (Mb/min)**
Un cliente	Unicast IPv4	6,95%	11%	166,245
	Multicast IPv4	14,18%	11%	235,65
	Unicast IPv6	5,04%	11%	173,385
	Multicast IPv6	18,66%	16%	144,45
Cinco clientes	Unicast IPv4	15,94%	11%	601,785
	Multicast IPv4	16,58%	11%	252,765
	Unicast IPv6	14,46%	11%	418,83
	Multicast IPv6	17,95%	16%	146,835

Tabla 6: Valor promedio de los parámetros medidos en routers. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

		RENDIMIENTO GENERAL EN SERVIDOR		
PRUEBA		**USO DE CPU**	**USO DE MEMORIA**	**USO DE INTERFAZ (Mb/min)**
Un cliente	Unicast IPv4	8,68%	12.9%	237,6
	Multicast IPv4	14,68%	15%	547,68
	Unicast IPv6	33,65%	14%	152,82
	Multicast IPv6	41.08%	16.70%	159
Cinco clientes	Unicast IPv4	41,95%	13%	888,42
	Multicast IPv4	24,33%	10%	445,8
	Unicast IPv6	89,45%	26%	422,82
	Multicast IPv6	35,40%	16%	173,4

Tabla 7: Valor promedio de los parámetros medidos en el servidor. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Complementando las gráficas donde se compara el rendimiento del tipo de tráfico usado y el protocolo usado, se realizó un promedio de los parametros discriminando el router con el servidor. En las siguientes tablas se observan estos resultados comparativos del uso de unicast y de multicast:

		PROMEDIO EN ROUTERS		
PRUEBA		**USO DE CPU**	**USO DE MEMORIA**	**USO DE INTERFAZ (Mb/min)**
Un cliente	Unicast	5,99%	11,00%	169,815
	Multicast	16,42%	13,50%	190,05
Cinco clientes	Unicast	15,20%	11,00%	510,31
	Multicast	17,27%	13,50%	199,80

Tabla 8: Tabla comparativa de Unicast y Multicast en routers. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

		PROMEDIO EN SERVIDOR		
PRUEBA		**USO DE CPU**	**USO DE MEMORIA**	**USO DE INTERFAZ (Mb/min)**
Un cliente	Unicast	21,17%	13,63%	195,21
	Multicast	27,88%	15,69%	353,34
Cinco clientes	Unicast	65,70%	19,74%	655,62
	Multicast	29,87%	13,05%	309,60

Tabla 9: Tabla comparativa de Unicast y Multicast en servidor. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

A su vez se realizó la misma operación pero comparando el uso de IPv4 con el uso de IPv6. En las tablas 10 y 11 se observan los resultados:

		PROMEDIO EN ROUTERS		
PRUEBA		**USO DE CPU**	**USO DE MEMORIA**	**USO DE INTERFAZ (Mb/min)**
Un cliente	IPv4	10,56%	11,00%	200,95
	IPv6	11,85%	13,50%	158,92
Cinco clientes	IPv4	16,26%	11,00%	427,28
	IPv6	16,21%	13,50%	282,83

Tabla 10: Tabla comparativa de IPV4 e IPv6 en routers. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

		PROMEDIO EN SERVIDOR		
PRUEBA		**USO DE CPU**	**USO DE MEMORIA**	**USO DE INTERFAZ (Mb/min)**
Un cliente	IPv4	11,68%	14,68%	392,64
	IPv6	37,37%	15,17%	155,91
Cinco clientes	IPv4	33,14%	11,55%	667,11
	IPv6	62,43%	21,25%	298,11

Tabla 11: Tabla comparativa de IPV4 e IPv6 en servidor. Fuente: **Andrés Felipe Macías Díaz.** Facultad de Ingeniería de Telecomunicaciones, Universidad Santo Tomás, Bogotá, Colombia: 2013.

Llevando a cabo este análisis y dando a conocer los resultados obtenidos se finaliza el trabajo realizado en este proyecto de grado, mostrando finalmente que la mejor opción para una red a la hora de implementar un servicio de video como IPTV o video streaming es utilizar tráfico Multicast en IPv6, usando la herramienta de software libre VideoLAN. A continuación se presentarán las conclusiones basándose en los objetivos establecidos en este proyecto.

CONCLUSIONES

- Multicast es el tipo de tráfico que genera menor uso de las interfaces con respecto Unicast a la hora de conectar más de un cliente a la red, lo que lo hace mejor que Unicast a la hora de transportar flujo de video.

- El procesamiento en un router es mayor usando Multicast que Unicast, solo si alguna interfaz de ese router es punto de encuentro (RP), ya que es en ese punto donde tiene que multiplicar el video a todos los clientes. Otra razón puede ser que en Multicast se utilizan dos protocolos para su funcionamiento: OSPF y PIM-SM.

- En las mediciones realizadas se ve que IPv6 usa un poco mas de memoria y procesador que IPv4, esto se debe a diversos factores de los cuales no se pudo conseguir información, por ejemplo: no se tiene información del funcionamiento del sistema operativo de los equipos activos de red, ni si este está optimizado para realizar procesamiento paralelo en paquetes IPv4 o en IPv6, ya que los routers usados cuentan con procesador de cuatro núcleos, por esto, no se puede determinar a ciencia cierta el porqué de estos resultados. Otra oportunidad de mejora para un siguiente proyecto, es contar con mejores herramientas de gestión de red, las cuales permitan obtener datos de las variables analizadas con más resolución.

- El uso de la interfaz es independiente del uso de IPv4 o IPv6 y dependiente del tipo de tráfico transmitido en la red.

- Al implementar la herramienta VideoLAN se observó que es la más adecuada para funcionar con IPTV e IMS CORE ya que presenta compatibilidad con IPv6 y posee múltiples funciones para la emisión de canales Multicast. Sin embargo tiene la limitación del uso del protocolo RTSP en IPv6, lo que genera un uso muy elevado de CPU a la hora de generar tráfico Unicast para muchos clientes.

- El protocolo de enrutamiento unicast OSPFv3 es compatible para ser implementado en una red IP la cual pretenda ofrecer servicios multimedia en IPv6. Esto se debe a que OSPF es compatible con IPv6.

- PIM-SM es el protocolo de enrutamiento Multicast que ofrece buena funcionalidad y al ser compatible con IPv4 e IPv6 permitió transmitir el tráfico IPv4 e IPv6 en el ambiente de pruebas de red implementado, sin embargo para su funcionalidad fue necesario actualizar el sistema operativo de los routers usados en las pruebas.

- La herramienta de monitoreo de red MRTG no es una herramienta muy completa de monitoreo de red, ya que no permite la medición del uso de CPU y la ocupación de memoria, entre otros parámetros, para tener esta funcionalidad se debe implementar la herramienta FDDtool, con el fin de mostrar las gráficas en tiempo real, sin embargo en este proyecto no fue posible la implementación de esta solución, lo que obligó a medir las variables con una resolución no muy alta.

Anexo 1

new musica vod enabled
setup musica input /home/musica.mpeg

En esta sección se establece el flujo unicast que se transportó usando el protocolo RTSP a través de la red. El video que se transmite es un video bajo demanda, por lo tanto el cliente puede acceder y manipular la reproducción del video en cualquier momento. Con la opción *input* se especifica la ruta en la que se encuentra el video.

new channel1 broadcast enabled : se especifíca un nuevo canal de broadcast llamado *channel1*

setup channel1 input /home/andicom.mpeg loop : se añade la ruta del video a transmitir y con la opción loop se inicia un ciclo de reproducción infinito

setup channel1 output #rtp{access=tcp,mux=ts,dst=224.255.1.1, sdp=sap,sap, name="Canal 1"}: se configuran opciones de la salida RTP como el acceso TCP, multiplexor TS, la dirección multicast, el uso de SAP como protocolo de anuncio de los canales y el nombre del canal *Canal 1*.

control channel1 play: con esta opción se le ordena a VLC que ejecute el canal.

Esta misma configuración aplica para todos los canales que se quieran emitir.

new channel2 broadcast enabled
setup channel2 input /home/prisma.mpeg loop
setup channel2 output
#rtp{access=tcp,mux=ts,dst=224.255.1.2,sdp=sap,sap,name="Canal 2"}

new channel3 broadcast enabled
setup channel3 input /home/musica.mpeg loop
setup channel3 output
#rtp{access=tcp,mux=ts,dst=224.255.1.3,sdp=sap,sap,name="Canal 3"}

control channel2 play

control channel3 play

Anexo 2

```
<CE1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        3.3.3.3/32  Direct  0    0           D   127.0.0.1       LoopBack0
        6.6.6.6/32  OSPF    10   1           D   10.0.0.2        GigabitEthern1
       10.0.0.0/24  Direct  0    0           D   10.0.0.1        GigabitEthern1
       10.0.0.1/32  Direct  0    0           D   127.0.0.1       GigabitEthern1
     10.0.0.255/32  Direct  0    0           D   127.0.0.1       GigabitEthern1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Anexo 3

```
<CE2>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        3.3.3.3/32  OSPF    10   1           D   10.0.0.1        GigabitEthern0
```

6.6.6.6/32	Direct	0	0	D	127.0.0.1 LoopBack0
10.0.0.0/24	Direct	0	0	D	10.0.0.2 GigabitEthern0
10.0.0.2/32	Direct	0	0	D	127.0.0.1 GigabitEthern0
10.0.0.255/32	Direct	0	0	D	127.0.0.1 GigabitEthern0
127.0.0.0/8	Direct	0	0	D	127.0.0.1 InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1 InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1 InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1 InLoopBack0

Anexo 4

```
<CE2>display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.0.0.2
    Priority: 0
    Hash mask length: 30
    State: Elected
    Scope: Not scoped
    Uptime: 00:34:13
    Next BSR message scheduled at: 00:00:48
    C-RP Count: 1
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: 10.0.0.2
    Priority: 0
    Hash mask length: 30
    State: Elected
    Scope: Not scoped
    Wait to be BSR: 0
```

Anexo 5

```
<CE1>display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 4 (S, G) entries

 (172.18.10.133, 224.2.127.254)
```

RP: 10.0.0.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:00:21
Upstream interface: GigabitEthernet0/0/0
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information: None

(172.18.10.133, 224.255.1.1)
RP: 10.0.0.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:00:22
Upstream interface: GigabitEthernet0/0/0
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information: None

(172.18.10.133, 224.255.1.2)
RP: 10.0.0.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:00:22
Upstream interface: GigabitEthernet0/0/0
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information: None

(172.18.10.133, 224.255.1.3)
RP: 10.0.0.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:00:22
Upstream interface: GigabitEthernet0/0/0
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information: None

Anexo 6

<CE2>display pim routing-table
VPN-Instance: public net
Total 4 (*, G) entries; 4 (S, G) entries

(*, 224.2.127.254)
RP: 10.0.0.2 (local)
Protocol: pim-sm, Flag: WC
UpTime: 00:00:26

```
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet0/0/1
            Protocol: igmp, UpTime: 00:00:26, Expires: -

(172.18.10.133, 224.2.127.254)
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: SPT 2MSDP ACT
    UpTime: 00:05:40
    Upstream interface: GigabitEthernet0/0/0
        Upstream neighbor: 10.0.0.1
        RPF prime neighbor: 10.0.0.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet0/0/1
            Protocol: pim-sm, UpTime: 00:00:26, Expires: -

(*, 224.255.1.1)
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:19
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet0/0/1
            Protocol: igmp, UpTime: 00:00:19, Expires: -

(172.18.10.133, 224.255.1.1)
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: SPT 2MSDP ACT
    UpTime: 00:05:41
    Upstream interface: GigabitEthernet0/0/0
        Upstream neighbor: 10.0.0.1
        RPF prime neighbor: 10.0.0.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet0/0/1
            Protocol: pim-sm, UpTime: 00:00:19, Expires: -

(172.18.10.133, 224.255.1.2)
```

```
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: 2MSDP ACT
    UpTime: 00:05:41
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information: None

(172.18.10.133, 224.255.1.3)
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: 2MSDP ACT
    UpTime: 00:05:41
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information: None

(*, 239.195.255.255)
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:26
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet0/0/1
            Protocol: igmp, UpTime: 00:00:26, Expires: -

(*, 239.255.255.255)
    RP: 10.0.0.2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:26
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: GigabitEthernet0/0/1
            Protocol: igmp, UpTime: 00:00:26, Expires: -
```

Anexo 7

```
<CE1>display ospfv3 routing

Codes : E2 - Type 2 External, E1 - Type 1 External, IA - Inter-Area,
        N - NSSA, U - Uninstalled

OSPFv3 Process (1)
     Destination
Metric
       Next-hop
     2000:A::/64
1
       directly connected, GigabitEthernet0/0/1
     3333::3/128
0
       directly connected, LoopBack0
     6666::6/128
1
       via FE80::DED2:FCFF:FE59:2B82, GigabitEthernet0/0/1
     FC00:B::/64
2
       via FE80::DED2:FCFF:FE59:2B82, GigabitEthernet0/0/1
```

Anexo 8

```
<CE2>display ospfv3 routing

Codes : E2 - Type 2 External, E1 - Type 1 External, IA - Inter-Area,
        N - NSSA, U - Uninstalled

OSPFv3 Process (1)
     Destination
          Metric
       Next-hop
     2000:A::/64                                                    1
       directly connected, GigabitEthernet0/0/0
     3333::3/128                                                    1
       via FE80::DED2:FCFF:FE59:2BE3, GigabitEthernet0/0/0
     6666::6/128                                                    0
       directly connected, LoopBack0
     FC00:B::/64
1
```

directly connected, GigabitEthernet0/0/1

Anexo 9

```
<CE1>display current-configuration
[V200R002C01SPC200]
#
 sysname CE1
#
 snmp-agent community write %$%$bm2tF8%[=Op"^iSJ}*(V$6-$%$%$
 snmp-agent
#
 drop illegal-mac alarm
#
ipv6
#
router id 3.3.3.3
#
multicast routing-enable
#
set transceiver-monitoring disable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
ospfv3 1
 router-id 3.3.3.3
#
firewall zone local
 priority 16
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 172.18.10.129 255.255.255.0
 ipv6 address FC00:A::2/64
 ospfv3 1 area 0.0.0.2
 pim sm
#
interface GigabitEthernet0/0/1
 ipv6 enable
```

```
 ip address 10.0.0.1 255.255.255.0
 ipv6 address 2000:A::1/64
 ospfv3 1 area 0.0.0.2
 pim sm
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
interface LoopBack0
 ipv6 enable
 ip address 3.3.3.3 255.255.255.255
 ipv6 address 3333::3/128
 ospfv3 1 area 0.0.0.2
#
ospf 1
 area 0.0.0.1
  network 3.3.3.3 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 172.18.10.0 0.0.0.255
#
pim
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$-%%/-wD"uMp;NVLPKnn4,)}t-
g0[=2H_&!cN>sE$
user-interface vty 0 4
user-interface vty 16 20
#
voice
 #
 diagnose
#
return
```

Anexo 10

```
<CE2>display current-configuration
[V200R002C01SPC200]
#
 sysname CE2
#

 snmp-agent community write %$%$$hy}#4<u`C8Q807ZFQ9B,of]%$%$
```

```
 snmp-agent
#
 drop illegal-mac alarm
#
ipv6
#
router id 6.6.6.6
#
multicast routing-enable
#
set transceiver-monitoring disable
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
ospfv3 1
 router-id 6.6.6.6
#
firewall zone local
 priority 16
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 10.0.0.2 255.255.255.0
 ipv6 address 2000:A::2/64
 ospfv3 1 area 0.0.0.2
 pim sm
#
interface GigabitEthernet0/0/1
 ipv6 enable
 ip address 192.18.30.1 255.255.255.0
 ipv6 address FC00:B::2/64
 ospfv3 1 area 0.0.0.2
 pim sm
 igmp enable
 igmp version 3
#
interface GigabitEthernet0/0/2
#
```

```
interface NULL0
#
interface LoopBack0
 ipv6 enable
 ip address 6.6.6.6 255.255.255.255
 ipv6 address 6666::6/128
 ospfv3 1 area 0.0.0.2
#
ospf 1
 area 0.0.0.1
  network 6.6.6.6 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 192.18.30.0 0.0.0.255
#
pim
 c-bsr GigabitEthernet0/0/0
 c-rp GigabitEthernet0/0/0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$-
4(zY1;X<;J@iy.I6'N1,i`Ww0m3QKIGZU/x.F8$
user-interface vty 0 4
user-interface vty 16 20
#
voice
 #
 diagnose
#
return
```

Anexo 11

```
 <?xml version="1.0" encoding="UTF-8"?>

<key-value_pairs>
 <key-value_pair>
     <key>channel1</key>
     <value>rtsp://172.18.10.133:8000/channel1</value>
 </key-value_pair>

 <key-value_pair>
     <key>channel2</key>
     <value> rtsp://172.18.10.133:8000/channel2</value>
```

```
 </key-value_pair>

 <key-value_pair>
     <key>channel3</key>
     <value> rtsp://172.18.10.133:8000/channel3</value>
 </key-value_pair>
</key-value_pairs>
```

En este archivo se configuran los canales que el servidor de IPTV va a dejar emitir. Para ello es necesario tener el streaming funcionando en VideoLAN usando la misma ruta de transmisión "*rtsp://172.18.10.133:8000/channel3*", es decir usando el protocolo RTSP, la dirección IP 172.18.10.133:8000, el puerto 8000 y el mismo nombre de emisión VoD.

Bibliografía

1. *The UCT IMS IPTV Initiative.* **Richard Spiers, Robert Marston, Richard Good.** University of Cape Town, Rondebosch, South Africa : s.n. 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies. pp. 503-508.
2. **Fit, Dr Didnie.** *TCP/IP: Arquitectura, protocolos e implementación con IPv6 y seguridad de IP.* Estados Unidos : McGraw-Hill, 1998. 0-07-021389-5.
3. *Migración del protocolo IPv4 a IPv6.* **Mejía, Oscar Ávila.** pág.55 -60 , Depto. de Ingeniería eléctrica : Revista ContactoS, 2011, Vol. 79, pp. 55 – 60.
4. *Unique Local IPv6 Unicast Addresses.* **R. Hinden, B. Haberman.** October 2005. RFC 4193.
5. *Analysis of Internet Multicast Traffic Performance Considering Multicast Routing Protocol.* **Seiji Ueno, Toshihiko Kato, Kenji Suzuki.** KDD R&D Laboratories : s.n. pp. 95 – 104.
6. **Technologies, Huawei.** *Troubleshooting - IP Multicast.* s.l. : Huawei Technologies, 2011.
7. **Jose Manuel Huidobro Moya, Ramon Jesús Millan Tejedor.** *Redes de datos y convergencia.* Mexico D.F. : Alfaomega, 2007. 978-970-15-1278-4.
8. *OSPF for IPv6.* **R. Coltun, D. Ferguson, J. Moy.** July 2008. RFC 5340.
9. *Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network.* **Wijaya, C.** 2011.
10. *An Anatomy of IGP and BGP Routing Protocols.* **Mohammed Ali Yousef, Imad F.T. Alshaikhli, Abdulrahman Alkandari.** Malasya : s.n., 2012. International Conference on Advanced Computer Science Applications and Technologies. pp. 279-283.
11. **Certifications, Huawei Datacom.** *Building Carrier Routing Network Lab Guide.* Estados Unidos : Huawei Certifications, 2008.
12. **Cabezas, Jesús Gil.** *Protocolo de Transporte en Tiempo Real - RTP.* 2009.
13. *Internet Protocol Television (IPTV): Architecture,Trends, and Challenges.* **Sherali Zeadally, Hassnaa Moustafa.** DECEMBER 2011. IEEE SYSTEMS JOURNAL, VOL. 5, NO. 4. pp. 518-527.
14. *An effective simple method to reduce bandwidth usage over an access link in IPTV multicast delivery services.* **Masao IKEZAKI∗, Takeshige SUGAHARA∗, Masayoshi SHIMAMURA.** Kyushu Institute of Technology, Fukuoka, Japan : s.n., 2010. TENCON 2010. pp. 1460 – 1465.
15. **Technologies, Hangzhou H3C.** *SNMPv3 User Copy-and-Paste Function Configuration Examples.*
16. **Cyril Deguet, Alexis de Lattre.** *Guía de usuario de VLS.* s.l. : VideoLAN, 2004.
17. *NOVEL QUEUING MODEL FOR IMS-BASED IPTV SYSTEM.* **Wang Jianhui, Jin Hao, Wu Wenguang.** Beijing : s.n., 2009. Wireless Signal Processing & Network Lab (WSPN),. págs. 560 – 564.

18. *Multicast Instant Channel Change in IPTV Systems.* **Damodar Banodkar, K.K. Ramakrishnan, Shivkumar Kalyanaraman, Alexandre Gerber, Oliver Spatscheck.** AT&T Labs Research : s.n.
19. *Functional Architecture for NGN-Based Personalized IPTV Services.* **Gyu Myoung Lee, Chae Sub Lee.** JUNE 2009. IEEE TRANSACTIONS ON BROADCASTING, VOL. 55, NO. 2. pp. 329-342.
20. *Multimedia Distribution over IPTV and its Integration with IMS.* **Mohammed Abdul Qadeer, Afaq Hasan Khan.** Aligarh Muslim University, Aligarh : s.n., 2010. International Conference on Data Storage and Data Engineering. pp. 101 – 105.
21. **Co., Huawei Technologies.** *Building Carrier Routing Network Lab Guide.* s.l. : Huawei Certifications, 2008.
22. *Benchmarking Terminology for Network Interconnection Devices. RFC 1242.* **Bradner, S.** Harvard University : s.n., 1991.