UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TÍTULO:

SIMULACIÓN DE LA CONVERGENCIA DEL PROTOCOLO IPv4 A IPv6

AUTOR:

BORIS TEÓFILO VERA CARRIEL

Previa la obtención del Título

INGENIERO EN TELECOMUNICACIONES

TUTORA:

M. Sc. Luzmila Ruilova Aguirre

Guayaquil, Ecuador

2015

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Sr. **Boris Teófilo Vera Carriel** como requerimiento parcial para la obtención del título de INGENIERO EN TELECOMUNICACIONES.

TUTOR

_____

M. Sc. Luzmila Ruilova Aguirre

DIRECTOR DE CARRERA

_____

M. Sc. Miguel A. Heras Sánchez.

Guayaquil, a los 05 del mes de Septiembre del año 2015

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Boris Teófilo Vera Carriel**

DECLARÓ QUE:

El trabajo de titulación "SIMULACIÓN DE LA CONVERGENCIA DEL PROTOCOLO IPv4 A IPv6" previa a la obtención del Título de Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 05 del mes de Septiembre del año 2015

EL AUTOR

_____

BORIS TEÓFILO VERA CARRIEL

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Boris Teófilo Vera Carriel**

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: "SIMULACIÓN DE LA CONVERGENCIA DEL PROTOCOLO IPv4 A IPv6", cuyo contenido, ideas y criterios es de mi exclusiva responsabilidad y autoría.

Guayaquil, a los 05 del mes de Septiembre del año 2015

EL AUTOR

_____

BORIS TEÓFILO VERA CARRIEL

DEDICATORIA

El concepto de este proyecto de tesis está dedicado a mis padres, pilares fundamentales en mi vida y a mi abuelita Isabel Ibarra ya que no esta en este mundo siempre deseo verme como un profesional, sin ellos jamás hubiese podido conseguir lo que hasta ahora.

Su lucha insaciable ha hecho un gran ejemplo de seguir y destacar ya que me permitió esforzarme hacia la meta de ser un profesional

EL AUTOR

BORIS TEÓFILO VERA CARRIEL

AGRADECIMIENTO

En primer lugar a Dios por haberme guiado por el camino de la felicidad hasta ahora y en segundo lugar a mi familia a mi Padre Teófilo Vera a mi Madre Ana María Carriel a mis hermanos y a mis tíos por siempre darme el apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Y por último a mis compañeros del seminario como son Steven delgado , Andrés posligua porque en esta armonía grupal lo hemos logrado y a mis Profesores quien les llevo gran parte de mis conocimientos gracias por su paciencia y enseñanza. Finalmente a la Universidad Católica Santiago de Guayaquil y a la facultad técnica para el desarrollo la cual abrió nuestras puertas a jóvenes como nosotros preparándonos para el futuro formándonos personas de bien

EL AUTOR

BORIS TEÓFILO VERA CARRIEL

Índice General

Índice de Figuras

Capítulo 2:

Capítulo 3:

Índice de Tablas

Capítulo 3

Resumen

El propósito principal de realizar la simulación de la convergencia de los protocolos Ipv4 a Ipv6 fue la evaluación y comparación del desempeño de los dos protocolos(Ipv4 e Ipv6) sobre algunas herramientas, como el evaluador de protocolos de internet wireshark y jperf en términos de varios parámetros fueron analizados cuando los datos se transmiten de un cliente a otro, o de un servidor través de una red cableada .Los escenarios de simulación de las técnicas de Ipv4 e Ipv6 nos permitieron analizar el comportamiento de los protocolos en función de la potencia de cálculo disponible para ejecutar el experimento de simulación de redes. La red se compone de varios componentes como servidores, routers, clientes, etc. En general, el objetivo fue evaluar el rendimiento de la perdida de paquetes, latencia y otros parámetros

CAPÍTULO 1: GENERALIDADES DEL TRABAJO DE TITULACIÓN

1.1. Antecedentes.

El Internet ha crecido enormemente en los últimos años. Lo que comenzó como un experimento se ha convertido en la red en todo el mundo que hoy conocemos. Un gran número de usuarios se suscriben a servicios multimedia en línea, tales como la transmisión de vídeo. Servicios de mensajería como Skype y Gtalk están reemplazando a los teléfonos tradicionales para las llamadas de larga distancia a través de las zonas urbanas en muchos países.

El intercambio de información en términos generales se puede clasificar como unicast (uno a uno), difusión (uno a todos) y multicast (uno-a-muchos). Un ejemplo típico de la multidifusión es, Yahoo Messenger en varios hosts suscritos al servicio y el servidor se comunica sólo con aquellas máquinas que se han suscrito a la misma. Una de las mayores ventajas de la multidifusión es la conservación de ancho de banda.

El servidor multidifusión envía sólo un paquete y el router genera entonces múltiples paquetes para llegar a cada uno de los receptores. De esta manera los recursos de red se utilizan de manera eficiente. Además, la multidifusión garantiza una recepción oportuna de los datos por parte de los receptores. El enrutamiento unicast, el servidor envía un paquete a cada uno de los receptores.

1.2. Justificación del Problema.

Desde que la convergencia de datos y redes de voz, aplicaciones como videoconferencia y voz sobre IP (VoIP) han encontrado su camino en las redes empresariales. Puesto que tales aplicaciones son el ancho de banda intensivo, una solución multidifusión puede adoptarse cuando hay varios destinatarios de los mismos datos.

Se espera que el espacio de direcciones IPv4 se agoten con el tiempo, ya que el internet está creciendo cada día. La migración a la dirección IPv6 de 128 bits ya ha comenzado y reemplazaría a IPv4. Mientras que esta transición se encuentra en sus etapas iniciales, este trabajo de titulación ofrece la oportunidad de adquirir conocimientos básicos de IPv6, que es el futuro de Internet.

1.3. Definición del Problema.

Necesidad de diseñar modelos de simulación para evaluar la convergencia del protocolo IPv4 a IPv6 mediante enrutamientos multidifusión en redes IPv4 e IPv6.

1.4. Objetivos del Problema de Investigación.

En esencia, este trabajo de titulación tiene como objetivo:

1.4.1. Objetivo General.

Modelar escenarios de la convergencia del protocolo IPv4 a IPv6 mediante enrutamientos multidifusión en redes IPv4 e IPv6.

1.4.2. Objetivos Específicos.

- Describir la fundamentación teórica del protocolo de internet y de la coexistencia entre protocolos IPv4 e IPv6.
- Diseñar modelos o escenarios de simulación de cuatro protocolos en redes IPv4 e IPv6.
- Evaluar los resultados obtenidos de los cuatro escenarios propuestos como modelos de simulación en redes IPv4 e IPv6.

1.5. Hipótesis.

Mediante la evaluación de los escenarios experimentales propuestos permitirá comprobar el desempeño de las redes IPv4 e IPv6 a través de enrutamientos multidifusión.

1.6. Metodología de Investigación.

Este trabajo de titulación es cuantitativo, lo que implica que se irá agrupando los resultados de los experimentos realizados. El montaje experimental, consiste en cuatro routers Cisco. El primer y el último router de la cadena estaban conectados a Hubs. Cada centro tenía dos ordenadores conectados a él. Uno de los ordenadores era la fuente para el tráfico de multidifusión y los otros tres son receptores. El protocolo de enrutamiento unicast subyacente elegido es el Open Shortest Path First (OSPF), un protocolo de enrutamiento utilizado popularmente en redes empresariales.

CAPÍTULO 2: FUNDAMENTOS TEÓRICOS

2.1. Introducción del protocolo de internet (IP).

Con el agotamiento del espacio disponible de direcciones IPv4 a nivel IANA-to-RIR (Autoridad de Asignación de Números de Internet-a-Registro Regional de Internet), es sólo cuestión de tiempo antes del agotamiento de RIR, seguido por el agotamiento ISP. En el momento del agotamiento de las ISP´s, las organizaciones empresariales ya no serán capaces de obtener espacio de direcciones IPv4 para la expansión de redes o nuevas redes; que sólo se ofrecerán espacio de direcciones IPv6. La inevitabilidad de IPv6 ha llegado a primer plano.

IPv6 ofrece una serie de características avanzadas y el aumento masivo de la capacidad de espacio de direcciones es indiscutiblemente único para IPv6 y representa el objetivo de coronación para organizaciones hambrientas de direcciones IP. Por desgracia, este aumento de espacio de direcciones se produce a costa de los diferentes formatos de dirección, que afectan no sólo el enrutamiento de capa de red, sino también las aplicaciones que muestran las direcciones IP.

Las organizaciones con redes IPv4 necesitan implementar redes IPv6, enfrentan desafíos en la identificación de impactos existentes, la planificación de la transición y la ejecución de la migración a IPv6. Dada la dependencia de la organización común de comunicaciones externas para

atraer a nuevos clientes a través de Internet, apoyando enlaces socios dedicados, empleados en el hogar y el acceso a Internet para el correo electrónico, navegación web, etc., un plan general debe ser compilado para documentar el entorno actual, de los usuarios y las medidas finales previstas para el despliegue de IPv6.

Cuando discutimos el despliegue de IPv6, nos referimos a un estado inicial de una red IPv4 a la que se agregan o se superponen en el tiempo nodos y redes IPv6, lo que resulta en una sola red IPv6, o más probablemente, una red predominantemente con IPv6 continuo apoyado de IPv4. Se espera que la mayoría de las organizaciones caerán en este último escenario y utilizarán tanto IPv4 como IPv6 desde hace bastante tiempo.

Por lo tanto, el término "migración" como se usa en este trabajo de titulación puede ser considerado una sola red IPv4 a una red combinada IPv4-IPv6. En última instancia, la simplificación de la gestión impulsará el desmantelamiento de IPv4 para el ahorro y la eficiencia de costes, pero esto no puede ocurrir por un tiempo hasta que la familiaridad y la comodidad con IPv6 crecen.

El presente trabajo de titulación presenta una visión general de las principales tecnologías de migración que se pueden utilizar para la transición de una red IPv4 a una red IPv4-IPv6, y sugiere varios escenarios para implementar esa transición.

2.2. Generalidades de las Tecnologías de Migración de IP.

Una gran variedad de tecnologías están disponibles para facilitar la migración a IPv6. Ávila M., Ó. (2011) estas tecnologías serán discutidas de acuerdo a las siguientes categorías básicas:

- Doble pila (Dual-Stack): apoyo en los dispositivos de redes IPv4 e IPv6.
- Túneles (Tunneling): encapsulación de un paquete IPv6 dentro de un paquete IPv4 para la transmisión sobre una red IPv4.
- Traducción (Traslation): dirección o traducción de puertos de direcciones, a través de un dispositivo de puerta de enlace o código de traducción de código TCP/IP del host o router,

Este trabajo se refiere a la migración de aplicaciones y proporcionar algunos escenarios de ejemplo de migración y las consideraciones de impacto correspondientes. La implementación de la estrategia de migración seleccionada requerirá una coordinación efectiva de las siguientes acciones:

- Redes IPv4 e IPv6, asignaciones de subred, existentes y previstas.
- Las estrategias de asignación de direcciones de IPv4 e IPv6: estática, autoconfiguración, DHCP para redes IPv4 e IPv6.
- Configuración de registro de recursos DNS correspondiente a la resolución de nombres apropiados de direcciones para construcción de túneles o traducción.
- Compatibilidad entre cliente/host y router apoyado de las tecnologías de migración seleccionadas, incluida la traducción y/o construcción de túneles y consideraciones sobre la aplicación.

- Despliegue de puerta de enlace de la traducción, según sea apropiado.

2.3. Enfoque Doble pila (Dual-Stack).

El enfoque de doble pila consiste en la implementación de IPv4 e IPv6 pilas de protocolos en los dispositivos que requieren acceso a ambas tecnologías de capa de red, incluyendo routers, otros dispositivos de la infraestructura y los dispositivos de usuario final. Estos dispositivos se pueden configurar con IPv4 e IPv6 Direcciones, y pueden obtener estas direcciones a través de métodos definidos para los respectivos protocolos como habilitado por los administradores. Por ejemplo, una dirección IPv4 puede ser obtenida a través de DHCPv4, mientras que la dirección IPv6 puede ser configurado.

Las implementaciones pueden variar con doble pila enfoques con respecto a la extensión de la pila que se comparte en comparación con lo que es única para cada versión IP. Idealmente, sólo la capa de red se realizaría, usando una capa de aplicación común, el transporte y el enlace de datos. Otros enfoques pueden abarcar toda la pila hacia abajo a la capa física, lo que requiere una interfaz de red separada para IPv6 vs. IPv4.

Este enfoque, mientras que al contrario de los beneficios de un modelo de protocolo en capas, puede ser intencional e incluso deseable, especialmente en el caso de servidores de red con múltiples aplicaciones o servicios, algunos de los cuales soportan solamente una versión o la otra.

2.3.1. Despliegue de doble pila.

El despliegue de los dispositivos de doble pila comparte una interfaz de red común que implica el funcionamiento de redes IPv4 e IPv6 en el mismo enlace físico. Después de todo, Ethernet y otras tecnologías de capa 2 soportan cargas útiles de IPv4 o IPv6. Los dispositivos Dual-Stack requieren routers que soporten dichos enlaces.

Se espera que este enfoque de superposición vaya ser muy común durante la transición (véase la figura 2.1). Este diagrama se puede extender más allá de una red física LAN a una red multi-hop donde los routers soportan redes IPv4 e IPv6 y rutas de paquetes IPv4 entre hosts IPv4 nativos y los paquetes IPv6 entre hosts compatibles con IPv6.

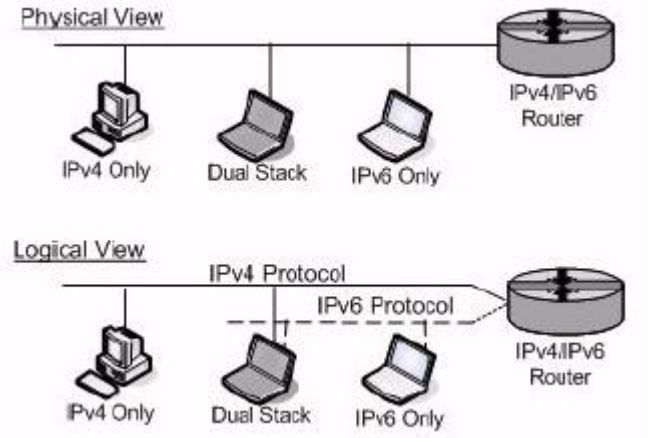

Figura 2. 1: Perspectivas de redes Dual-Stack.
Fuente:

Landy R., D. (2013) sostiene que los routers serían generalmente entre los primeros elementos de propiedad intelectual para ser actualizados para apoyar ambos protocolos.

Al actualizar un router para soportar IPv6, los puertos del switch a la que sus interfaces están conectados se puede configurar como una "VLAN IPv6". Entonces, otro IPv6 o dispositivos de doble pila, podrían configurarse como miembros de la una VLAN o múltiples VLAN podrían ser configurados del mismo modo. Un ejemplo de este despliegue se muestra en la figura 2.2.

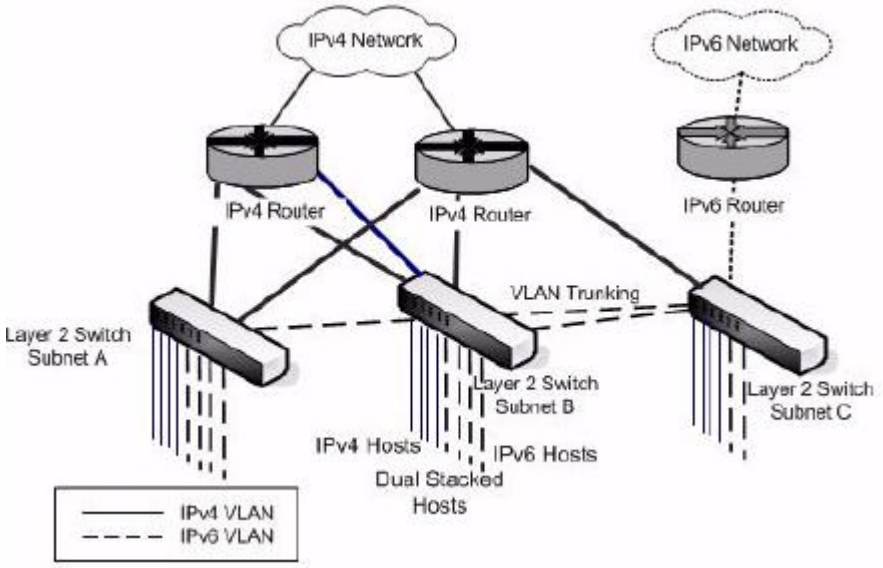

Figura 2. 2: Red VLAN doble apilado
Fuente:

2.3.2. Consideraciones DNS

Los DNS desempeñan un papel crucial en el funcionamiento correcto de cada tecnología de transición, ya que proporciona el vínculo vital entre la nomenclatura del usuario final y la dirección destino de IP. Los usuarios finales al intentar acceder a un host (anfitrión) pasa a ser un dispositivo de doble. Si la aplicación se puede configurar por los administradores para soportar tanto una dirección IPv4 (un tipo de registro de recursos) y consultar la dirección IPv6 (tipo de registro de recursos AAAA) puede recibir direcciones IPv4 e IPv6 del destino.

Si la aplicación no soporta de forma nativa una búsqueda de doble consulta, el "golpe en la pila" y "choque en la API" de técnicas de traducción compatibles con esta función. En cualquier caso, el nombre de ambas consultas del tipo de registro A y AAAA se pueden igualar, proporcionando la resolución del nombre de host a una o ambas direcciones IP de las versiones respectivas:

```
IPv4: dual-stack-host.example.com.  86400   IN  A       10.200.0.16
IPv6: dual-stack-host.example.com.  86400   IN  AAAA    2001:db8:200::A
```

La resolución del nombre de la dirección IP-to-host también puede ser configurada en DNS en el dominio .arpa apropiado:

```
IPv4: 16.0.200.10.in-addr.arpa. 86400 IN PTR dual-stack-host.example.com.
IPv6: A.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.8.b.d.0.1.0.0.2.ip6.arpa.
      6400 IN PTR dual-stack-host.example.com.
```

El nodo de pila dual, en sí mismo debe ser capaz de soportar la recepción de registros A y AAAA durante su propio procesamiento de la resolución de DNS y comunicarse con el destino previsto utilizando la dirección y el protocolo correspondiente al registro devuelto. La configuración de resolución puede permitir definición del protocolo de red preferida cuando ambos registros, una A y otra AAAA se devuelven desde la consulta, por no mencionar el protocolo utilizado al emitir la consulta DNS así mismos.

Además, como veremos en la siguiente sección sobre los enfoques de túneles, algunas tecnologías de túneles automáticos utilizan formatos de

dirección IPv6 específicos, por lo que las direcciones correspondientes a uno o más formatos de dirección de túnel, también pueden ser devueltos y se utilizan en la medida en que el host (anfitrión) resuelva el soporte de la tecnología de túnel correspondiente.

2.3.3. Consideraciones DHCP

El mecanismo para el uso de DHCP bajo una aplicación de doble pila es simplemente que cada pila utiliza su versión de DHCP. Es decir, con el fin de obtener una dirección IPv4, se utiliza DHCP, y para obtener una dirección o prefijo IPv6, utilizamos DHCPv6. Sin embargo, la información de configuración adicional es proporcionada por ambas formas de DHCP, como qué DNS o servidor NTP está en su uso.

La información obtenida puede conducir a un comportamiento incorrecto en el cliente en función de cómo se combina la información de ambos servidores juntos. Esta sigue siendo un área permanente de preocupación, como se documenta en el RFC 4477, pero el estándar actual es utilizar un servidor DHCP para IPv4 y un servidor DHCPv6 para IPv6, posiblemente implementado en un servidor físico común.

2.4. Enfoques de tunelización (Tunneling).

Una variedad de tecnologías de túneles ha sido desarrollada para apoyar IPv4 sobre IPv6, así como IPv6 sobre IPv4. Estas tecnologías generalmente se clasifican como: configurado o automático. Los túneles

configurados están predefinidos, mientras que los túneles automáticos se tratan de un túnel abierto de forma dinámica, a petición y "sobre la marcha". Posteriormente, hablaremos de estos dos tipos de túneles después de revisar algunos conceptos básicos de túneles.

En general, la tunelización de paquetes IPv6 a través de una red IPv4 implica prefijar cada paquete IPv6 con un encabezado IPv4 (véase la figura 2.3). Esto permite que el paquete tunelizado ser encaminado a través de una infraestructura de enrutamiento IPv4. El nodo de entrada del túnel, un router o un host, realiza la encapsulación. La dirección IPv4 de origen en el encabezado IPv4 se rellena con la dirección IPv4 de ese nodo y la dirección de destino es la del punto final del túnel.

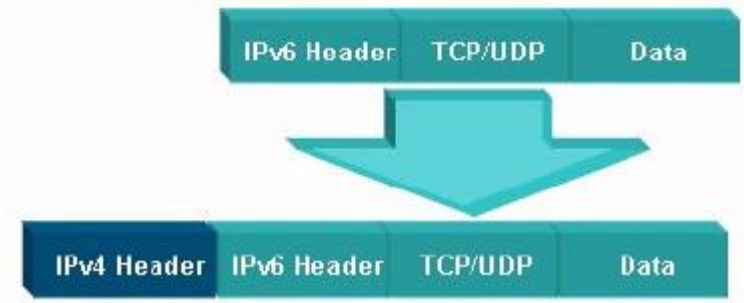

Figura 2. 3: IPv6 sobre IPv4 túnel
Fuente:

El campo de protocolo de la cabecera IPv4 se establece en 41 (decimal) que indica un paquete IPv6 encapsulado. El nodo de salida o punto final del túnel realiza el desencapsulamiento de la cabecera IPv4 y encaminar el paquete según sea apropiado para el destino final a través de IPv6.

2.5. Tipos de túneles

Mientras que el proceso de tunelización es el mismo para todos los tipos de túneles, hay una variedad de escenarios basados en puntos terminales del túnel definido. Probablemente, la configuración más común es un túnel de router a router se muestra en la figura 2.4, que es el enfoque típico para los túneles configurados.

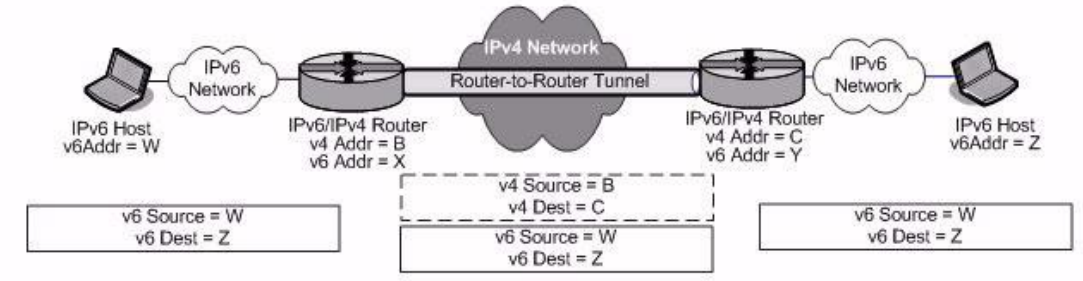

Figura 2. 4: Túnel de router a router.
Fuente:

De la figura 2.4, el originario host de IPv6 de la izquierda tiene una dirección IPv6 de W (por simplicidad y brevedad). Un paquete con destino para el host en el otro extremo del diagrama con dirección IPv6 de Z se envía a un router al servicio de la subred. Este router (con dirección IPv4 de B y dirección IPv6 de X) recibe el paquete IPv6. Configurado los paquetes de túnel con destino a la red en la que el host Z, el router encapsula el paquete IPv6 con un encabezado IPv4. El router utiliza su dirección IPv4 (B) como la dirección IPv4 de origen y la del extremo del túnel del router (con una dirección IPv4 de C) como dirección de destino, representada por debajo de la red IPv4 en el centro de la figura 2.4. El router del extremo derecho encapsula el paquete, quitando la cabecera IPv4 y encamina el paquete original de IPv6 a su destino (Z).

Otro escenario de tunelización es el Host a router, que dispone de un host IPv6/IPv4 capaz de soportar protocolos IPv4 e IPv6, la tunelización de un paquete a un router, que a su vez encapsula el paquete y las rutas de forma nativa a través de IPv6. Este flujo de paquetes y direcciones de cabecera se muestran en la figura 2.5. El mecanismo de túnel es el mismo que en el caso router a router, pero los puntos terminales del túnel son diferentes.

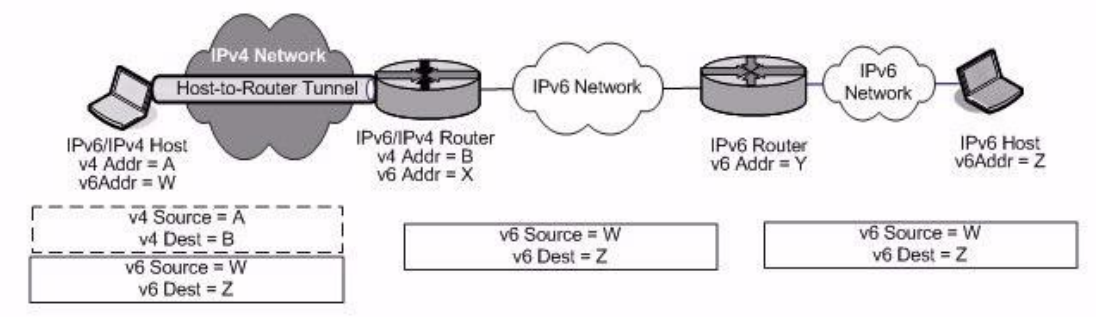

Figura 2. 5: Configuración del túnel Host-a-router.
Fuente:

La configuración Host a router mostrada en la figura 2.6, también es muy similar a un túnel de router a router. Al inicio, el host IPv6 de la izquierda del diagrama envía paquetes IPv6 a su router local, que encamina a un enrutador más cercano a su destino. El router está configurado para el túnel de paquetes IPv6 sobre el host IPv4, como se muestra en la figura 2.6.

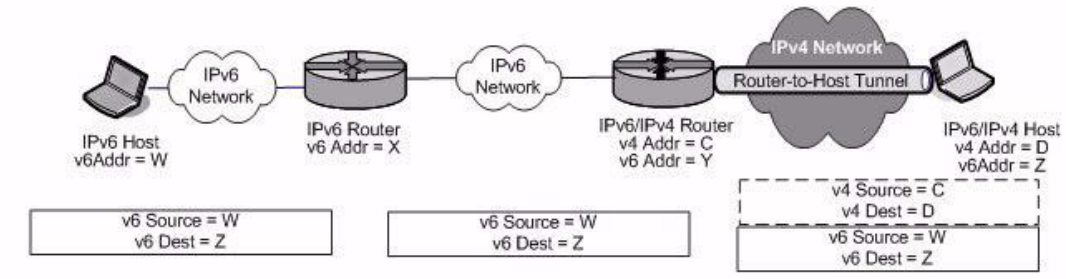

Figura 2. 6: Configuración del túnel router a host.
Fuente:

La configuración final de tunelización es una que se extiende de extremo a extremo (end-to-end), desde el host-a-host. Si la infraestructura de enrutamiento aún no ha sido actualizada para soportar IPv6, esta configuración de túnel permite acoger dos IPv6/IPv4 a comunicarse a través de un túnel a lo largo de una red IPv4 como se muestra en la figura 2.7. En este ejemplo, la comunicación es IPv4 de end-to-end.

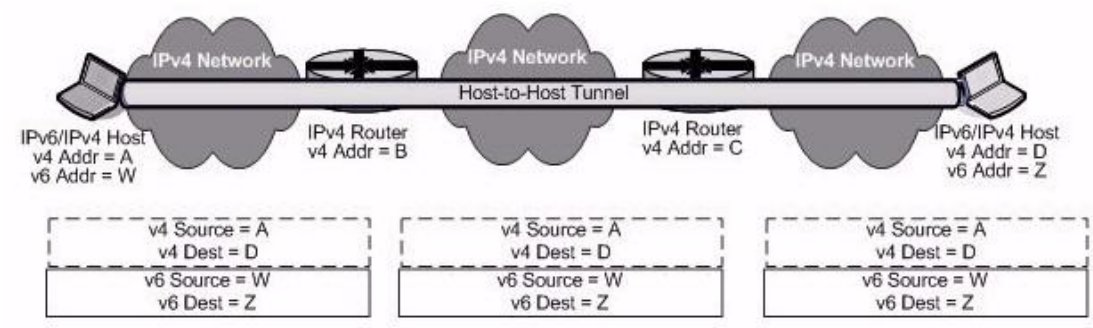

Figura 2. 7: Configuración del túnel host a host.
Fuente:

2.6. Tunelización automática de paquetes IPv6 sobre redes IPv4

Como se mencionó anteriormente, los túneles o bien se configuran o son automáticos. Túneles configurados están predefinidos por los administradores antes de comunicaciones, tanto como las rutas estáticas se preconfiguran. En los escenarios descritos en las figuras 2.4 a 2.7, se requiere la configuración de los respectivos puntos terminales del túnel para configurar el dispositivo para paquetes IPv6, es decir, sobre la base de destino, junto con otros parámetros de configuración de túnel que pueden ser requeridos por la ejecución del túnel, tales como tamaño máximo de paquete (a veces llamado MTU o unidad de transmisión máxima).

Un túnel automático no requiere configuración previa. Los túneles se crean basándose en la información contenida en el paquete IPv6, como la dirección IP de origen o destino. Según Coellar, J & Cedeño, J (2012) las técnicas de túneles automáticos son las siguientes:

- 6to4: túnel automático de router a router basado en un prefijo de dirección global en particular y dirección IPv4 incrustada.
- ISATAP: túnel automática de host a router, router a host o túnel de host a host basado en un formato particular de direcciones IPv6 con inclusión de una dirección IPv4 incrustada.
- 6over4: túnel automático de host a host utilizando IPv4 multidifusión
- Túnel Brokers: túnel de configuración automática mediante un servidor que actúa como intermediario en la asignación de recursos del túnel Gateway.
- Teredo: túnel automático a través de cortafuegos NAT en redes IPv4.
- Mecanismo de Transición Dual-Stack: permite tunelización automática de paquetes IPv4 a través de redes IPv6

2.6.1. 6to4.

6to4 es una técnica de IPv6 sobre IPv4 túnel que se basa en un formato de dirección IPv6 particular para identificar los paquetes 6to4 y túnel en consecuencia. El formato de la dirección consiste en un prefijo 6a4, 2002::/16, seguido de una dirección IPv4 globalmente única para el sitio de destino previsto. Esta concatenación forma un prefijo /48 visto en la figura 2.8.

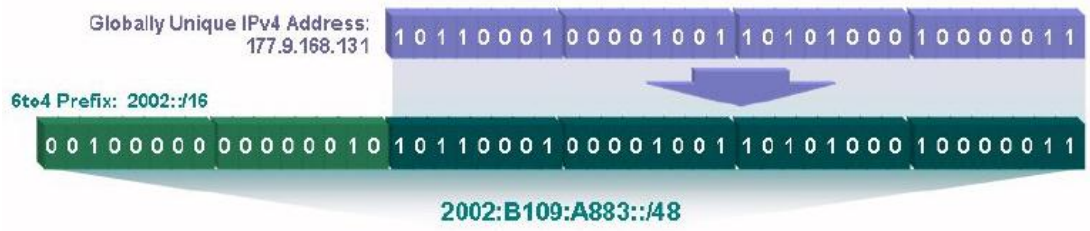

Figura 2. 8: 6to4 Dirección Prefijo Derivación
Fuente:

La única dirección IPv4 representa la dirección IPv4 de la terminación del router 6to4 del túnel 6to4. El prefijo 6to4 de 48 bits sirve como el prefijo de enrutamiento global y un ID de subred se puede añadir a los próximos 16 bits, seguido de un ID de interfaz para definir completamente la dirección IPv6. Los routers con soporte de túneles 6to4 (routers 6a4) deben emplearse, y hosts de IPv6 que se van a enviar/recibir a través de túneles 6to4 deben configurarse con una dirección 6to4 y se consideran hosts de 6to4.

Consideremos un ejemplo donde dos sitios que contienen hosts 6to4 quieren comunicarse y están interconectados a través de routers 6a4 conectados a una red IPv4 común; esto podría ser Internet o una red IPv4 interna. Para la figura 2.9, las direcciones IPv4 de las interfaces de los routers IPv4 son: 177.9.168.130 y 177.9.168.131, respectivamente. La transformación de estas direcciones IPv4 en direcciones 6to4, llegamos a 2002:B109:A882::/48 y 2002:B109:A883::/48, respectivamente.

Estos prefijos ahora identifican cada sitio en términos de accesibilidad 6to4. El host 6to4 de la izquierda es la subred ID=1 y, por simplicidad, tiene

interfaz ID=1. De este modo, la dirección 6to4 de este alojamiento es 2002:B109:A882:1::1. Esta dirección se configura en el dispositivo de forma manual o automática (configuración automática basada en ID de interfaz de los dispositivos y el anuncio del router del 2002:B109:A882: 1/64 prefijo). Del mismo modo, el host de 6a4 en el otro sitio reside en la subred ID=2 y la interfaz de ID=1, resultando en una dirección 6a4 de 2002:B109:A883:2::1.

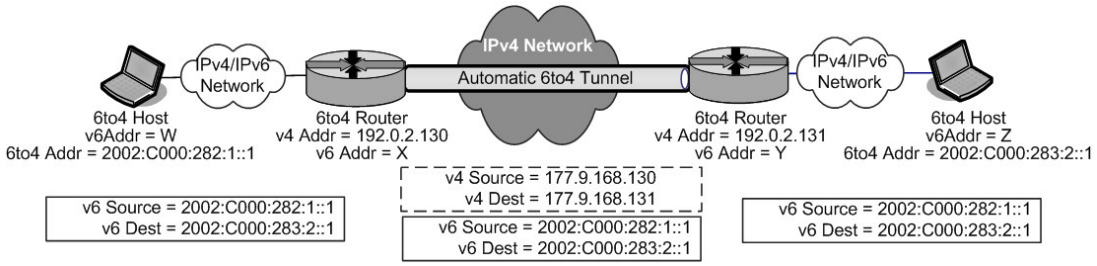

Figura 2. 9: 6to4 túnel Ejemplo.
Fuente:

Los registros de recursos AAAA y PTR correspondientes a estas direcciones 6to4 también deben añadirse a DNS dentro de los dominios correspondientes. Cuando nuestro host de la izquierda quiere comunicarse con otro host, una búsqueda de DNS volvería su dirección 6to4 y potencialmente a otras direcciones IPv6. El Host enviado utilizará su dirección 6to4 como la fuente y la dirección 6to4 como el destino.

Cuando este paquete es recibido por el router 6to4, el router encapsula el paquete utilizando un encabezado IPv4 (fuente) y direcciones IP del otro router 6to4 (destino). El router 6to4 recibe el paquete lo desencapsula y transmite el paquete en la red 2002:B109:A883:2/64 del host 6to4 destino.

Durante el proceso de migración de IPv4 a IPv6, 6to4 puede proporcionar un mecanismo eficiente para hosts IPv6 para comunicarse a través de redes IPv4. Como las redes son gradualmente migrados a IPv6, los routers de reenvío 6to4 (que son los routers IPv6 que también apoyan 6a4) pueden utilizarse para retransmitir paquetes de hosts en redes "puros" IPv6 a hosts IPv6 a través de redes IPv4.

El mismo esquema de direccionamiento y de túneles es aplicable, sin embargo, el router 6to4 requiere tener conocimiento sobre los enrutadores (routers) de reenvío 6to4 para asignar direcciones IPv6 unicast global (nativo) a una dirección 6to4 para el túnel. Hay tres formas de este conocimiento que son:

- Configurar rutas a destinos de redes IPv6 nativas con el enrutador de reenvío 6to4 como el siguiente salto (véase la figura 2.10).
- Utilizar los protocolos de enrutamiento normales, lo que permite el enrutador de reenvío 6to4 para anunciar rutas a redes IPv6. Este escenario se aplicaría cuando anuncian migración de rutas a redes IPv6 o internas. Si la red es puro IPv6 (ver figura 2.10) es una Internet IPv6, la siguiente opción de ruta por defecto es probable que una mejor alternativa.
- Configurar una ruta predeterminada al router de reenvío 6to4 para redes IPv6. Este escenario puede aplicarse cuando una conexión a Internet IPv6 es accesible sólo a través de una red IPv4 interna a la organización y pocas o no existen redes IPv6 puras dentro de la

organización. Una variante de este escenario es definir la ruta predeterminada en el próximo salto como la dirección de difusión por proximidad del router de reenvío 6to4 para redes IPv6. Esta variación soporta el escenario con múltiples routers de reenvío 6a4. El protocolo RFC 3068 define una dirección anycast para routers de reenvío 6to4: 2002:C058:6301:: /48. Esta dirección corresponde a la dirección IPv4 192.88.99.1.

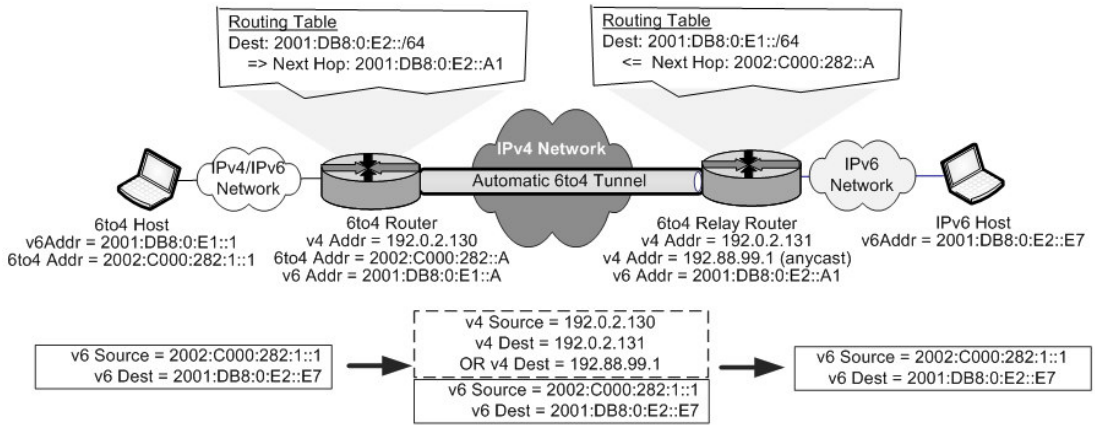

Figura 2. 10: 6to4 Host comunicación con un host IPv6 nativo
Fuente:

De la figura 2.10, vemos un host 6to4 en una transición de la red IPv4/IPv6 de la izquierda con una dirección IPv6 nativa y una dirección 6to4. Este host dispone la comunicarse con un host IPv6 nativo con la dirección IP 2001:DB8:0:E2::E7 en el lado derecho de la figura 2.10. Esta dirección IPv6 se devuelve dentro de una respuesta de registro de recursos AAAA desde un servidor DNS cuando se les pregunta por la dirección IP del host de destino. Por lo tanto nuestro host 6to4 a la izquierda, formula un paquete IPv6 utilizando su dirección (ver figura 2.10) como la dirección IP de origen

basado en políticas de selección de direcciones de host y la dirección IPv6 del host de destino como el destino IPv6 o 6to4.

Este paquete a continuación llega al router 6to4. El router tendría que tener un elemento de la tabla de enrutamiento a fin para dirigirse hacia la red destino 2001:DB8:0::E2/64, apuntando a la dirección 6to4 del router de reenvío 6to4 (véase la figura 2.10).

2.6.2. Protocolo de Direccionamiento de Túnel Automático Intra-Sitio (ISATAP).

ISATAP es un protocolo experimental que proporciona un túnel automático IPv6 sobre IPv4 para host a router, de router a host y configuraciones de host a host. Las direcciones ISATAP de IPv6 se forman utilizando una dirección IPv4 para definir su ID de interfaz. El ID de interfaz se compone de ::5EFE:a.b.c.d, donde a.b.c.d es la notación con punto decimal de IPv4.

Así que un ID de interfaz ISATAP correspondiente a 177.9.168.131 se denota como ::5EFE:177.9.168.131. La notación IPv4 proporciona una indicación clara que la dirección ISATAP contiene una dirección IPv4 sin tener que traducir la dirección IPv4 en hexadecimal. Esta interfaz ID de ISATAP se puede utilizar como una Identificación normal de interfaz en añadir prefijos de red admitidos para definir direcciones IPv6. Por ejemplo, el

vínculo local direcciones IPv6 mediante la interfaz ISATAP anterior es FE80::5EFE:177.9.168.131.

Los Hosts de soporte ISATAP tienen la obligación de mantener una lista de routers potenciales *(Potential Router Lista, PRL)* que contiene la dirección IPv4 y asociado al cronómetro de duración de dirección para cada router anunciado de una interfaz ISATAP. Los Hosts ISATAP solicitan información de soporte ISATAP de routers locales a través de solicitud de enrutador sobre IPv4.

El destino de solicitud debe ser identificado por el Host de la configuración manual antes de buscar el router en el DNS con un nombre de host "ISATAP" en el dominio de la resolución, o el uso de una opción de DHCP que indica direcciones IPv4 del router ISATAP. Un host ISATAP sería encapsular el paquete de datos IPv6 con un encabezado IPv4 como se muestra en la figura 2.11, utilizando la dirección IPv4 correspondiente al router elegido de la PRL.

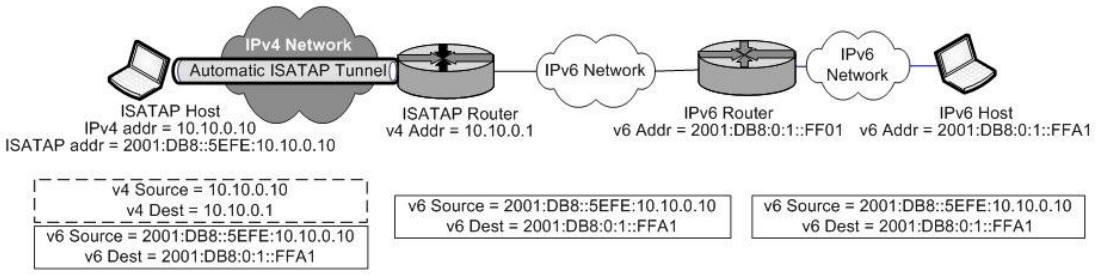

Figura 2. 11: ISATAP Host-to-Router Ejemplo
Fuente:

Los Hosts ISATAP pueden auto-configurar sus identificadores de interfaz ISATAP utilizando configuraciones de direcciones IPv4 si la dirección IPv4 se define estática o se obtiene a través de DHCP. El ID de interfaz ISATAP se puede añadir a una ID cuyo prefijo es de 64 bits de red global y de subred proporcionada por los routers ISATAP solicitados anteriormente.

De la figura 2.11, el Host de la izquierda del diagrama identifica la dirección IP del host de destino, en este caso, una dirección IPv6, utilizando un DNS. Un paquete IPv6 estaría formado por el Host utilizando su dirección IPv6 ISATAP como su dirección de origen y el destino de dirección de host IPv6 como dirección de destino. Este paquete está encapsulado en una cabecera IPv4, formando de esta manera un túnel automático.

La dirección de origen se establece en la dirección IPv4 del host ISATAP, la dirección de destino se establece en la dirección IPv4 del router ISATAP y el campo de protocolo se establece en decimal 41, lo que indica un paquete IPv6 encapsulado.

El router ISATAP no tiene que ser en la misma red física que el host y el túnel puede abarcar una red IPv4 genérica (cero o más saltos) entre el host y el router ISATAP. El router ISATAP elimina el encabezado IPv4 y encamina el paquete IPv6 restante al host de destino mediante el enrutamiento normal de IPv6.

El host de destino puede responder al host de origen utilizando la dirección ISATAP del host de origen. Desde la dirección de ISATAP contiene un prefijo de red/subred con ID único global, el paquete se encamina destino al enrutador ISATAP de servicio. Al procesar el ID de interfaz, el router ISATAP puede extraer la dirección IPv4 del host de destino y encapsular el paquete IPv6 con un encabezado IPv4 para el host original.

De manera similar, el Host IPv6 nativo a la derecha de la figura 2.11 podría haber iniciado la comunicación con el host ISATAP. Yendo de derecha a izquierda, el router ISATAP en este caso sería crear el túnel ISATAP para el Host.

Al igual que el túnel host a host (véase figura 2.7), los túneles ISATAP host a host pueden ser iniciadas por los hosts ISATAP que residen en una red IPv4, donde un prefijo de red de enlace local (misma subred) o global puede tener el prefijo a cada host ISATAP de interfaz ID.

2.6.3. 6over4

6over4 es una técnica de túnel automático que aprovecha IPv4 multicast. Se requiere IPv4 multicast y se considera una capa de enlace virtual o Ethernet virtual por el esquema 6over4. Debido a la perspectiva de la capa de enlace virtual, las direcciones IPv6 se forman utilizando un ámbito local de vínculo. Las Dirección IPv4 de un Host comprende la parte de ID de interfaz 6over4 de su dirección IPv6 tal como se muestra en la figura 2.12.

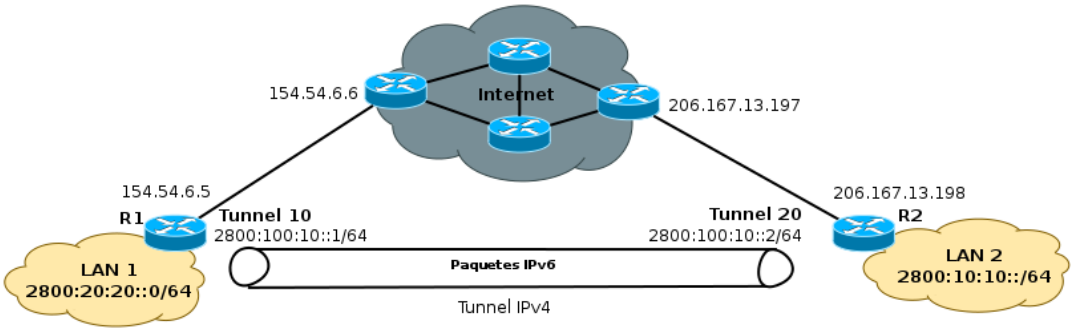

Figura 2. 12: Esquema del túnel 6over4.
Fuente: Coellar, J. & Cedeño, J. (2012).

Los túneles 6over4 pueden ser de la forma: host a host, host a router y de router a host, donde respectivos hosts y routers deben configurarse para soportar 6over4. Los paquetes IPv6 son un túnel en las cabeceras IPv4 utilizando direcciones multicast IPv4 correspondientes.

Todos los miembros del grupo de multidifusión reciben los paquetes de túnel, por tanto, la analogía de Ethernet virtual, y el destinatario elimina el encabezado IPv4 y procesa el paquete IPv6. Mientras al menos un enrutador IPv6 también ejecuta 6over4 es accesible a través del mecanismo de multicast IPv4, el router puede servir como punto final del túnel y encaminar el paquete a través de IPv6. 6over4 soporta IPv6 multicast y unicast, por lo que los Hosts pueden realizar routers IPv6 y descubrimiento de vecinos para localizar routers IPv6.

2.6.4. Túnel Brokers.

Los túneles Brokers, proporcionan otra técnica para tunelización automática a través de redes IPv4. El túnel Broker maneja peticiones de

túnel de los clientes de doble pila y servidores túnel Broker, que se conectan a la red IPv6 prevista. Los clientes de doble pila (Dual-Stack) que intentan acceder a una red IPv6 opcionalmente se pueden dirigir a través de la resolución de nombres DNS a un servidor web de túnel Broker para la entrada de credenciales de autenticación para autorizar el uso del servicio de Broker.

El túnel Broker, también puede administrar los certificados de servicios de autorización. El cliente también proporciona la dirección IPv4 al final del túnel, el número de direcciones IPv6 solicitados y si el cliente es un anfitrión o un router. Una vez autorizado, el túnel Broker lleva a cabo las siguientes tareas para la creación del túnel:

- Asigna y configura un servidor de túnel e informa al servidor de túnel seleccionado del nuevo cliente.
- Asigna una dirección IPv6 o un prefijo para el cliente basado en el número solicitado de direcciones y tipo de cliente (router o host)
- Registra el cliente FQDN en DNS
- Informa al cliente de su servidor de túnel asignado y el túnel asociado y parámetros IPv6 incluyendo dirección / prefijo y el nombre DNS.

Desde la perspectiva del usuario final, la creación de la conexión de túnel a la red IPv6 es similar a la creación de un estándar de conexión VPN. La figura 2.13 ilustra la interacción túnel Broker – cliente en la parte superior

de la figura, y el túnel resultante entre el cliente y el servidor de túnel asignado a continuación.

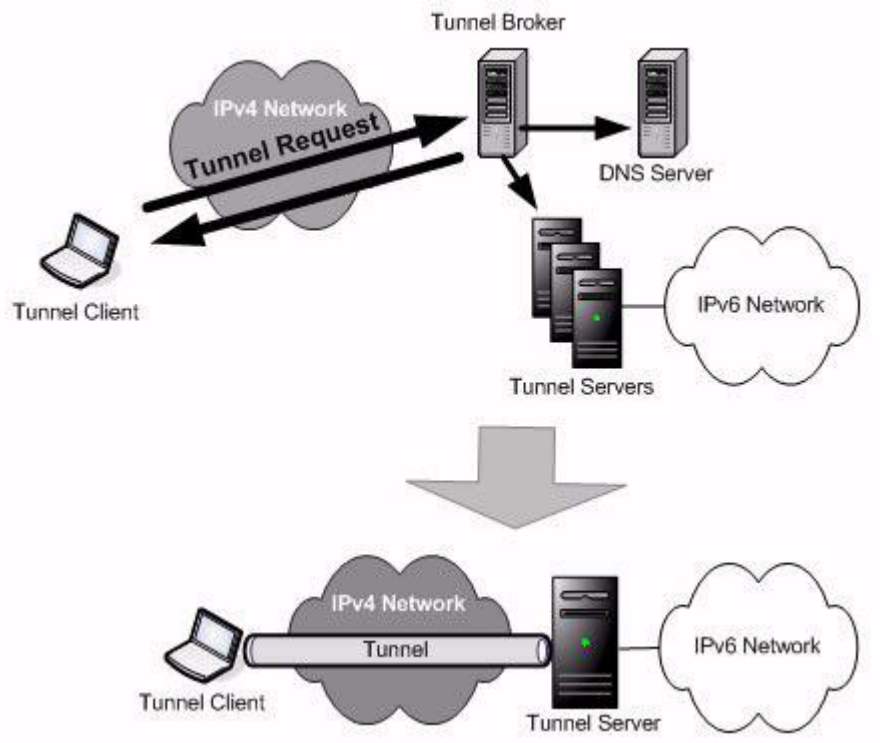

Figura 2. 13: Túnel Broker Interacción
Fuente:

2.6.5. Túnel Teredo.

Túnel a través de cortafuegos que realizan la traducción de direcciones de red (NAT) que puede ser un reto, si no imposible. Esto es así, porque muchos dispositivos NAT/firewall no permiten que el recorrido de los paquetes IPv4 con el campo de protocolo establecido en 41, que es el escenario de un túnel de paquetes IPv6 como se describió anteriormente.

El túnel Teredo, permite NAT transversales de paquetes IPv6 de túneles a través de UDP sobre IPv4 para túneles host a host automáticos. El túnel Teredo incorpora la cabecera UDP adicionales para facilitar

NAT/firewall transversal. La cabecera UDP adicionales "ocultan" el túnel para permitir su recorrido a través de dispositivos NAT/firewall, la mayoría de los cuales apoyan traducción de puertos UDP.

EL túnel Teredo se define en el protocolo RFC 4380 para proporcionar "acceso IPv6 de última instancia", debido a su cabecera, y se utilizará cada vez menos a medida que se despliegan 6to4 habilitadas o routers IPv6 firewall. Según Coellar, J. & Cedeño J. (2012) Teredo requiere los siguientes elementos (véase la figura 2.14):

- Cliente Teredo
- Servidor Teredo
- Relay Teredo

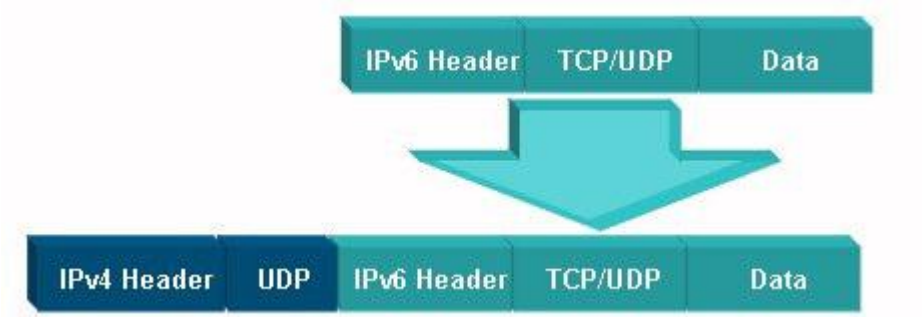

Figura 2. 14: Teredo Túneles añadir UDP luego IPv4 Cabeceras
Fuente:

El proceso de construcción de túneles Teredo comienza con un cliente Teredo realiza un procedimiento de calificación para descubrir un Relay Teredo más cercano al destino IPv6 host destinado e identificado al tipo de intervención firewall NAT que está en su lugar. Los Hosts Teredo deben ser pre-configurados con el servidor Teredo de dirección IPv4.

Determinar el Relay Teredo cercano implica el envío de un ping (solicitud de eco ICMPv6) al host de destino. El ping se encapsula con una cabecera UDP e IPv4 y se envía al servidor Teredo, que desencapsula y envía el paquete ICMPv6 nativo al destino. La respuesta del host de destino serán enviados a través de IPv6 nativo al Relay Teredo más cercana, en virtud del enrutamiento, luego de vuelta al host de origen.

De esta manera, el cliente determina los Relay Teredo apropiadas de dirección y de puerto IPv4. Las figuras 2.15 y 2.16 muestran los casos de que un cliente Teredo se pueda comunicar a un host IPv6 nativo.

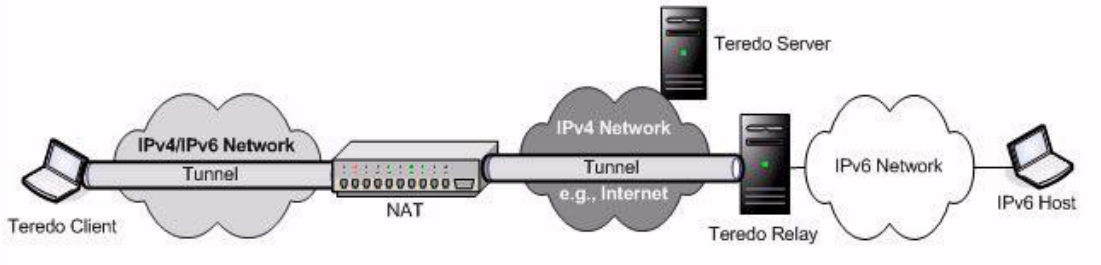

Figura 2. 15: Teredo de cliente a IPv6 anfitrión Conexión.
Fuente:

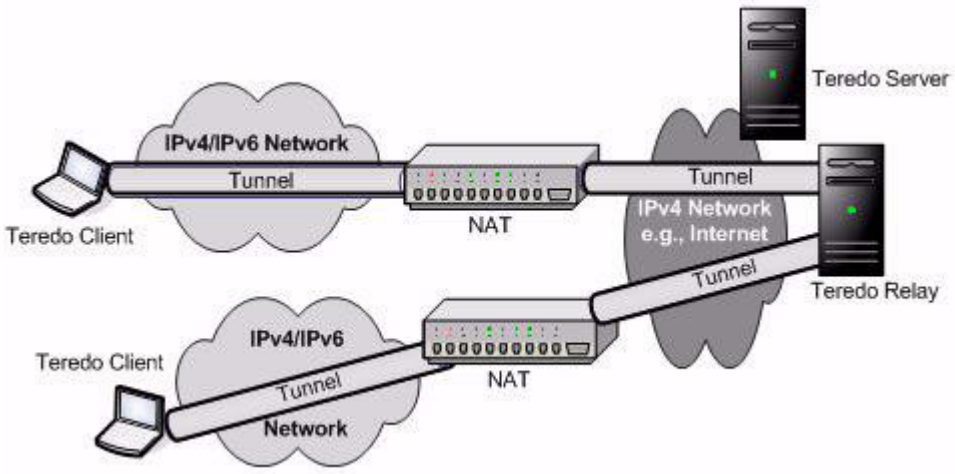

Figura 2. 16: Dos clientes Teredo Comunicar a través de Internet IPv4.
Fuente:

El tipo de intervención NAT puede conducir a la necesidad de realizar un paso adicional para inicializar las asignaciones de la tabla NAT. La dirección Teredo IPv6 tiene el formato que se muestra en la figura 2.17.

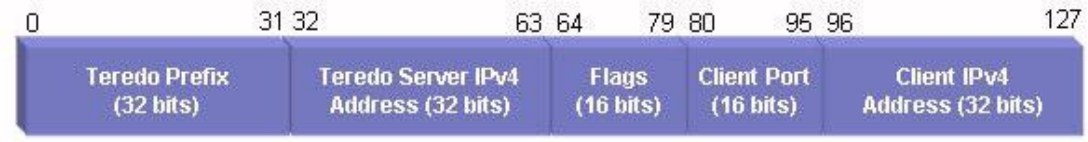

Figura 2. 17: Teredo IPv6 Dirección Formato
Fuente:

El prefijo Teredo es un pre-definido prefijo IPv6: 2001 :: / 32. La dirección IPv4 del servidor Teredo comprende los siguientes 32 bits. Banderas indican el tipo de NAT, ya sea como cono lleno (valor = 0x8000) o restringido o puerto con restricción (valor = 0x0000). Los campos puerto de cliente y cliente IPv4 dirección representan ofuscado valores de estos valores respectivos invirtiendo cada valor de bit.

CAPÍTULO 3: SIMULACIÓN Y EVALUACIÓN DE REDES MEDIANTE LOS PROTOCOLOS IPv4 E IPv6.

3.1. Configuración experimental

Para la presente sección se explica la configuración del hardware utilizado para la parte práctica o experimental de laboratorio, tal como se muestra en la tabla 3.1.

Tabla 3. 1: Configuración del hardware utilizado en la parte experimental.

Dispositivos	Cantidad
Router Cisco 2811	4
Hub NetGear 10/100	2
PCs con Windows 7	4

Elaborado por: Autor.

La configuración para la parte experimental consiste en conectar cuatro Routers Cisco 2811 mediante conexiones en serie back-to-back. Los concentradores (Hubs) NetGear serán conectados a la interfaz Ethernet en los enrutadores 1 y 4. Mientras que el enrutador 1 tiene 2 ordenadores (PCs) conectados a él a través del concentrador. Uno de los PCs es la fuente del tráfico multicast (multidifusión). Los otros dos PCs son conectados al enrutador 4 a través de otro Hub. En consecuencia, el grupo multicast tiene tres receptores.

Los routers se han configurado para ejecutarse como protocolo OSPF (*Open Shortest Path First,* el camino más corto primero) de enrutamiento unicast. La multidifusión independiente de protocolo en modo esparcido

(PIM-SM, *Protocol Independent Multicast-Sparse Mode*) se configuró en todas las interfaces en los cuatro enrutadores. Se va a utilizar el programa cliente-servidor JPerf, como generador de tráfico multidifusión. El rendimiento y la fluctuación se obtuvieron utilizando el software JPerf (interfaz gráfica en Java) basada en la herramienta de pruebas “Iperf”.

Para cada escenario, JPerf se ha ejecutado para diez períodos de 10 minutos y dos períodos de 1 hora. Para cada prueba, JPerf deberá transmitir 122 Kbytes por segundo a 1000 kbps.

Los resultados fueron obtenidos de los dos receptores: uno en la misma subred fuente (origen) y el otro en una subred diferente. Esto se hizo con el fin de comprender el impacto de enrutamiento del tráfico de multidifusión (multicast).

En la terminología JPerf, el cliente es el origen del tráfico de multidifusión y los servidores son los receptores del tráfico multidifusión. Además, se debe tener en cuenta que los receptores tienen que unirse al grupo multidifusión antes de que la fuente comience a enviar tráfico, de modo que cada uno de los receptores reciban todo el tráfico de multidifusión que fue enviado por la fuente y sin pérdida de paquetes.

Se utilizará el analizador de protocolos *“Wireshark”* para capturar paquetes en las tarjetas de interfaz de red de los dos receptores para

recopilar información adicional, para aprender el funcionamiento de los protocolos de multidifusión IGMP/MLD (IGMP para IPv4 y MLD para IPv6) y de los paquetes generados por el protocolo PIM-SM.

3.2. Escenarios experimentales.

En esta sección, la investigación realizada en el trabajo de titulación se realizó cuatro escenarios diferentes:

1. Solo redes actuales IPv4, que es el caso en la mayoría de las redes empresariales.
2. El futuro anticipado solamente para redes IPv6.
3. La etapa de transición provisional donde coexisten IPv4 e IPv6. Esta doble red se creó utilizando dos configuraciones diferentes:
    a. Dual-Stack, para el funcionamiento de protocolos IPv4 e IPv6.
    b. Túnel de encapsulación de enrutamiento genérico (*Generic Routing Encapsulation, GRE)* para él envió de paquetes PIv6IPv4.

El resto de esta sección se explicará en detalle los cuatro escenarios.

3.2.1. Escenario 1: Única red IPv4

El diagrama de red y el esquema de direccionamiento IP para la única red IPv4 se muestra en la figura 3.1.

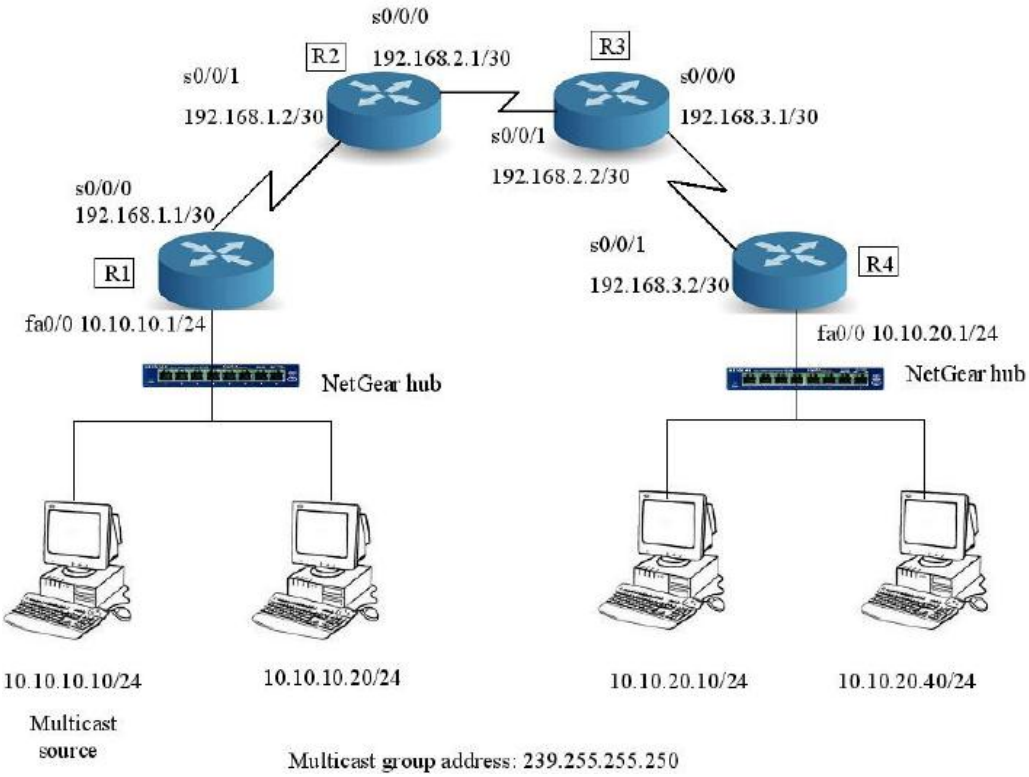

Figura 3. 1: Diagrama y esquema de direccionamiento de una red IPv4.
Elaborado por: Autor.

La fuente u origen del tráfico multidifusión es 10.10.10.10 y los otros tres PCs son los receptores. El tiempo de vida (TTL) de la fuente se establece en 10 (para contabilizar los cuatro routers que el tráfico tiene que viajar a través de algunos de los receptores de multidifusión).

3.2.2. Escenario 2: Única red IPv6

La figura 3.2 muestra la conectividad y el esquema de direcciones de la red IPv6. La fuente del tráfico multidifusión es 2001:175::10 y para los otros tres PCs son receptores. El tiempo de vida (TTL) de la fuente se establece en 10 (para contabilizar los cuatro routers que el tráfico tiene que viajar a través de algunos de los receptores de multidifusión).

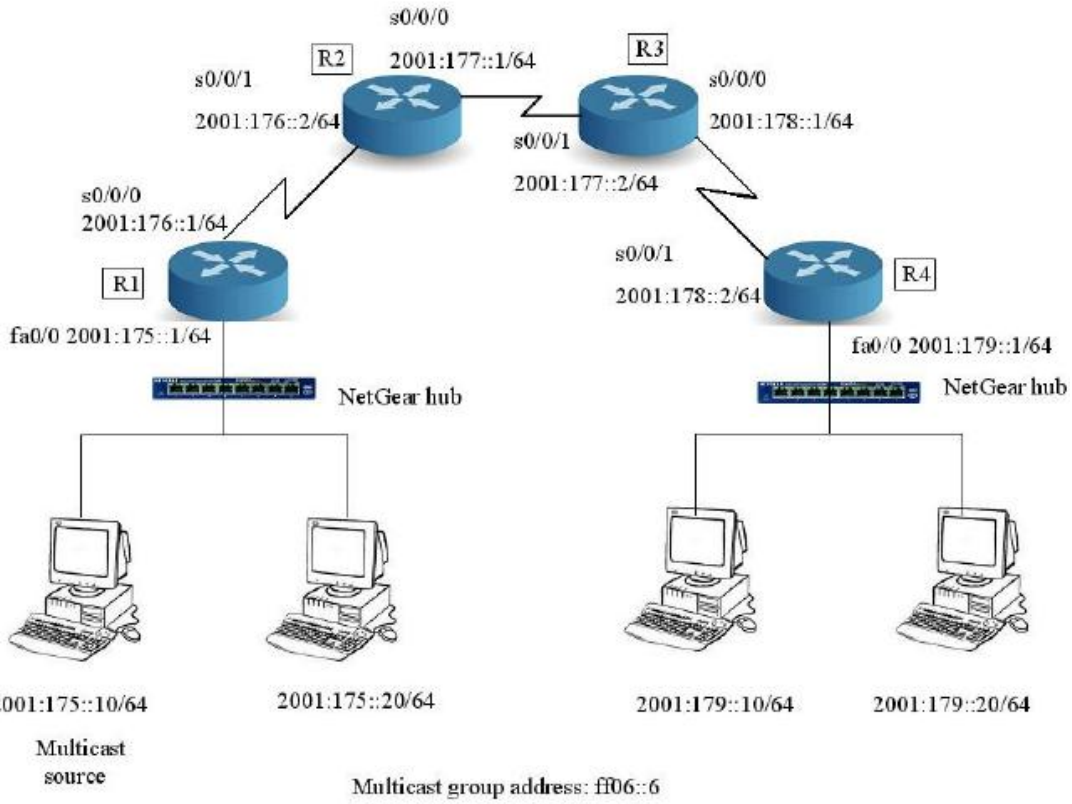

Figura 3. 2: Diagrama y esquema de direccionamiento de una red IPv6.
Elaborado por: Autor.

3.2.3. Escenario 3: Dual-Stack en Redes IPv4-IPv6

En este escenario, los hosts y routers se configuran con direcciones IPv4 e IPv6. La fuente de multidifusión genera dos secuencias de multidifusión separados, uno para IPv4 y otro para IPv6. El enrutador R4 tiene un receptor de IPv4 y un receptor IPv6.

En la figura 3.3 se muestran el diagrama y esquema de direccionamiento de IPv4/v6.

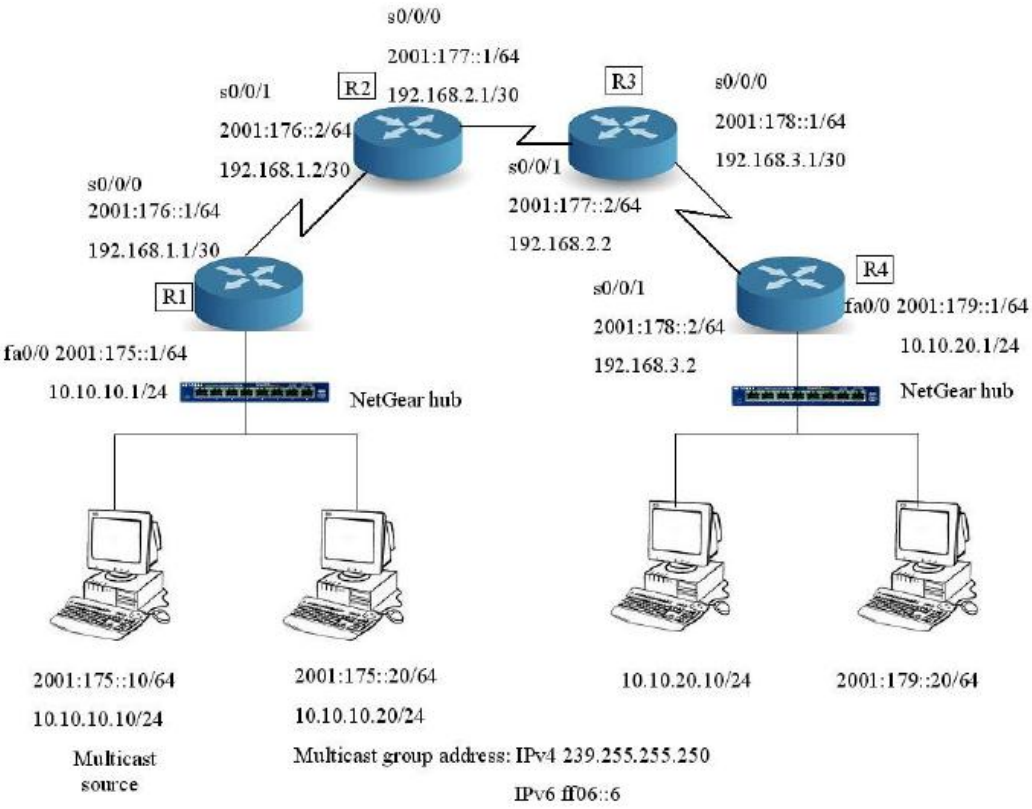

Figura 3. 3: Diagrama de red IPv4/IPv6 Dual-Stack y esquema de direccionamiento.
Elaborado por: Autor.

3.2.4. Escenario 4: Red IPv4-IPv6 – Túnel GRE

En este escenario, solamente dos redes IPv4 se conectan a través de una única red backbone IPv6. Por ejemplo, durante el período de migración de IPv4 a IPv6, el backbone (ISP) puede migrar a IPv6. En tal caso, las redes IPv4 finales se comunican entre sí a través de la red IPv6. Un túnel de encapsulamiento de ruta genérica *(Generic Routing Encapsulation, GRE)* IPv6 se estableció entre el IPv4 sólo para encapsular/desencapsular redes del tráfico IPv4.

GRE es un protocolo desarrollado por Cisco, que se utiliza para conectar redes que ejecutan diferentes protocolos, tales como la conexión

de una red IP e IPX y en este caso la conexión de dos redes IPv4 a través de una red troncal (backbone) de IPv6. Por tal motivo este escenario se configuró lógicamente el túnel GRE para IPv6. Los paquetes IPv4 que entran en el túnel se encapsulan con un encabezado IPv6 y se desencapsulan cuando el paquete llega al otro extremo del túnel.

Para la configuración OSPF, todas las interfaces en serie estarán en el Area 0. La interfaz rápida Ethernet de los enrutadores R1 y R4 y el túnel GRE estarán en el Area 1. En la figura 3.4 se muestra la conectividad de la red IPv4/IPv6.

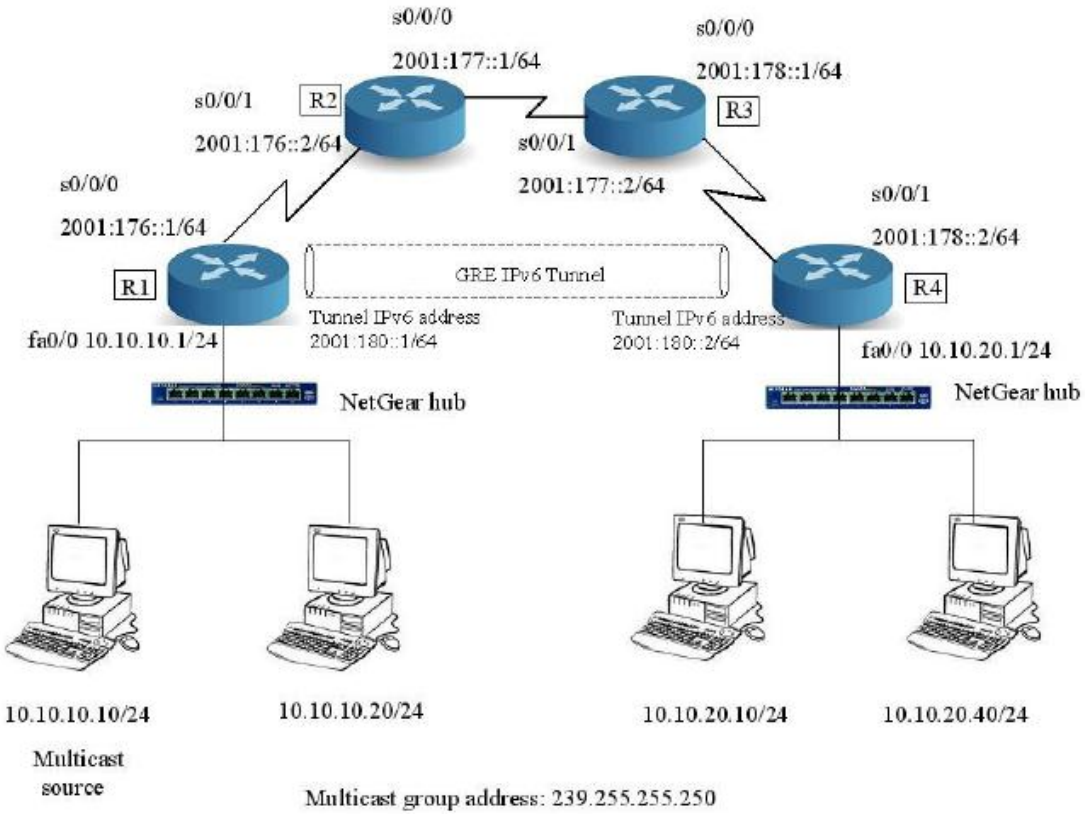

Figura 3. 4: Diagrama de red y esquema de direccionamiento – Túnel GRE.
Elaborado por: Autor.

3.3. Resultados y análisis experimentales

3.3.1. Resultados del escenario 1: Única red IPv4

A. Rendimiento y fluctuación (Jitter).

Desde la salida obtenida por el software JPerf, se observa que en todos los diez períodos de prueba de 10 minutos no hubo pérdida de paquetes y el rendimiento fue del 100%. La fluctuación de fase mostró alguna variación. La fluctuación de fase varía de 0 ms en algunas pruebas para un máximo de 7,792 ms. La figura 3.5 muestra la captura de pantalla del software JPerf.

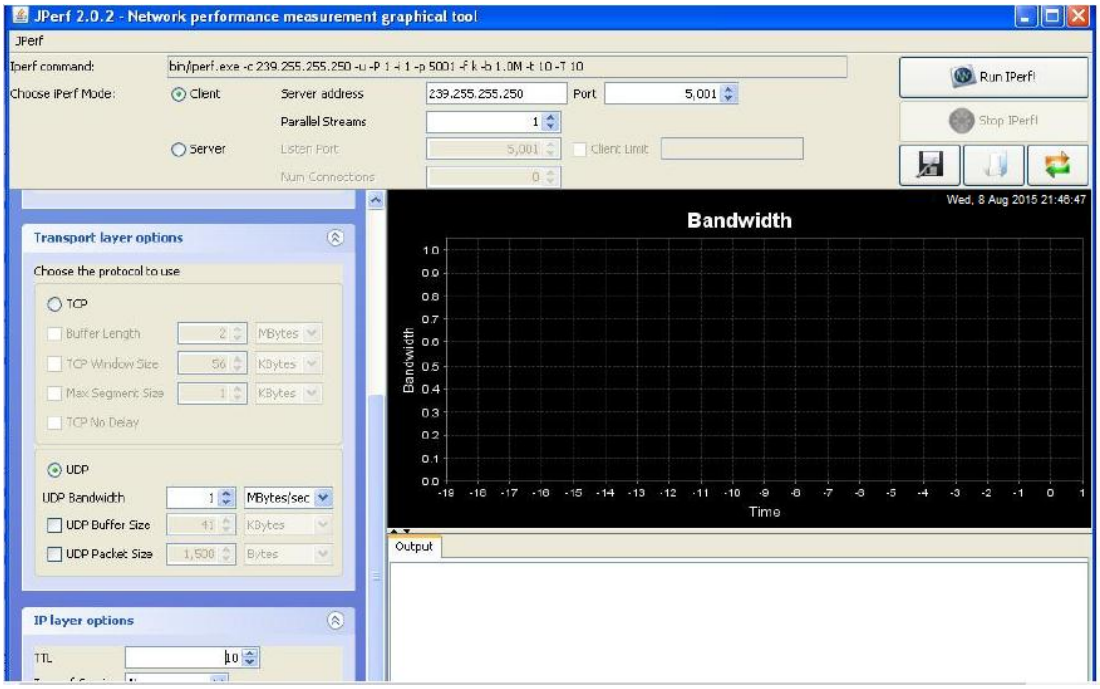

Figura 3. 5: Fuente IPv4 Multidifusión.
Elaborado por: Autor.

Al iniciar JPerf como receptor de multidifusión en el PC, se muestra la siguiente información:

```
bin/Jperf.exe -s -u -P 0 -i 1 -p 5001 -B 239.255.255.250 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Binding to local address 10.10.20.10
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
```

Aquí se puede observar que la dirección del grupo multidifusión es 239.255.255.250 a la que el host local (10.10.20.10) se une.

La gráfica de salida de JPerf fue capturada en diferentes puntos durante el período de 10 minutos. Está proporciona una gráfica en tiempo real del ancho de banda y la fluctuación de fase, tal como se muestra en la figura 3.6.

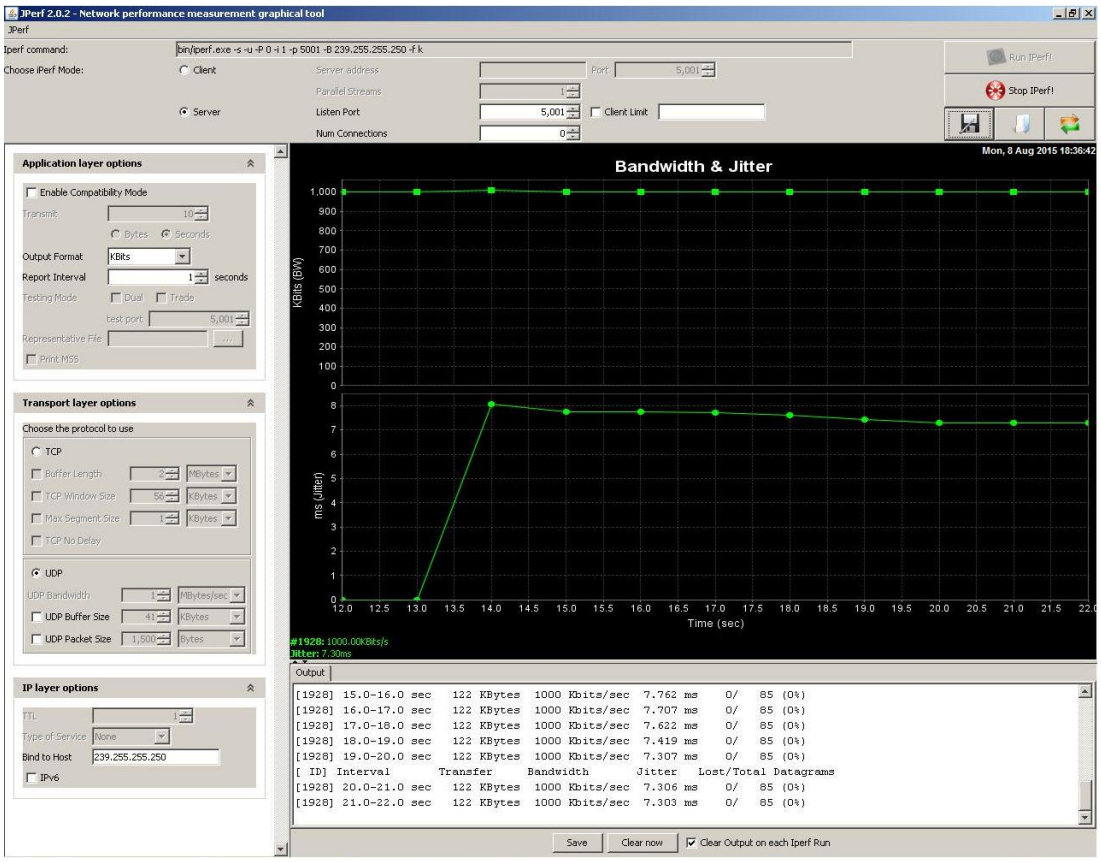

Figura 3. 6: Gráfica del ancho de banda y Jitter del receptor IPv4 multidifusión
Elaborado por: Autor.

En la tabla 3.1 se muestran los valores de transferencia, ancho de banda y fluctuación (Jitter) de los últimos 10 segundos de la salida JPerf capturados desde un receptor multidifusión.

Tabla 3. 2: Datos obtenidos del receptor IPv4 multidifusión.

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1928] 591.0-592.0 sec	122 KBytes	1000 Kbits/sec	7.293 ms	0/ 85 (0%)
[1928] 592.0-593.0 sec	122 KBytes	1000 Kbits/sec	7.282 ms	0/ 85 (0%)
[1928] 593.0-594.0 sec	122 KBytes	1000 Kbits/sec	7.251 ms	0/ 85 (0%)
[1928] 594.0-595.0 sec	122 KBytes	1000 Kbits/sec	7.212 ms	0/ 85 (0%)
[1928] 595.0-596.0 sec	122 KBytes	1000 Kbits/sec	7.146 ms	0/ 85 (0%)
[1928] 596.0-597.0 sec	122 KBytes	1000 Kbits/sec	6.955 ms	0/ 85 (0%)
[1928] 597.0-598.0 sec	123 KBytes	1011 Kbits/sec	8.315 ms	0/ 86 (0%)
[1928] 598.0-599.0 sec	122 KBytes	1000 Kbits/sec	8.314 ms	0/ 85 (0%)
[1928] 599.0-600.0 sec	122 KBytes	1000 Kbits/sec	8.311 ms	0/ 85 (0%)
[ID] Interval	**Transfer**	**Bandwidth**	**Jitter**	**Lost/Total Datagrams**
[1928] 0.0-600.0 sec	**73243 KBytes**	**1000 Kbits/sec**	**7.792 ms**	**0/51021 (0%)**

Elaborado por: Autor

Podemos observar que a partir de la salida anterior, durante el período de 10 minutos, se transfirieron 73.244 MB de datos a una velocidad 1 Mbps. La fluctuación es de 7.792 ms. La pérdida de paquetes es 0%, lo que implica un rendimiento de 100%. Dos muestras de prueba de 1 hora, también se obtuvieron del receptor multidifusión. Esto era para simular una aplicación multicast real, tales como un seminario de 1 hora. La fluctuación de fase variaba entre 0 ms y 7.817 ms y el rendimiento fue del 100% en ambos los casos de prueba.

B. Protocolo Overhead.

Se utilizó PIM-SM como el protocolo de enrutamiento de multidifusión. El protocolo no produjo gran parte de una sobrecarga (deducida a partir de las capturas de Wireshark). Los paquetes de mensajes PIMv2 fueron

enviados a intervalos de 30 segundos, según se ve las marcas de tiempo de la figura 3.7. Aparte de estos paquetes de saludo, el protocolo no era muy comunicativo en la red IPv4.

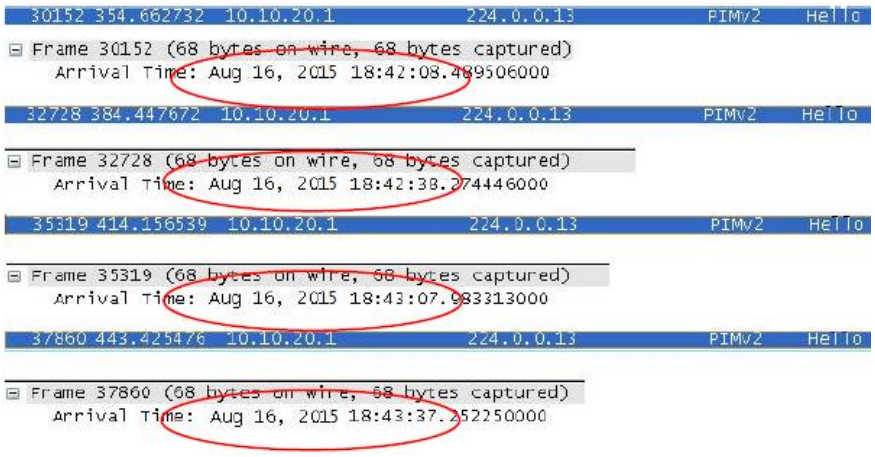

Figura 3. 7: Paquetes de saludo “Hello” de PIM para IPv4 multidifusión.
Elaborado por: Autor.

3.3.2. Resultados del escenario 2: Única red IPv6

A. Rendimiento y fluctuación (Jitter).

Al iniciar el software JPerf en el receptor, se muestra el siguiente mensaje:

```
bin/Jperf.exe -s -u -P 0 -i 1 -p 5001 -B ff06::6 -V -f k
------------------------------------------------------------
Server listening on UDP port 5001
Binding to local address ::
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
```

Es decir, que la dirección del grupo de multidifusión es ff06: 6. Como en el caso de una red IPv4, los resultados se obtuvieron de un receptor multidifusión para diez pruebas de 10 minutos y dos pruebas de 1 hora.

Se puede inferir de los resultados que IPv6 multicast no produzca ninguna pérdida de fluctuación (Jitter) de fase significativamente mayor o pérdida de paquetes como en el caso de una red IPv4. Durante las diez pruebas de 10 minutos, la fluctuación osciló entre 0 ms a 9.487 ms. El rendimiento fue del 100% en todas las diez pruebas. De estas pruebas se podemos concluir que la hipótesis de este trabajo de titulación no se cumple.

Para las dos pruebas de 1 hora, la fluctuación en una prueba fue de 0 ms y en la segunda prueba fue con 7.299 ms, con un rendimiento del 100% en ambos las pruebas. En la tabla 3.3 se muestran los valores de transferencia, ancho de banda y fluctuación (Jitter) de los últimos 10 segundos de la salida JPerf capturados desde un receptor multidifusión.

Tabla 3. 3: Datos obtenidos del receptor IPv6 multidifusión.

[ID]	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1928]	591.0-592.0 sec	122 KBytes	1000 Kbits/sec	8.302 ms	0/ 85 (0%)
[1928]	592.0-593.0 sec	122 KBytes	1000 Kbits/sec	8.292 ms	0/ 85 (0%)
[1928]	593.0-594.0 sec	122 KBytes	1000 Kbits/sec	8.265 ms	0/ 85 (0%)
[1928]	594.0-595.0 sec	122 KBytes	1000 Kbits/sec	8.230 ms	0/ 85 (0%)
[1928]	595.0-596.0 sec	122 KBytes	1000 Kbits/sec	8.173 ms	0/ 85 (0%)
[1928]	596.0-597.0 sec	122 KBytes	1000 Kbits/sec	8.005 ms	0/ 85 (0%)
[1928]	597.0-598.0 sec	122 KBytes	1000 Kbits/sec	7.795 ms	0/ 85 (0%)
[1928]	598.0-599.0 sec	122 KBytes	1000 Kbits/sec	7.794 ms	0/ 85 (0%)
[1928]	599.0-600.0 sec	122 KBytes	1000 Kbits/sec	7.792 ms	0/ 85 (0%)
[ID]	**Interval**	**Transfer**	**Bandwidth**	**Jitter**	**Lost/Total Datagrams**
[1928]	**0.0-600.0 sec**	**73244 KBytes**	**1000 Kbits/sec**	**7.305 ms**	**0/51022 (0%)**

Elaborado por: Autor

Desde la salida, se puede ver que durante el período de 10 minutos, se transfirieron 73.244 MB de datos a 1 Mbps con 0% de pérdida de paquetes. La fluctuación era 7.305 ms. En la figura 3.8 se muestra la captura de pantalla de la salida en vivo desde JPerf.

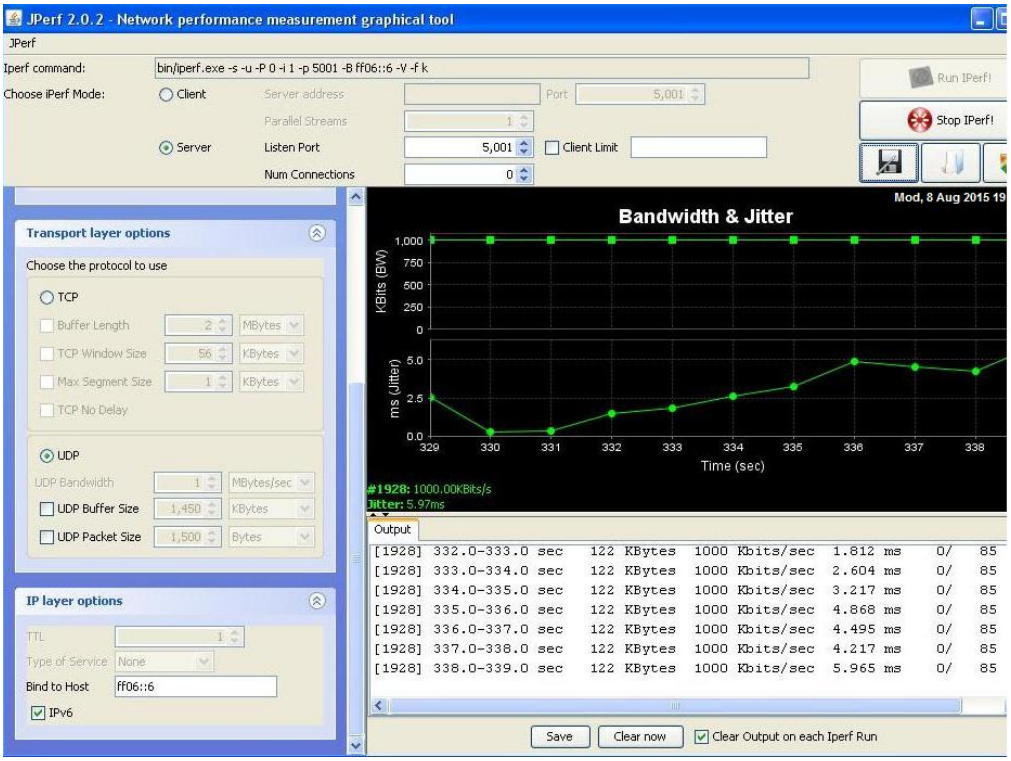

Figura 3. 8: Gráfica del ancho de banda y Jitter del receptor IPv6 multidifusión
Elaborado por: Autor.

B. Protocolo Overhead.

Comparamos con la red IPv4, observamos ver que no hay diferencias en la sobrecarga del protocolo PIM añadido que cuando se ejecutó sobre IPv6. Al igual que la red IPv4, el PIM envía paquetes de saludo a intervalos de 30 segundos como se puede ver en la figura 3.9 la captura de Wireshark.

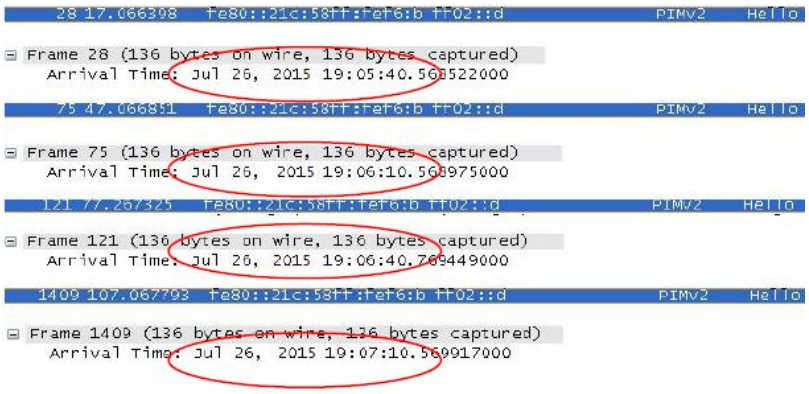

Figura 3. 9: Paquetes de mensajes PIM para IPv6 multicast
Elaborado por: Autor.

3.3.3. Resultados del escenario 3: Dual-Stack en Redes IPv4-IPv6.

A. Rendimiento y fluctuación (Jitter).

Para este escenario, se ha configurado una red de doble pila (Dual-Stack) de extremo a extremo. Las salidas de prueba se obtuvieron de un único receptor multidifusión IPv4 y de un único receptor multidifusión IPv6. En este escenario, había poca fluctuación (jitter) y pérdida de paquetes en casi todas las pruebas que se realizó. En las figuras 3.10 y 3.11 se muestran las capturas de pantalla de la muestra y los resultados de JPerf.

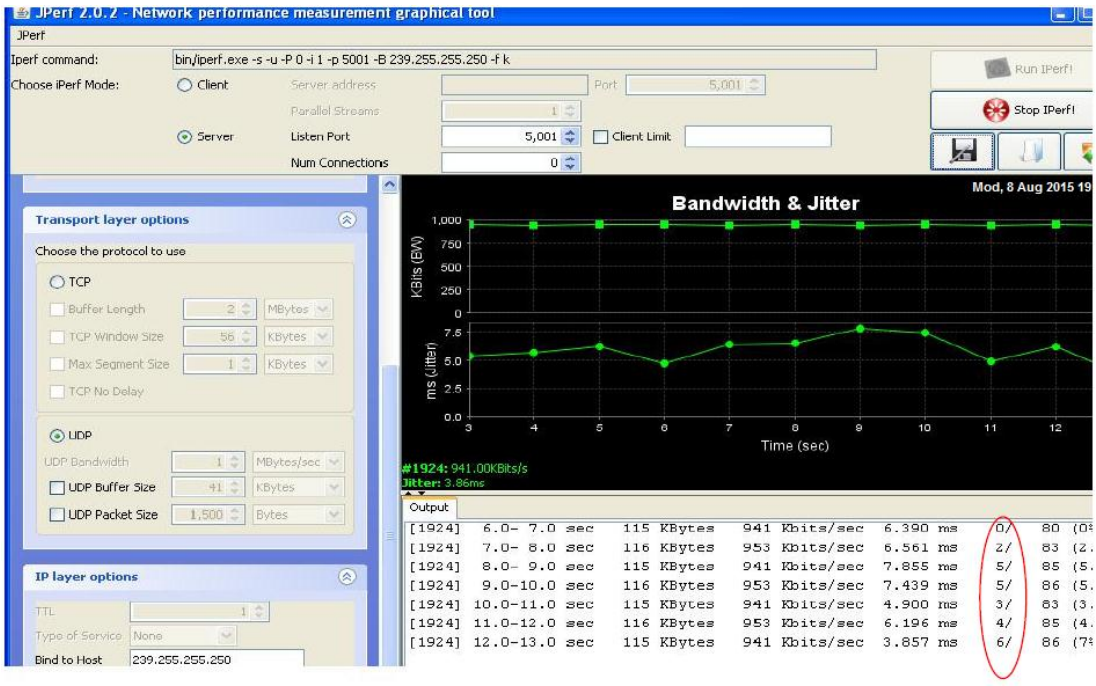

Figura 3. 10: Gráfica del ancho de banda y Jitter del receptor IPv4 en la red Dual-Stack.
Elaborado por: Autor.

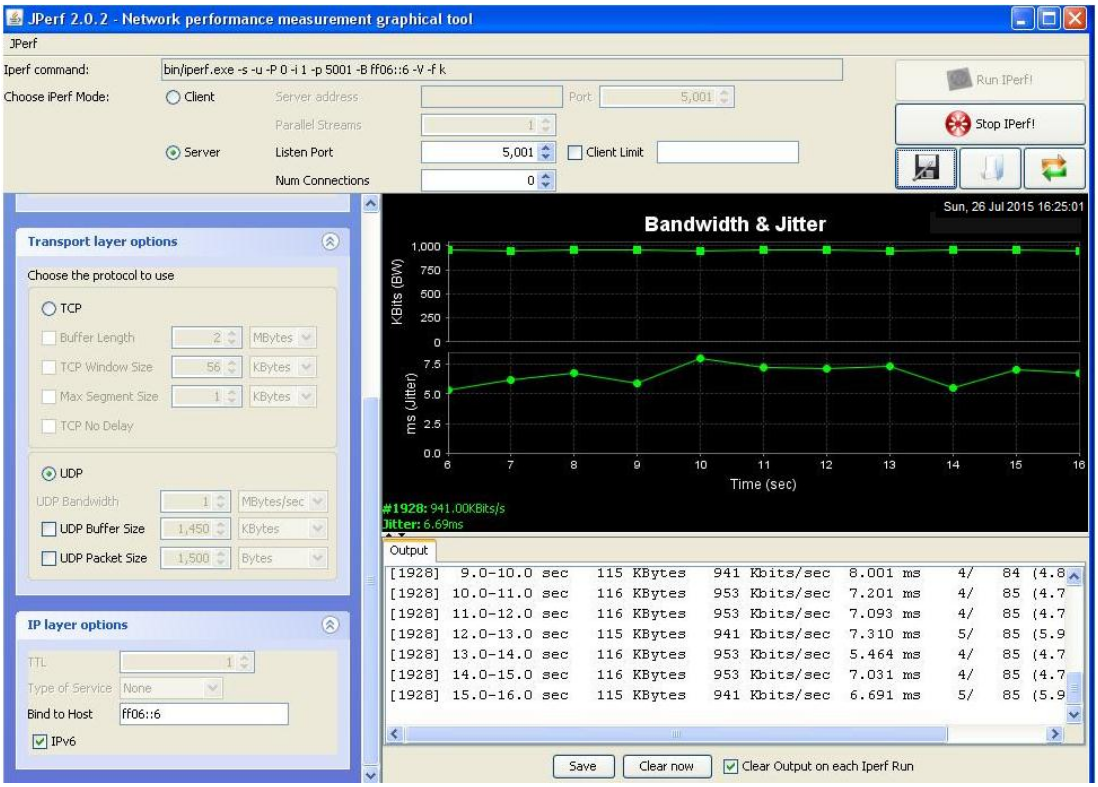

Figura 3. 11: Gráfica del ancho de banda y Jitter del receptor IPv6 en la red Dual-Stack.

Elaborado por: Autor.

En las tablas 3.4 y 3.5 se muestran los valores de transferencia, ancho de banda y fluctuación (Jitter) de los últimos 10 segundos de la salida JPerf capturados desde los receptores multidifusión IPv4 e IPv6 Dual-Stack.

Tabla 3. 4: Datos obtenidos del receptor IPv4 multidifusión Dual-Stack.

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1924] 591.0-592.0 sec	116 KBytes	953 Kbits/sec	5.800 ms	3/ 84 (3.6%)
[1924] 592.0-593.0 sec	115 KBytes	941 Kbits/sec	6.404 ms	5/ 85 (5.9%)
[1924] 593.0-594.0 sec	116 KBytes	953 Kbits/sec	6.948 ms	4/ 85 (4.7%)
[1924] 594.0-595.0 sec	115 KBytes	941 Kbits/sec	7.782 ms	5/ 85 (5.9%)
[1924] 595.0-596.0 sec	115 KBytes	941 Kbits/sec	5.511 ms	4/ 84 (4.8%)
[1924] 596.0-597.0 sec	116 KBytes	953 Kbits/sec	9.027 ms	5/ 86 (5.8%)
[1924] 597.0-598.0 sec	116 KBytes	953 Kbits/sec	4.183 ms	4/ 85 (4.7%)
[1924] 598.0-599.0 sec	115 KBytes	941 Kbits/sec	7.172 ms	6/ 86 (7%)
[1924] 599.0-600.0 sec	116 KBytes	953 Kbits/sec	7.661 ms	4/ 85 (4.7%)
[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1924] 0.0-600.5 sec	69424 KBytes	947 Kbits/sec	4.873 ms	2600/50961 (5.1%)

Elaborado por: Autor.

Tabla 3. 5: Datos obtenidos del receptor IPv6 multidifusión Dual-Stack.

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1928] 591.0-592.0 sec	116 KBytes	953 Kbits/sec	5.237 ms	4/ 85 (4.7%)
[1928] 592.0-593.0 sec	115 KBytes	941 Kbits/sec	6.996 ms	5/ 85 (5.9%)
[1928] 593.0-594.0 sec	116 KBytes	953 Kbits/sec	5.481 ms	5/ 86 (5.8%)
[1928] 594.0-595.0 sec	115 KBytes	941 Kbits/sec	5.986 ms	4/ 84 (4.8%)
[1928] 595.0-596.0 sec	118 KBytes	964 Kbits/sec	6.764 ms	4/ 86 (4.7%)
[1928] 596.0-597.0 sec	115 KBytes	941 Kbits/sec	6.676 ms	4/ 84 (4.8%)
[1928] 597.0-598.0 sec	116 KBytes	953 Kbits/sec	5.115 ms	4/ 85 (4.7%)
[1928] 598.0-599.0 sec	115 KBytes	941 Kbits/sec	6.401 ms	5/ 85 (5.9%)
[1928] 599.0-600.0 sec	116 KBytes	953 Kbits/sec	5.288 ms	4/ 85 (4.7%)
[ID] Interval	**Transfer**	**Bandwidth**	**Jitter**	**Lost/Total Datagrams**
[1928] 0.0-600.4 sec	**69519 KBytes**	**949 Kbits/sec**	**7.775 ms**	**2595/51022 (5.1%)**

Elaborado por: Autor.

De las tablas 3.5 y 3.5 podemos observar que para cada intervalo de transmisión de paquetes, hay algo de pérdida de paquetes. También se realizaron dos pruebas de 1 hora y la pérdida de paquetes se observó en ambos casos de prueba. La tabla 3.7 muestra el rendimiento para un receptor multicast IPv4 y un receptor de multidifusión IPv6 para todas las diez pruebas de 10 minutos:

Tabla 3. 6: Rendimiento para receptores IPv4 e IPv6 en redes Dual-Stack.

Prueba de 10 minutos	Rendimiento del receptor IPv4 en redes IPv4 (%)	Rendimiento del receptor IPv6 en redes IPv4 (%)
1	94.84	94.988
2	94.871	94.966
3	94.863	94.914
4	94.898	94.932
5	94.88	94.959
6	94.913	94.931
7	94.837	94.934
8	94.79	94.955
9	94.844	94.962
10	94.897	94.952

Elaborado por: Autor.

Para las pruebas realizadas en los cuatro escenarios, unos resultados de las muestras se obtuvieron de un receptor de multidifusión en la misma subred que la fuente y consistentemente, la fluctuación de fase de 0 ms en la mayoría de los casos y menos de 2 ms en otros casos. Así se puede concluir que cualquier variación en la pérdida de latencia y de paquetes fue causada por el enrutamiento del tráfico de multidifusión a través de los cuatro routers.

Este resultado en el escenario Dual-Stack (doble pila) es significativo, donde el receptor multidifusión que reside en la misma subred que la fuente tiene fluctuaciones (jitter) y pérdida de paquetes insignificantes. Una captura de pantalla de un host IPv4 en la misma subred se muestra en la figura 3.12.

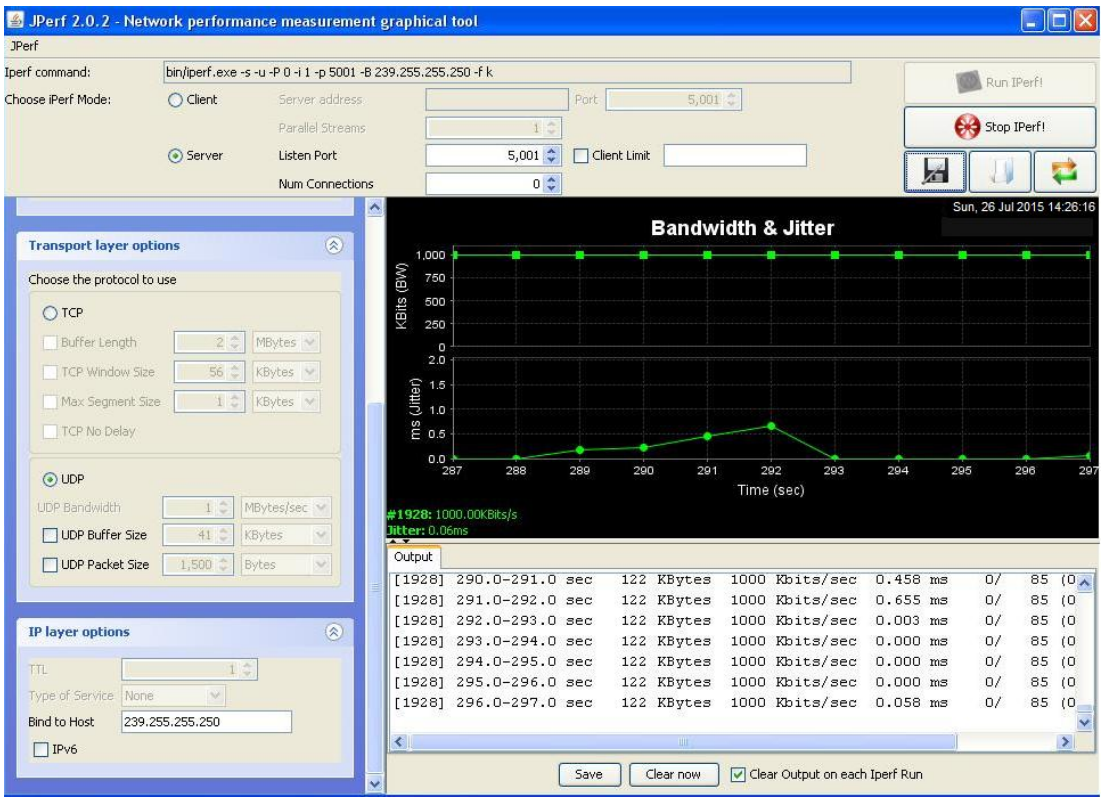

Figura 3. 12: Gráfica del ancho de banda y Jitter del receptor IPv4 en la misma subred de la fuente Dual-Stack.
Elaborado por: Autor.

En la tabla 3.7 se muestran los valores de transferencia, ancho de banda y fluctuación (Jitter) de los últimos 10 segundos de la salida JPerf capturados desde los receptores multidifusión IPv6 en la misma subred de la fuente de una red Dual-Stack.

Tabla 3. 7: Datos del receptor multidifusión IPv6 en la misma subred de Dual-Stack.

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1928] 591.0-592.0 sec	122 KBytes	1000 Kbits/sec	3.155 ms	0/ 85 (0%)
[1928] 592.0-593.0 sec	122 KBytes	1000 Kbits/sec	0.254 ms	0/ 85 (0%)
[1928] 593.0-594.0 sec	122 KBytes	1000 Kbits/sec	0.022 ms	0/ 85 (0%)
[1928] 594.0-595.0 sec	122 KBytes	1000 Kbits/sec	2.773 ms	0/ 85 (0%)
[1928] 595.0-596.0 sec	122 KBytes	1000 Kbits/sec	0.450 ms	0/ 85 (0%)
[1928] 596.0-597.0 sec	122 KBytes	1000 Kbits/sec	0.011 ms	0/ 85 (0%)
[1928] 597.0-598.0 sec	122 KBytes	1000 Kbits/sec	0.879 ms	0/ 85 (0%)
[1928] 598.0-599.0 sec	122 KBytes	1000 Kbits/sec	2.891 ms	0/ 85 (0%)
[1928] 599.0-600.0 sec	122 KBytes	1000 Kbits/sec	1.794 ms	0/ 85 (0%)
[ID] Interval	**Transfer**	**Bandwidth**	**Jitter**	**Lost/Total Datagrams**
[1928] 0.0-600.0 sec	**73207 KBytes**	**999 Kbits/sec**	**1.682 ms**	**2/50998 (0.0039%)**

Elaborado por: Autor.

B. Protocolo Overhead.

Como en el caso de los escenarios anteriores, el protocolo de enrutamiento PIM, no contribuye a cualquier tráfico enrutador significativo como puede verse en la figura 3.13. Cada 30 segundos, los paquetes de saludos se intercambian para redes IPv4 e IPv6 multidifusión.

No.	Time	Source	Destination	Protocol	Info
41	20.994324	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello
44	21.170146	10.10.20.1	224.0.0.13	PIMv2	Hello
93	50.706354	10.10.20.1	224.0.0.13	PIMv2	Hello
94	51.194460	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello
2143	80.454570	10.10.20.1	224.0.0.13	PIMv2	Hello
2330	81.194686	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello
9495	110.106749	10.10.20.1	224.0.0.13	PIMv2	Hello
9764	111.195071	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello
16940	140.106950	10.10.20.1	224.0.0.13	PIMv2	Hello
17061	140.595077	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello
24337	169.815151	10.10.20.1	224.0.0.13	PIMv2	Hello
24480	170.395362	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello
31694	199.491335	10.10.20.1	224.0.0.13	PIMv2	Hello
31820	199.995487	fe80::21c:58ff:fef6:b	ff02::d	PIMv2	Hello

Figura 3. 13: Paquetes de saludos PIM para redes IPv4-IPv6 de doble pila multidifusión.

Elaborado por: Autor.

3.3.4. Resultados del escenario 4: Túnel GRE - Redes IPv4-IPv6.

Este escenario es el más probable que ocurra durante el período de transición cuando tenga lugar la transición de una red IPv4 a una red IPv6. Mientras que los ISP's pueden iniciar la migración, los usuarios finales pueden no hacer la transición al mismo ritmo. El túnel GRE se configura para enrutar el tráfico multicast IPv4 a través de una red troncal (backbone) IPv6.

A. Rendimiento y Jitter

Similar a una sola red IPv4 o IPv6, esta red tampoco tiene muchas fluctuaciones y sin pérdida de paquetes durante todas las pruebas, tal como se muestra en la figura 3.14.

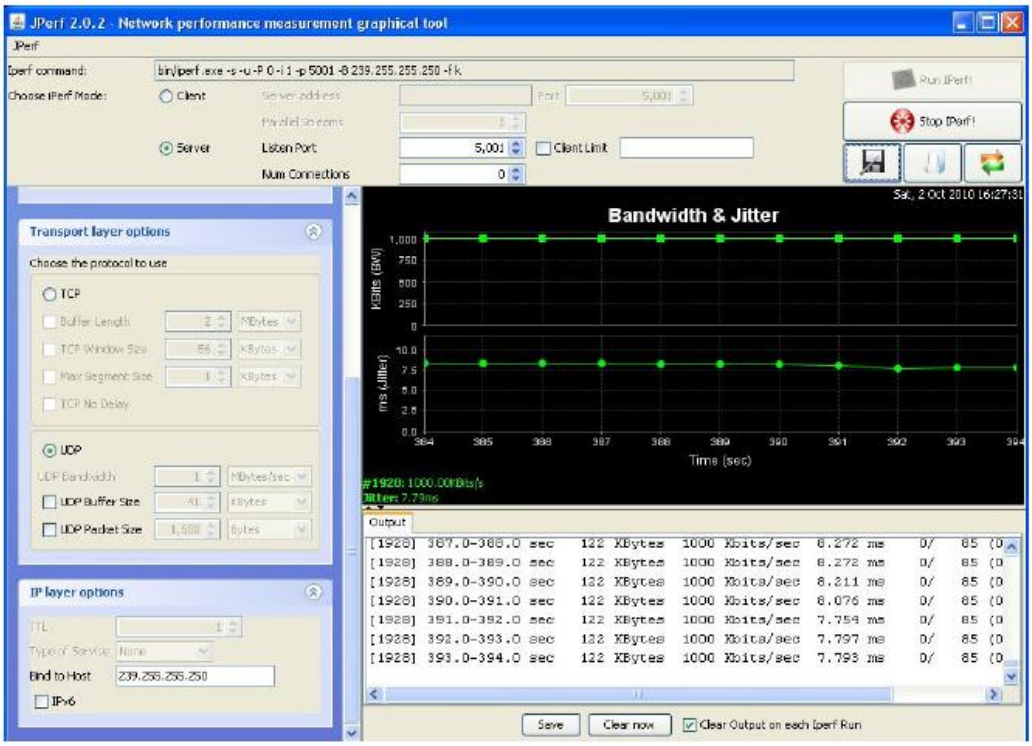

Figura 3. 14: Gráfica del ancho de banda y Jitter del receptor IPv4 a través del túnel GRE.
Elaborado por: Autor.

La tabla 3.8 muestra los valores de transferencia, ancho de banda y fluctuación (Jitter) de los últimos 10 segundos de la salida JPerf. En esta muestra, el jitter fue de 0.111 ms sin pérdida de paquetes. Durante todas las pruebas la fluctuación osciló entre 0 ms a 7.792 ms.

Tabla 3. 8: Datos del receptor multidifusión IPv4 a través del túnel GRE.

[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1928] 591.0-592.0 sec	122 KBytes	1000 Kbits/sec	0.002 ms	0/ 85 (0%)
[1928] 592.0-593.0 sec	122 KBytes	1000 Kbits/sec	0.000 ms	0/ 85 (0%)
[1928] 593.0-594.0 sec	122 KBytes	1000 Kbits/sec	0.000 ms	0/ 85 (0%)
[1928] 594.0-595.0 sec	122 KBytes	1000 Kbits/sec	0.000 ms	0/ 85 (0%)
[1928] 595.0-596.0 sec	122 KBytes	1000 Kbits/sec	0.000 ms	0/ 85 (0%)
[1928] 596.0-597.0 sec	122 KBytes	1000 Kbits/sec	0.000 ms	0/ 85 (0%)
[1928] 597.0-598.0 sec	122 KBytes	1000 Kbits/sec	1.078 ms	0/ 85 (0%)
[1928] 598.0-599.0 sec	122 KBytes	1000 Kbits/sec	0.004 ms	0/ 85 (0%)
[1928] 599.0-600.0 sec	122 KBytes	1000 Kbits/sec	0.118 ms	0/ 85 (0%)
[ID] Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
[1928] 0.0-600.0 sec	73244 KBytes	1000 Kbits/sec	0.111 ms	0/51022 (0%)

Elaborado por: Autor.

B. Protocolo Overhead.

Como en el caso de todos los escenarios, el único tráfico que PIM generado era los paquetes de saludo a intervalos de 30 segundos. Esto se puede ver a partir de la captura Wireshark a continuación, donde sólo el tráfico PIM se ha filtrado a cabo.

Figura 3. 15: Paquete de saludos en Túnel GRE para redes IPv4-IPv6 multidifusión.
Elaborado por: Autor.

3.4. Representación gráfica de los resultados.

Los resultados de la prueba de 10 minutos y 1 hora recogidas de los diferentes escenarios se muestran en las siguientes figuras.

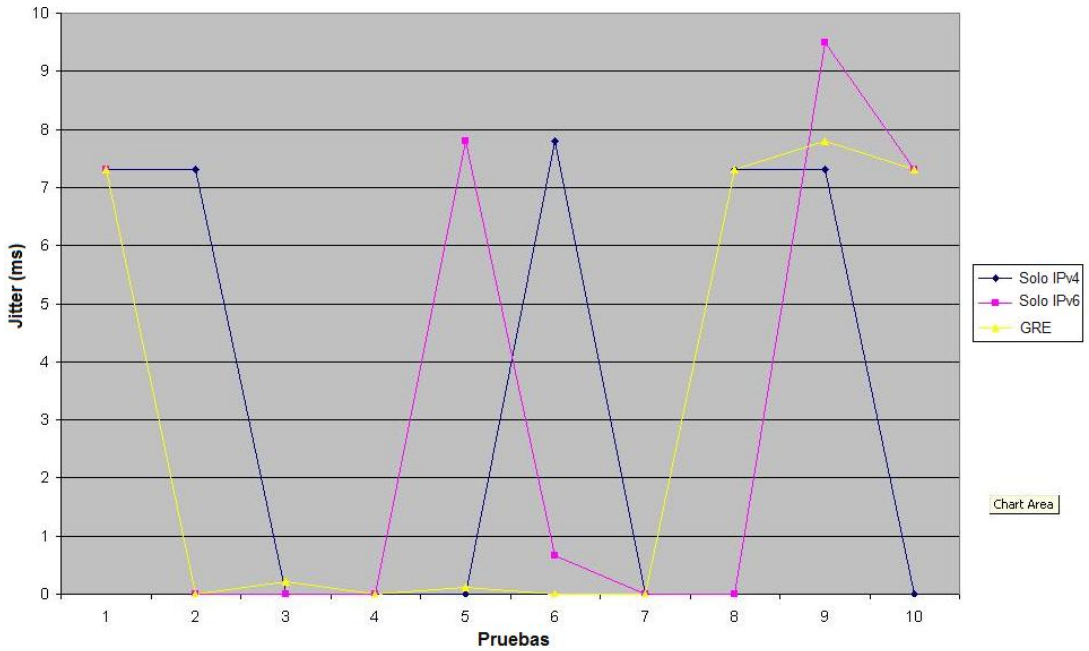

Figura 3. 16: Pruebas de multidifusión de 10 minutos para redes IPv4, IPv6 y túnel GRE.
Elaborado por: Autor.

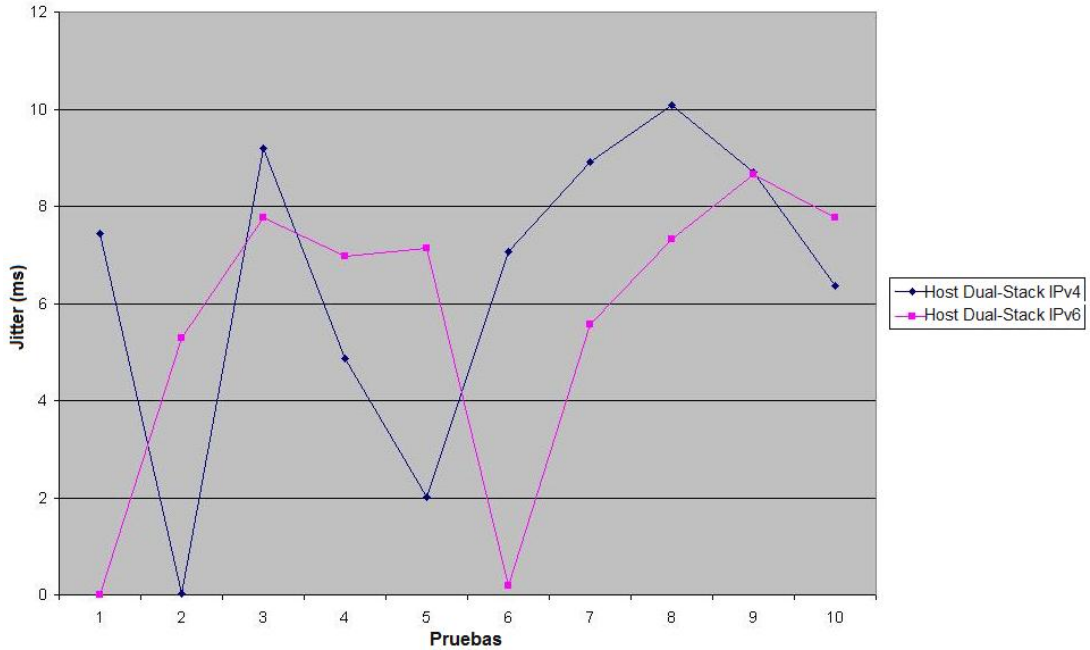

Figura 3. 17: Pruebas de multidifusión de 10 minutos para la red Dual-Stack.
Elaborado por: Autor.

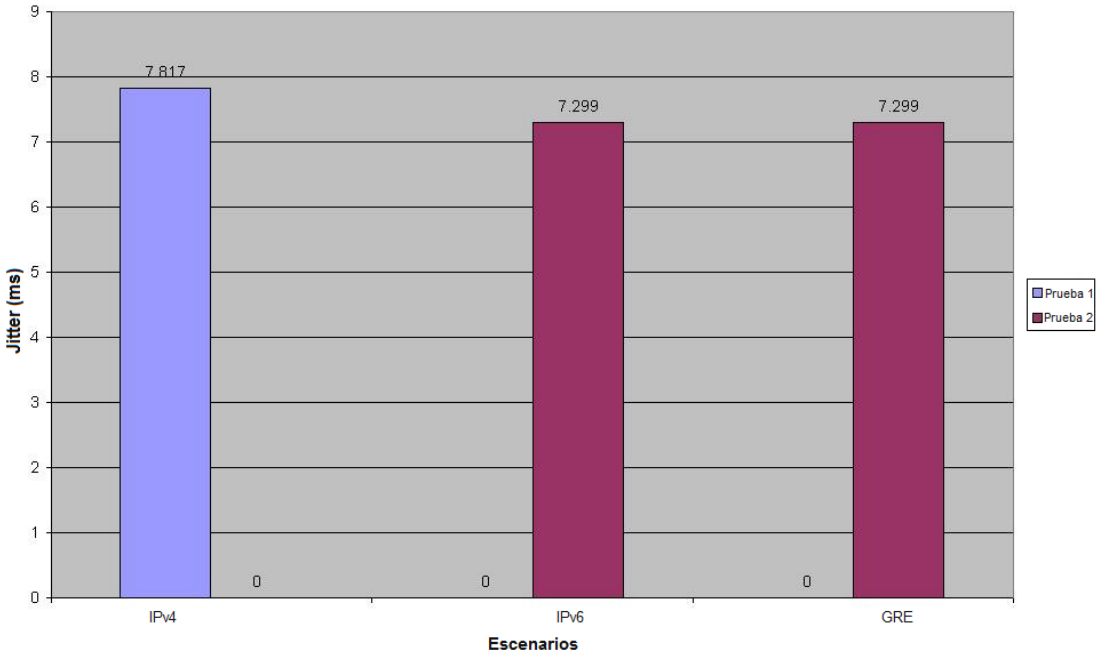

Figura 3. 18: Pruebas de multidifusión de 1hora para redes IPv4, IPv6 y túnel GRE.
Elaborado por: Autor.

Nota: Los valores en los gráficos indican la fluctuación de 0 ms en algunas de las pruebas

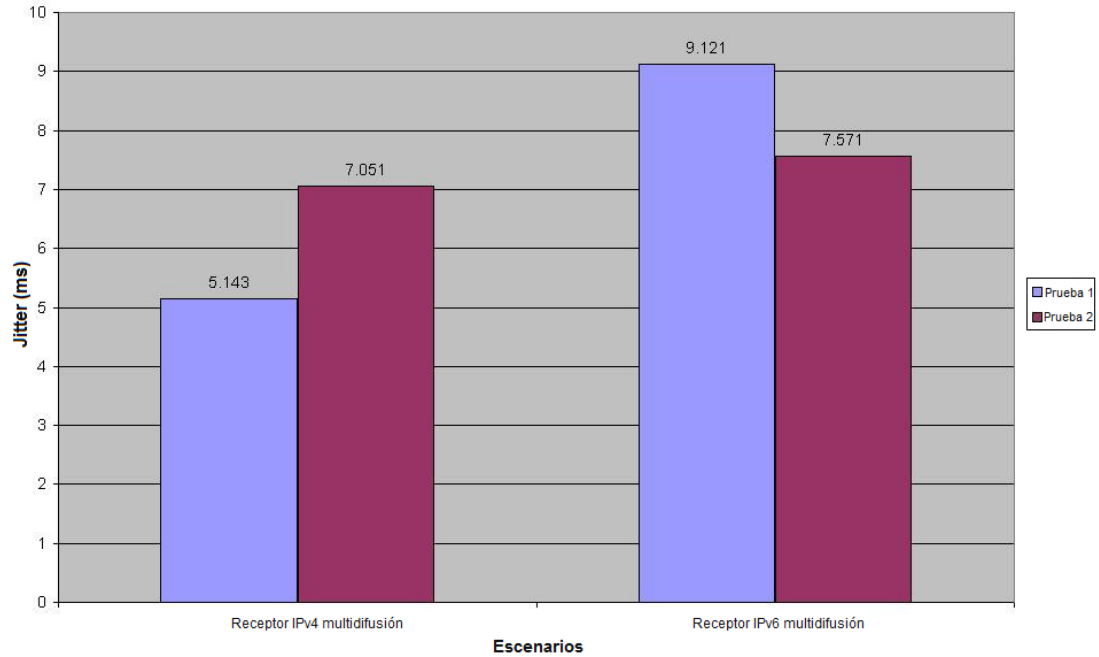

Figura 3. 19: Pruebas de multidifusión 1 hora para la red Dual-Stack.
Elaborado por: Autor.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES.

4.1. Conclusiones.

El mismo conjunto de los resultados se obtuvo de una red totalmente IPv4 y una red totalmente IPv6. Mientras que la diferencia en los resultados no difiere significativamente, los resultados refutan la hipótesis del trabajo de titulación que el protocolo de sobrecarga (Overhead), fluctuación (Jitter) y el rendimiento en una red IPv6 serían significativamente más grandes que una red IPv4, debido a su mayor espacio de direcciones. El protocolo Overhead en ambas redes sigue siendo el mismo.

En los experimentos llevados a cabo en el trabajo de titulación, la carga útil en el caso de IPv4 como IPv6 se mantuvo constante. Las unidades de transferencia máxima (MTU) de la interfaz permanecieron con sus valores predeterminados - tarjetas de interfaz de red (NIC) de PC tenían por defecto la MTU de 1500 y los routers de Cisco también se quedaron en el valor predeterminado de 1500.

En el caso de la red IPv4, no había sin fragmentación, mientras que en IPv6 la fragmentación fue manejada por el host (anfitrión). A pesar de la tarea adicional de la fragmentación, no hay ningún deterioro en el rendimiento de la red IPv6, lo que demuestra que IPv6 maneja la fragmentación de manera eficiente.

Dado que IPv6 fue diseñado como un reemplazo para IPv4, y diseñado para ser mejor que IPv4. El encabezado IPv6 es más sencillo que un encabezado IPv4. Por ejemplo, el campo de opciones, que se incluye en la cabecera IPv4, es una extensión de la cabecera IPv6. Así que sin ninguna opción, el encabezado IPv6 no es tan complejo como un encabezado IPv4. La comprobación en la detección de errores (checksum) en IPv4, es eliminada en IPv6 (otras capas se encargan de la detección de errores).

En el caso del período de transición durante la transición de IPv4 a IPv6, ambos protocolos podrían coexistir. De los resultados experimentales, puede observarse que una red Dual-Stack (doble pila) de extremo a extremo experimenta mayor pérdida de paquetes, en comparación con un túnel. Cabe indicar sin embargo, que en el caso de la red Dual-Stack hay dos secuencias de multidifusión - uno para IPv4 y uno para IPv6.

4.2. Recomendaciones.

- Todas las pruebas se llevaron a cabo en un entorno de laboratorio, sin ningún otro tipo de tráfico, a excepción de la generada con fines experimentales. Como paso siguiente, el resto del tráfico puede ser introducido en la red, para estudiar el rendimiento aún más cerca de la configuración del mundo real.
- Realizar estudios a futuro de cómo podría llevarse a cabo la MTU con diferentes tamaños de paquetes a través de la red y ver cómo afecta al rendimiento de las redes IPv4 e IPv6.

- Además la complejidad puede ser introducida en la red, agregando grupos de multidifusión y más receptores sean miembros de más de un grupo de multidifusión. Esto ayudaría a comprender lo que la latencia/fluctuación introducen al router cuando se tiene que procesar mayor tráfico y decisiones de enrutamiento multicast.
- Realizar el estudio del impacto de la escalabilidad que puede ser estudiada mediante el aumento del número de fuentes y receptores de multidifusión, ya sea en una configuración experimental cuando sea posible o usando una herramienta de simulación.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre, L. P., González, F., & Mejía, D. (2013). *Aplicaciones de MPLS, Transición de IPv4 a IPv6 y Mejores Prácticas de Seguridad para el ISP Telconet.* Revista Politécnica, 32.

Almario Zea, R. (2013). *Diseño y simulación de las herramientas básicas para la implementación de redes con soporte IPv6.*

Ávila M., Ó. (2011). *Migración del protocolo IPv4 a IPv6*. Depto. De Ingeniería Eléctrica, UAM.

Bolívar, L., Guerrero, F., & Polanco, O. (2012). *Design and implementation of IPv6 network for efficient transition from IPv4.* Ingeniería y competitividad, 14(2), 179-189.

Coellar, J & Cedeño, J (2012). *Propuesta para la Transición de IPv4 a IPv6 en el Ecuador a través de la Supertel.* Tesis de Maestría en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil.

Escobar, J., Jaimes, L., & Bautista, D. (2013). *Movilidad en IPV6: simulación con Network Simulator.* INGE CUC, 9(2), 21-30.

Facchini, H. A., Pérez, S., Dantiacq, A., & Cangemi, G. (2013). *Análisis de prestaciones de tráfico multicast en redes mixtas IPv4 e IPv6.* XV Workshop de Investigadores en Ciencias de la Computación.

Ferrer, S. (2011). *Migración a IPv6: un cambio necesario.* Datamation: la revista española de tecnología de la Información para empresa, (291), 24-25.

García, N., Sarmiento, D., & Trujillo, E. (2013). *Propuesta de conexión de entorno IPv6 mediante un backbone MPLS/IPv4.* Redes de Ingeniería, 4, 36-48.

Juárez, J., & Castro, J. (2014). *Análisis e implementación del protocolo de enrutamiento OSPF para IP versión 6.* Vínculos, 10(2), 189-198.

Landy R., D. (2013). *Propuesta de un Plan de Implementación para la migración a IPv6 en la red de la Universidad Politécnica Salesiana Sede-Cuenca.* Tesis previa a la obtención del Título de Ingeniero de Sistemas.

López O., J. (2015). *Análisis de las técnicas de tunneling para la coexistencia de IPv4 e IPv6 que brinde soporte a tráfico de VoIp.*

Medina, C. A. C., & Rodríguez, F. F. (2013). *Caracterización de IPv6.* Revista Tecnura, 17(36), 111-128.

Mercado, G., Pérez, C., Taffernaberry, J. C., Robles, M. I., Orbiscay, M., Tobar, S., Moralejo, R. & Pérez, S. (2011). *Implementación y Evaluación de métodos de Traslación de Protocolos para la transición IPv4-IPv6.* XVII Congreso Argentino de Ciencias de la Computación.

Salcedo, O., López, D., & Gamboa Quiroga, F. A. (2012). *Migración de redes de voz IPv4 a IPv6.* Tecnura, 16(31), 76-87.

Torres C., J., & Ortega S., B. (2012). *Análisis, diseño de una red MPLS con IPv6 en las UTICS de la Escuela Politécnica del Ejército* (Doctoral dissertation, SANGOLQUÍ/ESPE/2012).