RESUMEN – TRABAJO DE GRADO

AUTORES	Giniva Alejandra Coronel Coronel Cristian Fabian Sanchez Sanchez
FACULTAD	Facultad de Ingenierías
PLAN DE ESTUDIOS	Ingeniería de Sistemas
DIRECTOR	Fabian Ranulfo Cuesta Quintero
CODIRECTOR (si aplica)	No aplica
TÍTULO DE LA TESIS	Implementación de un prototipo de infraestructura de red IPv6 escalable y seguro en entornos de laboratorio para fortalecer ambientes de simulación en instituciones académicas
TITULO EN INGLES	Implementation of a scalable and secure IPv6 network infrastructure prototype in laboratory environments to strengthen simulation environments in academic institutions

RESUMEN
(70 palabras)

Este proyecto implementa un prototipo de infraestructura de red IPv6 escalable y segura en un entorno de laboratorio académico. Se diseñó una topología jerárquica con enrutamiento dinámico, túneles IPv6 sobre IPv4, VLAN y listas de control de acceso. Las pruebas demostraron conectividad estable, baja latencia y correcta propagación de rutas, validando su funcionalidad y escalabilidad. El modelo es replicable y fortalece la formación práctica en redes de estudiantes.

RESUMEN EN INGLES

This project implements a prototype of a scalable and secure IPv6 network infrastructure in an academic laboratory environment. A hierarchical topology was designed with dynamic routing, IPv6 tunnels over IPv4, VLANs, and access control lists. Testing demonstrated stable connectivity, low latency, and accurate route propagation, validating its functionality and scalability. The model is replicable and enhances students' hands-on networking training.

PALABRAS CLAVES	IPv6, Escalabilidad, VLAN, ACL, Redes académicas.
PALABRAS CLAVES EN INGLES	IPv6, Scalability, VLAN, ACL, Academic Networks.

CARACTERÍSTICAS

PÁGINAS: 62	PLANOS:	ILUSTRACIONES: 14	CD-ROM:

Implementación de un prototipo de infraestructura de red IPv6 escalable y seguro en entornos de laboratorio para fortalecer ambientes de simulación en instituciones académicas

Giniva Alejandra Coronel Coronel

Cristian Fabian Sánchez Sánchez

Faculta de Ingenierías, Universidad Francisco de Paula Santander Ocaña

Ingeniería de Sistemas

Magister Fabián Cuesta Quintero

20 de noviembre de 2025

Índice

1. Implementación de un prototipo de infraestructura de red IPv6 escalable y seguro en entornos de laboratorio para fortalecer ambientes de simulación en instituciones académicas. 8

1.1 Planteamiento del problema 8

1.2 Formulación del problema 9

1.3 Objetivos 9

1.3.1 Objetivo General *9*

1.3.2 Objetivos específicos *10*

1.4 Justificación 10

1.5 Delimitaciones 13

1.5.1 Delimitación Geográfica *13*

1.5.2 Delimitación Temporal *13*

1.5.3 Delimitación Conceptual *13*

1.5.4 Delimitación Operativa *14*

2. Marco Referencial 15

2.1 Marco histórico 15

2.1.1 Antecedentes a Nivel Internacional 16

2.1.2 Antecedentes a Nivel Nacional 18

2.1.3 Antecedentes a Nivel Regional *20*

2.2 Marco Contextual 21

2.3 Marco Conceptual 22

2.3.1 Red de datos 22

2.3.2 Seguridad en la red 22

2.3.3 Modelo de referencia 23
2.3.4 Escalabilidad 24
2.3.5 Infraestructura de red 25
2.3.6 Protocolo de Internet IPV4 / IPV6 25
2.3.7 ACL 26
2.3.8 Seguridad Informática 26
2.3.9 VLAN *27*
2.4 Marco Teórico 28
2.5 Marco Legal 30
2.5.1 Plan Nacional de Transición a IPv6 30
2.5.2 Ley 1341 de 2009 – Ley TIC 30
2.5.3 Resoluciones del MinTIC sobre infraestructura TIC 30
2.5.4 Generales-RITEL-Aclaración adopción a protocolo IPV6. ..... *31*
3. Diseño Metodológico 32
3.1 Tipo de Investigación 32
3.2 Población y muestra 32
3.2.1 Población 32
3.2.2 Muestra *33*
3.3 Diseño de instrumentos de recolección de la información y técnicas de análisis de datos. 33
3.4 Análisis de la información 33
4. Resultados 35
4.1 Diseño de la topología de red y definición de los componentes necesarios para la implementación de una infraestructura escalable basada en IPv6 en entornos de laboratorio. 35

4.1.1 Segmento de Oficina Central..... 37

4.1.2 Núcleo de la Infraestructura ISP..... 38

4.1.3 Oficina Remota..... 39

4.1.4 Descripción académica de la configuración de los routers en el prototipo IPv6..... 39

4.1.4.1 Router 0 – Gateway de la Oficina Central. El Router 0 actúa como el punto de salida del dominio local ubicado en la Oficina Central. Su configuración habilita:..... 40

4.1.4.2 Router 1 – Router Perimetral de la Oficina Central. Este router interconecta la oficina central con el ISP, traduciendo condiciones de laboratorio a escenarios reales de borde de red. 41

4.1.4.5 Router 3 – Núcleo del ISP (Backbone). Este dispositivo se configura únicamente con IPv4 y OSPF, simulando la infraestructura de un proveedor real que aún no migra a IPv6. 43

4.1.4.6 Router 4 – Router Perimetral de la Oficina Remota. Este equipo conecta la oficina remota al ISP y recibe el extremo del túnel IPv6. 44

4.1.4.7 Router 5 – Distribución IPv6 de la Oficina Remota. Este router extiende la red hacia el segmento final de la oficina remota..... *46*

4.2 Configuración del mecanismo de segmentación dinámica mediante VLAN y control de acceso mediante ACL, asegurando la seguridad y la eficiencia en la gestión del tráfico de datos en el prototipo de laboratorio. 48

4.2.1 Segmentación lógica y esquema de direccionamiento del switch de acceso 48

4.2.2 Configuración de VLAN y dominio de broadcast..... *48*

4.3 Realización de pruebas de desempeño al prototipo en términos de escalabilidad, seguridad y funcionalidad, validando su capacidad para fortalecer los ambientes de simulación en instituciones académicas. 50

5. Conclusiones 55

Referencias 56

Lista de Tablas

Pág.

Tabla 1. Dispositivos requeridos..... 35

Tabla 2. Arquitectura de enrutamiento 36

Lista de Figuras

Pág.

Figura 1. Modelos de Referencias 23

Figura 2. Escalabilidad en las redes 24

Figura 3. Red con VLAN 27

Figura 4 Diseño de topología de red. 36

Figura 5. Red Oficina Central 37

Figura 6. Núcleo Infraestructura ISP 38

Figura 7. Red Oficina Remota 39

Figura 8. Configuración Vlan 99 Administración 49

Figura 9. Uso del comando show ip interface brief router 0 50

Figura 10. Uso del comando show ip interface brief router 4 50

Figura 11. Uso del comando show interface tunnel 0 Router1 51

Figura 12. Uso del comando show interface tunnel 0 Router3 52

Figura 13. Uso del comando show IP OSPF Neighbor en los Routers 1 52

Figura 14. Uso del comando show IP OSPF Neighbor en el ISP 53

Figura 15. Uso del comando show IP OSPF Neighbor en los Routers 3 53

1. Implementación de un prototipo de infraestructura de red IPv6 escalable y seguro en entornos de laboratorio para fortalecer ambientes de simulación en instituciones académicas.

1.1 Planteamiento del problema

En el contexto educativo actual, las instituciones académicas enfrentan el desafío de ofrecer ambientes de simulación realistas y efectivos para la formación de estudiantes en áreas relacionadas con redes y telecomunicaciones. La rápida evolución de las tecnologías de red, particularmente la transición hacia IPv6 como estándar global, requiere que las universidades y centros de formación cuenten con infraestructuras que no solo sean funcionales, sino también escalables y seguras. Sin embargo, en muchos casos, las redes en entornos de laboratorio no están diseñadas para simular escenarios reales de producción, lo que limita la calidad de la enseñanza y la preparación de los estudiantes para los desafíos del mundo laboral (Cisco Networking Academy , 2021)

La implementación de redes con IPv6 en ambientes académicos presenta barreras importantes, entre ellas, la complejidad técnica de su configuración, la necesidad de integrar mecanismos de segmentación dinámica como VLAN y la aplicación de controles de acceso avanzados mediante listas de control de acceso (ACL). Estas características son esenciales para garantizar la seguridad y la eficiencia en el manejo del tráfico de datos, especialmente en redes que buscan replicar las condiciones reales de una infraestructura corporativa o institucional (Garimella, Yu-Wei , Nan , & Sanjay, 2007)

Además, muchas instituciones académicas enfrentan restricciones presupuestarias y técnicas, lo que dificulta la implementación de redes modernas y escalables. Esto pone en evidencia la necesidad de desarrollar prototipos que permitan aprovechar los recursos disponibles mientras se simulan condiciones reales de redes empresariales. Este vacío en la integración de soluciones IPv6 avanzadas y accesibles en entornos de laboratorio limita la capacidad de los estudiantes para adquirir competencias técnicas relevantes en un mercado laboral cada vez más competitivo.

1.2 Formulación del problema

¿Cómo diseñar e implementar un prototipo de infraestructura de red IPv6 que sea escalable y seguro, capaz de integrar segmentación dinámica mediante VLAN y mecanismos de control de acceso avanzados con ACL, para fortalecer los ambientes de simulación en instituciones académicas?

1.3 Objetivos

1.3.1 Objetivo General

Implementar un prototipo de infraestructura de red IPv6 escalable y seguro en entornos de laboratorio para fortalecer ambientes de simulación en instituciones académicas.

1.3.2 Objetivos específicos

Diseñar la topología de red y definir los componentes necesarios para la implementación de una infraestructura escalable basada en IPv6 en entornos de laboratorio.

Configurar mecanismos de segmentación dinámica mediante VLAN y control de acceso mediante ACL, asegurando la seguridad y la eficiencia en la gestión del tráfico de datos en el prototipo de laboratorio.

Realizar pruebas de desempeño al prototipo en términos de escalabilidad, seguridad y funcionalidad, validando su capacidad para fortalecer los ambientes de simulación en instituciones académicas.

1.4 Justificación

La transición hacia el protocolo IPv6 se ha convertido en un estándar indispensable para garantizar la escalabilidad y el funcionamiento adecuado de las redes modernas. Según la (Internet society, 2021), el agotamiento de las direcciones IPv4 ha impulsado la adopción global de IPv6, el cual no solo amplía la capacidad de direccionamiento, sino que también mejora aspectos clave como la seguridad, el rendimiento y la conectividad en redes complejas. En este contexto, las instituciones académicas enfrentan el desafío de preparar a los estudiantes con competencias prácticas en el diseño, configuración y gestión de infraestructuras IPv6, que son cada vez más demandadas en el mercado laboral.

A pesar de su importancia, muchos entornos académicos carecen de infraestructuras de laboratorio que simulen escenarios reales, lo que limita la formación práctica de los estudiantes. (Cisco Networking Academy , 2021), señala que el aprendizaje basado en simulaciones prácticas mejora significativamente la adquisición de habilidades técnicas, especialmente en redes

avanzadas. Sin embargo, las limitaciones presupuestarias y técnicas dificultan la implementación de infraestructuras escalables y seguras que integren tecnologías como VLAN, ACL y el protocolo IPv6.

El desarrollo de un prototipo de red escalable y seguro para entornos de laboratorio no solo abordará estas carencias, sino que también permitirá simular entornos reales de producción, fortaleciendo los ambientes de simulación en instituciones académicas. Según Chowdhury, Chakraborty y Biswas (2020), la implementación de segmentación dinámica mediante VLAN y el control de acceso con ACL son esenciales para garantizar la seguridad y eficiencia en redes modernas. Además, estos mecanismos ayudan a replicar condiciones reales en un ambiente controlado, preparando a los estudiantes para enfrentar escenarios complejos en su vida profesional.

Por otra parte, un prototipo bien diseñado contribuye al desarrollo de competencias alineadas con las necesidades de la Cuarta Revolución Industrial, donde la conectividad y la ciberseguridad son elementos clave. De acuerdo con Valdez y Álvarez (2020), la implementación de soluciones innovadoras en la formación académica fomenta no solo la adquisición de habilidades técnicas, sino también la capacidad de los estudiantes para resolver problemas reales de manera efectiva.

Este proyecto, por lo tanto, no solo responde a una necesidad académica, sino que también tiene un impacto social y tecnológico, ya que permite mejorar la calidad de la enseñanza, aumentar la competitividad de los egresados y, en última instancia, contribuir al desarrollo de soluciones tecnológicas sostenibles.

La justificación de este proyecto radica en varios puntos clave:

Relevancia Académica. Los laboratorios de redes en instituciones educativas suelen carecer de una infraestructura que simule condiciones reales, lo que limita la formación técnica avanzada. (Cisco Networking Academy , 2021) indica que los estudiantes expuestos a entornos de simulación realista desarrollan habilidades más profundas en diseño y gestión de redes. Este proyecto permitirá a los estudiantes trabajar con tecnologías emergentes, como IPv6, segmentación dinámica mediante VLAN y seguridad avanzada con ACL, proporcionando un entorno de aprendizaje que refleje escenarios del mundo laboral.

Escalabilidad y Sostenibilidad. La escalabilidad es un aspecto crucial en redes modernas, y la implementación de este prototipo permitirá a las instituciones académicas optimizar recursos existentes y ampliar capacidades según las necesidades futuras. Además, al integrar IPv6, el prototipo fomenta la sostenibilidad tecnológica, alineándose con las metas de modernización digital y reducción de la obsolescencia tecnológica (Internet society, 2021)

Impacto en la Seguridad. La seguridad es una preocupación crítica en redes actuales. El uso de listas de control de acceso (ACL) para limitar el tráfico no autorizado y de VLAN para segmentar la red son prácticas esenciales en infraestructuras modernas. Según Chowdhury et al. (2020), estas técnicas no solo mejoran la protección de los datos, sino que también optimizan el rendimiento de la red, al permitir un manejo eficiente del tráfico. Este proyecto proporcionará un modelo seguro para proteger redes educativas de ataques y accesos no deseados.

Alineación con los Objetivos Educativos. El proyecto contribuye al fortalecimiento de ambientes de simulación en instituciones académicas, mejorando la calidad educativa y fomentando competencias en áreas clave como la conectividad, la ciberseguridad y la gestión de redes. Esto impacta directamente en la preparación de los estudiantes para satisfacer las

demandas del mercado laboral, especialmente en un contexto donde la Cuarta Revolución Industrial requiere habilidades técnicas avanzadas (Valdez & Álvarez, 2020).

Beneficio Social y Tecnológico. La implementación de este prototipo no solo mejora la enseñanza técnica, sino que también tiene implicaciones sociales significativas. Al formar estudiantes con competencias relevantes, se contribuye al desarrollo de una fuerza laboral altamente capacitada, lo que impulsa el progreso tecnológico en la región y fortalece las capacidades institucionales para innovar. Además, este modelo puede ser replicado en otras instituciones educativas, ampliando su alcance e impacto.

1.5 Delimitaciones

1.5.1 Delimitación Geográfica

La siguiente investigación se desarrolló en la Universidad Francisco de Paula Santander Ocaña.

1.5.2 Delimitación Temporal

El desarrollo de la investigación tuvo un tiempo estipulado de 6 meses a partir de la aprobación del anteproyecto por parte del Comité Curricular.

1.5.3 Delimitación Conceptual

Para una mayor comprensión de la presente investigación, se profundizó en los siguientes conceptos: seguridad informática, IPv6, ACL, VLAN, Simulación.

1.5.4 Delimitación Operativa

La presente investigación se encaminó en realizar la implementación de un prototipo de infraestructura de red IPv6 escalable y seguro en entornos de laboratorio para fortalecer ambientes de simulación en instituciones académicas en el laboratorio de redes y telecomunicaciones del Departamento Sistemas e Informática.

2. Marco Referencial

2.1 Marco histórico

De acuerdo a (Lacnic, 2025) IPv6 es la última versión del Internet Protocol (IP) en el cual se sustenta la operación de Internet. Las especificaciones técnicas básicas de IPv6 se desarrollaron en la década de los 90s en el IETF (Internet Engineering Task Force). Al día de hoy el protocolo sigue añadiendo nuevas funcionalidades y se le considera un protocolo lo suficientemente maduro para soportar la operación de Internet en sustitución de IPv4.

El diseño de IPv6 comenzó a principios de la década de 1990. Publicada en 1995, la RFC 1752 fue la primera RFC sobre IPv6. En ese momento se llamaba IPng (next generation). Ya en aquellos primeros días de Internet, los desarrolladores previeron que el espacio de direcciones IPv4 se agotaría en algún momento. Estimaron que sucedería entre 2012 y 2015 (vista en retrospectiva, ¡fue una muy buena predicción!), por lo que decidieron que tenían tiempo suficiente no sólo para ampliar el espacio de direcciones sino también para intentar hacer que el protocolo fuera más escalable para grandes estructuras de Internet (Hagen, 2023).

Por otro lado, de acuerdo con (Barreño Gutiérrez, 2011) en su estudio expresa que el protocolo enrutado IPv6; es un nuevo protocolo que ha permitido el crecimiento exponencial de internet de nueva generación; para la cantidad de usuarios que día a día solicitan más y más servicios en la mundialmente llamada internet, este protocolo tiene una facilidad de implementación y configuración en dispositivos activos como enrutadores y dispositivos de capa 3 como conmutadores multicapa.

La función del protocolo IPv6 es la misma que la del protocolo IPv4, conectar dispositivos que se encuentran en redes diferentes. El protocolo de IPv6 mejora algunas de las

funcionalidades del protocolo IPv4 dando respuesta a las necesidades que han surgido tras 30 años de uso (de la Rosa Falguera, 2016).

El crecimiento extraordinario de las nuevas tecnologías y, en especial, la futura implementación del Protocolo IP en su versión 6 (IPv6) abre un enorme abanico de posibilidades, actividades y nuevas formas de comunicarse, trabajar, comprar, relacionarse con otras personas y, en definitiva, desempeñar las tareas cotidianas de nuestra vida (Santos Jaimes & Rico Bautista, 2007).

IPv6 cuenta con mejoras inherentes desde su liberación, añadiendo nuevas funcionalidades como la autoconfiguración y seguridad (IPsec), por lo que se considera que es adaptable a cualquier escenario de conectividad al ser una tecnología lo suficientemente madura para soportar la operación de Internet (Hagen, 2023)

A continuación, se presentan algunos antecedentes sobre infraestructura del protocolo IPv6.

2.1.1 Antecedentes a Nivel Internacional

Según el estudio desarrollado por los autores (Diawara Echeverría, 2024) consiste en desplegar una red IPv6 de acceso a internet dentro de la infraestructura de red de una empresa. Lo cual implica añadir una capa de red IPv6 que coexista con la infraestructura IPv4 existente, y crear las conexiones de vecindad necesarias en los routers mediante BGP, es asi que dentro de sus sos resultados se logró completar la tarea de implementar, desde cero, una red IPv6 completamente funcional y capaz de dar acceso a internet a los usuarios que se conecten a ella. Esta red brinda a la empresa Nasertic un paso más cerca de la transición de su infraestructura a IPv6, proporcionándoles una base sólida sobre la que cimentar futuras actualizaciones y expansiones en su red interna (Diawara Echeverría, 2024).

De igual manera la investigación (Clemente Lindao, 2022) de la idea del Cloud Computing, junto con las ventajas que tiene poder trabajar con un protocolo de internet versión 6 que trae nuevas características, que encajan con la computación en la nube y brindan los medios para desarrollar técnicas con las que se pueda tener un beneficio al momento de realizar una administración de red, de esta manera al ejecutar la interfaz que brindan los equipos Ubiquiti poder llevar a cabo un análisis y control óptimo en el área de redes.

De acuerdo a los autores en su investigación titulada "Análisis y Diseño de un sistema de comunicación basado en VoIP usando el protocolo IPv6 en la Universidad de la Costa", expresan que la suma importancia para el desarrollo de la propuesta de redes, se debe realizar un análisis del tema en el cual se realizará la investigación y desarrollo, en este caso es: Diseño de la transición del protocolo IPv4 a IPv6 en la empresa GrupoJativa con base en consideraciones de seguridad en implementación de ipv6, es así que ellos estudian las características tecnológicas e implementaciones de VoIP sobre los protocolos IPv4 e IPv6. y en su último objetivo diseñan una infraestructura de red de computadores real que soporte el protocolo IPv6 para la implementación del servicio VoIP (Herrera Alvear , 2021).

La Dirección General de Cómputo y de Tecnologías de la Información y Comunicación coordinó el proyecto de implementación del enrutamiento de IPv6 a nivel WAN, utilizando el mecanismo de transición Dual Stack. De esta manera, se logró su despliegue en el 100% de los enlaces dedicados de Internet, Red Privada Virtual y punto a punto, que conforman la RedUNAM (Jiménez Ramírez, 2024). Este proyecto sentó un precedente para que cada vez más entidades y dependencias universitarias se vayan sumando a la utilización de IPv6, logrando así que la UNAM sea un referente de su utilización a nivel mundial (Alves de Godoy, 2024).

Por otra parte se han desarrollado investigaciones en la implementación de seguridad en el protocolo Ivpv6 , como se evidencia en el siguiente artículo, donde se propone una tecnología de defensa activa para IPv6 que aborda los problemas de seguridad de los saltos y realiza una verificación experimental del modelo. Los experimentos han demostrado que este modelo puede resistir eficazmente la interceptación y el análisis de tráfico, así como los ataques DoS (Liu, Deng, & Xiao, 2024).

Los autores en su estudio (Pragya & Kumar, 2024) presentan el Direccionamiento IPv6 Basado en Tiempo y Ubicación (TLB-IPv6), un esquema de direccionamiento espacio-temporal sin estado. La idea tras esta estrategia es que dos objetos no pueden estar en la misma ubicación al mismo tiempo. La dirección IPv6 de destino se crea utilizando los datos de tiempo y ubicación del dispositivo y, posteriormente, se le asigna tras confirmar su singularidad mediante el protocolo de Detección de Direcciones Duplicadas (DAD). Además de mantener la información temporal y espacial, TLB-IPv6 garantiza una identidad distintiva para grandes redes.

2.1.2 Antecedentes a Nivel Nacional

De acuerdo al proyecto de grado presentado por los autores (Valbuena Caicedo & Rodriguez narvaez, 2024) donde plantean la adaptación del protocolo ipv6 al sistema por medio de métodos como tunelización, Dual stack, y traducción; para recolección de los datos el cual brindará mucho más espectro y solucionar el problema de saturación y contar en cada casino con muchos más equipos entre otros problemas que presenta el protocolo ipv4, los investigadores finalizan diciendo que el plan establecido en su trabajo de grado asegura una transición progresiva y segura hacia IPv6, minimizando riesgos y garantizando la compatibilidad y eficiencia en las máquinas electrónicas tragamonedas.

Según los autores (Ramírez , Guzmán Pantoja , & Beltran Diaz, 2015) proponen una guía de transición de IPv4 hacia IPv6 en el segmento de servidores que se exponen a internet en la Agencia Colombiana para la Reintegración (ACR) con base en consideraciones de seguridad en implementaciones realizadas sobre IPv6, dentro de sus objetivos se trazan el identificar una estrategia que se base en lineamientos, recomendaciones y buenas prácticas a nivel de seguridad para la implementación de IPv6 y la Construcción de guía para llevar a cabo la transición de IPV4 a IPV6.

De igual manera en el estudio (Chica Mora, 2020) se plantearon fases básicas las cuales buscaron que la migración se logre con la mayor transparencia posible, pensando en la normalidad de los procesos de la empresa que asuma el reto, cada fase cuenta con una serie de actividades que incorporándolas en un cronograma dará vía al cambio entre el IPV4 e IPV6, una recomendación importante para preservar la seguridad de la información es la verificación de las segmentaciones de los bloques IPV6, cuando estos se han configurado por zonas DMZ (Zonas desmilitarizadas), la base es lo requerido por cada entidad, quienes establecen sus respectivos niveles y/o criterios de seguridad.

El presente trabajo hace referencia a la implementación de buenas prácticas en el diseño esquematizado de redes, los cuales deben contener elementos optimizados que permitan mejorar la conectividad entre los elementos tecnológicos que componen la topología de red de datos. FULL), para la cual fue realizado este proyecto, se planteó un diseño de zona desmilitarizada (DMZ) con una configuración pertinente que ayudara a elevar la seguridad que actualmente posee la FULL (Sánchez Restrepo & Herrera Pinto, 2018).

s así que en la investigación desarrollada por (Plan de adopción del protocolo IPv4 a IPV6 para el sector microempresario de la ciudad de Bogotá, 2021) se Identifica la mejor

estrategia que permita adoptar IPv6, de manera transparente sobre el servicio del usuario, estableciendo un plan de proyecto que bosqueje la estrategia de habilitación del protocolo IPv6. y alineándola con la política y normatividad de IPv6 establecida por el MinTIC, donde el objetivo principal es Elaborar propuesta técnica de un plan de adopción del Protocolo de Internet versión 6 –IPv6 que permita realizar el despliegue del protocolo en empresas privadas en el sector microempresario de Bogotá.

2.1.3 Antecedentes a Nivel Regional

Este artículo (Barrientos Avendaño y otros, 2019) se contextualiza desde el concepto de internet de las cosas (IoT), su seguridad, la interoperabilidad de los dos protocolos IPV4 e IPV6 y redes definidas por software. Teniendo en cuenta las arquitecturas y tecnologías existentes, se propone una infraestructura de granja inteligente que permita dar soporte a todos los procesos que se llevan a cabo dentro de la granja de la Universidad Francisco de Paula Santander Ocaña.

El plan de implementación de IPv6 en la Corporación Autónoma Regional de la Frontera Nororiental, genero un diseño de una red IPv6 basado en un análisis de la red IPv4, utilizando como referencia el pliego presentado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Este permitió a la entidad tener una mirada holística de la infraestructura de red interna y saber qué tan preparada se encuentra para realizar la migración, determinando el porcentaje de compatibilidad de hardware y software con el nuevo protocolo (Paba Pabón, 2022).

Asi mismo se llevó a cabo el trabajo de grado titulado “Propuesta del diseño de comunicación de las oficinas de Crediservir en Norte de Santander por medio de EIGRP para

IPv6” donde el objetivo de esta investigación es dar una solución a los problemas presentados en las pruebas realizadas con los dispositivos CISCO con el protocolo EIGRP enfocado en IPv6 en la topología seleccionada (López Rojas, 2018).

En la investigación (Paramo Melo, 2020) El tema de Seguridad IPsec en el protocolo IPV6, dado que existe una necesidad vigente a nivel mundial de que todas las organizaciones implementen este protocolo a la mayor brevedad posible dado el agotamiento de direccionamiento actual de IPv42 , se hace necesario la migración a un estándar que proporcione la esencia de IPv4 sumado a atributos necesarios en la actualidad como protocolo más seguridad, movilidad, mayor rendimiento, soporte a aplicaciones en tiempo real, compatibilidad, asignación de IPs desde el cliente.

2.2 Marco Contextual

El presente proyecto se llevó a cabo en la Universidad Francisco de Paula Santander Ocaña, ubicada vía acolsure el campus principal, en el laboratorio de Redes y Telecomunicaciones del programa de Ingeniería de Sistemas, utilizando los diferentes equipos necesarios y el simulador con Packet Tracer.

Actualmente la Universidad cuenta con 4 (cuatro) facultades, una de ellas, es la Facultad de Ingenierías, que dispone de 3 programas como son: Ingeniería de Sistemas, Civil y Mecánica. Todos están acreditados y cuentan con laboratorios que permiten llevar a la práctica los conocimientos adquiridos en la parte teórica.

En el Laboratorio de redes, se realizan prácticas por parte de los estudiantes del programa de Ingeniería de Sistemas, en diferentes asignaturas, como: Teoría General de las Comunicaciones, Redes de Computares, Administración de Servidores, Comunicaciones

Inalámbricas y Seguridad Informática, entre otros. Cuenta con computadores, dispositivos de red, video beam y herramientas para las prácticas.

2.3 Marco Conceptual

A continuación, se brindan algunos conceptos necesarios para la interpretación del presente proyecto:

2.3.1 Red de datos

Las redes de datos son infraestructuras que han sido creadas para poder transmitir información a través del intercambio de datos (universidadviu, 2018). Para (IBM, 2024) La conexión en red, o interconexión informática, es el proceso de conectar dos o más dispositivos informáticos, como computadoras de escritorio, dispositivos móviles, routers o aplicaciones, para permitir la transmisión y el intercambio de información y recursos.

2.3.2 Seguridad en la red

La seguridad de redes es el campo de la ciberseguridad centrado en la protección de las redes y sistemas informáticos frente a ciberamenazas e internos (IBM, 2024). De igual marera (Trend, 2025) expresa que la seguridad de redes es un término amplio para describir la protección de todos los recursos de cómputo ante ataques y fallas en la disponibilidad, confidencialidad e integridad. Esto involucra anti-malware, firewalls, detección de intrusiones, tecnología para la prevención de la pérdida de datos y otras protecciones. Para (Fortinet, 2025) La seguridad de red se refiere a las tecnologías, políticas, personas y procedimientos que

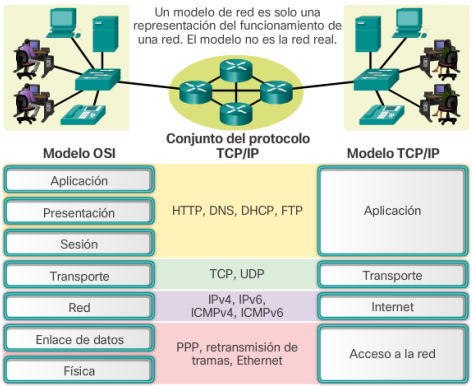
defienden cualquier infraestructura de comunicación de ciberataques, acceso no autorizado y pérdida de datos.

2.3.3 Modelo de referencia

TCP/IP es un modelo práctico que aborda desafíos de comunicación específicos y se basa en protocolos estandarizados. Por el contrario, OSI sirve como un marco integral e independiente del protocolo diseñado para abarcar varios métodos de comunicación de red (Fortinet, 2025). El modelo de referencia OSI ISO de siete capas se propuso por primera vez alrededor de 1983 para permitir la conectividad (o interfuncionamiento) entre diferentes sistemas informáticos, la arquitectura TCP/IP es funcionalmente equivalente al modelo de referencia OSI, pero este posee 4 capas (Cisco, 2003).

Figura 1.

Modelos de Referencias OSI y TCP/IP



Nota. Fuente (Cisco Networking Academy , 2021)

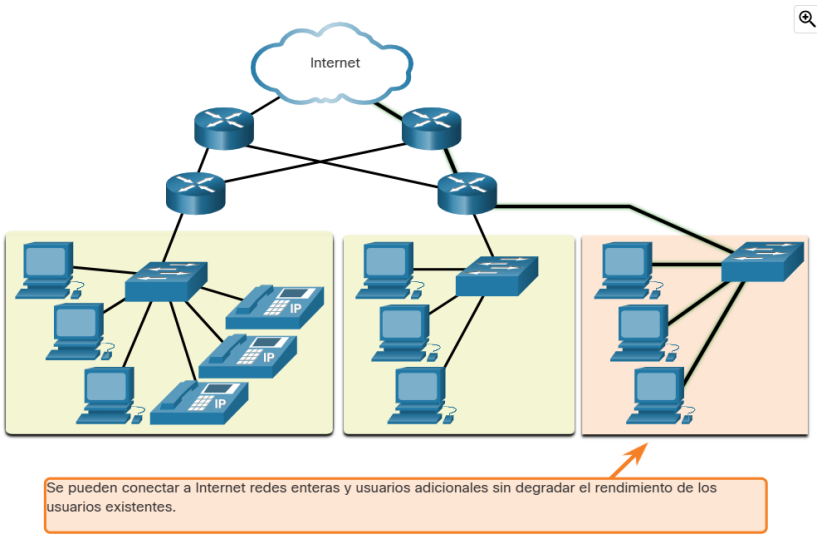
Las redes de datos son infraestructuras que han sido creadas para poder transmitir información a través del intercambio de datos (universidadviu, 2018). Para (IBM, 2024) La conexión en red, o interconexión informática, es el proceso de conectar dos o más dispositivos informáticos, como computadoras de escritorio, dispositivos móviles, routers o aplicaciones, para permitir la transmisión y el intercambio de información y recursos.

2.3.4 Escalabilidad

Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Lo hace sin degradar el rendimiento de los servicios a los que están accediendo los usuarios existentes (CISCO, 2025)

Figura 2.

Escalabilidad en las redes



Nota. Fuente (Cisco Networking Academy , 2021)

2.3.5 Infraestructura de red

Según (Redhat, 2021) La infraestructura de red es una parte de la infraestructura de la TI que incluye el hardware, el software, los sistemas y los dispositivos que posibilitan el flujo de los datos en toda la empresa para conectar a los usuarios, los dispositivos, las aplicaciones y el Internet, entre otras cosas. (CISCO, 2025) infraestructura de red se elige una topología de red jerárquica, que nos permite agrupar equipos con funciones específicas, separándolo en tres niveles para facilitar el diseño, la implementación y su mantenimiento, esta topología nos permite que la red sea más confiable y escalable.

2.3.6 ***Protocolo de Internet IPV4 / IPV6***

IPv4 e IPv6 son dos versiones del sistema de direccionamiento del Protocolo de Internet (IP). La IP es un conjunto de reglas de comunicación que proporcionan el intercambio de datos a través de Internet (Carneiro Portela, dos Santos, Lucena de Souza, Line Oliveira, & Washington , 2025). En esencia, Internet es una colección de miles de millones de dispositivos que comparten datos entre sí a través de tecnologías de red. El IP utiliza un sistema de numeración para dar a cada dispositivo conectado un número de identificación o una dirección únicos. (Gallegos Osorio, 2024) IPv4 usa un formato de direcciones de 32 bits y puede albergar más de cuatro mil millones de espacios de direcciones. Con la expansión de los sistemas de Internet e Internet de las cosas (IoT), el IPv4 demuestra ser insuficiente en su rango de direccionamiento. Se está eliminando gradualmente y reemplazando con IPv6 (Gallegos Osorio, 2024), ya que utiliza un formato de direcciones de 128 bits y puede alojar más de 1x1036 direcciones (AWS, 2024).

2.3.7 ACL

Una lista de control de acceso a la red (ACL) está compuesta por reglas que permiten el acceso a un entorno informático o lo rechazan. De alguna manera, una ACL es como una lista de invitados en un club exclusivo. Solo las personas de la lista están permitidas en las puertas. Esto permite a los administradores garantizar que, a menos que el dispositivo presente las credenciales adecuadas, no pueda obtener acceso (Fortinet, 2025), según (CISCO, 2025) Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

2.3.8 ***ACL de red***

Las ACL de red administran el acceso a una red. Para ello, proporcionan instrucciones a los conmutadores y enrutadores en cuanto a los tipos de tráfico que pueden interactuar con la red. También dictan lo que cada usuario o dispositivo puede hacer una vez que están adentro (Fortinet, 2025).

2.3.9 Seguridad Informática

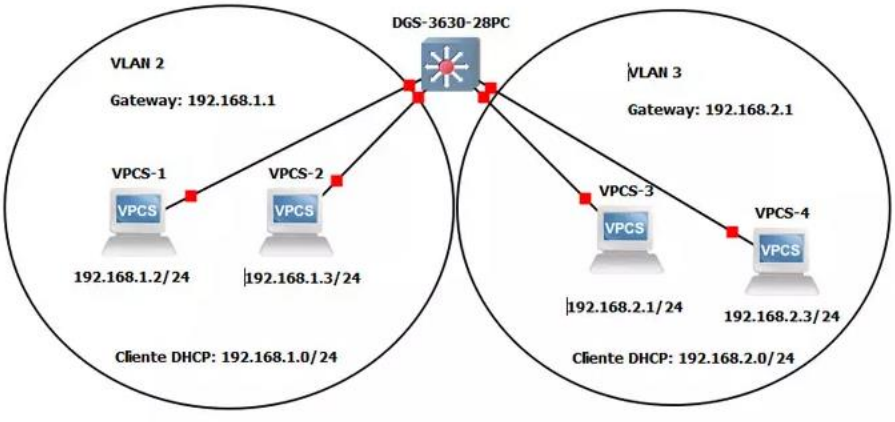
Según (Udecataluña, 2023) La seguridad informática o ciberseguridad, es la protección de la información con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal objetivo es que, tanto personas como equipos tecnológicos y datos, estén protegidos contra daños y amenazas hechas por terceros. Para (IBM, 2024) la seguridad informática es la práctica de proteger los sistemas informáticos, redes, dispositivos digitales, datos de acceso no autorizado, filtraciones de datos, ataques cibernéticos y otras actividades maliciosas.

2.3.10 VLAN

Las VLAN o también conocidas como «Virtual LAN» nos permite crear redes lógicamente independientes dentro de la misma red física, haciendo uso de switches gestionables que soportan VLANs para segmentar adecuadamente la red (Redes Zone, 2024) (Salsa Yunika & Nul Ichsan, 2025). Según Las VLAN redes empresariales y de campus para permitir que los que los usuarios reciban direcciones IP de la misma subred, aunque no estén conectados al mismo enrutador o conmutador. Además, las VLAN simplifican la asignación de direcciones entre diferentes unidades administrativas y permiten que usuarios físicamente dispares sean tratados como una unidad (Garimella, Yu-Wei , Nan , & Sanjay, 2007). De igual manera (Shahriar & Fan, 2020) describen en su artículo que se conoce como VLAN a un grupo de dispositivos en una o más LAN que están configurados para conectarse como si estuvieran conectados a través del mismo cable.

Figura 3.

Red con VLAN



Nota. Fuente (Redes Zone, 2024)

2.4 Marco Teórico

La generación IPv6 propuesta se basa en un enfoque matemático híbrido que conserva la confidencialidad de la dirección IP y previene ataques de denegación de servicio (DoS) de nodos nuevos y existentes en la red. En este artículo, se analiza el protocolo híbrido propuesto para ataques DoS de nodos nuevos y existentes. Los resultados demuestran que la tasa de configuración exitosa, la sobrecarga y el consumo de energía son mejores que los enfoques existentes, a saber, la detección de direcciones duplicadas de procesadores de paquetes independientes del protocolo de programación (P4DAD), la técnica de prevención de coincidencias (Gankotiya, Kumar, & Singh Vaisla, 2024) .

Hoy en día, Nos enfrentamos a la transición de IPv4 a IPv6, que durará varios años o posiblemente décadas. Existen diferentes tecnologías de transición a IPv6 que permiten la comunicación entre hosts que utilizan las dos versiones incompatibles del Protocolo de Internet en diversos escenarios, pero también implican problemas de seguridad adicionales. En este artículo, se desarrolló una metodología para la identificación de posibles problemas de seguridad de diferentes tecnologías de transición a IPv6 y sus implementaciones, basada en el enfoque STRIDE y su aplicación a las tecnologías de transición a IPv6 (Lencse & Kadobayashi, 2018).

Según (Carneiro Portela, dos Santos, & Severino, 2025) en su investigación analizaron los protocolos de red IPV4 e IPV6 en sus aspectos conceptuales. De acuerdo con los análisis comparativos realizaron con base en el alcance delimitado de la investigación, fue posible identificar que el protocolo IPV6 trae ventajas técnicas significativas en relación al protocolo IPV4, entre ellas: la presencia de una capa de seguridad para soportar a las organizaciones que utilizan IPV6, la capacidad de ampliar el número de *hosts* (dispositivos) disponibles en una red

de computadoras. Esta información es relevante porque contribuye directamente a que los agentes técnicos de una organización pública o privada puedan tomar decisiones más asertivas y realizar las configuraciones adecuadas de entornos de red con mayor capacidad tecnológica.

En la actualidad, diversos investigadores han propuesto múltiples modelos para la generación de direcciones objetivo en IPv6. No obstante, los modelos existentes aún presentan limitaciones, como una baja tasa de aciertos y la producción de patrones repetitivos en la generación de direcciones. Con el fin de obtener un conjunto más dinámico y variado de direcciones candidatas para la detección de objetivos, se plantea un modelo de generación de direcciones IPv6 activas basado en un enfoque de difusión. Este modelo inicia dividiendo las direcciones semilla recopiladas según el tipo de identificador de interfaz. Posteriormente, estas direcciones se transforman de datos discretos a continuos. Los datos transformados son procesados por el modelo de difusión para generar nuevas direcciones IPv6. Finalmente, se realiza una verificación de alias en las direcciones generadas para minimizar el uso innecesario de recursos durante la detección. Los experimentos realizados demuestran que este modelo basado en difusión supera en tasa de aciertos a los métodos de generación actuales (Yang, Yao, & Wang, 2025).

De acuerdo a (Hilal, Sattle, Gasser, & Vermeulen, 2024) Se han estudiado bastante bien en la Internet IPv4, aunque su impacto en IPv6 sigue siendo incierto. En este artículo, analizamos por primera vez la infraestructura hipergigante IPv6. Se realizó un estudio pionero de redes IPv6 externas para 14 hipergigantes y comparamos su implementación con IPv4. Se encontraron redes IPv6 externas en 2000 sistemas autónomos (AS), en comparación con los más de 6000 AS externos para IPv4.

2.5 Marco Legal

A continuación, se presenta el marco legal en Colombia sobre el uso del protocolo Ipv6.

2.5.1 Plan Nacional de Transición a IPv6

Dentro del documento de “Lineamientos para la adopción de IPv6 en Colombia", su objetivo es establecer una hoja de ruta para que las entidades públicas y privadas implementen IPv6, por tal motivo desde su contenido estipulan; diagnóstico del estado del protocolo IPv4, recomendaciones técnicas para la transición y estrategias de capacitación, adquisición de tecnología y soporte (MinTIC, 2024).

2.5.2 Ley 1341 de 2009 – Ley TIC

Artículo relevante: Fomenta el desarrollo y la adopción de tecnologías de la información, lo cual incluye el uso de estándares y protocolos modernos como IPv6.

Reforma: Esta ley fue modificada por la Ley 1978 de 2019, que impulsa el cierre de la brecha digital y mejora la infraestructura de conectividad (Función Pública , 2009).

2.5.3 Resoluciones del MinTIC sobre infraestructura TIC

El MinTIC ha emitido varias resoluciones técnicas y circulares donde se insta a los operadores y entidades a planificar la migración de IPv4 a IPv6, Se destaca la obligación de que los nuevos desarrollos tecnológicos y de red sean compatibles con IPv6 (MinTIC, 2024).

2.5.4 Generales-RITEL-Aclaración adopción a protocolo IPV6.

La Regulación por parte de la Comisión de Regulación de Comunicaciones (CRC) ha apoyado iniciativas para evaluar el estado de IPv6 y establecer condiciones regulatorias que faciliten su despliegue, Publicaciones de la CRC sobre la medición de adopción de IPv6 en Colombia (Comision de reculacion de comunicaciones CRC, 2020).

3. Diseño Metodológico

3.1 Tipo de Investigación

La investigación experimental implica exponer a un grupo de personas u objetos a condiciones específicas, tratamientos o estímulos, denominados variables independientes, con el fin de observar las reacciones, respuestas o efectos resultantes, conocidos como variables dependientes. En este tipo de investigación, los investigadores modifican o alteran una o varias variables independientes para observar y controlar cómo estas modificaciones afectan el comportamiento observado. Se considera que una investigación experimental es exitosa cuando la manipulación de una variable independiente produce un cambio en una variable dependiente. (Guevara Alban, G. P., et. al, 2020)

3.2 Población y muestra

3.2.1 Población

La población se encuentra conformada por los estudiantes del programa de Ingeniería de Sistemas, más específicamente los que se encuentran en las asignaturas de la línea de Infraestructura de TI como: Teoría General de las Comunicaciones, Redes de Computares, administración de servidores, comunicaciones inalámbricas y seguridad informática, quienes diariamente utilizan las instalaciones del Laboratorio de redes y telecomunicaciones.

3.2.2 Muestra

La muestra, es el grupo de personas o sucesos, sobre el cual, se recolectarán los datos, sin que necesariamente sea representativa del universo que se estudia (Sampieri Hernández & all, 1998). Debe ser de carácter finito ya que se tiene el dato exacto de la población, en este caso se tomó la totalidad de la cantidad de usuarios representados en la población, dado que es pequeña y se requería para obtener la información suficiente del caso de estudio.

3.3 Diseño de instrumentos de recolección de la información y técnicas de análisis de datos

Como ya se mencionó se aplicaron herramientas cualitativas que se describen a continuación:

1. La revisión documental. Permitió conocer las experiencias de otras entidades frente a la seguridad y mecanismos adoptados para contrarrestar los delitos informáticos.
2. Simulación. Con el simulador Packet Tracer, se implementó el diseño y se realizaron las respectivas configuraciones necesarias.

3.4 Análisis de la información

para el desarrollo del presente proyecto se llevó a cabo un proceso de análisis de la información basado en tres enfoques complementarios: revisión documental, observación directa y simulación. La revisión documental permitió identificar los principales estándares y lineamientos relacionados con la implementación del protocolo IPv6, así como conocer experiencias previas y marcos normativos tanto a nivel internacional como nacional, aportando así una base teórica sólida para sustentar el estudio.

Paralelamente, mediante la observación de entornos reales de red, se recolectó información valiosa sobre el estado actual de las infraestructuras, identificando prácticas comunes, limitaciones técnicas y el nivel de adopción del protocolo. Finalmente, a través de la simulación de escenarios controlados, se evaluó el comportamiento del protocolo IPv6 bajo distintas condiciones, comparando su rendimiento con IPv4 y analizando variables como la latencia, la tasa de éxito en la generación de direcciones y la eficiencia en el enrutamiento. La triangulación de estas tres fuentes de información permitió obtener una visión integral, objetiva y fundamentada del fenómeno estudiado, facilitando la formulación de conclusiones y recomendaciones pertinentes para la implementación efectiva de IPv6.

4. Resultados

4.1 Diseño de la topología de red y definición de los componentes necesarios para la implementación de una infraestructura escalable basada en IPv6 en entornos de laboratorio.

Para la implementación de la infraestructura propuesta se requirió un conjunto de dispositivos de red y equipos de cómputo que permitieran garantizar la conectividad, gestión y operación adecuada del sistema. A continuación, se describen los componentes necesarios:

Tabla 1.

Dispositivos requeridos

Dispositivo	Descripción	Cantidad
switch de acceso Cisco 2960	Los Switches proporcionan la conectividad principal a nivel de acceso para los diferentes dispositivos de la red permitiendo la segmentación básica, administración eficiente del tráfico y soporte para VLANs y garantizando un entorno estable y seguro para los usuarios.	2
Router0 (Cisco 2911)	Los routers serán responsables de la interconexión entre distintas redes, la gestión del enrutamiento dinámico y el establecimiento de comunicaciones seguras entre las diferentes áreas o sedes. El modelo Cisco 2911 ofrece un alto rendimiento y capacidades avanzadas de seguridad y administración.	5
Equipos de computo	Estos equipos serán utilizados por los usuarios finales para ejecutar aplicaciones, acceder a la red y realizar las tareas operativas necesarias. Su función es esencial para la interacción directa con los servicios proporcionados por la infraestructura.	6
Servidor	l servidor central se encargará de alojar los servicios principales de la red, tales como bases de datos, aplicaciones internas, sistemas de autenticación o almacenamiento compartido. Constituye un componente crítico para el funcionamiento coordinado y seguro del sistema.	1

La topología diseñada constituye un prototipo integral de infraestructura de red escalable y segura basada en el protocolo IPv6, orientada a fortalecer los ambientes de simulación en instituciones académicas. Su arquitectura se fundamenta en un modelo jerárquico distribuido que

replica escenarios reales de comunicación entre una oficina central, una oficina remota y una infraestructura de un proveedor de servicios (ISP), permitiendo la experimentación con mecanismos avanzados de direccionamiento, seguridad y tunelamiento.

Figura 4.

Diseño de topología de red.

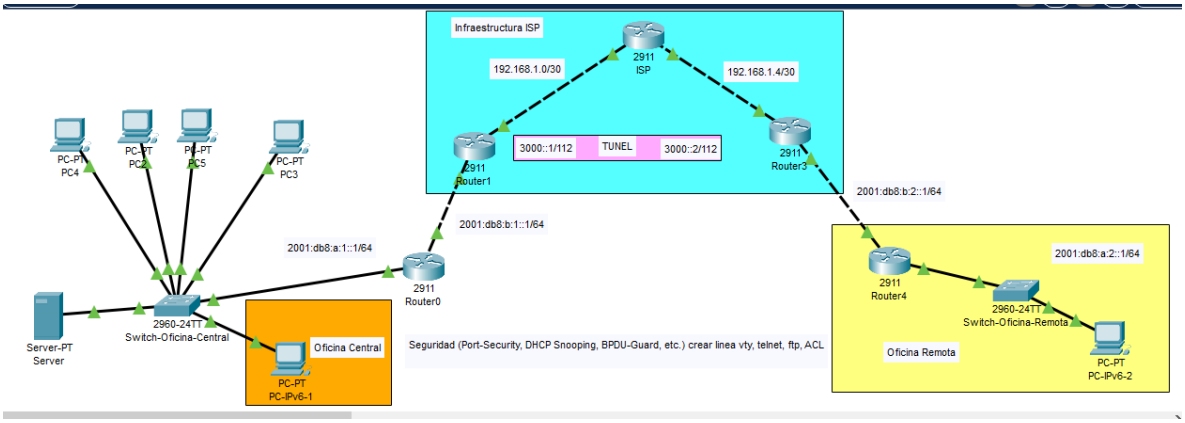


Tabla 2.

Arquitectura de enrutamiento

Router	Función Principal	Tecnología
Router 0	Gateway de Oficina Central	IPv6, RIPng
Router 1	Perímetro Central y extremo del túnel	IPv4, OSPF, IPv6, RIPng, Túnel IPv6-ipv4
Router 3	Núcleo ISP	IPv4, OSPF
Router 4	Perímetro Remoto y segundo extremo del túnel	IPv4, OSPF, IPv6, RIPng, Túnel IPv6-ipv4
Router 5	Distribución LAN remota	IPv6, RIPng

4.1.1 Segmento de Oficina Central

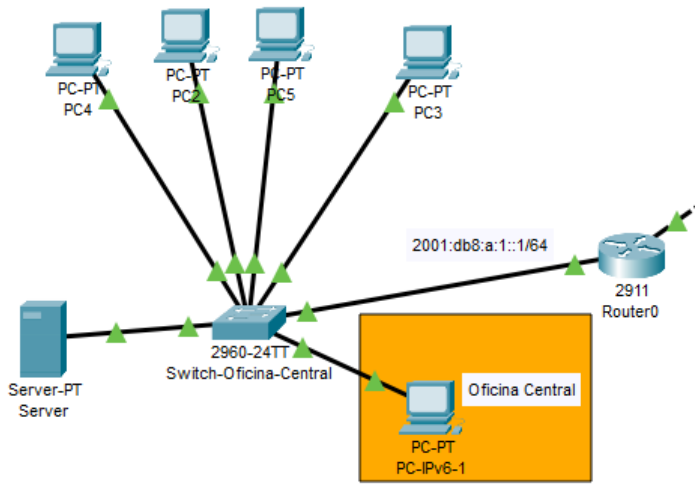
El dominio principal se compone de un switch de acceso Cisco 2960 (Switch-Oficina-Central) al cual se conectan múltiples estaciones de trabajo y un servidor institucional. Estos dispositivos se encuentran organizados en un esquema de direccionamiento IPv6 nativo, con prefijo 2001:db8:a:1::/64.

La oficina central incorpora funcionalidades de seguridad de Capa 2 como Port-Security, DHCP Snooping y control por VLAN, con el fin de garantizar la integridad del plano de datos y mitigar ataques internos propios de redes académicas de laboratorio.

El Router0 (Cisco 2911) actúa como el Gateway Predeterminado de este segmento y provee conectividad hacia la infraestructura del ISP.

Figura 5.

Red Oficina Central



4.1.2 Núcleo de la Infraestructura ISP

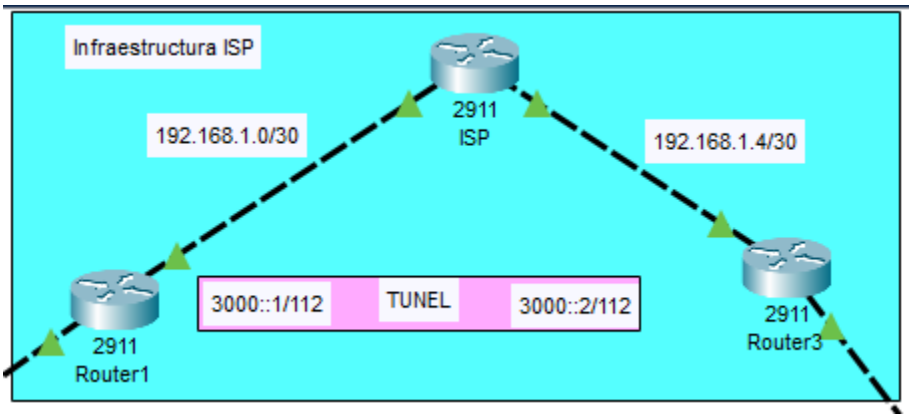
El prototipo incorpora un segmento intermedio que simula el comportamiento de un proveedor de servicios (ISP). Este núcleo está compuesto por tres routers Cisco 2911 interconectados mediante enlaces punto a punto con direccionamiento IPv4 (192.168.1.0/30 y 192.168.1.4/30), lo cual permite recrear un escenario híbrido de coexistencia IPv4–IPv6 en el que se evalúa la transición tecnológica hacia IPv6.

Con el fin de habilitar comunicación IPv6 extremo a extremo entre las sedes, el ISP implementa un túnel IPv6 sobre infraestructura IPv4, utilizando los prefijos 3000::1/112 y 3000::2/112. El túnel opera como un mecanismo de transporte que permite superar limitaciones del backbone IPv4 y evaluar estrategias de migración graduales en entornos educativos.

Este diseño favorece la comprensión práctica de conceptos como encapsulamiento, transición dual-stack, ruteo avanzado y gestión de proveedores de tránsito, fundamentales en cursos de redes orientados a niveles avanzados e investigación.

Figura 6.

Núcleo Infraestructura ISP



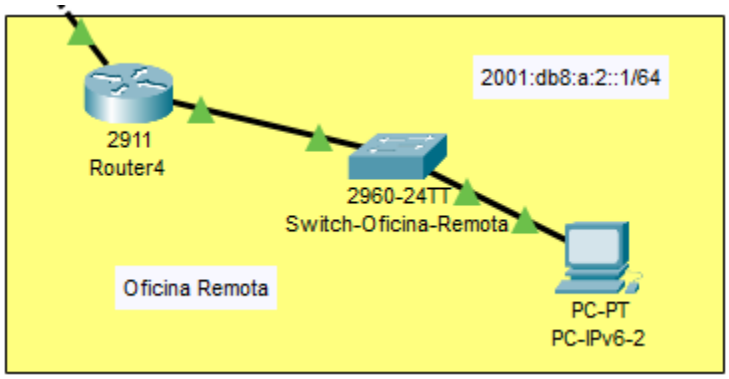
4.1.3 Oficina Remota

La oficina remota incorpora un segundo dominio de acceso, construido sobre un switch Cisco 2960 y un router 2911 (Router4). Su esquema de direccionamiento se organiza en el prefijo 2001:db8:a:2::/64, aislándolo lógicamente de la oficina central mediante técnicas de segmentación dinámica.

La conectividad entre ambas sedes se logra a través del enlace WAN IPv6 (2001:db8:b:2::1/64) que, a su vez, se enruta a través de la infraestructura ISP mediante el túnel antes descrito. En este segmento se sitúa una estación de trabajo adicional que permite validar la interoperabilidad, el ruteo extremo a extremo y los mecanismos de filtrado implementados.

Figura 7.

Red Oficina Remota



4.1.4 Descripción académica de la configuración de los routers en el prototipo IPv6

La configuración de los dispositivos de capa 3 constituye el eje funcional del prototipo, dado que permite habilitar la comunicación extremo a extremo entre la oficina central, el ISP simulado y la oficina remota. Para ello, se implementaron técnicas de enrutamiento dinámico, tunelamiento IPv6 sobre infraestructura IPv4 y mecanismos de seguridad y segmentación. A

continuación, se describe el rol técnico de cada router y la razón metodológica detrás de su configuración.

4.1.4.1 *Router 0 – Gateway de la Oficina Central.*

El Router 0 actúa como el punto de salida del dominio local ubicado en la Oficina Central. Su configuración habilita:

Enrutamiento IPv6 nativo.

Se activa el reenvío IPv6 mediante ipv6 unicast-routing, permitiendo al router operar como un nodo de capa 3 para el prefijo local 2001:db8:a:1::/64.

Conectividad LAN

La interfaz G0/1 recibe la dirección:

2001:db8:a:1::1/64 → Gateway del segmento de usuarios

Esta interfaz participa en el proceso de enrutamiento dinámico mediante RIPng, lo cual permite el intercambio automático de rutas con los demás routers del prototipo.

Conectividad WAN hacia el ISP

La interfaz G0/0 utiliza:

2001:db8:b:1::2/64 → Enlace punto a punto con Router Perimetral 1

Este enlace opera como tránsito hacia la infraestructura del ISP.

Ambas interfaces participan en RIPng, facilitando la propagación de rutas IPv6 dentro del entorno completo.

Configuración del router 0

Router>

Router>enable

```
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface g0/1
Router(config-if)#ipv6 address 2001:db8:a:1::1/64
Router(config-if)#no shutdown
Router(config-if)#ipv6 rip redv6 enable
Router(config-if)#interface g0/0
Router(config-if)#ipv6 address 2001:db8:b:1::2/64
Router(config-if)#no shutdown
Router(config-if)#ipv6 rip redv6 enable
Router(config-if)#exit
Router(config)#ipv6 router rip redv6
Router(config-rtr)#
```

4.1.4.2 *Router 1 – Router Perimetral de la Oficina Central.*

Este router interconecta la oficina central con el ISP, traduciendo condiciones de laboratorio a escenarios reales de borde de red.

Enlace WAN IPv6

La interfaz G0/0 utiliza:

2001:db8:b:1::1/64 → extremo del enlace con Router 0

Construcción del túnel IPv6 sobre infraestructura IPv4

Uno de los elementos clave del prototipo es el túnel manual IPv6ip, configurado en la interfaz Tunnel0:

- Dirección del túnel: 3000::1/112
- Origen del túnel: g0/1 (interfaz IPv4)
- Destino del túnel: 192.168.1.6 (Router Perimetral 4)

Este mecanismo permite transportar tráfico IPv6 a través del backbone ISP, que opera únicamente con OSPF IPv4. Su configuración ilustra una técnica real de transición entre protocolos en entornos de laboratorio.

El túnel participa igualmente en RIPng para garantizar el aprendizaje de rutas IPv6 remotas.

Interconexión con el ISP (IPv4)

La interfaz G0/1 utiliza:

- 192.168.1.2/30 → enlace hacia Router 3

Este segmento participa en OSPF área 0, proporcionando estabilidad en el enrutamiento del backbone.

Configuración del router perimetral 1

```
Router>
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface g0/0
Router(config-if)#ipv6 address 2001:db8:b:1::1/64
Router(config-if)#no shutdown
Router(config-if)#ipv6 rip redv6 enable
Router(config-if)#exit
Router(config)#ipv6 router rip redv6
```

```
Router(config-rtr)#exit
Router(config)#interface tunnel 0
Router(config-if)#ipv6 address 3000::1/112
Router(config-if)#tunnel destination 192.168.1.6
Router(config-if)#tunnel source g0/1
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#ipv6 rip redv6 enable
Router(config-if)#interface g0/1
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.2 255.255.255.252
Router(config-if)#exit
Router(config)#router ospf 100
Router(config-router)#network 192.168.1.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#
```

4.1.4.3 *Router 3 – Núcleo del ISP (Backbone)*.

Este dispositivo se configura únicamente con IPv4 y OSPF, simulando la infraestructura de un proveedor real que aún no migra a IPv6.

Enlaces punto a punto

- 192.168.1.1/30 → Hacia Router 1
- 192.168.1.5/30 → Hacia Router 4

Enrutamiento OSPF

Ambos enlaces se anuncian en:

- Área 0, el área de backbone

La ausencia deliberada de IPv6 permite demostrar la necesidad del túnel IPv6-ipv4, crítica en este modelo híbrido de transición.

Configuración del router 3 ISP

```
Router>
Router>enable
Router#config terminal
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#interface g0/1
Router(config-if)#ip address 192.168.1.5 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#router ospf 100
Router(config-router)#network 192.168.1.0 0.0.0.3 area 0
Router(config-router)#network 192.168.1.4 0.0.0.3 area 0
Router(config-router)#
```

4.1.4.4 *Router 4 – Router Perimetral de la Oficina Remota.*

Este equipo conecta la oficina remota al ISP y recibe el extremo del túnel IPv6.

Enlace al ISP (IPv4)

- 192.168.1.6/30 → Conecta con Router 3

- Participa en OSPF área 0

Extremo del túnel IPv6

La interfaz Tunnel0 se define con:

- Dirección: 3000::2/112
- Origen del túnel: g0/0
- Destino: 192.168.1.2 (Router 1)

Este túnel es crítico para garantizar la continuidad del tráfico IPv6 entre ambas sedes.

LAN de Oficina Remota

La interfaz G0/1 utiliza:

- 2001:db8:b:2::1/64 → Gateway de la red intermedia hacia Router 5

Participa en RIPng para el enrutamiento dinámico.

Configuración del router perimetral 4 remota

```
Router>

Router>enable

Router#configure terminal

Router(config)#interface g0/0

Router(config-if)#ip address 192.168.1.6 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#router ospf 100

Router(config-router)#network 192.168.1.4 0.0.0.3 area 0

Router(config-router)#exit

Router(config)#ipv6 unicast-routing

Router(config)#interface tunnel 0
```

```
Router(config-if)#ipv6 address 3000::2/112
Router(config-if)#tunnel destination 192.168.1.2
Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#ipv6 rip redv6 enable
Router(config-if)#exit
Router(config)#ipv6 router rip redv6
Router(config-rtr)#exit
Router(config)#interface g0/1
Router(config-if)#ipv6 address 2001:db8:b:2::1/64
Router(config-if)#ipv6 rip redv6 enable
Router(config-if)#no shutdown
Router(config-if)#
```

4.1.4.5 *Router 5 – Distribución IPv6 de la Oficina Remota*.

Este router extiende la red hacia el segmento final de la oficina remota.

Conectividad con Router 4

- 2001:db8:b:2::2/64 → Enlace punto a punto con Router 4

Segmento final de usuarios remotos

La interfaz G0/1 asigna:

- 2001:db8:a:2::1/64 → Segmento LAN de la Oficina Remota

Participación en RIPng

Ambas interfaces están habilitadas para el intercambio dinámico de rutas IPv6.

El Router 5 permite extender la topología hacia nuevos segmentos, cumpliendo los criterios de escalabilidad planteados en el proyecto

Configuración del router 5 remota

```
Router>

Router>enable

Router#configure terminal

Router(config)#interface g0/0

Router(config-if)#ipv6 address 2001:db8:b:2::2/64

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#ipv6 unicast-routing

Router(config)#interface g0/0

Router(config-if)#ipv6 rip redv6 enable

Router(config-if)#exit

Router(config)#interface g0/1

Router(config-if)#ipv6 address 2001:db8:a:2::1/64

Router(config-if)#no shutdown

Router(config-if)#ipv6 rip redv6 enable

Router(config-if)#exit

Router(config)#ipv6 router rip redv6

Router(config-rtr)#exit

Router(config)#
```

4.2 Configuración del mecanismo de segmentación dinámica mediante VLAN y control de acceso mediante ACL, asegurando la seguridad y la eficiencia en la gestión del tráfico de datos en el prototipo de laboratorio.

4.2.1 Segmentación lógica y esquema de direccionamiento del switch de acceso

La infraestructura de conmutación implementada en la red propuesta se basa en un esquema de segmentación lógica orientado a mejorar la seguridad, la administración y el rendimiento del dominio de capa 2. Para este propósito, se configuró un switch Cisco Catalyst utilizando una arquitectura centrada en la creación de VLANs y en la definición de una Switch Virtual Interface (SVI) para la administración remota del dispositivo. El presente apartado describe de manera detallada la estructura de direccionamiento y las políticas de segmentación establecidas.

4.2.2 Configuración de VLAN y dominio de broadcast.

El switch fue configurado para operar bajo un único dominio de broadcast funcional asociado a la VLAN 99 (ADMON). Esta VLAN se estableció como la red exclusiva para la gestión del equipo, siguiendo las mejores prácticas de seguridad recomendadas por Cisco y la literatura especializada, las cuales sugieren evitar el uso de la VLAN por defecto (VLAN 1) para la administración con el fin de mitigar riesgos asociados a ataques comunes de capa 2, tales como VLAN hopping o spoofing de tráfico de administración.

Todos los puertos físicos FastEthernet (Fa0/1 – Fa0/24) y GigabitEthernet (Gi0/1 – Gi0/2) fueron asignados como puertos de acceso dentro de la VLAN 99. Esta decisión fue orientada a centralizar el tráfico de administración y reducir la superficie de exposición del

dispositivo, permitiendo un control más estricto sobre el flujo de datos que ingresa y sale del plano de gestión.

Interfaz de administración (SVI). Para habilitar la administración remota mediante protocolos como Telnet o SSH, el switch dispone de una interfaz virtual de conmutación (SVI) asociada a la VLAN 99. La SVI fue configurada con la siguiente dirección IP:

- IP: 192.168.1.2
- Máscara: 255.255.255.0 (/24)
- VLAN asignada: 99 (ADMON)

Esta dirección constituye el punto de gestión central del dispositivo y permite la integración del switch dentro del esquema global de direccionamiento del sistema. La interfaz VLAN 1 permanece deshabilitada (shutdown), eliminando cualquier posibilidad de que el dispositivo sea administrado accidentalmente mediante la VLAN por defecto.

Figura 8.

Configuración Vlan 99 Administración

```
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
99   ADMON                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

4.3 Realización de pruebas de desempeño al prototipo en términos de escalabilidad, seguridad y funcionalidad, validando su capacidad para fortalecer los ambientes de simulación en instituciones académicas.

La validación del prototipo de infraestructura de red IPv6 se realizó mediante un conjunto de pruebas orientadas a evaluar su desempeño, escalabilidad, seguridad y funcionalidad dentro del entorno de laboratorio. Estas pruebas permitieron determinar si la solución propuesta cumple con los requerimientos para fortalecer los ambientes de simulación académica en instituciones educativas. Se aplicaron metodologías de evaluación propias del análisis de redes experimentales, incluyendo mediciones de latencia, estabilidad de los enlaces, correcta propagación del direccionamiento, segmentación dinámica mediante VLAN y mecanismos de protección de capa 2.

Figura 9.

Uso del comando show ip interface brief router 0

```
Router0#
Router0#SHOW IP INTERFACE BRIEF
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router0#
```

Nota. Ilustración, interfaces y túnel estado arriba router 0.

Figura 10.

Uso del comando show ip interface brief router 4

```
Router4#SHOW IP INTERFACE BRIEF
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router4#
```

Nota. Ilustración, interfaces y túnel estado arriba router 4.

Figura 11.

Uso del comando show interface tunnel 0 Router1

```
Router1#
Router1#show interface tunnel 0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.2 (GigabitEthernet0/1), destination 192.168.1.6
  Tunnel protocol/transport IPv6/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 185 bits/sec, 0 packets/sec
  5 minute output rate 196 bits/sec, 0 packets/sec
     1352 packets input, 231352 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     1350 packets output, 230496 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

Router1#
```

Nota. Ilustración, Configuración túnel estado arriba router 1.

Figura 12.

Uso del comando show interface tunnel 0 Router3

```
Router3#show interface tunnel 0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.1.6 (GigabitEthernet0/0), destination 192.168.1.2
  Tunnel protocol/transport IPv6/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 179 bits/sec, 0 packets/sec
  5 minute output rate 169 bits/sec, 0 packets/sec
     1379 packets input, 235600 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     1373 packets output, 235120 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

Router3#
```

Nota. Ilustración, Configuración túnel estado arriba router 3.

Figura 13.

Uso del comando show IP OSPF Neighbor en los Routers 1

```
Router1#
Router1#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.5       1   FULL/DR         00:00:38    192.168.1.1     GigabitEthernet0/1
Router1#
```

Nota. Ilustración, validación adyacencias OSPF router 1.

Figura 14.

Uso del comando show IP OSPF Neighbor en el ISP

```
ISP#
ISP#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.2       1   FULL/BDR        00:00:33    192.168.1.2     GigabitEthernet0/0
192.168.1.6       1   FULL/DR         00:00:33    192.168.1.6     GigabitEthernet0/1
ISP#
```

Nota. Ilustración, Validación adyacencias OSPF router ISP.

Figura 15.

Uso del comando show IP OSPF Neighbor en los Routers 3

```
Router3#
Router3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.5       1   FULL/BDR        00:00:30    192.168.1.5     GigabitEthernet0/0
Router3#
```

Nota. Ilustración, validación adyacencias OSPF router 3.

Uso del Comando Ping Ipv6 desde Pc Oficina Central A Oficina Remota

C:\>ping 2001:DB8:A:2::2

Pinging 2001:DB8:A:2::2 with 32 bytes of data:

Reply from 2001:DB8:A:2::2: bytes=32 time<1ms TTL=124

Reply from 2001:DB8:A:2::2: bytes=32 time=11ms TTL=124

Reply from 2001:DB8:A:2::2: bytes=32 time=12ms TTL=124

Reply from 2001:DB8:A:2::2: bytes=32 time=14ms TTL=124

Ping statistics for 2001:DB8:A:2::2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 14ms, Average = 9ms

Uso del comando Ping Ipv6 desde pc oficina remota a oficina central

C:\>ping 2001:DB8:A:1::2

Pinging 2001:DB8:A:1::2 with 32 bytes of data:

Reply from 2001:DB8:A:1::2: bytes=32 time<1ms TTL=124

Reply from 2001:DB8:A:1::2: bytes=32 time=10ms TTL=124

Reply from 2001:DB8:A:1::2: bytes=32 time=13ms TTL=124

Reply from 2001:DB8:A:1::2: bytes=32 time=10ms TTL=124

Ping statistics for 2001:DB8:A:1::2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 13ms, Average = 8ms

C:\>

5. Conclusiones

Se concluye que la estructura propuesta y los componentes seleccionados permiten establecer una infraestructura completamente funcional, escalable y adaptable a escenarios académicos. La integración de tecnologías como túneles IPv6 sobre IPv4, enrutamiento dinámico y direccionamiento estructurado según estándares RFC demostró ser adecuada para la construcción de un entorno de simulación moderno y coherente con los requerimientos actuales de redes avanzadas.

Se determinó que los mecanismos de seguridad implementados fortalecen de manera significativa el aislamiento lógico del tráfico y la protección del dominio de broadcast. Las configuraciones de Port-Security, DHCP Snooping, BPDU Guard contribuyeron a una arquitectura robusta, minimizando riesgos frecuentes como suplantación de dispositivos, accesos no autorizados o ataques internos de capa 2. Estos resultados validan la efectividad del prototipo para apoyar procesos formativos en seguridad de redes.

En cuanto a las pruebas de desempeño, escalabilidad y funcionalidad, se evidenció que la infraestructura desarrollada presenta niveles óptimos de estabilidad, baja latencia y ausencia significativa de pérdidas de paquetes, aun bajo escenarios de carga simulada. El prototipo respondió adecuadamente al crecimiento progresivo del direccionamiento y la activación de nuevas subredes, demostrando su capacidad para servir como entorno de laboratorio de alta fidelidad para instituciones académicas que requieran experimentar con tecnologías IPv6 y modelos de red modernos.

Referencias

Alves de Godoy, H. (06 de 08 de 2024). *Lacnicblog*. IPv6 y su importancia para la investigación y el desarrollo (I+D)

AWS. (3 de 02 de 2024). *AWS*. https://aws.amazon.com/es/compare/the-difference-between-ipv4-and-ipv6/

Barrientos Avendaño, E., Rico Bautista, D., Coronel Rojas, L., & Cuesta Quintero, F. R. (2019). Granja inteligente: Definición de infraestructura basada en internet de las cosas, IPV6 y redes definidas por software. *Risti - Revista Ibérica de Sistemas e Tecnologias de Informação*(E17), 16. https://www.proquest.com/openview/8230e23d4bc7e38273365da979b51a5a/1.pdf?cbl=1006393&pq-origsite=gscholar

Barreño Gutiérrez, R. (2011). *Elaboración de un estado de arte sobre el protocolo IPV6; y su implementación sobre protocolos de enrutamiento dinámico como RIPNG, EIGRP y OSPF basado sobre la plataforma de equipos cisco.* Tesis, Universidad Pontificia Bolivariana., Bucaramanga. Recuperado el 25 de 03 de 2025, de https://repository.upb.edu.co/handle/20.500.11912/1259?show=full

Carneiro Portela, S. I., dos Santos, J. A., Lucena de Souza, G. S., Line Oliveira, H., & Washington , F. (19 de 01 de 2025). Protocolos de red IPV4 e IPV6: aspectos conceptuales y análisis comparativo genérico. *Studies in Engineering and Exact Sciences, 6*(1), 23.

Carneiro Portela, S. I., dos Santos, J. A., & Severino, G. (2025). Protocolo de red IPV4 e IPV6: aspectos conceptuales y un análisis comparativo genérico. *Estudios en Ingeniería y Ciencias Exactas, 6*(1). doi:https://doi.org/10.54021/seesv6n1-031

Chica Mora, R. A. (2020). *Transición al protocolo ipv6, aspectos de seguridad informática para tener presente.* Bogotá: UNiversidad abierta y a Distancia unad. https://repository.unad.edu.co/bitstream/handle/10596/34367/rachicam.pdf?sequence=1

Cisco. (16 de 05 de 2003). *Cisco*. https://www.ciscopress.com/articles/article.asp?p=31731&seqNum=2

CISCO. (20 de 01 de 2025). *CISCO*. https://www.cisco.com/

Cisco Networking Academy . (22 de 6 de 2021). *Cisco Networking Academy* . https://www.netacad.com/es

Clemente Lindao, M. L. (2022). *Administración y control de una red IPv6 basado en infraestrcutura como un servicio para un modelo de computo virtual en el laboratorio de Telecomunicaciones con cifrado de extremoa extremo utilizando dispositivos ubiquiti.* Santal Elena, Ecuador. https://repositorio.upse.edu.ec/bitstream/46000/8590/1/UPSE-TTE-2022-0001.pdf

de la Rosa Falguera, R. (2016). *Fundamentos teórico-prácticos del protocolo IPv6.* Cataluya: Universidad Politecnica de Cataluya BarcelonaTech. Obtenido de https://upcommons.upc.edu/handle/2117/98250

Diawara Echeverría, J. (2024). *Despliegue y análisis de una red de acceso a internet con protocolos de nueva generación en IPv6.* Calaluña: Universidad Pública de Navarra. https://academica-e.unavarra.es/server/api/core/bitstreams/54f31d1e-08a8-4802-829b-7e5165204331/content

Fortinet. (15 de 03 de 2025). *Fortinet*. https://www.fortinet.com/lat/resources/cyberglossary/tcp-ip-model-vs-osi-model

Gallegos Osorio, K. D. (2024). *PLAN DE TRANSICIÓN DE IPV4 A IPV6 EN UNA RED LAN.* Pontificia Universidad Católica de Ecuador, Ambato. Recuperado el 10 de 04 de 2025, de https://repositorio.puce.edu.ec/server/api/core/bitstreams/75d1a72c-7c0a-446f-93c2-982e87269774/content

Garimella, P., Yu-Wei , E. S., Nan , Z., & Sanjay, R. (20 de 08 de 2007). Characterizing VLAN usage in an Operational Network. 305-306. https://dl.acm.org/doi/pdf/10.1145/1321753.1321772

Hagen, S. (16 de 10 de 2023). *Lacnicblog*. Obtenido de https://blog.lacnic.net/una-red-solo-ipv6-la-forma-mas-sencilla-y-segura-de-operar-una-red/

Herrera Alvear , S. S. (2021). *Análisis y Diseño de un sistema de comunicación basado en VoIP usando el protocolo IPV6.* Barranquilla, Colombia: Universidad de la Costa. https://repositorio.cuc.edu.co/server/api/core/bitstreams/bb9e2e5a-dad2-4f18-8b81-294b49c2819c/content

IBM. (01 de 07 de 2024). *IBM*. https://www.ibm.com/mx-es/topics/networking

IBM. (20 de 05 de 2024). *IBM*. https://www.ibm.com/mx-es/topics/it-security

Internet society. (3 de 12 de 2021). *Internet society*. Obtenido de https://www.internetsociety.org/es/

Jiménez Ramírez, L. (Octubre de 2024). Despliegue de IPv6 en la Facultad de Estudios Superiores Aragón. *Cuadernos técnicos Univewrsitarios de la DGTIC, 2*(4), 22 - 31. doi:https://doi.org/10.22201/dgtic.ctud.2024.2.4.82

Liu, W., Deng, W., & Xiao, X. (15 de 05 de 2024). Research on Active Defense Model for IPV6 Address Jump. (I. Xplore, Ed.) *IEEE Xplore* , 7. doi:10.1109/CEI60616.2023.10527888

Lacnic. (15 de 03 de 2025). *Lanic*. https://www.lacnic.net/5494/1/lacnic/que-es-ipv6

López Rojas, J. R. (2018). *Propuesta del diseño de comunicación de las oficinas de Crediservir en Norte de Santander por medio de EIGRP para IPv6.* Universidad Francisco de Paula Santander Ocaña, Norte de Santander, Ocaña. Obtenido de https://repositorioinstitucional.ufpso.edu.co/handle/20.500.14167/1234

MinTIC. (2012). https://mintic.gov.co/images/documentos/documentos_comentarios/proyecto_decreto_ley_1581_de_2012_proteccion_datos.pdf

Paba Pabón, J. S. (2022). *Plan de implementación para la migración del protocolo IPv4 a protocolo IPv6 en la Corporación Autónoma Regional de la Frontera Nororiental CORPONOR.* Universidad Francisco de Paula Santander OCaña, Ocaña. Obtenido de https://repositorioinstitucional.ufpso.edu.co/handle/20.500.14167/1183

Paramo Melo, R. (2020). *Protocolo de seguridad orientado a IPv6 - Ipsec.* Bogotá, Colombia . Recuperado el 05 de 04 de 2025, de https://repository.unad.edu.co/bitstream/handle/10596/38529/raparamom.pdf?sequence=4&isAllowed=y

(2021). *Plan de adopción del protocolo IPv4 a IPV6 para el sector microempresario de la ciudad de Bogotá.* Bogotá: Universidad Cooperativa de Colombia. Obtenido de https://repository.ucc.edu.co/server/api/core/bitstreams/0e5afa8a-ecd6-4010-b194-4349b4ee2e87/content

Policia Nacional de Colombia. (16 de 04 de 2024). https://www.policia.gov.co/sites/default/files/ley-1801-codigo-nacional-policia-convivencia.pdf

Pragya, & Kumar, B. (15 de 09 de 2024). A Novel IPv6 Address Generation Method for IoT Network. *IEEE Xplore*, 10. doi:10.1109/IC3I61595.2024.10828641

Ramírez , D. F., Guzmán Pantoja , J., & Beltran Diaz, J. A. (2015). *Diseño de la transición del protocolo ipv4 hacia ipv6 en la agencia colombiana para la reintegración-ACR con base en consideraciones de seguridad en implementación de ipv6.* Bogota: Universidad Católica de Colombia. https://repository.ucatolica.edu.co/server/api/core/bitstreams/013d3fd4-6bf2-4acf-a84f-c14a11071a6c/content

Redes Zone. (17 de 10 de 2024). *RedesZone*. https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

Redhat. (2 de 10 de 2021). *RedHat*. https://www.redhat.com/es/partners/network-infrastructure#:~:text=La%20infraestructura%20de%20red%20es,el%20Internet%2C%20entre%20otras%20cosas.

Salsa Yunika, I., & Nul Ichsan, I. (18 de 01 de 2025). Quality of Service on Virtual Local Area Network (VLAN) in Campus Network. *Sistemasi: Jurnal Sistem Informasi, 14*(1), 126-134.

Sampieri Hernández, R., & all, e. (1998). *Metodología de la Investigación* . México: Mcgraw-hill.

Sánchez Restrepo, Á. F., & Herrera Pinto, B. D. (2018). *Diseño de una Zona Desmilitarizada(DMZ) para la fundación universitaria Libertadores.* Fundación

Universitaria Libertadores, Cundinamarca, Bogotá. Obtenido de https://repository.libertadores.edu.co/server/api/core/bitstreams/bb8c0d63-427b-4e3f-94b4-42762da09b2b/content

Santos Jaimes, L. M., & Rico Bautista, D. W. (2007). IPV6 en la universidad de Pamplona : estado del arte. *Scientia Et Technica*, 7. https://www.redalyc.org/pdf/849/84903771.pdf

Shahriar, F., & Fan, J. (2020). Performance Analysis of FHRP in a VLAN Network with STP. *IEEE 3rd International Conference on Electronics Technology*, 5. Obtenido de https://www.researchgate.net/profile/Faisal-Shahriar-2/publication/341984562_Performance_Analysis_of_FHRP_in_a_VLAN_Network_with_STP/links/5eeb0a91458515814a675ccc/Performance-Analysis-of-FHRP-in-a-VLAN-Network-with-STP.pdf

Softonic. (2022). *SPSS Softonic*. https://spss.softonic.com/

Suresh Babu, C. V., Akshayah, N. S., Maclin Vinola , P., & Janapriyan, R. (2023). IoT-Based Smart Accident Detection and Alert System. *IGI Global*, 16. doi:10.4018/978-1-6684-8098-4.ch019

trend. (15 de 03 de 2025). *trend*. https://www.trendmicro.com/es_mx/what-is/network-security.html

Udecataluña. (15 de 11 de 2023). https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber

universidadviu. (9 de 10 de 2018). *universidadviu*. https://www.universidadviu.com/int/actualidad/nuestros-expertos/redes-de-datos-todo-lo-que-hay-que-saber-sobre-ellas

Valbuena Caicedo, C. F., & Rodriguez narvaez, M. A. (2024). *Análisis de transición gradual de direcciones en una red IPv4 a Ipv6 para la recoleccion y trasmisión de información de máquinas electrónicas tragamonedas* . Universidad Cooperqativa de Colombia, Cundinamarca, Bogotá. https://repository.ucc.edu.co/server/api/core/bitstreams/f5299223-0581-4401-9eab-dba295a8cdd5/content