UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS COMPARATIVO DE LOS MECANISMOS DE TÚNELES PARA LA TRANSICIÓN DE IPV4 A IPV6.

TORRES PAZ JEAN PAUL
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

ANÁLISIS COMPARATIVO DE LOS MECANISMOS DE TÚNELES PARA LA TRANSICIÓN DE IPV4 A IPV6.

TORRES PAZ JEAN PAUL
INGENIERO DE SISTEMAS

MACHALA
2022

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

ANÁLISIS COMPARATIVO DE LOS MECANISMOS DE TÚNELES PARA LA TRANSICIÓN DE IPV4 A IPV6.

TORRES PAZ JEAN PAUL
INGENIERO DE SISTEMAS

MOROCHO ROMAN RODRIGO FERNANDO

MACHALA, 24 DE FEBRERO DE 2022

MACHALA
2022

Titulación_TorresJean_20220220

INFORME DE ORIGINALIDAD

0%	0%	0%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1%

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado		

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, TORRES PAZ JEAN PAUL, en calidad de autor del siguiente trabajo escrito titulado ANÁLISIS COMPARATIVO DE LOS MECANISMOS DE TÚNELES PARA LA TRANSICIÓN DE IPV4 A IPV6., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 24 de febrero de 2022

TORRES PAZ JEAN PAUL
0705314656

DEDICATORIA

El presente trabajo se lo dedico en primer lugar a Dios por guiarme y darme fuerza y sabiduría para seguir adelante, a mis amados padres por haberme inculcado buenos valores, por haberme forjado como la persona que soy hoy en día, por motivarme y ayudarme a superarme día tras día y en general a mi familia que, aunque existan diferencias de pensamientos han estado conmigo impulsándome a seguir adelante y cumplir esta meta.

Jean Paul Torres Paz

AGRADECIMIENTO

En mi primer lugar, quiero agradecerle a Dios por haberme dado salud, vida, fortaleza para seguir adelante y seguir cumpliendo mis metas fijadas, por las bendiciones derramadas hacia mí y mi familia y por nunca abandonarme en los momentos más difíciles.

A mi madre Sra. Marlene Paz, por haberme dado la vida, por haberme forjado como el hombre que soy hoy en día e inculcarme los mejores valores éticos y morales, por cuidarme y siempre estar pendiente de mí y darme su apoyo hasta el último suspiro de su vida.

A mi padre Sr. Luis Torres, por haberme dado la vida, por su amor y apoyo incondicional en cualquier decisión que he tomado, por haberme enseñado a ser humilde y responsable, por ser siempre ese pilar fundamental y motivarme a seguir adelante a pesar de los obstáculos que se atraviesen.

Gracias padres, por todo el esfuerzo que suscitó el haberme criado para convertirme en el hombre profesional que tanto anhelaban, ustedes han sido los principales promotores de que esta meta se cumpla, sin ustedes nada de esto sería posible, los amo.

A la Ing. Yaritza Chamorro compañera de vida, amiga y consejera quien ha estado ahí en los buenos y malos momentos. Gracias por confiar en mí y darme esas fuerzas necesarias para seguir adelante.

A mi tutor Ing. Rodrigo Morocho, por haber dedicado su tiempo, paciencia y orientación, siendo guía fundamental para culminar este proceso con éxito. Es una persona admirable, además de su gran calidad humana y profesional.

A los docentes de la carrera, que contribuyeron en mi desarrollado profesional y académico durante estos años de estudio.

A la Universidad Técnica de Machala, por haberme brindado la oportunidad de ser un profesional y por abrirme las puertas a la sabiduría y educación.

Quedo eternamente agradecido con cada uno de ustedes… ¡Muchas bendiciones!

Jean Paul Torres Paz

RESUMEN

En la comunicación por internet, el protocolo IPv4 ha sido ampliamente utilizado hasta el punto de haber agotado ya sus direcciones según las estadísticas de LACNIC, es por eso que se ha desarrollado el protocolo IPv6, el cual ofrece una interacción con la arquitectura TCP/IP y permite la coexistencia con el protocolo IPv4, este nuevo protocolo permite el crecimiento de la internet de nueva generación de forma exponencial ya que proporciona muchas direcciones IP, las mismas que serán capaces de soportar todos los dispositivos que existen hoy en día y de los próximos años, lo cual daría solución a la problemática generada por el incremento del uso de internet. Hace varios años se ha venido planteando la posibilidad de emigrar de IPv4 a IPv6, pero no se ha logrado dicho objetivo, por tal motivo diferentes entidades se propusieron la idea de que, si un individuo no posee acceso al protocolo IPv6 nativo, éste tuviera la posibilidad de poder conectarse mediante la ayuda de algún mecanismo de transición de IPv4 a IPv6, tales como Dual Stack (Pilas Dobles), Traducción de Protocolo o Túneles. Los túneles proporcionan un encapsulamiento de paquetes IP sean version 4 o 6 para finalmente enviar estos paquetes a un nodo destino. Este proyecto se enfoca en los mecanismos de transición de IPv4 a IPv6 mediante la tunelización, es por ello que se desarrollará un análisis comparativo entre tres mecanismos de túneles, 6to4, 6over4 y GRE (Generic Routing Encapsulation), utilizando un emulador gráfico de red para entender su funcionamiento y rendimiento mediante pruebas experimentales. Para el desarrollo del proyecto se llevó a cabo las siguientes fases: identificación de la problemática, la necesidad de la coexistencia entre IPv4 e IPv6 mediante el uso de los mecanismos de túneles los cuales permiten que exista la compatibilidad de los hosts y redes IPv6 en redes IPv4 existentes y viceversa en algunos casos, búsqueda y recolección de información verídica de revistas científicas, libros y sitios de internet especializados para establecer características, ventajas y desventajas teniendo en cuenta los aspectos más relevantes de estos túneles, análisis de la información recabada de cada uno de los mecanismos de túneles mediante lectura compresiva, selección de túneles según la información obtenida para la realización de la comparativa, diseño y esquema de direccionamiento IP en sus dos versiones para la topología de acuerdo a los requerimientos de cada uno de los túneles, identificación y selección de equipos o herramientas que permitan la correcta emulación de los túneles y que también sean compatibles con los protocolos utilizados, configuración de los equipos en GNS3, obtención de resultados de las pruebas realizadas respecto de la conectividad entre dispositivos y tiempos de espera,

comparativa de los resultados adquiridos, a través del envío de paquetes ICMPv6, conclusiones acerca de cuál es el túnel más óptimo ya sea por su conectividad o características generales, el mismo que se podrá implementar en una infraestructura de red sin afecte el de la misma, y por último, recomendaciones sobre las mejoras o futuros estudios que se pueden realizar en base al proyecto desarrollado.

Palabras Claves: IPv4, IPv6, 6to4, 6over4, GRE.

ABSTRACT

In Internet communication, the IPv4 protocol has been widely used to the point of having already exhausted its addresses according to LACNIC statistics, that is why the IPv6 protocol has been developed, which offers an interaction with the TCP/IP architecture and allows the coexistence with the IPv4 protocol, This new protocol allows for the exponential growth of the new generation Internet, since it provides many IP addresses, which will be able to support all the devices that exist today and in the coming years, which would provide a solution to the problems generated by the increase in Internet use. For several years the possibility of migrating from IPv4 to IPv6 has been considered, but this objective has not been achieved. For this reason, different entities have proposed the idea that, if an individual does not have access to the native IPv6 protocol, it would be possible to connect with the help of some mechanism for transition from IPv4 to IPv6, such as Dual Stack, Protocol Translation or Tunnels. Tunnels provide an encapsulation of IP packets either version 4 or 6 to finally send these packets to a destination node. This project focuses on the transition mechanisms from IPv4 to IPv6 through tunneling, therefore a comparative analysis between three tunneling mechanisms, 6to4, 6over4 and GRE (Generic Routing Encapsulation) will be developed, using a graphical network simulator to understand their operation and performance through experimental tests. The following phases were carried out for the development of the project: Identification of the problem, the need for coexistence between IPv4 and IPv6 through the use of tunnel mechanisms that allow the compatibility of IPv6 hosts and networks in existing IPv4 networks and vice versa in some cases, search and collection of accurate information from scientific journals, books and specialized Internet sites to establish characteristics, analysis of the information gathered on each of the tunnel mechanisms through compressive reading, selection of tunnels according to the information obtained to carry out the comparison, design and IP addressing scheme in its two versions for the topology according to the requirements of each of the tunnels, identification and selection of equipment or tools that allow the correct emulation of the tunnels and that are also compatible with the protocols used, configuration of the equipment in GNS3, obtaining the results of the tests performed with respect to connectivity between devices and waiting times, comparison of the results acquired, Finally, the results obtained through the sending of ICMPv6 packets, conclusions about which is the most optimal tunnel either for its connectivity or general characteristics, the same that can be implemented in a network

infrastructure without affecting it, and finally, recommendations on improvements or future studies that can be carried out based on the project developed.

Keywords: IPv4, IPv6, 6to4, 6over4, GRE.

CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad el internet se ha convertido en parte primordial para la población, la forma de conectividad en el mundo se encuentra alcanzando sus límites lo cual ha sido provocado por la enorme cantidad de dispositivos como celulares, cámaras de vigilancia, computadoras, dispositivos inalámbricos, razón por la cual la versión actual del protocolo de internet (IPv4) ha llegado a sus límites en cuanto al reparto de direcciones.

El protocolo IPv6 presenta la solución a este problema de límite de direcciones que tiene el protocolo IPv4, para lo cual el protocolo IPv6 consta de millones de direcciones disponibles que difícilmente podrían llegar a usarse todas, con esto no se trata de reemplazar las direcciones IPv4 por las direcciones IPv6, sino más bien permitir que estos dos protocolos convivan dentro de un mismo dispositivo al mismo tiempo o de forma independiente.

Existe un amplio cúmulo de técnicas o mecanismos que han sido identificadas e implementadas para la coexistencia o transición de IPv4 a IPv6, una de las más importantes son los mecanismos de túneles. Los mecanismos de túneles permiten la coexistencia de ambos protocolos como son IPv4 e IPv6, mediante una técnica de integración y transición media entre nodos para trasmitir paquetes de datos.

De aquí la necesidad de estudiar y conocer la importancia de los mecanismos de túneles para la transición de IPv4 a IPv6, debido a la gran demanda de trasmisión de datos, a través de topologías con diferentes tipos de protocolos, lo cual prioriza el estudio de éstos para saber cómo funcionan dentro de la topología, permitiendo además realizar las pruebas pertinentes. Para así de esta manera notar si cumple con los objetivos planteados a la hora de seleccionar uno de estos mecanismos de túneles.

Es por eso, que el objetivo de este proyecto es realizar un análisis comparativo, mediante la emulación de los mecanismos de túneles para la transición de IPv4 a IPv6, llegando así a facilitar la información necesaria para dar a conocer el rendimiento, funcionamiento de los mecanismos de túneles en relación a sus tiempos de respuestas en determinados escenarios.

La estructura del documento está detallada de la siguiente manera:

Capítulo 1, presenta la necesidad de la elaboración de un análisis comparativo describiendo el ámbito de la aplicación, el establecimiento y la justificación de los requerimientos.

Capítulo 2, especifica el desarrollo del proyecto, donde se describe el diseño de la topología, fundamentación teórica, objetivos (generales y específicos), diseño y ejecución de la topología.

Capítulo 3, detalla la evaluación de la topología de red, donde exponemos el plan y la evaluación de los resultados, así mismo como las conclusiones y recomendaciones que se obtuvieron a partir de la propuesta planteada.

1. CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1. ÁMBITO DE APLICACIÓN: DESCRIPCIÓN DEL CONTEXTO Y HECHO DE INTERÉS

Debido al gran crecimiento que existe en cuanto al uso de la tecnología en el mundo, esto trae consigo mismo el uso de la red de internet, en la actualidad se utiliza el protocolo IPv4 e IPv6 para el funcionamiento de la internet, pero en el protocolo IPv4 existe un gran problema que es el agotamiento de las direcciones IP, ya que este protocolo consta de direcciones IP de 32 bits, dicho número de direcciones se han convertido en una limitante debido al gran crecimiento del uso de la internet.

Actualmente ya no existen direcciones IP para América Latina y el Caribe según LACNIC, es por eso que para poder llegar a una solución a este problema del agotamiento de las direcciones, se busca una transición al protocolo IPv6, el cual cuenta con direcciones IP de 128 bits lo cual resolverá el crecimiento continuo de la internet.

Hoy en día existen diversos mecanismos de transición de IPv4 a IPv6, para este trabajo se ha considerado a los mecanismos de túneles, los cuales utilizan técnicas que encapsulan paquetes IPv6 en paquetes IPv4, estos túneles pueden ser de dos maneras ya sean unidireccionales cuando el flujo de paquetes de túnel toma lugar en una dirección entre el nodo de entrada y el nodo de salida del túnel, o pueden ser bidireccionales las cuales se pueden obtener mediante la fusión de dos túneles unidireccionales, cada uno opuesto al otro. Una vez que nuestra topología se encuentre diseñada y configurada en el emulador GNS3, en base a la información consultada a partir de distintas fuentes, se procederá a realizar las pruebas pertinentes para la obtención de resultados.

El alcance de este proyecto es presentar, comprobar el rendimiento y funcionamiento de los mecanismos de túneles para la transición de IPv4 a IPv6 seleccionados mediante un análisis comparativo.

1.2. ESTABLECIMIENTO DE REQUERIMIENTOS

Para el diseño y configuración de las topologías de red para los mecanismos de túneles es necesario tener en cuenta algunos parámetros, los cuáles van a ser desarrollados y realizando las pruebas pertinentes para obtener el resultado más eficiente.

Este proyecto se encuentra estructurado de la siguiente manera:

- Recolección de información, ésta se considera la primera fase, en la cual se realizará un estudio en base a los mecanismos de túneles para la transición de IPv4 a IPv6 que se van a analizar, comparar y emular.
- Diseño de la topología de red, en el emulador GNS3, una herramienta de emulación, simulación, virtualización que facilita el diseño de redes y permite experimentar el comportamiento de las redes.
- Selección de los dispositivos de conmutación (Switch - Ethernet Switch), enrutamiento (Routers – Cisco 7200), dispositivos finales (Hosts - VPCS) y agregación de los enlaces con sus respectivas interfaces.
- Asignación del direccionamiento IPv4 e IPv6, tales como nombres de los dispositivos de la red para identificarlos de mejor manera y las puertas de enlace.
- Configuración de los protocolos de enrutamiento OSPFv2 u OSPFv3 según el caso, en cada uno de los routers, que permitirán la comunicación entre ellos y los dispositivos finales.
- Pruebas, una vez que se haya concluido las configuraciones y cada uno de los puntos anteriores se procede a hacer las pruebas respectivas para realizar el análisis comparativo sobre los tres mecanismos de túneles e informando cual es el recomendable para aplicar en una infraestructura de red.

1.3. JUSTIFICACIÓN DEL REQUERIMIENTO A SATISFACER

Este proyecto tiene su enfoque en el Dominio: Tecnologías de la información y la comunicación, y en la línea de investigación: Gobierno y Gestión de las Tecnologías de la Información (TI) establecido por la Universidad Técnica de Machala (UTMACH).

En el mundo tecnológico existen un sinnúmero de dispositivos que utilizan direcciones IPv4, así que pensar en una migración simultánea de IPv4 a IPv6 de cada uno de estos dispositivos es inasequible, debido a que los dispositivos o el software no permiten o no son compatibles con direcciones IPv6, es por eso que se han desarrollado diferentes mecanismos de transición de IPv4 a IPv6 entre ellos los Mecanismos de Túneles los cuales permiten la coexistencia de IPv4 e IPv6.

El objetivo principal de la presente propuesta es el análisis comparativo de los mecanismos de túneles para la transición de IPv4 a IPv6, usando el emulador GNS3, permitiendo de esta manera comprobar la eficiencia, carga administrativa, facilidad de configuración, impacto sobre la red de cada uno de los mecanismos de túneles analizados.

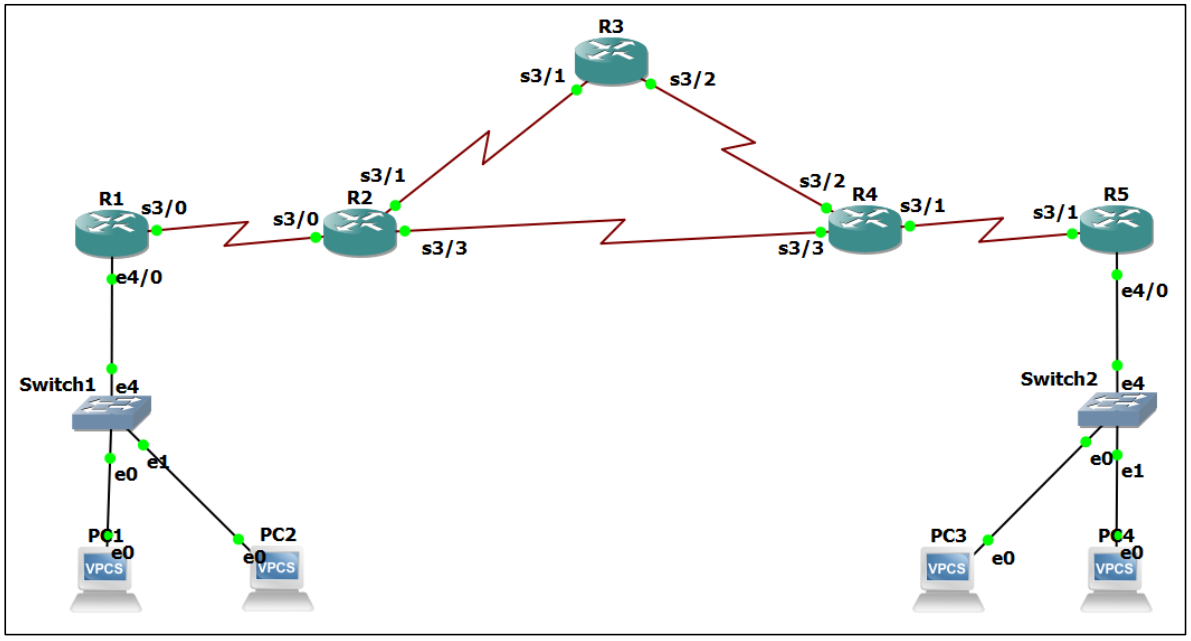
La topología diseñada y configurada con los mecanismos de túneles antes mencionados, permitirán establecer diferencias, similitudes, ventajas y desventajas al hacer uso de estos mecanismos de túneles según sea conveniente, además es importante destacar que, dentro de esta propuesta, se está brindando información acerca del funcionamiento y rendimiento de cada mecanismo de túneles seleccionado en determinado escenario.

2. CAPÍTULO II. DESARROLLO DEL PROYECTO

2.1. DEFINICIÓN DE LA TOPOLOGÍA DE RED

En la presente Ilustración, se muestra la topología diseñada con equipos Cisco, la misma que está configurada en un escenario en el simulado GNS3, y será objeto de las configuraciones básicas de cada uno de los mecanismos de túneles. Se hizo uso de la misma topología para los tres túneles y así realizar la evaluación de mejor manera el funcionamiento de cada uno de ellos. Dentro de la topología se observa una red compuesta por un conjunto de 5 routers c7200-adventerprisek9-mz.152-4.M7.bin (R1, R2, R3, R4 y R5) compatibles con los protocolos IPv4 e IPv6, 2 switch (SW-1 y SW-2) para las conexiones Ethernet entre el router R1 y los hosts PC1 y PC2 y router R5 y los hosts PC3 y PC4, finalmente 4 dispositivos finales (host) que son equipos VPCS (PC1, PC2, PC3 y PC4) que se encuentran por defecto dentro del emulador.

Ilustración 1: *Definición de la topología de red para los mecanismos de túneles.*



2.2. FUNDAMENTACIÓN TEÓRICA DE LA TOPOLOGÍA DE RED

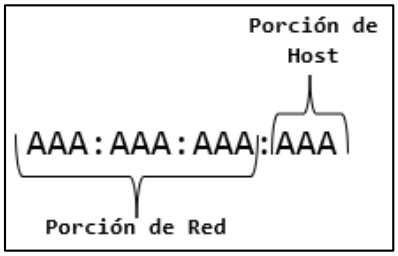
2.2.1. PROTOCOLO DE INTERNET VERSIÓN 4 (IPV4)

"Protocolo de Internet Versión 4, se encuentra compuesto por 32 bits; es una versión del protocolo de internet más utilizado a nivel mundial desde el año de 1981, encargado de direccionar y acceder a alrededor de 4.3 millones de dispositivos, debido al crecimiento de las nuevas tecnologías estos dispositivos

se han multiplicado, provocando el agotamiento de direccionesIPv4. Razón por la cual ha sido necesario migrar a un protocolo más amplio que garantice la conexión para nuevos usuarios."[1], [2]

En la ilustración 2, se puede observar la forma en la que se escribe una dirección IPv4, formada por cuatro campos de 8 bits separado por puntos cuya representación se da en números decimales.

Ilustración 2: *Formato básico de las direcciones IPv4*



2.2.1.1. CARACTERÍSTICAS DEL PROTOCOLO DE INTERNET IPV4

Entre las características de IPv4 se encuentran las siguientes:

- Posee tres clases de direcciones IP (Redes de clase A, B, C, D y E).
- No proporciona garantía en la entrega de datos.
- Espacio de direcciones IP limitadas.
- El valor mínimo para un octeto es de 0 y el mayor es 255.
- Fragmentación en los paquetes.
- Tamaño de la cabecera variable.

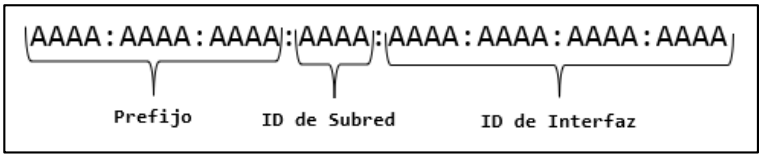
2.2.2. PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6)

"Protocolo de Internet Version 6 o conocido también como Protocolo de Internet de Próxima Generación (IPng), creado en el año de 1998 por Internet Engineering Task Force (IETF), nace para convertirse en el sucesor de IPv4 y de esta manera solucionar el agotamiento de direcciones ip, proporcionando así un suficiente espacio de direcciones para uso futuro. Con mejoras que permiten una mayor eficiencia de routers y una mayor seguridad, adaptándose a características de los nuevos servicios de telecomunicaciones." [3], [4]

"IPv6 posee un tamaño de 128 bits, el mismo que se encuentra conformado por 8 campos y cada uno de 16 bits, permitiendo así la coexistencia de alrededor de 340 billones de direcciones IP únicas para los nuevos dispositivos." [5]

En la ilustración 3, se puede observar la forma en la que deben ser escritas las direcciones IPv6, en donde cada letra "A" corresponde a un campo hexadecimal conformado por dígitos que van del 0 al 9 y de la A a la F respectivamente, separados por dos puntos.

Ilustración 3:*Formato básico de las direcciones IPv6*



2.2.2.1. CARACTERÍSTICAS DEL PROTOCOLO DE INTERNET IPV6

Entre las características que posee IPv6 se encuentran las siguientes: [6], [7]

- Mayor espacio de direcciones IP.
- Simplificación del formato del encabezado.
- Configuración automática de dispositivos.
- Posee mejoras con respecto a la seguridad.
- Capacidad de autenticación y privacidad.
- Reenvió de paquetes más rápido.

2.2.3. HERRAMIENTA GNS3

"GNS3 con sus siglas en inglés Graphical Network Simulator 3 fue lanzado en el año 2008, es un software de simulación de código abierto basado en Cisco, sin limitación del número de dispositivos que se utilizaran en el ambiente, imitando un escenario de red en tiempo real. GNS3 tiene asociado el analizador Wireshark para la captura y monitoreo de paquetes". [8], [9]

"Esta herramienta admite la emulación de los IOS de los dispositivos con interconectividad Cisco, puede ser instalada en entornos tales como: Linux, Windows y Mac. En cuanto a su licencia es de libre descarga, pero requiere de las imágenes de los dispositivos Cisco, mismas que pueden ser adquiridas directamente con el fabricante. GNS3 es una herramienta para el aprendizaje y

preparación de varias certificaciones como lo son: CCNA, CCNP y CCIE, posee una interfaz gráfica muy intuitiva para el usuario". [10], [11]

2.2.3.1. CARACTERÍSTICAS DE GNS3

Entre las características de GNS3, se encuentran las siguientes: [12], [13]

- Emulación y simulación de redes reales.
- Proporciona cortafuegos PIX, ASA, detención de intrusos, conmutadores frame relay.
- Compatible con una diversidad de dispositivos de red.
- Admite más comandos y parámetros en los dispositivos.
- Puede conectarse a dispositivos reales.

2.2.4. ROUTER

Un router o también llamada enrutador, permite establecer la conexión entre otros routers a través de protocolos de enrutamiento, y de esta manera puedan compartir información entre ellos, eligiendo la mejor ruta.

2.2.5. HOST

Un host son dispositivos intermediarios (computadores u otros dispositivos) que proporciona las interconexiones entre otros hosts dentro de una misma red, mediante un número IP definido y una puerta de enlace. El host funciona como el punto de inicio y final para la transferencia de información.

2.2.6. SWITCH

Un switch es un dispositivo que permite conectar diferentes dispositivos entre ellos, permitiendo de esta manera que los dispositivos conectados se comuniquen entre sí y compartan información. Usualmente se conecta a un router para para que exista el acceso a internet.

2.2.7. TOPOLOGÍAS DE RED

"Las topologías de red, son la forma en la que se encuentran conectados los dispositivos para intercambiar datos entre sí. Cada topología de red tiene una parte que representa la topología física que indica la configuración de los cables o dispositivos en la red, y otra parte que es la topología lógica que se refiere al flujo de información que se trasmite entre nodos." [14]

2.2.8. MECANISMOS DE TÚNELES

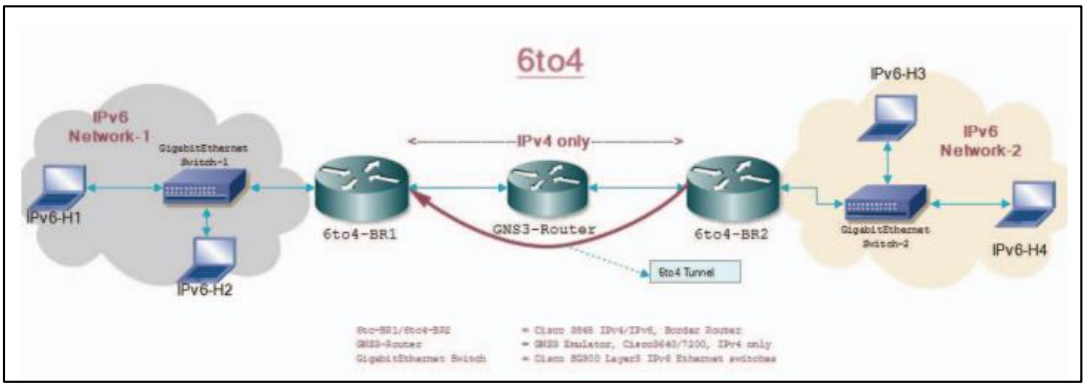
"La tunelización es una técnica para enviar paquetes IPv6 sobre una red IPv4 encapsulándolos para dirigirse a su punto de destino, esto se debe a que los encabezados de IPv4 e IPv6 son diferentes entre sí. Antes de que el paquete sea enviado tiene una ligera alteración es decir sufre una adición de un encabezado al túnel. Una vez que los paquetes han pasado por el túnel y han llegado a su destino, el encabezado se restaurará como al principio". [15]–[17]

2.2.8.1. TÚNEL 6TO4

"Es una tecnología en redes informáticas definido por RFC3056 que permite la comunicación entre sitios IPv6 sobre sitios IPv4, diseñado por IETF. Su característica principal es que son túneles generados dinámicamente, por lo que requieren configuración previa, su uso se da cuando los hosts habilitados para IPv6 son parte de una red solo IPv4". [18]–[20]

"Una desventaja de este modelo de túnel, es que no se puede elegir el servidor en el cual se desea ejecutar la tunelización. Su prefijo es 2002::/16". [21], [22]

Ilustración 4: *Arquitectura túnel 6to4*



Fuente: [23]

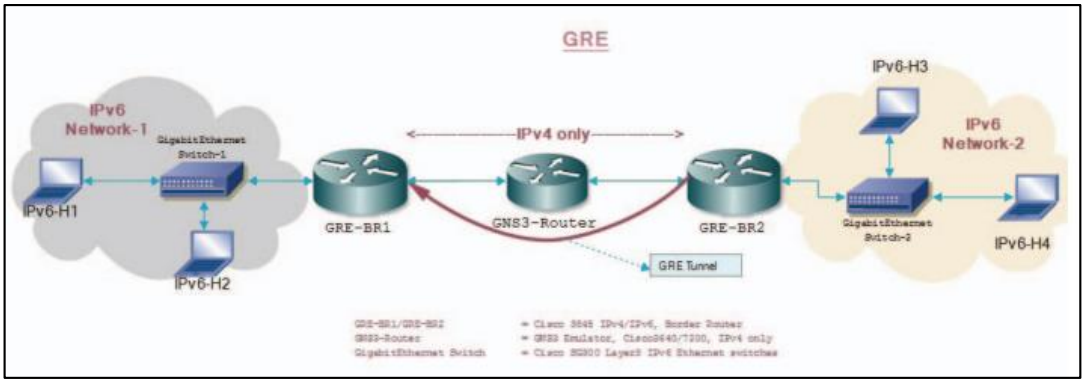
Tabla 1: Ventajas y Desventajas del túnel 6to4

Ventajas	Desventajas
• Se crean dinámicamente, no hace falta configurarlos. • El servicio no necesariamente deber ser proveído por el ISP (Internet Service Provider). • Mediante una sola dirección IPv4 publica se configura un túnel para varios host 6to4.	• Es muy difícil de controlar el tráfico que circula a través de él. • Se encuentra bajo el control de un tercero. • Vulnerable a ataques Dos y Spoofing. • Se requieren de direcciones IPv4.

2.2.8.2. TÚNEL GRE

"Generic Routing Encapsulation (GRE), es un túnel desarrollado originalmente por Cisco, permite encapsular la capa de red de protocolos mediante otros protocolos de capa de red, originalmente está definido en RFC1701 y RFC1702. El uso principal de este túnel es que proporciona conexión estable entre dos hosts o un host y un servidor, GRE puede encapsular multidifusión, difusión u otros tipos de tráfico no IP, suelen acoplarse a Internet Protocol Security (IPSec) para proporcionar seguridad de la red". [24], [25]

Ilustración 5: Arquitectura del túnel GRE



Fuente: [23]

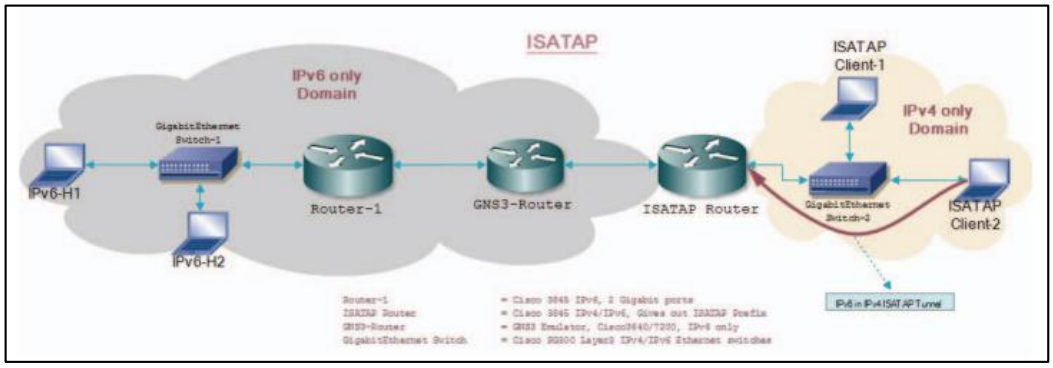
Tabla 2: Ventajas y Desventajas del túnel GRE

Ventajas	Desventajas
• Permiten conexiones entre redes IPv6 sobre IPv4. • Utilizado para canalizar el tráfico que no es IP a través de una red IP. • Admite la tunelización de multidifusión IP, permitiendo el uso de protocolos de enrutamiento a través del túnel.	• En una red de punto a multipunto, las redes de sucursales no pueden túneles y no pueden comunicarse.

2.2.8.3. TÚNEL ISATAP

"Intra-Site Automatic Tunnel Addressing Protocolo, este túnel es algo similar al túnel 6over4, pero no hace uso de la multidifusión, definido en la RFC5214 por la IETF. Permite desplegar IPv6 sobre una infraestructura IPv4 ya existente, insertando la dirección IPv4 de a interfaz en los últimos bits de la dirección IPv6. El ID de la interfaz se compone de ::5EFE:ab.b.c.d, donde a.b.c.d es la notación con pinto decimal de IPv4". [26]

Ilustración 6: Arquitectura del túnel ISATAP



Fuente: [23]

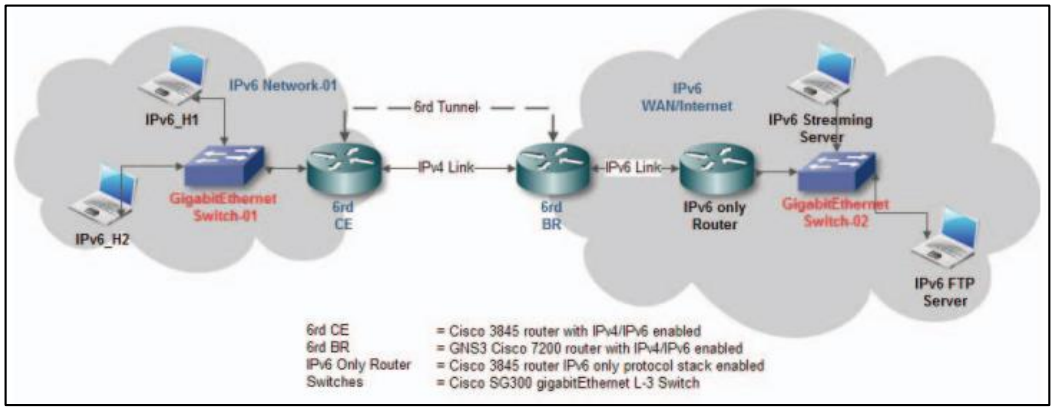
Tabla 3: Ventajas y Desventajas del túnel ISATAP

Ventajas	Desventajas
• Permiten conexiones entre redes IPv6 sobre IPv4. • Utilizado para canalizar el tráfico que no es IP a través de una red IP. • Admite la tunelización de multidifusión IP, permitiendo el uso de protocolos de enrutamiento a través del túnel.	• Problemas de seguridad en redes IPv4 e IPv6.

2.2.8.4. TÚNEL 6RD

"6 Rapid Deployment es una tecnología de tunelización derivado de 6to4. Han modificado el túnel 6to4 para crear un cis mejor mecanismo mediante la solución de los principales problemas arquitectónicos en 6to4 como el formato de direcciones. 6RD se implementa de una manera fácil sobre IPv4 sin ninguna agregación. Se encuentra estandarizado en el RFC5969 por la IETF y fue implementado por FREE". [23], [27]

Ilustración 7: Arquitectura del túnel 6RD



Fuente: [23]

Tabla 4: Ventajas y Desventajas del túnel 6RD

Ventajas	Desventajas
• Tiene control sobre el tráfico que transita a través de él. • Mejor control y disminuye el riesgo de ataques de Spoofing y DoS. • El relay 6to4 se encuentra dentro de la infraestructura del ISP. • El ISP es el encargado de todo el despliegue de 6rd.	• Es muy difícil de controlar el tráfico que circula a través de él. • Se encuentra bajo el control de un tercero.

2.2.8.5. TÚNEL 6IN4

"Unos de los métodos de tunelización más antiguos, fue desarrollado en el año de 1996 y reconocidos altamente hasta el día de hoy, se encuentra definido en el RFC 4213 por la IETF, utiliza el protocolo 41 y no trabaja mediante NAT, es compatible con todos los sistemas operativos modernos. Se encuentra diseñado para encapsular el tráfico IPv6 a través de enlaces IPv4 que hayan sido configurados manualmente, aunque este método es confiable y estable carece de la capacidad de convertirse en escalable". [28]

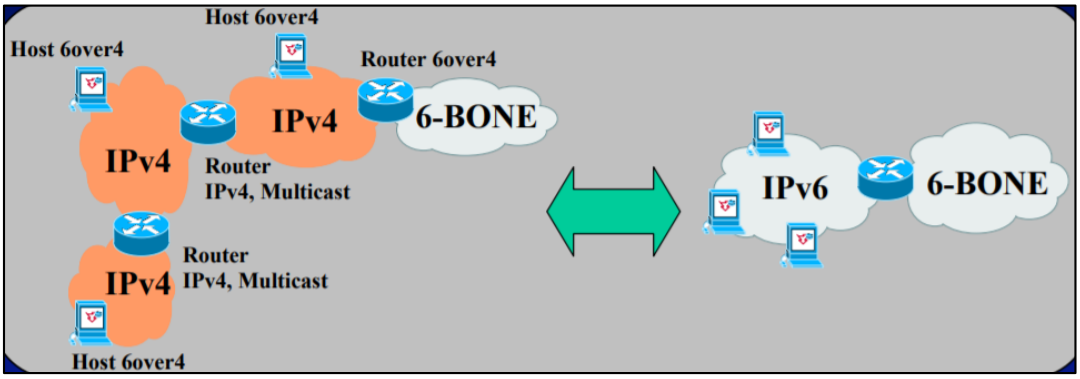
Tabla 5: Ventajas y Desventajas del túnel 6in4.

Ventajas	Desventajas
• Pueden ser configurados manualmente. • Permite encapsular paquetes IPv6 directamente dentro de paquetes IPv4. • Encapsulamiento simple.	• Solo realiza un salto IPv6, aunque existan varios IPv4.

2.2.8.6. TÚNEL 6OVER4

"Es un mecanismo de transición de IPv6, para trasmitir paquetes de IPv6 entre nodos de doble pila sobre una red IPv4 con multicast habilitado, favoreciendo la coexistencia de IPv4. Utiliza IPv4 como Ethernet virtual para IPv6, este mecanismo admite la generación de direcciones Link-Local, se encuentra definido en RFC 2529 por IETF. Los túneles 6over4 pueden ser de: host a host, host a router y de router a host.". [28]

Ilustración 8: Arquitectura del túnel 6over4



Fuente: [29]

Tabla 6: Ventajas y Desventajas del túnel 6over4

Ventajas	Desventajas
• Soporta redes IPv4 multidifusión. • Cualquier host que se quiera incluir en 6over4 sobre una red IPv4 puede establecer una interfaz de red virtual IPv6.	• No está soportado por los sistemas operativos más comunes.

2.2.8.7. TÚNEL TEREDO

"Método de tunelización extremadamente popular, que no requiere de configuraciones especiales, fue desarrollado en febrero del año 2006 por Christian Huitema en la compañía Microsoft y estandarizado por la IETF en RFC4380. Se lo usa para establecer comunicación entre el cliente y el servidor y de tal manera facilite la comunicación entre dispositivos, permite

trabajar sobre entornos mixtos que se encuentren basados en IPv4 e IPv6, funcionan a través de una red NAT.” [28]

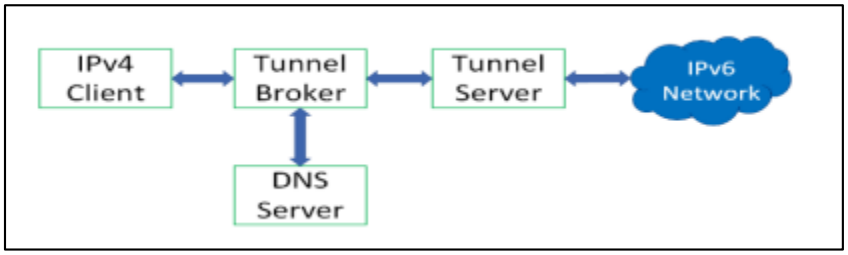
Tabla 7: Ventajas y Desventajas del túnel TEREDO.

Ventajas	Desventajas
• Permite conectividad IPv6 a un host incluso si se encuentra detrás de una red NAT.	• Vulnerable a ataques DoS y Spoofing. • Permite la conectividad IPv6 a un host por cada túnel.

2.2.8.8. TÚNEL BROKER

“Utiliza un mecanismo de tunelización de configuración automática para clientes IPv6 conectado a Internet IPv4. Se encuentra documentado en la RFC3053 por la IETF, desarrollado al inicio de la década del año 2000, tiempo en que la conectividad a IPv6 era muy pequeña, siendo su objetivo ofrecer una alternativa de conexión estable y constante. Permitiendo al usuario configurar correctamente su red y a partir de ese momento proveer conectividad IPv6 sobre IPv4”. [29]

Ilustración 9: Arquitectura del túnel BROKER



Fuente: [29]

Tabla 8: Ventajas y Desventajas del túnel BROKER.

Ventajas	Desventajas
• Permite al ISP controlar completamente el acceso a redes IPv6. • Fácil configuración y de ser administrados.	• Posee 2 cabeceras.

2.2.8.9. COMPARATIVA DE LOS MECANISMOS DE TÚNELES

En la siguiente tabla se muestra un listado de las características que poseen los mecanismos de túneles que se han investigado.

Tabla 9: Comparativa de los mecanismos de túneles.

Características	6to4	6RD	6in4	6over4	GRE	ISATAP	TEREDO	BROKER
Desarrollador	IETF	IETF	IETF	IETF	CISCO IETF	IETF	Christian Huitema Microsoft	IETF
Escalabilidad	Alta	Alta	Alta	Media	Media	Alta	Alta	Alta
Complejidad	Baja	Media	Media	Alta	Media	Media	Baja	Alta
Overhead	20 bytes	20 bytes	20 bytes	-	24 bytes	-	-	-
Red Acceso	IPv6	IPv6	IPv4	IPv4	IPv4 IPv6	IPv4	IPv4	IPv4
Prestaciones	Alta	Alta	Alta	Baja	Media	Media	Media	Media
Facilidad HA (High Availability)	Alta	Alta	Alta	Media	Media	Alta	Media	Media

Dada la investigación realizada se eligieron 3 mecanismos de túneles para ser evaluados: Túnel 6to4, Túnel 6over4 y Túnel GRE. Estos túneles han sido seleccionados basados en algunas investigaciones que se detallarán en el siguiente apartado.

Según, [30] indica varios mecanismos para permitir la adopción gradual de IPv6. Específicamente examina el mecanismo más utilizado, 6to4. Presenta las características operativas e identifica los principales requerimientos de gestión.

Otro estudio realiza una revisión sistemática de transición de IPv4 a IPv6 donde compara a estos dos protocolos y cada una de sus estructuras, así mismo describe los métodos de traducción y tunelización entre ellos el túnel 6over4, donde lo detalla como uno de los mejores túneles y que incluye mejoras respecto del túnel 6to4. [28]

Y, por último, un estudio sobre el uso del Túnel GRE en el que varias empresas lo ponen a prueba sobre distintos escenarios, en los cuales predomina la tecnología propietaria Cisco, determinándose que es la configuración óptima. [35]

En estos estudios se basa la selección de los tres tipos de túneles para la emulación y posterior comparación de los mismos dentro de una topología mixta, la cual permitirá recomendar a las organizaciones la implementación de un mecanismo de túnel que impacte lo menos posible el rendimiento de su red.

2.2.9. PROTOCOLOS DE ENRUTAMIENTO

"Los protocolos de enrutamiento son de suma importancia debido a que permiten la comunicación, enviar y recibir paquetes entre un nodo de origen hacia un nodo de destino que no precisamente se encuentran cerca, en sus inicios se configuraban manualmente a través de rutas estáticas". [31], [32]

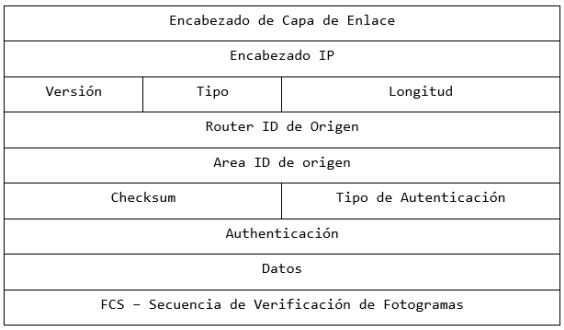
2.2.10. PROTOCOLO DE ENRUTAMIENTO OSPFV2

"Open Shortest Path First Version 2 (OSPFv2) es un protocolo de enrutamiento de estado de enlace para IPv4, desarrollado en el año de 1988 por el grupo Internet Engineers Task Force (IETF), para ser el reemplazo de RIP (Routing Information Protocol), se clasifica como un protocolo de puerta de enlace interior (IGP), es un protocolo de enrutamiento estándar abierto y un IGP particularmente mucho más eficiente y rápido que RIP." [33], [34]

"Se encuentra definido en RFC 2328, utilizan el algoritmo de Dijkstra para encontrar la ruta más corta y elegir la mejor ruta para el envió de paquetes. Hace

uso de un parámetro nombrado router ID para identificar el dispositivo de origen." [35]

Ilustración 10: Cabecera de OSPFv2.



2.2.10.1. CARACTERÍSTICAS DE OSPFV2

Entre las características se describen las siguientes: [36]

- Admite la jerarquía de dos niveles.
- Convergencia rápida.
- Protocolo sin clase.
- Admite VLSM (Variable Length Subnet Mask – Máscara de Subred de Longitud Variables) y CIDR (Classles Inter-Domain Routing).
- Admite autenticación MD5.
- Es escalable funciona bien en redes de tamaño pequeños y grandes.

2.2.10.2. VENTAJAS Y DESVENTAJAS DE OSPFV2

La tabla que se muestra a continuación describe las ventajas y desventajas que posee OSPFv2: [37]

Tabla 10: Ventajas y Desventajas de OSPFv2

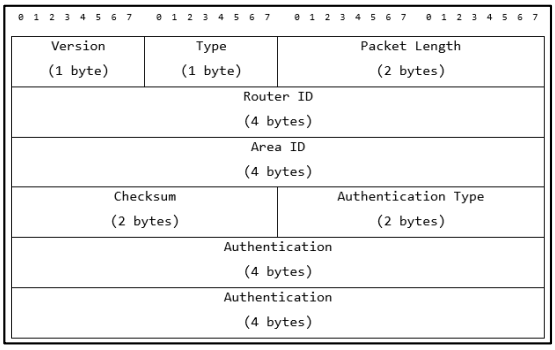
Ventajas	Desventajas
• Convergencia más rápida que protocolos de vector distancia. • Maneja el ancho de banda de los enlaces como base de la métrica. • No tiende a sufrir de bucles de enrutamiento • Escala en redes grandes.	• Solo soporta protocolos del conjunto TCP/IP. • Mayor uso de memoria RAM y del router.

2.2.11. PROTOCOLO DE ENRUTAMIENTO OSPFV3

"Open Shortest Path First Version 3 (OSPFv3) o en español Primero la Ruta más Corta Versión 3, es un protocolo de enrutamiento IGP basado en la tecnología de estado de enlace, es utilizado para configurar redes con el protocolo IPv6, se encuentra definido por la IEEE RFC 5340, siendo estandarizado por primera vez en el año de 1989. Para el cálculo de la ruta más corta utiliza el algoritmo de Dijkstra, para la selección de la mejor ruta. De esta forma se podrán comparar dos algoritmos de encaminamiento y evaluar cuál de los dos es apto según la topología de red." [38], [39]

"Este protocolo se ejecuta en la interfaz de los routers y se pueden configurar varias instancias de OSPFv3 en un enlace lógico, se encuentra compuesto por tres procesos mientras está siendo configurado, primero busca vecinos, segunda crea adyacencias y tercero comparte la información de enrutamiento". [40], [41]

Ilustración 11: *Cabecera de OSPFv3.*



2.2.11.1. CARACTERÍSTICAS DE OSPFV3

Entre las características de OSPFv3 se describen las siguientes: [42], [43]

- Se encuentra basado en OSPFv2.
- Trabaja con direcciones IPv6.
- Soporta diseño jerárquico.
- Posee rápida convergencia.
- Es compatible con VLSM.
- Diseñado para superar algunas limitaciones existentes en otros protocolos de enrutamiento.

2.2.11.2. VENTAJAS Y DESVENTAJAS DE OSPV3

En la tabla que se muestra a continuación se puede observar las principales ventajas y desventajas que posee OSPFv3: [44], [45]

Tabla 11: Ventajas y Desventajas de OSPFv3

Ventajas	Desventajas
• Convergencia más rápida y escalabilidad en redes extensas. • Admite varias rutas. • Soporta dispositivos de todos los fabricantes, porque es un estándar de carácter público. • Emplea un menor ancho de banda. • Los router tiene conocimiento total de la red. • La actualización de la tabla de enrutamiento es rápida cuando se presentan cambios.	• No posee soporte para direcciones IPv4. • Consume altos recursos de CPU y memoria del router. • Requiere dispositivos más eficaces y más memorias porque sus algoritmos son más complejos.

2.3. OBJETIVOS DE LA TOPOLOGÍA DE RED

2.3.1. OBJETIVO GENERAL

Desarrollar un análisis comparativo de los mecanismos de túneles para la transición de IPv4 a IPv6, utilizando el emulador GNS3 para comprender su funcionamiento y rendimiento mediante pruebas experimentales.

2.3.2. OBJETIVOS ESPECÍFICOS

- Analizar teóricamente los mecanismos de túneles para la transición de IPv4 a IPv6.
- Seleccionar los mecanismos de túneles que se utilizarán en la experimentación.
- Identificar las herramientas y equipos necesarios que sean compatibles para la configuración de las topologías.
- Configurar los equipos de la red, así como los protocolos de enrutamiento y los mecanismos de túneles objetos de estudio.
- Realizar un análisis comparativo de los resultados obtenidos acerca el comportamiento de las topologías y pruebas de conectividad.

2.4. DISEÑO DE LA TOPOLOGÍA DE RED

La topología de red se encuentra diseñada con equipos compatibles con los protocolos IPv4 e IPv6, esto permitirá la comunicación a través de configuraciones de comando mediante la consola, de esta manera será posible mostrar su funcionamiento y realizar el análisis comparativo de los túneles.

A continuación, se muestra las diferentes tablas de direccionamiento IPv6 e IPv4 de los tres mecanismos de túneles seleccionados, las mismas que han sido asignadas a las interfaces de los router y dispositivos finales, así mismo como la longitud de prefijo, puertas de enlace.

Tabla 12: *Direccionamiento del túnel 6to4.*

Device	Interface	IP Address	Máscara de Subred	Default Gateway
Router 1 (R1)	Serial 3/0 (S3/0)	10.0.1.1	255.255.255.0	N/A
	Ethernet 4/0 (E4/0)	2002:A00:101::1/64	N/A	
	Tunnel 0	2002:A00:101::/64		
Router 2 (R2)	Serial 3/0 (S3/0)	10.0.1.2	255.255.255.0	N/A
	Serial 3/1 (S3/1)	10.0.2.1		
	Serial 3/3 (S3/3)	10.0.4.1		
Router 3 (R3)	Serial 3/1 (S3/1)	10.0.2.2	255.255.255.0	N/A
	Serial 3/2 (S3/2)	10.0.3.2		
Router 4 (R4)	Serial 3/1 (S3/0)	10.0.5.2	255.255.255.0	N/A
	Serial 3/2 (S3/1)	10.0.3.1		
	Serial 3/3 (S3/3)	10.0.4.2		
Router 5 (R5)	Serial 3/1 (S3/1)	10.0.5.1	255.255.255.0	N/A
	Ethernet 4/0 (E4/0)	2002:A00:501::1/64	N/A	
	Tunnel 0	2002:A00:501::/64		
Switch 1 (SW-1)	Ethernet 0 (E0)	N/A	N/A	N/A
	Ethernet 1 (E1)			
	Ethernet 4 (E4)			
Switch 2 (SW-2)	Ethernet 0 (E0)	N/A	N/A	N/A
	Ethernet 1 (E1)			
	Ethernet 4 (E4)			
PC1	Ethernet 0 (E0)	2002:A00:101::2/64	N/A	N/A
PC2	Ethernet 0 (E0)	2002:A00:101::3/64	N/A	N/A
PC3	Ethernet 0 (E0)	2002:A00:501::2/64	N/A	N/A
PC4	Ethernet 0 (E0)	2002:A00:501::3/64	N/A	N/A

Tabla 13: Direccionamiento del túnel 6over4.

Device	Interface	IP Address	Máscara de Subred	Default Gateway
Router 1 (R1)	Serial 3/0 (S3/0)	10.0.1.1	255.255.255.0	N/A
	Ethernet 4/0 (E4/0)	10.0.0.1	255.255.255.0	
		1000:ABC:1:DCA::1/64	N/A	
	Tunnel 0	1000:A00:101:1::2/64		
Router 2 (R2)	Serial 3/0 (S3/0)	10.0.1.2	255.255.255.0	N/A
	Serial 3/1 (S3/1)	10.0.2.1		
	Serial 3/3 (S3/3)	10.0.4.1		
Router 3 (R3)	Serial 3/1 (S3/1)	10.0.2.2	255.255.255.0	N/A
	Serial 3/2 (S3/2)	10.0.3.2		
Router 4 (R4)	Serial 3/1 (S3/0)	10.0.5.2	255.255.255.0	N/A
	Serial 3/2 (S3/1)	10.0.3.1		
	Serial 3/3 (S3/3)	10.0.4.2		
Router 5 (R5)	Serial 3/1 (S3/1)	10.0.5.1	255.255.255.0	N/A
	Ethernet 4/0 (E4/0)	10.0.6.1		
		1000:ABC:1:DCB::1/64	N/A	
	Tunnel 0	1000:A00:101:1::1/64		
Switch 1 (SW-1)	Ethernet 0 (E0)	N/A	N/A	N/A
	Ethernet 1 (E1)			
	Ethernet 4 (E4)			
Switch 2 (SW-2)	Ethernet 0 (E0)	N/A	N/A	N/A
	Ethernet 1 (E1)			
	Ethernet 4 (E4)			
PC1	Ethernet 0 (E0)	1000:ABC:1:DCA::2/64	N/A	N/A
		10.0.0.2	255.255.255.0	10.0.0.1
PC2	Ethernet 0 (E0)	1000:ABC:1:DCA::3/64	N/A	N/A
		10.0.0.3	255.255.255.0	10.0.0.1
PC3	Ethernet 0 (E0)	1000:ABC:1:DCB::2/64	N/A	N/A
		10.0.6.3	255.255.255.0	10.0.6.1
PC4	Ethernet 0 (E0)	1000:ABC:1:DCB::3/64	N/A	N/A
		10.0.6.2	255.255.255.0	10.0.6.1

Tabla 14: Direccionamiento del túnel GRE.

Device	Interface	IP Address	Máscara de Subred	Default Gateway
Router 1 (R1)	Serial 3/0 (S3/0)	10.0.1.1	255.255.255.0	N/A
	Ethernet 4/0 (E4/0)	1000:ABC:1:DCA:1/64	N/A	
	Tunnel 0	1000:A00:101:1::1/64		
Router 2 (R2)	Serial 3/0 (S3/0)	10.0.1.2	255.255.255.0	N/A
	Serial 3/1 (S3/1)	10.0.2.1		
	Serial 3/3 (S3/3)	10.0.4.1		
Router 3 (R3)	Serial 3/1 (S3/1)	10.0.2.2	255.255.255.0	N/A
	Serial 3/2 (S3/2)	10.0.3.2		
Router 4 (R4)	Serial 3/1 (S3/0)	10.0.5.2	255.255.255.0	N/A
	Serial 3/2 (S3/1)	10.0.3.1		
	Serial 3/3 (S3/3)	10.0.4.2		
Router 5 (R5)	Serial 3/1 (S3/1)	10.0.5.1	255.255.255.0	N/A
	Ethernet 4/0 (E4/0)	1000:ABC:1:DCB:1/64	N/A	
	Tunnel 0	1000:A00:101:1::2/64		
Switch 1 (SW-1)	Ethernet 0 (E0)	N/A	N/A	N/A
	Ethernet 1 (E1)			
	Ethernet 4 (E4)			
Switch 2 (SW-2)	Ethernet 0 (E0)	N/A	N/A	N/A
	Ethernet 1 (E1)			
	Ethernet 4 (E4)			
PC – 1	Ethernet 0 (E0)	1000:ABC:1:DCA:2/64	N/A	N/A
PC – 2	Ethernet 0 (E0)	1000:ABC:1:DCA:3/64	N/A	N/A
PC – 3	Ethernet 0 (E0)	1000:ABC:1:DCB:2/64	N/A	N/A
PC – 4	Ethernet 0 (E0)	1000:ABC:1:DCB:3/64	N/A	N/A

2.4.1. CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO EN LOS DISPOSITIVOS

Para los procesos de configuración se hace uso de direcciones IPv4 con prefijo /24 y direcciones IPv6 con prefijo /64, la misma que será distribuida en las diferentes interfaces de los dispositivos.

2.4.1.1. CONFIGURACIÓN DEL DIRECCIONAMIENTO DE LOS ROUTERS

Para realizar las respectivas asignaciones de direcciones a los dispositivos (routers) a ser utilizados, es necesario acceder al modo de configuración global, para esto se utilizó el siguiente comando:

```
Router# configure terminal
```

Dentro del modo de configuración, habilitamos el direccionamiento IPv6, el mismo que se lo realiza mediante el comando:

```
Router(config)# ipv6 unicast-routing
```

Posteriormente accedemos a las interfaces de los routers para asignarles las respectivas direcciones IPv6 y activamos la interfaz. Esto es posible mediante los siguientes comandos:

```
Router (config)# interface < tipo y número >
Router (config – if) # ipv6 address < dirección ipv6 y prefijo >
Router (config – if) # no shutdown
```

Así mismo accedemos a las interfaces de los routers para asignarles las respectivas direcciones IPv4 y activamos la interfaz, se utilizan los siguientes comandos:

```
Router (config)# interface < tipo y número >
Router (config – if) # ip address < dirección ip y prefijo >
Router (config – if) # no shutdown
```

Este procedimiento se lo hace en todas las interfaces de los demás routers que se van a utilizar.

Ilustración 12: *Direccionamiento IPv6 en Ethernet 4/0 del router 1.*

```
R1(config)#ipv6 unicast-routing
R1(config)#interface e4/0
R1(config-if)#ipv6 address 1000:ABC:1:DCA::1/64
R1(config-if)#no shutdown
R1(config-if)#
*Feb 11 04:01:40.959: %LINK-3-UPDOWN: Interface Ethernet4/0, changed state to up
*Feb 11 04:01:41.959: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet4/0
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#exit
```

Ilustración 13: *Direccionamiento IPv4 en Serial 3/0 del router 1.*

```
R1(config)#interface s3/0
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Feb 11 04:04:46.139: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
R1(config-if)#
*Feb 11 04:04:47.147: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0
```

Ilustración 14: *Direccionamiento IPv4 en Serial 3/0 del router 2.*

```
R2(config)#interface s3/0
R2(config-if)#ip address 10.0.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Feb 11 04:03:27.919: %LINK-3-UPDOWN: Interface Serial3/0, changed state to up
R2(config-if)#
*Feb 11 04:03:28.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0,
```

Ilustración 15: *Direccionamiento IPv4 en Serial 3/1 del router 2.*

```
R2(config-if)#interface s3/1
R2(config-if)#ip address 10.0.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface s3/1
*Feb 11 04:03:56.635: %LINK-3-UPDOWN: Interface Serial3/1, changed state to up
R2(config-if)#interface s3/3
*Feb 11 04:03:57.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1,
```

Ilustración 16: *Direccionamiento IPv4 en Serial 3/3 del router 2.*

```
R2(config-if)#interface s3/3
*Feb 11 04:03:57.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1,
R2(config-if)#interface s3/3
R2(config-if)#ip address 10.0.4.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Feb 11 04:04:17.239: %LINK-3-UPDOWN: Interface Serial3/3, changed state to up
R2(config-if)#
*Feb 11 04:04:18.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/3,
```

Ilustración 17: *Direccionamiento IPv4 en Serial 3/1 del router 3.*

```
R3#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface s3/1
R3(config-if)#ip address 10.0.2.2 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
*Feb 11 04:04:13.503: %LINK-3-UPDOWN: Interface Serial3/1, changed state to up
R3(config-if)#
*Feb 11 04:04:14.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1
```

Ilustración 18: *Direccionamiento IPv4 en Serial 3/2 del router 3.*

```
R3(config-if)#interface s3/2
R3(config-if)#ip address 10.0.3.2 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
*Feb 11 04:04:38.611: %LINK-3-UPDOWN: Interface Serial3/2, changed state to up
R3(config-if)#
*Feb 11 04:04:39.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/2
```

Ilustración 19: *Direccionamiento IPv4 en Serial 3/2 del router 4.*

```
R4#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface s3/2
R4(config-if)#ip address 10.0.3.1 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#
*Feb 11 04:05:09.355: %LINK-3-UPDOWN: Interface Serial3/2, changed state to up
R4(config-if)#
*Feb 11 04:05:10.363: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/2
```

Ilustración 20: *Direccionamiento IPv4 en Serial 3/3 del router 4.*

```
R4(config-if)#interface s3/3
R4(config-if)#ip address 10.0.4.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#
*Feb 11 04:05:38.739: %LINK-3-UPDOWN: Interface Serial3/3, changed state to up
R4(config-if)#
*Feb 11 04:05:39.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/3
```

Ilustración 21: *Direccionamiento IPv4 en Serial 3/1 del router 4.*

```
R4(config-if)#interface s3/1
R4(config-if)#ip address 10.0.5.2 255.255.255.0
R4(config-if)#no shut
R4(config-if)#
*Feb 11 04:05:59.479: %LINK-3-UPDOWN: Interface Serial3/1, changed state to up
R4(config-if)#
*Feb 11 04:06:00.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1
```

Ilustración 22: *Direccionamiento IPv6 en Ethernet 4/0 del router 5.*

```
R5(config)#ipv6 unicast-routing
R5(config)#interface e4/0
R5(config-if)#ipv6 address 1000:ABC:1:DCB::1/64
R5(config-if)#ip address 10.0.6.1 255.255.255.0
R5(config-if)#no shut
R5(config-if)#
*Feb 11 04:19:10.879: %LINK-3-UPDOWN: Interface Ethernet4/0, changed state to up
*Feb 11 04:19:11.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet4/0
```

Ilustración 23: Direccionamiento IPv4 en Serial 3/1 del router 5.

```
R5(config-if)#
*Feb 11 04:19:10.879: %LINK-3-UPDOWN: Interface Ethernet4/0, changed state to up
*Feb 11 04:19:11.879: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet4/0
R5(config-if)#interface s3/1
R5(config-if)#ip address 10.0.5.1 255.255.255.0
R5(config-if)#exit
```

Las direcciones IP varían dependiendo del mecanismo de túnel, para realizar las pruebas respectivas.

2.4.1.2. CONFIGURACIÓN DEL PROTOCOLO OSPFv2

Una vez direccionada la red adecuadamente se procede a realizar la activación del protocolo en cada una de las interfaces de los routers desde la terminal, en primer lugar, accedemos al modo de configuración global, para lo cual hacemos uso de este comando:

Router # configure terminal

Luego se debe asignar un identificador de proceso, mediante el uso del siguiente comando:

Router (config)# router ospf 1

Una vez aplicado el comando anterior se debe configurar un identificar único de router para el proceso, utilizando el siguiente comando:

Router (config – router) # router-id < identificador del router >

A continuación, se deben especificar las redes por las que se enviarán los mensajes de actualización de rutas, cada red debe estar identificada con un área a la cual pertenece, para ellos se utiliza el siguiente comando:

Router (config – router) # network < dirección red > < máscara wildcard > area < id área >

Ilustración 24: Configuración protocolo OSPFv2 en el Router 1.

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 10.0.0.0 0.0.0.255 area 0
R1(config-router)#exit
```

Ilustración 25: *Configuración protocolo OSPFv2 en el Router 2.*

```
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#
*Feb 11 04:04:45.703: %LINEPROTO-5-UPDOWN: Line protocol on
R2(config-router)#network 10.0.1.0 0.0.0.255 area 0
R2(config-router)#
*Feb 11 04:05:31.939: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1
 Done
R2(config-router)#network 10.0.2.0 0.0.0.255 area 0
R2(config-router)#network 10.0.4.0 0.0.0.255 area 0
R2(config-router)#
```

Ilustración 26: *Configuración protocolo OSPFv2 en el Router 3.*

```
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network
*Feb 11 04:05:05.819: %LINEPROTO-5-UPDOWN: Line protocol on
R3(config-router)#network 10.0.2.0 0.0.0.255 area 0
R3(config-router)#network 10.0.2.0 0.0.0.255 area 0
*Feb 11 04:05:20.947: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2
 Done
R3(config-router)#network 10.0.3.0 0.0.0.255 area 0
R3(config-router)#
```

Ilustración 27: *Configuración protocolo OSPFv2 en el Router 4.*

```
R4(config)#router ospf 1
R4(config-router)#router-id 4.4.4.4
R4(config-router)#netwo
*Feb 11 04:06:25.587: %LINEPROTO-5-UPDOWN: Line protocol on
R4(config-router)#network 10.0.3.0 0.0.0.255 area 0
R4(config-router)#network 10.0.3.0 0.0.0.255 area 0
*Feb 11 04:06:43.467: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3
 Done
R4(config-router)#network 10.0.4.0 0.0.0.255 area 0
R4(config-router)#
*Feb 11 04:06:52.079: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2
 Done
R4(config-router)#network 10.0.5.0 0.0.0.255 area 0
R4(config-router)#
```

Ilustración 28: *Configuración protocolo OSPFv2 en el Router 5.*

```
R5(config)#router ospf 1
R5(config-router)#router-id 5.5.5.5
R5(config-router)#network 10.0.5.0 0.0.0.255 area 0
R5(config-router)#network 10.0.6.0 0.0.0.255 area 0
```

2.4.1.3. CONFIGURACIÓN DEL PROTOCOLO OSPFv3

Una vez direccionada la red adecuadamente se procede a realizar la activación del protocolo en cada una de las interfaces de los routers desde la terminal, en primer lugar, accedemos al modo de configuración global, para lo cual hacemos uso de este comando:

```
Router # configure terminal
```

Luego se debe asignar un identificador de proceso, mediante el uso del siguiente comando:

```
Router (config)# ipv6 router ospf < número de proceso >
```

Una vez aplicado el comando anterior se debe configurar un identificador único de router para el proceso, para esto se usa el siguiente comando:

```
Router (config – rtr )# router-id < identificador del router >
```

Una vez aplicados los comandos de implementación, regresamos al modo de configuración global mediante el comando **exit**.

Ahora vamos a configurar el protocolo dentro de cada interfaz, con el siguiente comando:

```
Router (config)# interface < tipo y número >
Router (config – if) # ipv6 ospf < número de proceso > area < número de area >
```

Ilustración 29: *Configuración protocolo OSPFv3 en el Router 1.*

```
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#
*Feb 17 12:46:44.467: %OSPFv3-4-NORTRID: Process OSPFv3-1-IPv6
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#interface e4/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#exit
R1(config)#
```

Ilustración 30: Configuración protocolo OSPFv3 en el Router 5.

```
R5#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#ipv6 router ospf 1
R5(config-rtr)#router-id 5.5.5.5
R5(config-rtr)#exit
R5(config)#interface e4/0
R5(config-if)#ipv6 ospf 1 area 0
R5(config-if)#exit
R5(config)#
```

2.4.1.4. CONFIGURACIÓN DE LOS HOST

La configuración es sencilla, lo único que se debe hacer es asignar la dirección IP, con su respectivo prefijo y en el caso de usar se asigna también la puerta de enlace, que generalmente es la dirección del router con el que se encuentra conectado, para esto usamos los siguientes comandos para IPv6 e IPv4 respectivamente:

PC > ip < dirección ipv6 y prefijo >

PC > ip < dirección ipv4 y prefijo > < gateway >

Estos comandos son utilizados para configurar el direccionamiento en los dispositivos finales u hosts, como se muestra en las siguientes imágenes.

Ilustración 31:Direccionamiento PC1.

```
PC1> ip 1000:ABC:1:DCA::2/64
PC1 : 1000:abc:1:dca::2/64

PC1> ip 10.0.0.2/24 10.0.0.1
Checking for duplicate address...
PC1 : 10.0.0.2 255.255.255.0 gateway 10.0.0.1

PC1> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    10.0.0.2/24          10.0.0.1          00:50:79:66:68:00  10046  127.0.0.1:10047
       fe80::250:79ff:fe66:6800/64
       1000:abc:1:dca::2/64
```

Ilustración 32:Direccionamiento PC2.

```
PC2> ip 1000:ABC:1:DCA::3/64
PC1 : 1000:abc:1:dca::3/64

PC2> ip 10.0.0.3/24 10.0.0.1
Checking for duplicate address...
PC1 : 10.0.0.3 255.255.255.0 gateway 10.0.0.1

PC2> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    10.0.0.3/24          10.0.0.1          00:50:79:66:68:01  10048  127.0.0.1:10049
       fe80::250:79ff:fe66:6801/64
       1000:abc:1:dca::3/64
```

Ilustración 33:Direccionamiento PC3.

```
PC3> ip 1000:ABC:1:DCB::3/64
PC1 : 1000:abc:1:dcb::3/64

PC3> ip 10.0.6.3/24 10.0.6.1
Checking for duplicate address...
PC1 : 10.0.6.3 255.255.255.0 gateway 10.0.6.1

PC3> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC3    10.0.6.3/24          10.0.6.1          00:50:79:66:68:02  10050  127.0.0.1:10051
       fe80::250:79ff:fe66:6802/64
       1000:abc:1:dcb::3/64
```

Ilustración 34:Direccionamiento PC4.

```
PC4> ip 1000:ABC:1:DCB::2/64
PC1 : 1000:abc:1:dcb::2/64

PC4> ip 10.0.6.2/24 10.0.6.1
Checking for duplicate address...
PC1 : 10.0.6.2 255.255.255.0 gateway 10.0.6.1

PC4> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC4    10.0.6.2/24          10.0.6.1          00:50:79:66:68:03  10052  127.0.0.1:10053
       fe80::250:79ff:fe66:6803/64
       1000:abc:1:dcb::2/64
```

2.4.1.5. CONFIGURACIÓN DEL TÚNEL 6TO4

Una vez realizado el direccionamiento en las interfaces de los routers, procedemos a la creación del túnel 6to4, para esto vamos a usar los siguientes comandos.

Router (config)# interface < tipo y número >

Router (config – if) # ipv6 unnumbered < interfaz tipo y número >

Router (config – if) # tunnel source < interfaz de inicio de túnel o dirección ip >

Router (config – if) # tunnel mode < tipo de encapsulado > < tipo de túnel >

Una vez aplicados cada uno de estos comandos el túnel quedará de la siguiente manera:

Ilustración 35: *Configuración del túnel 6to4 en el router 1.*

```
R1(config)#interface tunnel 0
R1(config-if)#ipv6 unnumbered e4/0
R1(config-if)#tunnel source s3/0
R1(config-if)#tunnel mode ipv6ip 6to4
R1(config-if)#
```

Ilustración 36: *Configuración del túnel 6to4 en el router 5.*

```
R5(config-if)#ipv6 unnumbered e4/0
R5(config-if)#tunnel source s3/1
R5(config-if)#tunnel mode ipv6ip 6to4
R5(config-if)#
```

2.4.1.6. CONFIGURACIÓN DEL TÚNEL 6OVER4

De la misma manera ya realizado el direccionamiento en las interfaces de los routers, procedemos a la creación del túnel 6over4, para esto vamos a usar los siguientes comandos.

Router (config)# interface < tipo y número >

Router (config – if) # tunnel mode < tipo de encapsulado >

Router (config – if) # ipv6 address < dirección ipv6 del túnel >

Router (config – if) # tunnel source < interfaz de inicio de túnel o dirección ip >

Router (config – if) # tunnel destination < dirección ip de destino del túnel >

Una vez aplicados cada uno de estos comandos el túnel quedará de la siguiente manera:

Ilustración 37: *Configuración del túnel 6over4 en el router 1.*

```
R1(config)#interface tunnel 0
R1(config-if)#
*Feb 11 04:39:25.439: %LINEPROTO-5-UPDOWN: Line
R1(config-if)#tunnel mode ipv6ip
R1(config-if)#ipv6 address 1000:A00:101:1::2/64
R1(config-if)#tunnel source s3/0
R1(config-if)#tunnel destination 10.0.5.1
R1(config-if)#
```

Ilustración 38: *Configuración del túnel 6over4 en el router 5.*

```
R5(config)#interface tunnel 0
R5(config-if)#
*Feb 11 04:38:25.079: %LINEPROTO-5-UPDOWN: Line
R5(config-if)#tunnel mode ipv6ip
R5(config-if)#ipv6 address 1000:A00:101:1::1/64
R5(config-if)#tunnel source s3/1
R5(config-if)#tunnel destination 10.0.1.1
R5(config-if)#
```

2.4.1.7. CONFIGURACIÓN DEL TÚNEL GRE

Así mismo, ya realizado el direccionamiento en las interfaces de los routers, procedemos a la creación del túnel GRE, para esto vamos a usar los siguientes comandos.

Router (config)# interface < tipo y número >

Router (config – if) # tunnel mode < tipo de túnel > < tipo de encapsulado >

Router (config – if) # ipv6 address < dirección ipv6 del túnel >

Router (config – if) # tunnel source < interfaz de inicio de túnel o dirección ip >

Router (config – if) # tunnel destination < dirección ip de destino del túnel >

Una vez aplicados cada uno de estos comandos el túnel quedará de la siguiente manera:

Ilustración 39: Configuración del túnel GRE en el router 1.

```
R1(config)#interface tunnel 0
R1(config-if)#
*Feb 16 19:38:07.619: %LINEPROTO-5-UPDOWN: Line
R1(config-if)#tunnel mode gre ip
R1(config-if)#ipv6 address 1000:A00:101:1::1/64
R1(config-if)#tunnel source s3/0
R1(config-if)#tunnel destination 10.0.5.1
R1(config-if)#
```

Ilustración 40: Configuración del túnel GRE en el router 1.

```
R5(config)#interface tunnel 0
R5(config-if)#tunnel mod
*Feb 16 19:32:26.175: %LINEPROTO-5-UPDOWN: Line
R5(config-if)#tunnel mode gre ip
R5(config-if)#ipv6 addres 1000:A00:101:1::2/64
R5(config-if)#tunnel source s3/1
R5(config-if)#tunnel destination 10.0.1.1
R5(config-if)#
```

2.4.1.8. RESULTADOS DE LA CONFIGURACIÓN

Una vez realizada la configuración en los dispositivos, vamos a observar el resultado en cada uno de los routers, haciendo uso del comando:

Router # show running-config

O también podemos revisar la configuración por interfaz mediante el comando:

Router # show run interface < tipo y número>

En las siguientes ilustraciones podremos verificar el uso de los dos comandos mostrados con anterioridad:

Ilustración 41: *Configuración del Router3*

```
R3#show running-config
Building configuration...

Current configuration : 1659 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
interface Serial3/1
 ip address 10.0.2.2 255.255.255.0
 serial restart-delay 0

interface Serial3/2
 ip address 10.0.3.2 255.255.255.0
 serial restart-delay 0
!
router ospf 1
 router-id 3.3.3.3
 network 10.0.2.0 0.0.0.255 area 0
 network 10.0.3.0 0.0.0.255 area 0
```

Ilustración 42: *Configuración de la interfaz Ethernet 4/0 del router 1.*

```
R1#show run interface e4/0
Building configuration...

Current configuration : 112 bytes
!
interface Ethernet4/0
 no ip address
 duplex half
 ipv6 address 1000:ABC:1:DCA::1/64
 ipv6 ospf 1 area 0
end
```

Ilustración 43: *Configuración de la interfaz Serial 3/0 del router 1.*

```
R1#show run interface s3/0
Building configuration...

Current configuration : 86 bytes
!
interface Serial3/0
 ip address 10.0.1.1 255.255.255.0
 serial restart-delay 0
end

R1#show run interface tunnel0
Building configuration...

Current configuration : 149 bytes
!
```

Ilustración 44: Configuración de la interfaz Tunel 0 del router 1.

```
R1#show run interface tunnel0
Building configuration...

Current configuration : 149 bytes
!
interface Tunnel0
 no ip address
 ipv6 address 1000:A00:101:1::1/64
 ipv6 ospf 1 area 0
 tunnel source Serial3/0
 tunnel destination 10.0.5.1
end
```

2.5. EJECUCIÓN DE LA TOPOLOGÍA DE RED CON OSPFv2 Y OSPFv3

Una vez que ya estén correctamente aplicadas las configuraciones de las topologías, al momento de realizar la ejecución es necesario aplicar pruebas de conectividad a través del envío de paquetes mediante el comando ping ya que es la mejor manera de corroborar si existe comunicación entre los dispositivos, el comando va sujeto de la siguiente manera:

ping < dirección ipv4 o ipv6>

Al ejecutarlo el comando presentará la siguiente información:

Ilustración 45: Prueba de conectividad, mediante ping Router1 a Router 3 con OSPFv2.

```
R1#ping 10.0.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/76/104 ms
R1#
```

Además, se puede hacer una visualización de las tablas de enrutamiento ya sea IPv4 o IPv6 mediante los siguientes comandos:

Router # show ip route

Router # show ipv6 route

En las siguientes ilustraciones podremos constatar el uso de ambos comandos.

Ilustración 46: *Tabla de enrutamiento IPv4 del Router 1.*

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.1.0/24 is directly connected, Serial3/0
L        10.0.1.1/32 is directly connected, Serial3/0
O        10.0.2.0/24 [110/128] via 10.0.1.2, 00:28:19, Serial3/0
O        10.0.3.0/24 [110/192] via 10.0.1.2, 00:28:19, Serial3/0
O        10.0.4.0/24 [110/128] via 10.0.1.2, 00:28:19, Serial3/0
O        10.0.5.0/24 [110/192] via 10.0.1.2, 00:28:19, Serial3/0
```

Ilustración 47: *Tabla de enrutamiento IPv6 del Router 1.*

```
R1#show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, l - LISP
C   1000:A00:101:1::/64 [0/0]
     via Tunnel0, directly connected
L   1000:A00:101:1::1/128 [0/0]
     via Tunnel0, receive
C   1000:ABC:1:DCA::/64 [0/0]
     via Ethernet4/0, directly connected
L   1000:ABC:1:DCA::1/128 [0/0]
     via Ethernet4/0, receive
O   1000:ABC:1:DCB::/64 [110/1010]
     via FE80::C805:EFF:FE7C:0, Tunnel0
L   FF00::/8 [0/0]
     via Null0, receive
```

3. CAPÍTULO III. EVALUACIÓN DE LA TOPOLOGÍA DE RED

3.1. PLAN DE EVALUACIÓN

Se plantea la comparación entre tres topologías iguales, con equipos de la línea Cisco que soportan los protocolos IPv6 e IPv4.

Una vez que se analizaron los mecanismos de túneles a comparar y se configuraron los mismos en las topologías.

3.2. RESULTADOS DE LA EVALUACIÓN

3.2.1. COMPARATIVA ENTRE LOS MECANISMOS DE TÚNELES

En la siguiente tabla se muestra un listado de las características que poseen los mecanismos de túneles que se han simulado dentro de GNS3.

__Tabla 15:__ Comparativa entre los túneles 6to4, 6over4 y GRE.

Características	6to4	6over4	GRE
Seguridad	Baja	Baja	Baja
Prefijo	2002::/16	Asignado por Administrador	Asignado por Administrador
Implementación	Media	Alta	Media
Mantenimiento	Sencillo	Complejo	Sencillo
Transparencia al Cliente	No	No	No
Recursos	Medio	Alto	Alto
Propietario	Libre	Libre	Libre

Tal y como se presenta en la tabla 15 se puede determinar que el túnel 6to4 es el que posee las características necesarias que evidencian porque es uno de los túneles más usados en el mundo, ya sea por su facilidad de implementación, mantenimiento y consumo de recursos que lo catalogan como uno de los mejores mecanismos de túneles.

3.2.2. DISEÑO DE PRUEBAS

Para la comparación entre los tres mecanismos de túneles se diseñaron pruebas de envío de paquetes ICMPv6 entre los routers y entre los hosts de los extremos, las mismas que han sido realizadas en las tres topologías.

3.2.2.1. COMPARATIVA ROUTER 1 A LA ETHERNET4/0 DEL ROUTER 5.

Se realiza un envío de paquetes desde el Router 1 al Router 5 mediante el comando ping extendido, el mismo que tendrá un tamaño de 100 bytes y se repetirá 10 veces. Se aplicará las mismas características para los 3 túneles a comparar. El comando que se utilizó es el siguiente:

ping <ip a enviar> **size** <cantidad de bytes> **repeat** <número de secuencias>

Ilustración 48: *Ping desde Router 1 a Ethernet 4/0 del Router 5, topología túnel 6to4.*

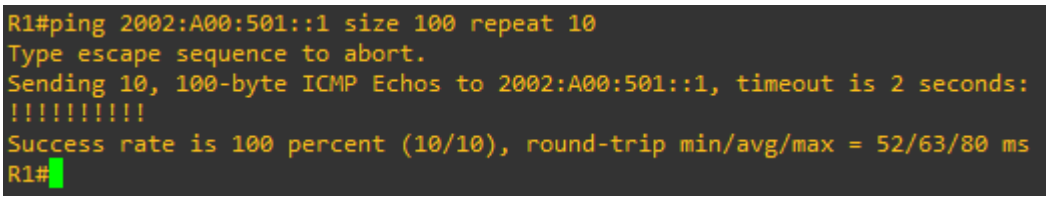


Ilustración 49: *Ping desde Router 1 a Ethernet 4/0 del Router 5, topología túnel 6over4.*

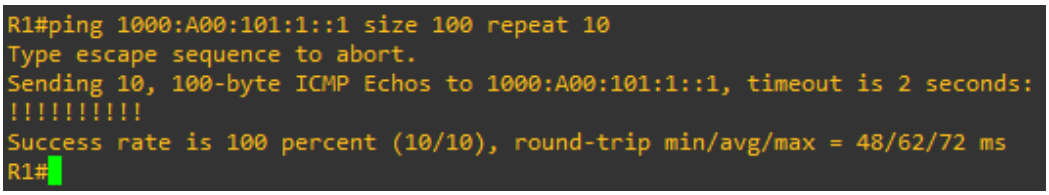


Ilustración 50: *Ping desde Router 1 a Ethernet 4/0 del Router 5, topología túnel GRE.*

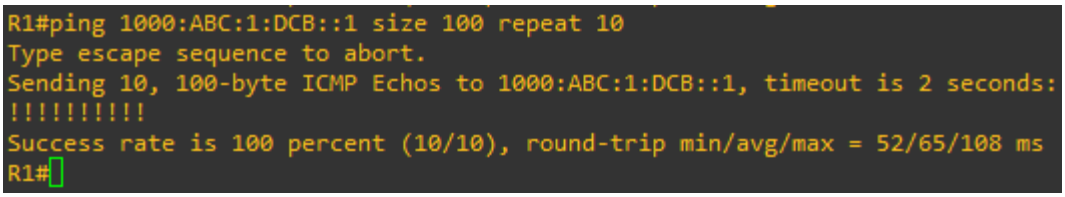


Tabla 16: *Comparativa de envío de paquetes entre el router 1 y router 5 con los túneles 6to4, 6over4 y GRE.*

Características	6to4			6over4			GRE		
Secuencias	10			10			10		
Bytes	100			100			100		
Tiempo de Espera (ms)	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
	52	63	80	48	62	72	52	65	108
Paquetes Perdidos	0			0			0		
Tasa de Éxito (%)	100			100			100		

Tal y como se presenta en las ilustraciones 48, 49 y 50, se observa el resultado que se obtiene cuando se aplicó el comando ping con los parámetros definidos, de los cuales se observa un envío de paquetes desde el router 1 hacia la dirección IP del puerto Ethernet4/0 del router 5 con los tres túneles seleccionados, esta puede ser verificada en la tabla 16. Además, se puede determinar que el Túnel que hace los envíos de paquetes entre interfaces de forma más rápida es el Túnel 6over4, frente a los demás túneles.

3.2.2.2. COMPARATIVA ROUTER 5 A LA ETHERNET4/0 DEL ROUTER 1.

De la misma forma se realiza el envío de paquetes desde el Router 5 al Router 1 mediante el comando ping extendido, el mismo que tendrá un tamaño de 100 bytes y se repetirá 10 veces. El comando que se utilizó es el siguiente:

ping <ip a enviar> **size** <cantidad de bytes> **repeat** <número de secuencias>

Ilustración 51: *Ping desde Router 5 a Ethernet 4/0 del Router 1, topología túnel 6to4.*

```
R5#ping 2002:A00:101::1 size 100 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 2002:A00:101::1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 52/59/72 ms
R5#
```

Ilustración 52: *Ping desde Router 5 a Ethernet 4/0 del Router 1, topología túnel 6over4.*

```
R5#ping 1000:A00:101:1::2 size 100 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1000:A00:101:1::2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 48/57/64 ms
R5#
```

Ilustración 53: *Ping desde Router 5 a Ethernet 4/0 del Router 1, topología túnel GRE.*

```
R5#ping 1000:ABC:1:DCA::1 size 100 repeat 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1000:ABC:1:DCA::1, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 56/80/108 ms
R5#
```

Tabla 17: Comparativa de envío de paquetes entre el router 5 y router 1 con los túneles 6to4, 6over4 y GRE.

Características	6to4			6over4			GRE		
Secuencias	10			10			10		
Bytes	100			100			100		
Tiempo (ms)	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
	52	59	72	48	57	64	52	80	108
Paquetes Perdidos	0			0			0		
Tasa de Éxito (%)	100			100			100		

Tal y como se presenta en las ilustraciones 51,52 y 53, se observa el resultado que se obtiene cuando se aplicó el comando ping con los parámetros definidos, de los cuales se observa un envío de paquetes desde el router 5 hacia la dirección IP del puerto Ethernet4/0 del router 1 con los tres túneles seleccionados, esta puede ser verificada en la tabla 17. Además, se puede determinar que el Túnel que hace los envíos de paquetes entre interfaces de forma más rápida sigue siendo el Túnel 6over4, frente a los demás túneles.

3.2.3. PRUEBAS DE COMANDO PING DESDE LOS HOSTS

3.2.3.1. COMPARATIVA DEL HOST PC1 AL HOST PC3

En esta prueba se realiza un envió de 10 paquetes tipo ICMPv6, desde el host (PC1) del Router 1 al host (PC3) del Router 5. Para esto se utilizó el comando ping para las 3 topologías, el comando usa las variables "-l" para definir la cantidad de bytes y "-c" para definir la cantidad de paquetes a enviar. El comando es el siguiente:

```
ping <ip a enviar>  -l <cantidad de bytes>  -c <número de secuencias>
```

Luego de hacer uso de este comando tenemos como resultado lo que se muestra en las siguientes ilustraciones:

Ilustración 54: *Ping Host PC1 a Host PC3, topología túnel 6to4.*

```
PC1> ping 2002:a00:501::2 -l 100 -c 10

2002:a00:501::2 icmp6_seq=1 ttl=60 time=226.349 ms
2002:a00:501::2 icmp6_seq=2 ttl=60 time=136.445 ms
2002:a00:501::2 icmp6_seq=3 ttl=60 time=123.051 ms
2002:a00:501::2 icmp6_seq=4 ttl=60 time=121.513 ms
2002:a00:501::2 icmp6_seq=5 ttl=60 time=123.310 ms
2002:a00:501::2 icmp6_seq=6 ttl=60 time=121.675 ms
2002:a00:501::2 icmp6_seq=7 ttl=60 time=123.143 ms
2002:a00:501::2 icmp6_seq=8 ttl=60 time=122.192 ms
2002:a00:501::2 icmp6_seq=9 ttl=60 time=122.192 ms
2002:a00:501::2 icmp6_seq=10 ttl=60 time=122.959 ms
```

Ilustración 55: *Ping Host PC1 a Host PC3, topología túnel 6over4.*

```
PC1> ping 1000:abc:1:dcb::3 -l 100 -c 10

1000:abc:1:dcb::3 icmp6_seq=1 ttl=60 time=232.451 ms
1000:abc:1:dcb::3 icmp6_seq=2 ttl=60 time=122.659 ms
1000:abc:1:dcb::3 icmp6_seq=3 ttl=60 time=120.237 ms
1000:abc:1:dcb::3 icmp6_seq=4 ttl=60 time=120.805 ms
1000:abc:1:dcb::3 icmp6_seq=5 ttl=60 time=105.985 ms
1000:abc:1:dcb::3 icmp6_seq=6 ttl=60 time=122.395 ms
1000:abc:1:dcb::3 icmp6_seq=7 ttl=60 time=123.492 ms
1000:abc:1:dcb::3 icmp6_seq=8 ttl=60 time=121.685 ms
1000:abc:1:dcb::3 icmp6_seq=9 ttl=60 time=123.379 ms
1000:abc:1:dcb::3 icmp6_seq=10 ttl=60 time=122.792 ms
```

Ilustración 56: *Ping Host PC1 a Host PC3, topología túnel GRE.*

```
PC1> ping 1000:ABC:1:DCB::2 -l 100 -c 10

1000:ABC:1:DCB::2 icmp6_seq=1 ttl=60 time=241.537 ms
1000:ABC:1:DCB::2 icmp6_seq=2 ttl=60 time=122.249 ms
1000:ABC:1:DCB::2 icmp6_seq=3 ttl=60 time=120.829 ms
1000:ABC:1:DCB::2 icmp6_seq=4 ttl=60 time=121.192 ms
1000:ABC:1:DCB::2 icmp6_seq=5 ttl=60 time=123.612 ms
1000:ABC:1:DCB::2 icmp6_seq=6 ttl=60 time=121.191 ms
1000:ABC:1:DCB::2 icmp6_seq=7 ttl=60 time=122.290 ms
1000:ABC:1:DCB::2 icmp6_seq=8 ttl=60 time=122.915 ms
1000:ABC:1:DCB::2 icmp6_seq=9 ttl=60 time=120.944 ms
1000:ABC:1:DCB::2 icmp6_seq=10 ttl=60 time=121.515 ms
```

Observando las ilustraciones 54, 55 y 56 se observa que los paquetes enviados poseen los mismos parámetros, pero para el análisis de rendimiento de cada túnel se debe calcular de forma manual.

En base a los datos obtenidos en las pruebas de host, se los va a representar en una tabla, donde nos permitirá establecer los valores de cada uno de los parámetros en relación a los paquetes enviados de un host a otro.

Tabla 18: *Comparativa de envío de paquetes entre Host PC1 y Host PC3.*

Características	**6to4**			**6over4**			**GRE**		
Secuencias	10			10			10		
Bytes	100			100			100		
Tiempo de espera (ms)	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
	121.513	134.283	226.349	105.985	131.588	232.451	120.829	133.827	241.537
Paquetes Perdidos	0			0			0		
Tipo de Paquetes	ICMPv6			ICMPv6			ICMPv6		
TTL	60			60			60		

En la tabla 18 se puede notar los parámetros utilizados para el envío de paquetes de tipo ICMPv6, así mismo como los tiempos de espera en mínimos, medios y máximos.

En la prueba realizada, se muestra que el TTL de los tres túneles son iguales. Dados los resultados de los tiempos de espera, se observa que el túnel 6over4 es el túnel que hace el envío de paquetes de manera rápida, frente al túnel GRE y 6to4.

3.2.3.2. COMPARATIVA DEL HOST PC4 AL HOST PC2

De igual manera en esta prueba se realiza un envió de 10 paquetes tipo ICMPv6, desde el host (PC4) del Router 5 al host (PC2) del Router 1. Para esto se utilizó el comando ping para las 3 topologías, el comando usa las variables “-l” para definir la cantidad de bytes y “-c” para definir la cantidad de paquetes a enviar. El comando es el siguiente:

```
ping <ip a enviar>  -l <cantidad de bytes>  -c <número de secuencias>
```

Luego de hacer uso de este comando tenemos como resultado lo que se muestra en las siguientes ilustraciones:

Ilustración 57: *Ping Host PC4 a Host PC2, topología túnel 6to4.*

```
PC4> ping 2002:a00:101::3 -l 100 -c 10

2002:a00:101::3 icmp6_seq=1 ttl=60 time=182.440 ms
2002:a00:101::3 icmp6_seq=2 ttl=60 time=122.598 ms
2002:a00:101::3 icmp6_seq=3 ttl=60 time=122.034 ms
2002:a00:101::3 icmp6_seq=4 ttl=60 time=120.347 ms
2002:a00:101::3 icmp6_seq=5 ttl=60 time=125.434 ms
2002:a00:101::3 icmp6_seq=6 ttl=60 time=122.167 ms
2002:a00:101::3 icmp6_seq=7 ttl=60 time=122.645 ms
2002:a00:101::3 icmp6_seq=8 ttl=60 time=121.848 ms
2002:a00:101::3 icmp6_seq=9 ttl=60 time=123.629 ms
2002:a00:101::3 icmp6_seq=10 ttl=60 time=123.994 ms
```

Ilustración 58: *Ping Host PC4 a Host PC2, topología túnel 6over4.*

```
PC4> ping 1000:ABC:1:DCA::3 -l 100 -c 10

1000:ABC:1:DCA::3 icmp6_seq=1 ttl=60 time=121.495 ms
1000:ABC:1:DCA::3 icmp6_seq=2 ttl=60 time=122.027 ms
1000:ABC:1:DCA::3 icmp6_seq=3 ttl=60 time=123.882 ms
1000:ABC:1:DCA::3 icmp6_seq=4 ttl=60 time=122.832 ms
1000:ABC:1:DCA::3 icmp6_seq=5 ttl=60 time=122.771 ms
1000:ABC:1:DCA::3 icmp6_seq=6 ttl=60 time=122.564 ms
1000:ABC:1:DCA::3 icmp6_seq=7 ttl=60 time=121.783 ms
1000:ABC:1:DCA::3 icmp6_seq=8 ttl=60 time=123.158 ms
1000:ABC:1:DCA::3 icmp6_seq=9 ttl=60 time=121.771 ms
1000:ABC:1:DCA::3 icmp6_seq=10 ttl=60 time=122.955 ms
```

Ilustración 59: *Ping Host PC4 a Host PC2, topología túnel GRE.*

```
PC4> ping 1000:ABC:1:DCA::2 -l 100 -c 10

1000:ABC:1:DCA::2 icmp6_seq=1 ttl=60 time=226.638 ms
1000:ABC:1:DCA::2 icmp6_seq=2 ttl=60 time=137.032 ms
1000:ABC:1:DCA::2 icmp6_seq=3 ttl=60 time=120.461 ms
1000:ABC:1:DCA::2 icmp6_seq=4 ttl=60 time=120.954 ms
1000:ABC:1:DCA::2 icmp6_seq=5 ttl=60 time=121.161 ms
1000:ABC:1:DCA::2 icmp6_seq=6 ttl=60 time=126.374 ms
1000:ABC:1:DCA::2 icmp6_seq=7 ttl=60 time=122.285 ms
1000:ABC:1:DCA::2 icmp6_seq=8 ttl=60 time=122.100 ms
1000:ABC:1:DCA::2 icmp6_seq=9 ttl=60 time=120.554 ms
1000:ABC:1:DCA::2 icmp6_seq=10 ttl=60 time=122.548 ms
```

Observando las ilustraciones 57, 58 y 59 se observa que los paquetes enviados poseen los mismos parámetros, pero para el análisis de rendimiento de cada túnel se debe calcular de forma manual.

En base a los datos obtenidos en las pruebas de host, se los va a representar en una tabla, donde nos permitirá establecer los valores de cada uno de los parámetros en relación a los paquetes enviados de un host a otro.

Tabla 19: *Comparativa de envío de paquetes entre Host PC4 y Host PC2.*

Características	**6to4**			**6over4**			**GRE**		
Secuencias	10			10			10		
Bytes	100			100			100		
Tiempo (ms)	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
	120.347	128.714	182.440	121.495	122.523	123.882	120.461	134.011	226.638
Paquetes Perdidos	0			0			0		
Tipo de Paquetes	ICMPv6			ICMPv6			ICMPv6		
TTL	60			60			60		

De igual manera en la tabla 19 se puede notar los parámetros utilizados para el envío de paquetes de tipo ICMPv6, así mismo como los tiempos de espera en mínimos, medios y máximos.

En la prueba realizada, se muestra que el TTL es igual en los tres túneles son iguales.

Dados los resultados de los tiempos de espera, se observa que el túnel 6over4 es el túnel que hace el envío de paquetes de manera más rápida, frente a los túneles 6to4 y GRE.

En relación a las dos comparativas, los resultados obtenidos en las pruebas realizadas mediante el envío de paquetes ICMPv6 a través de la herramienta ping que fue utilizado en las tres topologías, se llega a la conclusión que al realizar el envío de paquetes el túnel 6over4 es aquel que posee ventaja en cuanto al tiempo de espera con respecto al túnel 6to4 y GRE, por lo tanto, se establece que el mejor rendimiento y comunicación es el túnel 6over4. En cuanto a características en general como implementación, mantenimiento y recursos el mejor mecanismo de túnel es 6to4, por ello es el más utilizado a nivel mundial.

3.3. CONCLUSIONES

- Debido al gran incremento de tráfico en la red, ha permitido que los mecanismos de túneles de transición vayan desarrollándose con la finalidad de mejorar la interconexión en las redes IPv4 e IPv6.
- Mediante la descripción de las principales ventajas, desventajas y características de los mecanismos de túneles, se logró tener una idea más clara de los beneficios que podrían brindar dentro de una infraestructura de red, al momento de hacer la transición de IPv4 a IPv6.
- Se hizo la selección de tres mecanismos de túneles según sus características para la emulación y análisis de resultados mediante la realización de las pruebas experimentales.
- Se usó las interfaces seriales para la conexión entre enrutadores, también se utilizó interfaces ethernet para interconectar enrutadores y dispositivos finales, teniendo de esta manera una topología con diferentes enlaces lo que se conoce como topología mixta.
- Los tiempos de espera al hacer el envío de paquetes ICMPv6 en el mecanismo de túnel 6over4 son menores respecto de los otros estudiados, mientras que otras características como recursos, implementación, mantenimiento favorecen al túnel 6to4.

3.4. RECOMENDACIONES

- Realizar una indagación más profunda en diversas fuentes bibliográficas confiables para enriquecer el conocimiento adquirido.
- Al momento de emular enrutadores Cisco en GNS3 es recomendable tener en cuenta los IOS que se van a utilizar para que sean compatibles con el emulador, investigar los recursos que estos consumirán del computador, para evitar inconvenientes al momento de la configuración e instalación.
- Al realizar las pruebas de análisis para la comparación de los mecanismos de túneles, se recomienda, que se haga uso de los mismos equipos en el emulador para los tres mecanismos, de esta forma se podrá garantizar que los resultados sean posibles de analizar correctamente.
- En futuros trabajos realizar estudios, configuración y pruebas relacionadas a la seguridad que ayuden a garantizar la entrega de paquetes, y así evitar que los atacantes vulneren a los mecanismos de túneles y accedan a la información compartida por medio de estos.

BIBLIOGRAFÍA

[1] A. Zakari, M. Musa, G. Bekaroo, S. A. Bala, I. A. T. Hashem, y S. Hakak, «IPv4 and IPv6 Protocols: A Comparative Performance Study», 2019, pp. 1-4. doi: 10.1109/ICSGRC.2019.8837050.

[2] A. Salinas González, A. Escobar Díaz, y H. Vacca González, «Technological transition from IPv4 to IPv6 at SNR: A success case: Transición tecnológica de IPv4 a IPv6 en SNR: un caso de éxito.», *Transição Tecnológica IPv4 Para O IPv6 Em SNR Uma História Sucesso*, vol. 17, n.º 2, pp. 1-28, may 2021, doi: 10.16925/2357-6014.2021.02.12.

[3] L. Y. B. Sánchez, B. V. Suárez, S. S. Pareja, y J. J. P. Aguilar, «Uso de Mininet y Openflow 1.3 para la enseñanza e investigación en redes IPv6 definidas por software», *Rev. Educ. En Ing.*, vol. 12, n.º 24, pp. 89-96, 2017.

[4] K.-H. Li y K.-Y. Wong, «Empirical Analysis of IPv4 and IPv6 Networks through Dual-Stack Sites», *Information*, vol. 12, n.º 246, p. 246, jun. 2021, doi: 10.3390/info12060246.

[5] S. S. Tomar, A. Rawat, S. Tokekar, y P. D. Vyavahare, «Investigations on equal cost multi-path feature in dynamic routing protocols in IPv6 networks», presentado en 2019 IEEE Conference on Information and Communication Technology, CICT 2019, 2019. doi: 10.1109/CICT48419.2019.9066199.

[6] B. R. Dawadi, D. B. Rawat, y S. R. Joshi, «Software Defined IPv6 Network: A New Paradigm for Future Networking», *J. Inst. Eng.*, vol. 15, n.º 2, pp. 1-13, jul. 2019.

[7] D. G. C. Méndez, A. S. C. Barahona, P. M. M. Naranjo, y H. M. V. Yánez, «Implementación de un prototipo como sistema detector de intrusos para detectar ataques dirigidos al protocolo ipv6 desarrollado con herramientas open source», *Cumbres*, vol. 3, n.º 2, pp. 129-141, 2017.

[8] I. J. Okonkwo y I. D. Emmanuel, «Comparative study of EIGRP and OSPF protocols based on network convergence», *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, n.º 6, pp. 39-45, 2020, doi: 10.14569/IJACSA.2020.0110605.

[9] B. Korniyenko, L. Galata, y L. Ladieva, «Research of Information Protection System of Corporate Network Based on GNS3», 2019, pp. 244-248. doi: 10.1109/ATIT49449.2019.9030472.

[10] M. A. Calle, J. D. Tovar, Y. J. C. Pino, y J. C. Cuéllar, «Comparación de parámetros para una selección apropiada de herramientas de simulación de redes», *Inf. Tecnológica*, vol. 29, n.º 6, pp. 253-266, 2018.

[11] E. Chua, A. Magbag, A. T. Manaloto, M. J. Rabena, y M. R. Rodavia, «Comparative Study on Networking Simulation Tools Using Correlation Analysis», 2018, pp. 123-127. doi: 10.1109/ISET.2018.00035.

[12] S. Liu, H. Wang, J. Liu, y M. Xian, «Feasibility analysis of network security teaching platform based on KVM and GNS3», 2019, pp. 310-313. doi: 10.1109/ITCA49981.2019.00075.

[13] G. Bagyalakshmi *et al.*, «Network Vulnerability Analysis on Brain Signal/Image Databases Using Nmap and Wireshark Tools», *Ieee Access*, vol. 6, pp. 57144-57151, 2018, doi: 10.1109/ACCESS.2018.2872775.

[14] «Tema 2. Redes de comunicación: Topología y enlaces.» 2017. [En línea]. Disponible en: https://www.uv.es/rosado/courses/sid/Capitulo2_rev0.pdf

[15] M. R. A. Ahmed y S. S. A. Shaikhedris, «Network Migration and Performance Analysis of IPv4 and IPv6», presentado en Proceedings of: 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering, ICCCEEE 2020, 2021. doi: 10.1109/ICCCEEE49695.2021.9429664.

[16] D. E. Idrissi, N. Elkamoun, y R. Hilal, «Study of the impact of the transition from IPv4 to IPv6 based on the tunneling mechanism in mobile networks», *Procedia Comput. Sci.*, vol. 191, pp. 207-214, ene. 2021, doi: 10.1016/j.procs.2021.07.026.

[17] S. A. Abdulla, «Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms», *Int. J. Secur. Netw.*, vol. 12, n.º 2, pp. 83-102, 2017, doi: 10.1504/IJSN.2017.083830.

[18] J. M. V. Ruiz, C. S. Cardenas, y J. L. M. Tapia, «Implementation and testing of IPv6 transition mechanisms», 2017, vol. 2017-January, pp. 1-6. doi: 10.1109/LATINCOM.2017.8240145.

[19] S. E.S.G.S y M. Haji, «Analysis Tunneling IPv4 and IPv6 on VoIP Network», *Kinet. Game Technol. Inf. Syst. Comput. Netw. Comput. Electron. Control*, vol. 3, oct. 2018, doi: 10.22219/kinetik.v3i4.708.

[20] A. M. Hirzan, N. Bahaman, y W. Adhiwibowo, «Voice Over Internet Protocol Performance Evaluation in 6to4 Tunneling Network», *J. Transform.*, vol. 18, p. 108, ago. 2020, doi: 10.26623/transformatika.v18i1.2356.

[21] M. S. Ali y T. A. Yahiya, «Performance Analysis of Native Ipv4/Ipv6 Networks Compared to 6to4 Tunnelling Mechanism», 2018, pp. 250-255. doi: 10.1109/ICOASE.2018.8548911.

[22] K. El Khadiri, O. Labouidya, N. Elkamoun, y R. Hilal, «Performance evaluation of IPv4/IPv6 transition mechanisms for real-time applications using OPNET Modeler», *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, n.º 4, pp. 387-392, 2018, doi: 10.14569/IJACSA.2018.090454.

[23] T. Saraj, A. Hanan, M. S. Akbar, M. Yousaf, A. Qayyum, y M. Tufail, «IPv6 tunneling protocols: Mathematical and testbed setup performance analysis», 2016, pp. 62-68. doi: 10.1109/CIACS.2015.7395568.

[24] S. Singalar y R. M. Banakar, «Performance Analysis of IPv4 to IPv6 Transition Mechanisms», presentado en Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018, 2018. doi: 10.1109/ICCUBEA.2018.8697539.

[25] Z. Ashraf y M. Yousaf, «Optimized convergence of OsPFv3 in large scale hybrid IPv4-IPv6 network», presentado en 2018 14th International Conference on Emerging Technologies, ICET 2018, 2019. doi: 10.1109/ICET.2018.8603633.

[26] D. E. Kurniawan, N. C. Kushardianto, y A. H. Thohari, «Simulation and Analysis Network Performance of IPv4, IPv6 and ISATAP Tunneling on Polibatam Network Laboratory», presentado en Proceedings of the 2019 2nd International Conference on Applied Engineering, ICAE 2019, 2019. doi: 10.1109/ICAE47758.2019.9221668.

[27] Y. Sookun y V. Bassoo, «Performance analysis of IPv4/IPv6 transition techniques», 2016, pp. 188-193. doi: 10.1109/EmergiTech.2016.7737336.

[28] G. K. Ordabayeva, M. Othman, B. Kirgizbayeva, Z. D. Iztaev, y A. Bayegizova, «A systematic review of transition from IPV4 to IPV6», presentado en ACM International Conference Proceeding Series, 2020. doi: 10.1145/3410352.3410735.

[29] R. Munadi, D. D. Sanjoyo, D. Perdana, y F. Adjie, «Performance analysis of tunnel broker through open virtual private network», *Telkomnika Telecommun. Comput. Electron. Control*, vol. 17, n.º 3, pp. 1185-1192, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12231.

[30] M. M. Chinguel Rodríguez, «Revisión Sistemática de los mecanismo de Transición para la Migración de IPv4-IPv6», 2019, [En línea]. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6214/Chinguel%20Rodriguez%20Milagros%20Maribel.pdf?sequence=1

[31] A. A. Castro, G. D. S. Marín, G. L. A. Méndez, y C. E. S. Forero, «A Preliminary Study of Routing Protocols in a Tactical Data Link Ad Hoc Network in Colombian Maritime Scenario», *Ship Sci. Technol.*, vol. 14, n.º 27, pp. 75-92, 2020.

[32] J. Tang, «Research on IPv6 Protocol Transition Mechanism», 2021, pp. 702-705. doi: 10.1109/ICSP51882.2021.9408680.

[33] R. K. Cv y H. Goyal, «IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark», presentado en Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019, 2019. doi: 10.1109/ViTECoN.2019.8899746.

[34] K. El Khadiri, O. Labouidya, N. E. Kamoun, y R. Hilal, «Study of the impact of routing on the performance of IPv4/IPv6 transition mechanisms», *Lect. Notes Netw. Syst.*, vol. 66, pp. 43-51, 2019, doi: 10.1007/978-3-030-11914-0_5.

[35] D. el Idrissi, N. EL KAMOUN, y H. Rachid, «Study of the impact of failure on GRE Tunnel», oct. 2019, pp. 1-4. doi: 10.1109/CMT.2019.8931368.

[36] H. Karna, V. Baggan, K. Ashok, A. Sahoo, K. Pradeepta, y Dr. P. Sarangi, «Performance Analysis of Interior Gateway Protocols (IGPs) using GNS-3», nov. 2019.

[37] N. Jain y A. Payal, «Comparison between IPv4 and IPv6 using OSPF and OSPFv3 on Riverbed Modeler», 2019, vol. 2019-December. doi: 10.1109/ANTS47819.2019.9118101.

[38] R. Mehra y K. V. Krishnan, «Analyzing security attack on layer 2 and comparing the performance of different routing protocols», 2018, pp. 611-616. doi: 10.1109/RTEICT42901.2018.9012126.

[39] J. V. J. S., S. Kumar, A. K. Sahoo, y V. Kumar, «Performance Evaluation Of OSPFv3 Routing Protocol On IPv6 Heterogeneous Network», *Int. J. Recent Res. Asp.*, vol. 5, n.º 1, pp. 270-275, mar. 2018.

[40] «Performance Evaluation and Comparison of Dynamic Routing Protocols for Suitability and Reliability-Web of Science Core Collection». https://www.webofscience.com/wos/woscc/full-record/WOS:000443939400005 (accedido 17 de febrero de 2022).

[41] F. Z. Sinthia, A. Nasir, B. Paul, M. R. A. Rashid, y M. N. Adnan, «Implementation of OSPFv3 in IPv4 and IPv6 for Establishing a Wide Area Network», *Adv. Intell. Syst. Comput.*, vol. 1270, pp. 473-481, 2021, doi: 10.1007/978-981-15-8289-9_46.

[42] W. Indra y F. Alex, «QoS Analysis on OSPFv3 And RIPng Using GRE Tunneling on IPv6 Integrated Ipv4 Network», *MATEC Web Conf.*, vol. 215, p. 01005, ene. 2018, doi: 10.1051/matecconf/201821501005.

[43] K. E. Khadiri, O. Labouidya, N. Elkamoun, y R. Hilal, «Comparative Study between Dynamic IPv6 Routing Protocols of Distance Vectors and Link States», presentado en Proceedings - 2018 International Conference on Wireless Networks and Mobile Communications, WINCOM 2018, 2019. doi: 10.1109/WINCOM.2018.8629745.

[44] J. U. N. Tao, M. I. N. Du, y Y. U. E. Wu, «Design and discussion of network engineering teaching experiment based on 6to4 tunnel», 2020, pp. 54-58. doi: 10.1145/3447490.3447501.

[45] J. O. Zamora, J. J. G. Merino, J. D. L. Martí, V. A. Baeza, I. S. Gadea, y E. R. Carrero, «Creación de nuevos escenarios prácticos para redes de comunicación», en *Memòries del Programa de Xarxes-I3CE de qualitat, innovació i investigació en docència universitària: convocatòria 2018-19, 2019, ISBN 978-84-09-15746-4, pág. 305*, 2019, p. 305. Accedido: 17 de febrero de 2022. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7244245