UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

TESIS DE GRADO

MODELO DE MIGRACIÓN DE RED IPV4 AL PROTOCOLO IPV6 PARA REDES EMPRESARIALES

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN: INGENIERÍA DE SISTEMAS INFORMÁTICOS

POR: ANA CAROLINA CHUI SALAS
TUTOR: M.SC. REYNALDO ZEBALLOS DAZA

LA PAZ – BOLIVIA
2022

HOJA DE CALIFICACIONES

UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÁTICA

Tesis de Grado:

MODELO DE MIGRACIÓN DE RED IPV4 AL PROTOCOLO IPV6 PARA REDES EMPRESARIALES

Presentado por: Ana Carolina Chui Salas

Para optar por el grado Académico de Licenciada en Informática

Mención Ingeniería de Sistemas Informáticos

Nota Numeral: 100

Nota Literal: Cien

Ha sido: Aprobada con Mención Honorifica

Director de la Carrera de Informatica: M.Sc Hermenegildo Nogales

Tutor: Lic. Reynaldo Javier Zeballos Daza

Asesor: Lic. Reynaldo Javier Zeballos Daza

Tribunal: Lic. Brigida Alexandra Carvajal Blanco

Tribunal: Lic. Manuel Ramiro Flores Rojas

Tribunal: M.Sc. Menfi Morales Rios

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

Esta tesis se la dedico a Dios quien me guio por el buen camino, me dio las fuerzas necesarias para superar los momentos difíciles y poder culminar con éxito mi tan anhelada carrera.

A mis padres Osvaldo Chui e Irma Salas por su apoyo, comprensión, amor y sacrificio para ayudarme con los recursos económicos en mi formación académica.

A mis hermanos Lic. Diego Chui y Lic. Paola Chui, que con su presencia, cariño y respaldo me impulsan a salir adelante además de celebrar mis logros como suyos.

A mis amigos y amigas, quienes sin esperar nada a cambio compartieron conmigo alegrías y tristezas durante los 5 años de carrera.

AGRADECIMIENTOS

Esta Tesis de Grado es un esfuerzo en el cual directa o indirectamente participaron distintas personas que deseo agradecer en este apartado.

A Dios por la fuerza y la sabiduría que me dio para cumplir con todas mis metas y sueños también por la grandiosa familia que me dio y me apoyo en todo momento.

A mi Tutor y gran Docente de la carrera de Informática Lic. Reynaldo por sus sugerencias, correcciones y el tiempo que invirtió en este trabajo. A mi Docente de taller de Licenciatura Ph. D. Fátima por su dedicación, paciencia y consejos brindados para poder culminar con éxito este trabajo.

A mis padres, que son lo más sagrado que tengo en la vida, por ser siempre mis principales motivadores y los formadores de lo que soy ahora como persona.

A mi hermano, pues fue el principal cimiento para la construcción de mi vida profesional, siempre ha buscado la manera de ayudarme, brindándome su confianza y apoyo incondicional. Mi hermana quien me ha escuchado y aconsejado con la paciencia que la caracteriza, ha sido un soporte emocional importante. Mi cuñada Blanca quien nunca me negó un favor y mi sobrina Constanza que con sus risas y juegos, se encargaba de disipar mi estrés y preocupación.

A mis amigos Nitia, Enrique, Adad, Alvaro, Carlos, Mireya, Aramiz, Henry, Omar, Milenka, Melissa, que hicieron divertido todo este trayecto, ya que con su amistad me alientan a seguir mejorando como amiga, estudiante y persona.

A mi amuleto de la buena suerte, mi gatita Katy, mi compañera fiel durante los últimos 8 años y todas las noches de desvelo, nada más bastaba verte dormida a mi lado para no sentirme sola y trabajar a gusto.

También le agradezco a BTS, por el mensaje que transmiten con su música y como personas, me ayudaron a encontrarme a mí misma cuando veía todo gris y perdí el rumbo de lo que quería ser, inspirándome a seguir luchando, me brindaron momentos gratos llenos de felicidad. Gracias a ellos comprendí que debo amarme por quien soy, por quien fui y por quien espero ser. “La vida continúa y hay que vivirla, nacimos para ser reales no perfectos”. MUCHAS GRACIAS.

achuisalas@gmail.com

RESUMEN

El interés por internet ha ido creciendo de manera exponencial en todo el mundo extendiendo este servicio a diversos dispositivos, provocando así el agotamiento de direcciones IPv4 que se tenía disponibles obligando a las empresas a utilizar recursos recuperados. Como solución a esta problemática se crea un nuevo protocolo de direccionamiento: IPv6, aunque su despliegue total no es una realidad para las pequeñas empresas en Bolivia.

La presente tesis plantea un Modelo de migración de red IPv4 al protocolo IPv6 para redes empresariales, el cual se estructura en cuatro fases que responden al criterio metodológico de la investigación proyectiva.

En la fase exploratoria se darán pautas acerca del protocolo IPv4 y sus limitaciones, las características del protocolo IPv6, también los mecanismos de migración que existen. La fase descriptiva presenta un análisis de los diferentes mecanismos de transición, con la cual se definió que la técnica de migración Túnel GRE es la que mejor se ajusta al modelo, en la fase proyectiva se implementó el modelo de migración en un prototipo de red empresarial en el simulador Cisco Packet Tracert donde se hicieron las pruebas al modelo para la fase evaluativa, obteniendo Menor Latencia, Mayor rendimiento y 0% de pérdida de paquetes.

Se concluye de las pruebas, que el modelo de migración mitiga el agotamiento de direcciones IPv4, mejorando la calidad de servicio de la Red de Datos; aplicándose el modelo en cualquier empresa siempre que se tenga en cuenta la topología de red correspondiente y los límites del modelo.

Palabras Claves: Internet, protocolo, IPv4, IPv6, migración, red de datos.

ABSTRACT

Interest in the Internet has been growing exponentially throughout the world, extending this service to various devices, thus causing the exhaustion of IPv4 addresses that were available, forcing companies to use recovered resources. As a solution to this problem, a new addressing protocol is created: IPv6, although its full deployment is not a reality for small companies in Bolivia.

This thesis proposes a migration model from the IPv4 network to the IPv6 protocol for business networks, which is structured in four phases that respond to the methodological criteria of projective research.

In the exploratory phase, guidelines will be given about the IPv4 protocol and its limitations, the characteristics of the IPv6 protocol, as well as the migration mechanisms that exist. The descriptive phase presents an analysis of the different transition mechanisms, with which it was defined that the GRE Tunnel migration technique is the one that best fits the model, in the projective phase the migration model was implemented in a business network prototype in the Cisco Packet Tracert simulator where the tests were made to the model for the evaluation phase, obtaining Lower Latency, Higher performance and 0% packet loss.

It is concluded from the tests that the migration model mitigates the exhaustion of IPv4 addresses, improving the quality of service of the Data Network; applying the model in any company as long as the corresponding network topology and the limits of the model are taken into account.

Keywords: Internet, protocol, IPv4, IPv6, migration, data network.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1. INTRODUCCIÓN

Actualmente, el interés por Internet ha ido creciendo de manera exponencial en todo el mundo, lo cual ha significado para las redes de computadoras una mejora continua en su estructura para brindar un mejor servicio, incrementando la disponibilidad, confiabilidad e integridad. Sin embargo, el uso excesivo de dispositivos móviles conectados a internet nos ha conducido al agotamiento de direcciones IP. "El 19 de Agosto de 2020, LACNIC agotó su pool de direcciones IPv4, contando actualmente sólo con recursos recuperados y devueltos y una reserva destinada exclusivamente a infraestructura crítica". (LACNIC, 2021)

LACNIC, que ha asignado 189,3 millones de direcciones IPv4 a más de 11.200 organizaciones y empresas de América Latina y el Caribe, enfatizó su llamado a "acelerar el despliegue de IPv6 en sus redes y acelerar el crecimiento de Internet" en la región. La Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), promueve la migración a IPv6 siendo participe de un taller sobre "Despliegue de Implementación del IPv6 en Bolivia" (ATT, 2016), que contó con la participación internacional del personal del Registro de Direcciones de Internet para Latinoamérica y el Caribe (LACNIC). Sin embargo hasta la fecha no se tiene un modelo de migración a IPv6 para redes empresariales, mucho menos una guía de procedimientos para la transición.

La implementación del protocolo IPV6, permitirá una mejor comunicación en cualquier ordenador, mayor espacio de direccionamiento, seguridad, autoconfiguración, movilidad y privacidad en la información que viaja en la red.

Para llevar a cabo la transición de una red con protocolo IPV4 a IPV6 en una empresa, se debe generar el pre diseño, diseño, simulaciones, pruebas, antes de empezar cualquier manipulación de equipos, información o configuraciones sobre estos. Si hay alguna manipulación incorrecta de esta información, se puede generar fallas sobre la red o errado funcionamiento de la misma.

Como el énfasis es generar la transición de una red empresarial en protocolo IPV4, al protocolo IPv6, es importante implementar dicha red en un simulador el cual cuente con

toda la información de equipos, configuraciones, seguridad de red y servicios para poder generar y manipular cambios, así como la respectiva transición de los protocolos y las respectivas pruebas.

1.1. ANTECEDENTES

1.1.1. Internacional

Estados Unidos

- Nguyen, P., & Nguyen, Q. (2016). "Transition from IPv4 to IPv6 Best Transition Method for Large Enterprise Networks" (Licenciatura). Lahti University of Applied Sciences.

  Este estudio analizó las experiencias de varias grandes empresas que habían implementado IPv6. Los factores clave sobre el éxito y el fracaso de la implementación de IPv6 se sintetizaron a partir de los hallazgos de esas empresas. Tomando así todas las características de la red y poder inducir cuál de las técnicas estudiadas podría acomodarse mejor, teniendo en cuenta la opción de las empresas en cuanto a requerimientos se refiere, estos son tomados como puntos referenciales para continuar el funcionamiento correcto de la Red. Los resultados de los datos recopilados revelan varios factores importantes que afectan el proyecto de implementación de IPv6. Por lo tanto, se concluyó una solución, el método de transición más aplicable.

1.1.2. Latinoamérica

Perú

- Enriquez Castillo, A. L., & Ñurega Sanchez, G. M. (2017). "Migración de IPv4 a IPv6 de la Red de datos de la Universidad Nacional de Trujillo" (Licenciatura). Universidad Nacional de Trujillo.

  Estudió a fondo del protocolo IPv6, describiendo las principales técnicas que permiten la coexistencia entre IPv4 e IPv6, como técnicas Dual Stack, que permiten a IPv4 y a IPv6 coexistir en los mismos dispositivos y redes.

Técnicas de Tunneling, que permiten el transporte de tráfico de IPv6 a través de la infraestructura de IPv4 existente y Técnicas de traducción, que permiten comunicar nodos IPv6 con nodos IPv4. En base al análisis de las diferentes técnicas de migración se cree conveniente usar el mecanismo Tunneling-6to4 que es el que más se adecua al escenario y permite la coexistencia de ambos protocolos.

Ecuador

- Carofilis Moreira, U. A. (2017). "Estudio para la migración del protocolo IPv4 al protocolo IPv6. Caso de estudio plenario de la asamblea nacional" (Maestría). Pontificia Universidad Católica del Ecuador.

  Realizó un análisis al caso de estudio, con el cual permitió diseñar un plan de implementación para migrar la red del Plenario de la Asamblea Nacional hacia el protocolo IPv6, no sin antes explicar las características del protocolo IPv4, incluyendo los beneficios y problemas que proporciona el nuevo protocolo. La situación de la red de la asamblea fue analizada rigurosamente, así como sus elementos de hardware y software, lo que permitió definir en qué medida estos soportaban la migración. Algunas metodologías para la migración fueron analizadas dentro del marco teórico y se diseñó la solución para la migración al protocolo IPv6

1.1.3. Nacional

La Paz

- Yapu Apaza, H. (2016). "Plan de implementación para la migración de IPv4 a IPv6 en la red de COTEL" (Licenciatura). Universidad Mayor de San Andrés.

  Elaboró un plan estratégico de implementación para la migración del protocolo IPv4 al protocolo IPv6 en la red de COTEL Ltda. Para permitir que la compañía pueda garantizar la conectividad a Internet de todos sus clientes y cumplir con la demanda actual y futura de servicios basados en IPv6, de esta manera el proveedor de servicios de Internet COTEL Ltda., continuará operando en el ámbito de las telecomunicaciones a un mayor nivel de

competitividad. Se logró evaluar los distintos equipos y componentes de la actual infraestructura de red, con el objetivo de determinar los cambios a efectuar antes de iniciar el proceso de migración, donde se definió conservar la actual infraestructura realizando previamente actualizaciones al software de la empresa.

- Roca Marín, R. D. (2009). "Propuesta de estrategia nacional para la implementación de IPv6 en Bolivia" (Licenciatura). Universidad Mayor de San Andrés.

  Desarrolló una estrategia para la implementación del protocolo IPv6 en Bolivia basándose en una serie de buenas prácticas institucionales, dirigidas a las instituciones gubernamentales, académicas y privadas. Identificándolos también a los principales actores que deben intervenir para el despliegue de IPv6, concluyendo que no se necesita una gran inversión en hardware ni en software, la mayor inversión será en capital humano; es decir que se necesita de la participación y capacitación del personal.

Cochabamba

- Llanos Gómez, R. A. (2016). Plan de migración de IPv4 a IPv6 para una red de un proveedor de servicios de internet (ISP). Journal Boliviano de Ciencias, 12(36).

  Identificó la red genérica de un proveedor de servicios Internet, que sirvió para realizar la propuesta de migración de IPV4 a IPV6 en las redes de proveedores de Internet ISP, migración basada en las fases sistemáticas planteadas que permitieron realizar el propósito de la Transición.

  Elaborando así un plan de migración IPv4 a IPv6 para una red genérica un proveedor de servicios de Internet (ISP).

  El plan detalla los pasos metódicos de las fases propuestas que se debe tomar a consideración para la migración de IPv4 a IPv6, a demás cita procesos de enrutamiento y direccionamiento.

- Cooperativa de Telecomunicaciones Cochabamba Ltda. (COMTECO). La Cooperativa de Telecomunicaciones de Cochabamba es el operador que ha impulsado hasta el momento el despliegue de IPv6 en Bolivia (LACNIC, 2015), siendo responsable del alto indicador relativo de Bolivia en cuanto a usuarios potencialmente habilitados para IPv6. Es prestadora de servicios de televisión por cable, telefonía móvil a través de su participada NUEVATEL - VIVA, larga distancia, banda ancha, internet satelital, televisión satelital y otros. A fines de 2010 tomó la decisión de desplegar IPv6 en su red, en 2012 solicitó un prefijo IPv6 a LACNIC y en 2013 levantó un enlace BGP en IPv6 con su proveedor de tránsito y publicó el prefijo 2803:9400::/32. En marzo de 2014 se realizaron las primeras pruebas y se inició el despliegue al cliente el 22 de agosto de 2014 con la técnica Dual Stack. Actualmente, mientras crece su base de usuarios IPv6, continúa desarrollando estas tareas de transición a IPv6: configuración de los elementos de la granja de servidores, DNS, Firewalls, Antispam y portales de autenticación.

1.2 PLANTEAMIENTO DEL PROBLEMA

IPv4 es la versión 4 del Protocolo de Internet (IP o Internet Protocol) y constituye la primera versión de IP que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet.

Proporciona 2^{32} direcciones IP, es decir poco más de 4 mil millones de direcciones, en un comienzo esta parecía una cantidad suficiente para poder conectar a todos los usuarios a Internet, pero muchas de estas están reservadas para propósitos especiales como redes privadas, multidifusión, etc.

Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar; y hasta la fecha internet fue cambiando en distintos aspectos desde el incremento en la cantidad de usuarios y el uso de dispositivos móviles conectados a internet, hasta el surgimiento de nuevas tendencias tecnológicas como el IoT que conectan una cantidad considerable de dispositivos; lo cual implica una mayor demanda de

direcciones, pero el direccionamiento con clases ha hecho que el uso y la repartición de las direcciones IPv4 sean ineficiente. En consecuencia esto nos ha llevado al Agotamiento de direcciones IPv4, impulsando así la creación de IPv6 como su reemplazo a largo plazo.

Si las redes utilizan únicamente direcciones IPv4, disminuye las posibilidades de ampliar la red, se podrían perder servicios, la implementación de tendencias tecnológicas podría causar problemas y mantener la red resultara más costoso debido a que el precio de las direcciones IPv4 van en aumento; todo esto afecta la red disminuyendo la estabilidad, disponibilidad y seguridad a nivel IP. (Véase Anexo 1)

1.2.1. Formulación del problema

¿Cómo mitigar el agotamiento de direcciones IPv4 disponibles para redes Empresariales?

1.3 HIPÓTESIS

El modelo de migración de red al protocolo IPv6 mitigará el agotamiento de direcciones IPv4 disponibles para redes Empresariales en al menos un 50%.

1.3.1. Variables de Estudio

A. Variable Dependiente

- Agotamiento de direcciones IPv4.

B. Variable Independiente

- Modelo de migración de red al protocolo IPv6.

1.4. OBJETIVOS

1.4.1. Objetivo General

Desarrollar un modelo de migración de red al protocolo IPv6, para mitigar el agotamiento de direcciones IPv4 disponibles para redes Empresariales.

1.4.2. Objetivos Específicos

- Recolectar información sobre las técnicas de migración al protocolo IPv6
- Optar por una técnica de transición para la migración del protocolo IPV4 a IPv6
- Diseñar una solución para la migración a IPv6
- Implementar un prototipo de red empresarial con la técnica de migración optada

1.5. JUSTIFICACIÓN

1.5.1. Justificación Social

Las necesidades de las empresas por siempre conectadas a Internet han aumentado exponencialmente, exigiendo nuevas capacidades que IPV4 no proporciona, como: la seguridad, privacidad, velocidad, multimedia, teleconferencias y aplicaciones de gran demanda. Es por eso, que se ha visto en la necesidad de diseñar un modelo que permita la coexistencia con el protocolo IPv6.

1.5.2. Justificación Tecnológica

Servirá como guía para futuras investigaciones acerca del protocolo IPV6, ayudando y esclareciendo algunas interrogantes, como las ventajas que implica migrar a dicho protocolo. Además usando el protocolo IPV6 se promoverá el uso de nuevas tecnologías que solo este protocolo brinda, colocando a Empresas en la vanguardia sobre nuevas tecnologías de información.

1.5.3. Justificación Económica

Generará ahorro a largo plazo, ya que mantener una red IPV6 será menos costoso que una red IPV4. Por lo tanto, la migración a IPv6 realizado con antelación es más económico que una migración tardía.

1.6. LÍMITES Y ALCANCES

1.6.1. Límites

Los límites están definidos principalmente en la aplicación de la siguiente ya que una empresa deberá autorizar la implementación del modelo. Por lo tanto la presente solo se limita al desarrollo de un modelo de migración al protocolo IPv6 en un software simulador, mas no así la implementación del modelo.

1.6.2. Alcances

El alcance fundamental que tendrá la investigación será analizar las ventajas que traerá la migración de IPv4 a IPv6 en aspectos como son la seguridad, comunicación y escalabilidad y las limitaciones por las que atraviesa el protocolo IPv4. También se realizará un vasto estudio que permitirá definir una técnica de transición adecuada para el modelo.

CAPITULO II: MARCO TEÓRICO

Internet ha experimentado un crecimiento exponencial en los últimos años, expandiendo su servicio a diversos dispositivos y para que estos puedan comunicarse deben tener una dirección IP asignada. El protocolo IP cuenta con la versión 4 y 6, también existen mecanismos de migración para la coexistencia de ambos protocolos en una misma red de datos.

2.1. INTERNET.

El nombre Internet procede de las palabras en inglés Interconnected Networks, que significa "redes interconectadas". Internet es la unión de todas las redes y computadoras distribuidas por todo el mundo, por lo que se podría definir como una red global en la que se conjuntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí. En esta "red de redes" como también es conocida, participan computadores de todo tipo, desde grandes sistemas hasta modelos personales. En la red se dan citas instituciones oficiales, gubernamentales, educativas, científicas y empresariales que ponen a disposición de millones de personas su información.

Internet fue el resultado de un experimento del Departamento de Defensa de Estados Unidos, en el año 1969, que se materializó en el desarrollo de arpanet, una red que enlazaba universidades y centros de alta tecnología con contratistas de dicho departamento. Tenía como fin el intercambio de datos entre científicos y militares. A la red se unieron nodos de Europa y del resto del mundo, formando lo que se conoce como la gran telaraña mundial (World Wide Web). En 1990 ARPAnet dejó de existir (Yirda, 2021).

2.2. PROTOCOLOS DE INTERNET

El Internet son redes interconectadas en donde se comunican dos o más hosts(computadoras, tabletas, móviles, etc), y utiliza un conjunto protocolos de comunicación empleados para conformar Internet que pertenecen a la familia TCP/IP (Transmisión Control Protocol/ Internet Protocol).

TCP/IP es un conjunto de protocolos de red y 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 la hace capaz de soportar las comunicaciones entre equipos conectados a gran número de redes heterogéneas, independientes de un vendedor. Su origen es: solucionar las comunicaciones a través de la red ARPANET para el Departamento de Defensa de USA (Departamen of Defense 1.972). Comienza su utilización en DARPA (Agencia de proyectos de investigación avanzada para la defensa). En 1983 se convierte en estándar para DoD (ARPANET + MILNET) (Kurose & Ross, 2017, p. 4).

Sus principales características son:

- Utiliza conmutación de paquetes.
- Proporciona una conexión fiable entre dos máquinas en cualquier punto de la red.
- Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.
- Se apoya en los protocolos de más bajo nivel para acceder a la red física (Ethernet, Token-Ring)

2.3. PROTOCOLO DE INTERNET VERSION 4 (IPV4)

IPv4 es la versión 4 del Protocolo de Internet constituyéndose en la primera versión de IP que es implementada de forma extensiva y como principal protocolo utilizado en el Nivel de Red del Modelo TCP/IP para Internet.

IPv4 es un protocolo orientado hacia datos que se utiliza para comunicación entre redes a través de interrupciones (switches) de paquetes a través de Ethernet, el propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra.

2.3.1. Características del protocolo IPv4

El protocolo IPv4 tiene algunas de las siguientes características (Montañez, 2018):

- Es un protocolo de un servicio de datagramas no fiable, también referido como de menor esfuerzo.

- No proporciona garantía en la entrega de datos.
- No proporciona ni garantías sobre la corrección de los datos.
- Puede resultar en paquetes duplicados o en desorden.

IPv4 utiliza direcciones de 32 bits (4 bytes) que limita el número de direcciones posibles a utilizar a 4, 294,967,295 direcciones únicas. Sin embargo, muchas de estas están reservadas para propósitos especiales como redes privadas, Multidifusión, etc. Debido a esto se reduce el número de direcciones IP que realmente se pueden utilizar, es esto mismo lo que ha impulsado la creación de IPv6(actualmente en desarrollo) como reemplazo eventual dentro de algunos años para IPv4 (Montañez, 2018).

2.3.2. Encabezado de un paquete IPv4

Los diagramas de encabezado del protocolo, que se leen de izquierda a derecha y de arriba hacia abajo, La figura 1 proporciona una representación visual de consulta para analizar los campos de protocolo.

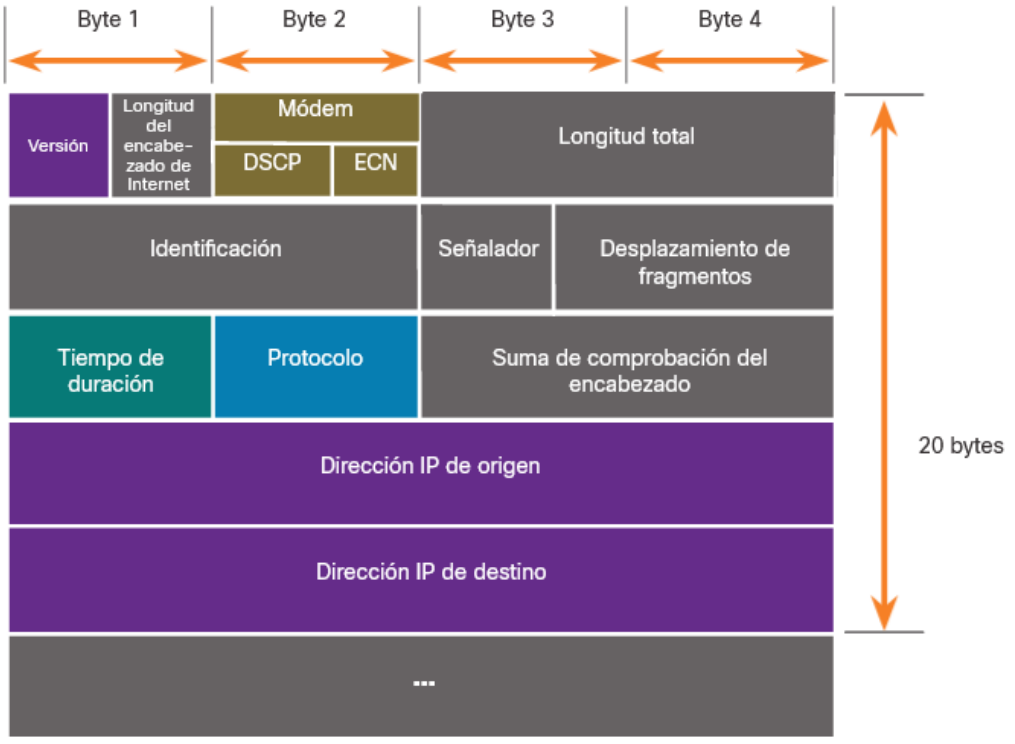


Figura 1 - Campos de un paquete IPv4

Fuente: Cisco, (2021).

Los campos significativos en el encabezado IPv4 incluyen lo siguiente:

- **Versión -** Contiene un valor binario de 4 bits establecido en 0100 que identifica esto como un paquete IPv4.
- **Longitud del encabezado de Internet (IHL) -** Identifica el paquete.
- **Servicios diferenciados o DiffServ (DS)** - Este campo, formalmente conocido como Tipo de servicio (ToS), es un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los seis bits más significativos del campo DiffServ son los bits de punto de código de servicios diferenciados **(DSCP)** y los dos últimos bits son los bits de notificación de congestión explícita **(ECN)** (Cisco, 2021).
- **Longitud total –** Valida el paquete.
- **Identificación y Señalador -** Reordenan un paquete fragmentado.
- **Desplazamiento de fragmentos** - Lleva un control de los fragmentos. Un router puede tener que fragmentar un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña (Cisco, 2021).
- **Suma de comprobación de encabezado -** Se utiliza para detectar daños en el encabezado IPv4.
- **Tiempo de duración (TTL) -** TTL contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. El dispositivo de origen del paquete IPv4 establece el valor TTL inicial. Se reduce en uno cada vez que el paquete es procesado por un router. Si el campo TTL llega a cero, el router descarta el. Debido a que el router disminuye el TTL de cada paquete, el router también debe volver a calcular la suma de comprobación del encabezado (Cisco, 2021).
- **Protocolo -** Este campo se utiliza para identificar el protocolo del siguiente nivel.
- **Dirección IPv4 de origen -** Contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete
- **Dirección IPv4 de destino -** Contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete.

Los dos campos a los que se hace más referencia son los de dirección IP de origen y de destino En estos campos, se identifica de dónde viene el paquete y a dónde va. Por lo general, estas direcciones no cambian mientras se viaja desde el origen hasta el destino.

2.4. DIRECCIONES IPV4

Una dirección IPv4 es un número de 32 bits formado por cuatro octetos (números de 8 bits) en una notación decimal como se muestra en la figura 2, están separados por puntos. Un bit puede ser tanto un 1 como un 0 (2 posibilidades), por lo tanto la notación decimal de un octeto tendría 2 elevado a la 8va potencia de distintas posibilidades (256 de ellas para ser exactos). Ya que se empieza a contar desde el 0, los posibles valores de un octeto en una dirección IP van de 0 a 255.

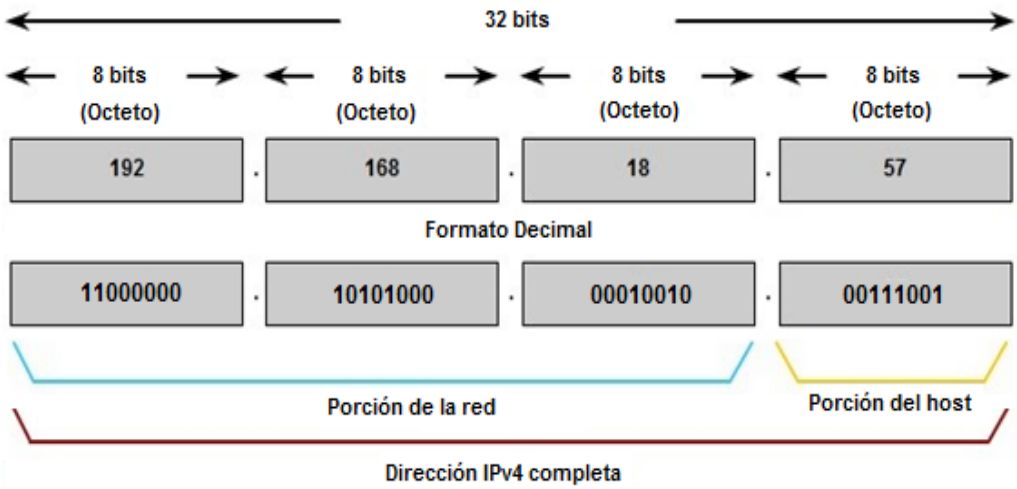


Figura 2 - Formato de direccion IPv4

Fuente: Elaboración propia

Si una dirección IPv4 está hecha de cuatro secciones con 256 posibilidades en cada sección, para encontrar el número de total de direcciones IPv4, solo debes de multiplicar 256*256*256*256 para encontrar como resultado 4,294,967,296 direcciones (Cespedes, 2013). Para ponerlo de otra forma, se tienen 32 bits entonces, 2 elevado a la 32^{va} potencia te dará el mismo número obtenido.

2.4.1. Direcciones IPv4 públicas

Una dirección IP consta de dos partes, la primera identifica la dirección de la red y la segunda sirve para identificar los equipos en la red. Las direcciones IPv4 públicas son direcciones que se enrutan globalmente entre routers de proveedores de servicios de Internet (ISP), algunos ejemplos se muestran en la figura 3. Identifica el equipo en Internet este tipo de dirección es única y no se puede repetir. Estas direcciones no se deben poner en una computadora interna ya que puede ocasionar conflictos al momento de comunicarse con el exterior (Cisco, 2021).

También tienen su rango característico y las direcciones que no estén incluidas en las clases de una IP privada son direcciones públicas.

Figura 3 - Ejemplo de direcciones IPv4 públicas

Fuente: (Molina A., 2018)

2.4.2. Direcciones IPv4 privadas

Sin embargo, no todas las direcciones IPv4 disponibles pueden usarse en Internet. Existen bloques de direcciones denominadas direcciones privadas que la mayoría de las organizaciones usan para asignar direcciones IPv4 a los hosts internos.

A mediados de la década de 1990, con la introducción de la World Wide Web (WWW), se introdujeron direcciones IPv4 privadas debido al agotamiento del espacio de direcciones IPv4. (Cisco, 2021).

Las direcciones IPv4 privadas no son exclusivas y permite que cualquier red interna puede usarlas, identifica los equipos dentro de una red de área local (LAN) es decir dentro de una empresa o red doméstica, y tienen un rango en las que se las clasifica en clase A, B, C; Algunos ejemplos se muestran en la figura 4.

- CLASE A: 10.0.0.0 hasta 10.255.255.255
- CLASE B: 172.16.0.0 hasta 172.16.31.255
- CLASE C: 192.168.0.0 hasta 192.168.255.255

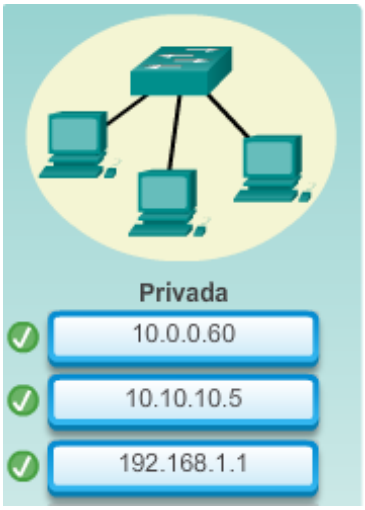


Figura 4 - Ejemplo de direcciones IPv4 privadas

Fuente: (Molina A., 2018)

2.4.3. Direccionamiento con clase antigua

En 1981, las direcciones IPv4 de Internet se asignaban mediante el direccionamiento con clase, según se define en RFC 790. A los clientes se les asignaba una dirección de red basada en una de tres clases: A, B o C. RFC dividía los rangos de unidifusión en las siguientes clases específicas:

- **Clase A (0.0.0.0/8 a 127.0.0.0/8)** - diseñada para admitir redes extremadamente grandes. La clase A reserva el primer octeto de la IP para indicar la dirección de red y los tres octetos restantes para las direcciones de host, resultando asi más de 16 millones de direcciones de host por red,

por lo que las redes de clase A corresponden fundamentalmente a organismos gubernamentales, grandes universidades, etc.

- **Clase B (128.0.0.0 /16 - 191.255.0.0 /16)** - diseñada para satisfacer las necesidades de redes de tamaño moderado a grande. La clase B usa los dos octetos de alto orden para indicar la dirección de red y los dos octetos restantes para las direcciones de host, resultando así más de 65,000 direcciones de host por red que se utilizan generalmente en grandes empresas, universidades de tipo medio, y organizaciones gubernamentales etc.
- **Clase C (192.0.0.0 /24 - 223.255.255.0 /24)** - diseñada para admitir redes pequeñas. La clase C trabaja con los primeros tres octetos para indicar la red y el octeto restante para las direcciones de host, contando con 254 direcciones de host por red que corresponden principalmente a pequeñas empresas, organismos locales, etc.

También existe un bloque de multidifusión de clase D que va de 224.0.0.0 a 239.0.0.0, y un bloque de direcciones experimentales de clase E que va de 240.0.0.0 a 255.0.0.0., se usan solo para fines de estudio e investigación.

En ese momento, con el número limitado de computadoras que utilizaba Internet, el direccionamiento con clase era un medio eficaz para asignar direcciones las redes de clase A y B tienen un número muy grande de direcciones de host y la clase C tiene muy pocas. Las redes de clase A representaron el 50% de las redes IPv4. Esto hizo que la mayoría de las direcciones IPv4 disponibles no se utilizaran.

A mediados de la década de 1990, con la introducción de la World Wide Web (WWW), el direccionamiento de clase fue obsoleto para asignar de manera más eficiente el limitado espacio de direcciones IPv4. La asignación de direcciones con clase se reemplazó con direcciones sin clase, que se usa hoy en día. El direccionamiento sin clases ignora las reglas de las clases (A, B, C). Las direcciones de red IPv4 públicas se asignan en función del número de direcciones que se pueden justificar (Cisco, 2021).

2.5. LIMITACIONES DE IPV4

2.5.1. Agotamiento de direcciones IP

Aunque se manejen 4.294.967.296 millones de direcciones, no es suficiente para la creciente demanda de redes que existen hoy en día (LACNIC, 2021). Por esta razón se ha utilizado NAT, para asignar una dirección pública a varias privadas, es un buen método para poder reutilizar las direcciones privadas, pero entonces va a conllevar a que en las comunicaciones se produzcan cuellos de botella (Kurose & Ross, 2017, p. 286). Surge entonces un nuevo protocolo denominado IPv6 con un número casi infinito de direcciones. Podemos definir entonces que es una dirección IP, todo computador conectado a Internet tiene una dirección IP, que se representa mediante un número binario de 32 bits, dividida en cuatro octetos, por ejemplo, una dirección IPv4 sería: 164.12.123.65. Para poder extender la cantidad de direcciones disponibles, las IPv6 están compuestas por 8 segmentos de 16 bits cada uno, que en total suman 128 bits, que se escriben como ocho grupos de cuatro dígitos hexadecimales, por ejemplo, una dirección IPv6 sería: 2001:0db8:85a3:08 d3:1319:8a2e:0370:7334. (Kurose & Ross, 2017, p. 289).

2.5.2. Soporte para la entrega de datos en tiempo real

Aplicaciones nuevas como video y audio, requieren QoS (Calidad de servicio), por ello, se necesita una arquitectura flexible que permita afrontar el reto que supone la movilidad de sus usuarios (Kurose & Ross, 2017, p. 284).

2.5.3. Requerimientos de Seguridad a nivel IP

La seguridad en IPv4 se consigue mediante IPSec, que es una colección de estándares diseñados específicamente para crear conexiones, punto a punto, seguras utilizando encriptación fuerte y criptografía de clave pública, que proporcionan autentificación, integridad y confidencialidad de los mensajes (Cespedes, 2013).

- **Confidencialidad**

  El tráfico de IPSec está cifrado. El tráfico de IPSec capturado no se puede descifrar si no se conoce la clave de cifrado.

- **Autenticación**

  El tráfico de IPSec está firmado digitalmente con la clave de cifrado compartida de manera que el destinatario pueda comprobar que lo envió el interlocutor IPSec.

- **Integridad de los datos**

  El tráfico de IPSec contiene una suma de comprobación criptográfica que incorpora la clave de cifrado. El destinatario puede comprobar que el paquete no se ha modificado durante la transmisión

IPSec no es actualmente parte de IPv4, pero sí de IPv6, que protege los datos IPv6 cuando se envían a través de la red.

2.5.4. Expansión en la tabla de enrutamiento de Internet

Con el aumento de nodos o servidores que están conectados a Internet, aumentan las rutas de red por lo que los routers deben manejar tablas de enrutamiento con mayor información y esto produce un aumento de recursos de la red en cuanto a memoria y procesamiento (Kurose & Ross, 2017, p. 286).

2.5.5. Necesidad de mejorar aplicaciones Multimedia

Una de las limitaciones inherentes a IPv4, es que no está preparado para soportar las nuevas aplicaciones de Internet como la transmisión de vídeo

y audio en tiempo real, aunque se han ido incorporando gradualmente ciertas mejoras (Llanos, 2016).

La adopción de IPv6 puede aumentar de manera sustancial el alcance de mercado y las ofertas de servicios dentro de este sector. La tecnología puede emplearse para videoconferencias donde pueden conectarse en diversos dispositivos fijos y móviles de uso común.

2.6. PROTOCOLO IPV6

A principios de los 90, tras la primera alerta sobre el posible agotamiento de direcciones IP. La IETF anunció la creación de grupos de trabajo de "IP de próxima generación", quienes presentaron sus primeras recomendaciones sobre el nuevo protocolo que debería reemplazar a IPv4. En el mismo año se publicó oficialmente la primera versión del protocolo IPv6 (Cespedes, 2013). En muchos aspectos, IPV6 es considerado como una evolución respecto al protocolo IPV4. Ya que se han mantenido los conceptos principales del protocolo, añadiendo nuevas y mejores características que buscan solucionar los problemas existentes en el protocolo IPV4 (Molina, 2018).

2.6.1. Características del protocolo IPV6

Las principales características de IPV6 son (Kurose & Ross, 2017, p. 290):

- **Mayor número de direcciones:** El tamaño de una dirección aumenta desde 32 a 128 bits lo que se traduce en alrededor de 3,4·1038 direcciones disponibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.
- **Direccionamiento jerárquico:** Las direcciones IPv6 globales están diseñadas para crear una infraestructura eficiente, jerárquica y resumida de enrutamiento basada en la existencia de diversos niveles de ISP. Esto permite contar con tablas de enrutamiento más pequeñas y manejables.

- **Nuevo formato de cabecera:** Aun cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado 14 campos que en la práctica eran poco usados, de forma de hacer más eficiente el manejo de los paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.
- **Autoconfiguración:** IPv6 incorpora un mecanismo de auto configuración de direcciones, "stateless address configuration", mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

- **Nuevo protocolo para interactuar con vecinos:** El protocolo de descubrimiento de vecinos, reemplaza a los protocolos ARP y "Router Discovery" de IPV4.
- Una de sus mayores ventajas es que elimina la necesidad de los mensajes del tipo "broadcast"

2.6.2. Encabezado de un Paquete IPV6

La cabecera básica IPv6 es más simple que la de IPv4 como se muestra en la figura 5, ésta tiene 8 campos en lugar de 12. El campo Longitud de Cabecera es removido así como el de Checksum, se agrega el campo Etiqueta de Flujo. De las extensiones son removidos los campos de fragmentación. El tamaño de la cabecera básica es de 40 octetos, que es el doble de la de IPv4. Esto es debido en parte a que se incrementaron los campos Dirección origen y Dirección destino de 4 octetos a 16 octetos cada uno, o sea que el tamaño de las direcciones es 4 veces mayor (Kurose & Ross, 2017, p. 289).

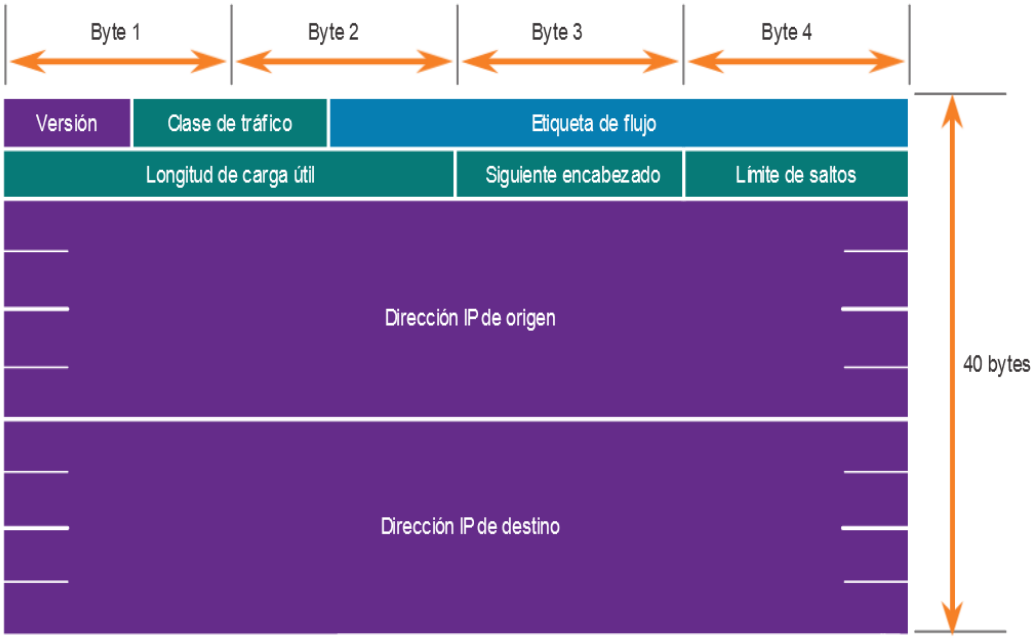


Figura 5 - Campos de un paquete IPv6

Fuente: (Cisco, 2021)

La cabecera posee los siguientes 8 campos (Kurose & Ross, 2017, p. 291):

- **Versión:** Indica la versión del protocolo IP, en este caso su valor es igual a 6.
- **Clase de tráfico:** Incluye información que permite a los "routers" clasificar el tipo de tráfico al que el paquete pertenece, aplicando distintas políticas de enrutamiento según sea el caso. Realiza la misma función que el campo "Type of Service" de IPv4.
- **Etiqueta de flujo:** Identifica a un flujo determinado de paquetes, permitiendo a los "routers" identificar rápidamente paquetes que deben ser tratados de la misma manera.
- **Longitud de carga útil:** Indica el tamaño de la carga útil del paquete. Las cabeceras adicionales son consideradas parte de la carga para este cálculo.
- **Siguiente encabezado:** Indica cual es el siguiente cabecera es la siguiente cabecera adicional presente en el paquete. Si no se utilizan, apunta hacia la cabecera del protocolo capa 4 utilizado.

- **Límite de saltos:** Indica el máximo número de saltos que puede realizar el paquete. Este valor es disminuido en uno por cada "router" que reenvía el paquete. Si el valor llega a cero, el paquete es descartado.
- **Dirección de Origen:** Indica la dirección IPv6 del nodo que generó el paquete.
- **Dirección de Destino:** Indica la dirección de destino final del paquete.

2.7. DIRECCIONES IPv6

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cada cuatro bits está representado por un solo dígito hexadecimal; para un total de 32 valores hexadecimales, como se muestra en la figura 6. Las direcciones IPv6 no distinguen entre mayúsculas y minúsculas, y pueden escribirse en minúsculas o en mayúsculas (Cisco, 2021).

La figura anterior también muestra que el formato preferido para escribir una dirección IPv6 es x: x: x: x: x: x: x: x, donde cada "x" consta de cuatro valores hexadecimales. El término octeto hace referencia a los ocho bits de una dirección IPv4. En IPv6, un "hexteto" es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada "x" es un único hexteto que tiene 16 bits o cuatro dígitos hexadecimales (Carofilis, 2017).

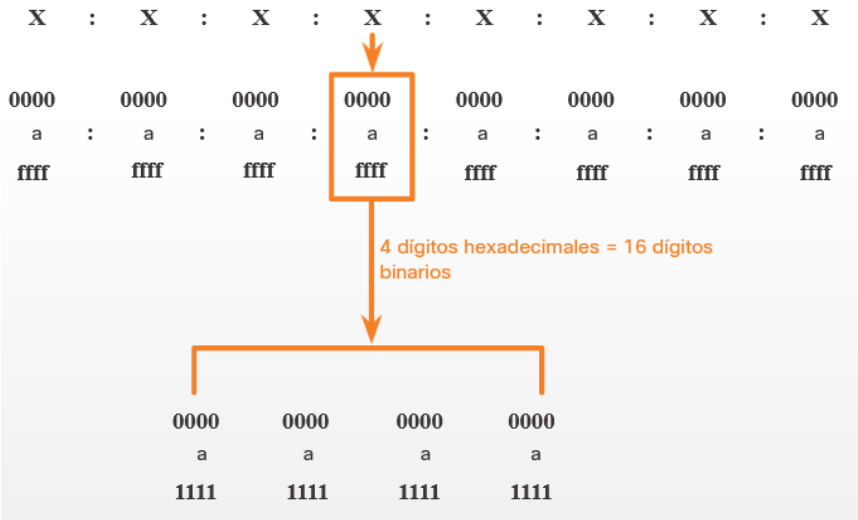


Figura 6 - Formato de dirección IPv6

Fuente: (Cespedes, 2013).

Al igual que IPv4 clasifica las direcciones en públicas y privadas, IPv6 tiene su propia clasificación las direcciones: Unicast, Anycast y Multicast.

2.7.1. Dirección Unicast

Identifica una interfaz de un solo nodo, esto quiere decir que un paquete enviado a una dirección Unicast es entregado solo a la interfaz identificada con dicha dirección, es equivalente a las direcciones IPv4 actuales. Los dispositivos IPv4 tienen una sola dirección, las direcciones IPv6 suelen tener dos direcciones de unidifusión:

- **Dirección de unidifusión global (GUA):** - es similar a una dirección IPv4 pública.

  Estas son direcciones enrutables de Internet globalmente exclusivas. Las GUA pueden configurarse estáticamente o asignarse dinámicamente.

- **Dirección local de enlace (LLA):** - se requiere para cada dispositivo habilitado para IPv6. Los LLA se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término "enlace" hace referencia a una subred. Las LLA se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local (Cisco, 2021).

2.7.2. Dirección Anycast

Identificador para un conjunto de interfaces, típicamente pertenecen a diferentes nodos. Un paquete enviado a una dirección anycast es entregado a dicha dirección y esté más cerca. Nos permite crear, por ejemplo ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada, si la primera cae (Montañoz, 2018, pág. 31).

2.7.3. Dirección Multicast

> Identificador para un conjunto de interfaces por lo general pertenecientes a diferentes nodos. Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (multidifusion) (Montañoz, 2018, pág. 31).

A diferencia de IPv4, IPv6 no tiene una dirección de difusión. Sin embargo, existe una dirección IPv6 de multidifusión de todos los nodos que brinda básicamente el mismo resultado.

2.8. DIFERENCIAS IPV4 E IPV6

Revisando todo lo descrito del protocolo IP en su versión 4 y versión 6 hasta este punto, la Tabla 1 refleja las principales diferencias que existe entre estos protocolos, así también las mejoras que presenta el IPv6 sobre IPv4.

Tabla 1 - Diferencias entre el protocolo IPv4 e IPv6

	IPV4	**IPV6**
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes)
IPSec	La compatibilidad es opcional.	La compatibilidad es obligatoria.
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los enrutadores controlen la QoS en el encabezado IPv6, utilizando el campo Etiqueta de flujo.

Fragmentación	La llevan a cabo los enrutadores y el host que realiza el envío.	No la llevan a cabo los enrutadores, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada.	Se utiliza el Descubrimiento de enrutadores ICMP, y es opcional.	El Descubrimiento de enrutadores ICMP queda sustituido por la Solicitud de enrutadores ICMPv6 y los mensajes de anuncio de enrutador, y es obligatorio
Configuración manual	Debe configurarse manualmente o a través de DHCP.	No requiere configuración manual o a través de DHCP.

DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Tamaño de paquete	Debe admitir un tamaño de 576 bytes (posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (sin fragmentación).

Fuente: Elaboración propia.

2.9. PROTOCOLOS DE ENRUTAMIENTO

El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento, actualmente adopta los mismos protocolos de enrutamiento que son utilizados en las redes IPv4. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos de enrutamiento más utilizados, los cuales se muestran seguidamente divididos en protocolos internos y externos (Kurose & Ross, 2017, p. 311).

2.9.1. Protocolos de enrutamiento interno

Existen dos opciones fundamentales para trabajar con el enrutamiento interno: (OSPF, IS-IS), estos usan estructuras jerárquicas, tienen en cuenta la formación de estado y envían actualizaciones de manera optimizada. (Montañez Prieto, J. P., 2014, p. 12) Otra opción es (RIP), el cual debe ser habilitado en las interfaces requeridas.

a. OSPFv3

OSPFv3 tiene la misma funcionalidad que OSPFv2, pero utiliza IPv6 como transporte de la capa de red, por lo que se comunica con pares de OSPFv3 y anuncia rutas IPv6 (Enriquez, 2014, p. 11).

- Open Shortest Path First version 3, OSPFv3. Protocolo IGP de tipo link-state.
- Utiliza el algoritmo del camino de Dijkstra más corto.
- Agrupa los routers en áreas.
- Basado en el protocolo OSPFv2.
- Protocolo específico para IPv6

b. RIPng

Está diseñado para que los routers intercambien información de rutas mediante una ruta de una red basada en IPv6. Es un protocolo de enrutamiento vector-distancia cuya finalidad es determinar mediante la métrica la ruta más óptima de forma automática y la dirección. Cada router que implementa RIPiG tiene una tabla de enrutamiento el cual posee una entrada para cada destino que se quiere alcanzar en todo el sistema de funcionamiento RIPng. (Enriquez, 2014, p. 12) Cada entrada de la tabla de enrutamiento cuenta con la siguiente información:

- El prefijo IPv6 de destino.
- Una métrica que identifica el número de saltos desde el router al destino.
- La dirección IPv6 del siguiente router y la ruta hacia el destino.
- Una bandera para guiar el cambio de ruta.
- Varios contadores asociados con la ruta. (Montañez Prieto, J. P., 2014, p. 12)

2.9.2. Protocolo de enrutamiento externo

El protocolo de enrutamiento externo, en la actualidad por defecto es Border Gateway Protocol versión - MP (BGP-MP). O Protocolo de tipo vector distancia. El protocolo BGP combina información de enrutamiento entre vecinos, con esta información diseñan un grafo de conectividad entre los sistemas autónomos (Enriquez, 2014, p. 12).

a. BGP

- Puerto TCP 179.
- Cuatro tipos de mensajes: Open, Update, Keep alive, Notification
- Dos tipos de conexión: eBGP, iBGP

2.10. TÉCNICAS DE MIGRACIÓN A IPV6

Dado que el protocolo predominante en la actualidad en Internet es IPv4, e Internet se ha convertido en algo vital, no es posible su sustitución, es decir, no es posible apagar la Red, ni siquiera por unos minutos y cambiar a IPv6 (Carofilis, 2017).

No basta con actualizar unos pocos equipos, es una operación que tendría que involucrar a cualquier organización, sea empresa, administración pública o proveedor de acceso o contenidos de una forma sincronizada, lo cual es imposible (Llanos, 2016).

Precisamente por ello, la organización encargada de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), diseñó junto con el propio IPv6, una serie de mecanismos que llamamos de transición y coexistencia que permiten la comunicación e interoperabilidad IPv4-IPv6, que son conocidos como Mecanismos de Transición, que son las tecnologías que facilitan y facilitarán la transición de Internet de su infraestructura IPv4 al sistema de direccionamiento de nueva generación IPv6, los que suelen ser clasificados en tres grupos (Llanos, 2016):

- Pila-doble/dual (Dual-Stack)
- Túneles o Tunneling
- Traducción de Encabezado

2.9.1. Pila Doble - Dual Stack

Este es el mecanismo de transición más simple y más económicos, que consiste en proveer a las terminales y los routers un soporte completo para los protocolo IPv4 e IPv6. Cada nodo es configurado con ambos protocolos como se muestra en la figura 7, por lo cual puede interactuar con nodos IPv4 usando mensajes IPv4 y con nodos IPv6 usando paquetes IPv6, sin necesidad de realizar costos procesos de encapsulación o traslación.

Para esto se deben configurar con direcciones específicas de cada protocolo, permite activar y desactivar una de las pilas, por este motivo un nodo puede tener 3 modos de funcionamiento más que un mecanismo de transición es un mecanismo de integración (Cisco, 2021).

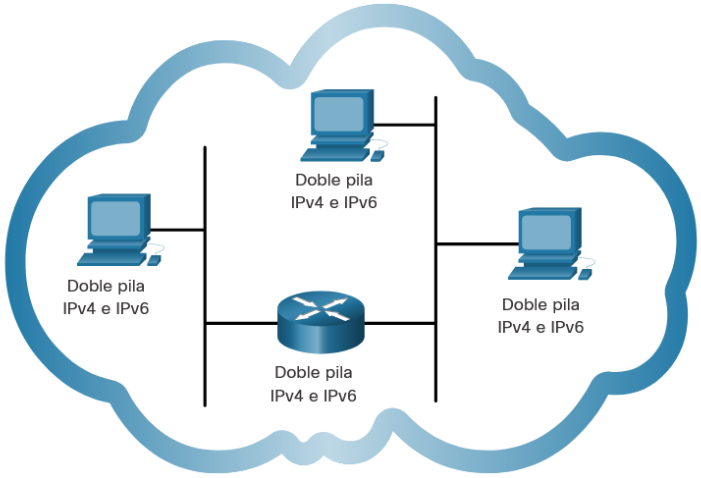


Figura 7 - Técnica de migración Dual Stack

Fuente: (Cisco, 2021).

- Es decir cuando la pila IPv4 esta activada y la pila IPv6 desactivada, se comporta como un solo nodo IPv4.
- Cuando la pila IPv6 está activa y la pila IPv4 desactivada, se comporta como un solo nodo IPv6.
- Cuando se habilitan las pilas IPv4 e IPv6, el nodo puede utilizar los dos protocolos.

Un nodo IPv4/IPv6 utiliza una dirección para cada versión de protocolo, para que haya comunicación entre dos computadoras que estén en dos diferentes segmentos de red, se utilizan mecanismos como son configuraciones estáticas que quiere decir que manualmente el administrador le agregue una dirección IP a cada terminal. También existe el DHCP que se configura las computadoras y los routers para que se asignen automáticamente direcciones IP sin necesidad de hacerlo manual, en IPv6 también se utiliza la configuración estática y automática (Carofilis, 2017, p. 45).

2.9.2 Túneles o Tunneling

Este mecanismo es un proceso en que la información de un protocolo se encapsula en un paquete de otro protocolo, lo que se conoce como encapsulación. Permite que redes IPv6 aisladas se puedan comunicar sin necesidad de actualizar la estructura de ruteo entre ellas (Cisco, 2021).

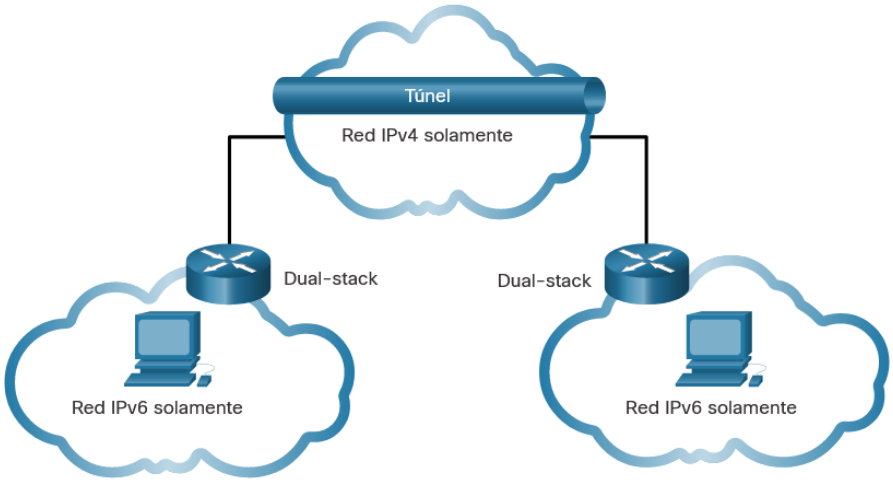


Figura 8 - Técnica de migración Túnel

Fuente: (Cisco, 2021).

La figura 8 anterior nos muestra el encapsulamiento de paquetes IPv6 en IPv4, para conectar 2 terminales IPv6 empleando la infraestructura IPv4 de Internet. Nótese que los routers que enlazan el mundo IPv4 con el mundo IPv6 tienen que ser Dual Stack. Es decir muestra cómo se componen los paquetes IPv6 encapsulados

por un router Dual Stack, para enviarlos por una red IPv4. El Router de origen del túnel le agrega una cabecera IPv4, en la cual las direcciones de origen y destino son las correspondientes a las de inicio y fin del túnel (Carofilis, 2017, p. 46).

El Router donde finaliza el túnel es el encargado de desencapsular el paquete IPv6 (eliminando la cabecera IPv4) y retransmitirlo hacia el destino final.

En el nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, y lo pone 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 el primer nodo IPv4 que conforma el túnel. Los nodos IPv4 del Túnel encaminan el paquete, sin tener constancia de que el paquete IPv4 que están manejando contiene un paquete IPv6, finalmente cuando el paquete llega al extremo receptor IPv6 del túnel, este determina que el paquete IPv4 contiene un paquete IPv6 que debe ser extraído (Cisco, 2021).

a. Túneles manuales

Un paquete IPv6 encapsulado en un paquete IPv4 para ser encaminado sobre una infraestructura de enrutamiento IPv4, estos son los túneles punto a punto que necesitan ser configurados manualmente.

b. Túneles Automáticos

Los nodos IPv6 pueden utilizar diferentes tipos de direcciones compatibles con IPv4, IPv6, el túnel automático es un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4. La configuración de los túneles entre routers y host se pueden realizar de diferentes formas:

- **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.
- **Host a Router**: utiliza también utiliza un túnel automático en donde un host IPv6/IPv4 puede encapsular paquetes IPv6 a un router intermedio IPv6/IPv4 que es accesible mediante una infraestructura de ruteo IPv4.

- **Host a Host:** utiliza un túnel manual en donde los host IPv6/IPv4 que están interconectados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.
- **Router a Host:** utiliza un túnel manual en donde los routers IPv6/IPv4 pueden encapsular paquetes IPv6 a su destino final.

2.8.3 Traducción de encabezados

Este método permite un enrutamiento transparente de la comunicación entre nodos que solo poseen soporte a una versión del protocolo IP, o que utilizan doble pila. Pueden operar de diversas formas o en capas distintas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa como se muestra en la figura 9, realizando conversiones de direcciones, o actuando en el intercambio del tráfico TCP a UDP (Carofilis, 2017, p. 47).

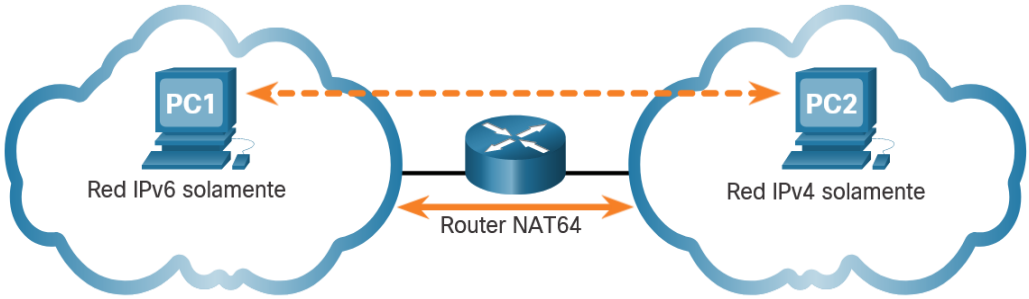


Figura 9 - Técnica de migración Túnel

Fuente: (Cisco, 2021).

Para que un nodo en una red IPv6 se puede comunicar con un nodo remoto en una red IPv4 debe usar los mecanismos de translación. Dentro de estos se encuentra NAT-PT, network Address Translation – Port Translation, que realiza un mapeo dirección IPv6 en direcciones IPv4 modificando la cabecera de los paquetes (Cisco, 2021).

a. Traducción de IPV4 a IPV6

Cuando el traductor recibe un datagrama IPv4 que contiene una dirección destino que está fuera de la red IPv4, entonces traduce el encabezado de ese datagrama por uno IPv6 y lo reenvía basándose en la dirección IPv6 destino. Una descripción básica y rápida de esta traducción consiste en que el encabezado IPv4 del paquete es removido y reemplazado por uno, como se muestra en la figura 10 (Enriquez, 2014, p. 40).

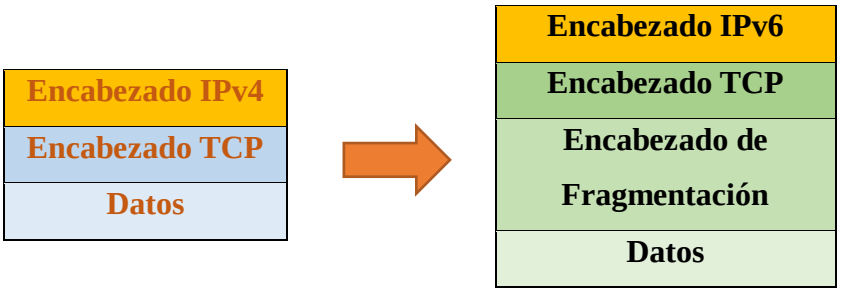


Figura 10 - Proceso de traducción de IPV4 a IPV6

Fuente: Elaboración propia.

b. Traducción de IPV6 a IPV4

Por el contrario de la traducción IPv4 a IPv6, cuando el traductor recibe un datagrama IPv6 destinado a una dirección IPv4-mapeada, éste traduce el encabezado IPv6 a un encabezado IPv4. Nuevamente, el encabezado original es removido y sustituido, en este caso, por un encabezado IPv4, como se muestra en la figura 11 (Enriquez, 2014, p. 41).

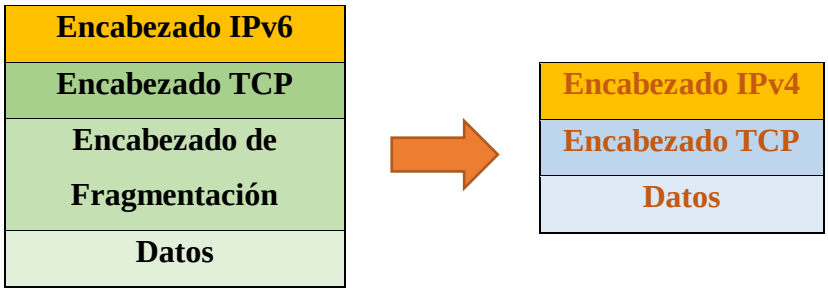


Figura 11 - Proceso de traducción de IPV6 a IPV4

Fuente: Elaboración propia.

CAPÍTULO III MARCO METODOLÓGICO

3.1. Enfoque de investigación

El presente trabajo se desarrolla siguiendo un enfoque Cuantitativo, ya que se basa en la recolección de datos para probar hipótesis, con base en la medición numérica en el análisis estadístico para medir patrones de comportamiento del modelo.

3.2. Tipo de Investigación

El tipo de investigación es Proyectiva, ya que consiste en la elaboración o diseño de un modelo de simulación, como solución a un problema o necesidad de tipo práctico, ya sea de un área particular o una institución. Toda investigación proyectiva, requiere de un marco teórico (Hurtado, 2008).

3.3. Instrumentos y Técnicas

En la presente investigación se utilizan las siguientes técnicas y métodos que permitan probar los objetivos planteados:

3.3.1. Métodos de Análisis de Datos

Para analizar los datos usaremos:

- Análisis Documental: El planteamiento del diseño lógico vendrá del análisis documental sobre libros, páginas web oficiales, etc. referente al tema. Luego recolectamos datos necesarios, para realizar una lectura comprensiva y resumen de los datos que son de nuestro interés. Todo esto servirá para definir la técnica de migración a seguir.

3.3.2. Herramientas

La herramienta principal para desarrollar el modelo de migración es el programa Packet Tracert, software diseñado, desarrollado y aprovisionado por la empresa Cisco. Este simulador es uno de los más completos puesto que cuenta con equipos de red, computadores, servidores entre otros;

configuraciones de equipos, procesos de seguridad y pruebas en tiempo real.

Esta herramienta se destaca por la simplicidad, por disponer de interfaz bastante robusta y por ser una solución lista para funcionar, o sea, ya trae el IOS disponible para los diversos equipos de red. También se puede hacer simulaciones de conectividad (pings, traceroutes) todo ello desde las mismas consolas incluidas. Una de las grandes ventajas de utilizar este programa es que permite ver cómo deambulan los paquetes por los diferentes equipos (switchs, routers, PCs) con la opción Simulación, además de poder analizar de forma rápida el contenido de cada uno de ellos en las diferentes capas y datos.

3.4. Etapas de la Investigación

Para el desarrollo apropiado de la investigación se propone llevar a cabo las siguientes fases las cuales se fundamentan en el criterio metodológico de la investigación proyectiva (Hurtado, 2008):

Fase exploratoria.- En esta primera fase se exploran estudios anteriores al tema o contexto a desarrollar, con la idea de observar la metodología aplicada, los aportes y los alcances, así como las teorías y conceptos relacionados.

Fase descriptiva.- En este apartado se describen las situaciones y las necesidades del modelo de migración y los componentes que conforman el mismo, con el objetivo de entender el proceso causal propuesto como solución a la problemática.

Fase proyectiva.- Se centra en el diseño del modelo. Analiza y concluye con un diseño, propuesta o plan de acción que debe estar basado en el proceso causal en cadena. Los elementos que se consideran dentro de este diseño son los siguientes:

– La identificación de destinatarios y responsables, a través de la que se describe el perfil de cada red que puede estar involucrada en la propuesta.

– La finalidad de la propuesta, que tiene que ver con los objetivos específicos o logros que se pretenden alcanzar con el modelo.

– La temática y contenido, que se refiere a las áreas de conocimiento relacionadas con las acciones a ejecutar dentro del plan.

– El desarrollo de actividades, en donde se describen las acciones que se van a ejecutar por áreas o eventos del plan.

Fase evaluativa.- Aplica los instrumentos y recoge datos de estudio para obtener los resultados de la implementación del modelo propuesto en prototipo. Así mismo, recomienda distintas acciones para la fase ejecutora o interactiva puedan mejorar o cambiar.

Fase ejecutora.- En esta fase se realizan las implementaciones físicas del modelo, pero no realizaremos esta fase, ya que el proceso de la tesis se centra en el desarrollo del Modelo de Migración de IPV4 a IPV6 de la Red de datos Empresarial

CAPÍTULO IV DESARROLLO

4.1. Fase Exploratoria

En esta fase se estudian todos los conceptos relacionados al tema. Y se lleva a cabo la siguiente actividad:

4.1.1. Recolección de Información

Inicialmente se efectuó la recopilación de información propuesta sobre el protocolo IPv6. De igual manera es de importancia tener conocimiento sobre el direccionamiento en IPv6, sus reglas y su estructura. Los protocolos de enrutamiento, cómo se configuran y de qué manera se utilizan, allí se puede encontrar: EIGRP, OSPF, BGP; los métodos de transición en donde se pueden apreciar varios de estos como: Dual stack, tunelización, traducción NAT64, los cuales son los más conocidos y más usados, fueron enfatizados en el capítulo 2. Por lo anterior, también se debe tener en cuenta los equipos que permiten hacer uso del protocolo IPv6, aunque durante la implementación se hace referencia a equipos Cisco, también se nombrarán otros dispositivos que permiten IPv6.

4.2. Fase Descriptiva

En esta fase se muestra la representación del modelo. Y se llevan a cabo las siguientes actividades:

4.2.1. Descripción del modelo

La representación del modelo, se presenta con el desarrollo de un diseño general del modelo de migración a IPv6 para redes empresariales, con características esenciales relacionadas al modelo para así poder encontrar solución al problema planteado en el presente trabajo de tesis, este se compone por tres elementos como se ve en la figura 12 los cuales forman el núcleo central del mismo.

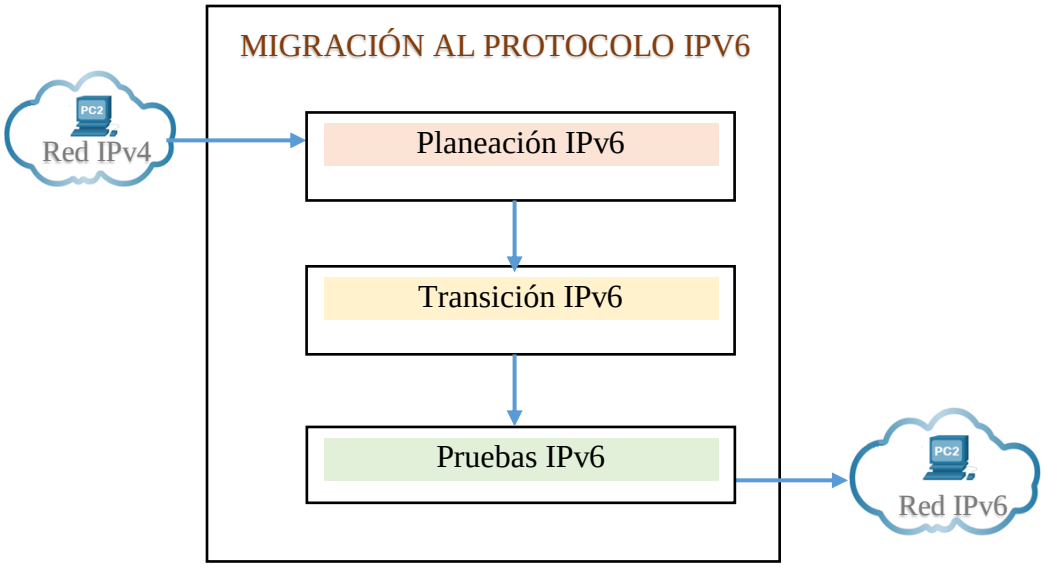


Figura 12 - Descripción general del modelo de migración IPV4 a IPV6 para redes empresariales

Fuente: Elaboración propia.

4.2.2. Componentes del modelo

Los componentes del modelo son los siguientes: 1) Planeación IPv6, 2) Transición IPv6, 3) Pruebas IPv6.

4.2.2.1. Planeación IPv6

Dentro del proceso de la migración de protocolo de una red de datos dentro de una empresa o entidad, se deben tener en cuenta una serie de actividades a seguir las cuales garantizaran un correcto análisis de la red y sus dispositivos para preparar el camino hacia la migración de protocolo de direccionamiento IPv6, dentro de esas actividades están las siguientes: Hacer el respectivo diagnostico a los equipos de la red en la cual se pretende hacer el proceso para la migración del protocolo de direccionamiento, esto permitirá conocer si la red soporta el protocolo IPv6 para su migración. Una vez hecha esta actividad, se comienza a trabajar con el plan para la migración hacia el protocolo de direccionamiento IPv6, haciendo las recomendaciones necesarias si en alguno de los casos uno de los dispositivos o

servicios con los que cuenta la entidad o empresa no soporta IPv6, es entonces donde se comienza a identificar un nuevo dispositivo que, si soporte el protocolo de IPv6, y así garantizar que el protocolo IPv6 sea completamente implementado.

Luego de hacer el respectivo diagnóstico se busca por medio del análisis previo de la red como se encuentra conectada toda la red de datos dentro de la empresa en la cual se busca hacer la migración al protocolo IPv6, identificando cual es el proveedor de internet o si tiene varios proveedores de internet en caso de que falle uno de ellos tener el otro disponibles, a esto se le llama redundancia, también, se identifica la topología, si la empresa o entidad cuenta con un canal dedicado de internet y cuáles la velocidad del servicio de ISP.

4.2.2.2. Transición IPv6

a. Elección de técnica de Migración

- **Análisis de los diferentes mecanismos de migración a IPv6**

  Posteriormente, se realiza el primer y segundo objetivo específico, el cual tiene como fin investigar y definir las diferentes técnicas de migración a IPv6 con el propósito de seleccionar la que se usará en esta investigación. Se consideran los siguientes mecanismos: Pila-doble/dual, Túneles y Traducción de Encabezado

  El uso de la Pila Dual limita el aprovechamiento de todo el campo de direccionamiento que ofrece IPv6, y no disminuye el uso de direcciones IPv4. El mecanismo de traducción descrito anteriormente en el capítulo 2, suena a una solución atractiva, ya que no presenta un límite en cuanto a direcciones se refiere. A decir verdad, es quizás este mecanismo uno de los más agresivos utilizados durante la migración. Con agresivo nos referimos a que, si se observa bien el proceso y se analizan los encabezados generados y los eliminados, podemos ver como al realizar la traducción, ciertos campos son perdidos totalmente en este proceso. Ahora bien, no es sólo el direccionamiento lo que en realidad califica a los métodos anteriores como inefectivos. El tipo de conectividad (el soporte que brinda) es lo que interesa.

La pila dual solo se realiza para ambientes compatibles: IPv4 a IPv4 sobre un ambiente versión 4 o IPv6 a IPv6 sobre un ambiente IPv6, pero nunca para un ambiente mixto como IPv4 a IPv4 sobre IPv6. Con respecto a la traducción, se puede decir que trabaja de manera similar a lo que es la pila dual; ya que el traductor acepta paquetes de cualquiera de los protocolos (como si fuera un nodo IPv4/IPv6) permitiendo que la comunicación sea como la de la pila dual IPv4-a-IPv4 o IPv6-a-IPv6 y los traduce según las necesidades de envío. Mientras Tunneling es un mecanismo que más se adecua a nuestro escenario para llevar a cabo la migración. Se encuentra entre las técnicas más usadas para realizar las migraciones, fue diseñado para permitir conectividad IPv6 aún sin la cooperación (soporte) de los proveedores de servicios de Internet, pudiendo conectar redes IPv4 mediante paquetes IPv6 y viceversa. A continuación mostraremos la comparación de las Técnicas de Migración a IPv6 en la Tabla 2.

Tabla 2 - Comparación de las tecnicas de migración

Tipo de Mecanismo	Conectividad	Descripción	Ventajas	Desventajas
Pila Doble – Dual Stack	Solo entre sistemas del mismo tipo (IPv4 –Ipv4, IPv6 –Ipv6)	• Trabaja con ambos protocolos (IPv4 e IPv6). • Procesa solo los encabezados IP. • Uno de los más populares dentro de su tipo.	• Fácil de implementar. • Una solución inmediata y accesible. • Los nuevos dispositivos IPv6 relacionarse rápidamente con el resto de los dispositivos.	• No trabaja en ambientes mixtos (IPv4 sobre IPv6 y viceversa). • Si la red no es IPv6, no se ve beneficiada de las características de esta versión
Mecanismos de Traducción	De IPv6 a IPv4 y de IPV4 a IPv6.	• Para hacer dos protocolos “compatibles” realiza la traducción de encabezados. • Se necesita de un traductor que lleve a cabo la traducción.	• Permite a nodos IPv4 comunicarse con nodos IPv6. • Fácil de soportar por un dispositivo. • Puede manejar paquetes encriptados, ya que no modifica capas superiores.	• Al realizar la traducción IPv6 a IPv4 se pierden muchos campos, y con estos beneficios de IPv6. • Se ignoran la mayoría de los encabezados de extensión.
Tunneling	IPv6 a IPv6 sobre IPv4 e IPv4 a IPv4 sobre IPv6.	• Crea túneles automáticamente • Algoritmo más popular dentro de su clase.	Ayuda a conectar redes IPv6 aisladas entre si	No cuenta con encriptación sin embargo es algo que puede ser subsanado

Fuente: Elaboración propia

Como se detalla en la tabla 2, los 3 mecanismos de transición tienen ventajas y desventajas al momento de ser implementados, sin embargo el mecanismo que más se ajusta a las necesidades del modelo de migración es la Tunelización el cual permite la comunicación de redes IPv6 sobre una IPv4 así podrán configurarse las LAN solo con IPv6, a diferencia de la Pila Dual o Traducción que mantiene el direccionamiento IPv4 intacto limitando así el ahorro de las mismas.

Para seleccionar la técnica de migración también se debe considerar otros parámetros por eso se hace una revisión bibliográfica de artículos científicos para obtener los resultados que tuvieron esos investigadores y tomarlos como base para el criterio de selección, con las siguientes métricas se evaluaron a las técnicas de migración:

- Latencia: Se refiere a la cantidad de tiempo incluida las demoras que les toma a los datos transferirse desde un host hasta otro.
- Rendimiento: Es la cantidad de bits transferidos a través de los medios durante un periodo de tiempo.
- Uso del CPU: Es el nivel de uso en porcentaje del consumo del CPU en la ejecución de un proceso.

Tabla 3 - Resultados de los artículos científicos sobre la métrica latencia

LATENCIA		
ARTÍCULO CIENTÍFICO / **TÉCNICA**	**(Sookun & Basso, 2016)**	**(Altangerel, Tsogbaatar, & Yamkhin, 2016)**
Dual Stack	82.2 [ms]	84.5 [ms]
6RD	196.8 [ms]	X
6to4	230.9 [ms]	70.5 [ms]
ISATAP	221.95 [ms]	70.3 [ms]
IPv6IP	X	74.6 [ms]
TUNEL GRE	X	**65.3 [ms]**
NAT64	210.5 [ms]	X

Fuente: Elaboración propia

Este indicador es importante debido a que es un factor que influye mucho en las conexiones a internet. Para seleccionar una técnica de transición óptima debe tener la latencia más baja. Como resultado en la Tabla 3 se obtuvo que la técnica Túnel GRE tiene menor Latencia con 65.3[ms], y por el contrario la técnica 6to4 es la que mayor latencia presenta con 230.9 [ms] por lo cual se considera que no es optima para el modelo.

Tabla 4 - Resultados de los artículos científicos sobre la métrica rendimiento

RENDIMIENTO		
ARTÍCULO CIENTIFICO / **TÉCNICA**	**(Sookun & Basso, 2016)**	**(Altangerel, Tsogbaatar, & Yamkhin, 2016)**
Dual Stack	82.2	84.5
6RD	84.4	X
6to4	70.1	65.1
ISATAP	71.96	43.8
IPv6IP	X	79.1
TUNEL GRE	X	75.8
NAT64	X	X

Fuente: Elaboración propia

Un rendimiento más alto significa un mejor rendimiento de red. Por lo tanto, esta métrica es de vital importancia en esta investigación. Según la Tabla 4 el mecanismo más optimo es 6RD. Pero este mecanismo no se puede implementar ya que se tendría que obtener el prefijo que LACNIC asigna al ISP, la segunda opción es Dual Stack, este mecanismo es descartado debido a que consume mucho recurso por el trabajo simultáneo de los protocolos. Por lo tanto, la técnica con mayor rendimiento es el IPv6IP seguida del Tunel GRE.

Tabla 5 - Resultados de los artículos científicos sobre la métrica Uso de CPU

USO DE CPU		
ARTÍCULO CIENTÍFICO / **TÉCNICA**	**(Sookun & Basso, 2016)**	**(Altangerel, Tsogbaatar, & Yamkhin, 2016)**
Dual Stack	17 - 19%	X
6RD	10 - 12%	12 - 13%
6to4	11 - 13%	X
ISATAP	11 - 12%	X
IPv6IP	X	X
TUNEL GRE	11 - 12%	10 - 11%
NAT64	X	X

Fuente: Elaboración propia

Si el Uso del CPU es muy elevado necesitará mayores recursos informáticos, por lo tanto, se debería evaluar si los equipos informáticos soportarían este mecanismo, en conclusión, este indicador es de mucha importancia. En este indicador se seleccionó la técnica de Tunel GRE debido a que tiene un promedio de uso de CPU del 10 – 11% siendo este el mas bajo a comparación de las demas técnicas.

Después de haber obtenido los resultados de cada mecanismo de transición bajo las metricas de evaluación, la técnica que mejores resultados muestra es el Tunel GRE por lo tanto es la técnica mas indicada para implementarse en el modelo de migración.

4.2.2.3. Pruebas IPv6

Dentro del proceso de la transición de la red empresarial IPv4 a IPv6, se debe hacer una simulación de la red, para probar la funcionalidad de la nueva red de datos con el modelo de migración a IPv6 implementado, esta simulación se

implementa en el software de simulación Cisco Packet Tracer, con las configuraciones tal cual como se implementaría en una red física.

4.3. Fase Proyectiva

4.3.1. Construcción del modelo de migración de red IPv4 al protocolo IPv6

El desarrollo del modelo se realiza con la construcción e implementación del mecanismo de transición a IPv6 Túnel GRE, propuesto en la sección 4.3.1 de este trabajo de tesis.

El modelo consta de seis elementos fundamentales:

A. **Implementación de la red IPv4 en el simulador:** Actualmente el activo más valioso para una empresa es la información, por lo cual no se puede correr el riesgo de perder la misma, y mucho menos dejar a los usuarios sin conexión. El simulador nos permite comprobar el funcionamiento de una red y los cambios que se producen en la misma, sin tener que modificar la red real, siendo muy útil para implementar la migración a IPv6 y ver cómo afectarían en el comportamiento y rendimiento de la red.

B. **Diagnóstico de los equipos de la red:** El diagnóstico, es un pilar fundamental del modelo, se requiere la realización de la validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6 en las Empresas; dentro de dicha validación, es necesario revisar la compatibilidad del protocolo IPv6 con los equipos de la red identificando claramente cuáles elementos (equipos y software) soportan IPv6, cuales requieren actualizarse y/o no soportan el nuevo protocolo, de tal manera que la información recogida, sea insumo para el inicio de la siguiente actividad.

C. **Adquisición de segmento IPv6 y diseño del plan de direccionamiento IPv6:** La adquisición de un segmento IPv6 se debe acordar con un ISP (Proveedor de Servicios de Internet), por ejemplo la empresa COMTECO con sede en

Cochabamba-Bolivia es reconocido por LACNIC como uno de los mayores promotores de IPv6 en América Latina y efectúa el aprovisionamiento de la misma (LACNIC, 2021).

La elaboración del plan de direccionamiento en IPv6 tiene como base la topología de la red de la empresa. Se habilita el plan de direccionamiento IPv6 definido para cada uno de los componentes de hardware y software de acuerdo con el diagnóstico previo a los equipos; respetando el funcionamiento de la red bajo las políticas de enrutamiento y las políticas de seguridad que se tenía con IPv4, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado.

D. **Transición de los protocolos y servicios a IPv6:** Se deben configurar aquellos protocolos implementados en la red en su versión 6 tales como los protocolos de enrutamiento y la configuración de las direcciones IPv6 en las interfaces de los equipos. Para la transición de los servicios (DHCP, DNS, CORREO, etc.) se realiza la configuración de la dirección IPv6 de forma estática o dinámica según los requerimientos de la red.

E. **Configuración de la técnica de migración: Túnel GRE:** Con los protocolos y servicios migrados a IPv6 lo que resta es poder comunicarlas mediante la configuración del Túnel GRE para lograr una comunicación de IPv6 a IPv6 sobre IPv4, lo que permite la coexistencia de ambos protocolos en la red.

F. **Pruebas de funcionamiento de la red con protocolo IPv6 sobre el simulador:** La migración a IPv6 no debe afectar en el funcionamiento de la red es por eso que se debe probar que la comunicación entre usuarios se lleva a cabo con completa normalidad, esto es posible de verificar mediante la ejecución del comando Ping entre distintos equipos y destinos.

La interacción de los elementos es primordial para el desempeño de la solución propuesta. El prototipo del modelo de migración a IPv6 esta implementado en Packet Tracert una herramienta de simulación de Redes

4.3.1.1. Arquitectura del modelo

La construcción del modelo se presenta a continuación en un gráfico tomando los puntos mencionados anteriormente.

La Figura 13 muestra el funcionamiento del modelo propuesto en este trabajo de tesis, basado en un proceso causal en cadena.

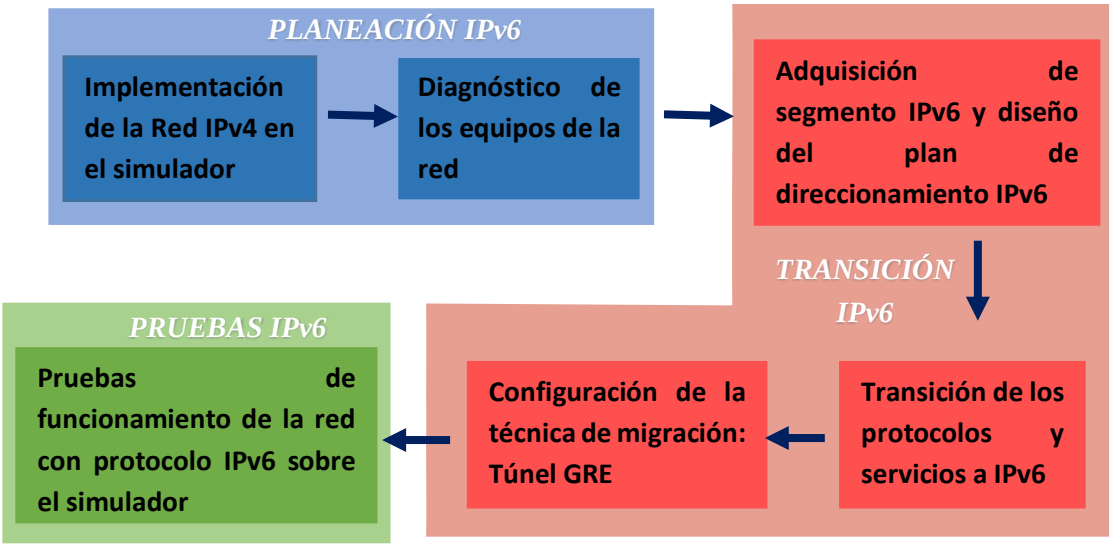


Figura 13 - Modelo de migración de red IPv4 al protocolo IPv6 para redes empresariales

Fuente: Elaboración Propia

4.3.2. Implementación del prototipo

4.3.2.1. Implementación de la Red IPv4 en el simulador

Como caso de estudio tenemos, una red típica de una pequeña empresa de nuestro medio, cuenta actualmente con los siguientes equipos: 3 Routers Cisco 2911 Series, 7 Switchs Cisco Catalyst 2960 Series, 3 Laptops, 12 Computadoras de escritorio y 4 servidores. Estos equipos se encuentran detallados en la Tabla 3. Actualmente las direcciones IPv4 se están agotando y a futuro solo se trabajará con direcciones IPv6.

Por tal motivo si la red desea seguir comunicándose sin tener ningún tipo de problema cuando se trabaje con IPv6 debería emplear una transición para que ambas redes puedan comunicarse mediante una red IPV4.

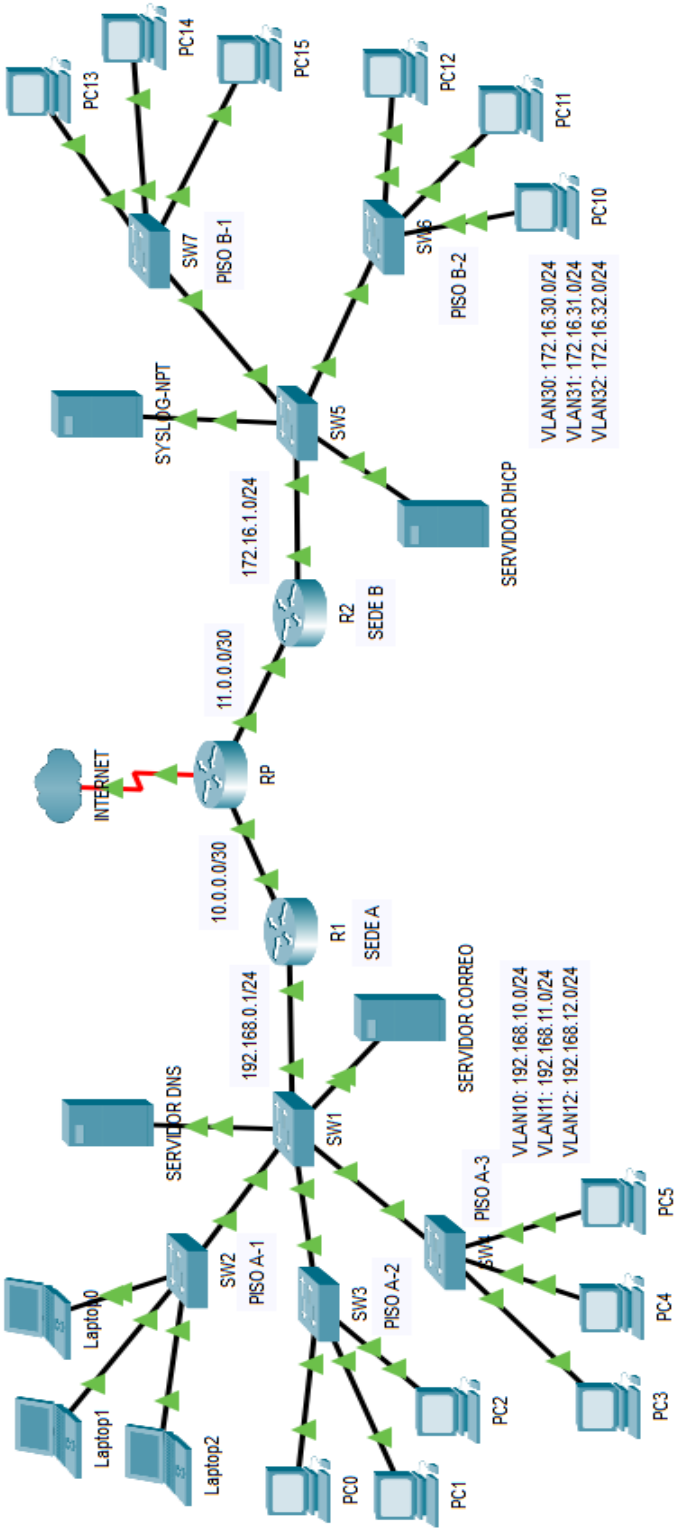


Figura 14 - Topologia de Red empresarial IPv4 implementada en el simulador

Fuente: Elaboración Propia

4.3.2.2. Diagnóstico de los equipos de la Red

Antes de considerar la migración a IPv6 debemos conocer el estado de los equipos de la red, para determinar si estos son capaces de soportar el protocolo en su versión 6, a continuación la Tabla 6 describe las características de los equipos de comunicación, la Tabla 7 describe las características de los servidores y la Tabla 8 describe las características de los equipos de cómputo.

Tabla 6 - Descripción de las caracteristicas de los equipos de comunicación de la red IPv4

Cantidad	Equipo	Hostname	Características
3	Router	RP R1 R2	**Marca:** Cisco **Modelo:** 2901 Series **Puertos Gigabit Ethernet:**2 **Soporte IPv6:** Si
7	Switch	SW1 SW2 SW3 SW4 SW5 SW6 SW7	**Marca:** Cisco **Modelo:** Catalyst 2960 **Puertos Ethernet:**24 puertos 10/100 **Soporte IPv6:** Si

Fuente: Elaboración Propia

Tabla 7 - Descripción de las caracteristicas de los servidores la red IPv4

Cantidad	Equipo	Hostname	Características
4	Servidores	SERVIDOR CORREO SERVIDOR DNS SERVIDOR DHCP SYSLOG-NPT	**Tipo de Servidor:** Aplicación **Sistema Operativo:** Windows **Soporte IPv6:** Si

Fuente: Elaboración Propia

Tabla 8 - Descripción de las caracteristicas de los equipos de computo de la red IPv4

Cantidad	Equipo	Hostname	Características
3	Laptop	• Laptop1 • Laptop2 • Laptop3	**Procesador:** Intel Core i5 **Memoria Ram:**4 GB **Sistema Operativo:** Windows 10 **Soporte IPv6:** Si
12	Computadoras de escritorio	• PC0 • PC1 • PC2 • PC3 • PC4 • PC5 • PC10 • PC11 • PC12 • PC13 • PC14 • PC15	**Procesador:** Intel Core i5 **Memoria Ram:**4 GB **Sistema Operativo:** Windows 10 **Soporte IPv6:** Si

Fuente: Elaboración Propia

4.3.2.3. Adquisición de segmento IPv6 y Diseño del plan de direccionamiento IPv6

Inicialmente se debe solicitar el segmento en IPV6 con su proveedor de servicios de internet para que, al momento de generar el diseño y simulaciones, sea lo más real posible. Sin embargo con propósitos demostrativos se utilizara el segmento de red IPv6 2001:DB8:CAFE:A::/64. El plan de direccionamiento IPv6 es diseñado acorde a las necesidades de la red, también se mantiene las VLAN's y puertos asignados con el direccionamiento IPv4, para evitar que la migración sea agresiva y demande mayor tiempo su implementación.

Tabla 9 - Plan de direccionamiento IPv6 de los equipos de comunicación

Dispositivo	Interfaz	Dirección IPv6	Dirección Link-Local
R1	G0/1	2001:DB8:CAFE:A::1/64	FE80::2
	G0/1.10	2800:10:12:A::1/64	FE80::2
	G0/1.11	2800:10:12:B::1/64	FE80::2
	G0/1.12	2800:10:12:C::1/64	FE80::2
R2	G0/1	2001:DB8:CAFE:B::1	FE80::3
	G0/1.30	2800:10:12:D::1/64	FE80::3
	G0/1.31	2800:10:12:F::1/64	FE80::3
	G0/1.32	2800:10:12:G::1/64	FE80::3

Fuente: Elaboración Propia

Las interfaces destinadas a las Vlans según el plan de direccionamiento IPv6 se especifican en la Tabla 9, incluyendo las direcciones de enlace local.

Tabla 10 - Plan de direccionamiento IPv6 de los equipos de cómputo

Dispositivo	VLAN	Dirección IPv6	Default Gateway	Dirección Link-Local
Laptop0	10	2800:10:12:A::2/64	2800:10:12:A::1/64	FE80::2
PC0	10	2800:10:12:A::3/64	2800:10:12:A::1/64	FE80::2
PC3	10	2800:10:12:A::4/64	2800:10:12:A::1/64	FE80::2
Laptop1	11	2800:10:12:B::2/64	2800:10:12:B::1/64	FE80::2
PC1	11	2800:10:12:B::3/64	2800:10:12:B::1/64	FE80::2
PC4	11	2800:10:12:B::4/64	2800:10:12:B::1/64	FE80::2
Laptop2	12	2800:10:12:C::2/64	2800:10:12:C::1/64	FE80::2
PC2	12	2800:10:12:C::3/64	2800:10:12:C::1/64	FE80::2
PC5	12	2800:10:12:C::4/64	2800:10:12:C::1/64	FE80::2
PC12	30	2800:10:12:D::4/64	2800:10:12:D::1/64	FE80::3
PC13	30	2800:10:12:D::3/64	2800:10:12:D::1/64	FE80::3
PC11	31	2800:10:12:E::4/64	2800:10:12:E::1/64	FE80::3
PC14	31	2800:10:12:E::3/64	2800:10:12:E::1/64	FE80::3
PC10	32	2800:10:12:F::4/64	2800:10:12:F::1/64	FE80::3
PC15	32	2800:10:12:F::3/64	2800:10:12:F::1/64	FE80::3

Fuente: Elaboración Propia

El plan de direccionamiento IPv6 de los equipos de cómputo vease Tabla 11, esta ordenado según el ID de las Vlans para tener un mejor control y evitar confusiones en su implementación.

Tabla 11 - Plan de direccionamiento IPv6 de los servidores

Dispositivo	**Dirección IPv6**	**Dirección Link-Local**	**Puerta de enlace predeterminada**
Servidor Correo	2001:DB8:CAFE:A::2/64	FE80::2	2001:DB8:CAFE:A::1
Servidor DNS	2001:DB8:CAFE:A::3/64	FE80::2	2001:DB8:CAFE:A::1
SYSLOG-NPT	2001:DB8:CAFE:B::2/64	FE80::3	2001:DB8:CAFE:B::1
Servidor DHCP	2001:DB8:CAFE:B::3/64	FE80::3	2001:DB8:CAFE:B::1

Fuente: Elaboración Propia

Los servidores y los equipos de cómputo cuentan con una dirección denominada puerta de enlace predeterminada (Default-Gateway) como se especifica en la Tabla 10 y 11, estas direcciones pertenecen al nodo que dirige el tráfico de datos para el enlace con otras redes.

Para implementar este plan de direccionamiento IPv6 se debe configurar las direcciones en todos los dispositivos de la topologia de red implementada en el simulador Cisco Packet Tracer, comenzando por el enrutador **R1**, seguido del enrutador **R2** como se ve en la Figura 15 y Figura 16 respectivamente.

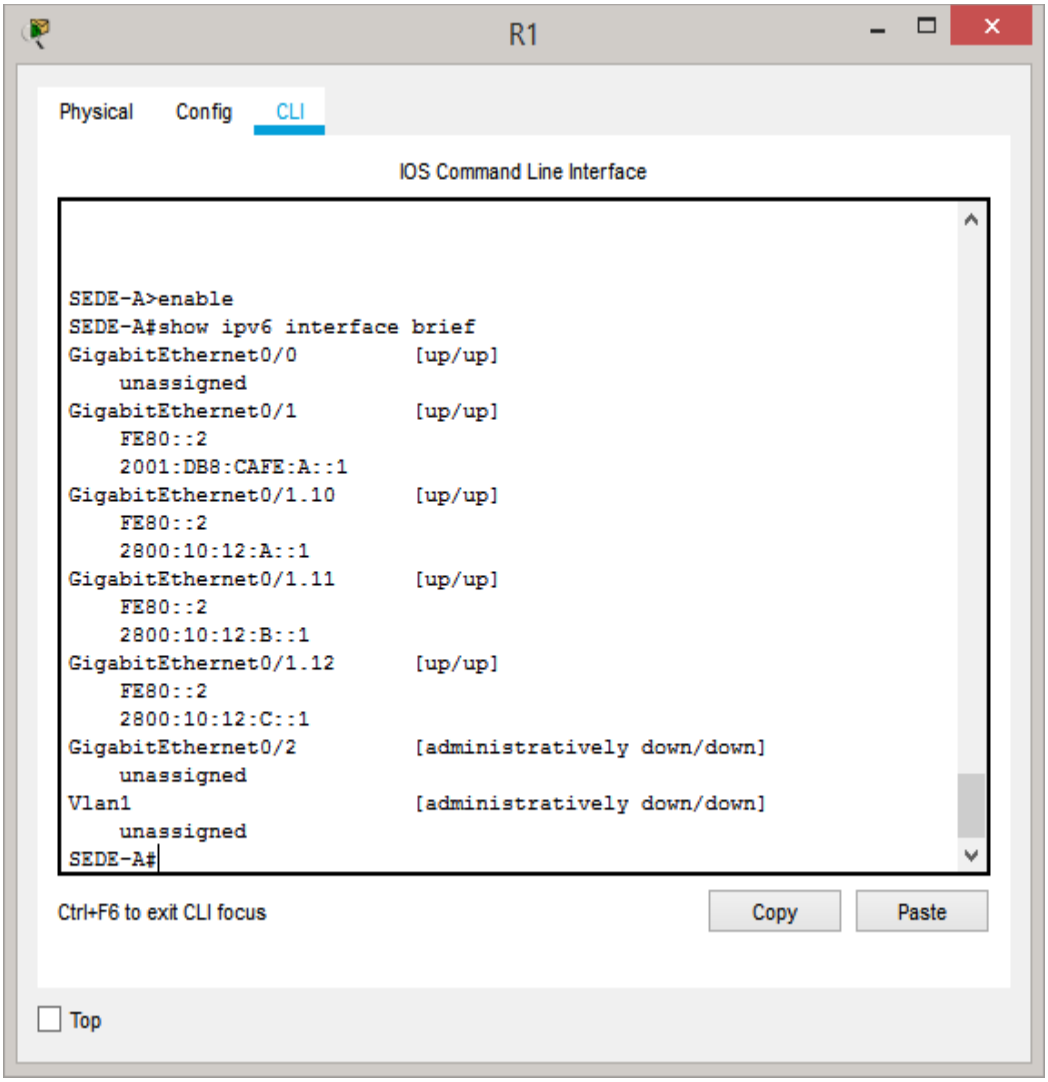


Figura 15 - Asignación de direcciones IPv6 en las interfaces de R1

Fuente: Elaboración Propia

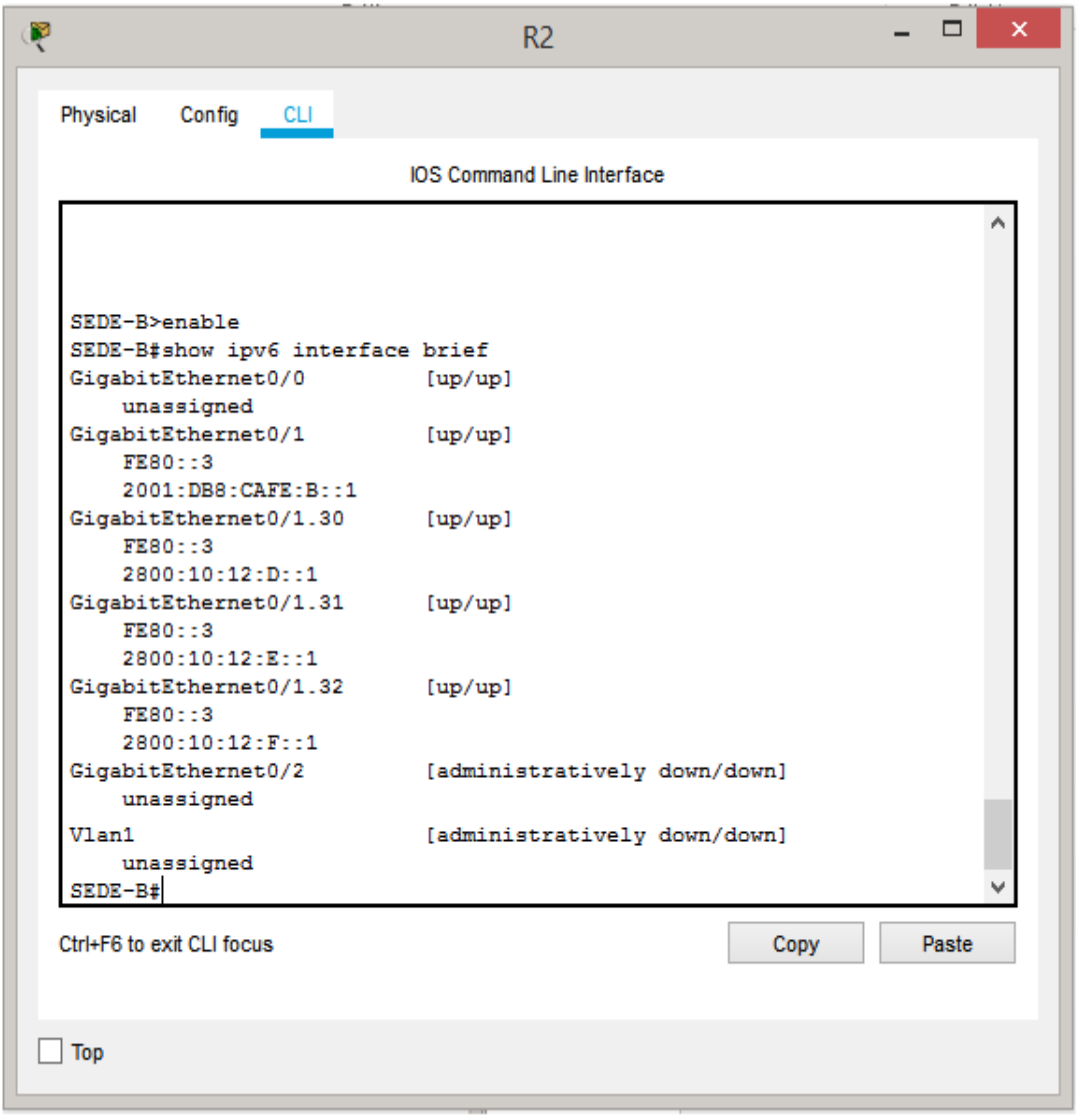


Figura 16 - Asignación de direcciones IPv6 en las interfaces de R2

Fuente: Elaboración Propia

4.3.2.4. Transición de los protocolos y servicios a IPv6

En primera instancia se hará la transición del protocolo de enrutamiento, el cual es de OSPF V2 para IPv4 a OSPF V3 para IPv6, se debe habilitar el protocolo de enrutamiento en los routers que tienen direccionamiento IPv6 utilizando el comando en modo configuración **ipv6 router ospf 1** permitiendo esto el ingreso a la estructura del protocolo OSPF, donde se dispone a establecer los siguientes

parámetros, interfaces pasivas las cuales el router no enviará la tabla de enrutamiento ya que por estas se propaga la red LAN evitando saturación o procesamiento elevado del router, el parámetro más importante es el **router-ID** el cual es el identificador para cada router, se debe contar con un identificador distinto. Para tener en cuenta, se tiene que saber que la activación del protocolo y su respectiva área se ejecuta dentro de cada una de las interfaces, el ID de R1 es **1.1.1.1** y el resto de las configuraciones se observa en la Figura 17.

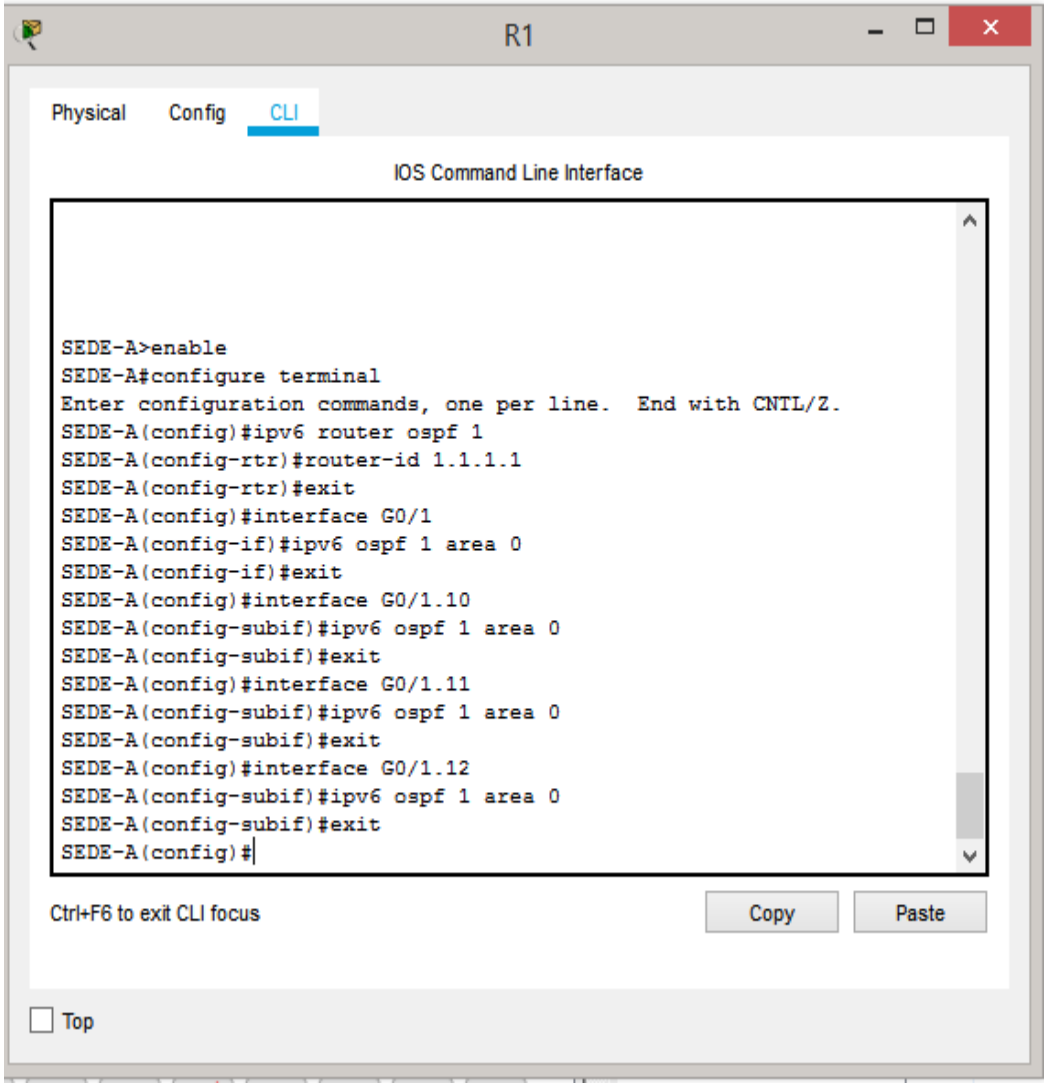


Figura 17 - Configuración del protocolo OSPFv3 en R1

Fuente: Elaboración Propia

El ID de R2 es **2.2.2.2** y las configuraciones para la transición del protocolo OSPF se observa en la Figura 18.

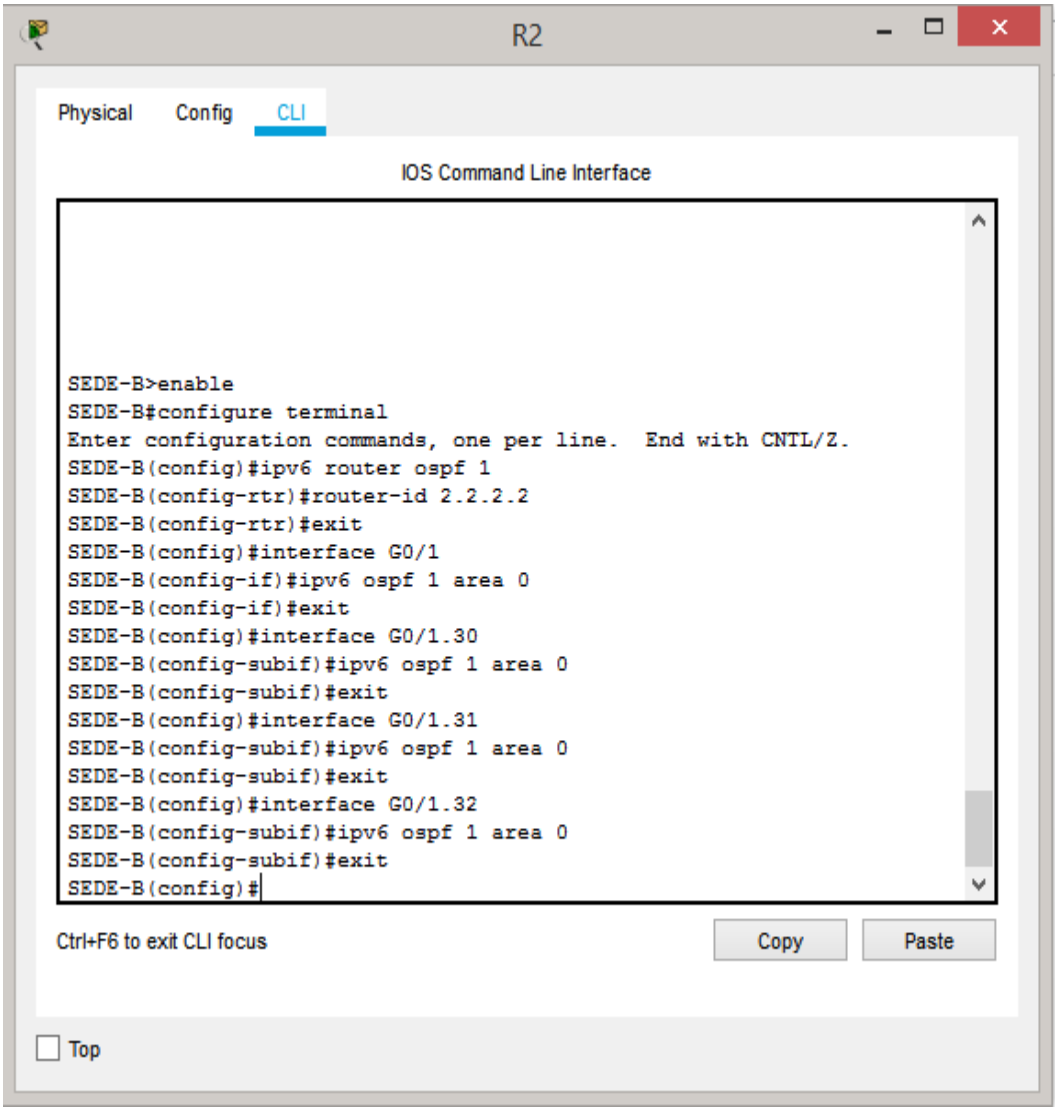


Figura 18 - Configuración del protocolo OSPFv3 en R2

Fuente: Elaboración Propia

Para la configuración de los servicios DHCP,DNS, SYSLOG-NTP y CORREO se realiza por medio de servidores, los cuales se encuentran conectados en las diferentes sedes para evidenciar que la red converge con protocolo IPV6, cabe aclarar que todos los servidores deben contar con una dirección IPV6 configurada de forma estática según el diseño del plan de direccionamiento propuesto, dado que

ninguno de estos pueden contar con direccionamiento dinámico a causa de que los equipos de las diferentes sedes deben solicitar los servicios a estos servidores y en caso de contar con direccionamiento dinámico esto impedirá que conozcan la ubicación de cada servidor. Como se ve en la Figura 19 los servidores están conectados de la siguiente manera.

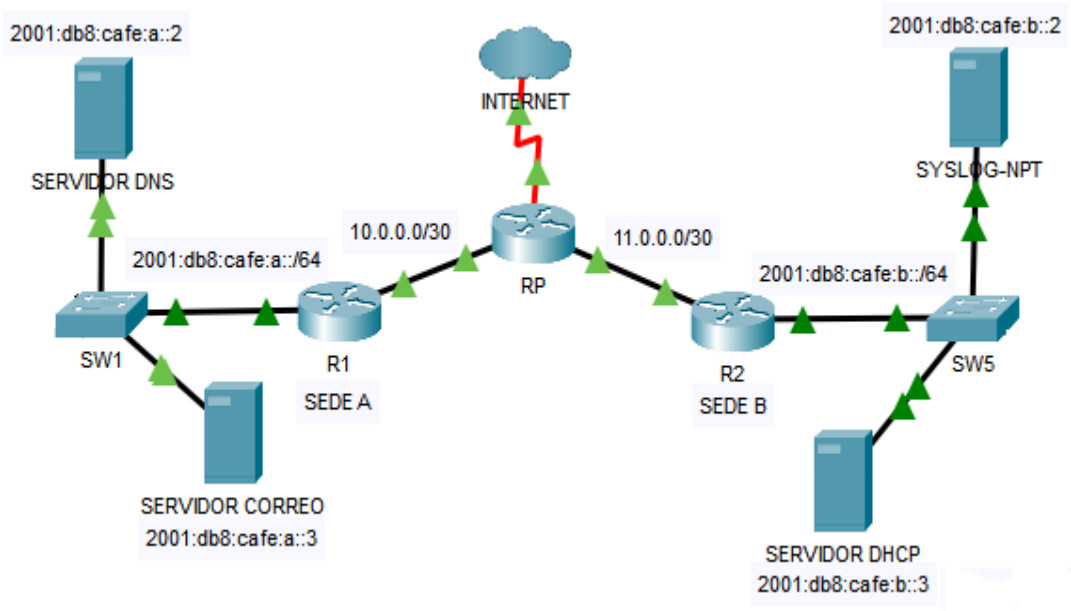


Figura 19 - Topología de los servidores

Fuente: Elaboración Propia

En primer lugar se establecerá el servicio DHCP encargado de brindar direccionamiento dinámico para los equipos que se encuentren en la red, a continuación se crea el Pool de direcciones, esta configuración cuenta con los segmentos: Nombre del Pool, la IP del servidor DNS, prefijo y Nombre del dominio (Figura 20).

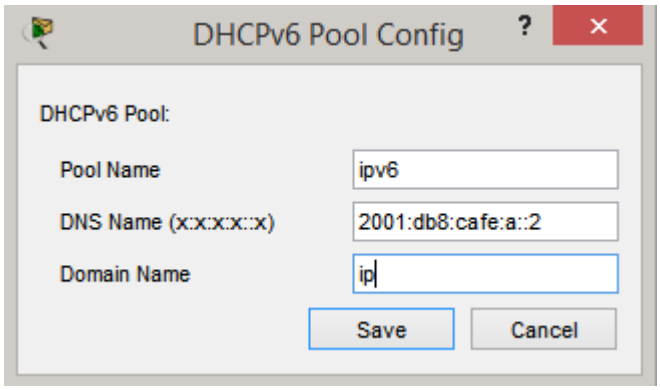


Figura 20 - Creación del Pool de direcciones

Fuente: Elaboración Propia.

Luego debe configurarse la dirección IP para el pool creado anteriormente, solo se necesita la dirección IPv4 y su prefijo, lo demás se mantiene por defecto Figura 21.

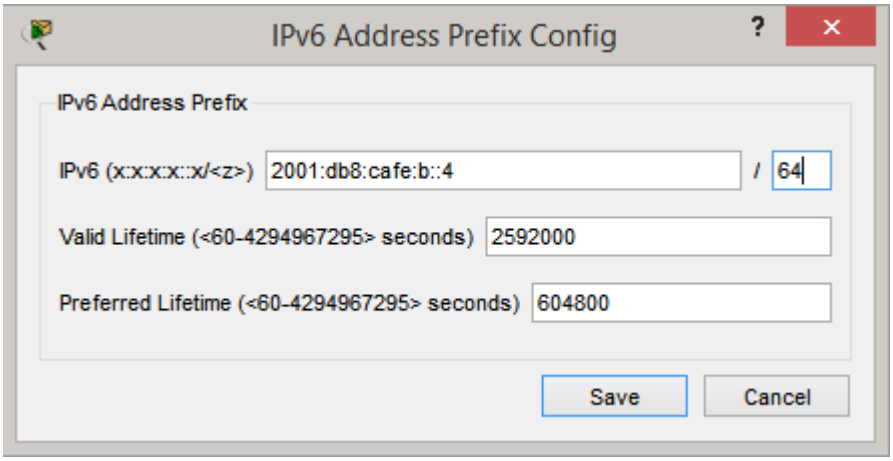


Figura 21 - Creación del Pool de direcciones

Fuente: Elaboración Propia

Al final la configuración en el servidor DHCP queda de la siguiente manera como se observa en la Figura 22.

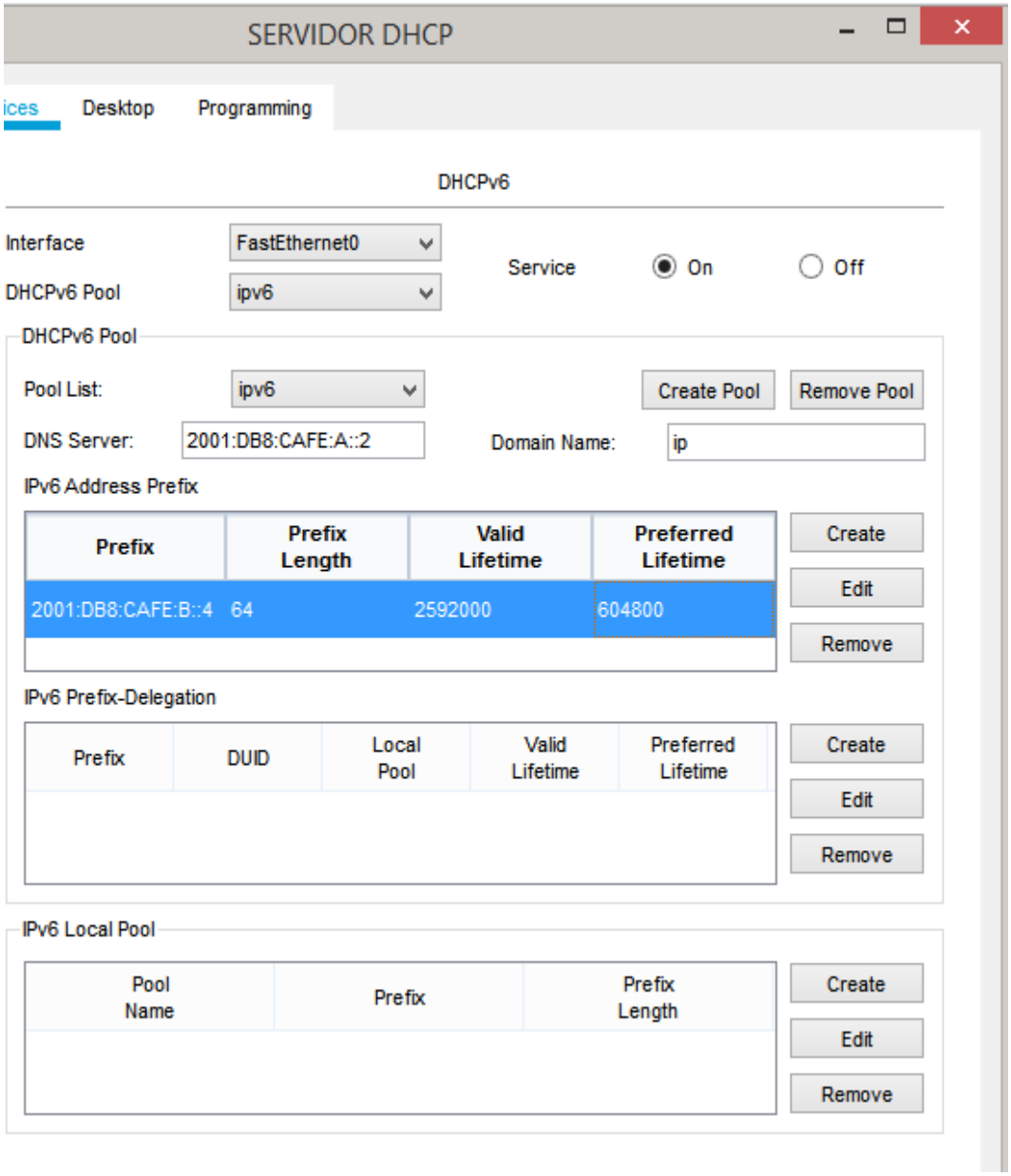


Figura 22 - Configuración del servidor DHCP

Fuente: Elaboración Propia

Seguidamente, para la configuración del servidor DNS el cual permite traducir un direccionamiento IPV6 a un nombre de dominio o viceversa, cuando un servidor DNS se encuentra dentro de una red LAN es porque la empresa u organización cuenta con Intranet la cual será accedida solo por los usuarios conectados en esta y no es publicada en internet, en la actualidad los servidores DNS son brindados por un

tercero o un ISP, estos permitirán conexión a internet a los equipos conectados en la red de la compañía. En la Figura 23 se muestra el nombre de dominio www.labelcompany.net el cual se configuro en el servidor DNS con la IPV6 2001:DB8:CAFE:A::2

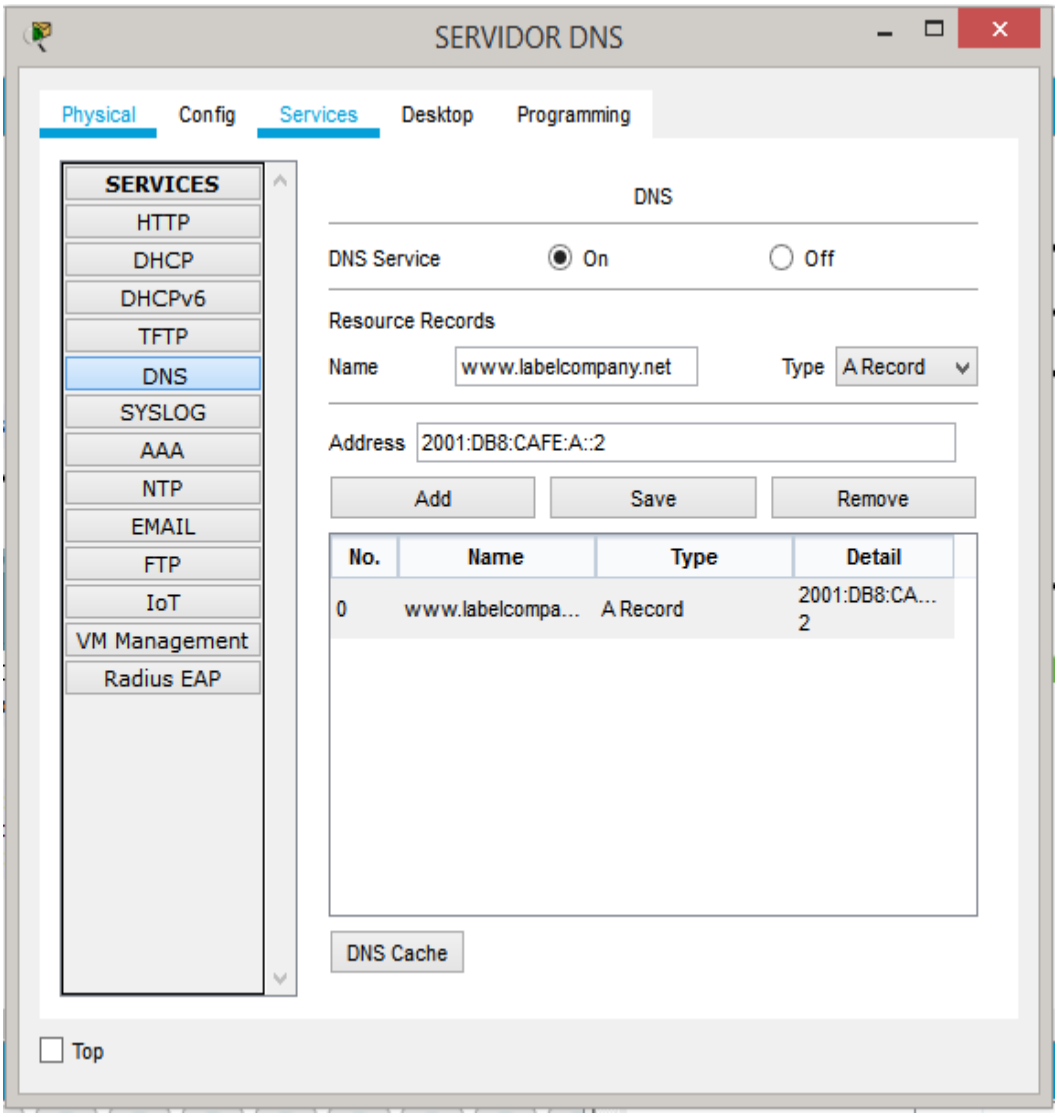


Figura 23 - Configuración del servidor DNS

Fuente: Elaboración Propia

Dando continuidad a la configuración de los servidores solicitados, para ejecutar la configuración del servidor de correo se procede a establecer el dominio

labelcompany.net, sobre este dominio se crearan todas las cuentas de correo que se utilizan sin importar la sede en la que se encuentre la persona, para la creación de un nuevo usuario bajo el dominio antes indicado se debe asociar un usuario y asignar una clave que permita autentica su identidad, en la Figura 24 se puede visualizar el dominio con los usuarios creados (Administrativos, usuarios).

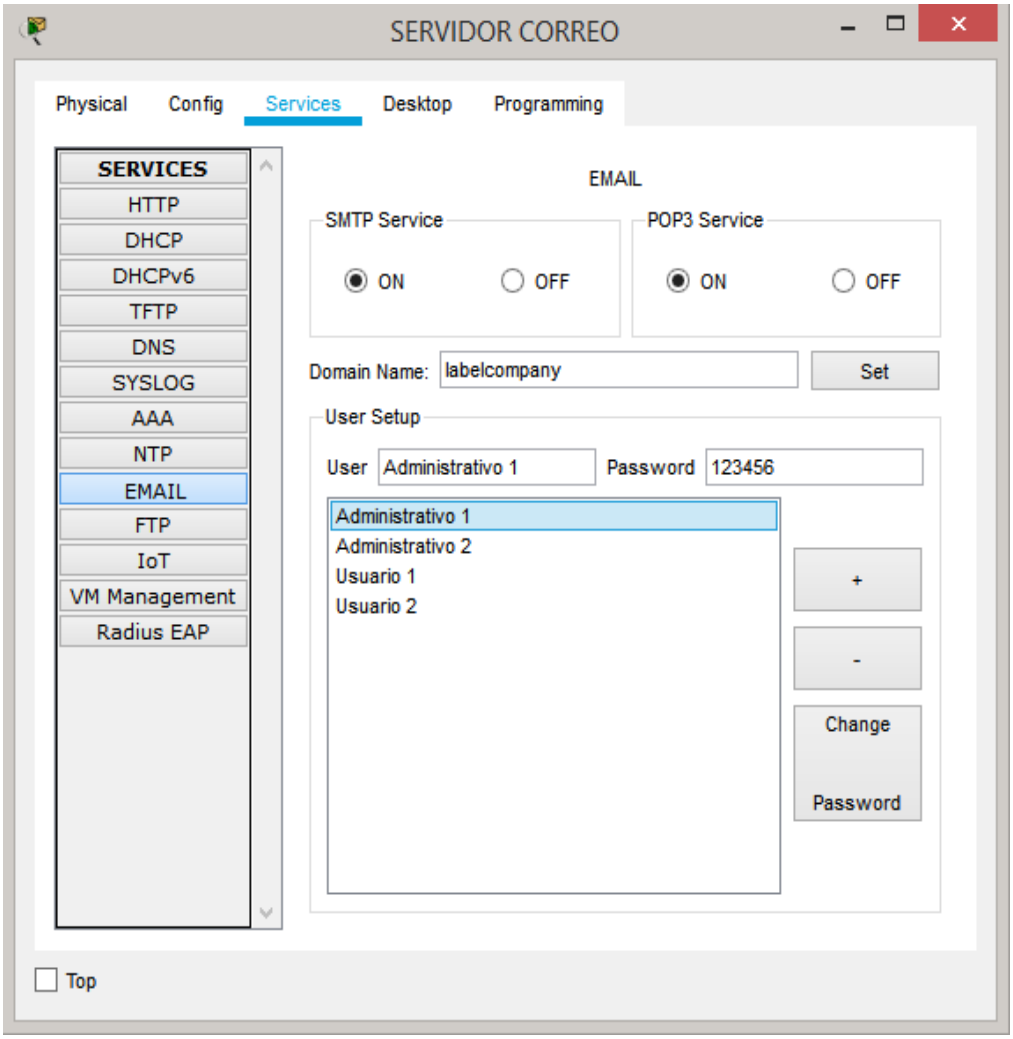


Figura 24 - Configuración del servidor de CORREO

Fuente: Elaboración Propia

Por último, y no menos importante, se configuraron los servicios NTP- SYSLOG, los cuales se puede aprovisionar en el mismo servidor; es de recordar que es el encargado de brindar y propagar la fecha y hora sobre la red, replicando estos parámetros en todos los equipos de comunicación, cómputo y servidores además este

servicio permite el funcionamiento del servicio syslog, el cual permite almacenar registro de todas las actividades realizadas en los diferentes router ubicados en sus diferentes sedes, el almacenamiento de esta información se efectúa mediante el registro en el servidor syslog visualizando fecha y hora del suceso o actividad realizada en los equipos, para mayor entendimiento se expone el siguiente ejemplo: si en el router de la sede A se desconecta una interfaz o se apaga el equipo este cambió sobre el equipo será almacenado en el servidor.

4.3.2.5. Configuración de la técnica de migración: Túnel GRE

Es un método que por medio de túneles encapsula los paquetes de datos y los envía por estos, generalmente esto se realiza para dos escenarios en específico, cuando se quieren comunicar dos redes que manejan protocolo IPV6 sobre una red IPv4 o dos redes IPv4 sobre una IPv6, esta última es poco común.

En este caso las sedes A y B manejan IPV6-only, y la principal mantiene su direccionamiento IPV4, es necesario ingresar a los routers, para activar los túneles, estos realizan la función de simular un enlace entre ambas puntas, donde se encapsularán los paquetes desde el origen y se desencapsula en el destino. La Figura 25 muestra el Tunnel 1 entre la Sede A y Sede B y la dirección IPv6 asignada.

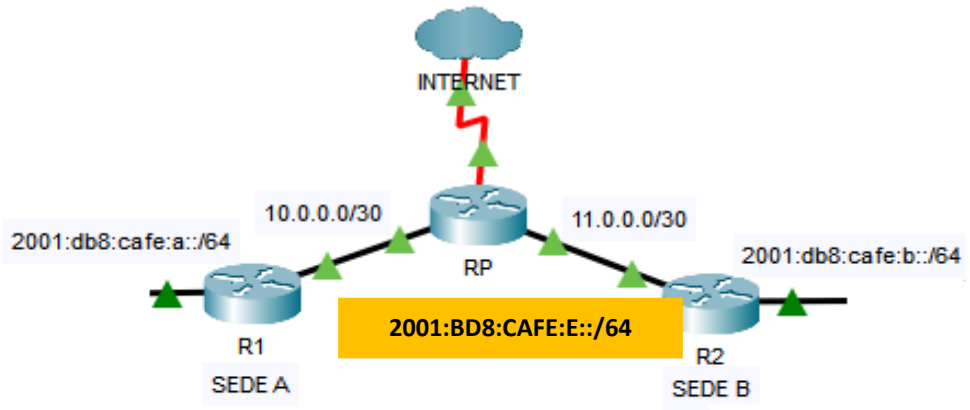


Figura 25 - Tunelización Sede A y Sede B

Fuente: Elaboración Propia

Al ingresar al router, se entra al modo configuración y seguidamente se crea una interfaz lógica conocida como Tunnel, la cual lleva direccionamiento IPV6. Esta se

maneja como una interfaz física normal, se agrega la IP que responda a la red resaltada en amarillo de la Figura 25 la cual es 2001:db8:CAFE:E::/64, es de aclarar que sobre esta interfaz también es obligatorio adicionar el enrutamiento OSPFv3 para que se pueda establecer la comunicación con las demás sedes, esto se efectúa como anteriormente se indica en la transición de protocolos a IPv6.

Adicionalmente para que el túnel funcione correctamente, se debe colocar el origen del túnel, en este caso es la interfaz por donde físicamente pasaría el tráfico hacia la otra sede. Y el destino, es la IP a donde llegarían los paquetes encapsulados, el cual sería la IP WAN del router de la sede B. Una vez que se establece el TUNNEL GRE, el modo del túnel debe soportar IPV6, por ende se utiliza el comando **tunnel mode IPV6ip**, toda esta configuración se ve en la Figura 26.

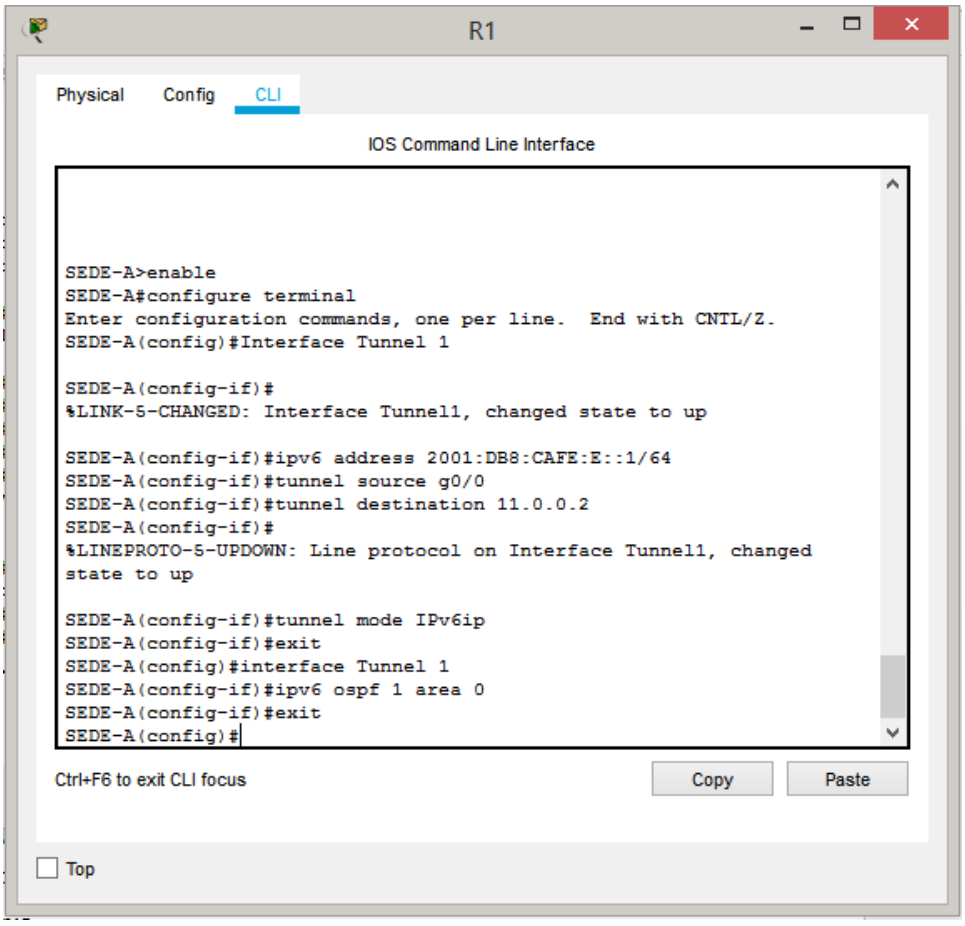


Figura 26 - Configuración del Túnel entre Sede A y Sede B en R1

Fuente: Elaboración Propia

Este procedimiento ha de efectuarse igualmente en el router de la sede B. donde los parámetros que cambiarían son el destino y el origen, como se indica en la Figura 27

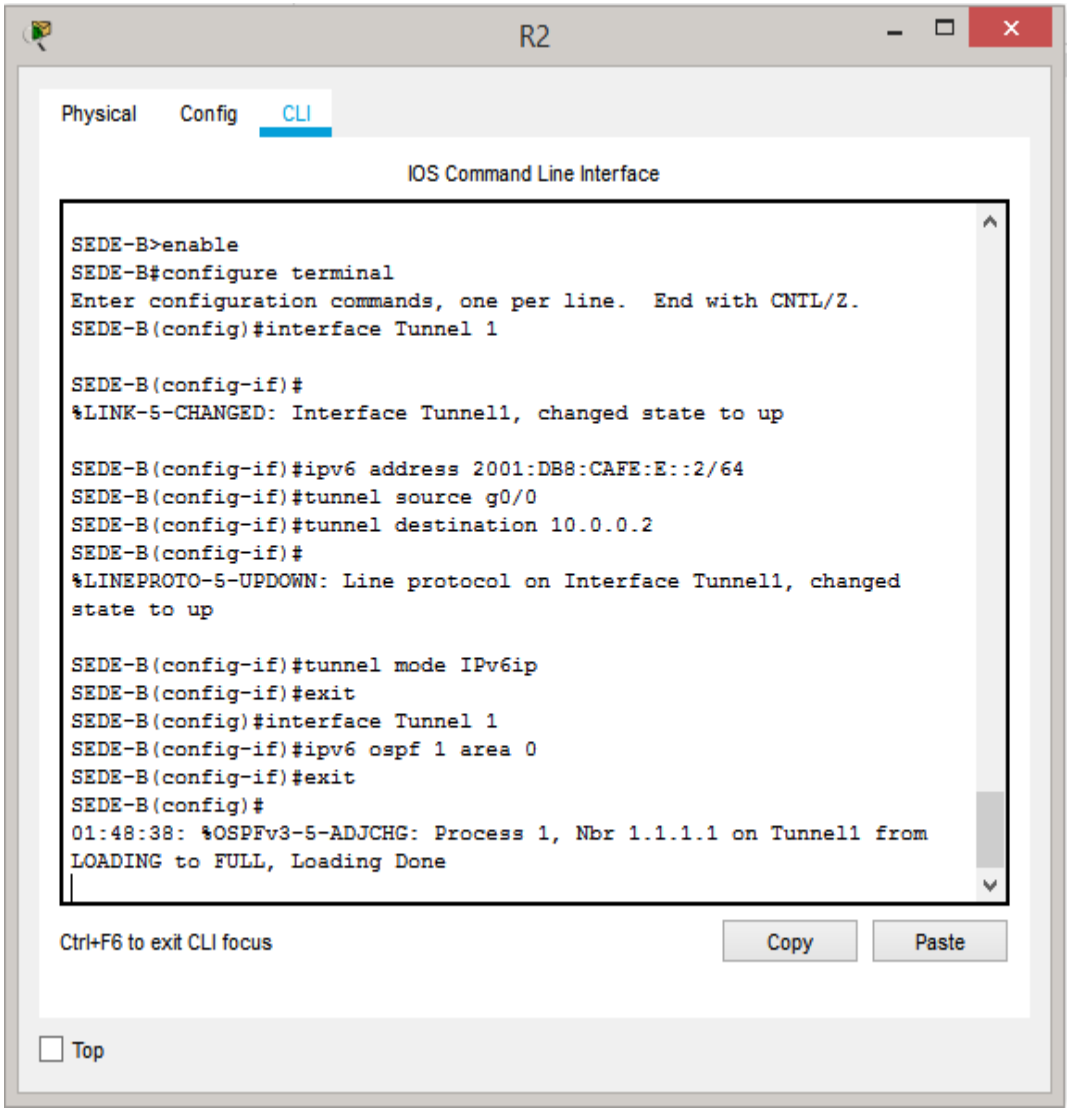


Figura 27 - Configuración del Túnel entre Sede A y Sede B en R2

Fuente: Elaboración Propia

4.3.2.6. Pruebas de funcionamiento de la red con protocolo IPv6

Se verifica la tabla de enrutamiento de las sedes implicadas, la Figura 28 pertenece a la sede A y la Figura 29 a la sede B, en donde se observa la conectividad entre las 2 sedes mediante IPv6 gracias al protocolo OSPFv3 con el comando **show ipv6 route**.

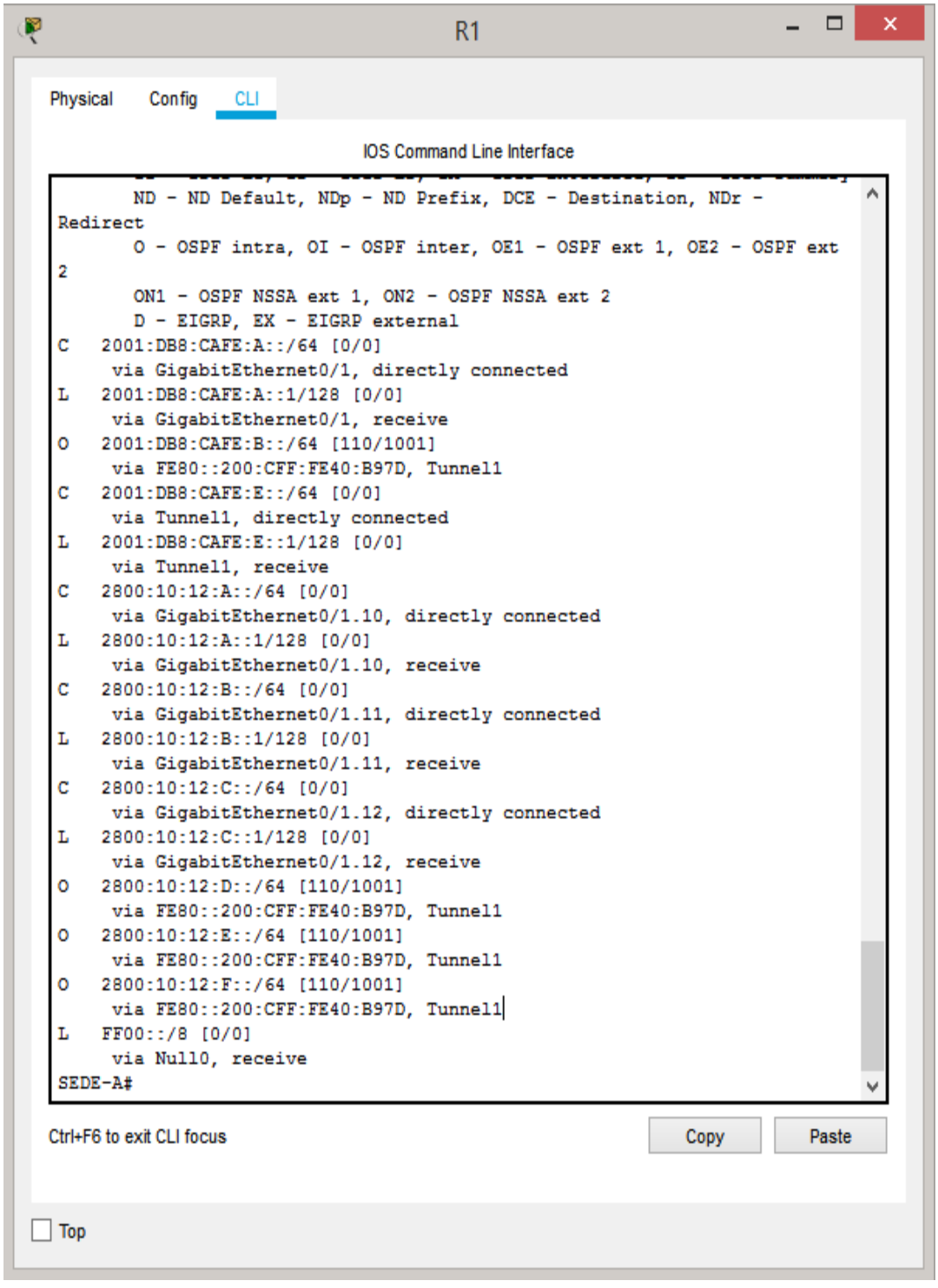


Figura 28 - Tabla de enrutamiento del router R1

Fuente: Elaboración Propia

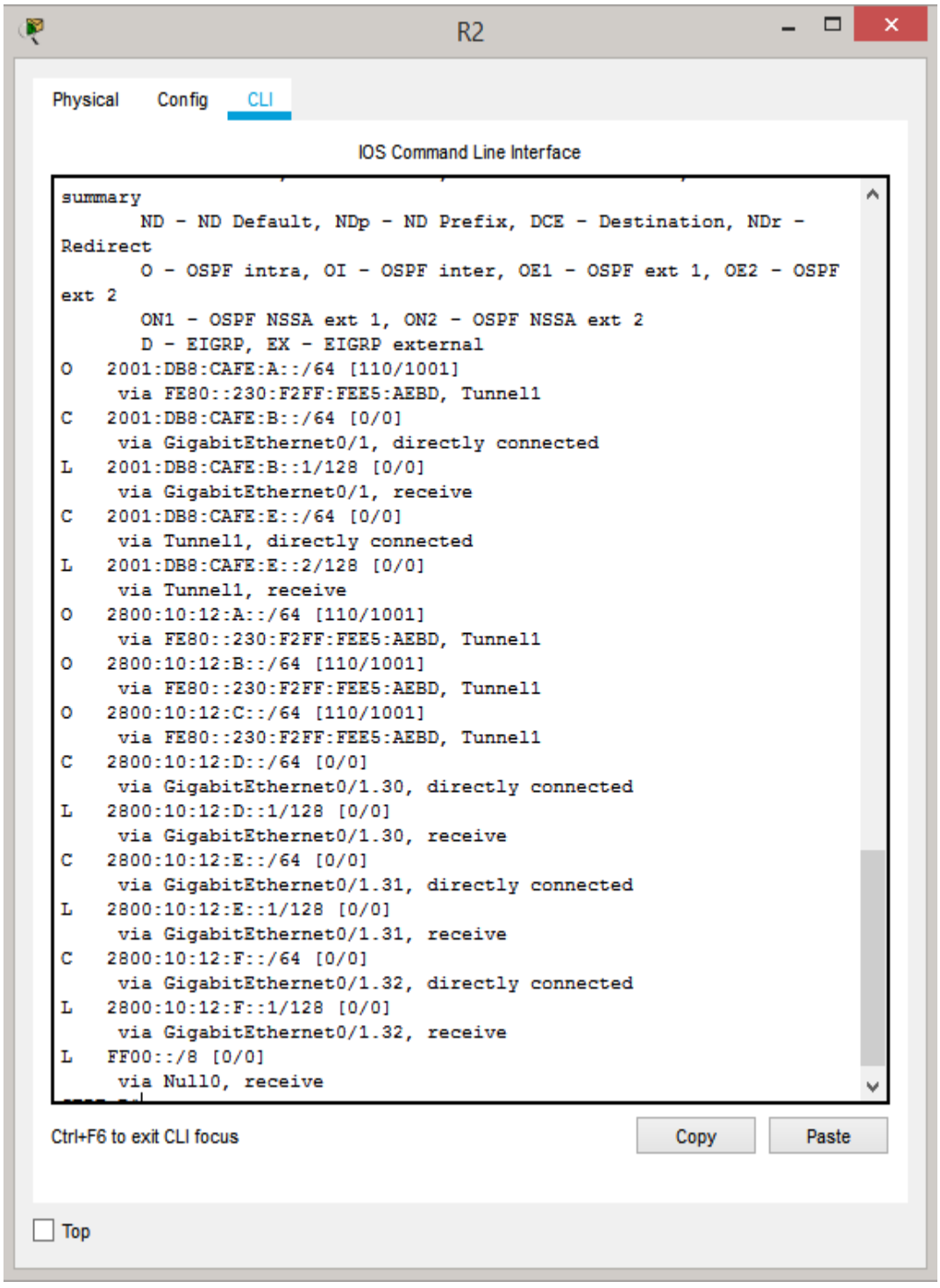


Figura 29 - Tabla de enrutamiento del router R2

Fuente: Elaboración Propia

También se puede verificar la conectividad entre las sedes mediante el comando PING, se envía 4 paquetes como se ve en la Figura 30 y Figura 31.

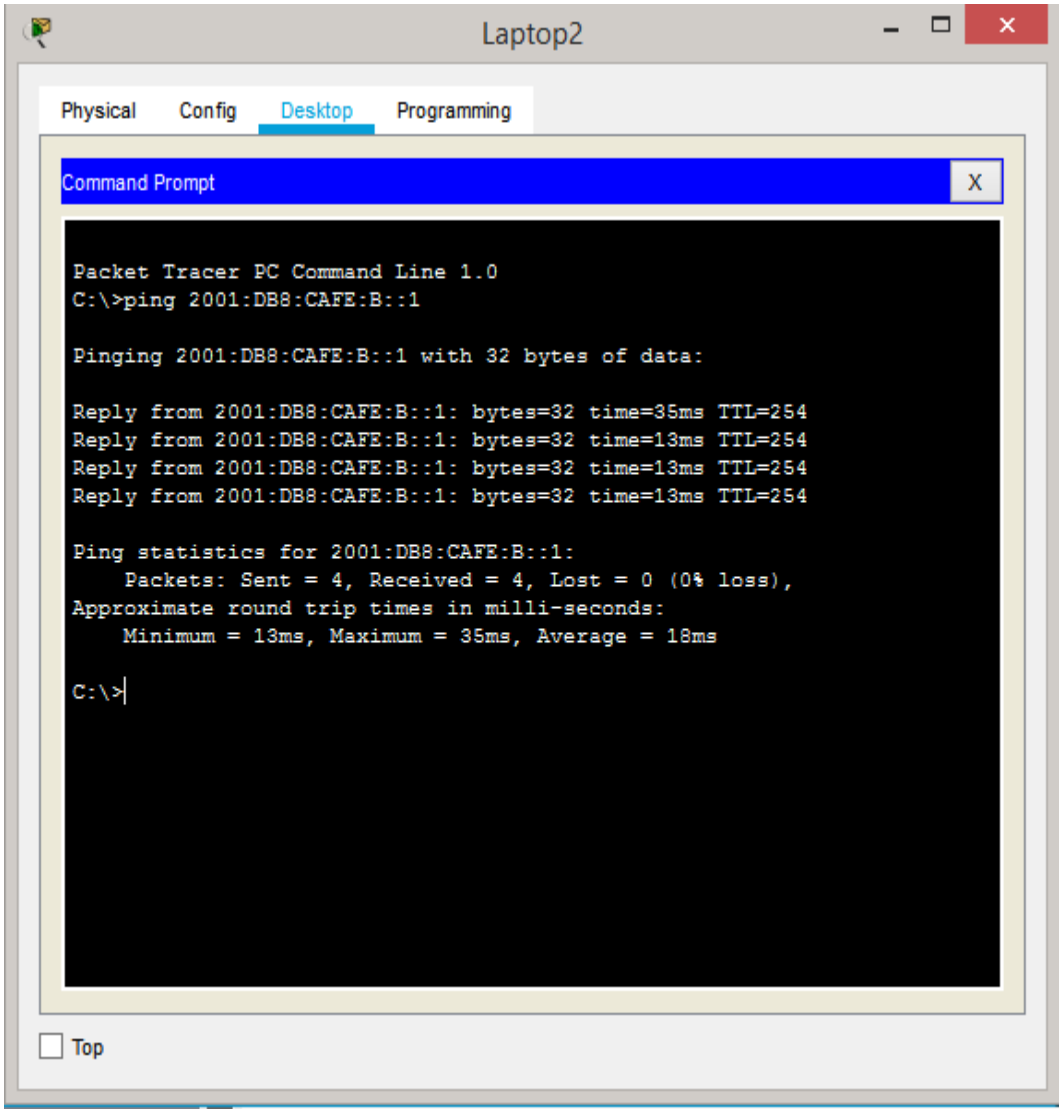


Figura 30 - Ping de Laptop2 de la Sede A hacia Sede B

Fuente: Elaboración Propia

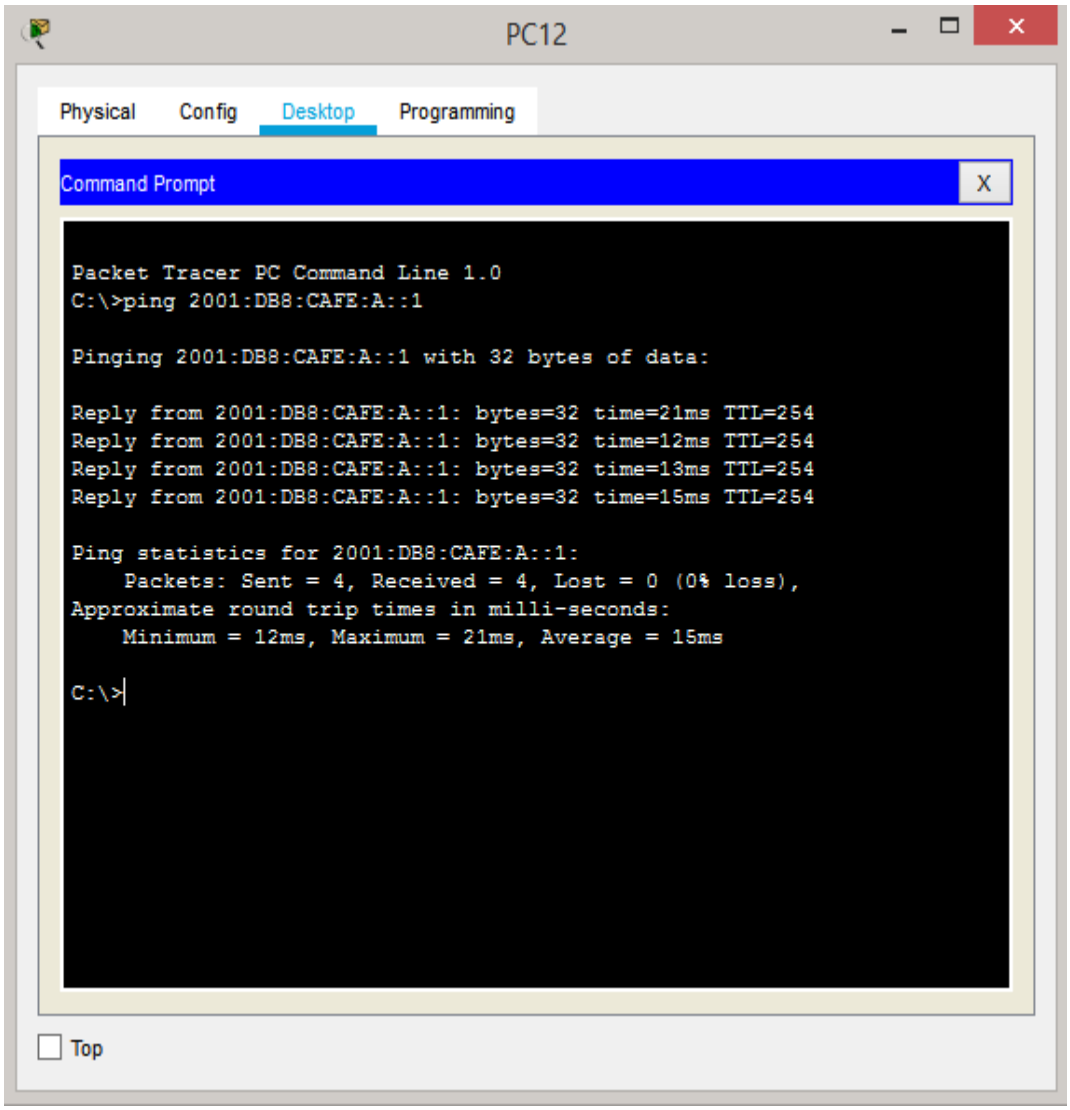


Figura 31 - Ping de PC12 de la Sede B hacia Sede A

Fuente: Elaboración Propia

Con respecto a la transición del protocolo IPv6, el resultado obtenido se puede observar con una prueba de PING entre dos computadores, una de la sede A y otra de la sede B. Igualmente, para identificar un mayor detalle de la trazabilidad del paquete se hará el uso del comando TRACERT entre estas dos computadoras como se ve en la Figura 32.

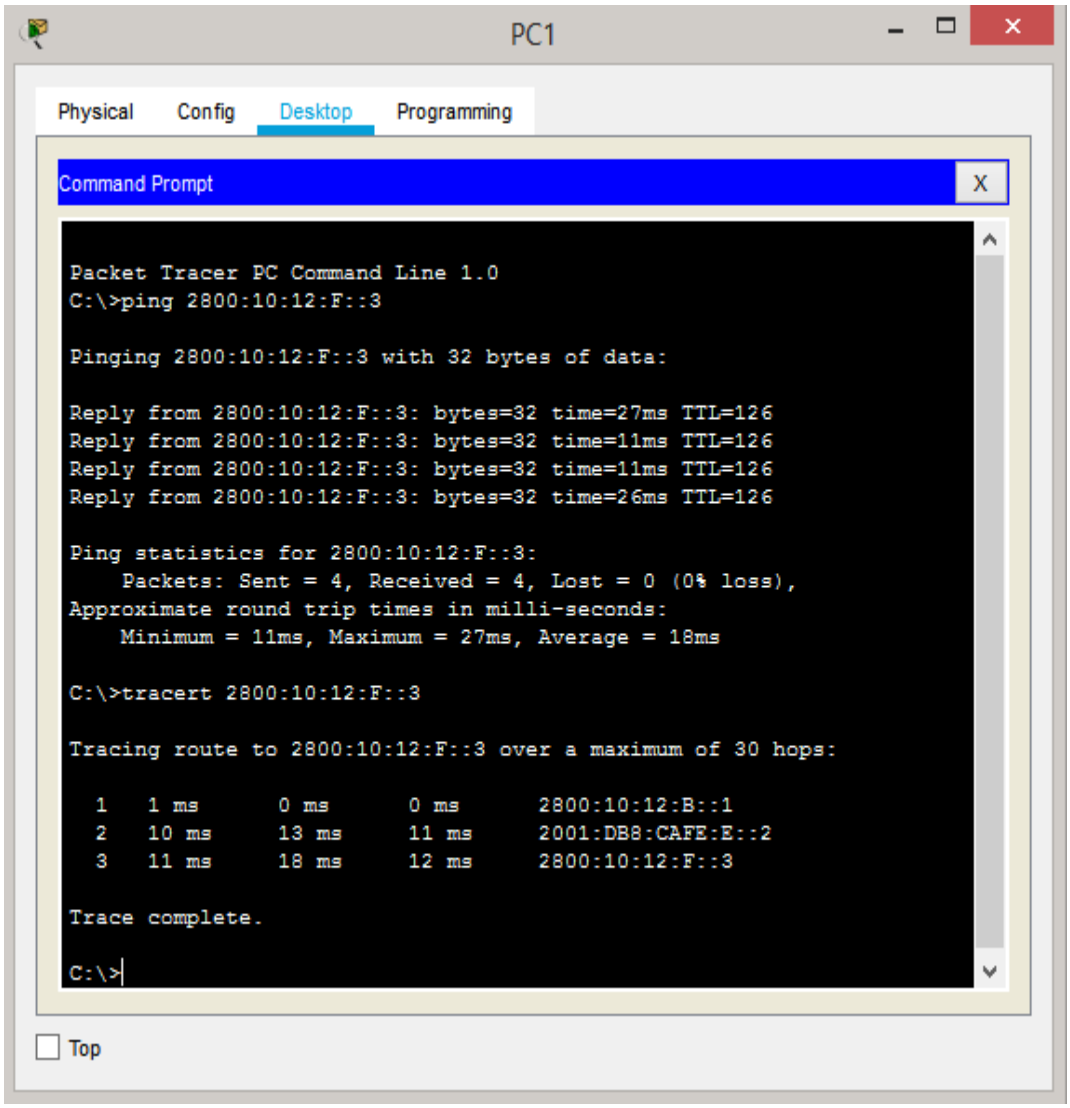


Figura 32 - Ejecución del comando Ping y Tracert entre PC1 y PC15

Fuente: Elaboración Propia

Se aprecia cómo los paquetes pasan por el túnel que tiene como dirección 2001:DB8:CAFE:E::2 y no se desvían por las interfaces físicas.

4.3.3. Límites del modelo

El modelo de migración solo contempla redes de datos de dos hasta tres redes WAN, en este caso de tener 2 redes WAN las interfaces que conectan con Internet o el ISP deben mantener su direccionamiento IPv4, si por el contrario se tiene 3 redes WAN la red principal debe actuar como puente para la tunelización y mantener su direccionamiento IPv4.

4.4. Fase Evaluativa

La evaluación al Modelo de migración implementado en el prototipo de red IPv4 De modo que se pueda evaluar el rendimiento de la red se hace una revisión a los artículos científicos donde se evalué el rendimiento de una red para poder extraer las métricas que utilizaron, en la siguiente tabla se puede apreciar los artículos consultados y sus respectivas métricas:

Tabla 12 - Métricas utilizadas en los artículos científicos para evaluar el rendimiento de una Red de datos

N°	ARTÍCULO CIENTÍFICO	MÉTRICAS			
1	(Siddika, Hossen, & Saha, 2017)	Rendimiento	Latencia	Tamaño de ventana TCP	
2	(Khaleel & Fayyadh , 2018)	Rendimiento	Latencia	Retraso de acceso a los medios	
3	(Narayanan, 2013)	Rendimiento	Latencia		
4	(Vivas, Silva, & Muñoz, 2017)	Velocidad de transferencia	Latencia	Tasa de transferencia	Pérdida de paquetes
5	(Aravind & Padmavathi, 2015)	Rendimiento	Latencia		
6	(Sookun & Basso, 2016)	Rendimiento	Latencia	Pérdida de paquetes	Utilización de CPU
7	(Altangerel, Tsogbaatar, & Yamkhin, 2016)	Rendimiento	Latencia		
8	(Komal, 2015)	Rendimiento	Latencia	Pérdida de paquetes	

Fuente: Elaboración propia

De los ocho artículos expuestos en la tabla 12, se agruparon las métricas para saber la cantidad que se repiten en todos los artículos científicos. En lo que se obtuvo lo siguiente:

Tabla 13 - Cantidad de veces que se utiliza la métrica en los artículos científicos

N°	MÉTRICA	CANTIDAD
1	Latencia	8
2	Rendimiento	7
3	Perdida de Paquetes	3
4	Uso de CPU	1
5	Retraso de acceso a los medios	1
6	Tamaño de ventana TCP	1
7	Velocidad de transferencia	1
8	Tasa de transferencia	1

Fuente: Elaboración propia

Según lo expuesto en la Tabla 13 las métricas que se van a utilizar son las tres primeras: Latencia, Rendimiento y Pérdida de paquetes por ser las que más se utilizan en los artículos científicos. Las fórmulas de la Tabla 14 (Vivas, Silva, & Muñoz, 2017), nos permiten calcular el valor de las métricas.

Tabla 14 - Forma de calcular el valor de las metricas

N°	MÉTRICA	FÓRMULA	VARIABLES
1	Latencia	$L = TV - TI\ [ms]$	TV: Tiempo de Vuelta TI: Tiempo de Ida
2	Rendimiento	$R = \frac{TP}{L}\ \left[\frac{Bytes}{s}\right]$	TP: Tamaño del paquete L: Latencia
3	Perdida de Paquetes	$\%PP = \frac{\#PP * 100}{\#PE}\ [\%]$	#PP: Número de paquetes perdidos #PE: Número de paquetes enviados

Fuente: Elaboración propia

4.4.1. Pruebas al modelo

A. Latencia

Para el cálculo de la Latencia en la red IPv4 e IPv6 se realiza 3 pruebas con ayuda del comando ping enviando 20 paquetes

- La prueba 1 efectúa el ping de PC1 en la sede A hacia PC15 de la sede B en la red IPv4 (Véase Anexo 3) y la red IPv6 (Véase Anexo 4).
- La prueba 2 efectúa el ping de Laptop0 en la sede A hacia PC12 de la sede B en la red IPv4 (Véase Anexo 5) y la red IPv6 (Véase Anexo 6).
- La prueba 3 efectúa el ping de PC13 en la sede B hacia PC5 de la sede A en la red IPv4 (Véase Anexo 7) y la red IPv6 (Véase Anexo 8).

Tabla 15 - Resultados del calculo de Latencia

Nro de Paq.	LATENCIA [ms]					
	Prueba 1		Prueba 2		Prueba 3	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	X	10	41	21	X	11
2	10	13	21	11	27	12
3	29	12	28	11	10	24
4	27	25	22	14	11	27
5	64	11	15	15	22	11
6	204	11	35	24	13	35
7	10	10	23	12	21	11
8	19	10	25	12	11	23
9	13	22	69	11	12	27
10	13	12	29	14	11	24
11	27	24	27	30	12	13
12	14	53	29	24	13	20
13	11	27	23	12	29	25
14	28	69	27	15	27	23
15	17	22	132	24	13	26
16	13	26	28	21	13	25
17	14	12	11	21	11	12
18	13	14	29	22	22	13
19	10	27	14	12	13	25
20	11	11	40	26	12	21
PROM	**29**	**21**	**33**	**18**	**16**	**20**

Fuente: Elaboración propia

La Tabla 15 nos muestra el tiempo que le tomo a cada paquete llegar a su destino y el promedio estos valores para cada prueba y red.

Tabla 16 - Análisis del promedio de Latencia en las pruebas

	Prueba 1	**Prueba 2**	**Prueba 3**
IPv4	29	33	16
IPv6	21	18	20
Mayor Latencia	IPv4	IPv4	IPv6

Fuente: Elaboración propia

La Tabla 16 nos advirte que la red que mayor latencia presenta es la red IPv4, dado que obtuvo mayores valores en dos de las tres pruebas.

B. Rendimiento

Luego que ya se obtiene la latencia, se aplica la fórmula de rendimiento de la Tabla 14 dividiendo el tamaño del paquete entre la latencia, los resultados para el rendimiento se observan en la Tabla 17.

Tabla 17 - Resultados del cálculo del Rendimiento

Nro de Paq.	RENDIMIENTO [Bytes/s]					
	Prueba 1		Prueba 2		Prueba 3	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	X	3200	780	1524	X	2909
2	3200	2462	1524	2909	1185	2667
3	1103	2667	1143	2909	3200	1333
4	1185	1280	1455	2286	2909	1185
5	500	2909	2133	2133	1455	2909
6	157	2909	914	1333	2462	914
7	3200	3200	1391	2667	1524	2909
8	1684	3200	1280	2667	2909	1391
9	2462	1455	464	2909	2667	1185
10	2462	2667	1103	2286	2909	1333
11	1185	1333	1185	1067	2667	2462
12	2286	604	1103	1333	2462	1600
13	2909	1185	1391	2667	1103	1280
14	1143	464	1185	2133	1185	1391
15	1882	1455	242	1333	2462	1231
16	2462	1231	1143	1524	2462	1280
17	2286	2667	2909	1524	2909	2667
18	2462	2286	1103	1455	1455	2462
19	3200	1185	2286	2667	2462	1280
20	2909	2909	800	1231	2667	1524
PROM	2036	2063	1277	2028	2266	1796

Fuente: Elaboración propia

Tabla 18 - Analisis del rendimiento en las redes

RED	Prueba 1	Prueba 2	Prueba 3
IPv4	2036	1277	2266
IPv6	2063	2028	1796
Mayor Rendimiento	IPv6	IPv6	IPv4
Menor Rendimiento	IPv4	IPv4	IPv6

Fuente: Elaboración propia

La tabla 18 indica que la red con mayor rendimiento en dos de las tres pruebas, es la red IPv6 por lo que se deduce que las redes que mayor latencia presentan disminuyen su rendimiento.

C. Perdida de Paquetes

La pérdida de paquetes se produce cuando uno de los paquetes enviados no llega a su destino, para las pruebas se hace el envío de 20 paquetes como indica la Tabla 19, a la cual se le asigna una X en caso de que el paquete se haya perdido y TPP representa el total de paquetes perdidos por prueba.

Tabla 19 - Resultados de la cantidad de paquetes perdidos

Nro de Paq.	PÉRDIDA DE PAQUETES					
	Prueba 1		Prueba 2		Prueba 3	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	X	10	41	21	X	11
2	10	13	21	11	27	12
3	29	12	28	11	10	24
4	27	25	22	14	11	27
5	64	11	15	15	22	11
6	204	11	35	24	13	35
7	10	10	23	12	21	11
8	19	10	25	12	11	23
9	13	22	69	11	12	27
10	13	12	29	14	11	24
11	27	24	27	30	12	13
12	14	53	29	24	13	20
13	11	27	23	12	29	25
14	28	69	27	15	27	23
15	17	22	132	24	13	26
16	13	26	28	21	13	25
17	14	12	11	21	11	12
18	13	14	29	22	22	13
19	10	27	14	12	13	25
20	11	11	40	26	12	21
TPP	**1**	**0**	**1**	**0**	**0**	**0**

Fuente: Elaboración propia

Para calcular el porcentaje de la pérdida de paquetes se aplica la fórmula de la Tabla 14 con el total de paquetes perdidos y la cantidad de paquetes enviados.

Tabla 20 - Resultados del cálculo de porcentaje de paquetes peridos

RED	PÉRDIDA DE PAQUETES [%]		
	Prueba 1	**Prueba 2**	**Prueba 3**
IPv4	5%	5%	0%
IPv6	0%	0%	0%
Red con mayor %PP	IPv4	IPv4	Ninguna

Fuente: Elaboración propia

La red con mayor porcentaje de paquetes perdidos es la Red IPv4, con un 5% de perdida, a diferencia de red IPv6 que presenta un 0% de paquetes perdidos como indica la Tabla 20.

CAPÍTULO V PRUEBA DE HIPÓTESIS

El presente trabajo de investigación, plantea la hipótesis: "El modelo de migración de red al protocolo IPv6 mitigará el agotamiento de direcciones IPv4 disponibles para redes Empresariales en al menos un 50%". Por lo tanto se implementa el modelo de migración en tres prototipos de Redes de Datos distintos en diseño de topología de red y direccionamiento IPv4 bajo el escenario Empresarial RED 1 (Véase Anexo 9), RED 2 (Véase Anexo 10) y RED 3 (Véase Anexo 11); Con la herramienta de simulación Cisco Packet Tracert.

Para fines de prueba de hipótesis se debe calcular la Tasa de Utilización en cada una de las redes. Según el manual de políticas de LACNIC la Tasa de Utilización es el porcentaje de direcciones IPv4 que la organización o empresa utiliza, y se obtiene de la siguiente manera (LACNIC, 2020):

$$\mathrm{TU} = \frac{\#\mathrm{D_I} + \#\mathrm{D_E}}{\mathrm{TDU}} * 100\ [\%]$$

Donde:

TU= Tasa de Utilización.

$\#D_I$= Número de direcciones asignadas en Interfaces Físicas y Lógicas.

$\#D_E$ = Número de direcciones asignadas a los Equipos de Cómputo y/o Servidores.

TDU = Total de direcciones en uso.

La Tabla 21 contiene los resultados de la tasa de utilización obtenidos en RED 1, RED 2 Y RED 3.

Tabla 21 - Resultados tasa de utilización

TASA DE UTILIZACIÓN [%]				
	$\#D_I$	**$\#D_E$**	**TDU**	**TU**
RED 1	5	0	32	16
RED 2	2	0	35	6
RED 3	7	8	40	38

Fuente: Elaboración propia.

Con los datos obtenidos en la Tabla 21 podemos obtener el porcentaje en que el modelo de migración mitiga el agotamiento de direcciones IPv4.

Tabla 22 - Porcentaje de mitigación de direcciones IPv4

DISMINUCIÓN DE USO DE DIRECCIONES IPV4 [%]			
	TU sin Modelo	**TU con Modelo**	**Porcentaje de disminución de uso de direcciones IPv4**
RED 1	100%	16%	84%
RED 2	100%	6%	94%
RED 3	100%	38%	62%

Fuente: Elaboración propia

Por lo expuesto en la Tabla 22 podemos afirmar que el Modelo de migración de Red IPv4 al protocolo IPv6 para Redes Empresariales mitiga el agotamiento de direcciones IPv4 disponibles para redes Empresariales en al menos un 50%. Por lo tanto se acepta la hipótesis de investigación.

CAPÍTULO VI CONCLUSIONES Y RECOMENDACIONES

En este último capítulo se presentan las conclusiones a las que se ha llegado después de haber realizado el presente trabajo, así como algunas recomendaciones para aquellos que deseen realizar futuras investigaciones siguiendo la misma línea de estudio ya sea para mejorar aspectos del mismo tema o para aplicar una metodología distinta.

6.1. CONCLUSIONES

- Se desarrolló un Modelo de migración de red IPv4 al protocolo IPv6 para redes empresariales, que mitiga el agotamiento de direcciones IPv4, mejorando calidad de servicio de la Red de Datos.
- Se realizó una profunda investigación acerca del protocolo IPv6 y las técnicas de migración, el cual aporta soluciones a los problemas de crecimiento de Internet e incorpora funcionalidades que mejoran su comportamiento en aspectos de seguridad y configuración Con este protocolo varias empresas y compañías podrán hacer uso de nuevas aplicaciones y funciones, las cuales poseerán un diseño y software más robusto, donde se podrán conectar una gran cantidad de equipos, resaltando que se poseerá una mayor disponibilidad, integridad y confidencialidad que el protocolo antecesor. Aunque la transición a IPV6 en términos de enrutamiento y direccionamiento es relativamente rápida, se debe tener en cuenta que para la migración se encuentre al 100% tardará algunos años, dado que algunas aplicaciones y servidores solo permiten el protocolo IPv4.
- Se realizó un estudio comparativo y analítico de artículos científicos sobre las diferentes técnicas de migración, y se determinó conveniente optar por la técnica de Tunelización GRE para llevar a cabo la migración, ya que obtuvo mejores resultados en las métricas Latencia, Rendimiento y Uso de CPU
- Se diseñó la solución para la migración a IPv6 mediante una arquitectura de modelo causal en cadena.
- Se implementó un prototipo de red empresarial con el modelo de migración, al se le realizaron pruebas en base a tres métricas: Latencia Rendimiento y

Porcentaje de pérdida de paquetes. El prototipo de red con el modelo arrojo los mejores resultados obteniendo Menor Latencia, Mayor rendimiento y 0% de pérdida de paquetes sobre el prototipo de red IPv4.

- La escalabilidad de redes es uno de los beneficios más importantes y notorios dentro de la implementación del protocolo IPV6, esto puede ser de gran utilidad en las empresas para el diseño del plan de direccionamiento, ya que generalmente los ISP brindan un pool de IP con máscara /64, lo que proporciona una cantidad inmensa de direcciones asignables ayudando a realizar cambios significativos sin tener repercusiones negativas sobre sus servicios o direccionamiento de dispositivos.

6.2. RECOMENDACIONES

La implementación del protocolo IPv6 es un reto, sin embargo éste debe ser enfrentado y superado tarde o temprano para lo cual es necesario tener el conocimiento suficiente sobre IPv6. Los profesionales relacionados con el área de redes deben capacitarse para la implementación y administración de una red IPv6, debido a que este protocolo es el sucesor innegable del protocolo IPv4.

Las redes empresariales deben tener muy en cuenta el crecimiento de internet, y las nuevas tecnologías que emergen, para evitar futuros problemas de escalabilidad y disponibilidad deben considerar la implementación del Modelo de migración red IPv4 al protocolo IPv6.

BIBLIOGRAFÍA

1. ATT - Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes. (2016) *Memoria institucional 2016*. Recuperado de: https://att.gob.bo/sites/default/files/archivospdf/Memoria%20Institucional%202016.pdf
2. Carofilis Moreira, U. A. (2017). *Estudio para la migración del protocolo IPv4 al protocolo IPv6. Caso de estudio plenario de la asamblea nacional* (Maestría). Pontificia Universidad Católica del Ecuador. Recuperado de: http://repositorio.puce.edu.ec/bitstream/handle/22000/14002/Tesis%20Ulises%20Carofilis%20capt%201-2-3-4%20UV.pdf?sequence=1&isAllowed=y
3. Cisco, (2021). *Introducción a las Redes,* de: https://contenthub.netacad.com/itn.
4. Cespedes, M. (2013). *Historia del protocolo TCP/IP y IPv4 - IPv6*. Redes I. Recuperado el 01 de Junio de 2021, de: http://redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-IPv4-IPv6.html
5. Enriquez Castillo, A. L., & Nureña Sánchez, G. M. (2014). *Diseño Lógico de la Migración de IPV4 a IPV6 de la Red de Datos de la Universidad Nacional de Trujillo* (Licenciatura). Universidad Nacional de Trujillo. Recuperado de: https://dspace.unitru.edu.pe/bitstream/handle/UNITRU/11301/ENRIQUEZ%20CASTILLO,%20Alexander%20L.%20-%20NURE%C3%91A%20S%C3%81NCHEZ,%20Gabriela%20M.pdf?sequence=1&isAllowed=y
6. Hurtado de Barrera, J. (2008). *La investigación proyectiva*. Investigación holística. Recuperado el 24 de Mayo de 2021, de: http://investigacionholistica.blogspot.com/2008/02/la-investigacin-proyectiva.html
7. Hurtado de Barrera, J. (2010). *Metodología de la Investigación* (4th ed., p. 134). Caracas, Venezuela: Quirón Ediciones. Recuperado de: https://dariososafoula.files.wordpress.com/2017/01/hurtado-de-barrera-

metodologicc81a-de-la-investigaciocc81n-guicc81a-para-la-comprensiocc81n-holicc81stica-de-la-ciencia.pdf

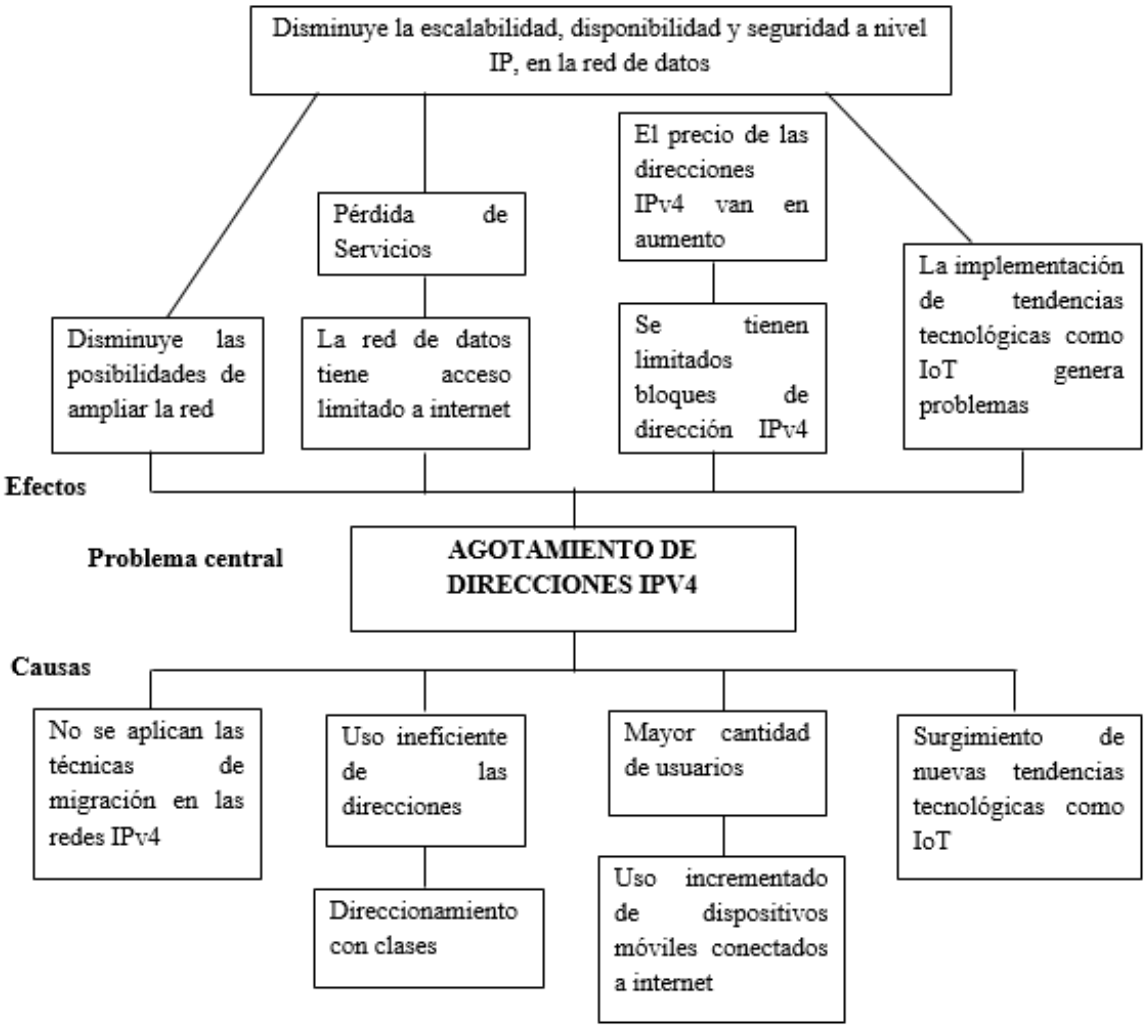
8. Kurose, J., & Ross, K. (2017). *Redes de computadoras un Enfoque Descendente* (7th ed.). Madrid: Pearson Educación.
9. LACNIC (2021). *Fases de agotamiento de IPv4*. Recuperado el 26 de Mayo de 2021, de: https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-IPv4
10. LACNIC (2015). *Despliegue de IPv6 para el desarrollo socio económico en América Latina y el Caribe*. Recuperado el 04 de Junio de 2021, de: https://www.lacnic.net/innovaportal/file/3035/1/caf-lacnic-despliegue-IPv6-para-desarrollo-socio-economico-en-lac.pdf
11. Llanos Gómez, R. A. (2016). *Plan de migración de IPv4 a IPv6 para una red de un proveedor de servicios de internet (ISP).* Journal Boliviano de Ciencias, 12(36). Recuperado de: http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid= S2075-89362016000100006&lng=pt&nrm=iso
12. MinTIC - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2021). *Guía de Transición de IPv4 a IPv6 para Colombia*. Recuperado el 16 de junio de 2021, de : https://mintic.gov.co/portal/715/articles125210_Guia_Transicion_IPV4_IPV6_ Colombia _27052021.pdf
13. Molina, A. (2018, junio 11). *Agotamiento de las direcciones IPv4*. Recuperado el 16 de junio de 2021, de: https://openwebinars.net/blog/agotamiento-de-las-direcciones-IPv4/
14. Montañez Prieto, J. P. (2018). *Propuesta para la migración del protocolo IPv4 a protocolo IPv6 para la secretaria del Sisben de la alcaldía de Tunja* (Licenciatura) Universidad nacional abierta y a distancia. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/19074/7169456.pdf;jsessionid=1E40E8B5226A3A4D49D6A4E65E27EEC6.jvm1?sequence=1
15. Nguyen, P., & Nguyen, Q. (2016). *Transition from IPv4 to IPv6 Best Transition Method for Large Enterprise Networks* (Licenciatura). Lahti University of Applied

Sciences. Recuperado de: https://www.theseus.fi/bitstream/handle/10024/40098/Nguyen_Phu.pdf

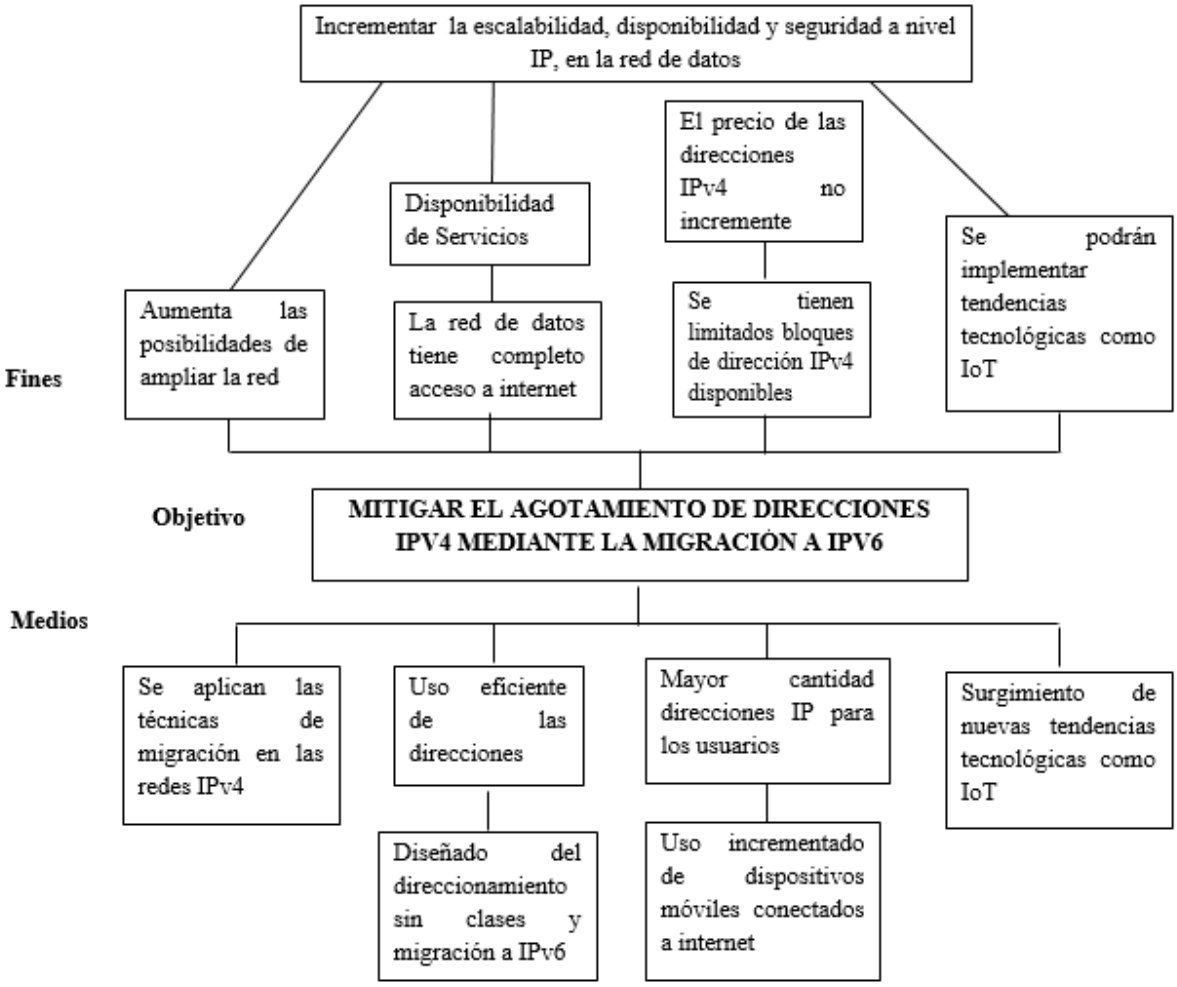
16. Roca Marín, R. D. (2009). *Propuesta de estrategia nacional para la implementación de IPv6 en Bolivia* (Licenciatura). Universidad Mayor de San Andrés. Recuperado de: https://repositorio.umsa.bo/handle/123456789/1554
17. Yapu Apaza, H. (2016). *Plan de implementación para la migración de IPv4 a IPv6 en la red de COTEL* (Licenciatura). Universidad Mayor de San Andrés. Recuperado de: https://repositorio.umsa.bo/bitstream/handle/123456789/9341/PG-1427Yapu%20apaza% 2c%20Hugo.pdf?sequence=1&isAllowed=y
18. Yirda, A. (2021). *Definición de Internet*. Recuperado el 04 de Junio de 2021, de: https://conceptodefinicion.de/internet/

ANEXOS

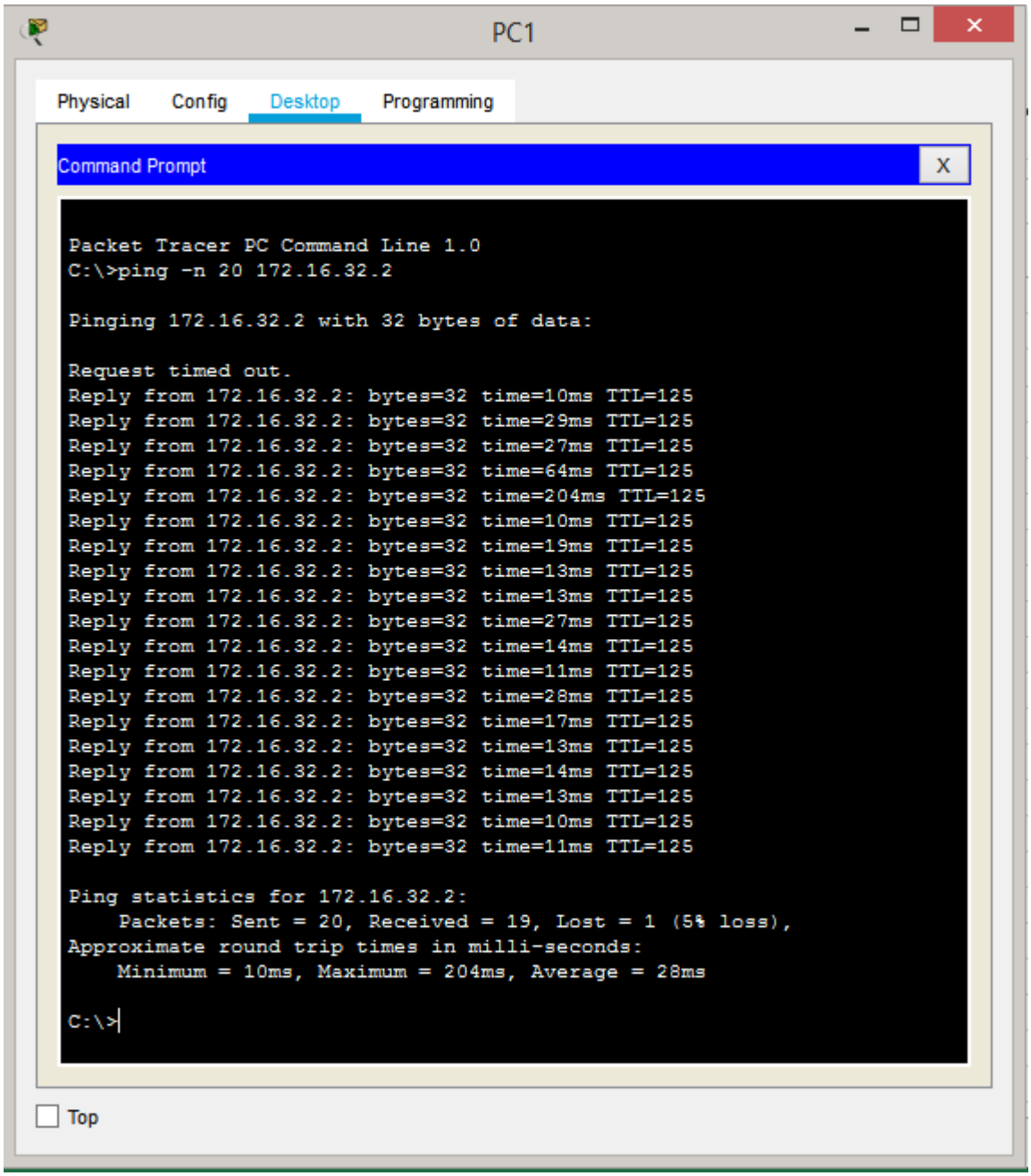
ANEXO 1 Árbol de Problemas



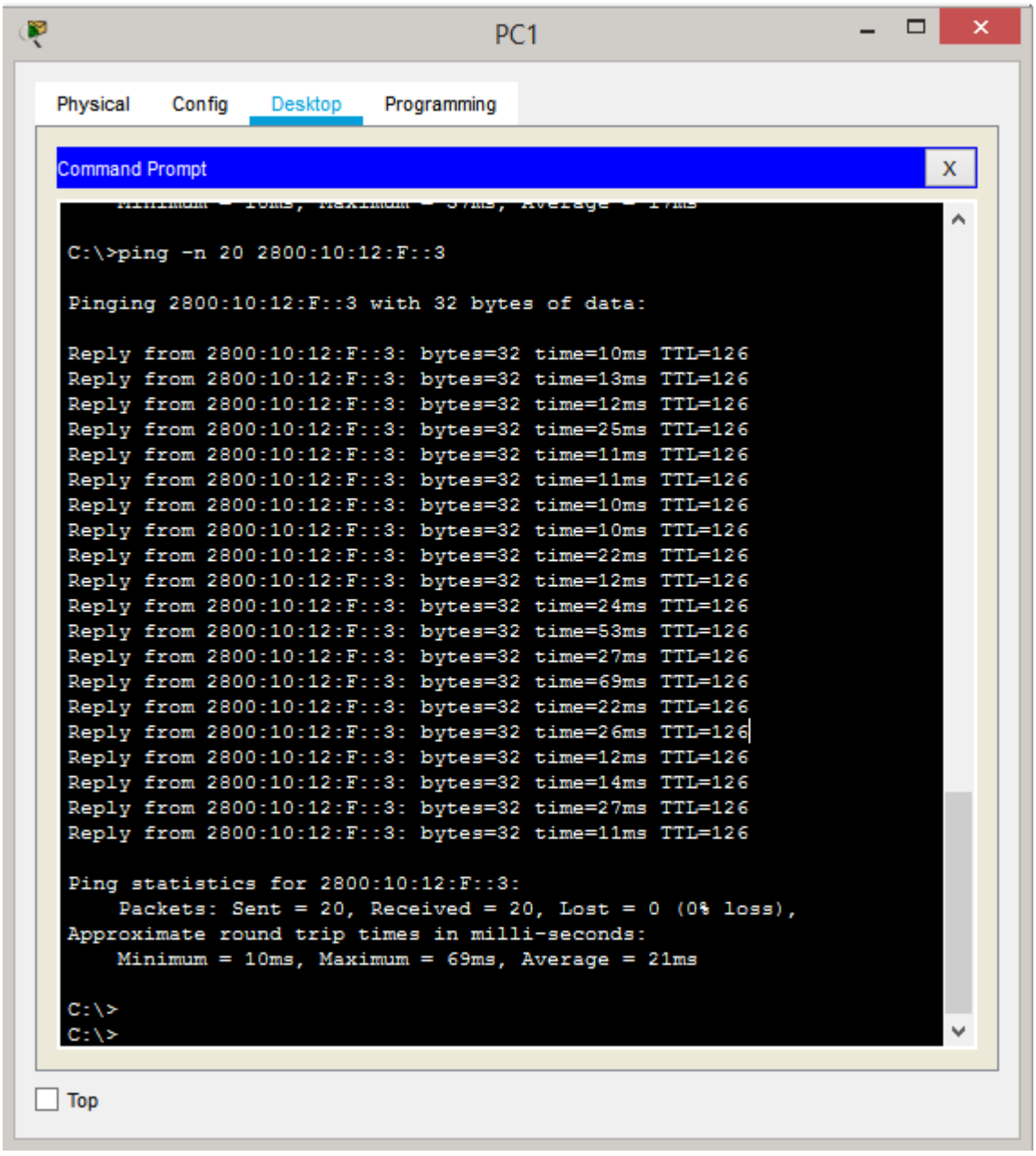
ANEXO 2 Árbol de Objetivos



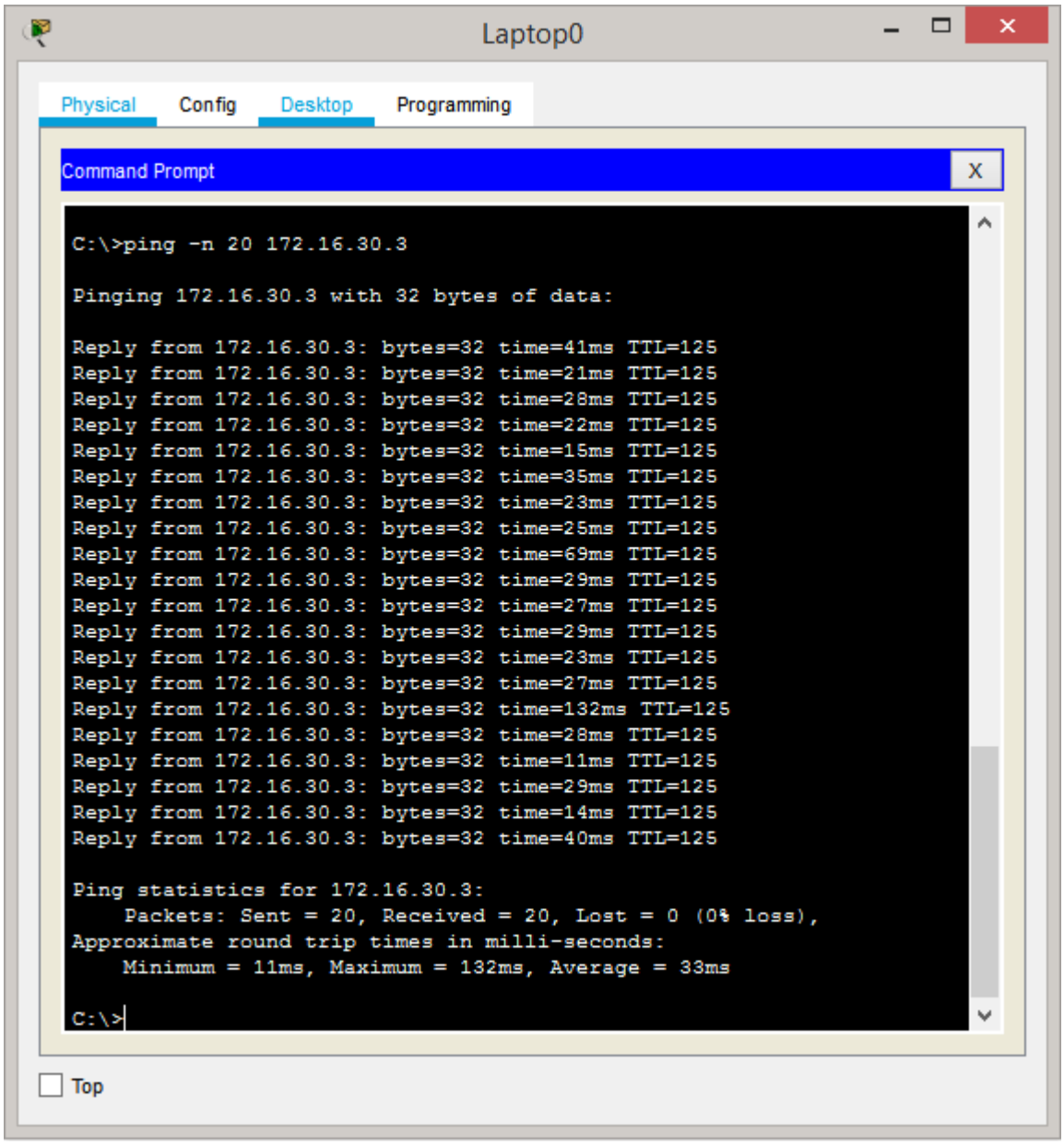
ANEXO 3 Prueba 1 en la Red IPv4



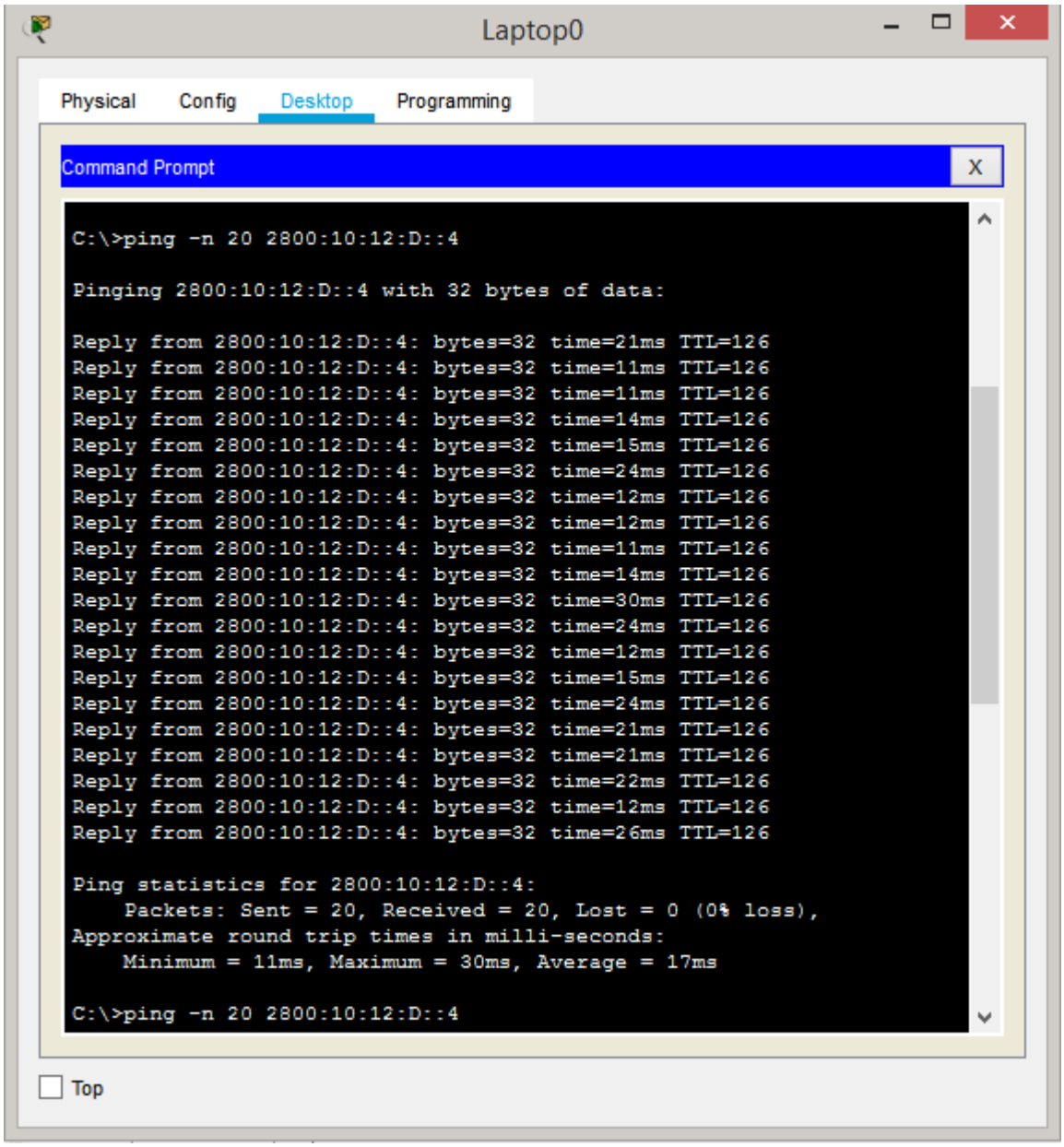
ANEXO 4 Prueba 1 en la Red IPv6



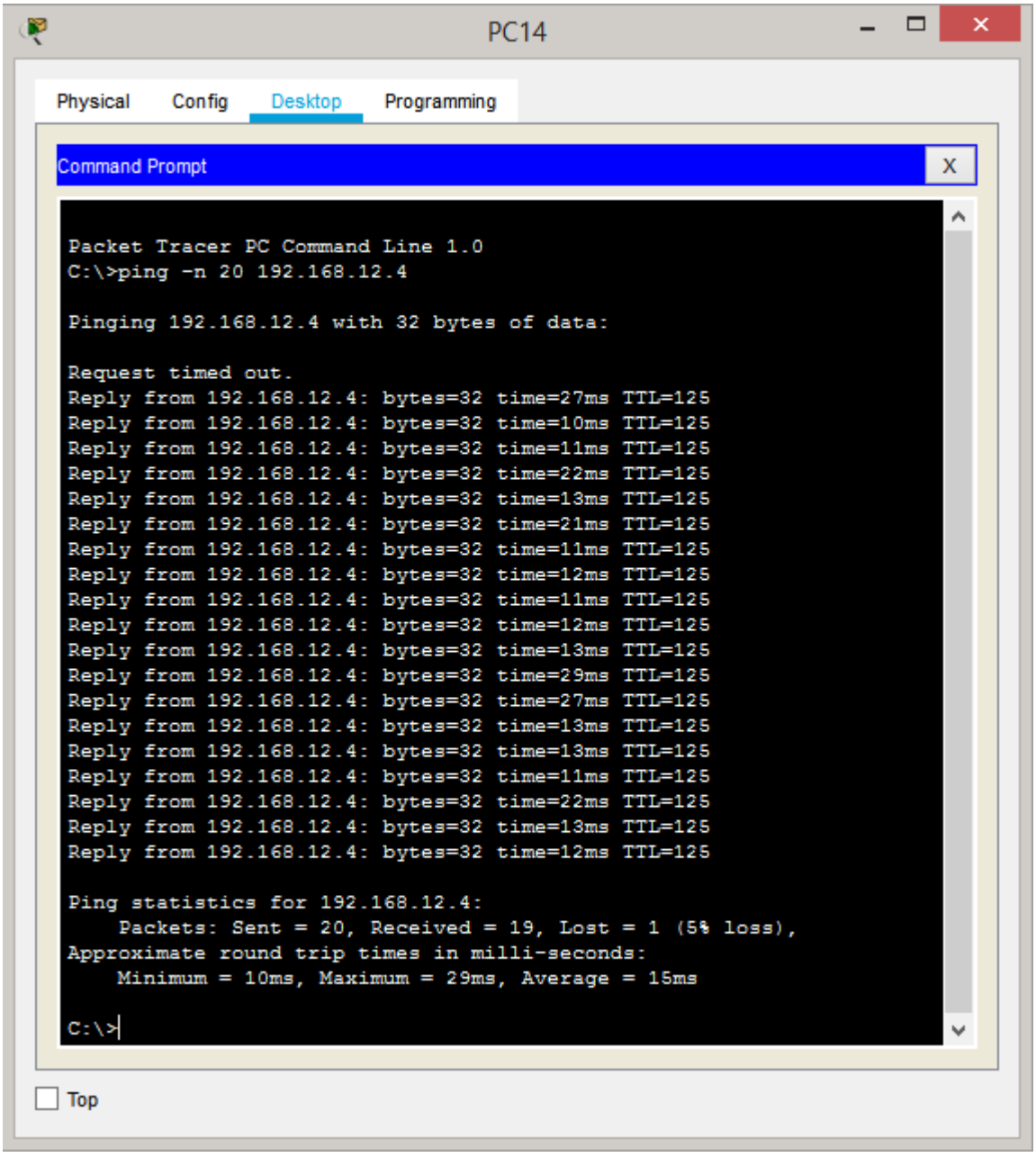
ANEXO 5 Prueba 2 en la Red IPv4



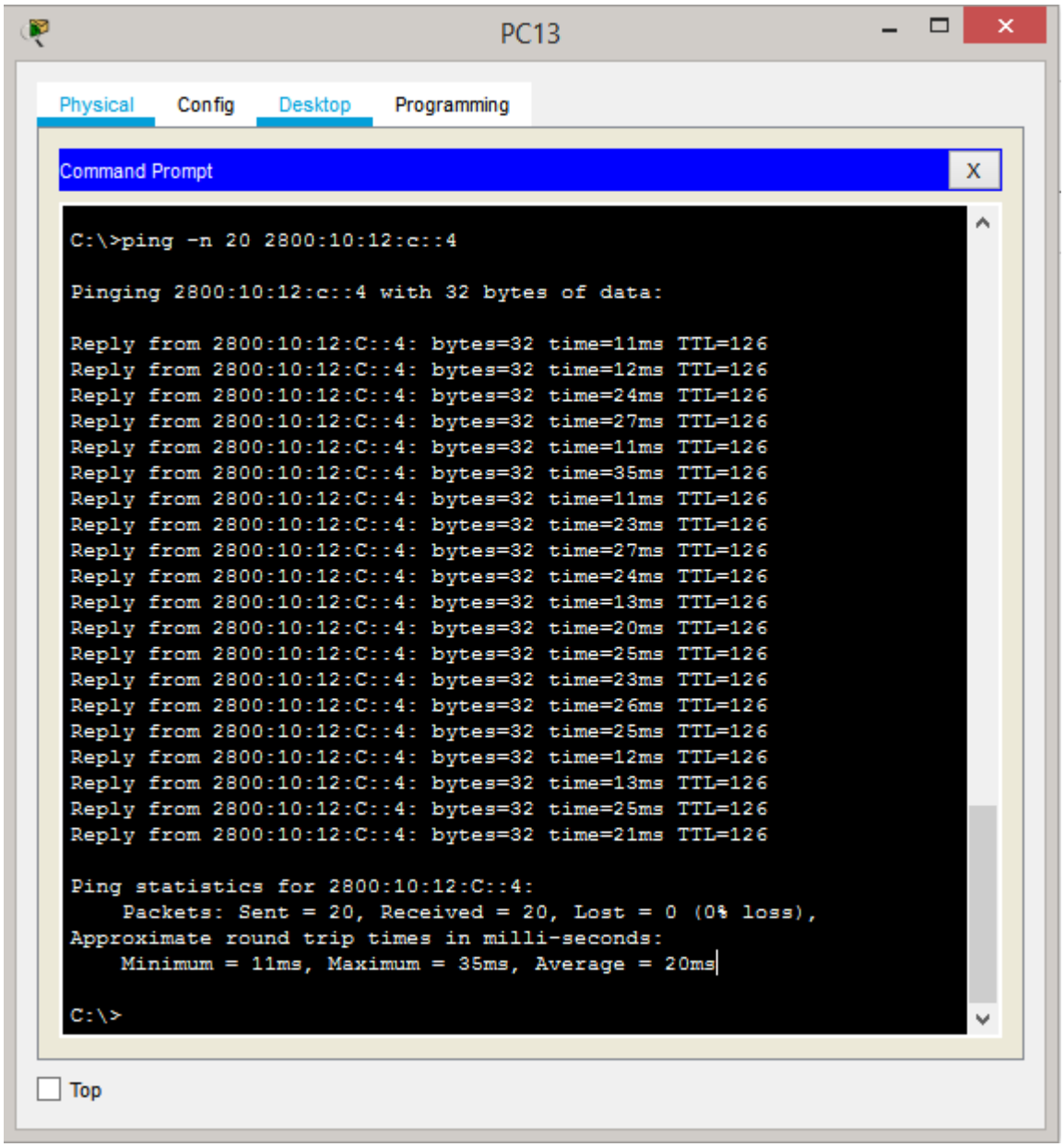
ANEXO 6 Prueba 2 en la Red IPv6



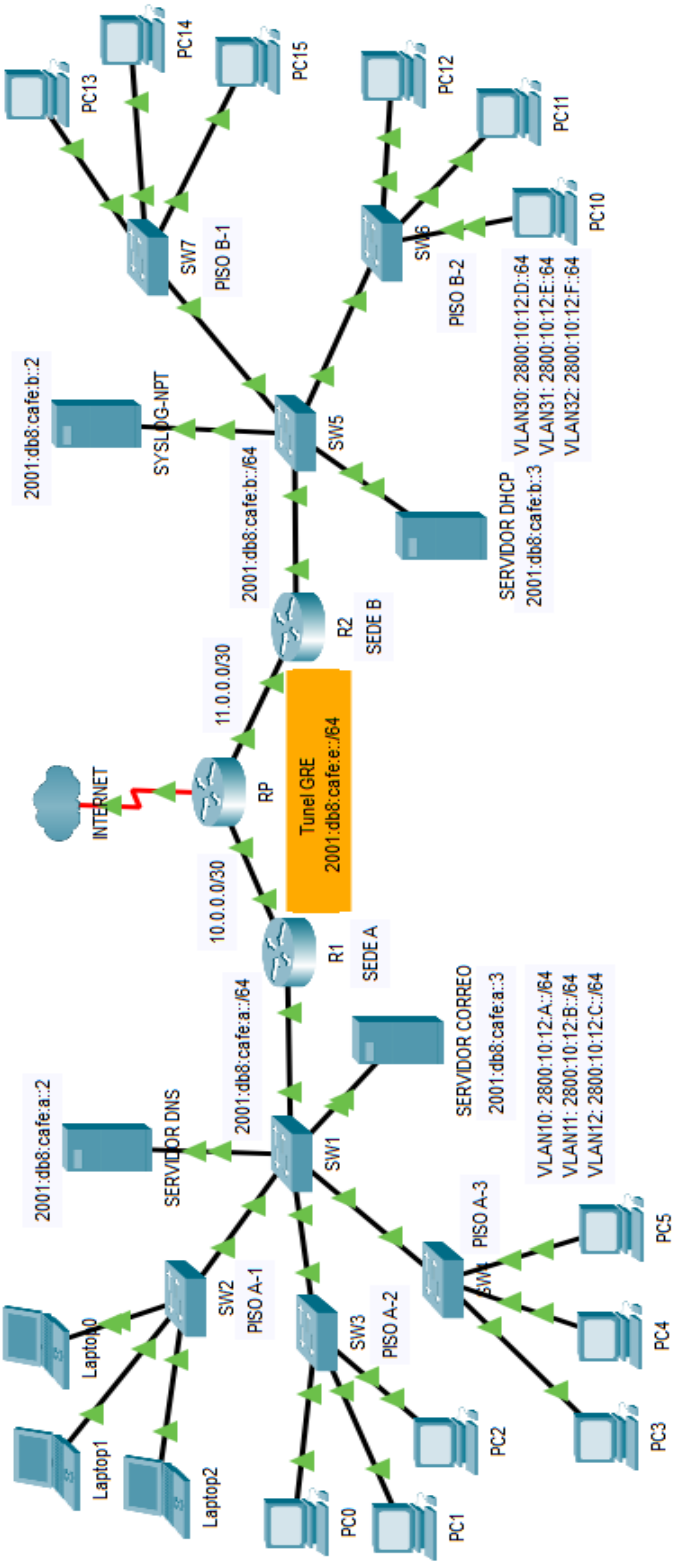
ANEXO 7 Prueba 3 en la Red IPv4



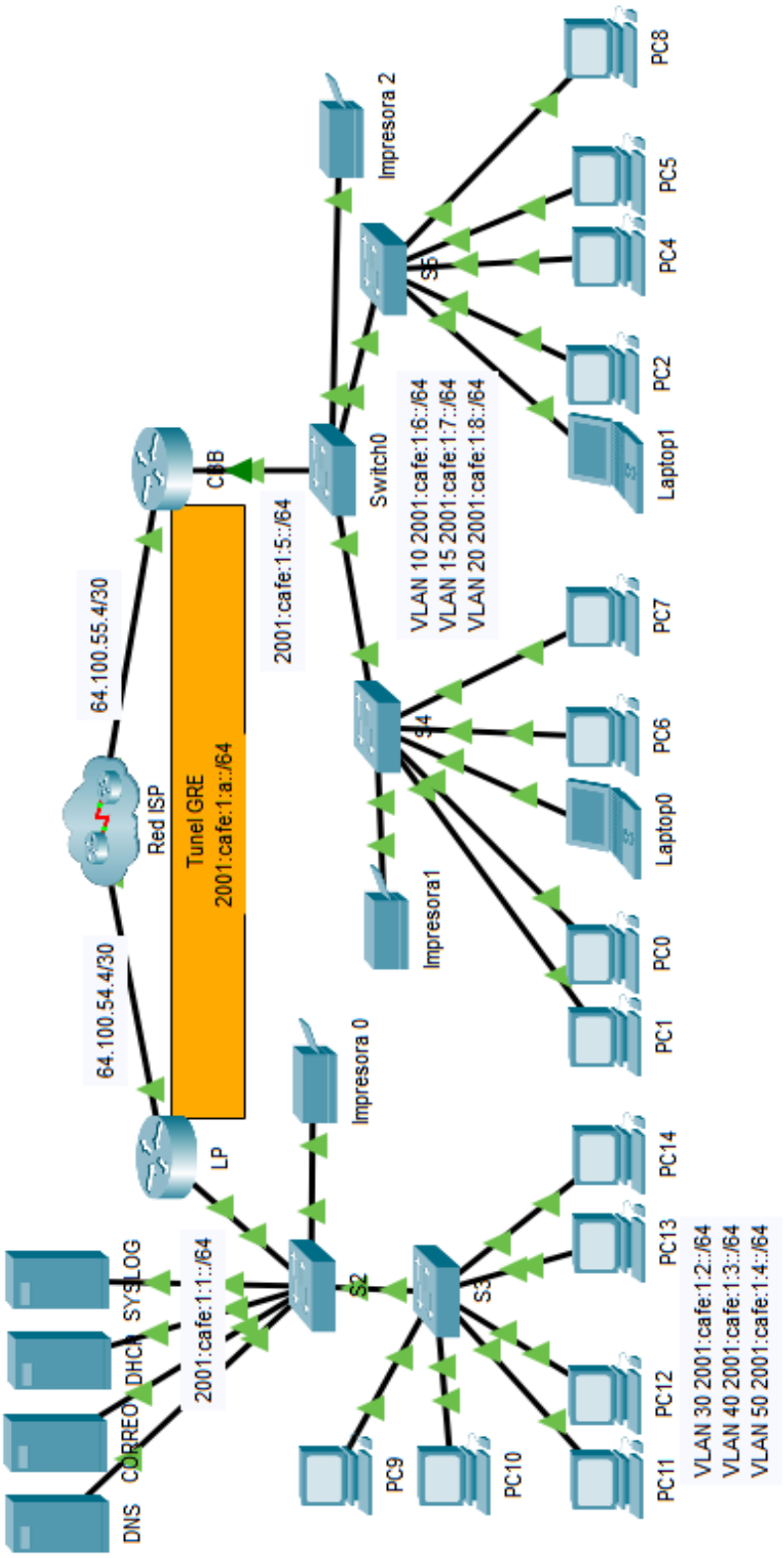
ANEXO 8 Prueba 3 en la Red IPv6



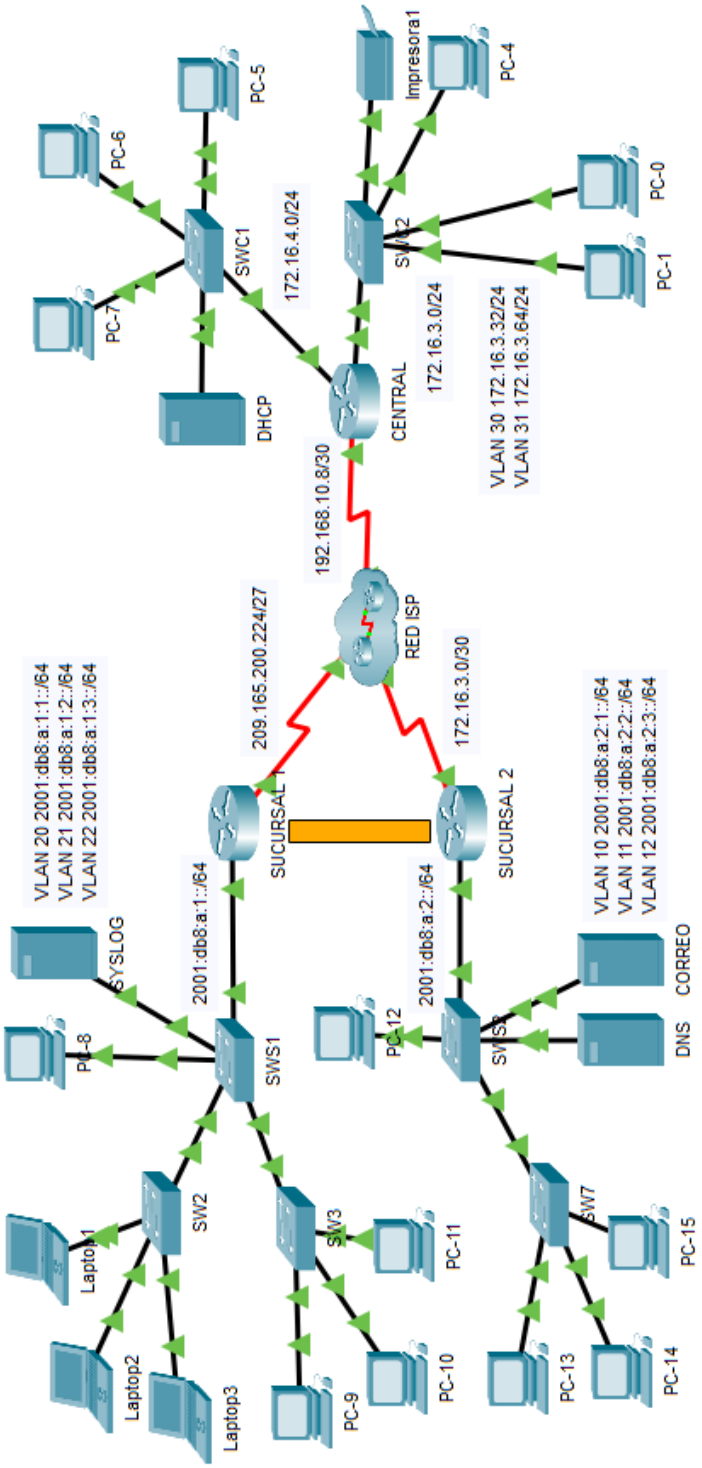
ANEXO 9 Topología de Red 1 implementada en el simulador



ANEXO 10 Topología de Red 2 implementada en el simulador



ANEXO 11 Topología de Red 3 implementada en el simulador



ANEXO 12 Direccionamiento de la Red 1

Dispositivo	Interfaz	Dirección IP	Puerta de enlace predeterminada
RP	S0/0/0	192.1.0.1/30	
	G0/0	10.0.0.1/30	
	G0/1	11.0.0.1/30	
R1	G0/0	10.0.0.2/30	
	G0/1	2001:DB8:CAFE:A::1/64	
	G0/1.10	2800:10:12:A::1/64	
	G0/1.11	2800:10:12:B::1/64	
	G0/1.12	2800:10:12:C::1/64	
	TUNNEL1	2800:10:12:E::1/64	
R2	G0/0	10.0.0.2/30	
	G0/1	2001:DB8:CAFE:B::1	
	G0/1.30	2800:10:12:D::1/64	
	G0/1.31	2800:10:12:F::1/64	
	G0/1.32	2800:10:12:G::1/64	
	TUNNEL1	2800:10:12:E::2/64	
Servidor Correo	NIC	2001:DB8:CAFE:A::2/64	2001:DB8:CAFE:A::1
Servidor DNS	NIC	2001:DB8:CAFE:A::3/64	2001:DB8:CAFE:A::1
SYSLOG-NPT	NIC	2001:DB8:CAFE:B::2/64	2001:DB8:CAFE:B::1
Servidor DHCP	NIC	2001:DB8:CAFE:B::3/64	2001:DB8:CAFE:B::1
Laptop0	NIC	2800:10:12:A::2/64	2800:10:12:A::1/64
PC0	NIC	2800:10:12:A::3/64	2800:10:12:A::1/64

PC3	NIC	2800:10:12:A::4/64	2800:10:12:A::1/64
Laptop1	NIC	2800:10:12:B::2/64	2800:10:12:B::1/64
PC1	NIC	2800:10:12:B::3/64	2800:10:12:B::1/64
PC4	NIC	2800:10:12:B::4/64	2800:10:12:B::1/64
Laptop2	NIC	2800:10:12:C::2/64	2800:10:12:C::1/64
PC2	NIC	2800:10:12:C::3/64	2800:10:12:C::1/64
PC5	NIC	2800:10:12:C::4/64	2800:10:12:C::1/64
PC12	NIC	2800:10:12:D::4/64	2800:10:12:D::1/64
PC13	NIC	2800:10:12:D::3/64	2800:10:12:D::1/64
PC11	NIC	2800:10:12:E::4/64	2800:10:12:E::1/64
PC14	NIC	2800:10:12:E::3/64	2800:10:12:E::1/64
PC10	NIC	2800:10:12:F::4/64	2800:10:12:F::1/64
PC15	NIC	2800:10:12:F::3/64	2800:10:12:F::1/64

ANEXO 13 Direccionamiento de la Red 2

Dispositivo	Interfaz	Dirección IP	Puerta de enlace predeterminada
R1	G0/0	2001:CAFE:1:1::1/64	
	G0/1	64.100.54.6/30	
	G0/0.30	2001:CAFE:1:2::1/64	
	G0/0.40	2001:CAFE:1:3::1/64	
	G0/0.50	2001:CAFE:1:4::1/64	
	TUNNEL0	2001:CAFE:1:A::1/64	
R2	G0/0	2001:CAFE:1:5::1/64	
	G0/2	64.100.55.6/30	
	G0/0.10	2001:CAFE:1:6::1/64	
	G0/0.15	2001:CAFE:1:7::1/64	
	G0/0.20	2001:CAFE:1:8::1/64	
	TUNNEL1	2001:CAFE:1:A::2/64	
Servidor Correo	NIC	2001:CAFE:1:1::2/64	2001:CAFE:1:1::1
Servidor DNS	NIC	2001:CAFE:1:1::3/64	2001:CAFE:1:1::1
SYSLOG-NPT	NIC	2001:CAFE:1:1::4/64	2001:CAFE:1:1::1
Servidor DHCP	NIC	2001:CAFE:1:1::5/64	2001:CAFE:1:1::1
Impresora0	NIC	2001:CAFE:1:1::6/64	2001:CAFE:1:1::1
PC9	NIC	2001:CAFE:1:2::2/64	2001:CAFE:1:2::1
PC10	NIC	2001:CAFE:1:2::3/64	2001:CAFE:1:2::1
PC11	NIC	2001:CAFE:1:3::2/64	2001:CAFE:1:3::1
PC12	NIC	2001:CAFE:1:3::3/64	2001:CAFE:1:3::1
PC13	NIC	2001:CAFE:1:4::2/64	2001:CAFE:1:4::1

PC14	NIC	2001:CAFE:1:4::3/64	2001:CAFE:1:4::1
Impresora1	NIC	2001:CAFE:1:5::2/64	2001:CAFE:1:5::1
Impresora2	NIC	2001:CAFE:1:5::5/64	2001:CAFE:1:5::1
PC1	NIC	2001:CAFE:1:6::2/64	2001:CAFE:1:6::1
PC0	NIC	2001:CAFE:1:6::3/64	2001:CAFE:1:6::1
Laptop1	NIC	2001:CAFE:1:6::4/64	2001:CAFE:1:6::1
PC2	NIC	2001:CAFE:1:6::5/64	2001:CAFE:1:6::1
Laptop0	NIC	2001:CAFE:1:7::2/64	2001:CAFE:1:7::1
PC6	NIC	2001:CAFE:1:7::3/64	2001:CAFE:1:7::1
PC4	NIC	2001:CAFE:1:7::4/64	2001:CAFE:1:7::1
PC5	NIC	2001:CAFE:1:7::5/64	2001:CAFE:1:7::1
PC7	NIC	2001:CAFE:1:8::2/64	2001:CAFE:1:8::1
PC8	NIC	2001:CAFE:1:8::3/64	2001:CAFE:1:8::1

ANEXO 14 Direccionamiento de la Red 3

Dispositivo	Interfaz	Dirección IP	Puerta de enlace predeterminada
R-1	S0/0/1	192.168.10.10/30	
	G0/0	172.16.4.1/24	
	G0/1	172.16.2.1/24	
	G0/0.30	172.16.2.33/27	
	G0/0.31	172.16.2.65/27	
R-2	S0/1/0	209.165.200.225/27	
	G0/1	2001:DB8:A:1::1/64	
	G0/0.20	2001:DB8:A:1:1::1/64	
	G0/0.21	2001:DB8:A:1:2::1/64	
	G0/0.22	2001:DB8:A:1:3::1/64	
	TUNNEL0	2001:DB8:B:1::1/64	
R-3	S0/0/0	172.16.3.1/30	
	G0/0	2001:DB8:A:2::1/64	
	G0/0.10	2001:DB8:A:2:1::1/64	
	G0/0.11	2001:DB8:A:2:2::1/64	
	G0/0.12	2001:DB8:A:2:3::1/64	
	TUNNEL1	2001:DB8:B:1::2/64	
Servidor Correo	NIC	2001:DB8:A:2::2/64	2001:DB8:A:2::1
Servidor DNS	NIC	2001:DB8:A:2::3/64	2001:DB8:A:2::1
SYSLOG-NPT	NIC	2001:DB8:A:1::2/64	2001:DB8:A:1::1
Servidor DHCP	NIC	172.16.4.2/24	172.16.4.1

PC-7	NIC	172.16.4.3/24	172.16.4.1
PC-6	NIC	172.16.4.4/24	172.16.4.1
PC-5	NIC	172.16.4.5/24	172.16.4.1
Impresora1	NIC	172.16.2.34/27	172.16.2.33
PC-4	NIC	172.16.2.35/27	172.16.2.33
PC-0	NIC	172.16.2.66/27	172.16.2.65
PC-1	NIC	172.16.2.67/27	172.16.2.65
PC-8	NIC	2001:DB8:A:1::3/64	2001:DB8:A:1::1
Laptop1	NIC	2001:DB8:A:1:1::2/64	2001:DB8:A:1:1::1
Laptop2	NIC	2001:DB8:A:1:2::2/64	2001:DB8:A:1:2::1
Laptop3	NIC	2001:DB8:A:1:3::2/64	2001:DB8:A:1:3::1
PC-9	NIC	2001:DB8:A:1:1::3/64	2001:DB8:A:1:1::1
PC-10	NIC	2001:DB8:A:1:2::3/64	2001:DB8:A:1:2::1
PC-11	NIC	2001:DB8:A:1:3::3/64	2001:DB8:A:1:3::1
PC-13	NIC	2001:DB8:A:2:1::2/64	2001:DB8:A:2:1::1
PC-14	NIC	2001:DB8:A:2:2::2/64	2001:DB8:A:2:2::1
PC-15	NIC	2001:DB8:A:2:3::2/64	2001:DB8:A:2:3::1
PC-12	NIC	2001:DB8:A:2::4/64	2001:DB8:A:2::1