UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIRÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROPUESTA TECNOLÓGICA

"MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA"

Proyecto de Titulación presentado previo a la obtención del Título de Ingeniero en Informática y sistemas computacionales

Autores:

Galarza Mena Richard Alexander

Jaya Condorcana Cristian Mauricio

Tutor:

Mgs. Ing. Jorge Bladimir Rubio Peñaherrera

Latacunga-Ecuador

Septiembre-2020

DECLARACIÓN DE AUTORÍA

"Nosotros, Galarza Mena Richard Alexander y Jaya Condorcana Cristian Mauricio y declaramos ser autores de la presente de la propuesta tecnológica: **"MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA"**, siendo el Ing. MSc. Jorge Bladimir Rubio Peñaherrera tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en la presente propuesta tecnológica, son de nuestra exclusiva responsabilidad.

…...…… ……..

JAYA CONDORCANA CRISTIAN MAURICIO **GALARZA MENA RICHARD ALEXANDER**

C.I.: 050385475-4 **C.I.: 050296508-0**

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor de la Propuesta Tecnológica sobre el título:

"MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA", de Jaya Condorcana Cristian Mauricio y Galarza Mena Richard Alexander de la carrera de **INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES**, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS** de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Septiembre 2020

……..

Mgs. Ing. Jorge Bladimir Rubio Peñaherrera
CC: 050222229-2
Tutor de Titulación

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD de Ciencias de la Ingeniería y Aplicadas; por cuanto, los postulantes: Jaya Condorcana Cristian Mauricio y Galarza Mena Richard Galarza con el título de Proyecto de titulación: **"MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA"**, han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, Septiembre 2020

Para constancia firman:

Lector 1 (Presidente)
Ing. MSc. Llano Casa Alex Christian
CC:0502589864

Lector 2
Ing. Mg. Cadena Moreano José Augusto
CC: 0501552798

Lector 3
Ing. MSc. Medina Matute Victor Hugo
CC:0501373955

AVAL DE IMPLEMENTACIÓN

EMPRESA G&S INGENIEROS.CIA LTDA

Latacunga, Septiembre 2020

CERTIFICACIÓN:

Mediante el presente pongo a consideración que los señores Richard Alexander Galarza Mena con C.I. 0502965080 y Cristian Mauricio Jaya Condorcana con C.I. 0503854754, egresados de la Unidad Académica Ciencias de la Ingeniería y Aplicadas han realizaron su Propuesta Tecnológica en la EN LA EMPRESA G&S INGENIEROS.CIA LTDA con el tema **"MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA EN EL PERIODO 2020",** trabajo que fue presentado y aprobado de manera satisfactoria.

Es todo cuanto puedo certificar, permitiendo hacer uso del presente certificado para los fines legales pertinentes

Atentamente,

……

Ing. Christian Rubén Vaca Farinango

GERENTE DE G&S INGENIEROS.Cia Ltda

AGRADECIMIENTO

He pasado ya tanto tiempo en esta noble institución con buenos y malos momentos que he sabido sobre llevar gracias al apoyo que me han brindado principalmente Dios que me dio la bendición de todas las personas que han estado junto a mí en cada uno de los pasos para alcanzar uno de mis sueños más anhelados, mis padres que pese a todas las dificultades siempre está ahí para darme fuerzas y salir adelante, a mis hermanos Elizabeth y Steven que siempre están con sus ánimos para que no decaiga , gracias a mi familia que con su apoyo ayuda y comprensión han sido parte fundamental de mi vida .

Quiero agradecer también a la Universidad Técnica de Cotopaxi por darme la oportunidad de forjarme como profesional en sus establecimientos, a cada uno de los ingenieros que formaron parte de mi desarrollo educativo con su conocimiento y consejos

Cristian

AGRADECIMIENTO

Ante todo, agradezco a Dios por darme la vida de igual manera, por darme una madre luchadora y cariñosa que nunca se dio por vencida para que cumple este objetivo a pesar de las dificultades que se le presento. También agradezco al Ing. Jorge Rubio por brindarnos su conocimiento y tiempo al momento de realizar nuestra Propuesta Tecnológica, a su vez doy las gracias al Sargento Loachamin jefe del departamento de Sistemas de la Fuerza Area, quien también aporto con un granito de arena para poder llegar con el objetivo propuesto. Y para finalizar retribuyo a mis amigos de la universidad quienes me apoyaron con su moral y alegría.

Richard

DEDICATORIA

Todo este esfuerzo va dedicado para esas personas tan importantes en mi vida en especial para mis padres y en honor a la memoria de María Sebastiana Chicaiza querida y amada abuelita.

A su vez agradezco a mi mujer Yadira Guanoluisa quien me apoyado en todo momento.

Cristian

Este trabajo tecnológico lo dedico a mi madre Fanny Mena quien es mi inspiración y motivación, debido a que siempre me apoyado en la buenas y malas durante estos 6 años de vida universitaria las cuales fueron súper difíciles para nosotros. También dedico este triunfo a mi abuelita Mariana Regalado y a su mi padre Wilson Galarza que están en el cielo y sé que desde arriba de sentirán muy orgullosos de mi por haber cumplido un objetivo más en mi vida.

Richard

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TITULO: "MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA".

Autores:

Richard Alexander Galarza Mena

Cristian Mauricio Jaya Condorcana

RESUMEN

La presente propuesta tecnológica se desarrollará con la finalidad de instalar el protocolo IPV6 en la red de la empresa G&S INGENIEROS Cia.Ltda. aplicando el método de transición llamado "Tunneling" dentro de esta técnica se puede encontrar túneles configurados y automáticos es por ello que se dispuso a utilizar un túnel automático; llamado six to four tunnel, debido a que este túnel trabajará con un IP de origen y una IP de destino para poder comunicarse, a este proceso se le conoce como conexión de punto a punto y para el proceso de datos tendrá una encriptación PtP (Point-to-Point). Y, con ayuda de esta empresa que se mencionó anteriormente podremos trabajar de una manera eficaz debido a que trabaja con un proveedor de internet que ofrece IPV4; como bien sabemos en la actualidad este protocolo trabaja con 32 bits y esto provoca un colapso de dirección; debido al número de computadoras y otros dispositivos que se conectan a internet, por ende es necesario implementar redes locales con protocolos de IPV6 dentro de la empresa, gracias a sus 128 bits que trabaja y estos son capaces de adaptarse a un número significativo de conexiones, además que brinden seguridad y una velocidad adecuada a la hora del envío y recepción de la información que se maneja por parte de los usuarios.

Palabras claves: Migración de datos, Protocolo IPV4, Protocolo IPV6, Tunneling, Seguridad y velocidad en la red, six to four tunnel, PtP (Point-to-Point).

……

Ing. Mgs. Jorge Bladimir Rubio Peñaherrera
CC: 050222229-2
Tutor de Titulación

COTOPAXI TECHNICAL UNIVERSITY

FACULTY OF ENGINEERING SCIENCES AND APPLIED

TITLE: "MIGRATION OF DATA FROM IPV4 TO IPV6 THROUGH THE BROKER TUNNEL METHOD IN THE COMPANY G&S INGENIEROS. LTDA CIA".

Authors:

Richard Alexander Galarza Mena

Cristian Mauricio Jaya Condorcana

ABSTRACT

This technological proposal will be developed with the aim of installing the IPV6 protocol on the network of the company G&S INGENIEROS Cia.Ltda. applying the transition method called "Tunneling" within this technique you can find configured and automatic tunnels, that is why it was arranged to use an automatic tunnel; called a six to four tunnel, because this tunnel will work with a source IP and a destination IP to communicate, this process is known as point-to-point connection and for the data process will have PtP (Point-to-Point) encryption. And, with the help of this company mentioned above we will be able to work effectively because it works with an Internet provider that offers IPV4; as we know today this protocol works with 32 bits and this causes a direction collapse; due to the number of computers and other devices that connect to the internet, it is therefore necessary to implement local networks with IPV6 protocols within the company, thanks to their 128 bits that work and these are able to adapt to a significant number of connections in addition to providing security and an adequate speed when sending and receiving information that is handled by users.

Keywords: Data Migration, IPV4 Protocol, IPV6 Protocol, Tunneling, Network Security and Speed, Six to four tunnel, PtP (Point-to-Point).

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que: La traducción del resumen de la Propuesta Tecnológica al Idioma Inglés presentado por los señores de la Carrera de **Ingeniería en Informática y Sistemas Computacionales** de la **Facultad de Ciencias de la Ingeniería y Aplicadas: Richard Alexander Galarza Mena**, portador de la C.I. **050296508-0** y **Cristian Mauricio Jaya Condorcana**, portador de la C.I. **050385475-4** cuyo título versa **"MIGRACIÓN DE DATOS DE IPV4 A IPV6 A TRAVÉS DEL METODO DE TUNNEL DE BROKER EN LA EMPRESA G&S INGENIEROS.CIA LTDA**" lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente certificado de la manera ética que estimaren conveniente.

Latacunga, Septiembre 2020

Atentamente,

Mgc. Emma Herrera
DOCENTE CENTRO DE IDIOMAS
C.C. 050227703-1

1. INFORMACIÓN GENERAL.

1.1. Propuesto por:

Richard Alexander Galarza Mena y Cristian Mauricio Jaya Condorcana

1.2. Tema aprobado:

Migración de datos de ipv4 a ipv6 a través del método de Tunnel de Broker en la empresa G&S INGENIEROS.Cia Ltda.

1.3. Carrera:

Ingeniería en Informática y Sistemas Computacionales

1.4. Director del proyecto de titulación:

Mgs. Ing. Jorge Bladimir Rubio Peñaherrera

1.5. Equipo de Trabajo:

Datos personales del coordinador de proyecto de investigación:

Nombres: Jorge Bladimir

Apellidos: Rubio Peñaherrera

Fecha de nacimiento: 16 de mayo de 1976

Teléfonos: 0995220308

E-mail: jorge.rubio@utc.edu.ec

Estudios: Universidad Técnica de Cotopaxi

Pontificia Universidad Católica del Ecuador sede Ambato.

Títulos obtenidos: Ingeniero en Informática y Sistemas Computacionales

Diploma Superior en Gerencia Informática

Magister en Gerencia Informática mención Desarrollo de Software y Redes

Datos Personales del Autor:

Nombres: Cristian Mauricio

Apellidos: Jaya Condorcana

Fecha de nacimiento: 30 de enero de 1996

C.C: 0503854754

Teléfono: 0983979945

Correo electrónico: cristian.jaya4754@utc.edu.ec

Estudios: Universidad Técnica de Cotopaxi (UTC)

Datos Personales del Autor:

Nombres: Richard Alexander

Apellidos: Galarza Mena

Fecha de nacimiento: 3 de septiembre de 1996

C.C: 050296508-0

Teléfono: 0984235740

Correo electrónico: richard.galarza5080@utc.edu.ec

Estudios: Universidad Técnica de Cotopaxi (UTC)

1.6. Lugar de ejecución:

Provincia Cotopaxi, Cantón Latacunga, Parroquia La Matriz.

1.7. Tiempo de duración del proyecto:

6 meses

1.8. Fecha de entrega:

13 de febrero del 2020

1.9. Línea de investigación:

Tecnologías de la Información y Comunicación:

1.10. Sub líneas de investigación de la Carrera:

Diseño, Implementación y configuración de Redes y Seguridad Computacional, Aplicando normas y estándares internacionales.

1.11. Tipo de propuesta tecnológica

Migración de datos

2. DISEÑO INVESTIGATIVO DE LA PROPUESTA TECNOLÓGICA

2.1. TITULO DE LA PROPUESTA TECNOLÓGICA

Migración de datos de ipv4 a ipv6 a través del método de Tunnel de Broker en la empresa G&S INGENIEROS.Cia Ltda.

2.2. TIPO DE PROPUESTA ALCANCE

Desarrollo:

Migración de datos de Ipv4 a Ipv6 en la empresa G&S INGENIEROS.Cia Ltda. con el objetivo de mejorar la red y la seguridad ya que el nuevo protocolo serás más rápido al momento de navegar y enviar paquetes ya que trabajara con 128 bits.

2.3. ÁREA DE CONOCIMIENTO

Área: Ciencias

Sub-área: Informática

2.4. SINOPSIS DE LA PROPUESTA TECNOLOGICA

Tecnológicamente, esta tesis propone migrar los datos de Ip4 a Ipv6 utilizando el método de Tunnel de Broker debido a que esta técnica evita las dependencias al momento de actualizar los Routers y los hosts; permitiéndoles que tengan una red más segura, más rápida y actual. Institucionalmente, el trabajo de investigación beneficiará directamente a la empresa G&S INGENIEROS.Cia Ltda. por cuanto mejorará el rendimiento de la red y la respectiva seguridad de la información que se maneje y por ende se brindará un mejor servicio a terceros.

2.5. OBJETO DE ESTUDIO Y CAMPO DE ACCIÓN

2.5.1. Objeto de estudio

Mejorar la velocidad y la seguridad en la red de una manera eficiente en la empresa G&S INGENIEROS. Cía. Ltda.

2.5.2. Campo de acción

Migración de datos de IPv4 a IPv6 a través del método de Tunnel de Broker.

2.6. SITUACIÓN PROBLEMÁTICA Y PROBLEMA.

2.6.1. Situación problemática.

A partir de la investigación de [1] menciona que en la actualidad el número de usuarios que recurren a la internet ha aumentado de forma considerable por ende las direcciones IPv4 ha sido una preocupación desde los años 80, debido a que existe una gran demanda de dispositivos que deben estar conectados de forma permanente a una red, desde el año 1981 el protocolo IPv4 con 4.3 millones de direcciones ha sido el encargado de llevar una conexión a través del internet, en su momento ingresó en una fase de agotamiento debido a que esta dirección se encuentra saturado y no permite el crecimiento de la infraestructura tecnológica. Una de las partes fundamentales de la infraestructura de Internet y de las todas las redes de computadoras es el protocolo IP. La versión del protocolo que se ha ido utilizando por mucho tiempo, por su gran poder y escalabilidad, fue el protocolo IPv4, pero desafortunadamente IPv4 quedó pequeño para todo el desarrollo y crecimiento de aplicaciones de las redes de computadoras que actualmente existen. Es por ello que la IETF decidió dar el paso como parte de la evolución misma de IP para llegar a su nueva versión la cual denominaron IPv6 o IPng.

El mencionado protocolo ha comenzado desplegándose en el continente europeo aproximadamente desde el 2002, pero la penetración en Suramérica es prácticamente inexistente y en países en vía de desarrollo se está quedando rezagado. A principios del 2011 se ha conocido que, INTERNEXA distribuidor de redes de telecomunicaciones terrestres se convierte en una empresa pionera en el continente que integra protocolo IPv6 en cada uno de sus 21.217 KM de red de fibra óptica a lo largo de Venezuela, Colombia, Perú, Ecuador, Chile y en los próximos meses, Argentina y Brasil.

En el Ecuador, la primera institución en facilitar la apertura al Internet fue Ecuanex, el cual es un nodo de Internet creado por la Corporación Interinstitucional de Comunicación Electrónica. Esta red integra la red mundial del Institute for Global Communications/Alliance for Progressive Communications (IGC/APC), que brinda este servicio a las organizaciones no gubernamentales y de desarrollo[2].

La Corporación Ecuatoriana de Información, estableció en octubre de 1992 otro nodo, Ecuanet. una entidad sin fines de lucro patrocinado por el Banco del Pacífico, la ESPOL, la Universidad Católica Santiago de Guayaquil y otras entidades. Dicha red se conecta directamente al NSFNET, por medio del sistema de comunicaciones del Banco Pacífico[2].

Algunas Instituciones públicas en el Ecuador a partir del año 2012, iniciaron con planes de investigación para realizar análisis de lo que conlleva los aspectos administrativos, económicos y técnicos para que si en un momento dado quisieran hacer una migración a Ipv6 les sirva como guía y tengan conocimiento sobre una migración.[3] IPv4 demuestra algunos inconvenientes en las instituciones como por ejemplo se ha tomado la F.C.A. como modelo para analizar los inconvenientes que presenta como es el desperdicio de banda de ancha, bajo rendimiento al momento de la transmisión, la poca seguridad al momento de enviar paquetes de datos.

En la empresa G&S INGENIEROS.Cia Ltda. ubicada en la provincia de Cotopaxi cantón Latacunga trabajan con el protocoló IPV4 lo cual es preocupante debido a que esta IP fue creada en la década de los 70 con una estructura de 32 bits y ahora que estamos en pleno siglo XXI puede ocurrir que se eleve el número de usuarios de internet, también puede existir saturación en las direcciones o a su vez tener problemas en la arquitectura, gracias a que se siguen creando más servicios y estos están alojados en la red del internet. De tal manera que después de un tiempo la empresa no pueda adquirir más equipos, la velocidad de la red puede empeorar y en cuanto a la seguridad pueda estar expuesta a ataques cibernéticos.

2.6.2. Problema.

En la empresa G&S INGENIEROS.Cia Ltda. ubicada en la provincia de Cotopaxi cantón Latacunga trabajan con el protocoló IPV4 lo cual es preocupante debido a que esta IP fue creada en la década de los 70 con una estructura de 32 bits y ahora que estamos en pleno siglo XXI puede ocurrir que se eleve el número de usuarios de internet, también puede existir saturación en las direcciones o a su vez tener problemas en la arquitectura, gracias a que se siguen creando más servicios y estos están alojados en la red del internet. De tal manera que después de un tiempo la empresa no pueda adquirir más equipos, la velocidad de la red puede empeorar y en cuanto a la seguridad pueda estar expuesta a ataques cibernéticos.

2.7. HIPÓTESIS O FORMULACIÓN DE PREGUNTAS DIRECTRICES.

¿Si aplica la migración de datos de Ipv4 a Ipv6 a través del método de Tunnel de Broker, se podrá mejorar la velocidad y la seguridad en la red de una manera eficiente en la empresa G&S INGENIEROS.Cia Ltda.?

2.7.1. Variable independiente.

Migración los datos de Ipv4 a ipv6 a través del método de Tunnel de Broker.

2.7.2. Variable dependiente.

Mejorar la velocidad y la seguridad en la red de una manera eficiente en la empresa G&S INGENIEROS.Cia Ltda.

2.8. OBJETIVOS.

2.8.1. Objetivo General.

Migrar los datos de IPV4 a IPV6 a través del método de Tunnel de Broker para de esta manera mejorar la velocidad y seguridad en la red de la empresa G&S INGENIEROS.Cia Ltda.

2.8.2. Objetivos Específicos.

- Realizar una investigación del estado del arte acerca de la migración de datos de Ipv4 a Ipv6 en la actualidad, mediante fuentes bibliográficas confiables.
- Describir la fundamentación teórica del protocolo de internet y de la coexistencia entre protocolos IPv4 e IPv6.
- Explicar los diferentes mecanismos de transición de IPv4 a IPV6, para detallar las ventajas y desventajas al momento de migrar datos al nuevo protocolo.
- Implementar el método de transición más adecuado para migrar los datos de IPv4 a Ipv6 dentro de la empresa G&S INGENIEROS.Cia Ltda.

2.8.2.1. Tareas.

- ✓ Revisar en fuentes bibliográficas todo lo relacionado con a la migración de datos e Ipv4 a Ipv6.
- ✓ Investigar sobre el protocolo de internet y la coexistencia entre protocolos IPv4 e IPv6.
- ✓ Estudiar los mecanismos de transición, con sus respectivas ventajas y desventajas para poder migrar datos al nuevo protocolo.
- ✓ Después de analizar los mecanismos de transición, seleccionamos el método adecuado para realizar la migración de datos en la empresa G&S INGENIEROS.Cia Ltda.

2.9. DESCRIPCIÓN DEL DESARROLLO DE LAS ACTIVIDADES Y TAREAS EN RELACIÓN A LOS OBJETIVOS PLANTEADOS.

La **Tabla 1.** que se enseña a continuación, detalla la relación de los objetivos con las actividades, descripción y los resultados de las actividades con el fin de obtener una secuencia lógica en el desarrollo de presente proyecto.

Tabla 1. Sistema de tareas en relación a los objetivos planteados.

Objetivos	Actividades	Resultados	Medios de verificación
Realizar una investigación del estado del arte acerca de la migración de datos de Ipv4 a Ipv6 en la actualidad, mediante fuentes bibliográficas confiables.	Revisar información bibliográfica de libros, tesis y artículos científicos. Lectura de la información recogida de todo lo relacionado con a la migración de datos e Ipv4 a Ipv6	Fundamentación teórica confiable del proyecto de investigación.	Libros Revistas científicas Tesis
Describir la fundamentación teórica del protocolo de internet y de la coexistencia entre protocolos IPv4 e IPv6.	Escritura de la fundamentación teórica encontrada. Analizar investigaciones similares	Diagnostico amplio del protocolo de internet con relación al ipv4 e ipv6.	Investigación documental Revistas científicas
Explicar los diferentes mecanismos de transición de IPv4 a IPV6, para detallar	Estudiar los mecanismos de transición más relevantes.	Selección del método para implementar en dicha empresa.	Investigación documental de configuraciones Anexos

las ventajas y desventajas al momento de migrar datos al nuevo protocolo.	Analizar el mecanismos de transición, trabajaremos con el método de Tunnel de Broker	Asociarse con método de tunelización	
Implementar el método de transición más adecuado para migrar los datos de IPv4 a Ipv6 dentro de la empresa G&S INGENIEROS.Cia Ltda.	Implementación del método seleccionado. Configuraciones en los dispositivos -Tipo de encapsulamiento - Tipo de cableado	Envío y recepción de paquetes.	Prototipos Investigación documental

Fuente: Grupo de investigación.

3. MARCO TEÓRICO

3.1. Antecedentes.

En el presente trabajo especial de grado se analizaron diversas fuentes de información relacionadas con el tema, orientándose directamente con la transición al nuevo Protocolo de Internet (IP). A continuación, se exhibirán algunos trabajos de investigación elaborados previamente:

En septiembre 11 el autor [4] presento ante la Escuela de Ingeniería en Telecomunicaciones de la Universidad Católica Andrés Bello el trabajo especial de grado titulado “Estudio sobre la red de la empresa NETUNO para la implementación de IPv6 en su plataforma de multiservicio para el segundo semestre de 2011". Esta investigación se enfoca en el área de Redes o Telemática y concluye que el método más idóneo y eficiente para su implementación es Dual Stack logrando así la convivencia IPv4/IPv6. Sin embargo, indican que este mecanismo debería trabajar con los Túneles para obtener un funcionamiento más óptimo de la red.

En la tesis propuesta por el autor[5], “Propuesta de un plan de implementación para la migración a IPv6 en la red de la Universidad Politécnica Salesiana sede Cuenca-Ecuador” nos habla que

el objetivo de la propuesta es realizar un análisis de los mecanismos y requerimientos necesarios para llevar a cabo el proceso de transición en la red de datos de la universidad mencionada, para ello deciden estructurar cuatro actividades concretas, analizar la situación actual del cableado estructurado de la red, investigar distintos mecanismos de transición, analizar ventajas y desventajas de la migración y desarrollar el plan de implementación para la migración de IPv4 a IPv6.

También el autor [6] presentó ante la Escuela de Ingeniería en Telecomunicaciones de la Universidad Católica Andrés Bello el trabajo especial de grado titulado "Diseño de una estrategia de migración de la red actual de la Universidad Católica Andrés Bello a una red basada en IPv6". Teniendo como propósito diseñar una estrategia de transición para la migración a una red basada en IPv6, concluyendo que el mejor mecanismo de transición para su migración es Dual Stack a nivel de servidores, túnel TEREDO en caso de trabajar con direcciones privadas y túnel 6to4 en caso de trabajar con direcciones públicas.

Por otra parte, el autor [7], presenta en agosto de 2009 ante la Escuela Politécnica Nacional (Quito, Ecuador), el proyecto titulado "Estudio para la Evaluación de Mecanismos de Migración de IPv4 a IPv6 para la empresa proveedora de Internet MILLTEC S.A", en la cual concluye la migración a IPv6 es posible y factible pero es un proceso que lleva tiempo, se puede afirmar que los cambios requeridos son a nivel de software y la mayoría de los equipos en la actualidad cuentan con soporte para IPv6.

Según el autor[8], presenta la investigación con el propósito de la transición del protocolo ipv4 hacia ipv6 en la agencia colombiana para la reintegración- ACR con base en consideraciones de seguridad en implementación de ipv6 basándose en lineamientos dados por el Gobierno se hace un plan diagnóstico y seguido se propone una estrategia para llevar a cabo la transición. Finalmente se concluye que el proceso de transición permitirá que se trabajen a la par el protocolo versión 4 y el protocolo versión 6, lo que no afectará de manera abrupta los procesos cotidianos en la ACR. Por otra parte, se recomienda ir realizando una transición parcial, diseñar un segmento de red para realizar pruebas y así evitar problemas en aplicaciones críticas de la entidad.

El autor[9] en la siguiente propuesta tecnológica nos habla de un diseño del plan de migración y seguridad de IPv4 a IPv6 para una red educativa, sostiene que ante la sensible condición y desventajas del direccionamiento IPv4, considera que las instituciones deben estudiar la nueva versión del protocolo de internet IPv6, incluyendo la correcta configuración de los dispositivos

de red de esta manera poder proteger el acceso a información debido a que el trabajo de titulación tiene como objetivo presentar una planificación con los cambios necesarios que se deben realizar en la red actual de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil para la migración de IPv6 analizando aspectos relacionados a las técnicas de transición y parámetros de administración de seguridad de red.

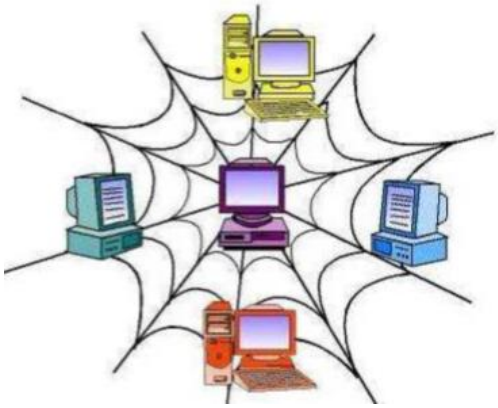
Algunas de las referencias observadas anteriormente dan a conocer la importancia de la transición a IPv6 y su implementación en diversas empresas e instituciones educativas, generando así un incentivo a nivel nacional e internacional para avanzar con la aplicación del nuevo Protocolo de Internet.

3.2. Marco conceptual.

3.2.1. Red de datos.

Conocido también como red de computadoras y red de comunicaciones.

Figura 1: Red de datos.



Fuente:[1]

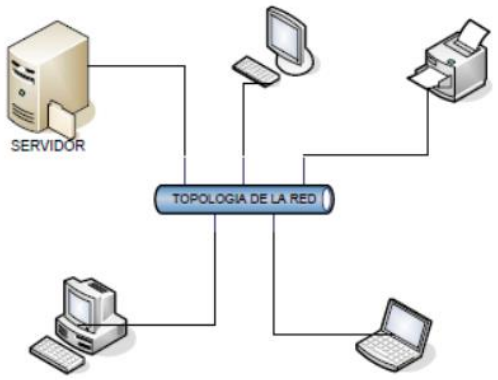
El autor [1] lo define como el conjunto de elementos de software y hardware conectados a través de dispositivos físicos que permiten él envió y la recepción de datos con la finalidad de compartir cualquier tipo de información véase la figura 1. De acuerdo al alcance de la transmisión de datos, puede ser red de área local(LAN), red de área metropolitana(MAN), red de área extensa(WAN) entre otras.

3.2.1.1. Red de área local (LAN).

(Local Area Network) son aquellas redes de propiedad privada como menciona el autor[10] que geográficamente están dentro de un área relativamente pequeña que se encuentran en un sólo edificio o campus de pocos kilómetros de longitud. La figura 2 muestra este tipo de red. Las

redes de área local tradicionales se ejecutan actualmente a una velocidad de 10 a 100 Mbps (Mega bits por segundo), pero según los últimos avances, estas redes podrían llegar a una velocidad medida en giga bits por segundo. Algunas de las topologías lógicas utilizadas en este tipo de redes, pueden ser Ethernet, Token Ring y FDDI, la más utilizada actualmente es Ethernet.

Figura 2: Ejemplo de red de área local.

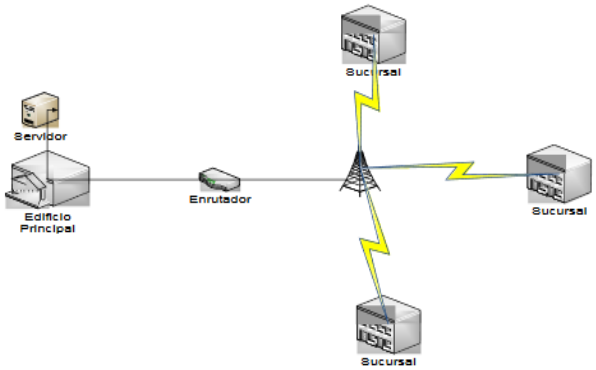


Fuente:[10]

3.2.1.2. Red de área metropolitana (MAN).

(Metropolitan Area Network) según[11] son aquellas redes que se encuentran localizadas en diferentes distribuidos en distancias no superiores al ámbito urbano, una MAN consta generalmente de dos o más redes LAN en un área geográfica común equivalente a una cuidad aproximadamente 10 kilómetros entre procesadores. Se utilizan para enlazar servicios tales como el control de tráfico y semáforos, servicios públicos como el internet y hasta servicios bancarios y comerciales. Este ejemplo de una red MAN se ilustra en la figura 3.

Figura 3: Ejemplo de red de área metropolitana.



Fuente:[11]

3.2.1.3. Red de área extensa.

Según[12] también se la conoce como WAN por sus siglas en inglés, Wide Area Network son redes que han sido diseñadas para operar entre área geográfica extensas, ofrecer recursos remotos de tiempo completo y en tiempo real, conectado a servicios locales para intercambiar información digital entre lugares distantes sean en el mismo país o en países diferentes, un continente e incluso un planeta. Esto quiere decir que se puede considerar Internet como una red WAN, pues ésta abarca todo el planeta. Las redes de área amplia se utilizan para interconectar las redes LAN que anteriormente mencionamos, una red WAN se ve ilustrada en la figura 4.

Figura 4: Ejemplo de una red de área extensa.

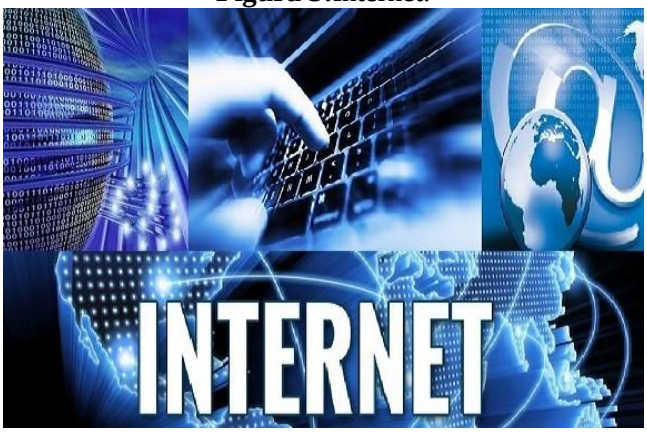
Fuente:[12]

En la figura 4 se observa una red WAN conectado por medio de un enlace serial, una red LAN hacia la nube del internet. Cabe mencionar que no necesariamente tiene que conectarse a internet, también se podría utilizar una WAN para interconectar dos LAN remotas que estén separados por una gran distancia.

3.2.2. Internet.

Luego de haber comprendido lo que es una red de computadoras y cuáles son los medios de transmisión físicos por donde viajan los datos o el término que el usuario común conoce como Internet: El autor [13] define a el Internet como una red integrada por miles de redes y computadoras interconectadas en todo el mundo mediante cables y señales de telecomunicaciones, que utilizan una tecnología común para la transferencia de datos.

Figura 5: Internet.



Fuente: [13]

3.2.2.1. Protocolos de internet.

Según [14] TCP/IP, proviene de dos de los protocolos más importantes de la familia de protocolos de internet, Transmission Control Protocol (TCP) y el Internet Protocolo (IP), lo cual es la base del Internet debido a que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa.

Para [15] los protocolos TCP e IP son muy significativos. Su nombre representa al conjunto de protocolos que conforman la arquitectura formada por cinco niveles o capas, los cuales como se observa en la siguiente **Tabla 2**.

1. **Aplicación.** Están contenidos los protocolos SMTP, para el correo electrónico; FTP, para las transferencias de archivos; TELNET, para la conexión remota, y HTTP, Hypertext Transfer Protocol.
2. **Transporte.** Se comprende a los protocolos TCP y UDP, que se ocupan del manejo y el transporte de los datos.
3. **Internet.** Se ubica en el nivel de la red para enviar los paquetes de información.
4. **Físico**. Es el análogo al nivel físico del OSI.
5. **Red.** Es el correspondiente a la interfaz de la red.

Tabla 2. Modelo TCP/IP.

TCP/IP	
Niveles	**Protocolos**
1. Aplicación	FTP, HTTP, SSH, SSL, Telnet, SMTP, NFS, etc.
2. Transporte	TCP, UDP

3. Internet	IP , ICMP, ARP, RARP
4. Físico	Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, etc.
5. Red	Ethernet, CSMA, Token-ring, ATM, etc.

Fuente: Grupo de investigación.

3.2.3. Direcciones Ip.

Según [16] una dirección Ip consiste en "32 bits que normalmente se expresan en forma decimal, en cuatro grupos de tres dígitos separados por puntos, tal como 167.216.245.249. Cada número estará entre cero y 255. Cada número entre los puntos en una dirección IP se compone de 8 dígitos binarios (00000000 a 11111111); los escribimos en la forma decimal para hacerlos más comprensibles, pero hay que tener bien claro que la red entiende sólo direcciones binarias".

Figura 6: Dirección IP.

Fuente:[17]

3.2.3.1. Clases de direcciones IP.

Podemos clasificar las direcciones Ip dependiendo de diferentes criterios: desde el punto de vista de la accesibilidad, desde el punto de vista de la perdurabilidad y dependiendo de la clase.

Accesibilidad.

- **Direcciones IP públicas:** aquellas que son visibles por todos los hosts conectados a Internet. Para que una máquina sea visible desde Internet debe tener asignada obligatoriamente una dirección IP pública, y no puede haber dos hosts con la misma dirección IP pública.
- **Direcciones IP privadas:** aquellas que son visibles únicamente por los hosts de su propia red o de otra red privada interconectada por medio de routers. Los hosts con direcciones IP privadas no son visibles desde Internet, por lo que si quieren salir a ésta

deben hacerlo a través de un router o un proxy que tenga asignada una IP pública. Las direcciones IP privadas se utilizan en redes privadas para interconectar los puestos de trabajo.

Perdurabilidad.

- **Direcciones IP estáticas:** Son direcciones estáticas aquellas asignadas de forma fija o permanente a un host determinado, por lo que cuando una máquina con este tipo de IP se conecte a la red lo hará siempre con la misma dirección IP. Normalmente son usados por servidores web, routers o máquinas que deban estar conectadas a la red de forma permanente, y en el caso de direcciones IP públicas estáticas hay que contratarlas, generalmente a un ISP (proveedor de Servicios de Internet).
- **Direcciones IP dinámicas:** aquellas que son asignadas de forma dinámica a los hosts que desean conectarse a Internet y no tienen una IP fija. Un ejemplo típico de este tipo de direcciones IP es el de una conexión a Internet mediante módem. El ISP dispone de un conjunto de direcciones IP para asignar a sus clientes, de forma que cuando uno de ellos se conecta mediante módem se le asigna una de estas IP, que es válida durante el tiempo que dura la conexión. Cada vez que el usuario se conecte lo hará pues con una dirección IP distinta.

3.2.4. ISP (Internet Service Provider).

Según [18] los proveedores de servicio de Internet (ISP, Internet Service Provider) son empresas que proporcionan el servicio de acceso a Internet alámbrico e inalámbrico mediante una cuota mensual. El costo del servicio de acceso a internet varía de acuerdo a la velocidad de conexión. En caso de que el servicio de conexión utilice banda ancha usa medios como ISDN (Integrated Services Digital Network), inalámbricos, cable coaxial, o Ethernet.

El servicio de conexión de banda ancha puede ser a través de la línea telefónica. También es posible contratar conexiones por Satélite. Las velocidades de la conexión de banda ancha van de 64kbps hasta 1GB.

Figura 7: ISP (Internet Service Provider).

Fuente: [12]

3.2.5. Protocolo de internet versión 4 (Ipv4).

3.2.5.1. Definición.

Según[19] este protocolo fue diseñado para permitir la trasmisión de datos a través de redes de comunicaciones, incluyendo la red Internet. Definido en la capa de red del modelo de referencia (OSI). Esta Ip tiene como misión encaminar o enrutar los datos hacia su destino, entregando la información generada en la capa de red, sin comprobar la integridad del contenido.

Figura 8: Protocolo versión 4.

Fuente:[20]

3.2.5.2. Desventajas:

Según[20] estos son los principales aspectos negativos que tiene el protocolo IPv4.

- ✓ Es un protocolo de un servicio de mensaje no fiable.
- ✓ No proporciona garantía de entrega de datos.

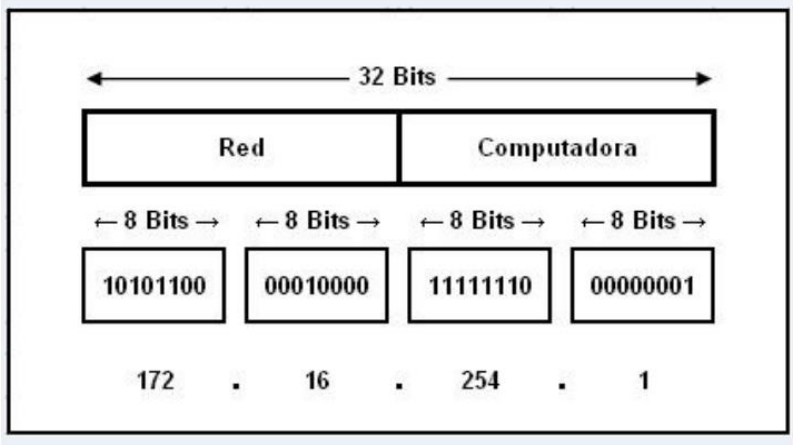
- ✓ No proporciona garantía sobre corrección de los datos.
- ✓ Hace llegar paquetes duplicados.
- ✓ Esta versión es capaz de generar aproximadamente 4.000 millones de combinaciones.

3.2.5.3. Formato de los paquetes de IPV4.

Según[21] Una dirección IP versión 4 tiene una longitud de 32 bits que están divididos en 4 grupos de 8 bits, separados por puntos y que son representados de forma decimal Cada bit en el octeto tiene un peso binario. El valor mínimo para un octeto es 0 y el valor máximo es 255.

A continuación, se muestra el formato básico de esta dirección IP con sus 32 bits agrupados en 4 octetos

Figura 9: Protocolo versión 4.

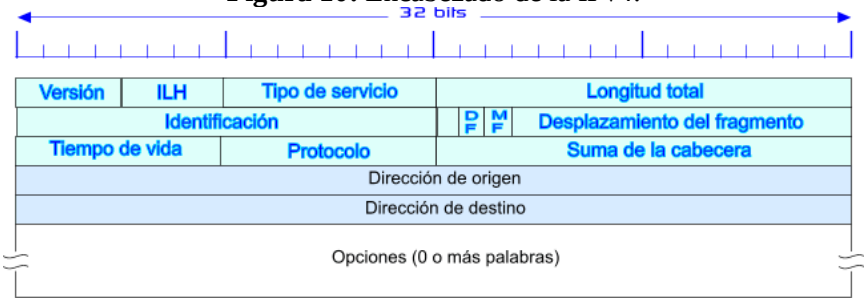


Fuente: [22]

3.2.5.4. Cabecera del protocolo IPv4.

Según [23] un datagrama es un paquete de datos que constituye el mínimo bloque de información en una red.

Figura 10: Encabezado de la IPv4.



Fuente:[1]

A continuación, en la siguiente **Tabla 3** se muestra el significado de cada una de las partes de un datagrama IPv4.

Tabla 3. Partes de un datagrama IPv4.

Nombre	Significado
Versión	Indica o lleva el registro de la versión del protocolo al que pertenece el datagrama.
I.H.L. (Internet Header Length),	Especifica la longitud en palabras de 32 bits, el valor mínimo es de 5, cifra que se aplica cuando no hay opciones, el valor máximo de este campo de 4 bits es el 15.
Tipo de servicio	Aquel que permite saber la importancia de los datos enviados, determinando la forma en que serán tratados en la transmisión de 8 bits.
Campo longitud total	Indica la longitud completa en bytes del datagrama de 16 bits, incluyendo el encabezado y los datos.
Campo identificación	Importante en el ensamblaje de un datagrama cuando están viajando, debido a que cuando llega un fragmento a una computadora tiene un valor en donde está indicando a que paquete pertenece.
Desplazamiento de Fragmento.	En paquetes fragmentados indica la posición. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.
Campo TTL (tiempo de vida)	Es un contador que se utiliza para limitar el tiempo de vida de un paquete, para que el paquete no ande vagando en la red.
Protocolo	Indica el protocolo de las capas superiores al que debe entregarse el paquete, es decir, qué hacer con el datagrama que está manejando.
Suma de verificación del encabezado	Verifica únicamente el encabezado, permite controlar su integridad para establecer si se ha modificado durante la transmisión.
Dirección IP de origen.	Indican el número de red y el número de host del remitente y permiten que el destinatario responda.
Dirección IP de destino	Indican el número de red y el número de host del destinatario

Fuente: Grupo de investigación.

3.2.6. Protocolo de internet versión 6 (Ipv6).

3.2.6.1. Definición.

Según [24] el protocolo IPv6 es “la nueva versión del protocolo IP, llamado también protocolo de la siguiente generación. Ha sido diseñado por el IETF (Fuerza de Tareas de Ingeniería de

Internet) para reemplazar en forma gradual a IPv4". Este protocolo IPv6 incorpora nuevas características con respecto a IPv4 como mayor espacio de direccionamiento, calidad de servicio (QoS), seguridad (IPsec), y movilidad, cubriendo de esta forma con las principales necesidades de los clientes.

Figura 11: Protocolo de internet versión IPv6.

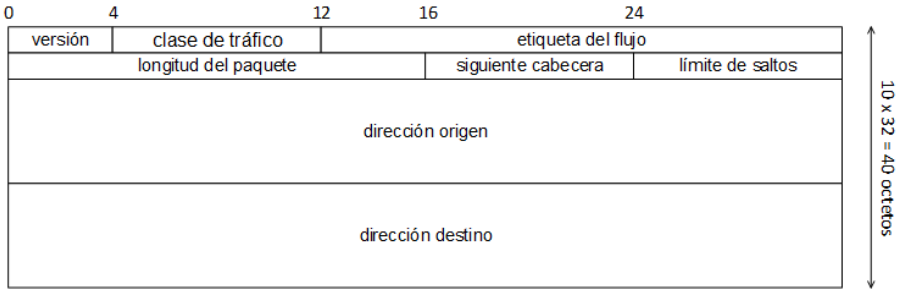
Fuente: [24]

3.2.6.2. Cabecera IPv6.

El autor[25] menciona que el protocolo IPv6 es un protocolo que permite aumentar el tamaño de direcciones IP de 32 a 128 bits, es decir 2^128 posibles direcciones, que se pueden mostrar como 32 dígitos hexadecimales. Este aumento en el espacio de direcciones no sólo proporciona mayor número de hosts, sino una jerarquía de direcciones mayor suficiente para las necesidades de crecimiento.

La cabecera IPv6 elimina o hace opcionales varios de los campos de la cabecera IPv4, con el fin de obtener una cabecera de tamaño fijo, más simple y reduciendo el tiempo de procesamiento de los paquetes.

Figura 12: Protocolo de internet versión IPv6.



Fuente : [26]

3.2.6.3. Direccionamiento IPv6.

Según[27] en IPv6 se han identificado diferentes tipos de direcciones entre ellos tenemos.

- **Unicast.**

Identifican a una interfaz única, esto quiere decir, que un paquete destinado a una dirección unicast será entregado únicamente a la interfaz identificada con dicha dirección. Dicha dirección se divide en 5 grupos las cuales son:

1) Direcciones link-local: Siempre comienza con el prefijo FE80::/10. Estas direcciones son utilizadas por los nodos para comunicarse con nodos vecinos dentro de un mismo enlace.
2) Direcciones Globales: Estas direcciones son enrutables y accesibles a nivel global sobre la porción de IPv6 en Internet. Las direcciones globales pueden ser sumarizadas para lograr un enrutamiento más eficiente, como también en IPv6 equivalen a las direcciones públicas utilizadas en IPv4. Que poseen el rango de direcciones 2000: :/16 a 3FFF::/ 16.
3) Direcciones site-local: sirven para identificar las interfaces de una misma área topológica perteneciente a un edificio o campus. Estas direcciones son equivalentes a las direcciones privadas de IPv4 y no son accesibles desde otros sitios. Los routers no deben enviar tráfico site-local fuera de la organización correspondiente. Cabe mencionar que siempre comienzan en fecO::.
4) Direcciones especiales IPv6: en Ipv6 existen dos tipos de direcciones especiales, las no especificadas (“0:0:0:0:0:0:0:0” o "::") que indican la ausencia de una dirección y las direcciones de loopback (0:0:0:0:0:0:0: 1 ó ::1), lo que le permite a un nodo enviarse paquetes a sí mismo.
5) Direcciones Compatibles: ayudan a la migración de IPv4 a IPv6, existen cuatro tipos de direcciones, las cuales son: direcciones 6to4, direcciones IPv4 compatibles, direcciones 6over4 y direcciones ISATAP. En el caso de 6to4 el prefijo utilizado es el 2002::/ 16.

- **Anycast.**

Como se mencionó este tipo de direcciones permite enviar un datagrama a un nodo que pertenece a un grupo de nodos que puede estar en la misma subred o topológicamente en diferentes enlaces de una red, con la propiedad que ese datagrama que es enviado a una dirección Anycast es enrutada a la interface más cercana que tenga dicha dirección, de acuerdo a las métricas de distancia de los protocolos de enrutamiento.

El mecanismo Anycast es usado para descubrir los servicios en una red o para proveer una redundancia. Un posible futuro uso de las direcciones Anycast es para identificar el conjunto de enrutadores que pertenecen a una organización que provee el servicio de Internet[27]. Otro

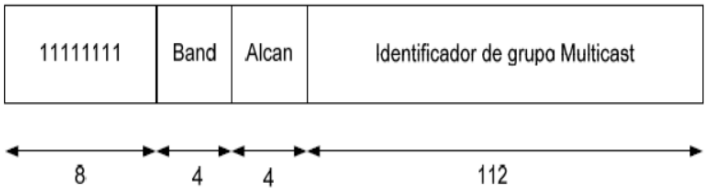
posible uso es para identificar el conjunto de enrutadores que pertenecen a una subred en particular.

- **Multicast.**

Una dirección IPv6 Multicast es un identificador de un grupo de interfaces. Multicast permite hacer un uso eficiente del ancho de banda al enviar un número mínimo de datagramas a un número máximo de nodos, es un mecanismo de direccionamiento de uno a varios[28]. Un prefijo especial identifica a un datagrama multicast, y una dirección especial dentro de ese prefijo identifica a cada grupo de nodos, una dirección Multicast IPv6 debe iniciar con un valor hexadecimal de "FF" en su primer octeto.

Cabe mencionar que IPv4 utiliza el Broadcast para varios propósitos. En su lugar IPv6 utiliza Multicast. Este permite enviar datagramas con objetivos más específicos a varios nodos en una red. Por ejemplo, los enrutadores IPv6 intercambian información específica usando una dirección específica en todos los enrutadores, el formato de una dirección Multicast se muestra en la figura 13**.**

Figura 13: Formato de una dirección Multicast.



Fuente:[27]

A continuación, se muestra en la **Tabla 4**. el resumen con los tipos de direcciones IPv6 y sus prefijos correspondientes.

Tabla 4. Tipos de direccionamiento y sus prefijos.

Tipo de dirección	Prefijo
Link-Local	FE80::/10
Unspecified	::/128
Loopback	::1/128
Global Unicast	2000::/3
Direcciones 6to4	2000::/16
Multicast	FF00::/8

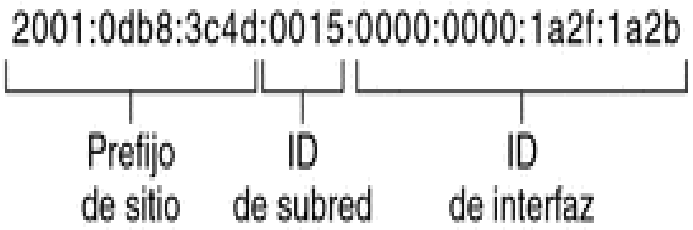
Anycast	

Fuente: Grupo de Investigación.

3.2.6.4. Formato de una dirección Ipv6.

Para[29] las direcciones IPv6 están compuestas con 8 campos de 16 bits de largo, que se encuentran separados por dos puntos (:), el cual cada campo está representado por 4 caracteres hexadecimales (0-f). Un ejemplo de la dirección IPv6 se muestra en la siguiente figura 14.

Figura 14: Formato de la dirección IPv6.



Fuente:[29]

Se puede aplicar las siguientes reglas a la dirección IPv6 con la única finalidad de simplificar la escritura y de esta manera poderla memorizar.

1. No se hace distinción entre mayúsculas y minúsculas. “ABC9” es equivalente a “abC9“.
2. Los ceros al inicio de un campo son opcionales. “0db8” es equivalente a “db8”.
3. Una sucesión de campos con ceros puede ser reemplazados por “::” por ejemplo “2001:0000:0000:abc9” es igual a “2001::abc9”.

3.2.7. Tipos de enrutamiento.

El enrutamiento en IPv6 es el proceso mediante el cual se mantiene una tabla de enrutamiento actualizada ya sea estáticamente o dinámicamente, tal como se hace en IPv4. Para enviar un paquete IPv6 más allá de los medios de comunicación locales se requiere de un enrutador[23]v. Los enrutadores verifican la dirección destino del paquete IPv6 y buscan el prefijo que le corresponde dentro de su tabla de enrutamiento. Una vez que el enrutador haya encontrado el prefijo para llegar al destino, entonces el paquete es reenviado de acuerdo con la información del siguiente salto. Si los enrutadores no encuentran la correspondencia en su tabla de enrutamiento, entonces el paquete es desechado.

Al igual que en IPv4, el enrutamiento en IPv6 se puede hacer estático o dinámico, y dentro del enrutamiento dinámico existen los mismos protocolos de enrutamiento, pero con algunas modificaciones necesarias para poder soportar el nuevo protocolo IPv6.

3.2.7.1. Enrutamiento Dinámico.

Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia[5]. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

3.2.7.2. Enrutamiento Estático.

Este enrutamiento define las rutas que los paquetes viajan por la red. Al configurar manualmente las rutas estáticas para redes pequeñas ya no es necesario utilizar protocolos de enrutamiento dinámico[12].

Los dispositivos Ethernet reenvían los paquetes con información de la ruta que está configurado de formas manuales aprendidas mediante el protocolo de enrutamiento estático, además definen un camino de modo explícito entre dos dispositivos de red. A diferencia de un protocolo de enrutamiento dinámico, las rutas estáticas no se actualizan automáticamente y debe volver a configurar manualmente si cambia la topología de la red.

3.2.7.3. Las ventajas de usar rutas estáticas:

- Incluyen la seguridad y la eficiencia de los recursos.
- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
- Las rutas estáticas utilizan menos ancho de banda que protocolos de enrutamiento dinámico y ciclos de CPU no se utilizan para calcular y comunicar las rutas.

3.2.7.4. La principal desventaja de usar rutas estáticas:

- Es la falta de reconfiguración automática, si cambia la topología de red.

3.2.8. Mecanismos de Transición.

3.2.8.1. Definición.

Cabe mencionar que son herramientas importantes para hacer de la transición un proceso menos traumático para los usuarios y las aplicaciones, estos mecanismos de transición pueden ser utilizados solos o en combinación.

3.2.8.2. Tipos de mecanismo de transición.

Según[30] los protocolos IPv4 e IPv6, se han desarrollado técnicas que permitan lograr tal cometido, a manera general se tiene:

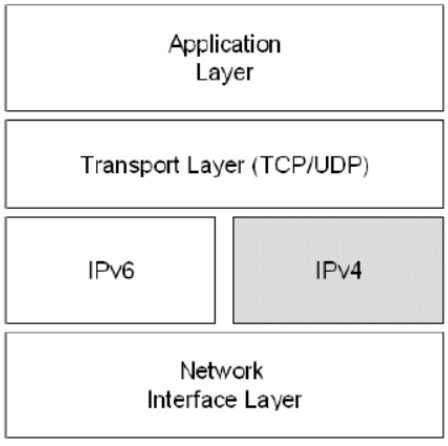
- **Dual Stack.**

Este tipo de mecanismo implementa las pilas de ambos protocolos, IPv4 e IPv6 en cada nodo de la red. Cada nodo de doble pila en la red tendrá dos direcciones de red, una IPv4 y otra IPv6. Tiene un enfoque muy sencillo de implementar que requiere que los hosts y los routers soporten ambas versiones de IP y, por tanto, servicios y aplicaciones tanto IPv4 como IPv6[30].

Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6. La desventaja es que se deben de tener tablas de enrutamiento para ambos protocolos, y es más deben contener soportes para los dos protocolos.

Por el cual el mecanismo de doble pila es fundamental para introducir IPv6 en las arquitecturas IPv4 actuales y se prevé que siga siendo muy utilizado durante el próximo futuro. Su punto flaco es que obliga a que cada máquina retenga una dirección IPv4, cada vez más escasas. Así, a medida que se difunde IPv6, la técnica de doble pila tendrá que ser aplicada allí donde específicamente ayuda al proceso de transición. En un nodo con el presente mecanismo implementado, se incluyen las pilas de los dos protocolos paralelamente como se muestra en la figura 15**.**

Figura 15: Distribución de capas en Dual Stack.



Fuente: [30]

- **Tunelización.**

Para[31] la tunelización es un mecanismo en el que un paquete es encapsulado, dentro de otro tipo de paquete. Es decir, los túneles pueden ser usados para llevar tráfico IPv6 encapsulándolo en paquetes IPv4 y tunelizándolo a través de toda la infraestructura de enrutamiento IPv4.

Los túneles pueden ser usados para llevar tráfico IPv6 encapsulándolo en paquetes IPv4 y tunelizándolo a través de toda la infraestructura de enrutamiento IPv4. Un túnel tiene dos puntos finales, el primero es el punto de entrada y el segundo es el punto de salida. El túnel puede ser implementado en diferentes maneras:

- **Enrutador a enrutador.** Los enrutadores IPv6/IPv4 interconectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos.
- **Host a enrutador:** Los host IPv6/IPv4 pueden tunelizar paquetes IPv6 a un enrutador IPv6/IPv4 intermediario que se alcanza por medio de una infraestructura IPv4.
- **Host a host.** Los host IPv6/IPv4 que están conectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos mismos.
- **Enrutador a host.** Los enrutadores IPv6/IPv4 pueden tunelizar hacia sus destinos finales que son host IPv6/IPv4.

Tipos de túneles.

- **Túneles manuales.**

Según[14] es la forma más sencilla de configurar una conexión IPv6 a través de una red IPv4, aunque no es fácil de administrar. La mayoría de hosts doble pila y elementos de red soportan el estándar IPv6 en túneles IPv4, también conocidos como protocolo 41. El principio detrás de la "tunelación" es el encapsular paquetes IPv6 en paquetes IPv4, es decir, empaquetar paquetes dentro de otros paquetes, en realidad es una técnica muy poderosa.

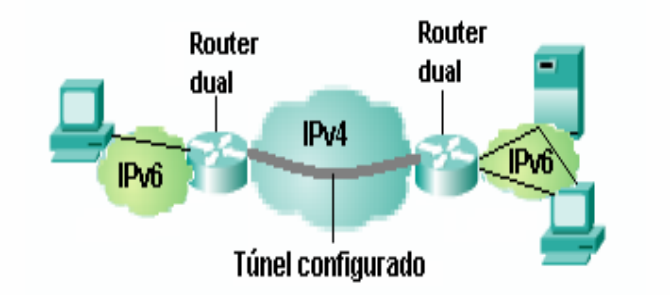
Un túnel manual está compuesto por dos direcciones, un par de IPv4 y un par de IPv6. El par IPv4 es la pareja formada por la dirección de la máquina cliente o router y la dirección del servidor de túnel en el lado proveedor. Las direcciones IPv6 generalmente son proporcionados por las fuentes, ya sea como dos direcciones o como uno de prefijo /64.

Los Túneles Manuales son fáciles de configurar, debido a que se encuentran ampliamente disponibles. Sin embargo, no ofrecen ningún tipo de autenticación y función de vigilancia. El

mayor inconveniente de utilizar el túnel manual es la participación de las personas cada vez que un túnel se ha creado o cuando es modificado, pues debemos configurar manualmente algunas direcciones.

Este mecanismo es muy útil para conectar dos islas informáticas bien conocidas y muy poco probable que cambien, como pueden ser una sucursal y la oficina principal como se muestra en la siguiente figura.

Figura 16: Túnel Manual.



Fuente:[14]

- **Túneles automáticos.**

Los túneles automáticos permiten a los nodos IPv6/IPv4 comunicarse por medio de la infraestructura IPv4 sin la necesidad de una pre configuración del túnel. La dirección del punto final del túnel está determinada por la dirección compatible IPv4 destino. Este tipo de dirección IPv6 es asignada exclusivamente a los nodos que utilizan túneles automáticos[14].

Los túneles automáticos emplean direcciones IPv6 de destino que son compatibles con IPv4, es decir, que el paquete de datos puede ser enviado sin inconvenientes. Ahora, si la dirección IPv6 de destino resulta ser una dirección nativa, entonces el paquete no puede ser enviado mediante el túnel automático. Los mecanismos más populares de túneles automáticos son: el túnel 6to4, Teredo e ISATAP, todos ellos se ejecutan en los sistemas operativos de MICROSOFT.

Según[9] en su investigación presenta las características más importantes de estos protocolos utilizados en el túnel automático:

- Permite a nodos IPv4/IPv6 comunicarse a través de la infraestructura IPv4.
- Los paquetes destinados a direcciones compatibles IPv4, mecánicamente son enviados por un túnel automático.
- La dirección de destino IPv4 se obtiene de la dirección compatible IPv4.
- La dirección IPv4 del nodo está incrustada en su dirección IPv6.

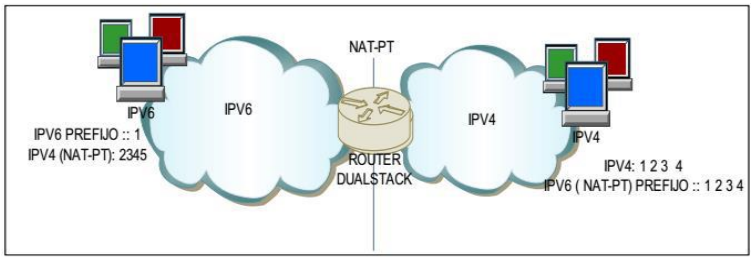
- **Traducción.**

Esto es básicamente traducción de direcciones de red (con todos sus problemas concomitantes), esta vez entre IPv4 e IPv6. Una pasarela de traducción IPv6 a IPv4 permite un nodo interno IPv6 acceder a nodos IPv4 externos y permitir que las respuestas de esos nodos IPv4 heredados sean devueltas al nodo IPv6 interno de origen[32].

Las conexiones desde un nodo IPv6 interno a nodos externos IPv6 o dual-stack se harían como de costumbre a través de IPv6 (sin pasar por la puerta de enlace (Gateway). Esto sería útil para desplegar IPv6 sólo nodos en un mundo predominantemente IPv4. Un Gateway IPv4 a IPv6 permitiría a un nodo interno IPv4 acceder a nodos IPv6 externos y permitir que las respuestas de esos nodos IPv6 externos se devuelvan al nodo IPv4 interno.

Las conexiones desde un nodo IPv4 interno a nodos IPv4 externos, o a nodos de doble pila, se realizarían como de costumbre por medio de IPv4 (sin pasar por la pasarela de traducción). Esto sería útil para desplegar nodos IPv4 en un mundo predominantemente IPv6. Algunos de estos mecanismos requieren modificaciones considerables (e interacción con) DNS, como NAT-PT y NAT64 + DNS64 como se muestra a continuación en la figura 22.

Figura 17: Mecanismo de Traducción NAT-PT.



Fuente: [14]

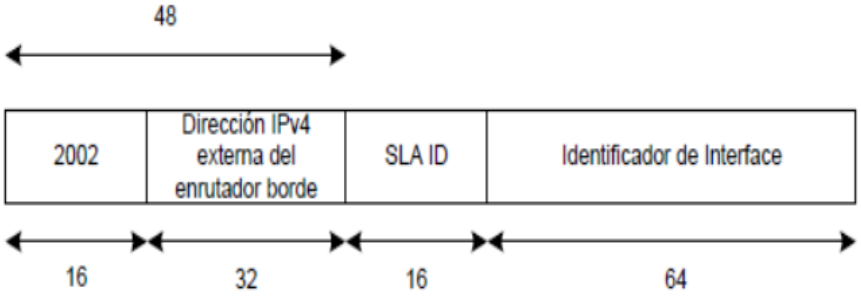
3.2.8.3. Técnicas para establecer túneles.

Para[9] el IETF definió protocolos y técnicas para establecer túneles entre nodos:

- **Túneles 6to4.**

En esta técnica los extremos del túnel están determinados por las direcciones globales IPv4 embebidas dentro de direcciones IPv6 6to4. La dirección 6to4 está construida en base al prefijo 6to4 2002::/16 seguido por los 32 bits de la dirección IPv4 externa del enrutador de borde del sitio, dando como resultado un prefijo de /48 para el sitio, tal y como se muestra en la figura 21.

Figura 18: Estructura de la dirección 6to4.



Fuente:[9]

Los túneles 6to4 pueden ser configurados entre dos enrutadores en la orilla de sus respectivas redes, o entre un enrutador y un host. El único inconveniente de esta técnica para establecer túneles es que solo permiten enviar tráfico IPv6 entre hosts con prefijos de enrutamiento 2002.

- **Túnel ISATAP.**

Una alternativa a los túneles 6to4 son los túneles ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). ISATAP también utiliza la infraestructura IPv4 como enlace virtual, pero no hace uso de multidifusión, por lo que el enlace es NBMA (Non-Broadcast Multiple Access)[13].

ISATAP, al igual que 6to4, crea un identificador de interfaz basado en la dirección IPv4 de la interfaz. Las direcciones en ISATAP pueden ser configuradas manual o automáticamente, pero la dirección IPv4 de la interfaz debe estar embebida en los últimos 32 bits de la nueva dirección IPv6. Al igual que 6to4, la dirección IPv4 debe ser única, y si es usada para acceder a Internet debe ser global.

- **Túnel 6over4.**

En la investigación de[19] sostiene que este método es una tecnología de túneles automáticos que provee conectividad “unicast” y “multicast” IPv6 entre nodos a través de una intranet IPv4.

Según la investigación realizada por[19] se ha liberado las siguientes características sobre los túneles 6over4.

- El túnel 6over4 maneja la infraestructura IPv4 como una asociación simple con capacidades “multicast”, esto significa que el proceso de descubrimiento de vecinos como la resolución de direcciones y descubrimiento de ruteadores, trabaja como un enlace físico con capacidades “multicast” que deberán ser habilitados en IPv4.

Para facilitar las comunicaciones “multicast” IPv6 es una infraestructura IPv4 con “multicast” habilitado, se define el siguiente mapeo para traducir una dirección IPv6 “multicast” en una dirección IPv4 “multicast”.

- **Túnel Teredo.**

Teredo, también conocido como un traslado de direcciones de red (NAT) para IPv6, se diseñó para que hosts IPv4 obtengan direcciones IPv6 a través una o más capas de NAT creando túneles sobre el protocolo UDP. Éste es un mecanismo de túneles automáticos de host a host que provee conectividad IPv6, mientras que los hosts dual stack se ubican detrás de uno o más NATs, por encapsulamiento de paquetes IPv6 en mensajes UDP de IPv4[11].

Según[31] Teredo usa dos entidades:

1. **Server Teredo.**

El Server escucha requerimiento de los clientes en el puerto 3544 del protocolo UDP, respondiendo con una dirección IPv6 para que la usen. Las direcciones Teredo tienen la siguiente estructura: Prefijo Teredo (32 bits): Dirección IPv4 del Servidor Teredo: Flags (16 bits): Puerto externo (16 bits): Dirección externa (32bit).

2. **Relay Teredo.**

El método reenvía paquetes IPv6 (con IPv4 encapsulado) enviados desde el cliente al Teredo Relay, y también redirige los paquetes recibidos desde el Teredo Relay. De hecho, el Relay actúa como un router IPv6. Esta técnica es por lejos una herramienta de “último recurso”, solo diseñada para cuando ningún otro método funcione. El método usado por Teredo es complejo, y no se puede garantizar que trabaje correctamente debido a la gran cantidad de distintas implementaciones de NAT existentes.

3.2.8.4. Cuadro comparativo de ventajas y desventajas de los 3 mecanismos de transición.

A continuación, en la siguiente **Tabla 5** detallaremos las ventajas y desventajas de tradicionales mecanismos de transición.

Tabla 5. Comparación de los distintos mecanismos de transición.

Comparación entre mecanismos de transición					
Tipo de Mecanismo	**Nombre**	**Conectividad**	**Descripción**	**Ventajas**	**Desventajas**
Doble pila	Pila-dual	Solo entre sistema del mismo tipo(IPv4-IPv4, IPv6-IPv6)	-Trabaja con ambos protocolos (IPv4 e IPv6) -Procesa solo los encabezados IP. -Uno de los más populares en su tipo. -Se basa en DHCP y direcciones compatibles para asignación de direcciones.	-Fácil de implementar. -Una solución inmediata y accesible. -Permite a los nuevos dispositivos IPv6 relacionarse rápidamente con los demás dispositivos.	-No trabaja en ambientes mixtos (IPv4 sobre IPv6 y viceversa). -Si la red no es IPv6, no se ve beneficiadas de las características de esta versión.
Tunelización	6to4	IPv6 a IPv6 sobre IPv4	-Crea túneles automáticamente. -Algoritmo más popular dentro de su clase.	-Ayuda a conectar redes IPv6 aisladas entre si	

	6over4	IPv6 a IPv6 sobre IPv4	-Se comporta como una red virtual.	-Permite la autoconfiguración. -Conserva todas las característica de IPv6	-Necesita soporte de ruteo multicast(IPv4 raramente cuenta con este soporte)
Traducción	SIIT (Stateless IP/CMP Translator)	De IPv6 a IPv4 y de IPv4 a IPv6	-Para hacer dos protocolos compatibles realiza la traducción del encabezado -Se necesita de un traductor que lleve a cabo la tarea de traducción.	-Permite a nodos IPv4 conectarse con nodos IPv6 -Fácil de soportar por un dispositivo -No se afecta el checksum de capa de transporte. -Puede manejar paquetes encriptados, ya queno modifica capas superiores	-Al realizar la traducción de IPv6 a IPv4 se pierde muchos campos y estos son beneficios de IPv6. -Se ignora la mayoría de los encabezados de extensión. -Por el manejo de dos protocolos, se necesita de utilizar dos tablas de ruteo diferente. -Al trabajar con direcciones IPv4 compatibles, se reduce el campo de direccionamiento. -Se reduce el tamaño de MTU lo que resulta en fragmentación

Fuente: Grupo de investigación.

4. METODOLOGÍA

A continuación, se presenta los diferentes tipos, métodos y técnicas de investigación al cual se ha acudido para la presente Propuesta Tecnológica.

4.1. Tipos de Investigación.

4.1.1. Investigación Bibliográfica.

Se utiliza este tipo de investigación como fuente principal de la búsqueda de información documental ya sea de libros, tesis, revistas certificadas etc. La cual se pone énfasis en la investigación para la migración de datos de Ipv4 a Ipv6, para así abstraer la información y ponerlo en práctica en dicha propuesta tecnológica.

4.1.2. Investigación Aplicada.

Se busca dar una solución práctica a la problemática que tiende la empresa G&S INGENIEROS Cia.Ltda., permitiendo colaborar con la asociación con el objetivo de migrar los datos de IPV4 a IPV6 a través del método de tunneling y así poder mejor la velocidad y seguridad.

4.1.3. Investigación de Campo.

Permite conocer los problemas, necesidad o situación del ambiente de trabajo y plantear una solución directamente con los involucrados, y a la vez escuchando las propuestas, ideas, observaciones sobre el proceso de información.

4.2. Método Teórico de Investigación.

4.2.1. Método Histórico

Se utiliza este método para buscar sistemas relacionadas con la propuesta en mención, para recolectar información y conocer las herramientas utilizadas con los sistemas anteriores, y sirva de guía.

4.2.2. Método Deductivo.

Con este método se verifica que las conclusiones obtenidas en el proceso de migración de datos de IPv4 a IPv6 a través del método de tunneling sean verdaderas.

4.3. Técnicas de Investigación.

4.3.1. La Observación.

Con esta técnica se permite involucrarse directamente con los usuarios y sus actividades administrativas debido a que puede mirar lo que hace, como se está haciendo y quien realiza cada actividad en si como se lleva a cabo cada tarea o proceso, tiempo que dura el proceso desde su entrega hasta su posible culminación.

4.3.2. La Entrevista.

Mediante esta técnica se busca extraer toda la información requerida del personal involucrado tomando en cuenta a quien entrevistar y que rol cumple cada persona en la empresa G&S INGENIEROS.Cia Ltda. Siendo los involucrados quienes aportan con ideas, opiniones y otros comentarios de suma importancia.

4.4. Metodología implementada.

4.4.1. Mecanismos de migración (Tunneling).

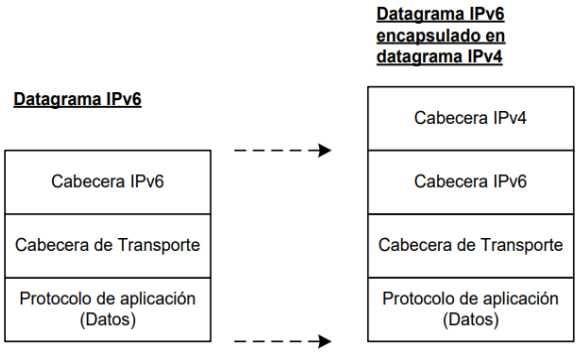
Este método permite transmitir paquetes IPv6 mediante una infraestructura IPv4, es decir se encapsula el contenido del paquete IPv6 en un paquete IPv4.A su vez el autor [2] menciona lo mismo debido a que el nodo IPv6 que está unido con el túnel, toma el paquete IPv6, y lo dispone en el campo de datos de un paquete IPv4. Este paquete IPv4 tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que es parte del túnel. Los nodos IPv4 del túnel orientan el paquete, sin tener certeza de que el paquete IPv4 que están manejando tiene un paquete IPv6. Por último, cuando el paquete llega al final del receptor IPv6 del túnel, este determina que el paquete IPv4 contiene un paquete IPv6 que debe ser extraído.

4.4.2. Encapsulamiento.

Para [33] el encapsulamiento de datagramas IPv6 sobre una red IPv4 usa el número de protocolo IPv4 41. El nodo encapsulado puede ser de un host o de un enrutador y el desencapsulado puede ser también cualquiera de los dos.

El datagrama IPv6 es puesto dentro de la carga útil de un datagrama IPv4, tal y como se muestra en la gráfica 23.

Figura 19: Encapsulamiento de un datagrama IPv6.



Fuente: [33]

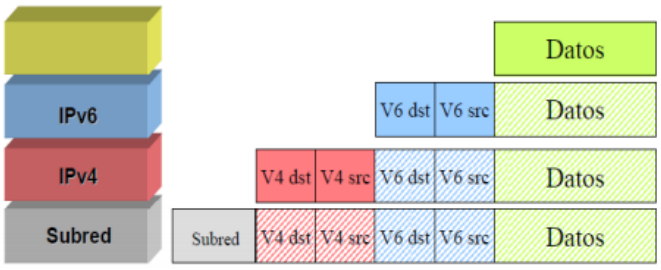
La dirección IPv4 origen y destino del datagrama IPv4 son las direcciones del nodo encapsulado y desencapsulado, las cuales pueden ser o no las direcciones IPv6 origen y destino del datagrama IPv6. Los pasos del encapsulamiento de un paquete IPv6 son los siguientes:

- ✓ El punto de entrada del túnel (el encapsulador) decrementa el campo IPv6, límite de saltos, en una unidad, encapsula el paquete IPv6 en la cabecera IPv4, y transmite el paquete encapsulado a través del túnel. Si fuera necesario el paquete IPv4 es fragmentado.
- ✓ El punto de salida del túnel (el desencapsulador) desencapsula el paquete. Si el paquete fue fragmentado, lo reensambla. Luego el punto de salida remueve la cabecera IPv4 y procesa el paquete IPv6 a su destino original.

4.4.3. Túneles configurados.

- ➢ Túneles usados extensivamente: mbone, multiprotocolo sobre IP, MIP.
- ➢ RFC 2893: Túneles Ipv6 en Ipv4.

Figura 20: Estructura de direccionamiento Ipv6.



Fuente:[1]

4.4.4. Túneles automáticos.

Para [1] Los nodos IPv6 pueden utilizar diferentes tipos de direcciones compatibles con IPv4, IPv6 ó 6to4, el túnel automático no es más que un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4. La configuración de los túneles entre routers y host puede utilizarse de diferentes formas:

1. Router a Router: utiliza un mecanismo de túnel automático en donde los routers IPv6/IPv4 que están separados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

2. Host a Router: utiliza un mecanismo de túnel automático en el que un host IPv6/IPv4 encapsula paquetes IPv6 a un router intermedio IPv6/IPv4 que es accesible mediante una infraestructura de ruteo IPv4.

3. Host a Host: el mecanismo de túnel que utiliza es manual en donde los host IPv6/IPv4 que están interconectados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

4. Router a Host: utiliza un mecanismo de túnel manual en el cual los routers IPv6/IPv4 pueden encapsular paquetes IPv6 hacia su destino final.

4.4.5. Método 6to4.

EL autor [33] indica que el método 6to4 es un mecanismo (RFC 3056) para que los sitios IPv6 puedan comunicarse entre sí, utilizando la red IPv4, sin la necesidad de contar con un túnel explícito. De la misma manera el escritor [2] define que los sitios de IPv6 se puedan comunicar entre sí a través de la red IPv4 sin la necesidad de especificar una configuración explícita del túnel. La red de área amplia IPv4 se trabaja como una capa de enlace punto a punto de unidifusión en la que los dominios de IPv6 se comunican por los routers 6to4 conocidos como puertas de enlace 6to4. Esto se realiza como un mecanismo de transición utilizado durante el período de coexistencia de IPv4 e IPv6.

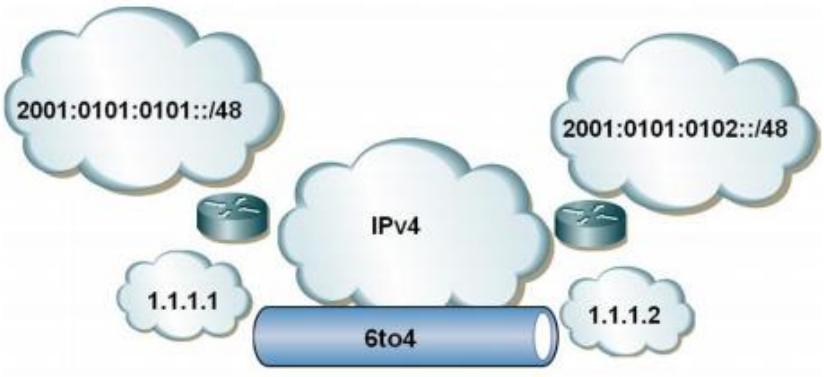
"El método 6to4 utiliza el prefijo de dirección global: 2002: WWXX: YYZZ: :/48"

WWXX:YYZZ : se refiere a la parte correspondiente al ID de agregación del siguiente nivel de una dirección global y la representación, en formato hexadecimal separado por dos puntos, de una dirección IPv4 pública (w.x.y.z) asignada al sitio o host.

La dirección 6to4 completa de un host 6to4 seria de la siguiente manera:

2002:WWXX:YYZZ:[SLAID]:[IdDeInterfaz]

Figura 21: Esquema del túnel 6to4.



Fuente:[34]

A continuación, se detallan ciertas definiciones importantes:

- Pseudo interface 6to4. Es aquel punto que es equivalente a la interface de IPv6, donde acontece el encapsulamiento 6to4 de los paquetes IPv6 dentro de paquetes IPv4.
- Prefijo 6to4. Es aquel prefijo diseñado con las mismas características especificadas en el protocolo RFC 3056.
- Dirección 6to4. Es aquella dirección IPv6 diseñada mediante el prefijo 6to4
- Dirección IPv6 nativa. Es aquella dirección IPv6 diseñada mediante cualquier otro prefijo sin provenir del 6to4.
- Enrutador 6to4 o de borde. Es aquel enrutador capaz de soportar pseudo interfaces del 6to4.
- Host 6to4. Es aquel host IPv6 que tiene por lo menos una dirección 6to4.
- Sitio 6to4. Es un sitio en el cual internamente se está corriendo IPv6 usando direcciones 6to4. 62
- Enrutador Relay. Este es un enrutador configurado para soportar rutas con tráfico de direcciones IPv6 nativa y direcciones 6to4.

El túnel 6to4 es un mecanismo temporal para la transición durante el período de tiempo en que coexistan los dos protocolos IPv4 e Ipv6, no ha sido considerada como una solución permanente. La dirección 6to4 está construida en base al prefijo 6to4 2002::/16 seguido por los 32 bits de la dirección IPv4 externa del enrutador de borde del sitio, dando como resultado un prefijo de /48.

4.5. Obtención del Diagrama Lógico.

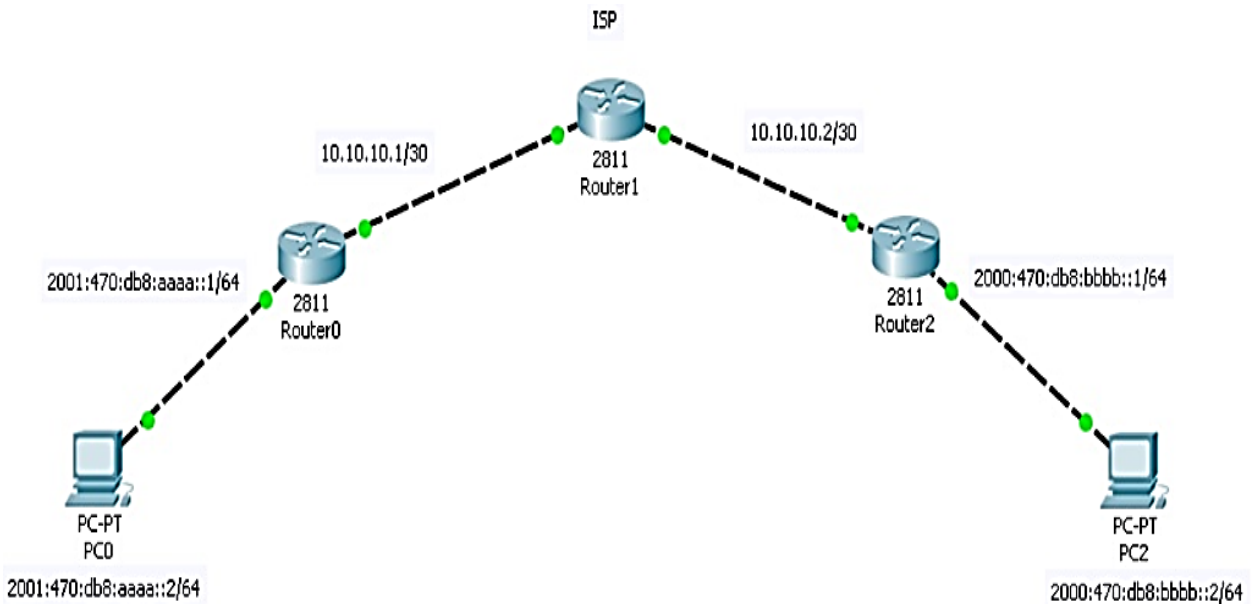


Tabla 6: Direcciones del diagrama lógico.

Equipos	**Direcciones IPv6**
Router 1	2001:470:db8:aaaa::1/64
Router 2	2000:470:db8:bbbb::1/64
PC1	2001:470:db8:aaaa::2
PC2	2000:470:db8:bbbb::2

Fuente: Grupo de investigación.

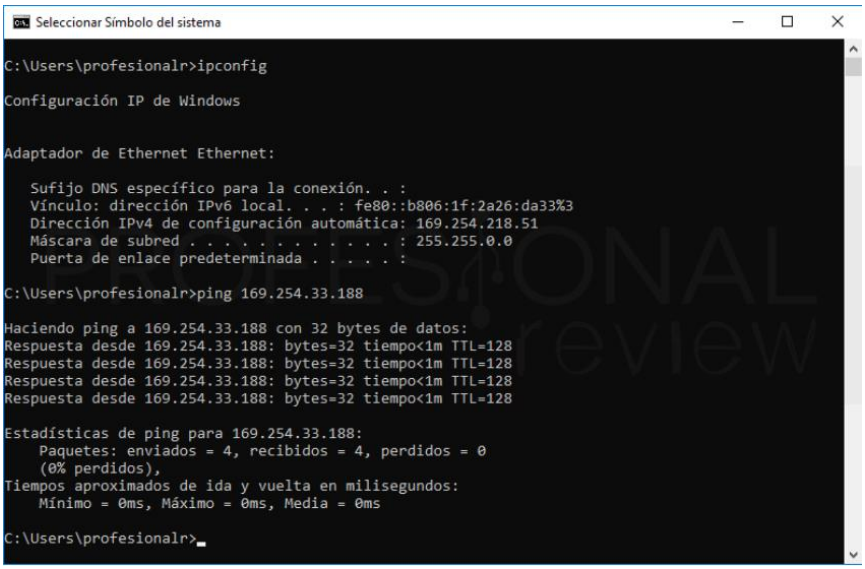
5. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

5.1. Resultado de la Hipótesis.

Para evidenciar la hipótesis se puede argumentar mediante los resultados y través de la implementación que se realizó en dicha empresa generando resultados favorables debido a que la transmisión de datos fue exitosa debido a que los datos fueron encriptados de una manera segura a través del túnel creado.

A continuación, observáremos el Antes y el Después:

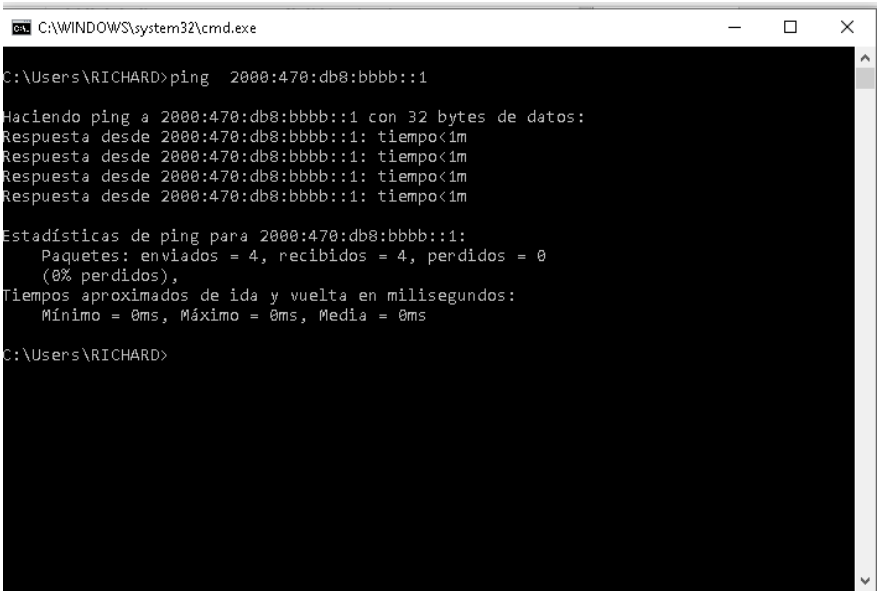
Figura 22: Tiempo de envió con IPv4.



Fuente: Grupo de investigación.

En esta figura 22 podemos observar que trabaja con una direccion ipv4 que ha sido asignado por el proveedor de internet este consta una cabecera de 32 bit con un tiempo que se medirá en milisegundos a su vez tendrá un tiempo de vida, esta estructura viene por defecto en el Protocolo de IPV4.

Figura 23: Tiempo de envió con IPv6.



Fuente: Grupo de investigación.

La figura 23 representa la comunicación actual que tiene la empresa debido a que este protocolo que trabaja con 128 bit es decir que la comunicación va hacer más rápido en cuanto al tiempo de ejecución y sin tiempo de vida.

5.2. Resultados para la migración de datos de Ipv4 a Ipv6 a través del método de Tunnel.

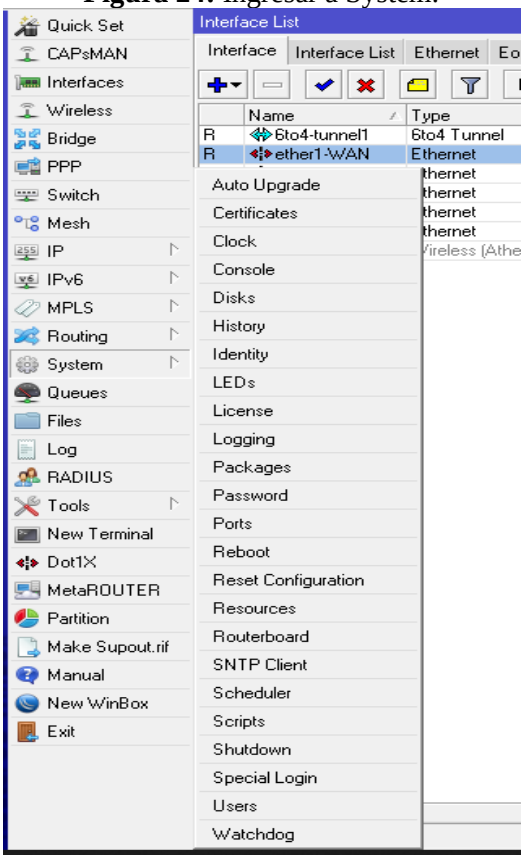
Para realizar esta migración se tuvo que configurar un Tunnel llamado “6to4-tunnel” dentro de un router Mikrotik que se obtuvo dentro de la empresa. A continuación, observaremos dicha configuración.

5.2.1. Configuración del Tunnel entre dos equipos para crear una red.

5.2.1.1. Habilitar el protocolo ipv6 dentro del Mikrotik.

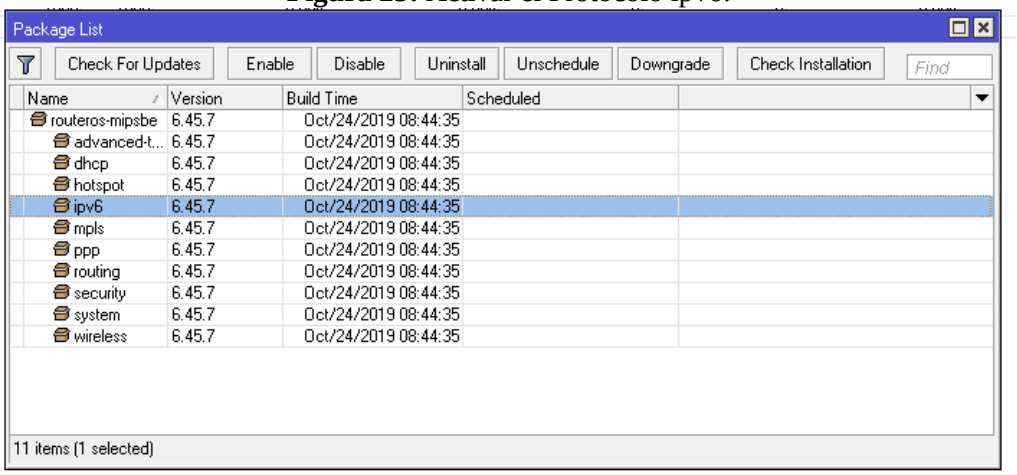
Antes de poder configurar el método 6to4 dentro de los equipos tenemos que instalar el módulo de IPv6: Para esto tuvimos que ingresar al router; instalando Winbox, después de instalar este software ingresaremos a System, escogemos la opción Packages y nos aparece todos los módulos instalados en nuestro router; por el momento la opción de ipv6 se encontraba deshabilitada es por eso que seleccionamos la opción de IPv6 y le damos un clic en Enable. Para finalizar volvemos a la pestaña de System y seleccionamos Reboot y equipo se reinicia por completo; esto se puede demostrar en la figura 22 y en la figura 23.

Figura 24: Ingresar a System.



Fuente: Grupo de investigación.

Figura 25: Activar el Protocolo ipv6.

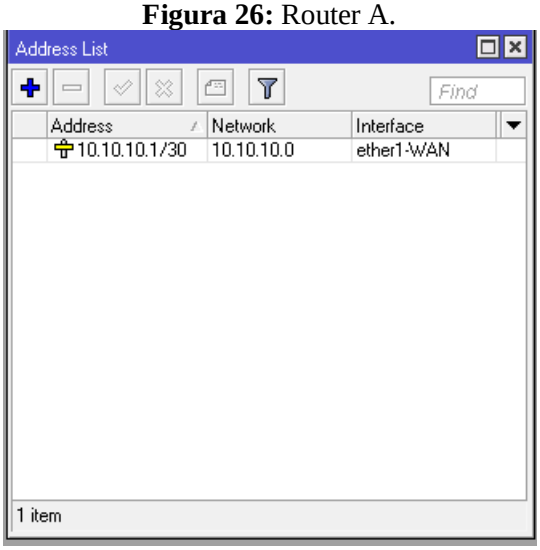


Fuente: Grupo de investigación.

5.2.1.2. Determinar una dirección con el protocolo IPv4.

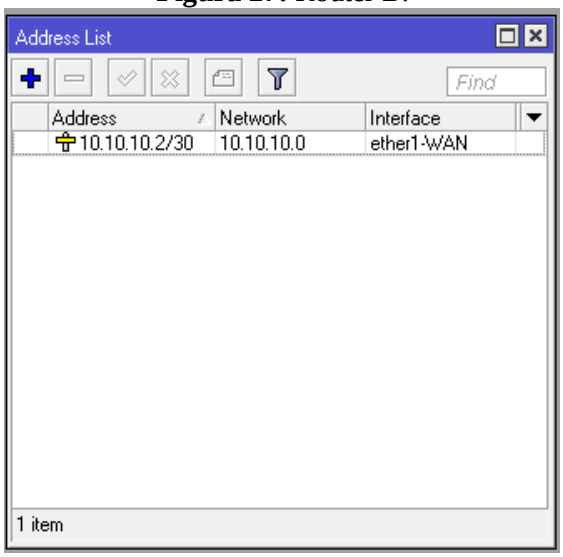
Después de realizar el paso anterior necesitamos asignar una dirección utilizando protocolo IPv4 debido a que esta vendría a tomar la dirección que nos brinda el proveedor de internet (ISP) normal. Esta configuración tendremos que hacer en los dos segmentos de red como se puede observar en la figura 24 y en la figura 25; Se utilizó el prefijo /30 porque necesitamos que la Network empiece desde 0 esta asignación se realizó en los dos equipos.

Figura 26: Router A.



Fuente: Grupo de investigación.

Figura 27: Router B.



Fuente: Grupo de investigación

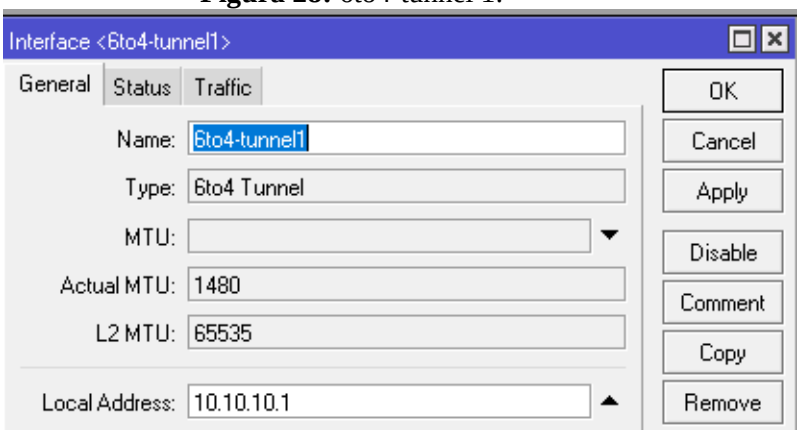
5.2.1.3. Configurar el Tunnel 6to4.

Para crear el túnel tenemos que fijar una dirección local y una dirección remota dentro de cada router:

- **Fijar una dirección local.**

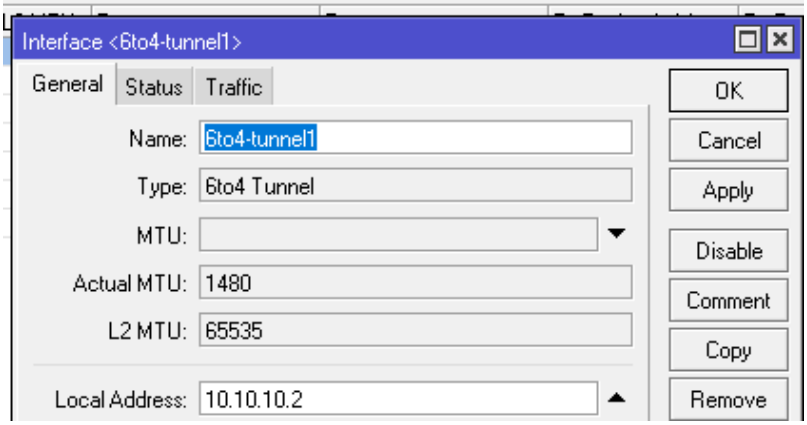
Esta dirección local o conocida como dirección de origen fue asignada anteriormente en el **router A**: como la 10.10:10:1, de la misma manera se utilizó para el **router B**: como la 10.10.10.2 estas trayectorias ya fueron asignadas al puerto ether1-Wan: y ahora se utilizará para hacer la conexión del Tunnel como se puede observar en la figura 26 y en la figura 27.

Figura 28: 6to4-tunnel 1.



Fuente: Grupo de investigación.

Figura 29: 6to4-tunnel 2.

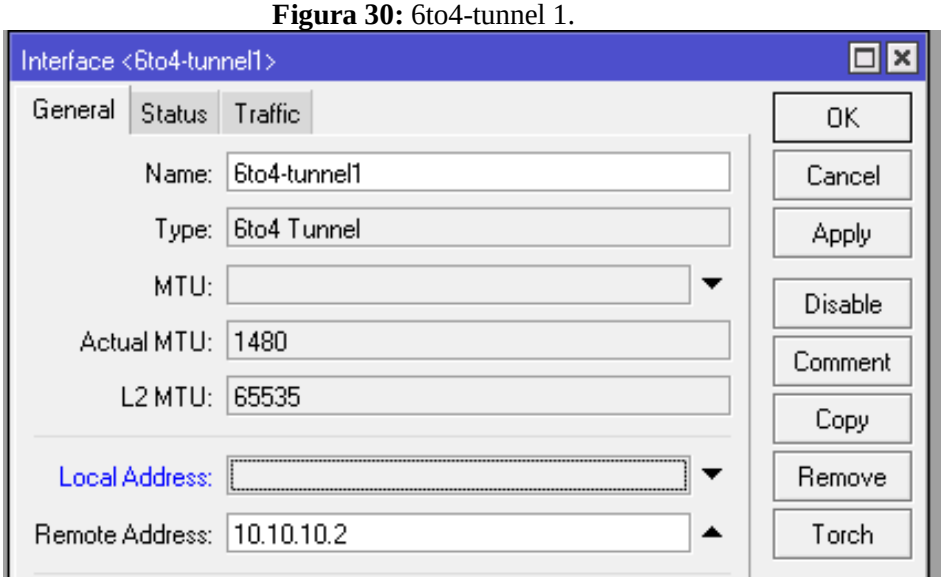


Fuente: Grupo de investigación.

- **Fijar una dirección remota.**

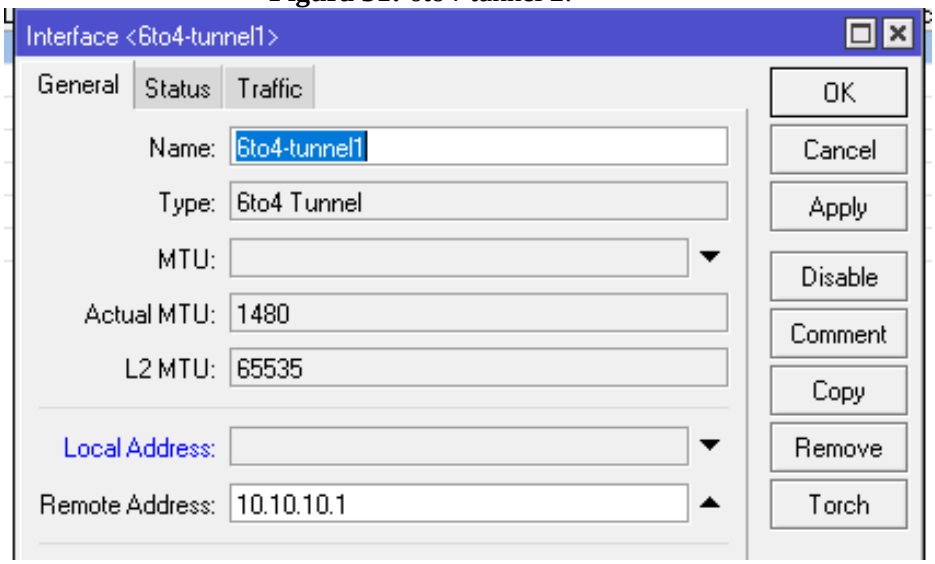
Esta dirección remota o conocida como dirección de destino fue asignada anteriormente en el **router A**: como la 10.10:10:2, de la misma manera se utilizó para el **router B**: como la 10.10.10.1 debido a que estas direcciones son los enlaces para poder comunicarnos. Todo lo mencionado se pude evidenciar en la figura 28 y en la figura 29.

Figura 30: 6to4-tunnel 1.



Fuente: Grupo de investigación.

Figura 31: 6to4-tunnel 2.

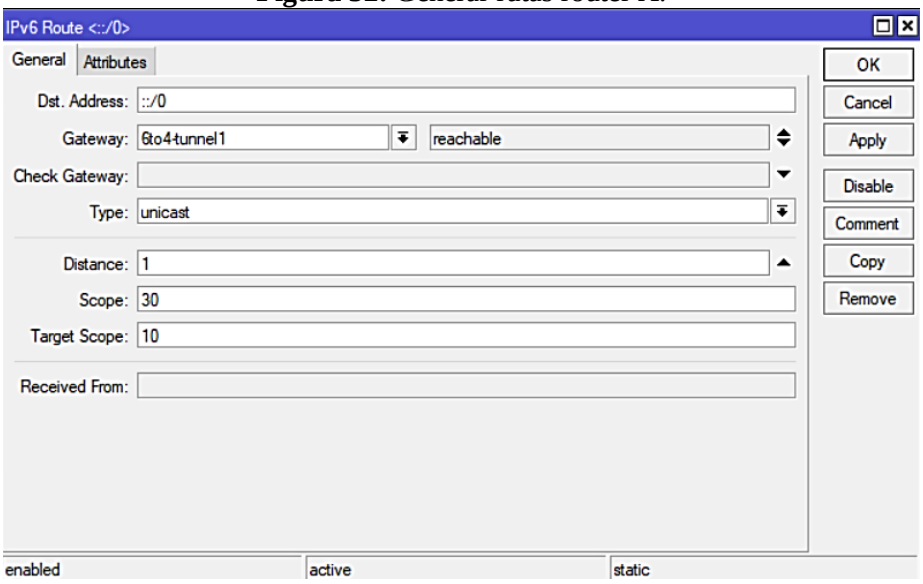


Fuente: Grupo de investigación.

- **Fijar las rutas para comunicar el Tunnel 6to4.**

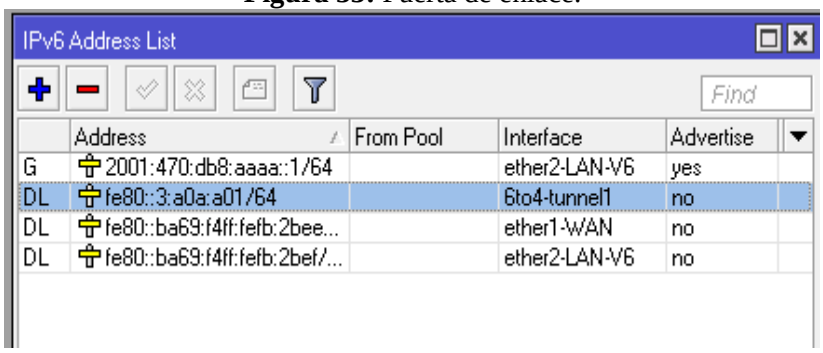
Las rutas es el camino hacia una red, para esto se utilizará un Gateway debido a que esta servirá como puerta de enlace para que funcione el Tunnel; en este caso sería el 6to4-tunnel1 al momento de poner aplicar instintivamente se pone unicast; es porque vamos a utilizar una conexión de punto a punto esto se puede observar en la figura 30 y figura 32. En si este proceso se realizó para los dos equipos la única diferencia es la puerta de enlace que se genera de tal manera que el **router A**: trabajará con la fe80::3:a0a:a01 y el **router B** trabajará con la fe80::3:a0a:a02 estas direcciones se generan automáticamente después de realizar este proceso y esto lo podemos mirar en la figura 31 y figura 33.

Figura 32: Generar rutas router A.



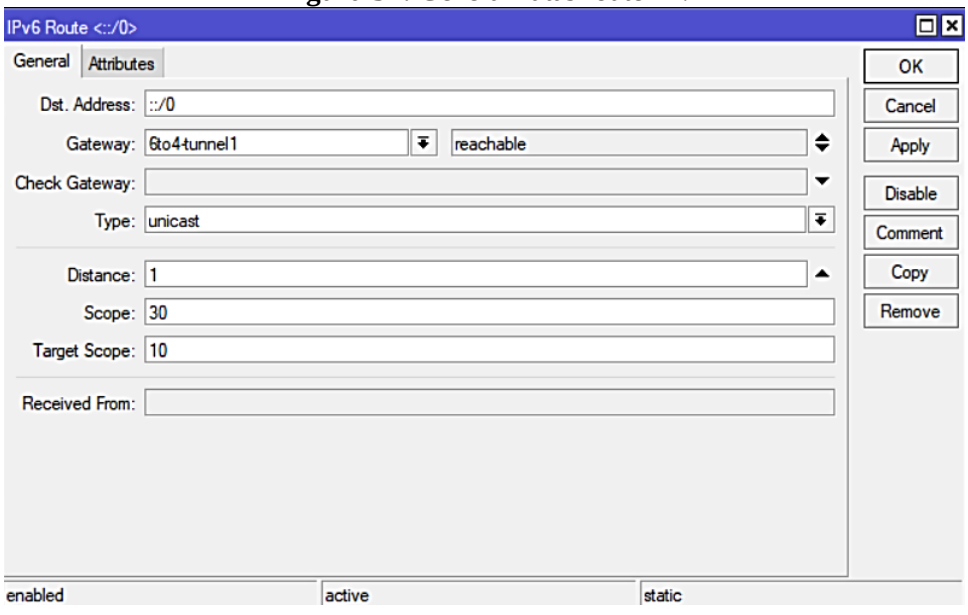
Fuente: Grupo de investigación.

Figura 33: Puerta de enlace.



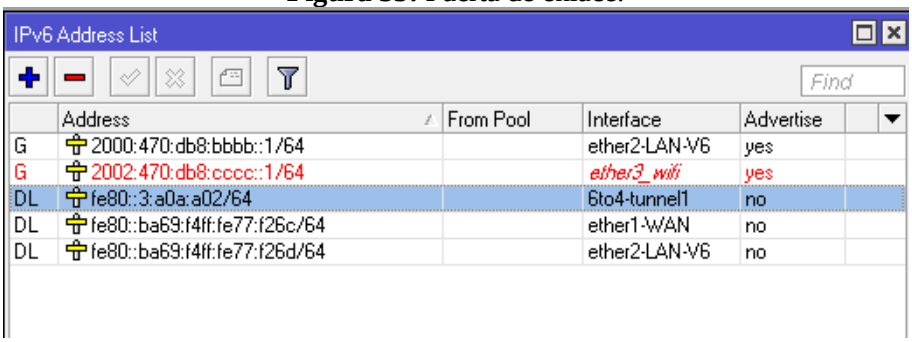
Fuente: Grupo de investigación.

Figura 34: Generar rutas router B.



Fuente: Grupo de investigación.

Figura 35: Puerta de enlace.

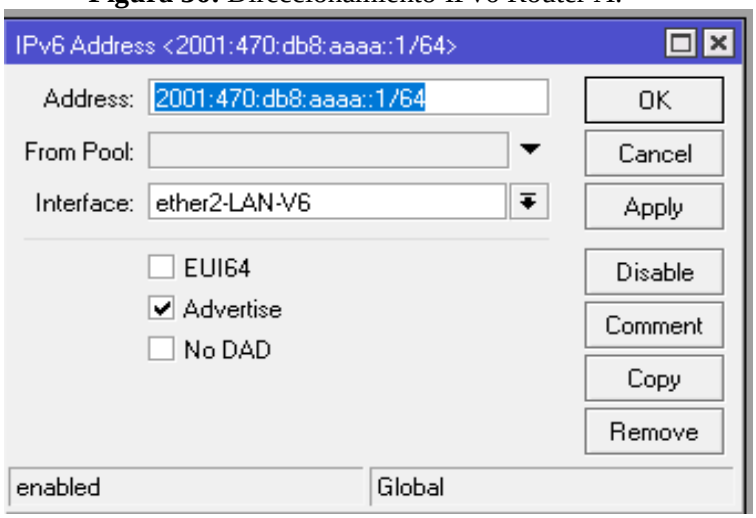


Fuente: Grupo de investigación.

5.2.1.4. Determinar una dirección con el protocolo ipv6.

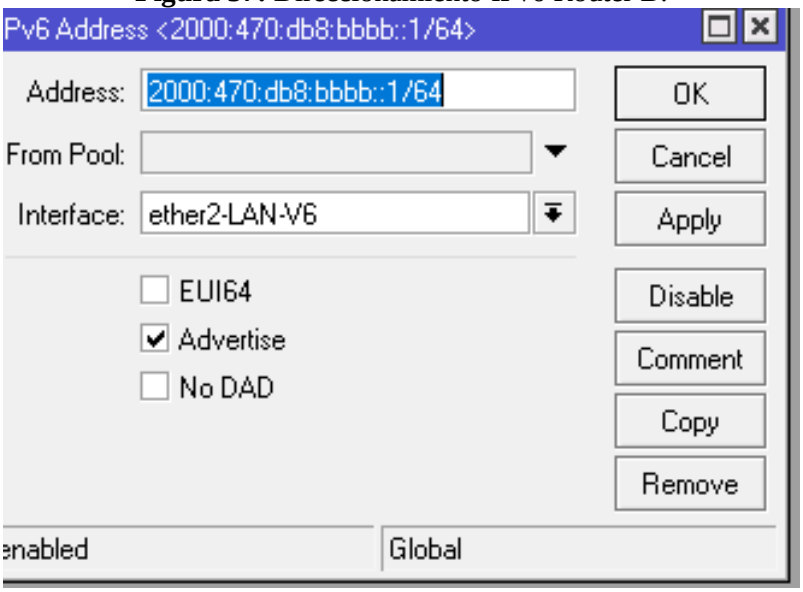
Después de realizar el proceso de Tunnel ahora asignaremos las direcciones utilizando protocolo IPv6 de tal manera que este direccionamiento nos servirá para el proceso de migración. Es por eso que el **router A**: tiene la dirección 2001:470:db8:aaaa::1/64 esta dirección va al puerto ether2-LAN-V6 de la misma manera el **router B**: tiene la dirección 2001:470:db8:aaaa::1/64 y va al mismo puerto todo lo mencionado se puede para verificar esto en la figura 34 y figura 35.

Figura 36: Direccionamiento IPv6 Router A.



Fuente: Grupo de investigación.

Figura 37: Direccionamiento IPv6 Router B.



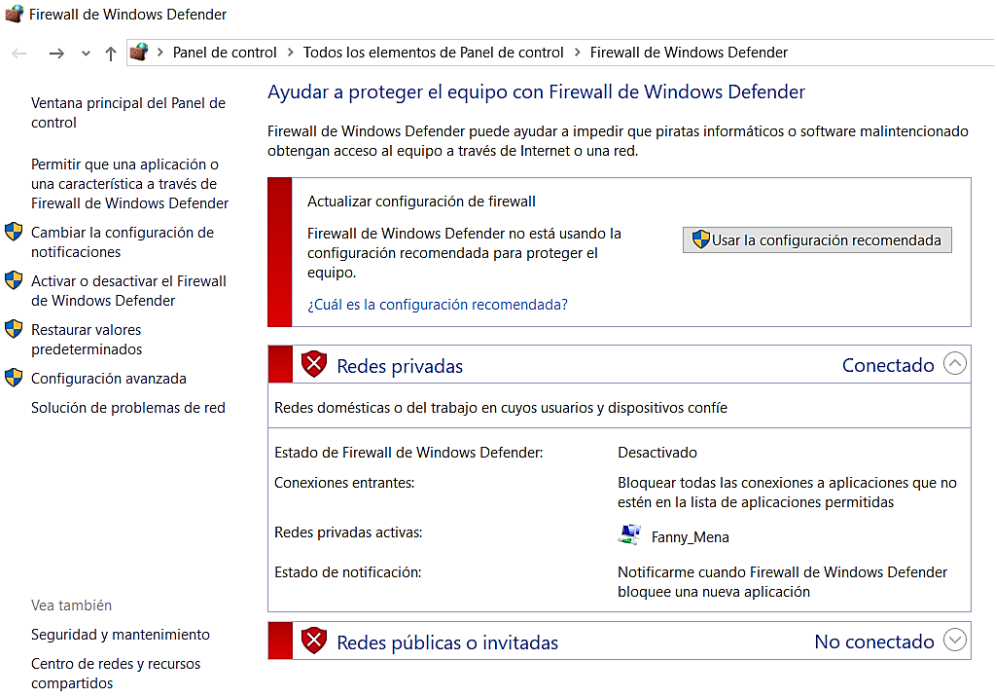
Fuente: Grupo de investigación.

5.2.1.5. Configuración de las maquinas.

- **Desactivar firewall de las maquinas.**

Ingresar a las máquinas y configurar el firewall para que no funcione o mejor dicho desactivarlo para que así pueda funcionar la comunicación entre maquinas como se puede observar en la figura 36.

Figura 38: Firewall de Windows.

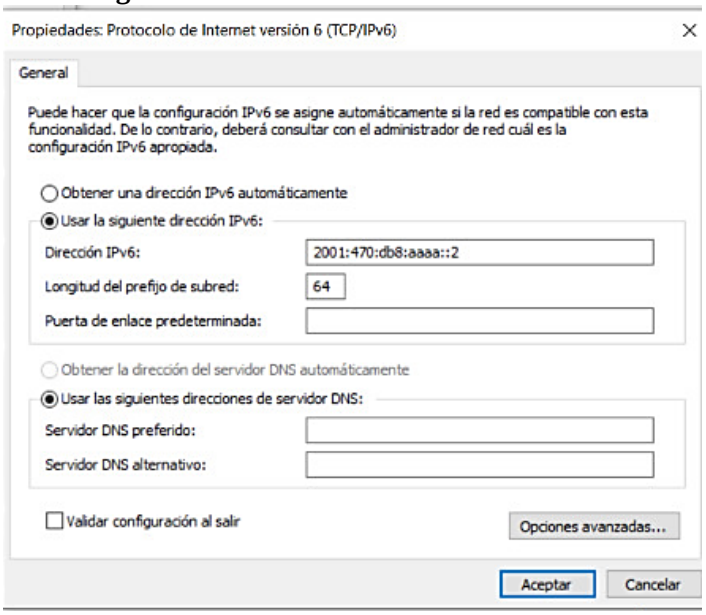


Fuente: Grupo de investigación.

- **Fijar la dirección ipv6 dentro de las maquinas.**

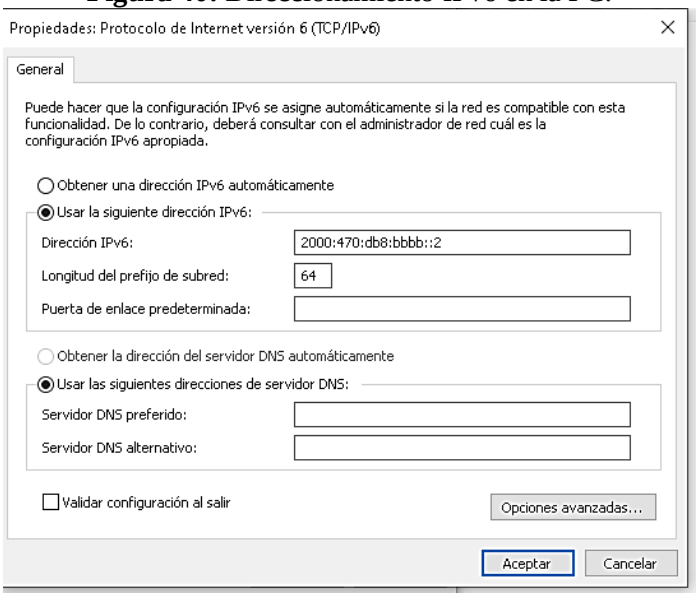
Aquí utilizaremos el direccionamiento estático porque anteriormente se le asigna una dirección dentro de los **router A** para este caso se manejara la dirección 2001:470:db8:aaaa::2 como se ve en la figura 37 mientras que la el **router B** utiliza la dirección 2000:470:db8:bbbb::2. Así mismo se puede ver en la figura 38.

Figura 39: Direccionamiento IPv6 en la PC.



Fuente: Grupo de investigación.

Figura 40: Direccionamiento IPv6 en la PC.

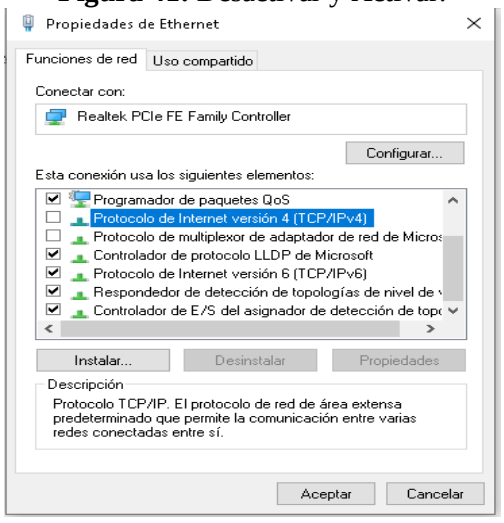


Fuente: Grupo de investigación.

- **Desactivar el protocolo ipv4.**

En esta fase tenemos que desactivar el protocolo IPv4 y a su vez activar el protocolo Ipv6 para así poder probar la conectividad entre las maquinas utilizando el nuevo protocolo de Ipv6; esta función se realiza en todas la maquinas que se vayan a conectar de tal manera que quede como en la figura 39.

Figura 41: Desactivar y Activar.



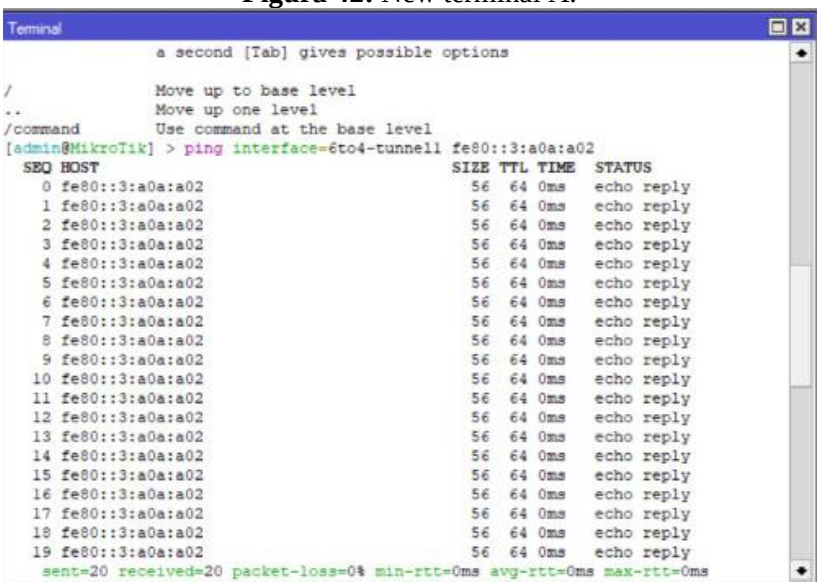
Fuente: Grupo de investigación.

5.2.1.6. Verificar la comunicación entre los túneles a través de la terminal del Mikrotik.

Ingresamos al **Mikrotik A** y seleccionamos la opción de new terminal e ingresamos el siguiente comando ping interface=6to4=tunnell fe80::3:a0a:a01 ponemos esta dirección ya esta es la

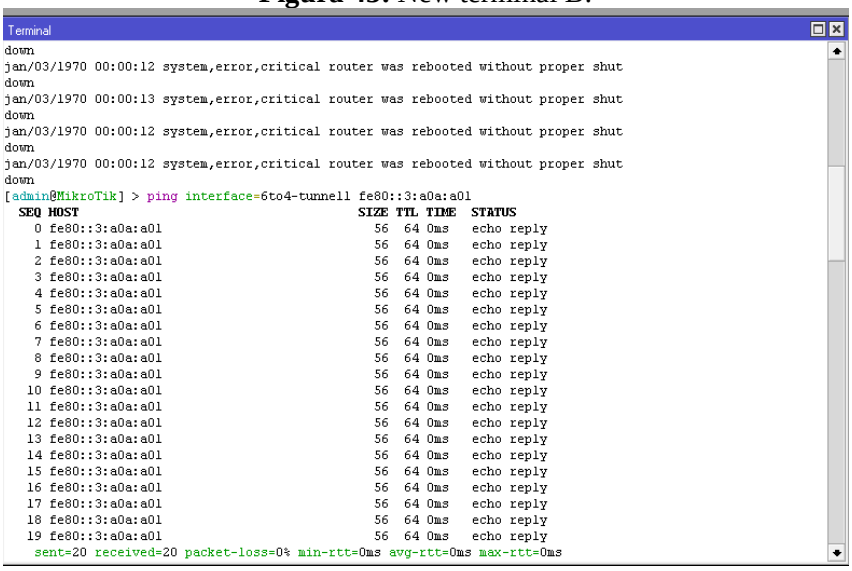
puerta de enlace que creo el Tunnel automáticamente; A su vez hacemos los mismo en **Mikrotik B** solo que cambiamos de ruta de enlace debido que para este router utilizaremos el ping interface=6to4=tunnell fe80::3:a0a:a02 y como se puede observar en la figura 40 y figura 41 efectivamente hay comunicación entre túneles.

Figura 42: New terminal A.



Fuente: Grupo de investigación.

Figura 43: New terminal B.

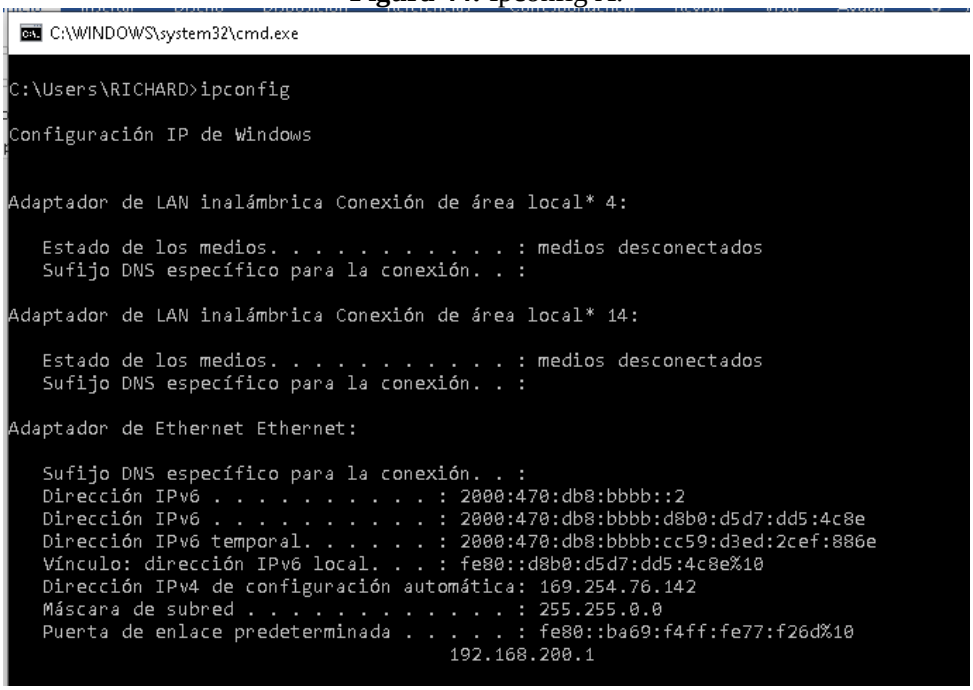


Fuente: Grupo de investigación.

5.2.1.7. Verificar si existe comunicación entre maquinas con el protocolo ipv6.

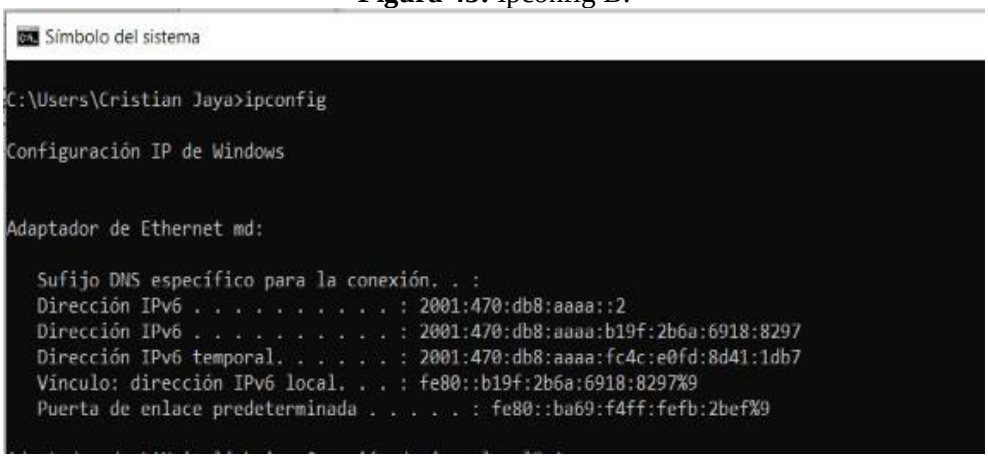
Buscar en la lupa la palabra ejecutar después de seleccionar se escribirá cmd, posteriormente aparecerá una pantalla como se muestra en la figura 42 y figura 43 se ejecutará el comando Ipconfig para verificar cual fue la dirección asignada para las dos maquinas

Figura 44: Ipconfig A.



Fuente: Grupo de investigación.

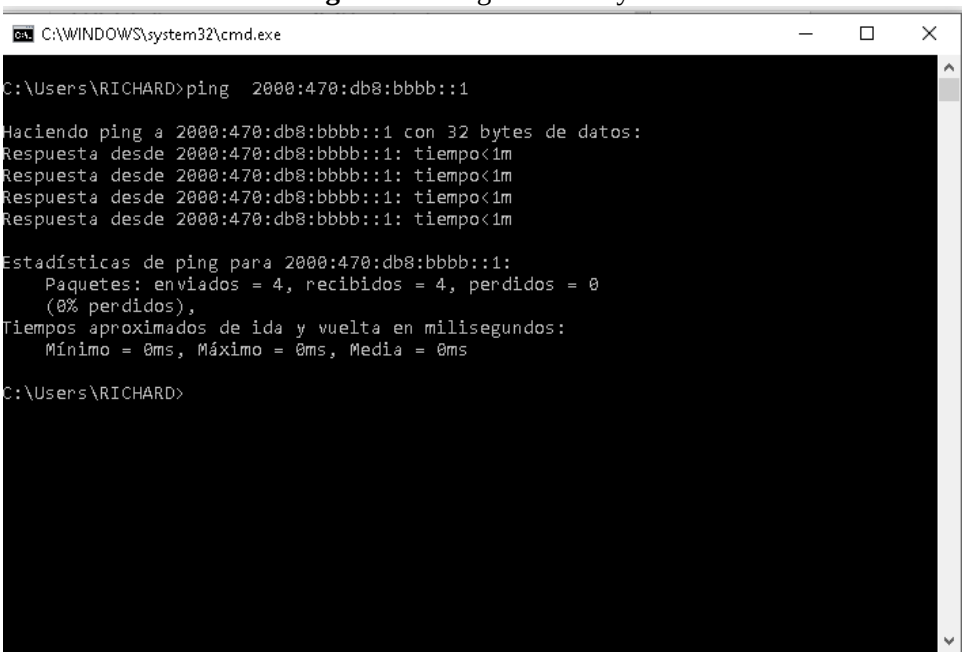
Figura 45: Ipconfig B.



Fuente: Grupo de investigación.

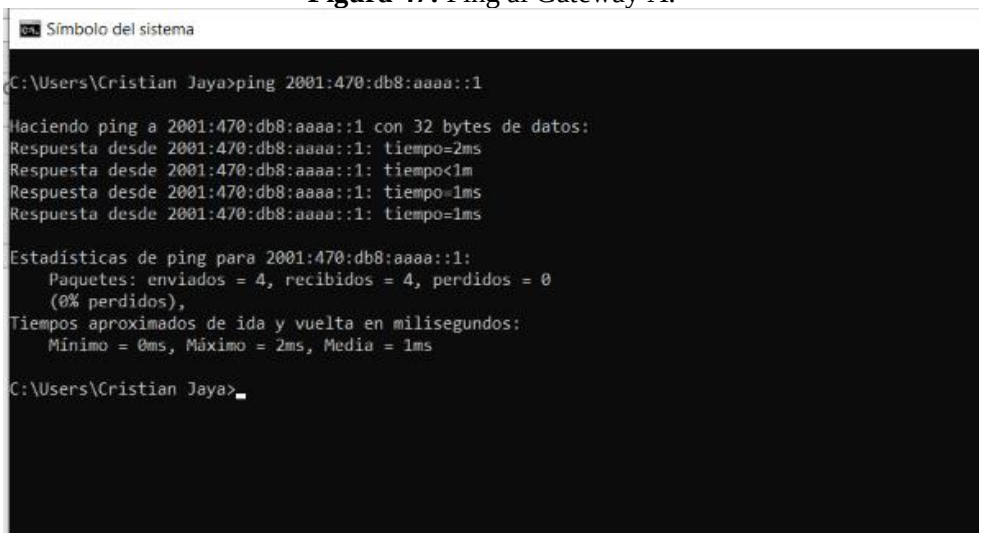
En la figura 44 y figura 45 podemos observar que estamos realizando un ping al Gateway para ver si llega al **router B** y a su vez al **router A** y como se puede evidenciar hay conectividad al Gateway.

Figura 46: Ping al Gateway B.



Fuente: Grupo de investigación.

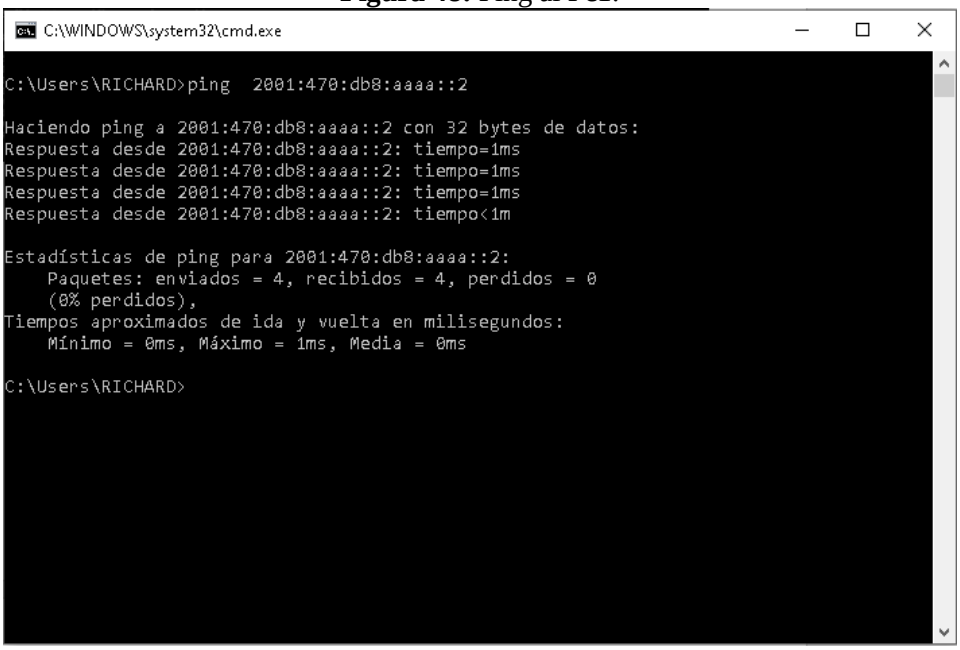
Figura 47: Ping al Gateway A.



Fuente: Grupo de investigación.

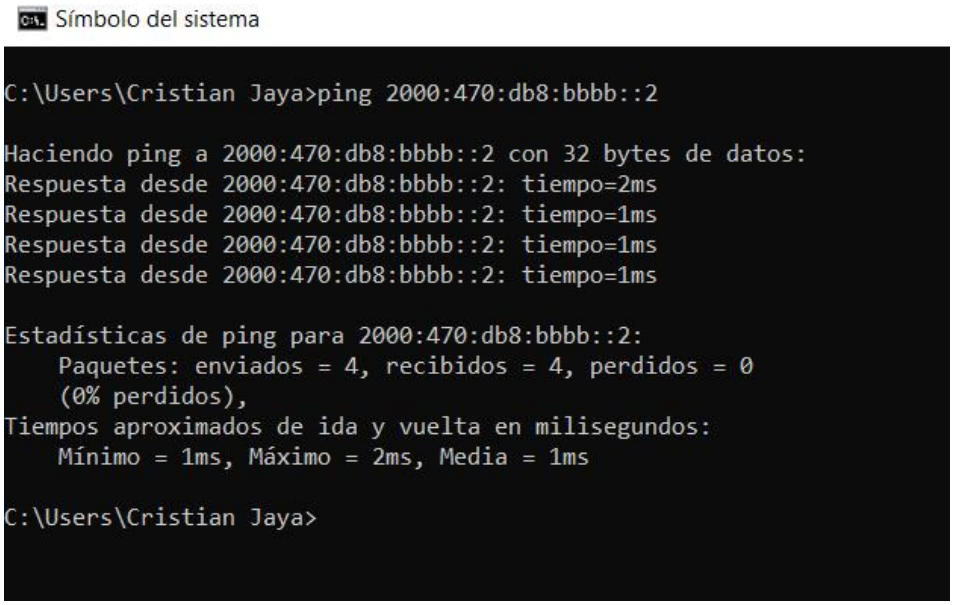
Después de hacer un ping al Gateway se realizará un ping al **Pc1** y al **Pc2** para ver si existe comunicación y cómo podemos observar en la figura 46 y figura 47 hay conectividad de extremo a extremo.

Figura 48: Ping al Pc1.



Fuente: Grupo de investigación.

Figura 49: Ping al Pc2.



Fuente: Grupo de investigación.

6. PRESUPUESTO Y ANÁLISIS DE IMPACTOS.

6.1. Presupuesto

En las siguientes tablas se especifican los diferentes valores de inversión en el desarrollo de la propuesta tecnológica de la empresa G&S INGENIEROS.Cia Ltda. Ubicado en la ciudad de Latacunga Provincia de Cotopaxi.

6.1.1. Costo de Equipos y Mano de Obra.

Tabla 7. Costo de equipos.

Recursos	Cantidad	V. Unitario	Valor Total
Routerboard Mikrotik Rb951g-2hnd	2	$ 150	$ 300
Switch Ethernet de 5-Puertos	1	$ 10	$ 10
Cable De Red, Rj45	5	$ 2	$ 10
Mano de obra	2	$70	$140
Total costo de equipos y mano de obra			**$ 460**

Fuente: Grupo de investigación.

6.1.2. Gastos Directos.

Tabla 8. Gastos Directos.

Recursos	Cantidad	V. Unitario	Valor Total
Resma de papel bond	2	$ 3,50	$ 7
Tinta de impresión	4	$ 10	$ 40
Carpeta	1	$ 1	$ 1
Anillados	3	$ 2,50	$ 7,50
Cuaderno	1	$ 1	$1
Esferos	2	$ 0,30	$ 0,60
Copias	20	$ 0,02	$ 0.40
Total Gastos Directos			**$ 57, 50**

Fuente: Grupo de investigación.

6.1.3. Gastos Indirectos.

Tabla 9. Gastos Indirectos.

Recursos	Total
Alimentación	$ 50
Trasporte	$ 50
Total Gastos Indirectos	**$ 100**

Fuente: Grupo de investigación.

6.1.4. Gasto Total.

Tabla 10. Gasto Total.

Descripción	Total
Total costo de equipos y M. obra	$ 460
Total Gastos Directos	$ 57, 50
Total Gastos Indirectos	$ 100

Total	**$ 617,50**

Fuente: Grupo de investigación.

6.1.5. Costo-Beneficio.

Los costos de los requerimientos para la migración de datos del protocolo IPv4 a IPv6 es de $320 dólares.

Tabla 11: Requerimientos de la propuesta.

Requerimientos	**Valor Total**
Routerboard Mikrotik Rb951g-2hnd	$ 300
Switch Ethernet de 5-Puertos	$ 10
Cable De Red, Rj45	$ 10
Total costo de los requerimientos	**$ 320**

Fuente: Grupo de investigación.

Los beneficios que se obtuvo al implementar la migración de datos son las siguientes.

Tabla 12: Beneficios de la implementación.

Beneficios
Confiabilidad en el manejo de información
Seguridad de la información que transmite la red
Mejor infraestructura tecnológica en la Empresa
Garantiza información integra

Fuente: Grupo de investigación.

6.2. Análisis de impactos

A continuación, se menciona los diferentes impactos sobre la migración de datos del protocolo IPv4 a IPV6 a través del método de tunneling el cual se implementó en la empresa G&S INGENIEROS.Cia Ltda.

6.3. Impacto técnico.

Se alcanzó la migración de datos mediante el protocolo IPv6 utilizando el encabezado del IPv4, lo cual refleja que existe una comunicación entre dos dispositivos, esto genera grandes expectativas para trabajar con el protocolo de IPV6.

Las herramientas tecnológicas que se utilizaron para realizar las configuraciones son:

- ✓ Win box
- ✓ Cisco Packet Tracer

6.4. Impacto social.

La migración de datos de ipv4 a IPv6 utilizando el método de tunneling favorece a la empresa G&S INGENIEROS.Cia Ltda. Permitiendo mejorar en el área de tecnología e investigación mismo que optimizara él envió de paquetes, almacenando y transmitiendo información de forma segura y de manera inmediata.

Con esto existe una mayor eficacia en el traslado de información entre los diferentes dispositivos que se encuentren conectado a la red mejorando el rendimiento en los procesos de migración de datos que realiza la empresa.

7. CONCLUSIONES Y RECOMENDACIONES.

7.1. Conclusiones.

- ✓ Después de analizar los diferentes estados de arte sobre la migración de datos de Ipv4 a Ipv6 en diferentes empresas e instituciones podemos evidenciar que su migración de datos es factible es por eso que el grupo investigador decidió trabajar con esta propuesta de migrar datos a través de un mecanismo de transición llamado “Tunneling” en la empresa G&S INGENIEROS.CIA LTDA.

- ✓ Al revisar los diferentes conceptos relacionados con el internet y la coexistencia entre protocolos Ipv4 e IPv6, el grupo investigador pudo tener una idea más claro al momento de aplicar un método de transición, debido a que podrá conocer qué tipo de direccionamiento va asignar a la configuración y de estar manera tener una solución rápida y eficaz al momento de migrar datos.

- ✓ Después de analizar el cuadro comparativo con sus respectivas ventajas y desventajas el grupo investigador pudo seleccionar el mecanismo de transición más adecuado para dicha empresa.

- ✓ Para finalizar el mecanismo de transición a escoger fue el de tunneling dentro de este existen túneles configurados y automáticos; para esta propuesta se utilizó un túnel automático llamo Six to for tunnel debido a que este método nos permitirá desglosar los datos en piezas más conocidas como paquetes, que se moverán a lo largo del "túnel" para ser transportados a su destino final. A medida que estos paquetes se mueven a través del túnel, son encriptados y encapsulados.

7.2. Recomendaciones.

- ✓ Uno de los primeros pasos experimentales de migración puede ser comenzar a migrar pequeñas subredes experimentales que formen parte de nuestra red, y que sea de uso exclusivo para ir observando cómo se desempeñará y así poder detectar a temprana hora, los posibles inconvenientes que puedan surgir en la transición, para que puedan ser corregidos y estar listos para cuando se tenga que migrar toda la red.

- ✓ A su vez el grupo investigador recomienda desactivar el firewall de cada máquina debido a que al momento de comunicar las dos máquinas a través del 6to4-tunnel con un ping la una maquina no puede reconocer la dirección asignada.

- ✓ Capacitar de forma inmediata al personal encargado para que estén en condiciones en utilizar el nuevo protocolo invitando percances.

8. REFERENCIAS

[1] Jackson Rivera Guarnizo, *Migración a Ipv6 En La Red De La Facultad De Ciencias Administrativas De La Universidad De Guayaquil*. 2014.

[2] U. Carofilis, ""ESTUDIO PARA LA MIGRACION DEL PROTOCOLO iPV4 AL PROTOCOLO iPV6. CASO DE ESTUDIO PLENARIO DE LA ASAMBLEA NACIONAL"," p. 104, 2017.

[3] J. C. M. José Coellar Solórzano, "PROPUESTA PARA LA TRANSICIÓN DE IPv4 A IPv6 EN EL ECUADOR A TRAVÉS DE LA SUPERTEL.," vol. 1, 2013.

[4] G. F.-T. and L. E. R. Galindo, "Estudio sobre la Red de la Empresa NETUNO para la Implementación de IPv6 en su Plataforma de Multiservicio para el Segundo Semestre de 2011.pdf."

[5] D. X. Landy Rivera, "Propuesta de un Plan de Implementación para la migración a IPV6 en la red de la Universidad Politécnica Salesiana Sede-Cuenca," p. 179, 2013.

[6] David L. García vargas, "Diseño de una estrategia de migración de la red actual de la Universidad Católica Andrés Bello a una red basada en IPv6.pdf."

[7] David F. Núñez Lara, "Estudio para la migración de IPv4 a IPv6 para la empresa proveedora de internet MILLTEC S.A, Quito: Tesis.Escuela de Electrónica.Ingeniería.Escuela Politecnica Nacional, 2009.," 2009.

[8] J. A. B. D. DIEGO FERNEY RAMÍREZ PULIDO, JAIME GUZMÁN PANTOJA, "DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA AGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6," 2015.

[9] A. A. Cujilán Rojas, "Diseño de un plan de migración y seguridad de IPV4 a IPV6 para una red educativa.," p. 160, 2017.

[10] E. F. Morales, "MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO," 2009.

[11] A. . Fallis, "'Rediseño De La Red Con Calidad De Servicios Para Datos Y Tecnologia De Voz Sobre Ip En El Ilustre Municipio De Ambato,'" *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[12] G. K. Chávez and L. G. Tuárez, “Propuesta de red de datos para la gestión de los servicios de red en el Campus Politécnico de la ESPAM MFL.,” p. 107, 2016.

[13] E. V. EDWIN ALEXANDER SEGURA CRUZ, “‘METODOLOGIA PARA HACER UNA TRANSICION EN UNA RED IPV4 A IPV6,’” *tesis*, 2017.

[14] DIANA CATALINA FONSECA CASTRO, “PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 BASADO EN LAS MIN TIC COLOMBIA PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 BASADO EN LAS,” 2017.

[15] A. Estrada-Corona, “Protocolos TCP/IP de internet,” *Rev. Digit. Univ.*, vol. 5, p. 7, 2004.

[16] R. Internet, “Direccionamiento IP,” pp. 1–13, 2010.

[17] C. S. Manayay Ramírez and R. E. Olivera Samamé, “Migración de IPv4 a IPv6 para mejorar la seguridad y velocidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo,” 2015.

[18] J. Ruiz-Vanoye, O. Díaz-Parra, R. Ponce Medellín, and M. Bernábe Loranca, “Proveedores de servicios de tecnología: ventajas y desventajas,” *Gestión las Pers. y Tecnol.*, no. 12, pp. 86–91, 2011.

[19] L. J. M. MORENO, “Propuesta de diseño para la transición del protocolo de internet versión 4 (IPv4) al protocolo de internet versión 6 (IPv6) en la empresa MARKET MIX S.A.S.,” 2015.

[20] D. Pantoja, “PLANIFICACIÓN DE PROCESOS PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 PARA LA CONTINUIDAD DEL SERVICIO EN LOS ISP’s,” no. June, 2016.

[21] E. A. S. C. EDWIN, “METODOLOGIA PARA HACER UNA TRANSICION EN UNA RED IPV4 A IPV6,” 2017.

[22] E. R. Camargo Acevedo, “Plan De Transicion De Protocolo De Red Ipv4 A Ipv6 En La Universidad Industrial De Santander.,” 2006.

[23] Gualpa Caicedo Leonardo Enrique Malán Mullo Marco Vinicio, “ESTUDIO ESTUDIO Y CONFIGURACIÓN PARA LA INTEGRACIÓN DE ELEMENTOS DE SEGURIDAD BAJO LINUX , CONFIGURABLE MEDIANTE UNA INTERFAZ

WEB QUE SOPORTE LOS PROTOCOLOS IPv4 E IPv6 SIMULTÁNEAMENTE,” p. 247, 2008.

[24] M. B. M. F. Ing., “‘PROVEEDOR DE SERVICIOS DE INTERNET INALÁMBRICO USANDO TECNOLOGÍA WI-FI CON IPV6 Y MPLS PARA LAS PARROQUIAS: SANTA ROSA, PILAHUÍN, PASA Y SAN FERNANDO’.,” 2013.

[25] Marco Antonio Tomy Baltazar, “Modelo de referencia de transicion de IPv4 a IPv6 para el sector Gobierno de Peru,” p. 75, 2017.

[26] S. Bazán and V. Franco, “Comunicación De Datos En La Red De La Sede Central Del Ministerio Público – Distrito Fiscal Cajamarca 2017 Central Del Ministerio Público – Distrito Fiscal Cajamarca 2017,” 2017.

[27] Ramírez Mosquera Danilo Enrique Hidalgo Pazmiño José de Jesús, “INVESTIGAR Y DESARROLLAR UNA GUÍA METODOLÓGICA DE LOS MECANISMOS DE TRANSICIÓN Y COEXISTENCIA IPV4-IPV6 EN EL ÁREA DE SISTEMAS DE LA FACULTAD DE INGENIERÍA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO,” 2010.

[28] J. Serrato, “IMPLEMENTACIÓN DE SERVICIOS PARA OFRECER CONECTIVIDAD IPv6 EN RedUNAM,” 2018.

[29] M. Gabriela, “PROPUESTA DE TRANSICIÓN DE SERVICIOS DE IPv4 A IPv6 PARA LA RED DE DATOS CABLEADA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL SAN MIGUEL DE IBARRA,” pp. 1–16, 2016.

[30] V. F. Sánchez Bazán, “Implementación del Protocolpo IPv6 para la comunicación de datos en la red de la sede central del Ministerio Público - Distrito Fiscal Cajamarca,” 2017.

[31] Danilo Santiago Hidalgo Villavicencio and L. R. G. Machado, “ESTUDIO DE LAS METODOLOGÍAS DE MIGRACIÓN DE IPv4 A IPv6 APLICADA A UNA PROPUESTA TÉCNICA PARA EL ISP FASTNET CIA.LTDA,” p. 206, 2013.

[32] J. D. Novoa, L. A. Gamboa, and G. A. Higuera, *LA TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6 EN UNA EMPRESA : REVISIÓN Y CASO TRANSITION TO THE PROTOCOL IPV4 TO IPV6 IN A COMPANY : REVISION AND CASE*. 2018.

[33] E. F. M. Cal, “MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO,” 2009.

[34] J. Coellar Solórzano and J. Cedeño Mendoza, “Propuesta para la transicion de IPv4 a IPv6 en el Ecuador de la Supertel,” 2013.

ANEXOS

ANEXO 1: Aplicación de la Entrevista.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

Instrucciones: Sírvase leer con atención las preguntas que se plantean a continuación y responda marcando la opción que usted considere pertinente.

Entrevista aplicada al Ing. Christian Rubén Vaca Farinango, gerente de G&S INGENIEROS.Cia Ltda. en el cual se pudo obtener respuestas claras para realizar la propuesta tecnológica en la empresa.

Pregunta 1

¿Cuál es el proveedor de servicio de Internet con la que trabaja su empresa?

- **Cnt**
- **Punto net**
- **Neflite**
- **MegaSpeed**

El proveedor de internet con la que nuestra empresa cuenta en la actualidad es CNT EP (Corporación Nacional de Telecomunicaciones), debido a que nos brindan un servicio más eficiente.

Pregunta 2

¿Qué tipo de protocolo esta implementada en su empresa?

- **IPv4**
- **IPv6**

Bueno en cuanto al protocolo que estamos utilizando dentro de la empresa es el protocolo IPv4 las cuales están asignadas en cada máquina de nuestra empresa con la funcionalidad principal que es compartir datos a través de máquinas en red.

Pregunta 3

¿Qué marcas de router y Switch tiene la empresa?

- **Tp-link**
- **Cisco**

- **Mikrotik**

En la empresa contamos con routers de marca MIKROTIK la cual está configurada con el protocolo IPv4 y nos brinda internet y Switch plano que sirve para conectar las diferentes máquinas que se encuentran conectado en la empresa, localizados en el primer piso y segundo piso, y porque elegimos eso fue porque son routers empresarial y se les puede definir el ancho de banda.

Pregunta 4

¿Estaría dispuesto a migrar todos sus datos a un nuevo protocolo?

- **Si**
- **No**

Bueno en cuanto al nuevo protocolo me supo manifestar mi encargo del departamento de TIC´s que este trabaja con 128 bits y de tal manera que podríamos trabajar de una manera más rápida al momento de enviar paquetes y de forma segura ya que en este protocolo no abra saturación de redes.

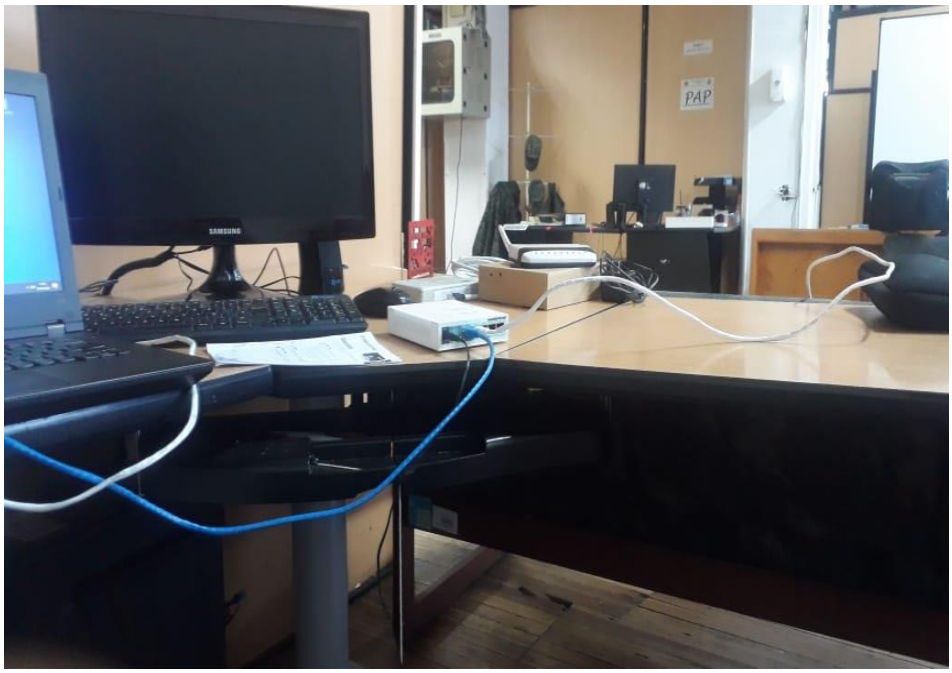
Pregunta 5

¿Conoce usted algunos de estos métodos de transición?

- **Dual Stack**
- **Tunneling**
- **Traducción**

Mi encargo del departamento de TIC´s me supo manifestar que existen 3 tipos de migración como el dual stack, tunneling y traducción. Como el dual están me menciona que es para grandes empresas el de tipo de tunneling se los puede configurar de forma manual y automáticamente este mecanismo es el más sonado a nivel empresarial y me gustaría utilizar la configuración de este Tunnel y el de traducción es la unión de los dos tipos de migración.

ANEXO 2: Conexión del primer equipo.

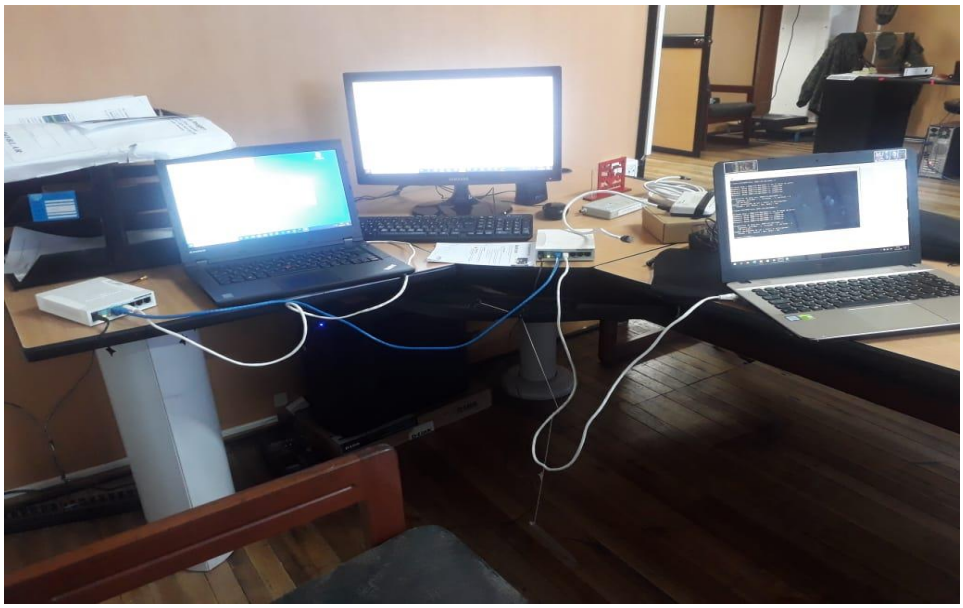


Fuente: Grupo de investigación.

ANEXO 3: Conexión del segundo equipo.

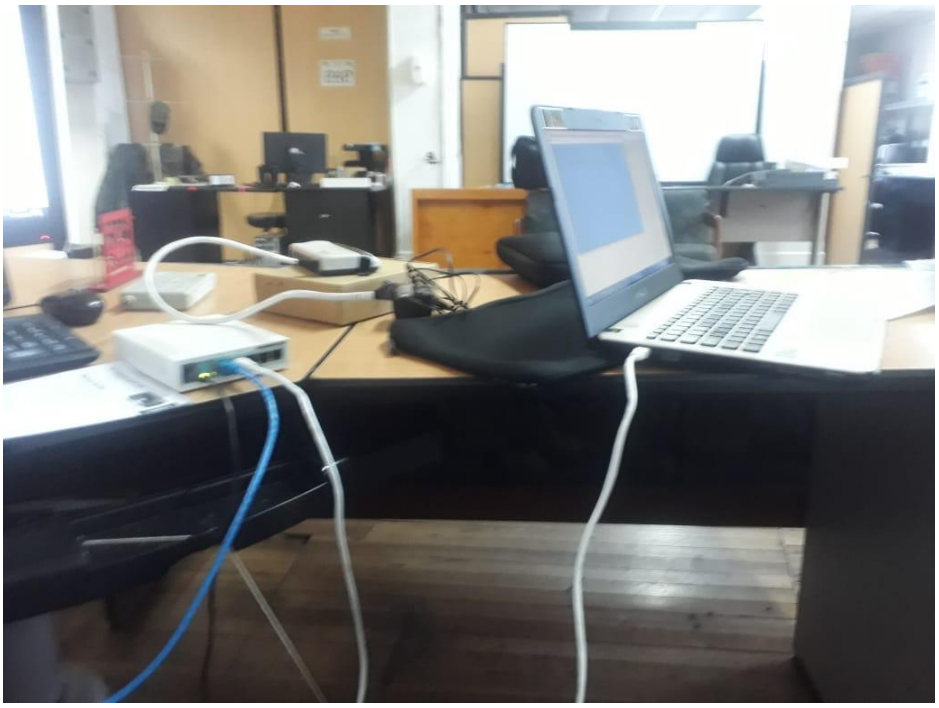
Fuente: Grupo de investigación.

ANEXO 4: Pruebas entre dos Equipos.



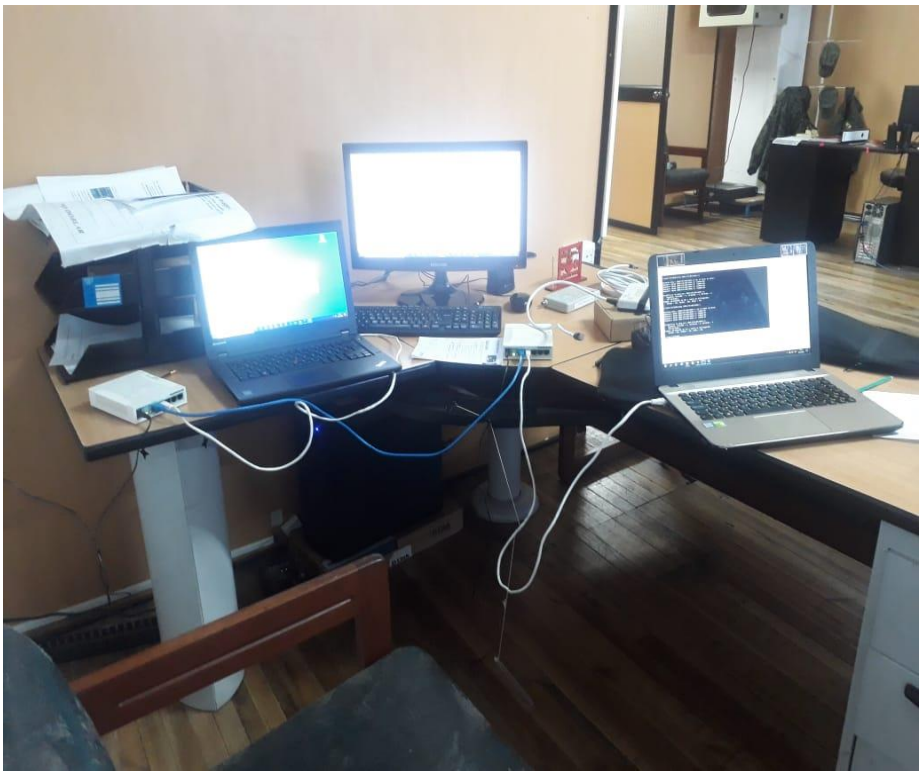
Fuente: Grupo de investigación.

ANEXO 5: Conexión entre el equipo y el router.



Fuente: Grupo de investigación.

ANEXO 6: Implementación total con la tunelización.



Fuente: Grupo de investigación.