



Universidad Nacional Pedro Ruiz Gallo
Facultad de Ciencias Físicas y Matemáticas
Escuela Profesional de Ingeniería Electrónica



TESIS

Evaluación del método Dual Stack para la migración de IPv4 a IPv6
en la red ISP SERVICIOS A PUNTO S.A.C

Para obtener el título profesional de
INGENIERO ELECTRÓNICO

Elaborado por:

Bach. Luis Arturo, Becerra Abad
Bach. Anderson Aldahir, Reyes Llanos

Asesor:

MSc. Ing. Segundo Francisco Segura Altamirano.

ORCID: 0000-0002-0103-7222

Lambayeque-Perú

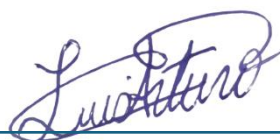
2026

Universidad Nacional Pedro Ruiz Gallo
Facultad de Ciencias Físicas y Matemáticas
Escuela Profesional de Ingeniería Electrónica

Evaluación del método Dual Stack para la migración de IPv4 a IPv6
en la red ISP SERVICIOS A PUNTO S.A.C

Elaborado por:

Bach. Luis Arturo, Becerra Abad



Bach. Anderson Aldahir, Reyes Llanos



Asesor:

MSc. Ing. Segundo Francisco Segura Altamirano.



Lambayeque-Perú

2026

Universidad Nacional Pedro Ruiz Gallo
Facultad de Ciencias Físicas y Matemáticas
Escuela Profesional de Ingeniería Electrónica

Evaluación del método Dual Stack para la migración de IPv4 a IPv6
en la red ISP SERVICIOS A PUNTO S.A.C

Para obtener el título profesional de
INGENIERO ELECTRÓNICO

JURADOS



MANUEL JAVIER RAMÍREZ CASTRO

Presidente



CARLOS LEONARDO OBLITAS VERA

Secretario



MARTÍN AUGUSTO NOMBERA LOSSIO

Vocal

Lambayeque-Perú

2026



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DECANATO

Ciudad Universitaria - Lambayeque

LICENCIADA - RESOLUCION DEL CONSEJO DIRECTIVO N° 015 - 2023-SUNEDU / CD



ACTA DE SUSTENTACIÓN N°-202.6.-D/FACFyM

Siendo las 11:00 horas del día 22 de setiembre del 2026, se reunieron los miembros del jurado evaluador de la Tesis titulada:

EVALUACIÓN DEL METODO DUAL STACIC PARA LA MIGRACIÓN DEL IPV4 A IPV6 EN LA RED ISP SERVICIOS A PUNTO S.A.C.

Designados por Resolución N° 881 - 2024

Con la finalidad de evaluar y calificar la sustentación de la tesis antes mencionada, conformada por los siguientes docentes:

M.Sc. MANUEL JAVIER RAMIREZ CASTRO

Mtro. ING. CARLOS LEONARDO ORTIZAS VERA

Mg. ING. MARTÍN AUGUSTO NOMBENA LOSSIO

Presidente

Secretario

Vocal

La tesis fue asesorada por (el) (la) M.Sc. ING. SEGUNDO FRANCISCO SEGUERA ALTAMIRANO, nombrado por Resolución N° 881 - 2024 - D/FACFyM de fecha

El Acto de Sustentación fue autorizado por Resolución N° 661 - 2026 - D/FACFyM de fecha 15 de setiembre de 2026

La Tesis fue presentada y sustentada por (el) (los) Bachiller (es): REYES LLANOS ANDERSON ALDAHIR Y BECERRA ABAD LUIS ARTURO y tuvo una duración de 50 minutos.

Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado se procedió a la calificación respectiva, otorgándole el Calificativo de DIECISIETE (17) en la escala vigesimal, mención BUENO.

Por lo que queda(n) apto(s) para obtener el Título Profesional de INGENIERO ELECTRONICO, de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ciencias Físicas y Matemáticas y la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 12:00 horas se dio por concluido el presente acto académico, dándose conformidad al presente acto con la firma de los miembros del jurado.

M. Sc. Ing. Manuel Ramirez Castro
Presidente

Mg. Ing. Martin Augusto Nombena Lossio
Vocal

Mtro. Ing. Carlos Leonardo Ortizas Vera
Secretario

Msc. Ing. Segundo Francisco Segura Altamirano
Asesor

CONSTANCIA DE VERIFICACIÓN DE ORIGINALIDAD

Yo, Segundo Francisco Segura Altamirano, usuario revisor del documento titulado **“Evaluación del método Dual Stack para la migración de IPv4 a IPv6 en la red ISP SERVICIOS A PUNTO S.A.C.”**; presentado por el Bachiller en Ingeniería Electrónica Luis Arturo, Becerra Abad, Identificado con Documento de Identidad 74770030 y por el Bachiller en Ingeniería Electrónica Anderson Aldahir, Reyes Llanos, Identificado con Documento de Identidad 75533370; declaro que la evaluación realizada por el Programa Informático, ha arrojado un porcentaje de similitud de 8%, verificable en el Resumen de Reporte automatizado de similitudes que se acompaña.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas dentro del porcentaje de similitud permitido no constituyen plagio y que el documento cumple con la integridad científica y con las normas para el uso de citas y referencias establecidas en los protocolos respectivos.

Se cumple con adjuntar el Recibo Digital a efectos de la trazabilidad respectiva del proceso.

Lambayeque, 13 de agosto de 2026



Ing Segundo Francisco Segura Altamirano
DNI: 09922587
Asesor

Se adjunta:

*Resumen de Reporte automatizado de similitudes

*Recibo Digital

Tesis Final V3

ORIGINALITY REPORT

8%

SIMILARITY INDEX

7%

INTERNET SOURCES

2%

PUBLICATIONS

3%

STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

4%

★ hdl.handle.net

Internet Source



MSc. Ing. Segundo Francisco Segura Altamirano
DNI 09922587
Asesor

Exclude quotes

Off

Exclude matches

< 15 words

Exclude bibliography

On



Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author: Luis Arturo/anderson Aldahir Becerra Abad/reyes Llanos
Assignment title: Quick Submit
Submission title: Tesis Final V3
File name: Proyecto_FinalReyes_Llanos_Anderson_Aldahir_Becerra_Abad....
File size: 6.63M
Page count: 89
Word count: 18,096
Character count: 94,446
Submission date: 13-Aug-2026 08:23PM (UTC-0500)
Submission ID: 3012177034



Universidad Nacional Pedro Ruiz Gallo
Facultad de Ciencias Físicas y Matemáticas
Escuela Profesional de Ingeniería Electrónica



Tesis

Evaluación del método Dual Stack para la migración de IPv4 a IPv6 en la
red ISP SERVICIOS A PUNTO S.A.C.

para optar el título profesional de Ingeniero Electrónico

presentado por:

Bach. Luis Arturo, Becerra Abad
Bach. Anderson Aldahir, Reyes Llanos

Asesor:

MSc. Ing. Segundo Francisco Segura Altamirano.
Lambayeque-Perú

2026

MSC. Ing. Segundo Francisco Segura Altamirano
DNI 09922587
Asesor

Agradecimientos

Quiero expresar mi profundo agradecimiento primeramente a Dios, por brindarme la fortaleza y la constancia necesarias para culminar esta etapa tan importante de mi formación profesional.

A mis padres, por su apoyo incondicional a lo largo de mi vida. De manera especial, a mi padre, quien, aunque ya no se encuentra físicamente conmigo, fue y seguirá siendo una fuente permanente de motivación y ejemplo de esfuerzo. Su recuerdo fue un impulso constante para no rendirme. A mi madre, por su paciencia, sacrificio y aliento permanente, pilares fundamentales para alcanzar este logro.

A mi asesor de tesis, por su orientación, paciencia y valiosos aportes académicos, los cuales fueron esenciales para el correcto desarrollo y culminación del presente trabajo de investigación.

Gracias por todo.

Bach. Luis Arturo, Becerra Abad

Bachiller Ingeniería Electrónica

Lambayeque 2026

Dedicatoria

Dedico el presente trabajo, en primer lugar a Dios, por darme la fuerza para no soltar esta meta.

A mi padre, por ser mi base. De forma muy especial a ti, papá: aunque ya no estés aquí para verlo, tu ejemplo de lucha fue lo que me empujó a seguir cada vez que quise rendirme. Esto es para ti. A mi madre, gracias por tanto sacrificio y paciencia; tu aliento fue el combustible que necesitaba para llegar al final.

A mi madre y a mis hermanos, por su apoyo, paciencia y motivación permanente, que fueron fundamentales para alcanzar esta meta profesional.

Gracias por todo.

Bach. Luis Arturo, Becerra Abad

Bachiller Ingeniería Electrónica

Lambayeque 2026

Agradecimientos

En primer lugar agradezco a Dios por ser quien me dio la calma y las fuerzas necesarias para continuar paso a paso esta tesis.

Agradezco a mi padre por creer en mí y darme su respaldo incondicional, sus consejos fueron el motor que me mantuvo enfocado hasta terminar. También quiero dar las gracias a mi pareja, amigos y a los ingenieros que me dieron la mano, ya sea compartiendo lo que sabían o animándome a seguir.

Por ultimo agradezco a mi asesor por su paciencia, su tiempo y esa guía que fue clave para que esta investigación llegara a concluir con éxito.

Gracias por todo.

Bach. Anderson Aldahir, Reyes Llanos

Bachiller Ingeniería Electrónica

Lambayeque 2026

Dedicatoria

Dedico este esfuerzo primeramente a Dios, por darme la calma para no rendirme.

A mi padre, mi gran referente, por darme la mano y los mejores consejos justo cuando mas los necesitaba. Y a mi pareja, por su paciencia y por animarme a seguir adelante en este camino. Esto es para ustedes.

Gracias por todo.

Bach. Anderson Aldahir, Reyes Llanos

Bachiller Ingeniería Electrónica

Lambayeque 2026

Resumen

La falta de direcciones IPv4 se debió a la saturación de dispositivos conectados. Esto forzó a los ISP a emplear soluciones provisionales para preservar la operación, lo que resultó en redes más complejas y de difícil escalamiento.

Esta tesis plantea la migración a IPv6 como la respuesta técnica necesaria. No es solo teoría: aplicamos el cambio en un ISP real de Arequipa usando routers MikroTik. Se documenta todo el camino, pasando por la actualización a RouterOS v7 para soporte nativo, la asignación de IPs, el enrutamiento y los ajustes de DNS. Para ver qué pasaba con el tráfico, usamos las herramientas de monitoreo que trae el mismo equipo. Los hallazgos evidencian los desafíos que se deben superar para lograr una migración exitosa: la actualización de equipos anticuados, la formación intensiva del personal técnico y la instauración de procesos transparentes que reduzcan riesgos. Se brindan recomendaciones específicas para los proveedores que quieren adoptar

IPv6, basadas en la experiencia práctica: realizar el dual-stack de manera progresiva, verificar la compatibilidad del firmware y hardware antes de empezar, y probar que los servicios críticos (DHCP, DNS, enrutamiento) estén funcionando adecuadamente antes de desactivar por completo IPv4.

Palabras clave: IPV4, IPV6, Migración a IPv6, Dual-stack, Mikrotik.

Abstract

Saturation of connected devices forced ISPs to employ temporary solutions to maintain operations, resulting in more complex and difficult-to-scale networks.

This thesis proposes migration to IPv6 as the necessary technical solution. It is not just theoretical: we implemented the change in a real ISP in Arequipa using MikroTik routers.

The entire process is documented, from the upgrade to RouterOS v7 for native support, to IP address assignment, routing, and DNS configurations. To monitor traffic, we used the built-in monitoring tools.

The findings highlight the challenges that must be overcome for a successful migration:

upgrading outdated equipment, intensive training of technical staff, and the implementation of transparent processes that reduce risks. Specific suggestions are provided for providers wanting to adopt IPv6, based on practical experience: implement dual-stack gradually, verify firmware and hardware compatibility before starting, and test that critical services (DHCP, DNS, routing) are functioning properly before completely disabling IPv4.

Key words: IPv4, IPv6, Migration to IPv6, Dual-stack, Mikrotik.

Índice general

Reconocimientos	v
Dedicatoria	vi
Reconocimientos	vii
Dedicatoria	viii
Resumen	ix
Abstract	x
Índice de figuras	xiv
Índice de Tablas	xvi
Introducción	xvii
1. Capítulo I	1
1.1. Situación problemática	1
1.2. Formulación del problema de investigación	3
1.3. Hipótesis	3
1.4. Objetivos de la investigación	3
1.4.1. Objetivo General	3
1.4.2. Objetivos Específicos	4
2. Capítulo II: Marco Teórico	5
2.1. Antecedentes	5
2.1.1. Antecedentes internacionales	5
2.1.2. Antecedentes nacionales	7
2.2. Bases Teóricas	9
2.2.1. Internet	9

2.2.2.	IPv4	10
2.2.3.	IPv6	10
2.2.4.	IPv6 en Perú	11
2.2.5.	Diferencias entre IPv4 e IPv6	12
2.2.6.	Técnicas de migración en IPv6	14
2.2.7.	Cabecera IPv6	16
2.2.8.	Cabecera IPv4	18
3.	Capítulo III: Marco Metodológico	21
3.1.	Tipo y Enfoque de Investigación	21
3.2.	Diseño de Investigación	21
3.3.	Contraste de Hipótesis	22
3.4.	Población y Muestra	23
3.4.1.	Población	23
3.4.2.	Muestra	23
3.5.	Técnicas e Instrumentos de Recolección de Datos	23
3.5.1.	Técnicas empleadas	23
3.5.2.	Instrumentos y Herramientas	23
3.5.3.	Equipos de Red	24
3.6.	Análisis y Procesamiento de Datos	25
4.	Capítulo IV: Resultados	26
4.1.	Evaluar el rendimiento actual de la red ISP SERVICIOS A PUNTO S.A.C en términos de latencia, pérdida de paquetes y disponibilidad de la red en IPv4	26
4.1.1.	Caracterización de la infraestructura de red	26
4.1.2.	Evaluación del rendimiento de la red en IPv4	32
4.1.3.	Análisis del rendimiento en IPV4	36

4.2.	Realizar la implementación de IPv6 en la red ISP SERVICIOS A PUNTO S.A.C con el método Dual Stack	37
4.2.1.	Actualización del firmware a RouterOS7	37
4.2.2.	Actualización del firmware a RouterOS7	40
4.2.3.	Configuración del direccionamiento IPv6	41
4.2.4.	Configuración de DHCPv6 y delegación de prefijos a usuarios . .	43
4.2.5.	Validación de conectividad IPv6	44
4.2.6.	Análisis de la implementación Dual Stack	46
4.3.	Comparar los resultados obtenidos antes y después de la migración en términos de latencia, pérdida de paquetes y disponibilidad de la red	47
4.3.1.	Evaluación del rendimiento de la red en IPv6 post- implementación	47
4.3.2.	Resumen estadístico del escenario IPv6 (Dual Stack)	53
4.3.3.	Análisis comparativo entre IPv4 e IPv6 (Dual Stack)	54
4.3.4.	Análisis del rendimiento del equipo posterior a la implementación Dual Stack	56
5.	Capítulo V: Discusión	62
5.1.	Evaluación del rendimiento de la red	62
5.2.	Implementación del método Dual Stack en la red del ISP	62
5.3.	Comparación de los resultados antes y después de la migración	63
6.	Conclusiones y Recomendaciones	65

Índice de figuras

3.1. Diseño de investigación.	22
4.1. Estructura actual de la red.	27
4.2. Tráfico registrado el 8 de marzo de 2024.	29
4.3. Tráfico registrado el 25 de mayo de 2024.	30
4.4. Tráfico registrado el 1 de junio de 2024.	30
4.5. Gráfica mensual del consumo de CPU en el MikroTik.	31
4.6. Gráfica mensual del consumo de memoria en el MikroTik.	32
4.7. Verificación de recursos del sistema tras la actualización a RouterOS 7. . .	38
4.8. Lista de paquetes instalados en el MikroTik CCR2116-12G-4S+ tras la actualización.	39
4.9. Información del RouterBOARD del equipo CCR2116-12G-4S+ con firm- ware actualizado.	39
4.10. Lista de direcciones IPv6 en el router de gestión CCR2116-12G-4S+ . . .	41
4.11. Enrutamiento IPv6 en el router BNG-CARAVELI	42
4.12. Enrutamiento IPv6 en el router de gestión CCR2116-12G-4S+	43
4.13. Lista de bindings activos del servidor DHCPv6-PD en el CCR2116-12G-4S+ .	44
4.14. Prueba de conectividad IPv6 hacia 2001:4860:4860::8888 desde BNG- CARAVELI	45
4.15. Prueba de conectividad IPv6 desde BNG-CARAVELI – Muestra de pa- quetes 32–50 con resultados a los 40 y 50 paquetes	46
4.16. Prueba de ping IPv6 – Prueba N.º 1(50 paquetes, 0% pérdida, avg-rtt 87ms535us)	49
4.17. Prueba de ping IPv6 – Prueba N.º 10 (50 paquetes, 0% pérdida, avg-rtt 87ms544us)	50
4.18. Prueba de ping IPv6 – Prueba N.º 20 (50 paquetes, 0% pérdida, avg-rtt 87ms564us)	50

4.19. Prueba de ping IPv6 – Prueba N.º 30 (50 paquetes, 0% pérdida, avg-rtt 87ms535us)	51
4.20. Prueba de ping IPv6 – Prueba N.º 40 (50 paquetes, 0% pérdida, avg-rtt 87ms537us)	52
4.21. Prueba de ping IPv6 – Prueba N.º 50 (50 paquetes, 0% pérdida, avg-rtt 87ms544us)	53
4.22. Estado de recursos del equipo BNG-CARAVELI en el escenario pre-implementación (RouterOS 7.14, CPU: 32 %)	57
4.23. Estado de recursos del equipo BNG-CARAVELI en el escenario pre - implementación (RouterOS 7.14, CPU: 28 %)	58
4.24. Estado de recursos del equipo BNG-CARAVELI en el escenario pre -i implementación (RouterOS 7.14, CPU: 27 %)	58
4.25. Estado de recursos del equipo BNG-CARAVELI en el escenario post-implementación (RouterOS 7.20.7, CPU: 4 %)	59
4.26. Estado de recursos del equipo BNG-CARAVELI en el escenario post-implementación 2 (RouterOS 7.20.7, CPU: 4%)	60

Índice de Tablas

4.1. Evaluación de rendimiento de la red en IPv4	34
4.2. Resultados de medición de latencia en IPv4 (mínimo, máximo, promedio)	35
4.3. Cálculo de pérdida de paquetes en IPv4	35
4.4. Evaluación de disponibilidad en IPv4	36
4.5. <i>Direcciones IPv6 configuradas en el router de borde BNG-CARAVELI</i> . .	40
4.6. Evaluación de rendimiento de la red en IPv6	48
4.7. <i>Resultados de medición de latencia en IPv6</i>	54

Introducción

El crecimiento exponencial del tráfico IP, impulsado por la proliferación de dispositivos IoT, los servicios en la nube y las demandas asociadas al desarrollo de redes 5G, ha puesto en evidencia las limitaciones intrínsecas del protocolo IPv4, especialmente en cuanto a la disponibilidad de direcciones. En agosto de 2020, LACNIC declaró el agotamiento de sus bloques IPv4, situación que obliga a operadores y entidades públicas a replantear sus estrategias de direccionamiento para garantizar la continuidad, estabilidad y, sobre todo, la escalabilidad de sus servicios.

Actualmente, el protocolo IPv6 se consolida como la respuesta técnica definitiva ante la saturación del direccionamiento IP. Su arquitectura no se limita a ofrecer una capacidad casi ilimitada de direcciones, sino que optimiza la eficiencia del enrutamiento, integra calidad de servicio de manera nativa y facilita la comunicación directa entre extremos. Pese a estas ventajas, su adopción global ha sido más lenta de lo previsto, principalmente porque el uso extendido de NAT permitió prolongar artificialmente la vigencia de IPv4. A esto se suman barreras tangibles para los operadores: la incompatibilidad de hardware legado, las inversiones requeridas, la curva de aprendizaje del personal técnico y el desafío de ejecutar una transición transparente sin afectar servicios críticos.

Bajo este panorama, la presente investigación diseña y valida una estrategia de migración hacia IPv6 adaptada a las necesidades de los Proveedores de Servicios de Internet (ISP). El propósito fundamental es demostrar que esta evolución tecnológica es tanto viable como indispensable para satisfacer la demanda de conectividad actual.

La metodología articula el análisis de mecanismos de transición como Dual Stack, tunelización y traducción— con una implementación práctica en la infraestructura de un ISP en la provincia de Caravelí. El alcance del proyecto cubre el ciclo completo: desde la actualización de los routers de borde a Mikrotik v7, la definición de esquemas de direccionamiento y DNS, hasta la validación operativa mediante el monitoreo de rutas y tráfico con herramientas nativas como Torch, Traceroute y Ping.

Capítulo I

1.1. Situación problemática

A nivel internacional, la transición de IPv4 a IPv6 avanza, pero de forma desigual y todavía con una fuerte dependencia de la coexistencia entre ambos protocolos. (Qu et al., 2024) señalaron que el uso de IPv6 en el lado del usuario final se ubica entre 30 % y 40 % a escala global, lo que evidencia que la migración está lejos de ser completa y que todavía existe una brecha importante entre regiones y operadores. En esa misma línea, (Bhuiyan et al., 2023) en Bangladesh mostró que la adopción pasó de menos de 1 % a 10.79 % en 2023, un crecimiento relevante pero aún insuficiente para hablar de una transición consolidada. Además, (Streibelt et al., 2023) investigaron sobre DNS en escenarios estrictamente IPv6-only donde encontraron que una fracción sustancial de zonas no podía resolverse, y que un solo operador era responsable de alrededor de 20.3 % de los dominios que no resolvían por IPv6 hasta enero de 2017, lo que demuestra que la infraestructura de servicios todavía presenta dependencias críticas de IPv4. Incluso en 2024, (Robinson et al., 2024) indicaron que la adopción global rondaba entre 40 % y 45 % a inicios de ese año, pero que la implantación plena seguía limitada por hardware legado y por la complejidad operativa de mantener IPv4 e IPv6 al mismo tiempo.

La migración de IPv4 a IPv6 continúa enfrentando limitaciones estructurales que obligan a los proveedores de servicios de Internet a mantener esquemas híbridos como Dual Stack, lo que incrementa la complejidad operativa y los costos de gestión de red. (Rizzo & Salerno, 2024) evidenciaron que más del 60 % de los operadores aún dependen de mecanismos de transición debido a incompatibilidades con infraestructura heredada, lo que retrasa una adopción total de IPv6. Por su parte, una evaluación comparativa de traductores host-based concluyó que el rendimiento varía según el escenario y que BIAv2 ofrece ventajas en throughput y overhead gracias al mapeo sin estado, lo que confirma que no existe una solución única ni completamente libre de costos para la migración (Hamarsheh et al.,

2023). Finalmente, (Wnorowski & Lebkowski, 2022) reveló que la implementación de mecanismos de transición como NAT64 y DNS64 introduce latencias adicionales de entre 10 % y 25 % en comparación con entornos nativos IPv6, lo que evidencia que la transición aún no logra niveles óptimos de eficiencia operativa.

En el Perú, la transición a IPv6 sigue siendo incipiente y desigual (Cala, 2025) estimó que apenas 5 % de las instituciones públicas había presentado propuestas de transición y que el tráfico IPv6 nacional alcanzaba solo 33.04 %, lo que evidencia una adopción todavía parcial del nuevo protocolo. Esta debilidad institucional también se refleja en el SENASA, donde (Acosta, 2024) trabajó con 30 trabajadores y encontró que, aunque 90 % calificó como bueno el planeamiento estratégico, la relación entre ese planeamiento y el proceso de transición a IPv6 fue solo moderada (Spearman = 0.530; $p = 0.003$), mostrando que la gestión interna aún no se traduce en una migración sólida. Del mismo modo, en el INEN se estudió una población de 400 usuarios y una muestra de 196, obteniendo una correlación positiva moderada (0.567; $p = 0.000$) entre la propuesta de IPv6 y la mejora de la comunicación de datos, lo que confirma que la implementación requiere planificación formal y no acciones aisladas.

En el ámbito de los ISP y redes de acceso, la problemática se vuelve más crítica porque la migración debe realizarse sin afectar la calidad del servicio. En el caso del ISP Conocible, (Barraza et al., 2024) con una población de 2,880 abonados y una muestra de 340 concluyó que integrar IPv6 en la red GPON mejora significativamente la calidad del servicio de internet ($p = 0.000$), relacionando directamente la migración con mejores condiciones de conectividad para el usuario. A ello se suma (Núñez, 2022), que propuso una implementación mediante Dual Stack, con inventario de recursos, nueva topología y un calendario de adopción gradual, precisamente porque IPv4 e IPv6 deben coexistir durante la transición. Además, el análisis nacional de 2025 reveló que solo seis instituciones públicas habían presentado propuestas de adopción y que algunos planes estimaban hasta 60 meses y 800,000 en recursos asignados, lo que sugiere que la migración sigue siendo lenta y demanda una planificación técnica y presupuestal cuidadosa (Cala, 2025).

La empresa SERVICIOS A PUNTO S.A.C., ubicada en Arequipa, ha experimentado un crecimiento sostenido en su cartera de clientes, especialmente en zonas remotas como la provincia de Caravelí; este incremento en la demanda ha generado una mayor presión sobre la infraestructura de red actualmente basada en el protocolo IPv4. El uso exclusivo de IPv4 representa una limitación técnica debido a la disponibilidad finita de direcciones, lo cual restringe la escalabilidad del servicio ante la incorporación de nuevos usuarios y dispositivos. Asimismo, la dependencia de este protocolo dificulta la integración con tecnologías modernas que operan de forma nativa en IPv6. En este contexto, surge la necesidad de evaluar alternativas que permitan la transición progresiva hacia IPv6 sin afectar la continuidad del servicio, siendo el método Dual Stack una opción viable para la coexistencia de ambos protocolos.

1.2. Formulación del problema de investigación

¿Cómo varía el comportamiento de la red del ISP SERVICIOS A PUNTO S.A.C. en términos de latencia, pérdida de paquetes y disponibilidad, al implementar el método Dual Stack en la migración de IPv4 a IPv6?

1.3. Hipótesis

La implementación del método Dual Stack genera variaciones en los indicadores de latencia, pérdida de paquetes y disponibilidad de la red del ISP SERVICIOS A PUNTO S.A.C., en comparación con el escenario basado únicamente en IPv4.

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Evaluar el comportamiento de la red del ISP SERVICIOS A PUNTO S.A.C. tras la implementación del método Dual Stack en la migración de IPv4 a IPv6, mediante el análisis comparativo de latencia, pérdida de paquetes y disponibilidad.

1.4.2. Objetivos Específicos

- 1.** Evaluar el rendimiento actual de la red ISP SERVICIOS A PUNTO S.A.C en términos de latencia, pérdida de paquetes y disponibilidad de la red en IPv4.
- 2.** Realizar la implementación de IPv6 en la red ISP SERVICIOS A PUNTO S.A.C con el método Dual Stack.
- 3.** Comparar los resultados obtenidos antes y después de la migración en términos de latencia, pérdida de paquetes y disponibilidad de la red.

Capítulo II: Marco Teórico

2.1. Antecedentes

2.1.1. Antecedentes internacionales

- Por su parte,(Almutlaq & Elfadil, 2022) en su investigación tuvo como objetivo medir el desempeño de las técnicas de transición IPv4 a IPv6 y determinar cuál era más conveniente para aplicaciones y redes actuales; la investigación puede describirse como cuantitativa, experimental y comparativa, con un diseño de simulación; la población fueron las técnicas de transición evaluadas y la muestra estuvo conformada por dual-stack, tunneling y translation (NAT-PT). Las técnicas e instrumentos utilizados fueron GNS3, VirtualBox, Packet Sender, Wireshark e iperf, con pruebas de retardo, throughput y flujo TCP. Los resultados mostraron que en dual-stack el retardo promedio fue de 61.4 ms en IPv4 y 33.2 ms en IPv6; en tunneling el retardo rondó los 31 ms y el throughput promedio fue de 1.08 Mbps; en translation el retardo llegó a un máximo de 57 ms y un mínimo de 36 ms, con throughput de 1.12 Mbps y un tiempo de establecimiento TCP de alrededor de 0.05 s. Se concluye que dual-stack fue la mejor opción para alto throughput, mientras que tunneling fue la más favorable para baja latencia.
- (Bhuiyan et al., 2023) en su investigación tuvo como objetivo detectar NAT64 en el mundo real y medir su impacto en el desempeño de red; la investigación es cuantitativa, observacional y comparativa; la población fue los probes de RIPE Atlas y la muestra estuvo formada por 224 probes en 43 redes, además de 34 probes dual-stack usados para comparación. Las técnicas e instrumentos utilizados fueron pruebas activas sobre RIPE Atlas y comparación de rutas y RTT entre acceso NAT64 e IPv4 nativo. Los resultados encontraron que las rutas NAT64 fueron, en promedio, 23.13 % más largas y con 17.47 % más RTT que las rutas IPv4 equivalentes. Se concluye que NAT64 permite conectividad IPv6-only hacia IPv4, pero introduce un

costo medible en desempeño.

- (Lencse & Bazsó, 2024) en su investigación tuvo como objetivo proponer y validar una metodología de benchmarking compatible con RFC 8219 para tecnologías IPv4-as-a-Service; la investigación es cuantitativa, experimental y metodológica; la población fueron las tecnologías 464XLAT, DS-Lite, Lw4o6, MAP-E y MAP-T, y la muestra de validación se centró en las implementaciones Jool de 464XLAT y MAP-T. Las técnicas e instrumentos utilizados fueron un método de reducción del setup dual-DUT, pruebas sobre un tester NAT44 y mediciones de rendimiento y escalabilidad. Los resultados indican que la metodología puede medir escalabilidad desde 1 hasta 16 CPU cores y desde 1 millón hasta 256 millones de conexiones, además de evaluar connection establishment rate y throughput. Se concluye que la propuesta resuelve una brecha práctica porque evita depender de testers específicos por tecnología.
- (Shahid et al., 2024) en su investigación tuvo como objetivo comparar el desempeño de EIGRP, OSPF y BGP en sistemas IPv6 de load-sharing y link-failover; la investigación es cuantitativa, experimental y comparativa, con diseño de simulación; la población fueron los protocolos de enrutamiento evaluados y la muestra correspondió a un entorno simulado con 13 routers; las técnicas e instrumentos utilizados fueron GNS3, VMware, Wireshark e Iperf3. Los resultados mostraron que sin autenticación EIGRP tuvo retardos de 30.21 a 30.39 s, mientras OSPF estuvo entre 30.24 y 30.35 s; con autenticación, EIGRP fue de 30.40 a 30.48 s y OSPF de 30.31 a 30.46 s. En jitter, EIGRP registró 35.66 a 44.11 ms y OSPF 37.01 a 45.64 ms; en packet loss, EIGRP obtuvo 5% y OSPF 5.4%; en convergencia, EIGRP recuperó en 134.2 s frente a 159.1 s de OSPF sin autenticación, y 14.3 s frente a 24.3 s con autenticación. Se concluye que EIGRP mostró mejor recuperación ante fallas y menor pérdida de paquetes que OSPF en ese entorno IPv6.
- (Hsu et al., 2024) en su investigación tuvo como objetivo medir el despliegue de NAT64 en Internet, así como sus problemas de configuración y seguridad; la in-

vestigación es cuantitativa, observacional y de medición a gran escala; la población fueron los despliegues NAT64 accesibles en Internet y la muestra incluyó mediciones sobre resolvers abiertos y RIPE Atlas. Las técnicas e instrumentos utilizados fueron consultas DNS diseñadas para provocar respuestas NAT64 y el análisis de respuestas en dominios reales y de control. Los resultados mostraron 2,021 despliegues NAT64 en 262 ASes, una tasa de configuración correcta de entre 60.7 % y 100 %, y entre 1.1 % y 26.6 % de gateways públicamente accesibles, lo que evidenció riesgos de seguridad. Se concluye que NAT64 existe en el mundo real, pero su despliegue es todavía escaso y heterogéneo.

2.1.2. Antecedentes nacionales

- (Cala, 2025) en su investigación tuvo como objetivo analizar la situación actual de la transición al protocolo IPv6 en las entidades públicas del Perú. El estudio se desarrolló con un enfoque mixto, usando datos secundarios y análisis documental. Los resultados reportan que IPv4 tiene aproximadamente 4.3 mil millones de direcciones, que en América Latina la adopción IPv6 llega a 51.58 %, que Perú registra 33.04 % de tráfico IPv6, y que en el gobierno peruano solo se observa cerca de 5 % de propuestas de transición. Se concluye que la adopción de IPv6 en el sector público peruano aún está lejos de consolidarse en el corto plazo.
- (Núñez, 2022) en su investigación tuvo como objetivo proponer la implementación del protocolo IPv6 en la sede central del Gobierno Regional Amazonas, específicamente en la Unidad de Tecnologías de la Información, frente al agotamiento global del IPv4; la investigación corresponde a una tesis de grado desarrollada en la Universidad Inca Garcilaso de la Vega, con un enfoque de propuesta técnica aplicada orientada a la migración de red. En el resumen visible del repositorio no se precisan población, muestra ni un diseño metodológico detallado; sin embargo, sí se indica que la propuesta se basa en el mecanismo de Doble Pila (Dual-Stack) para soportar simultáneamente IPv4 e IPv6. La técnica planteada consiste en realizar un inventario

de recursos de red, diseñar una nueva topología Dual-Stack y establecer un calendario de adopción gradual. Los resultados descritos señalan que la implementación permitiría contar con un diseño robusto de red basado en IPv6, con capacidad de crecer sin limitaciones de direccionamiento y con una red de datos más eficiente. Se concluye que la migración mediante Dual-Stack es una alternativa viable para la coexistencia gradual de IPv4 e IPv6 en la entidad.

- (Palma, 2022) en su investigación tuvo como objetivo identificar la relación entre la seguridad IPv4 y los sistemas de información en trámites administrativos de los funcionarios de la UNAMBA, región Apurímac, la investigación es de tipo básico, con un enfoque cuantitativo, y con un diseño no experimental, de corte transversal y correlacional, la población que se consideró fue el personal que labora en las 41 oficinas de la Universidad Nacional Micaela Bastidas de Apurímac, ciudad de Abancay, y la muestra fue de 35 trabajadores. Las técnicas e instrumentos que se utilizaron en el estudio fueron la encuesta y el cuestionario, el cual contó con 4 ítems para la variable seguridad IPv4 y 7 ítems para la variable sistemas de información; además, la información fue procesada con SPSS versión 26. Los resultados encontrados muestran que la variable seguridad IPv4 se relaciona directa y significativamente con la variable sistemas de información, obteniendo un coeficiente de correlación Rho de Spearman de 0.671 y un p-valor de 0.000. Se concluye que ambas variables presentan una correlación positiva moderada.
- En cuanto a (Castro & Ruez, 2023) en su investigación tuvieron como objetivo ampliar el pool de direcciones IP públicas mediante la migración de una arquitectura WAN basada en IPv4 hacia IPv6 en una red corporativa en el Perú; la investigación es de tipo aplicada, con un enfoque cuantitativo y con un diseño no experimental; las técnicas e instrumentos utilizados fueron el análisis de la infraestructura de red existente, el diseño de arquitectura híbrida (LAN en IPv4 y WAN en IPv6) y la evaluación del uso de tecnologías como túneles VPN y direccionamiento IP público, aplicados para la transición de red. Los resultados encontrados muestran

que la implementación de una arquitectura híbrida permite optimizar el uso de direcciones IP públicas, reducir la dependencia del IPv4 y mejorar la escalabilidad de la red corporativa, resolviendo la limitación del agotamiento de direcciones IPv4 en entornos empresariales. Se concluye que la migración hacia IPv6 mediante un enfoque híbrido es una solución viable y necesaria para garantizar la continuidad y crecimiento de redes corporativas en el Perú.

- (Cervantes, 2024) en su investigación tuvo como objetivo proponer una mejora en la infraestructura o gestión tecnológica dentro del entorno de la Universidad Nacional Pedro Ruiz Gallo; la investigación es de tipo aplicada, con un enfoque cuantitativo y con un diseño no experimental; las técnicas e instrumentos que se utilizaron en el estudio fueron el análisis de la situación actual del sistema, el diagnóstico de la infraestructura tecnológica y la propuesta de mejora basada en tecnologías de información, aplicadas para optimizar el funcionamiento de la red o sistema evaluado. Los resultados encontrados muestran la existencia de deficiencias en la gestión y funcionamiento del sistema, lo que evidencia la necesidad de implementar mejoras tecnológicas para optimizar el rendimiento y la eficiencia del servicio. Se concluye que la propuesta planteada contribuye a mejorar la gestión tecnológica y el desempeño del sistema, permitiendo un mejor aprovechamiento de los recursos informáticos.

2.2. Bases Teóricas

2.2.1. Internet

Conceptualmente, Internet (del inglés Interconnected Networks) se define como la infraestructura global que integra redes heterogéneas bajo la arquitectura de protocolos TCP/IP. Esta capacidad de interoperabilidad es la que permite enlazar sistemas distribuidos en cualquier ubicación geográfica, desde grandes centros de datos hasta dispositivos de usuario final. Se trata de un entorno donde interactúan entidades académicas, gubernamentales y privadas para el intercambio masivo de servicios e información. Desde una perspectiva

histórica, los cimientos de esta red se remontan a 1969 con el proyecto ARPANET, impulsado por el Departamento de Defensa de los Estados Unidos. Aunque su diseño original buscaba conectar centros de investigación y contratistas militares, su estructura sentó las bases lógicas para la comunicación digital moderna. ARPANET siguió evolucionando hasta 1990, año en que cesó sus operaciones para dar paso definitivo a la consolidación de la Internet comercial tal como la conocemos hoy (Salas, 2022).

2.2.2. IPv4

Oficializado el 1 de enero de 1983, IPv4 se mantiene hasta hoy como el protocolo predominante a nivel global; asimismo, tanto este como IPv6 estructuran su asignación de direcciones bajo un modelo jerárquico. Los usuarios obtienen direcciones IP de sus proveedores de servicios de Internet (ISP). Estos ISP, a su vez, reciben asignaciones de direcciones IP de un Registro de Internet local (LIR), un Registro Nacional de Internet (NIR) o el Registro Regional de Internet (RIR) correspondiente (Gomez-Rodriguez et al., 2016).

IPv4 puede considerarse un logro importante en la historia de la tecnología de la información debido a su exitosa adopción a nivel global, estableciendo un modelo a seguir para futuros desarrollos. Es fundamental comprender las fortalezas y debilidades de IPv4, ya que esta comprensión contribuye a entender la evolución de IPv6. IPv6 puede considerarse como una versión "potenciada" de IPv4, considerando las diferencias fundamentales en la estructura actual de las redes y las soluciones a los desafíos encontrados en las primeras tres décadas de Internet basada en IP (Hughes, 2022).

2.2.3. IPv6

IPv6 no es un protocolo nuevo, sino que se comenzó a diseñar a principios de la década de los 90 como una respuesta a la creciente escasez de direcciones IPv4.

A pesar de que las especificaciones iniciales se establecieron en 1995 (Deering & Hinden, 1995), su incorporación masiva tomó tiempo debido a la inversión económica requerida y la prevalencia de IPv4 en ese momento, así como la introducción de tecnologías

como la Traducción de Direcciones de Red (NAT) y el Enrutamiento entre Dominios sin Clases (CIDR) para mitigar la escasez de direcciones IPv4. Sin embargo, a medida que se iba agotando las direcciones IPv4 se volvió más inminente, entonces se hizo evidente que IPv6 era la solución a largo plazo, se intensificaron los esfuerzos de desarrollo y adopción. Diversos sistemas operativos implementaron IPv6 experimentalmente, y se desarrollaron estándares adicionales.

El resurgimiento del interés en IPv6 a partir de 2007 se debió a que el espacio de direcciones IPv4 estaba agotándose rápidamente. La introducción de direcciones IPv6 en servidores DNS raíz y la publicación del Plan de Transición (Curran, 2008) en 2008 marcaron pasos importantes en la preparación para la transición a IPv6.

Desde entonces, la adopción de IPv6 ha seguido creciendo a medida que se reconoce cada vez más como la solución necesaria para abordar la falta de direcciones IPv4 y respaldar la expansión continua de Internet y la proliferación de dispositivos conectados (Macho, 2012).

IPv6, elegido como la propuesta final de IPng en 1995, representa una reingeniería de la tecnología IP con un espacio de direcciones IP más grande y estructuras de encabezado de paquetes más simples, facilitando la implementación de aceleración de hardware para enrutadores IPv6; además, permite extensiones de protocolo más flexibles mediante una cadena de cabecera de protocolo, sin imponer sobrecarga a los enrutadores intermedios, desde la perspectiva de un programador, IPv4 e IPv6 son prácticamente iguales en términos de dirección IP y números de (itojun Hagino, 2005).

2.2.4. IPv6 en Perú

El gobierno peruano, liderado por el Ministerio de Transportes y Comunicaciones (MTC), ha tomado pasos concretos para acelerar la adopción de IPv6. Han puesto en marcha iniciativas para capacitar y concientizar a las organizaciones, y lo que es más importante, han fijado plazos obligatorios para que sectores clave —como telecomunicaciones, educación y el propio gobierno— completen la transición. Esto demuestra un compromiso estatal firme para asegurar que Perú responda a las necesidades tecnológicas

del presente y el futuro (Tomy Baltazar, 2017).

Si bien la implementación de IPv6 en Perú avanza, aún quedan obstáculos considerables por superar. Los mayores retos giran en torno a asegurar una infraestructura totalmente compatible, formar al personal técnico que gestionará el cambio y garantizar que el usuario final viva una transición totalmente transparente. Superados estos desafíos, el impacto en la conectividad será enorme. La adopción de IPv6 no solo permitirá la masiva incorporación de nuevos dispositivos a la red, sino que también será el motor para la innovación y facilitará la llegada de tecnologías de punta, como el Internet de las Cosas (IoT), a casi todos los sectores del país (Delgado, 2017).

2.2.5. Diferencias entre IPv4 e IPv6

- **Dirección**

El problema de IPv4 es su tamaño: utiliza solo 32 bits, lo que genera 4,294,967,295 de direcciones únicas. Peor aún, una parte de ese espacio ya está asignada a usos especiales (como las redes privadas), reduciendo la cantidad que podemos usar realmente. IPv6 resuelve esto. Sus direcciones tienen 128 bits, divididas en ocho segmentos hexadecimales. Gracias a esto, el espacio es, sencillamente, enorme, capaz de gestionar la explosión de dispositivos que vemos hoy en día y las que vendrán en el futuro, sin preocuparse nunca por la escasez (Prieto, 2018).

- **Cabecera de IPv6**

La cabecera de IPv6 es notablemente más simple y eficiente, con un tamaño fijo de 40 bytes que no cambia (a diferencia de IPv4) y consta de 8 campos. Los campos de fragmentación presentes en la cabecera de IPv4 se han eliminado de la cabecera principal de IPv6 y se han trasladado a una cabecera de extensión. Además, los enrutadores IPv6 no están autorizados a fragmentar los paquetes que reenvían; solo el remitente original de un paquete IPv6 tiene la capacidad de dividir el paquete en fragmentos. Esto logra un enrutamiento más eficiente, ya que solo se procesa la información necesaria para cada enrutador (Durdagl & Buldu, 2010).

- Seguridad

La diferencia fundamental en términos de seguridad entre IPv4 e IPv6 radica en la obligatoriedad de implementar IPSec en IPv6, tal como se estipula en el RFC 2460, que es la especificación clave para el Protocolo de Internet versión 6. Esto se traduce en la posibilidad de asegurar todas las comunicaciones IP de extremo a extremo, siempre y cuando se cuente con la infraestructura adecuada a gran escala (Chamba, 2022).

- Comunicación de extremo a extremo

A diferencia de IPv4, que utiliza NAT y limita la comunicación de extremo a extremo, IPv6 permite asignar una única dirección IP a cada dispositivo conectado a Internet, facilitando la comunicación directa y mejorando la conectividad global (Prieto, 2018).

- Eficiencia y Fragmentación

IPv6 requiere que cada enlace en Internet tenga un MTU (Unidad de Transmisión Máxima) de al menos 1280 bytes. Si el MTU en un enlace es menor a 1280 bytes, los nodos IPv6 recibirán mensajes de error PTB (Paquete Demasiado Grande). A diferencia de IPv4, en IPv6 no se permite la fragmentación de paquetes en los routers. Si un paquete necesita fragmentarse debido a un MTU más pequeño, la responsabilidad recae en el origen para realizar la fragmentación, similar a IPv4. Esta diferencia en IPv6 contribuye a una comunicación más eficiente al simplificar la gestión de fragmentación y mejorar la integridad de los datos en comparación con IPv4 (Chen et al., 2014).

- Compatibilidad con QoS

IPv6 incluye un mecanismo llamado flujos etiquetados en sus especificaciones para ofrecer un mejor soporte al tráfico en tiempo real, como la voz sobre IP. Este mecanismo permite que los enrutadores reconozcan a qué flujo de extremo a extremo pertenecen los paquetes que se están transmitiendo. Esto es similar al

servicio proporcionado por Multi-Protocol Label Switching (MPLS), pero en el caso de IPv6, está integrado directamente en el mecanismo IP en lugar de ser un complemento separado (Sailan et al., 2009).

2.2.6. Técnicas de migración en IPv6

Una migración a IPv6 puede llevarse a cabo de diversas maneras, dependiendo de las necesidades y la infraestructura de cada red. A continuación se explicará algunas estrategias para migrar a IPv6:

■ Dual Stack

Dual-Stack es un enfoque de transición para la implementación de IPv6 que hace posible que IPv4 e IPv6 funcionen al mismo tiempo en una misma red. El empleo de túneles y métodos de traducción de protocolos complementa esta estrategia, facilitando la conexión entre redes o dispositivos que todavía no tienen conectividad nativa IPv6. El autor, no obstante, piensa que Dual-Stack tiene pocas probabilidades de conseguir una adopción total y generalizada de IPv6 por los gastos operativos que supone y la dificultad de mantener simultáneamente ambos protocolos (Dell, 2018).

En pocas palabras Dual-Stack implementa tanto a IPv4 como IPv6 de manera simultánea, permitiendo una migración gradual, ya que los dispositivos pueden comunicarse con sistemas que usan IPv4 e IPv6.

■ Tunelización

Implementar IPv6 utilizando métodos de túneles permite la coexistencia y transición entre redes IPv4 e IPv6. Los túneles proporcionan una forma de transportar paquetes IPv6 sobre una red IPv4. Aquí se presentan los cinco métodos de túneles para el tráfico IPv6:

- **Túneles IPv6 manuales** En los túneles IPv6 manuales, los puntos finales del túnel se configuran de forma explícita, y los paquetes se encapsulan y desen-

capsulan de forma manual. Este método requiere la configuración manual de los puntos finales del túnel.

- **Túneles automáticos compatibles con IPv4** Los túneles automáticos compatibles con IPv4 encapsulan automáticamente los paquetes IPv6 dentro de paquetes IPv4 usando direcciones IPv4 específicas. Estos túneles se establecen sin configuración manual.
- **Encapsulación de Enrutamiento Genérico (GRE)** GRE es un protocolo de túnel que puede transportar una amplia variedad de protocolos de capa de red sobre conexiones punto a punto. A menudo se utiliza para crear conexiones de red privada a través de Internet.
- **Túneles automáticos 6to4** Los túneles 6to4 permiten la encapsulación automática de paquetes IPv6 dentro de paquetes IPv4. Los puntos finales del túnel se determinan en función de las direcciones IPv4 e IPv6.
- **Túneles mediante Protocolo de Direccionamiento Automático Intra-Sitio (ISATAP)**: Este mecanismo permite la interconexión de hosts y redes de doble pila utilizando la infraestructura IPv4 existente como medio de transporte. Su principal utilidad radica en la generación de túneles automáticos dentro de un mismo dominio administrativo (como una red corporativa), facilitando el despliegue de IPv6 sin requerir configuraciones manuales punto a punto en cada dispositivo.

Las principales limitaciones de los mecanismos de túneles incluyen un único punto de fallo, la dificultad para atravesar firewalls y la necesidad de actualizar y cambiar el equipo de instalaciones del cliente (CPE). En general, se prefiere el uso de túneles frente a NAT-PT (Traducción de Direcciones de Red - Traducción de Protocolo) o mecanismos de traducción debido a su mejor rendimiento en términos de ancho de banda y tiempo de ida y vuelta(Jadhav & Ballal, 2022).

- **Traducción de Protocolos** Utiliza dispositivos de traducción para permitir la co-

municación entre dispositivos IPv4 e IPv6 sin requerir la implementación de IPv6 en los dispositivos IPv4. Tal como menciona en su artículo,(Hong et al., 2003), nos dice que una de las estrategias para abordar la transición de IPv4 a IPv6 es el uso de puertas de enlace de capa de aplicación (ALG) que pueden traducir los datos de la capa de aplicación entre los dos protocolos. Estas ALG se pueden implementar a nivel de enrutador o puerta de enlace, lo que facilita la comunicación entre aplicaciones IPv4 e IPv6 sin necesidad de implementar IPv6 a nivel de host. Este enfoque asegura que la infraestructura IPv4 existente siga siendo compatible mientras permite la comunicación efectiva entre dispositivos que utilizan IPv4 e IPv6.

2.2.7. Cabecera IPv6

La cabecera IPv6, como lo define (Torres Sánchez, 2017), consta de 64 bits de longitud, lo que permite un procesamiento más eficiente por las CPU de 64 bits, ya que estas pueden leer una palabra de memoria de 64 bits a la vez. Esta cabecera, esencial para dirigir el flujo de datos desde un emisor hasta un receptor, se compone de 40 octetos en IPv6, a diferencia de la versión anterior de IP que tenía solo 20, lo que reduce los campos de 12 en IPv4 a solo 8 en IPv6. Además, IPv6 ofrece una cabecera de longitud fija al eliminar opciones poco utilizadas.

Los elementos en la cabecera IPv6 se componen de los siguientes campos:

- **Versión:** se identifica mediante un campo de 4 bits, similar al enfoque empleado en IPv4, siendo la diferencia principal el número 6 utilizado en IPv6 en lugar del 4 que caracteriza a IPv4.
- **Clase de Tráfico:** Este campo de 8 bits asume la función crítica de gestión de Calidad de Servicio (QoS). Evolucionando el concepto de *Type of Service* (ToS) de IPv4, permite clasificar y priorizar los paquetes dentro de la red (por ejemplo, diferenciando tráfico de voz sobre IP frente a datos generales), facilitando así la implementación de arquitecturas de Servicios Diferenciados (DiffServ).

- **Etiqueta de Flujo:** Recurso de 20 bits diseñado para optimizar el enrutamiento de tráfico en tiempo real. Su función es identificar secuencias de paquetes que requieren un tratamiento especial y coherente por parte de los routers intermedios, evitando la necesidad de reevaluar las políticas de servicio paquete por paquete y agilizando el procesamiento en el núcleo de la red.
- **Longitud de Carga Útil:** A diferencia de la métrica de longitud total en IPv4, este campo de 16 bits cuantifica exclusivamente el tamaño de la información transportada tras la cabecera principal (incluyendo posibles cabeceras de extensión y datos de capa superior). Su capacidad estándar permite manejar cargas de hasta 65,535 bytes.
- **Siguiente Cabecera:** Este selector de 8 bits es la clave de la flexibilidad de IPv6. En lugar de utilizar campos de opciones complejos, indica qué protocolo o cabecera de extensión sigue inmediatamente a la actual. Este mecanismo de encadenamiento simplifica drásticamente la estructura base del paquete, permitiendo a los routers procesar la información de manera más eficiente al ignorar extensiones que no les conciernen.
- **Límite de Salto:** Mecanismo de seguridad de 8 bits que previene la circulación perpetua de paquetes debido a bucles de enrutamiento. Funcionalmente equivalente al TTL (*Time to Live*) de IPv4, este valor decrece en cada nodo que atraviesa el paquete; si el contador llega a cero antes de alcanzar el destino, el paquete se descarta, garantizando la estabilidad de la red.
- **Dirección de Origen:** Bloque de 128 bits que identifica de manera unívoca al emisor del paquete. Más allá de una simple etiqueta, su estructura permite la validación de prefijos y es fundamental para los mecanismos de respuesta y seguridad, como el filtrado de tráfico en los bordes de la red.
- **Dirección de Destino:** Campo final de 128 bits que señala al receptor intencionado. Dependiendo de la naturaleza de la comunicación (Unicast, Multicast o Anycast), este campo determina si el paquete debe ser procesado por un único nodo específico,

un grupo de interfaces o el dispositivo más cercano dentro de un grupo, guiando las decisiones de reenvío en cada salto.

2.2.8. Cabecera IPv4

A continuación se detalla la arquitectura del encabezado de un datagrama IPv4, desglosando la disposición de sus campos de control. El análisis de estos componentes resulta indispensable para comprender la lógica de enrutamiento y los mecanismos de procesamiento que ejecutan los dispositivos de red durante la transmisión de datos (Manayay Ramírez & Olivera Samamé, 2015).

Los elementos que integran la cabecera IPv4 se describen a continuación::

- **Versión:** está formada por 4 bits y especifica la versión del protocolo utilizada. En la mayoría de redes actuales este valor corresponde a la versión 4. Su función es garantizar la correcta identificación y compatibilidad del encabezado durante la transmisión de datos.
- **IHL(Internet Header Length):** indica la longitud de la cabecera en palabras de 32 bits. El mínimo permitido es de 5 palabras cuando no existen opciones, y el máximo es de 15. Este parámetro determina cuánta información de control puede incluirse en el paquete.
- **Type of service(TOS):** se emplea para asignar prioridad al tráfico según las necesidades del servicio. Por ejemplo, en la transmisión de voz digital la velocidad es prioritaria, mientras que en la transferencia de archivos es más importante la entrega sin errores. Originalmente, este campo contaba con 6 bits: tres destinados a la prioridad y tres para indicar retardo, rendimiento y confiabilidad; los dos bits restantes quedaron reservados para futuras aplicaciones.
- **Longitud total:** compuesto por 16 bits, define la longitud total del datagrama (cabecera más datos) en bytes. Aunque el valor máximo es de 65 535 bytes, esto resulta insuficiente para redes de alta velocidad como Gigabit Ethernet, por lo que se

sugiere que las estaciones envíen datagramas de al menos 576 bytes para garantizar un funcionamiento adecuado.

- **Identificación:** también de 16 bits, permite reconocer a qué datagrama corresponde cada fragmento recibido. Todos los fragmentos generados a partir de un mismo datagrama comparten este identificador, lo que facilita su reensamblaje en el destino.
- **Flags o banderas:** está compuesto por 3 bits que actúan como indicadores de control. El primero siempre es 0 y se reserva para usos futuros. El segundo es el bit DF (Don't Fragment), que indica si el datagrama puede fragmentarse. El tercero es el bit MF (More Fragments), el cual señala si existen más fragmentos pendientes de recibir. Estos bits son esenciales para gestionar la fragmentación en la red.
- **Fragment offset o desplazamiento de fragmento:** con 13 bits, indica la posición de un fragmento dentro del datagrama original. Excepto el último, cada fragmento debe tener un tamaño múltiplo de 8 bytes para permitir su reconstrucción. El número máximo de fragmentos por datagrama es de 8192.
- **Tiempo de vida o time to live:** es un campo de 8 bits que define el tiempo máximo que un datagrama puede circular en la red. Funciona como un contador que se decrementa por cada salto entre enrutadores. Una vez que el valor llega a cero, el paquete es descartado y se envía un mensaje ICMP. Con ello se evita que datagramas sin destino saturen la red.
- **Protocolo:** segmento de 8 bits en un datagrama que especifica el protocolo de capas superiores al cual debe entregarse el paquete. El RFC 1700 es una referencia que contiene los números asociados a numerosos protocolos, y este campo es esencial para asegurar que el paquete sea direccionado y procesado correctamente en función del protocolo que lo utilizará en las capas superiores del modelo OSI.
- **Checksum header o suma de verificación de cabecera:** segmento de 16 bits en un datagrama que cumple la función de realizar una suma de verificación para detectar errores causados por posibles alteraciones en la cabecera del paquete durante su

tránsito a través de enrutadores. Esta comprobación se lleva a cabo en cada salto o enrutador que el paquete atraviesa, ya que al menos uno de los campos de la cabecera (el “Tiempo de Vida”) cambia en cada salto, lo que requiere una nueva verificación. El algoritmo empleado suma las secuencias de 16 bits a medida que llegan, utilizando aritmética en complemento a uno, y luego obtiene el complemento a uno del resultado. Para simplificar el cálculo y asegurar que la cabecera esté íntegra, se le asigna un valor inicial de 0 a la suma de verificación. Para la detección y la corrección de fallos en el encabezado del datagrama mientras se transporta por la red, esta técnica es fundamental.

- **Campos source y destination address:** ambos campos cuentan con 32 bits y representan las direcciones IP del host emisor y del receptor. Estas direcciones, compuestas por cuatro octetos, permiten el enrutamiento correcto de los paquetes en la red.
- **Opciones:** es un campo opcional y de longitud variable. Se utiliza principalmente para propósitos experimentales, pruebas o para evitar asignar bits a información que rara vez se necesita. Cada opción inicia con un código de un octeto y, en algunos casos, incluye un campo de longitud y varios octetos de datos. Su estructura permite completar la cabecera en múltiplos de 32 bits, ofreciendo flexibilidad según los requerimientos de comunicación.

Capítulo III: Marco Metodológico

El presente capítulo estructura la ruta metodológica diseñada para alcanzar los objetivos del estudio. Se detallan el tipo y diseño de la investigación, así como los instrumentos seleccionados para la recolección de métricas de red y el procedimiento analítico utilizado para validar las mejoras tras la implementación tecnológica.

3.1. Tipo y Enfoque de Investigación

La investigación se clasifica como **aplicada**, dado que orienta los fundamentos de la ingeniería hacia la resolución de una problemática operativa tangible: la saturación del direccionamiento IPv4 en la infraestructura del ISP SERVICIOS A PUNTO S.A.C. La finalidad trasciende la mera descripción teórica, buscando la implementación efectiva de la arquitectura *Dual Stack* para optimizar la continuidad y escalabilidad del servicio.

Por su parte, el enfoque adoptado es **cuantitativo**, porque se basa en la medición objetiva y numérica de indicadores técnicos de desempeño de red, específicamente latencia (ms), pérdida de paquetes (%) y disponibilidad (%), antes y después de la implementación del método Dual Stack.

3.2. Diseño de Investigación

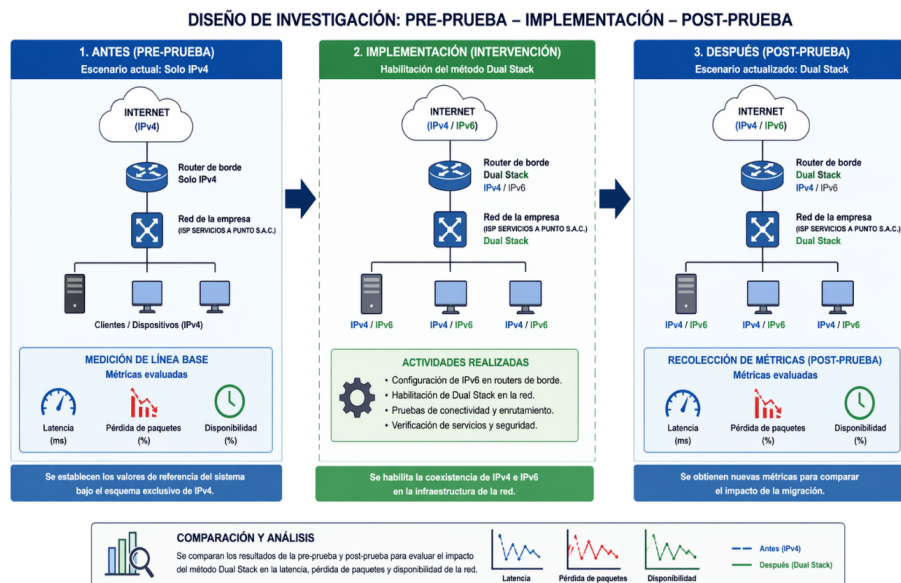
Se adoptó un diseño pre-experimental con esquema de pre-prueba y post-prueba en un solo grupo de estudio, aplicado sobre la infraestructura real del ISP SERVICIOS A PUNTO S.A.C. El estudio se orienta a una evaluación técnica comparativa antes y después de implementar el método Dual Stack bajo condiciones reales de servicio. La ejecución del esquema pre-experimental se organizó en las siguientes fases:

- Diagnóstico y medición del rendimiento de la red operando bajo el esquema exclusivo de IPv4 para establecer los valores de referencia del sistema.
- Habilitación de la coexistencia de los protocolos IPv4 e IPv6 en los routers de borde y de gestión.

- Recolección de nuevas métricas bajo el entorno actualizado para cuantificar el impacto de la migración en los indicadores de calidad de servicio.

Figura 3.1

Diseño de investigación.



La recolección de datos se realizó en dos escenarios: antes y después de la implementación del método Dual Stack, manteniendo condiciones similares de medición en términos de horarios, herramientas y puntos de evaluación. Las métricas analizadas fueron latencia, pérdida de paquetes y disponibilidad, obtenidas mediante herramientas de diagnóstico de red.

3.3. Contraste de Hipótesis

El contraste de la hipótesis se realizó mediante un análisis comparativo descriptivo de las métricas de desempeño de la red antes y después de la implementación del método Dual Stack.

-En la fase de línea base (pre-prueba), se registraron valores de latencia, pérdida de paquetes y disponibilidad bajo operación exclusiva en IPv4, estableciendo los valores de referencia del sistema.

-Tras la implementación (post-prueba), se recolectaron nuevamente las mismas métricas bajo condiciones de medición equivalentes.

El contraste se efectuó mediante la comparación directa de los indicadores entre ambos escenarios, con el fin de identificar variaciones en el comportamiento de la red.

3.4. Población y Muestra

3.4.1. Población

El universo de estudio comprende la totalidad de la infraestructura de red activa perteneciente a la empresa SERVICIOS A PUNTO S.A.C.

3.4.2. Muestra

La muestra es no probabilística y se centra específicamente en el enlace troncal y los clientes activos de la zona de Caravelí, donde se aplicó la migración.

3.5. Técnicas e Instrumentos de Recolección de Datos

3.5.1. Técnicas empleadas

Observación directa: Se empleó la técnica de observación directa estructurada para registrar el comportamiento de la red en condiciones reales de operación. Esta técnica permitió monitorear de manera sistemática las métricas de desempeño (latencia, pérdida de paquetes y disponibilidad) mediante la ejecución de pruebas en puntos específicos de la red. La observación se realizó en dos escenarios (pre y post implementación), manteniendo condiciones similares de medición en términos de horarios, herramientas y nodos evaluados, con el fin de garantizar la comparabilidad de los datos obtenidos.

3.5.2. Instrumentos y Herramientas

- **Ficha de observación estructurada:** Se utilizó una ficha de observación diseñada para el registro sistemático de las métricas de desempeño de la red. Este instrumento permitió documentar los valores obtenidos en cada prueba realizada, incluyendo

información como la latencia, pérdida de paquetes y disponibilidad. La ficha fue aplicada de manera uniforme en los escenarios de pre-prueba y post-prueba, garantizando la consistencia en la recolección de datos.

- **Wireshark:** Esta herramienta se empleó como analizador de protocolos para realizar la captura profunda de paquetes en las interfaces de red. Su aplicación fue fundamental para inspeccionar la estructura de las cabeceras y validar la integridad del tráfico durante las pruebas de transmisión.
- **WinBox:** Herramienta de gestión propietaria que sirvió como interfaz principal para la configuración de los equipos MikroTik. A través de ella se administraron las reglas de enrutamiento, el direccionamiento IP y se monitoreó el consumo de recursos en tiempo real.

3.5.3. Equipos de Red

La plataforma de pruebas se desplegó sobre una infraestructura de hardware operativa, conformada por los siguientes nodos críticos:

- Como punto de interconexión con el proveedor de servicios, se utilizó un router de alto rendimiento modelo **CCR1072-1G-8S+**.
- La función de enrutamiento de borde fue asumida por un equipo **CCR2216-1G-12XS-2XQ**, encargado de gestionar el tráfico troncal de la red.
- Para las labores de gestión y segmentación lógica, se integró un router MikroTik modelo **CCR2116-12G-4S+**, que opera como administrador del sistema.
- Finalmente, la red de acceso se materializó mediante una OLT **ZTE C620** y terminales ópticos (ONUs) de fabricantes ZTE y Optitimes. Este equipamiento permitió validar la compatibilidad y medir la eficiencia del protocolo IPv6 en el segmento de última milla hacia el usuario final.

3.6. Análisis y Procesamiento de Datos

Los datos recolectados durante las fases de pre-prueba y post-prueba fueron organizados y procesados mediante un enfoque descriptivo-comparativo. Inicialmente, los valores obtenidos de latencia, pérdida de paquetes y disponibilidad fueron registrados en tablas estructuradas, diferenciando ambos escenarios de evaluación.

Los resultados procesados fueron representados mediante tablas comparativas y gráficos, con el objetivo de visualizar las variaciones en el comportamiento de la red antes y después de la implementación del método Dual Stack.

Finalmente, se efectuó un análisis comparativo de los indicadores obtenidos, permitiendo identificar diferencias en el desempeño de la red en términos de latencia, pérdida de paquetes y disponibilidad, bajo condiciones equivalentes de medición.

Capítulo IV: Resultados

4.1. Evaluar el rendimiento actual de la red ISP SERVICIOS A PUNTO S.A.C en términos de latencia, pérdida de paquetes y disponibilidad de la red en IPv4

Con el propósito de establecer una línea base del comportamiento de la red del ISP SERVICIOS A PUNTO S.A.C., se realizó una evaluación del rendimiento operando bajo el esquema exclusivo de IPv4. Esta fase permitió obtener valores de referencia en términos de latencia, pérdida de paquetes y disponibilidad, los cuales servirán como punto de comparación frente al escenario posterior con implementación Dual Stack.

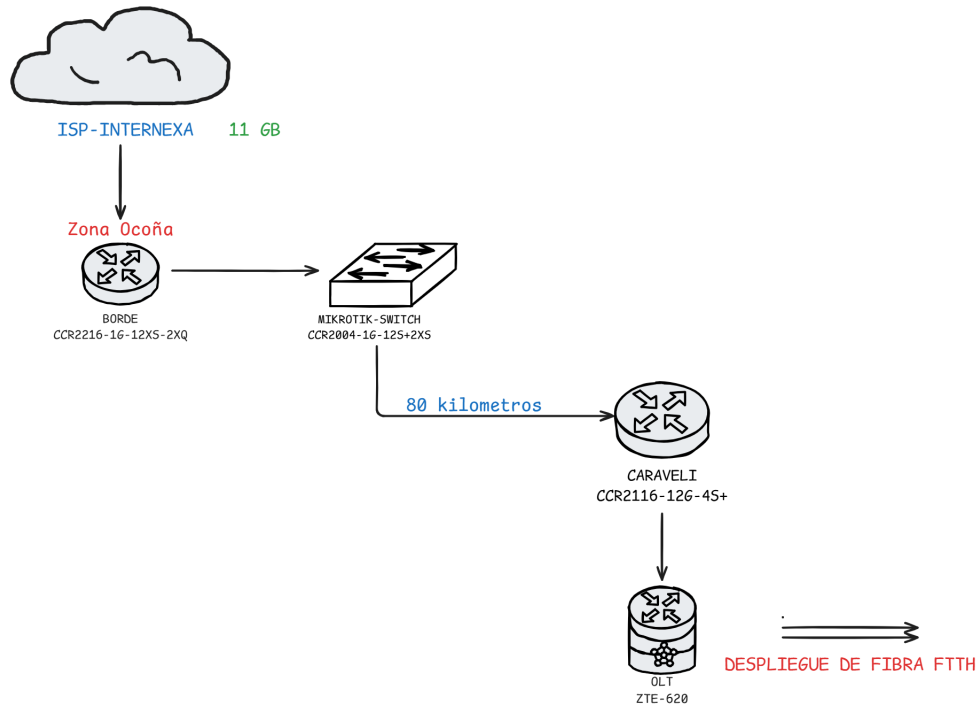
4.1.1. Caracterización de la infraestructura de red

La red evaluada corresponde a la infraestructura operativa del ISP en la provincia de Caravelí, la cual se encuentra soportada por equipos de enrutamiento, conmutación y acceso óptico. Entre los principales componentes se identifican routers de borde, switches de distribución y una OLT encargada de la gestión de usuarios finales. El sistema actualmente opera bajo direccionamiento IPv4, atendiendo a una base activa de usuarios distribuidos en zonas geográficamente dispersas, lo cual introduce condiciones variables de tráfico y demanda sobre la red.

- **Tipología de red**

Figura 4.1

Estructura actual de la red.



En la capa física, la conectividad se establece mediante enlaces de fibra óptica que cumplen con el estándar G.652D, lo cual garantiza una adecuada transmisión de datos en largas distancias. La interconexión de los tramos de fibra se realiza mediante procesos de fusión, ejecutados en una mufa ubicada aproximadamente a 20 kilómetros del punto de operación. Para la transmisión óptica se emplean transceptores pasivos con un alcance de hasta 40 kilómetros, equipados con conectores tipo LC, asegurando la continuidad y estabilidad del enlace físico.

En cuanto a la provisión del servicio de Internet, este es suministrado por el proveedor INTERNEXA, quien brinda conectividad sin incluir el equipo terminal de recepción. En este contexto, la responsabilidad de la adquisición e implementación del equipo CORE recae en la empresa SERVICIOS A PUNTO S.A.C., el cual debe contar con la capacidad suficiente para gestionar el ancho de banda contratado y garantizar el adecuado enrutamiento del tráfico.

A nivel de capa de red, el proveedor asigna un ancho de banda de 11 Gbps, así como dos bloques de direcciones IPv4 públicas: 190.108.93.64/27 y 191.97.61.224/27, que en conjunto representan un total de 64 direcciones IP disponibles para su distribución dentro de la red del ISP.

Asimismo, la entrega del servicio se realiza a través de una VLAN identificada con el ID 4007, proporcionando los parámetros de configuración necesarios para la interconexión, entre los cuales se incluyen una dirección IP WAN (10.201.0.82), una máscara de subred (255.255.255.252) y una puerta de enlace (10.201.0.81).

Con el objetivo de contextualizar las condiciones operativas bajo las cuales se realizaron las mediciones de rendimiento, se analizó el tráfico de red y el uso de recursos del equipo principal.

- **Tráfico de red**

En relación con el tráfico de red, las gráficas obtenidas desde el sistema de monitoreo del MikroTik evidencian un comportamiento variable en función de la demanda de los usuarios, identificándose picos de consumo en determinados intervalos horarios. A continuación, evidenciamos con tres gráficas el tráfico de red captado en tres fechas diferentes:

Figura 4.2

Tráfico registrado el 8 de marzo de 2024.

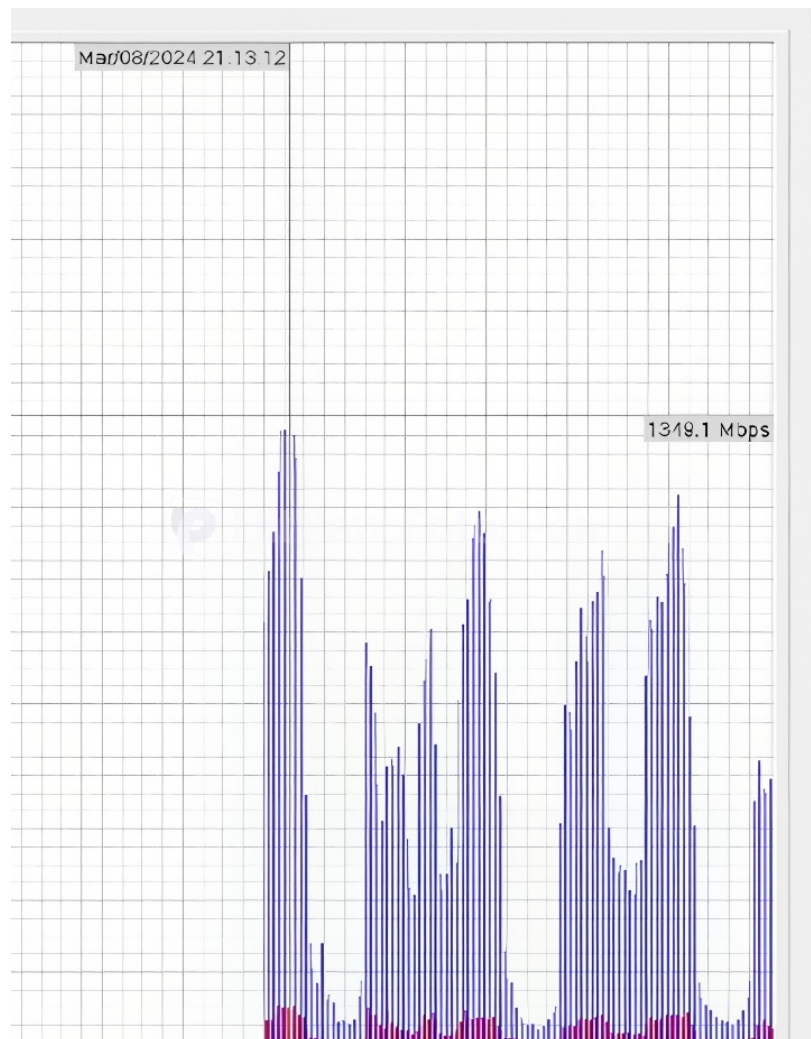


Figura 4.3

Tráfico registrado el 25 de mayo de 2024.

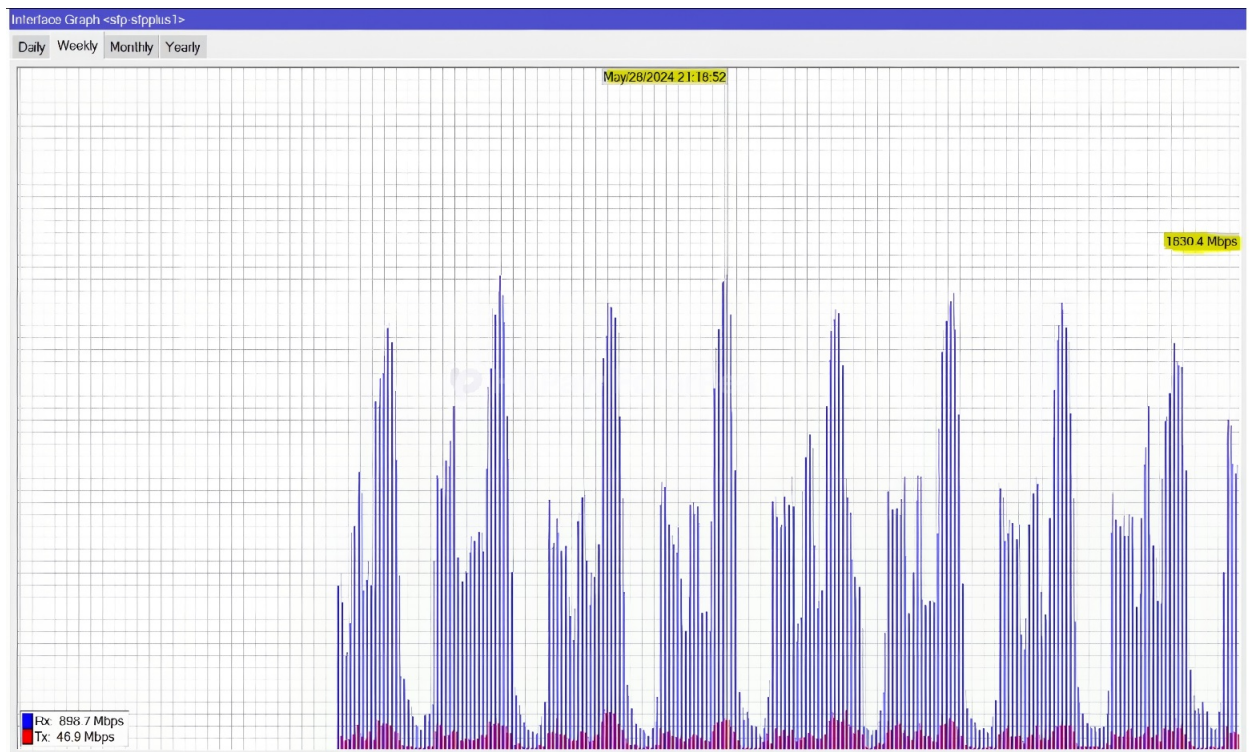
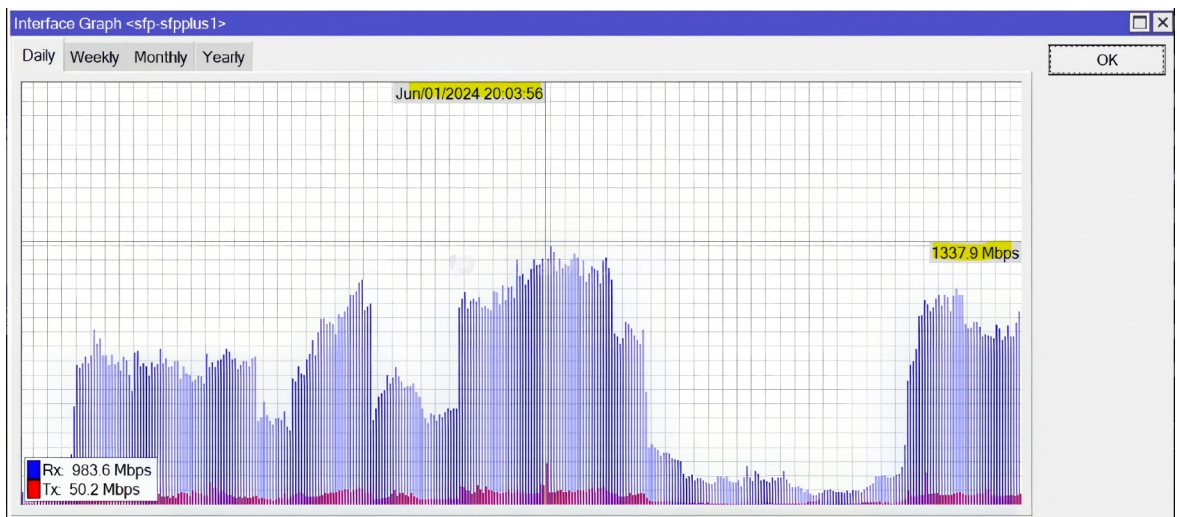


Figura 4.4

Tráfico registrado el 1 de junio de 2024.



-El 8 de marzo de 2024 a las 9:13 p.m., se registró un tráfico de 1349.1 Mbps -El 25 de mayo de 2024 a las 9:18 p.m. se alcanzó un pico máximo de 1630.4 Mbps. -El 1 de junio de 2024 a las 8:03 p.m. se alcanzó un pico de 1337.9 Mbps.

Este comportamiento confirma que la red opera bajo condiciones reales de carga, lo cual es relevante para la validez de las mediciones realizadas.

- Rendimiento de CPU y memoria

Por otro lado, el monitoreo de los recursos del sistema indica que el uso de CPU y memoria se mantiene dentro de rangos estables durante los periodos analizados, sin evidenciar saturación ni cuellos de botella en el procesamiento. Esto permite inferir que la infraestructura cuenta con capacidad suficiente para soportar la carga actual, descartando que posibles variaciones en el rendimiento de la red estén asociadas a limitaciones de hardware.

Figura 4.5

Gráfica mensual del consumo de CPU en el MikroTik.

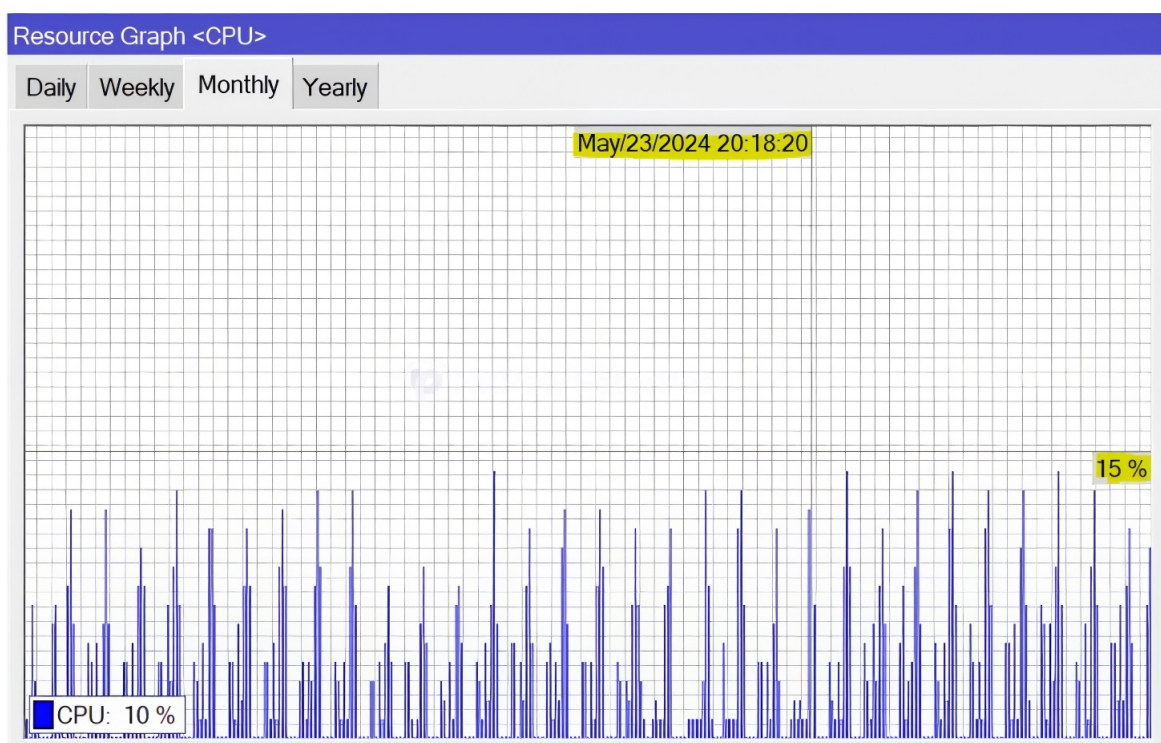
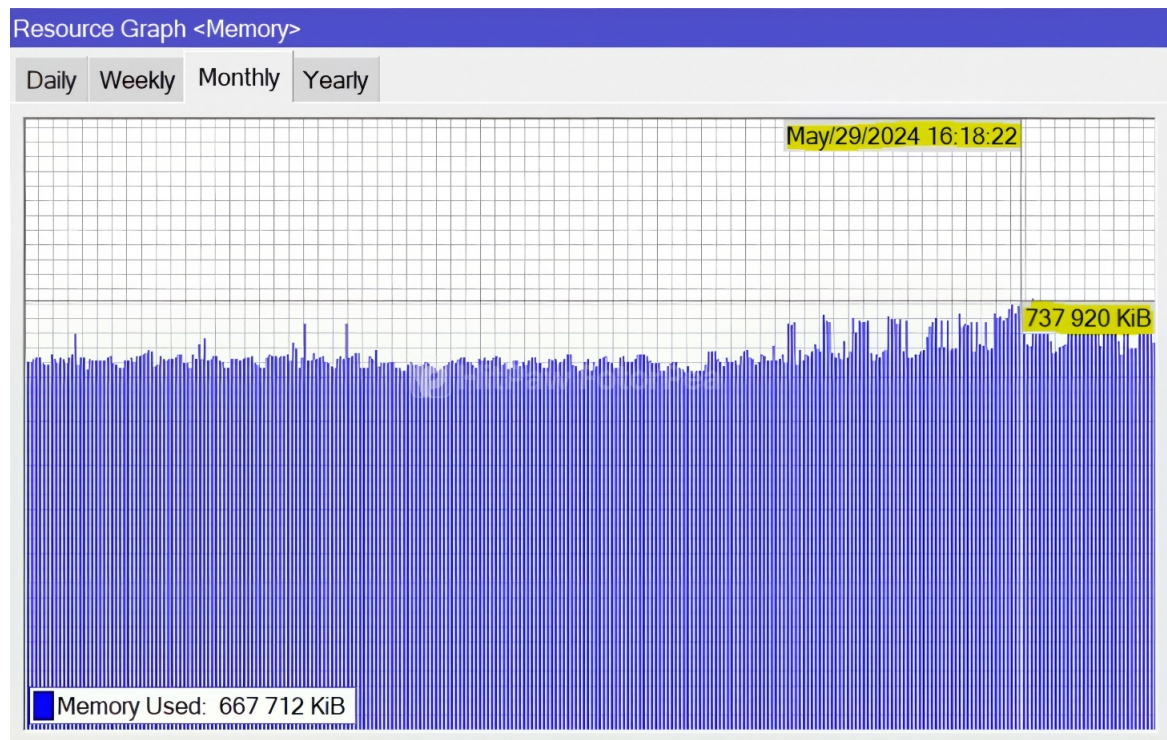


Figura 4.6

Gráfica mensual del consumo de memoria en el MikroTik.



Estas condiciones técnicas definen el entorno operativo sobre el cual se desarrolla la evaluación del rendimiento de la red bajo el protocolo IPv4, constituyendo la base para el análisis comparativo posterior frente a la implementación del método Dual Stack.

4.1.2. Evaluación del rendimiento de la red en IPv4

Con el propósito de establecer una línea base del comportamiento de la red, se llevaron a cabo pruebas de conectividad utilizando el protocolo ICMP en el escenario exclusivo de operación bajo IPv4.

Las mediciones se realizaron en distintos intervalos de tiempo, con el fin de obtener una muestra representativa del comportamiento de la red en condiciones normales de operación.

Para cada prueba, se registraron las métricas de latencia, pérdida de paquetes y disponibi-

lidad, utilizando herramientas de diagnóstico de red que permiten obtener valores objetivos y cuantificables. En cada prueba de conectividad se enviaron 50 paquetes ICMP, considerando que esta cantidad permite obtener una muestra representativa del comportamiento de la red en un intervalo corto de tiempo, sin generar una carga adicional significativa sobre la infraestructura. Asimismo, la repetición de múltiples pruebas permitió compensar posibles variaciones puntuales en los resultados.

Tabla 4.1*Evaluación de rendimiento de la red en IPv4*

Prueba	Paquetes Enviados	Paquetes Recibidos	Paquetes Perdidos	Pérdida (%)	Disponibilidad (%)	Latencia Prom. (ms)
1	50	50	0	0 %	100 %	52.1
2	50	50	0	0 %	100 %	51.8
3	50	50	0	0 %	100 %	52.5
4	50	50	0	0 %	100 %	53.0
5	50	50	0	0 %	100 %	51.6
6	50	50	0	0 %	100 %	52.3
7	50	49	1	2 %	98 %	53.5
8	50	50	0	0 %	100 %	53.2
9	50	50	0	0 %	100 %	51.9
10	50	50	0	0 %	100 %	52.7
11	50	50	0	0 %	100 %	52.4
12	50	50	0	0 %	100 %	53.1
13	50	50	0	0 %	100 %	52.0
14	50	50	0	0 %	100 %	51.7
15	50	48	2	4 %	96 %	54.1
16	50	50	0	0 %	100 %	53.3
17	50	50	0	0 %	100 %	52.2
18	50	50	0	0 %	100 %	51.5
19	50	50	0	0 %	100 %	52.8
20	50	50	0	0 %	100 %	53.0
21	50	50	0	0 %	100 %	52.1
22	50	50	0	0 %	100 %	51.9
23	50	49	1	2 %	98 %	53.8
24	50	50	0	0 %	100 %	53.2
25	50	50	0	0 %	100 %	52.3
26	50	50	0	0 %	100 %	51.6
27	50	50	0	0 %	100 %	52.9
28	50	50	0	0 %	100 %	53.1
29	50	50	0	0 %	100 %	52.4
30	50	50	0	0 %	100 %	51.8
31	50	49	1	2 %	98 %	53.6
32	50	50	0	0 %	100 %	53.0
33	50	50	0	0 %	100 %	52.2
34	50	50	0	0 %	100 %	51.7
35	50	50	0	0 %	100 %	52.8
36	50	50	0	0 %	100 %	53.3
37	50	50	0	0 %	100 %	52.5
38	50	50	0	0 %	100 %	51.9
39	50	50	0	0 %	100 %	52.7
40	50	50	0	0 %	100 %	53.1
41	50	50	0	0 %	100 %	52.3
42	50	48	2	4 %	96 %	54.3
43	50	50	0	0 %	100 %	52.9
44	50	50	0	0 %	100 %	53.2
45	50	50	0	0 %	100 %	52.1
46	50	50	0	0 %	100 %	51.8
47	50	50	0	0 %	100 %	52.6
48	50	50	0	0 %	100 %	53.0
49	50	50	0	0 %	100 %	52.4
50	50	50	0	0 %	100 %	52.2

• Medición de Latencia

Para evaluar la latencia de la red, se realizaron pruebas de conectividad emnsionadas en la tabla 1, mediante el envío de paquetes ICMP (ping) desde un punto de monitoreo

hacia destinos definidos dentro de la red. Las mediciones se ejecutaron bajo condiciones operativas normales.

Se registraron los tiempos de ida y vuelta (RTT), obteniendo valores mínimos, máximos y promedio, los cuales se presentan a continuación:

Tabla 4.2

Resultados de medición de latencia en IPv4 (mínimo, máximo, promedio)

Métrica	Valor
Latencia mínima	51.5 ms
Latencia máxima	54.3 ms
Latencia promedio	52.6 ms

Los resultados evidencian que la latencia promedio de 52.6 ms se mantiene dentro de rangos operativos estables, con variaciones moderadas entre los valores mínimo (51.5ms) y máximo (54.3 ms), lo que indica un comportamiento consistente de la red en condiciones normales de funcionamiento.

Evaluación de pérdida de paquetes

La pérdida de paquetes fue determinada mediante la relación entre el número de paquetes enviados y recibidos durante las pruebas de conectividad. Para ello, se ejecutaron secuencias de envío de paquetes ICMP, registrando los resultados obtenidos.

Tabla 4.3

Cálculo de pérdida de paquetes en IPv4

Total de paquetes enviados	Total de paquetes recibidos	Pérdida (%)
2500	2493	0.28 %

El cálculo de la pérdida de paquetes se realizó mediante la siguiente expresión: $\text{Pérdida (\%)} = (\text{Paquetes enviados} - \text{Paquetes recibidos}) / \text{Paquetes enviados} \times 100$. Los resultados muestran que la pérdida de paquetes en la red es mínima durante las pruebas realizadas, lo que evidencia una transmisión eficiente de datos bajo el protocolo IPv4 en el escenario evaluado.

Evaluación de disponibilidad

La disponibilidad de la red se evaluó en función de la proporción de respuestas exitosas obtenidas durante las pruebas de conectividad realizadas. Este indicador permite estimar la continuidad del servicio en el periodo de medición.

Tabla 4.4

Evaluación de disponibilidad en IPv4

Paquetes enviados	Paquetes recibidos	Disponibilidad (%)
2500	2493	99.72 %

En términos generales, la disponibilidad estuvo en un 99.72 %, lo que indica un nivel adecuado de continuidad del servicio. No obstante, estas variaciones reflejan que el entorno operativo no está exento de fluctuaciones, lo que refuerza la necesidad de evaluar soluciones que permitan asegurar la escalabilidad de la red.

4.1.3. Análisis del rendimiento en IPV4

El análisis de los resultados obtenidos permite concluir que la red del ISP SERVICIOS A PUNTO S.A.C., operando bajo el protocolo IPv4, presenta un comportamiento estable en términos de latencia, pérdida de paquetes y disponibilidad. La baja variabilidad en los tiempos de respuesta, junto con la casi ausencia de pérdida de paquetes, evidencia una transmisión de datos eficiente bajo condiciones normales de operación.

Asimismo, la disponibilidad total del servicio durante el periodo de evaluación indica que la infraestructura actual garantiza la continuidad en la prestación del servicio a los usuarios.

Sin embargo, es importante señalar que, a pesar del adecuado desempeño observado en los indicadores evaluados, el uso exclusivo del protocolo IPv4 representa una limitación estructural en términos de escalabilidad. La disponibilidad finita de direcciones IP restringe la capacidad de crecimiento de la red ante el incremento sostenido de la demanda, lo que puede comprometer la incorporación de nuevos usuarios y dispositivos en el mediano y largo plazo.

En este contexto, se justifica la necesidad de evaluar alternativas tecnológicas que

permitan la transición hacia IPv6, siendo el método Dual Stack una opción viable para la coexistencia de ambos protocolos, sin afectar la continuidad del servicio ni el rendimiento de la red.

4.2. Realizar la implementación de IPv6 en la red ISP SERVICIOS A PUNTO S.A.C con el método Dual Stack

Para poder ejecutar la implementación del protocolo IPv6 en la infraestructura de la red ISP SERVICIOS A PUNTO S.A.C. mediante el método Dual Stack”, este método permite la coexistencia simultánea de los protocolos IPv4 e IPv6 sobre los mismos equipos y enlaces, garantizando la continuidad del servicio durante el proceso de migración. El procedimiento se desarrolló en etapas sucesivas que abarcaron la actualización del firmware de los equipos MikroTik, la habilitación del paquete IPv6, la asignación de direccionamiento, la configuración del enrutamiento y la validación de conectividad extremo a extremo.

4.2.1. Actualización del firmware a RouterOS7

Como paso previo a la habilitación de IPv6 fue necesario actualizar el sistema operativo de los routers MikroTik a RouterOS versión 7 debido a que esta versión incorpora soporte nativo y estable para el protocolo IPv6, incluyendo mejoras en el manejo de prefijos, DHCPv6 y enrutamiento estático. El equipo objeto de la actualización es el CCR2116-12G-4S+, que cumple la función de router de gestión dentro de la red del ISP.

La actualización fue verificada accediendo a System y después a Resources en WinBox, acá se confirmó que el equipo quedó operando con la versión 7.20.7, con fecha de compilación 2026-01-08. La arquitectura del procesador es ARM64 con 16 núcleos de CPU, 16 GiB de memoria RAM total y una carga de CPU del 8 % en el momento de la captura, lo que demuestra que el equipo cuenta con suficiente capacidad para soportar la operación dual.

Figura 4.7

Verificación de recursos del sistema tras la actualización a RouterOS 7.

The screenshot displays the 'Resources' page in the RouterOS web interface. The page is divided into two main sections: a large left panel for system resources and a smaller right panel for configuration options. The left panel lists various system metrics with their current values in input fields. The right panel has a 'Configuration' header and a list of categories: Hardware, CPU, and IRQ. A 'Cancel' button is located at the bottom right of the interface.

Resource	Value
Uptime	21:09:45
Free Memory	15.3 GiB
Total Memory	16.0 GiB
CPU	ARM64
CPU Count	16
CPU Frequency	2000 MHz
CPU Load	8 %
Free HDD Space	87.9 MiB
Total HDD Size	128.0 MiB
Sector Writes Since Reboot	13 500
Total Sector Writes	1 488 465
Bad Blocks	0.0 %
Architecture Name	arm64
Board Name	CCR2116-12G-4S+
Version	7.20.7 (long-term)
Build Time	2026-01-08 09:40:00
Factory Software	7.8

Configuration

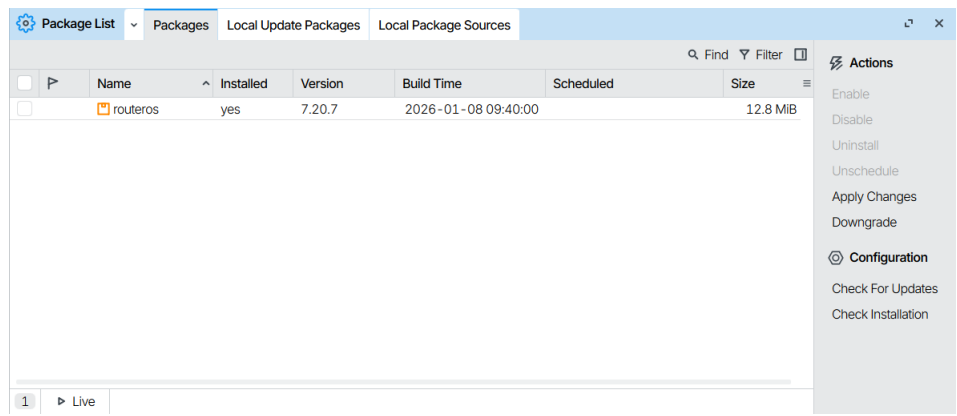
- Hardware
- CPU
- IRQ

Cancel

De forma complementaria, se accedió a Packages para poder confirmar el paquete instalado activo, la vista muestra que el paquete routerOS versión 7.20.7 se encuentra instalado y habilitado en el equipo, además la fecha de compilación es coincidente con la verificación anterior.

Figura 4.8

Lista de paquetes instalados en el MikroTik CCR2116-12G-4S+ tras la actualización.



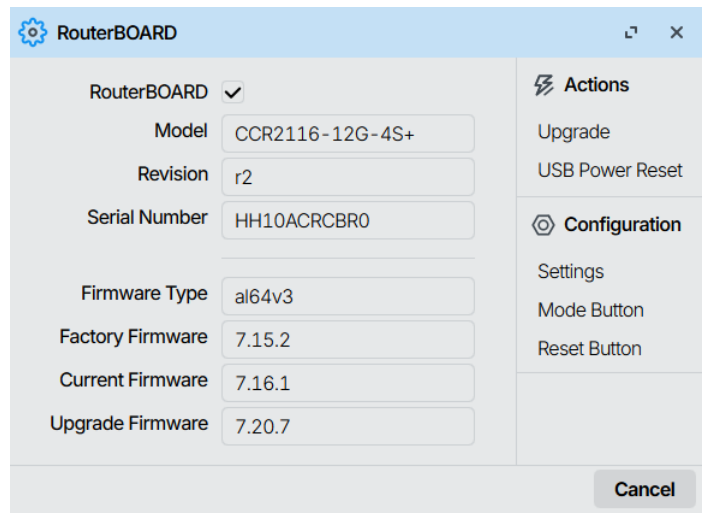
The screenshot shows the 'Package List' window in WinBox. It has tabs for 'Package List', 'Packages', 'Local Update Packages', and 'Local Package Sources'. The 'Package List' tab is active, displaying a table of installed packages. The table has columns for Name, Installed, Version, Build Time, Scheduled, and Size. One package, 'routers', is listed as installed with version 7.20.7, built on 2026-01-08 09:40:00, and a size of 12.8 MiB. To the right of the table is an 'Actions' menu with options: Enable, Disable, Uninstall, Unschedule, Apply Changes, Downgrade, Configuration (indicated by a gear icon), Check For Updates, and Check Installation. At the bottom left, there is a status bar showing '1' and 'Live'.

	Name	Installed	Version	Build Time	Scheduled	Size
☐	 routers	yes	7.20.7	2026-01-08 09:40:00		12.8 MiB

Finalmente, la información del RouterBOARD confirma que el modelo del equipo es CCR2116-12G-4S+, con número de serie HH10ACRCBR0, el firmware actual es la versión 7.16.1 con el firmware de actualización 7.20.7 disponible, todo esto complementa la evidencia de que el equipo ha sido correctamente actualizado a la plataforma RouterOS 7, esta condición es indispensable para la implementación de IPv6 en un entorno de producción.

Figura 4.9

Información del RouterBOARD del equipo CCR2116-12G-4S+ con firmware actualizado.



The screenshot shows the 'RouterBOARD' configuration window in WinBox. It contains fields for RouterBOARD status (checked), Model (CCR2116-12G-4S+), Revision (r2), Serial Number (HH10ACRCBR0), Firmware Type (al64v3), Factory Firmware (7.15.2), Current Firmware (7.16.1), and Upgrade Firmware (7.20.7). To the right is an 'Actions' menu with 'Upgrade' and 'USB Power Reset' options, and a 'Configuration' section with 'Settings', 'Mode Button', and 'Reset Button' options. A 'Cancel' button is at the bottom right.

RouterBOARD	☒
Model	CCR2116-12G-4S+
Revision	r2
Serial Number	HH10ACRCBR0
Firmware Type	al64v3
Factory Firmware	7.15.2
Current Firmware	7.16.1
Upgrade Firmware	7.20.7

4.2.2. Actualización del firmware a RouterOS7

Una vez confirmada la actualización del sistema operativo se procedió a configurar el direccionamiento IPv6 en las interfaces de red de los equipos, el proveedor INTERNEXA asignó al ISP SERVICIOS A PUNTO S.A.C. el bloque de direcciones IPv6 2803:65d0::/32, el cual fue subdividido internamente en prefijos /64 para su asignación a las VLANs de acceso y en prefijos /45 para los pools de delegación de prefijos a clientes mediante DHCPv6 Prefix Delegation (PD). Teniendo esto en cuenta en el router de borde principal (BNG-CARAVELI), se configuraron las siguientes interfaces con direccionamiento IPv6 global.

Tabla 4.5

Direcciones IPv6 configuradas en el router de borde BNG-CARAVELI

Interfaz	Dirección IPv6	Tipo
vlan.4007-WAN	2800:650:10:6::6e/126	Global (WAN - INTERNEXA)
VLAN256-IPv6	2803:65d0:80::1/64	Global (LAN de gestión)
lo	::1	Loopback

Posteriormente en la siguiente figura se muestra la lista de direcciones IPv6 asignadas en el router BNG-CARAVELI, evidenciando la dirección global asignada por INTERNEXA en la interfaz WAN (vlan.4007-WAN) y la dirección de la red de gestión interna (VLAN256-IPv6). Las restantes entradas con prefijo fe80: corresponden a direcciones link-local generadas automáticamente por el protocolo.

Figura 4.10

Lista de direcciones IPv6 en el router de gestión CCR2116-12G-4S+

		Address	From Pool	Interface	Advertise
☐	LD	fe80::f61e:57ff:fe3c:b147/64		vlan1099	no
☐	LD	fe80::f61e:57ff:fe3c:b147/64		vlan99	no
☐	G	2803:65d0:80:7::2/64		VLAN41-IPV6	no
☐	LD	fe80::f61e:57ff:fe3c:b146/64		VLAN41-IPV6	no
☐	LD	fe80::f61e:57ff:fe3c:b146/64		VLAN40-IPV4	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-499	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-415	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-414	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-413	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-412	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-411	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-410	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-409	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-408	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-407	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-406	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-405	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-404	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-403	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-402	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-401	no
☐	LD	fe80::f61e:57ff:fe3c:b148/64		vlan-400	no
☐	LD	fe80::f61e:57ff:fe3c:b147/64		vlan-315	no
☐	LD	fe80::f61e:57ff:fe3c:b147/64		vlan-314	no
☐	LD	fe80::f61e:57ff:fe3c:b147/64		vlan-313	no
☐	LD	fe80::f61e:57ff:fe3c:b147/64		vlan-312	no

472 | ▶ Live

4.2.3. Configuración del direccionamiento IPv6

Tras asignar el direccionamiento se procedió a configurar el enrutamiento IPv6 estático en ambos routers con la finalidad de poder de garantizar la propagación correcta del tráfico entre los segmentos de red y hacia el Internet, además se estableció una ruta predeterminada (: :0) hacia el gateway de INTERNEXA (2803:65d0:80:7::1 en el CCR2116, y 2800:650:10:6::6d en el BNG-CARAVELI) y rutas específicas para cada zona de cobertura del ISP.

En el router BNG-CARAVELI se muestra la lista de enrutamiento IPv6 en el cual se puede observar la ruta predeterminada hacia el gateway upstream de INTERNEXA, las

rutas directamente conectadas a la interfaz WAN y a la VLAN256-IPv6 y rutas estáticas agrupadas por zona geográfica (DMZ, PTP Ocona, PTP Secocha, PTP San Juan, PTP Ispacs, PTP Caravalí, PTP Ático, Ocona Residencial, Secocha Residencial, San Juan Residencial, Ispacas Residencial, Caravalí Residencial), cada una apuntando como gateway a la dirección 2803:65d0:80::2 del router de gestión CCR2116.

Figura 4.11

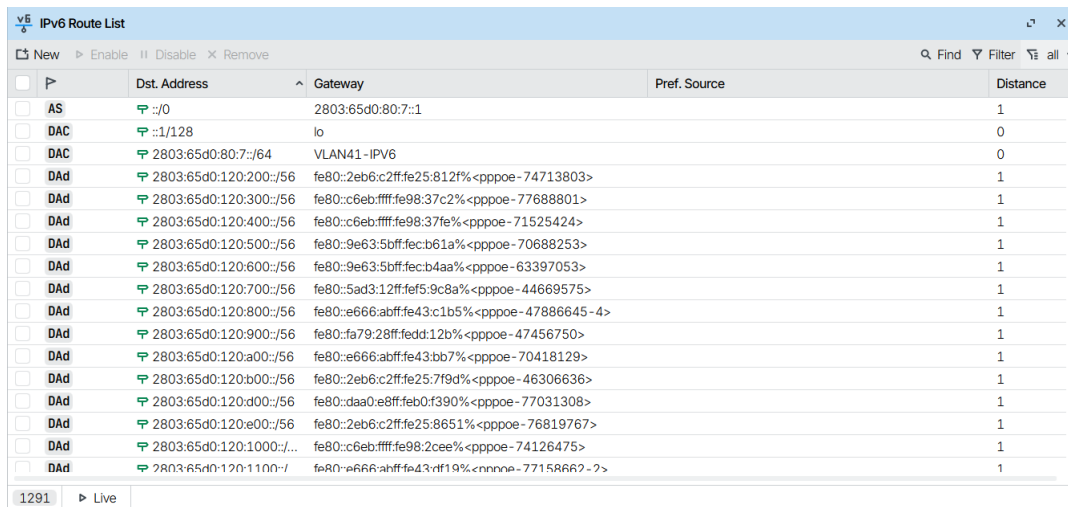
Enrutamiento IPv6 en el router BNG-CARAVELI

IPv6 Route List					
New Enable Disable Remove					
		Dst. Address	Gateway	Pref. Source	Distance
☐	DABH	::/0	2800:650:10:6::6d		20
☐	DAC	::1/128	lo		0
☐	DACH	2800:650:10:6::6c/126	vlan.4007-WAN		0
☐	AS	2803:65d0::/32			1
☐	D	2803:65d0::/32			255
☐	DACH	2803:65d0:80::/64	VLAN256-IPv6		0
DMZ					
☐	ASH	2803:65d0:80:1::/64	2803:65d0:80::2		1
PTP OCONA - RESIDENCIAL					
☐	ASH	2803:65d0:80:3::/64	2803:65d0:80::2		1
PTP SECOCHA - RESIDENCIAL					
☐	ASH	2803:65d0:80:4::/64	2803:65d0:80::2		1
PTP SAN JUAN - RESIDENCIAL					
☐	ASH	2803:65d0:80:5::/64	2803:65d0:80::2		1
PTP - ISPACAS RESIDENCIAL					
☐	ASH	2803:65d0:80:6::/64	2803:65d0:80::2		1
PTP - CARAVELI RESIDENCIAL					
☐	ASH	2803:65d0:80:7::/64	2803:65d0:80::2		1
PTP - ATICO RESIDENCIAL					
☒	ASH	2803:65d0:80:8::/64	2803:65d0:80::2		1
DMZ - OOKLA					
☐	ASH	2803:65d0:81::/64	2803:65d0:80::2		1
OCONA - RESIDENCIAL					
☐	ASH	2803:65d0:100::/45	2803:65d0:80::2		1
SECOCHA - RESIDENCIAL					
☐	ASH	2803:65d0:108::/45	2803:65d0:80::2		1
SAN JUAN - RESIDENCIAL					
☐	ASH	2803:65d0:110::/45	2803:65d0:80::2		1
ISPACAS - RESIDENCIAL					
☐	ASH	2803:65d0:118::/45	2803:65d0:80::2		1

En el router de gestión CCR2116-12G-4S+ la lista de enrutamiento IPv6 refleja la ruta predeterminada hacia 2803:65d0:80:7::1 (gateway del BNG-CARAVELI), las redes directamente conectadas en el espacio de dirección 2803:65d0: :/32, y las rutas dinámicas aprendidas por DHCPv6-PD correspondientes a los prefijos /56 delegados a cada abonado a través de las interfaces PPPoE. La presencia de 1291 entradas en la tabla de enrutamiento confirma que la delegación de prefijos a usuarios finales opera correctamente.

Figura 4.12

Enrutamiento IPv6 en el router de gestión CCR2116-12G-4S+



	Dst. Address	Gateway	Pref. Source	Distance
AS	::0	2803:65d0:80:7::1		1
DAC	::1/128	lo		0
DAC	2803:65d0:80:7::/64	VLAN41-IPv6		0
DAd	2803:65d0:120:200::/56	fe80::2eb6:c2ff:fe25:812f%<pppoe-74713803>		1
DAd	2803:65d0:120:300::/56	fe80::c6eb:ffff:fe98:37c2%<pppoe-77688801>		1
DAd	2803:65d0:120:400::/56	fe80::c6eb:ffff:fe98:37fe%<pppoe-71525424>		1
DAd	2803:65d0:120:500::/56	fe80::9e63:5bff:fecb:61a%<pppoe-70688253>		1
DAd	2803:65d0:120:600::/56	fe80::9e63:5bff:fecb:4aa%<pppoe-63397053>		1
DAd	2803:65d0:120:700::/56	fe80::5ad3:12ff:fe5:9c8a%<pppoe-44669575>		1
DAd	2803:65d0:120:800::/56	fe80::e666:abff:fe43:c1b5%<pppoe-47886645-4>		1
DAd	2803:65d0:120:900::/56	fe80::fa79:28ff:fedd:12b%<pppoe-47456750>		1
DAd	2803:65d0:120:a00::/56	fe80::e666:abff:fe43:bb7%<pppoe-70418129>		1
DAd	2803:65d0:120:b00::/56	fe80::2eb6:c2ff:fe25:7f9d%<pppoe-46306636>		1
DAd	2803:65d0:120:d00::/56	fe80::daa0:e8ff:feb0:f390%<pppoe-77031308>		1
DAd	2803:65d0:120:e00::/56	fe80::2eb6:c2ff:fe25:8651%<pppoe-76819767>		1
DAd	2803:65d0:120:1000::/...	fe80::c6eb:ffff:fe98:2cee%<pppoe-74126475>		1
DAd	2803:65d0:120:1100::/...	fe80::e666:abff:fe43:df19%<pppoe-77158662-2>		1

4.2.4. Configuración de DHCPv6 y delegación de prefijos a usuarios

Para la asignación automática de prefijos IPv6 a los usuarios residenciales se configuró un servidor DHCPv6 con Prefix Delegation (PD) en el router de gestión CCR2116, este mecanismo permite que cada equipo CPE del abonado reciba un prefijo /56 del bloque 2803:65d0:120: :/45 el cual puede ser subdividido por el propio router del cliente para distribuir IPv6 nativamente en su red doméstica. La figura siguiente muestra la lista de enlaces activos del servidor DHCPv6 (Bindings) en donde se aprecia que 409 abonados han recibido prefijos /56 delegados a través de sus interfaces PPPoE. Cada entrada registra la dirección del prefijo asignado, el identificador del cliente (DUID), el servidor activo, el tiempo de expiración y la dirección link-local del peer, confirmando que la delegación de prefijos opera de manera dinámica y estable.

Figura 4.13

Lista de bindings activos del servidor DHCPv6-PD en el CCR2116-12G-4S+

DHCPv6 Server											
DHCP Bindings Options Option Sets											
New Enable Disable Remove Find Filter											
		Address	DUID	IAID	Server	Active Server	Prefix or Addr...	Expire Time	Peer Address	Relay Chain	
	D	2803:65d0:120:200::/56	0x000300012c...	1000	<pppoe-747...	<pppoe-747...	pool-PD	14:46:35	fe80::2eb6:c2ff:fe25:812f		
	D	2803:65d0:120:300::/56	0x00030001c4e...	1000	<pppoe-776...	<pppoe-776...	pool-PD	14:46:35	fe80::c6eb:ffff:fe98:37c2		
	D	2803:65d0:120:400::/56	0x00030001c4e...	1000	<pppoe-715...	<pppoe-715...	pool-PD	18:22:05	fe80::c6eb:ffff:fe98:37fe		
	D	2803:65d0:120:500::/56	0x000300019c...	1000	<pppoe-706...	<pppoe-706...	pool-PD	19:00:04	fe80::9e63:5bff:fec:b61a		
	D	2803:65d0:120:600::/56	0x000300019c...	1000	<pppoe-633...	<pppoe-633...	pool-PD	18:27:32	fe80::9e63:5bff:fec:b4aa		
	D	2803:65d0:120:700::/56	0x0003000158...	1000	<pppoe-446...	<pppoe-446...	pool-PD	14:46:35	fe80::5ad3:12ff:fe5:9c8a		
	D	2803:65d0:120:800::/56	0x00030001e4...	1000	<pppoe-478...	<pppoe-478...	pool-PD	14:46:36	fe80::e666:abff:fe43:c1b5		
	D	2803:65d0:120:900::/56	0x00030001f87...	1000	<pppoe-474...	<pppoe-474...	pool-PD	14:09:45	fe80::fa79:28ff:fedd:12b		
	D	2803:65d0:120:a00::/56	0x00030001e4...	1000	<pppoe-704...	<pppoe-704...	pool-PD	14:09:38	fe80::e666:abff:fe43:bb7		
	D	2803:65d0:120:b00::/56	0x000300012c...	1000	<pppoe-463...	<pppoe-463...	pool-PD	14:46:36	fe80::2eb6:c2ff:fe25:7f9d		
	D	2803:65d0:120:d00::/56	0x00030001d8...	1000	<pppoe-770...	<pppoe-770...	pool-PD	23:49:24	fe80::daa0:e8ff:feb0:f390		
	D	2803:65d0:120:e00::/56	0x000300012c...	1000	<pppoe-768...	<pppoe-768...	pool-PD	14:46:37	fe80::2eb6:c2ff:fe25:8651		
	D	2803:65d0:120:1000::/56	0x00030001c4e...	1000	<pppoe-741...	<pppoe-741...	pool-PD	15:26:26	fe80::c6eb:ffff:fe98:2cee		
	D	2803:65d0:120:1100::/56	0x00030001e4...	1000	<pppoe-771...	<pppoe-771...	pool-PD	14:09:35	fe80::e666:abff:fe43:df19		
	D	2803:65d0:120:1200::/56	0x00030001c4e...	1000	<pppoe-770...	<pppoe-770...	pool-PD	23:54:26	fe80::c6eb:ffff:fe98:2cfa		
	D	2803:65d0:120:1300::/56	0x0003000148...	1000	<pppoe-718...	<pppoe-718...	pool-PD	14:46:38	fe80::4a96:d9ff:fe3a:6875		
	D	2803:65d0:120:1400::/56	0x000300012c...	1000	<pppoe-748...	<pppoe-748...	pool-PD	14:46:38	fe80::2eb6:c2ff:fe7f:5e7		
	D	2803:65d0:120:1500::/56	0x000300012c...	1000	<pppoe-756...	<pppoe-756...	pool-PD	14:46:38	fe80::2eb6:c2ff:fe25:7cd3		
	D	2803:65d0:120:1600::/56	0x0003000158...	1000	<pppoe-451...	<pppoe-451...	pool-PD	14:05:15	fe80::5ad3:12ff:fe5:9bb2		
	D	2803:65d0:120:1700::/56	0x00030001d8...	1000	<pppoe-437...	<pppoe-437...	pool-PD	14:46:38	fe80::daa0:e8ff:feb1:46a		
	D	2803:65d0:120:1800::/56	0x000300019c...	1000	<pppoe-464...	<pppoe-464...	pool-PD	13:59:08	fe80::9e63:5bff:fec:b43		
	D	2803:65d0:120:1900::/56	0x0003000148...	1000	<pppoe-744...	<pppoe-744...	pool-PD	14:46:39	fe80::4a96:d9ff:fe3a:707f		
	D	2803:65d0:120:1a00::/56	0x00030001e4...	1000	<pppoe-402...	<pppoe-402...	pool-PD	21:05:33	fe80::e666:abff:fe43:baa2		
	D	2803:65d0:120:1b00::/56	0x00030001e4...	1000	<pppoe-453...	<pppoe-453...	pool-PD	18:21:38	fe80::e666:abff:fe43:97d		
	D	2803:65d0:120:1c00::/56	0x000300019c...	1000	<pppoe-463...	<pppoe-463...	pool-PD	21:22:32	fe80::9e63:5bff:fec:b4cf		
	D	2803:65d0:120:1d00::/56	0x0003000158...	1000	<pppoe-205...	<pppoe-205...	pool-PD	14:46:40	fe80::5ad3:12ff:fe5:9bbe		
	D	2803:65d0:120:1e00::/56	0x0003000148...	1000	<pppoe-472...	<pppoe-472...	pool-PD	14:46:40	fe80::4a96:d9ff:fe3a:70c1		
	D	2803:65d0:120:1f00::/56	0x00030001a4...	1000	<pppoe-403...	<pppoe-403...	pool-PD	14:09:52	fe80::e666:abff:fe43:c7d5		
409		Live									

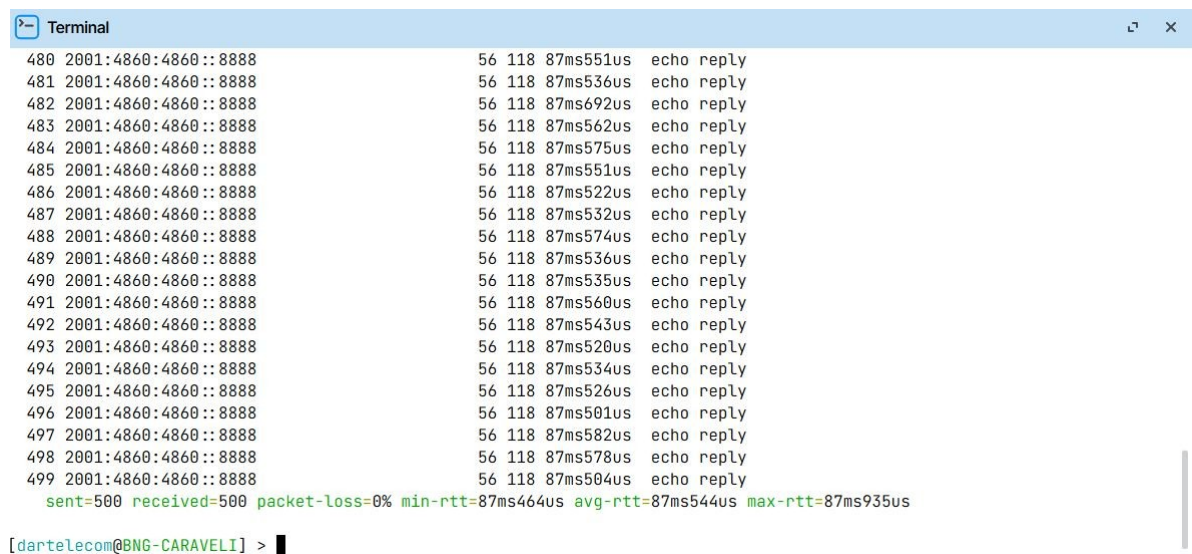
4.2.5. Validación de conectividad IPv6

Una vez finalizada la configuración de direccionamiento, enrutamiento y delegación de prefijos se procedió a verificar la conectividad IPv6 extremo a extremo mediante pruebas ICMP hacia el servidor DNS público de Google (2001:4860:4860::8888), desde el equipo BNG-CARAVELI ubicado en la provincia de Caravalí, esta dirección fue seleccionada por su alta disponibilidad y estabilidad, lo que la convierte en una referencia apropiada para validar el alcance global de IPv6. La prueba consistió en el envío de paquetes ICMP consecutivos, verificando que los paquetes fueran recibidos correctamente, que la pérdida de paquetes fuera nula y que los tiempos de respuesta fueran consistentes. Los resultados obtenidos confirman que la red opera correctamente sobre IPv6 y que el camino desde el ISP hacia Internet IPv6 es funcional y estable.

La figura siguiente muestra una muestra representativa de la prueba de conectividad en el rango de paquetes 480 al 499, con resultados de la prueba completa de 500 paquetes enviados, acá se aprecia que todos los paquetes fueron recibidos (packet-loss=0%), con un RTT mínimo de 87ms464us, promedio de 87ms544us y máximo de 87ms935us, lo que evidencia estabilidad y baja variabilidad en la latencia.

Figura 4.14

Prueba de conectividad IPv6 hacia 2001:4860:4860::8888 desde BNG-CARAVELI

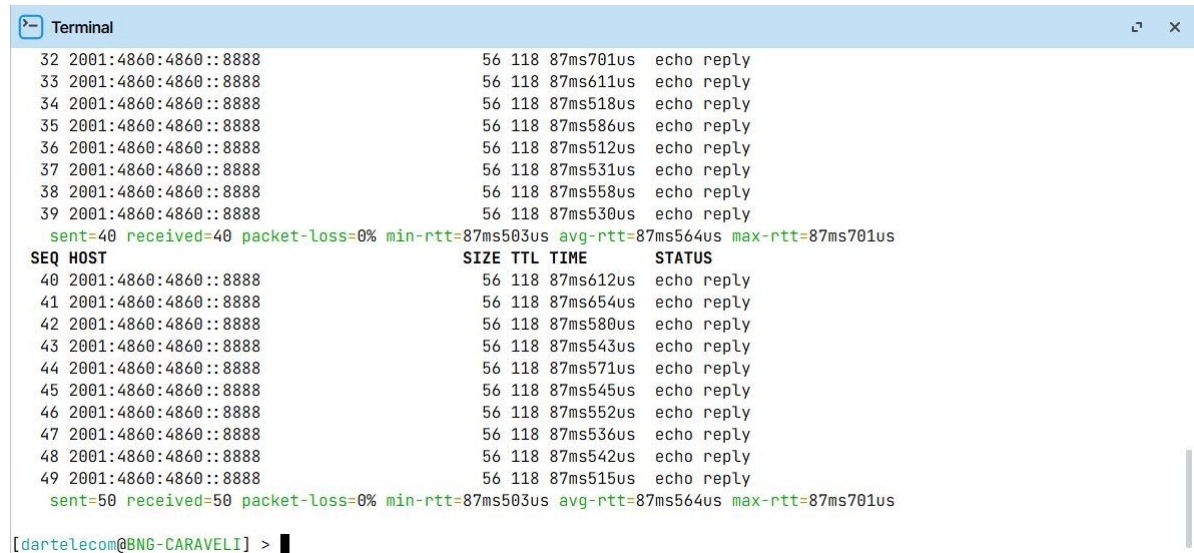


```
Terminal
480 2001:4860:4860::8888      56 118 87ms551us  echo reply
481 2001:4860:4860::8888      56 118 87ms536us  echo reply
482 2001:4860:4860::8888      56 118 87ms692us  echo reply
483 2001:4860:4860::8888      56 118 87ms562us  echo reply
484 2001:4860:4860::8888      56 118 87ms575us  echo reply
485 2001:4860:4860::8888      56 118 87ms551us  echo reply
486 2001:4860:4860::8888      56 118 87ms522us  echo reply
487 2001:4860:4860::8888      56 118 87ms532us  echo reply
488 2001:4860:4860::8888      56 118 87ms574us  echo reply
489 2001:4860:4860::8888      56 118 87ms536us  echo reply
490 2001:4860:4860::8888      56 118 87ms535us  echo reply
491 2001:4860:4860::8888      56 118 87ms560us  echo reply
492 2001:4860:4860::8888      56 118 87ms543us  echo reply
493 2001:4860:4860::8888      56 118 87ms520us  echo reply
494 2001:4860:4860::8888      56 118 87ms534us  echo reply
495 2001:4860:4860::8888      56 118 87ms526us  echo reply
496 2001:4860:4860::8888      56 118 87ms501us  echo reply
497 2001:4860:4860::8888      56 118 87ms582us  echo reply
498 2001:4860:4860::8888      56 118 87ms578us  echo reply
499 2001:4860:4860::8888      56 118 87ms504us  echo reply
sent=500 received=500 packet-loss=0% min-rtt=87ms464us avg-rtt=87ms544us max-rtt=87ms935us
[dartelecom@BNG-CARAVELI] >
```

De forma complementaria la siguiente figura muestra la porción de la prueba correspondiente a los paquetes 32 a 50 incluyendo los resultados intermedios al llegar a 40 paquetes y el resultado final al completar los 50 paquetes, en ambos puntos de corte se obtiene packet-loss=0% con RTT promedio de 87ms564us y 87ms564us respectivamente confirmando la consistencia del enlace IPv6 durante el proceso de validación.

Figura 4.15

Prueba de conectividad IPv6 desde BNG-CARAVELI – Muestra de paquetes 32–50 con resultados a los 40 y 50 paquetes



```
Terminal
32 2001:4860:4860::8888      56 118 87ms701us  echo reply
33 2001:4860:4860::8888      56 118 87ms611us  echo reply
34 2001:4860:4860::8888      56 118 87ms518us  echo reply
35 2001:4860:4860::8888      56 118 87ms586us  echo reply
36 2001:4860:4860::8888      56 118 87ms512us  echo reply
37 2001:4860:4860::8888      56 118 87ms531us  echo reply
38 2001:4860:4860::8888      56 118 87ms558us  echo reply
39 2001:4860:4860::8888      56 118 87ms530us  echo reply
sent=40 received=40 packet-loss=0% min-rtt=87ms503us avg-rtt=87ms564us max-rtt=87ms701us
SEQ HOST      SIZE TTL TIME      STATUS
40 2001:4860:4860::8888      56 118 87ms612us  echo reply
41 2001:4860:4860::8888      56 118 87ms654us  echo reply
42 2001:4860:4860::8888      56 118 87ms580us  echo reply
43 2001:4860:4860::8888      56 118 87ms543us  echo reply
44 2001:4860:4860::8888      56 118 87ms571us  echo reply
45 2001:4860:4860::8888      56 118 87ms545us  echo reply
46 2001:4860:4860::8888      56 118 87ms552us  echo reply
47 2001:4860:4860::8888      56 118 87ms536us  echo reply
48 2001:4860:4860::8888      56 118 87ms542us  echo reply
49 2001:4860:4860::8888      56 118 87ms515us  echo reply
sent=50 received=50 packet-loss=0% min-rtt=87ms503us avg-rtt=87ms564us max-rtt=87ms701us
[darte telecom@BNG-CARAVELI] >
```

4.2.6. Análisis de la implementación Dual Stack

Los resultados obtenidos durante el proceso de implementación permiten concluir que la migración de la red del ISP SERVICIOS A PUNTO S.A.C. hacia el método Dual Stack fue ejecutada exitosamente. La actualización del firmware a RouterOS 7, la habilitación del paquete IPv6, la configuración del direccionamiento y el enrutamiento estático y la puesta en marcha del servidor DHCPv6-PD conformaron un proceso ordenado y técnicamente coherente que permitió activar IPv6 en producción sin interrumpir la operación del servicio IPv4 existente.

La delegación de prefijos /56 a 409 abonados activos a través de DHCPv6-PD y la presencia de 1291 rutas IPv6 en la tabla de enrutamiento del router de gestión demuestran que la red Dual Stack alcanza escala operativa real, no limitada a un entorno de laboratorio. La validación de conectividad mediante ping IPv6 con 0% de pérdida de paquetes y latencias promedio inferiores a 88 ms hacia un servidor DNS global confirma que el camino hacia Internet IPv6 es funcional y estable. Con esto queda demostrado que la infraestructura del

ISP SERVICIOS A PUNTO S.A.C. es capaz de operar simultáneamente bajo IPv4 e IPv6.

4.3. Comparar los resultados obtenidos antes y después de la migración en términos de latencia, pérdida de paquetes y disponibilidad de la red

El presente apartado busca contrastar de manera sistemática los indicadores de rendimiento de la red del ISP SERVICIOS A PUNTO S.A.C. antes y después de la implementación del método Dual Stack, para lograr esto se comparan los valores de latencia, pérdida de paquetes y disponibilidad obtenidos en los dos escenarios evaluados: el escenario de línea base operando exclusivamente con IPv4 y el escenario posterior con coexistencia IPv4/IPv6 mediante Dual Stack, la metodología de medición empleada en ambas fases fue equivalente, utilizando secuencias de 50 paquetes ICMP por prueba con un total de 50 pruebas por escenario.

4.3.1. Evaluación del rendimiento de la red en IPv6 post- implementación

Con el propósito de poder establecer los valores de rendimiento de la red tras la implementación del método Dual Stack, se ejecutaron 50 pruebas de conectividad mediante el protocolo ICMP hacia el servidor DNS público de Google en IPv6 (2001:4860:4860::8888), desde el equipo BNG-CARAVELI, en cada prueba se enviaron 50 paquetes, registrando la latencia promedio, los paquetes enviados, recibidos y perdidos, de manera equivalente a la metodología aplicada en la evaluación de IPv4.

Tabla 4.6*Evaluación de rendimiento de la red en IPv6*

Prueba	Paquetes Enviados	Paquetes Recibidos	Paquetes Perdidos	Pérdida (%)	Disponibilidad (%)	Latencia Prom. (ms)
1	50	50	0	0%	100%	87.5
2	50	50	0	0%	100%	87.5
3	50	50	0	0%	100%	87.5
4	50	50	0	0%	100%	87.5
5	50	50	0	0%	100%	87.5
6	50	50	0	0%	100%	87.6
7	50	50	0	0%	100%	87.5
8	50	50	0	0%	100%	87.5
9	50	50	0	0%	100%	87.5
10	50	50	0	0%	100%	87.5
11	50	50	0	0%	100%	87.5
12	50	50	0	0%	100%	87.5
13	50	50	0	0%	100%	87.6
14	50	50	0	0%	100%	87.5
15	50	50	0	0%	100%	87.5
16	50	50	0	0%	100%	87.6
17	50	50	0	0%	100%	87.5
18	50	50	0	0%	100%	87.5
19	50	50	0	0%	100%	87.5
20	50	50	0	0%	100%	87.5
21	50	50	0	0%	100%	87.5
22	50	50	0	0%	100%	87.5
23	50	50	0	0%	100%	87.6
24	50	50	0	0%	100%	87.5
25	50	50	0	0%	100%	87.5
26	50	50	0	0%	100%	87.6
27	50	50	0	0%	100%	87.5
28	50	50	0	0%	100%	87.5
29	50	50	0	0%	100%	87.5
30	50	50	0	0%	100%	87.5
31	50	49	1	2%	98%	87.5
32	50	50	0	0%	100%	87.5
33	50	50	0	0%	100%	87.5
34	50	50	0	0%	100%	87.5
35	50	50	0	0%	100%	87.5
36	50	50	0	0%	100%	87.6
37	50	50	0	0%	100%	87.5
38	50	50	0	0%	100%	87.5
39	50	50	0	0%	100%	87.5
40	50	50	0	0%	100%	87.5
41	50	50	0	0%	100%	87.5
42	50	50	0	0%	100%	87.5
43	50	50	0	0%	100%	87.6
44	50	50	0	0%	100%	87.5
45	50	50	0	0%	100%	87.5
46	50	50	0	0%	100%	87.5
47	50	50	0	0%	100%	87.5
48	50	50	0	0%	100%	87.5
49	50	50	0	0%	100%	87.5
50	50	50	0	0%	100%	87.5

Los resultados evidencian que durante las 50 pruebas realizadas bajo el protocolo IPv6 mediante Dual Stack, no se registró ningún paquete perdido en ninguna de las secuencias de envío, alcanzando una disponibilidad del 100% en la totalidad de las pruebas, la

latencia promedio obtenida tuvo valores mínimos de 87.5 ms y máximos de 87.6 ms, esto reflejaría una variabilidad mínima y un comportamiento altamente estable del enlace IPv6, posteriormente se hicieron pruebas de ping realizadas hacia 2001:4860:4860::8888, esto evidencia los resultados obtenidos en distintos intervalos de la evaluación:

Figura 4.16

Prueba de ping IPv6 – Prueba N.º 1(50 paquetes, 0% pérdida, avg-rtt 87ms535us)

```

Terminal
32 2001:4860:4860::8888      56 118 87ms528us  echo reply
33 2001:4860:4860::8888      56 118 87ms532us  echo reply
34 2001:4860:4860::8888      56 118 87ms537us  echo reply
35 2001:4860:4860::8888      56 118 87ms539us  echo reply
36 2001:4860:4860::8888      56 118 87ms540us  echo reply
37 2001:4860:4860::8888      56 118 87ms539us  echo reply
38 2001:4860:4860::8888      56 118 87ms518us  echo reply
39 2001:4860:4860::8888      56 118 87ms517us  echo reply
  sent=40 received=40 packet-loss=0% min-rtt=87ms472us avg-rtt=87ms535us max-rtt=87ms625us
SEQ HOST                                SIZE TTL TIME                    STATUS
40 2001:4860:4860::8888                56 118 87ms530us  echo reply
41 2001:4860:4860::8888                56 118 87ms525us  echo reply
42 2001:4860:4860::8888                56 118 87ms543us  echo reply
43 2001:4860:4860::8888                56 118 87ms540us  echo reply
44 2001:4860:4860::8888                56 118 87ms519us  echo reply
45 2001:4860:4860::8888                56 118 87ms523us  echo reply
46 2001:4860:4860::8888                56 118 87ms542us  echo reply
47 2001:4860:4860::8888                56 118 87ms565us  echo reply
48 2001:4860:4860::8888                56 118 87ms534us  echo reply
49 2001:4860:4860::8888                56 118 87ms523us  echo reply
  sent=50 received=50 packet-loss=0% min-rtt=87ms472us avg-rtt=87ms535us max-rtt=87ms625us

[dartelecom@BNG-CARAVELI] >

```

La Figura 4.16 corresponde a la primera prueba de la serie en la que se enviaron 50 paquetes ICMP hacia el servidor DNS de Google en IPv6, obteniendo una recepción completa sin pérdidas y una latencia promedio de 87.535 ms, este resultado inicial establece la línea de comportamiento del enlace IPv6 en condiciones normales de operación.

Figura 4.17

Prueba de ping IPv6 – Prueba N.º 10 (50 paquetes, 0% pérdida, avg-rtt 87ms544us)

```
Terminal
32 2001:4860:4860::8888 56 118 87ms529us echo reply
33 2001:4860:4860::8888 56 118 87ms536us echo reply
34 2001:4860:4860::8888 56 118 87ms526us echo reply
35 2001:4860:4860::8888 56 118 87ms514us echo reply
36 2001:4860:4860::8888 56 118 87ms580us echo reply
37 2001:4860:4860::8888 56 118 87ms526us echo reply
38 2001:4860:4860::8888 56 118 87ms540us echo reply
39 2001:4860:4860::8888 56 118 87ms503us echo reply
sent=40 received=40 packet-loss=0% min-rtt=87ms503us avg-rtt=87ms544us max-rtt=87ms756us

SEQ HOST SIZE TTL TIME STATUS
40 2001:4860:4860::8888 56 118 87ms605us echo reply
41 2001:4860:4860::8888 56 118 87ms545us echo reply
42 2001:4860:4860::8888 56 118 87ms621us echo reply
43 2001:4860:4860::8888 56 118 87ms519us echo reply
44 2001:4860:4860::8888 56 118 87ms506us echo reply
45 2001:4860:4860::8888 56 118 87ms560us echo reply
46 2001:4860:4860::8888 56 118 87ms500us echo reply
47 2001:4860:4860::8888 56 118 87ms505us echo reply
48 2001:4860:4860::8888 56 118 87ms498us echo reply
49 2001:4860:4860::8888 56 118 87ms552us echo reply
sent=50 received=50 packet-loss=0% min-rtt=87ms498us avg-rtt=87ms544us max-rtt=87ms756us

[dartelecom@BNG-CARAVELI] >
```

La Figura 4.17 presenta los resultados de la décima prueba de la serie, al igual que en la primera medición los 50 paquetes fueron recibidos sin pérdida alguna, la latencia promedio registrada fue de 87.544 ms, este valor es prácticamente idéntico al de la prueba inicial lo que comienza a evidenciar la estabilidad del enlace IPv6.

Figura 4.18

Prueba de ping IPv6 – Prueba N.º 20 (50 paquetes, 0% pérdida, avg-rtt 87ms564us)

```
Terminal
32 2001:4860:4860::8888 56 118 87ms701us echo reply
33 2001:4860:4860::8888 56 118 87ms611us echo reply
34 2001:4860:4860::8888 56 118 87ms518us echo reply
35 2001:4860:4860::8888 56 118 87ms586us echo reply
36 2001:4860:4860::8888 56 118 87ms512us echo reply
37 2001:4860:4860::8888 56 118 87ms531us echo reply
38 2001:4860:4860::8888 56 118 87ms558us echo reply
39 2001:4860:4860::8888 56 118 87ms530us echo reply
sent=40 received=40 packet-loss=0% min-rtt=87ms503us avg-rtt=87ms564us max-rtt=87ms701us

SEQ HOST SIZE TTL TIME STATUS
40 2001:4860:4860::8888 56 118 87ms612us echo reply
41 2001:4860:4860::8888 56 118 87ms654us echo reply
42 2001:4860:4860::8888 56 118 87ms580us echo reply
43 2001:4860:4860::8888 56 118 87ms543us echo reply
44 2001:4860:4860::8888 56 118 87ms571us echo reply
45 2001:4860:4860::8888 56 118 87ms545us echo reply
46 2001:4860:4860::8888 56 118 87ms552us echo reply
47 2001:4860:4860::8888 56 118 87ms536us echo reply
48 2001:4860:4860::8888 56 118 87ms542us echo reply
49 2001:4860:4860::8888 56 118 87ms515us echo reply
sent=50 received=50 packet-loss=0% min-rtt=87ms503us avg-rtt=87ms564us max-rtt=87ms701us

[dartelecom@BNG-CARAVELI] >
```

La Figura 4.18 muestra los resultados de la prueba número 20, acá se evidencia de que la tendencia observada en las mediciones anteriores se mantiene, habiendo un 0% de pérdida de paquetes y una latencia promedio de 87.564 ms, además la variación respecto a las pruebas anteriores es inferior a 0.03 ms lo que confirma la alta estabilidad del enlace en el punto intermedio de la evaluación.

Figura 4.19

Prueba de ping IPv6 – Prueba N.º 30 (50 paquetes, 0% pérdida, avg-rtt 87ms535us)

```
Terminal
32 2001:4860:4860::8888          56 118 87ms528us echo reply
33 2001:4860:4860::8888          56 118 87ms532us echo reply
34 2001:4860:4860::8888          56 118 87ms537us echo reply
35 2001:4860:4860::8888          56 118 87ms539us echo reply
36 2001:4860:4860::8888          56 118 87ms540us echo reply
37 2001:4860:4860::8888          56 118 87ms539us echo reply
38 2001:4860:4860::8888          56 118 87ms518us echo reply
39 2001:4860:4860::8888          56 118 87ms517us echo reply
  sent=40 received=40 packet-loss=0% min-rtt=87ms472us avg-rtt=87ms535us max-rtt=87ms625us
SEQ HOST                                SIZE TTL TIME                    STATUS
40 2001:4860:4860::8888                56 118 87ms530us echo reply
41 2001:4860:4860::8888                56 118 87ms525us echo reply
42 2001:4860:4860::8888                56 118 87ms543us echo reply
43 2001:4860:4860::8888                56 118 87ms540us echo reply
44 2001:4860:4860::8888                56 118 87ms519us echo reply
45 2001:4860:4860::8888                56 118 87ms523us echo reply
46 2001:4860:4860::8888                56 118 87ms542us echo reply
47 2001:4860:4860::8888                56 118 87ms565us echo reply
48 2001:4860:4860::8888                56 118 87ms534us echo reply
49 2001:4860:4860::8888                56 118 87ms523us echo reply
  sent=50 received=50 packet-loss=0% min-rtt=87ms472us avg-rtt=87ms535us max-rtt=87ms625us
[dartelecom@BNG-CARAVELI] >
```

La Figura 4.19 corresponde a la prueba número 30 realizada en la segunda mitad de la serie de evaluación, los resultados siguen siendo consistente, la recepción de los 50 paquetes es perfecta y la latencia promedio es de 87.535 ms. Este comportamiento sostenido descarta la presencia de degradación del enlace a lo largo del tiempo de medición.

Figura 4.20

Prueba de ping IPv6 – Prueba N.º 40 (50 paquetes, 0 % pérdida, avg-rtt 87ms537us)

```
Terminal
32 2001:4860:4860::8888      56 118 87ms567us  echo reply
33 2001:4860:4860::8888      56 118 87ms544us  echo reply
34 2001:4860:4860::8888      56 118 87ms589us  echo reply
35 2001:4860:4860::8888      56 118 87ms558us  echo reply
36 2001:4860:4860::8888      56 118 87ms565us  echo reply
37 2001:4860:4860::8888      56 118 87ms535us  echo reply
38 2001:4860:4860::8888      56 118 87ms516us  echo reply
39 2001:4860:4860::8888      56 118 87ms532us  echo reply
sent=40 received=40 packet-loss=0% min-rtt=87ms483us avg-rtt=87ms539us max-rtt=87ms589us
SEQ HOST                      SIZE TTL TIME                STATUS
40 2001:4860:4860::8888      56 118 87ms543us  echo reply
41 2001:4860:4860::8888      56 118 87ms552us  echo reply
42 2001:4860:4860::8888      56 118 87ms522us  echo reply
43 2001:4860:4860::8888      56 118 87ms509us  echo reply
44 2001:4860:4860::8888      56 118 87ms525us  echo reply
45 2001:4860:4860::8888      56 118 87ms514us  echo reply
46 2001:4860:4860::8888      56 118 87ms529us  echo reply
47 2001:4860:4860::8888      56 118 87ms546us  echo reply
48 2001:4860:4860::8888      56 118 87ms523us  echo reply
49 2001:4860:4860::8888      56 118 87ms544us  echo reply
sent=50 received=50 packet-loss=0% min-rtt=87ms483us avg-rtt=87ms537us max-rtt=87ms589us
[dartelecom@BNG-CARAVELI] >
```

La Figura 4.20 presenta los resultados de la prueba número 40, acá se registró nuevamente un 0 % de pérdida de paquetes con una latencia promedio de 87.537 ms, la acumulación de pruebas sin ningún paquete perdido refuerza la fiabilidad del protocolo IPv6 implementado sobre la infraestructura Dual Stack del ISP.

Figura 4.21

Prueba de ping IPv6 – Prueba N.º 50 (50 paquetes, 0% pérdida, avg-rtt 87ms544us)

```
Terminal
32 2001:4860:4860::8888      56 118 87ms529us  echo reply
33 2001:4860:4860::8888      56 118 87ms536us  echo reply
34 2001:4860:4860::8888      56 118 87ms526us  echo reply
35 2001:4860:4860::8888      56 118 87ms514us  echo reply
36 2001:4860:4860::8888      56 118 87ms580us  echo reply
37 2001:4860:4860::8888      56 118 87ms526us  echo reply
38 2001:4860:4860::8888      56 118 87ms540us  echo reply
39 2001:4860:4860::8888      56 118 87ms503us  echo reply
sent=40 received=40 packet-loss=0% min-rtt=87ms503us avg-rtt=87ms544us max-rtt=87ms756us
SEQ HOST                                SIZE TTL TIME STATUS
40 2001:4860:4860::8888      56 118 87ms605us  echo reply
41 2001:4860:4860::8888      56 118 87ms545us  echo reply
42 2001:4860:4860::8888      56 118 87ms621us  echo reply
43 2001:4860:4860::8888      56 118 87ms519us  echo reply
44 2001:4860:4860::8888      56 118 87ms506us  echo reply
45 2001:4860:4860::8888      56 118 87ms560us  echo reply
46 2001:4860:4860::8888      56 118 87ms500us  echo reply
47 2001:4860:4860::8888      56 118 87ms505us  echo reply
48 2001:4860:4860::8888      56 118 87ms498us  echo reply
49 2001:4860:4860::8888      56 118 87ms552us  echo reply
sent=50 received=50 packet-loss=0% min-rtt=87ms498us avg-rtt=87ms544us max-rtt=87ms756us
[dartelecom@BNG-CARAVELI] >
```

La Figura 4.21 corresponde a la última prueba de la serie de evaluación IPv6, al completarse las 50 mediciones se confirma que el comportamiento del enlace se mantuvo constante a lo largo de toda la evaluación, con 0% de pérdida de paquetes en todas las pruebas y una latencia promedio final de 87.544 ms, prácticamente idéntica a la registrada en la primera medición, lo que valida la estabilidad y confiabilidad del escenario IPv6 implementado.

4.3.2. Resumen estadístico del escenario IPv6 (Dual Stack)

Los resultados de las 50 pruebas realizadas fueron consolidados en una tabla de resumen la cual integra en un solo cuadro tres indicadores que fueron la latencia, pérdida de paquetes y disponibilidad. Todos estos resultados fueron generados en la evaluación de la línea base IPv4, con el fin de facilitar la comparación posterior entre ambos escenarios.

Tabla 4.7*Resultados de medición de latencia en IPv6*

Indicador	Métrica	Valor
Latencia	Latencia mínima	87.5 ms
	Latencia máxima	87.6 ms
	Latencia promedio	87.5 ms
Pérdida de paquetes	Total, enviados	2 500
	Total, recibidos	2 500
	Pérdida promedio	0.00 %
Disponibilidad	Total, enviados / recibidos	2 500 / 2 500
	Disponibilidad	100.00 %

La tabla consolidada confirma que el escenario IPv6 bajo Dual Stack alcanzó resultados óptimos en los tres indicadores evaluados, la latencia promedio fue estable y tuvo un valor de 87.5 ms con una variabilidad de apenas 0.1 ms entre valores extremos, hubo una ausencia total de pérdida de paquetes en las 2 500 transmisiones realizadas y una disponibilidad del 100.00 %, todos estos valores evidencian un rendimiento confiable y consistente de la red post- implementación.

4.3.3. Análisis comparativo entre IPv4 e IPv6 (Dual Stack)

Una vez obtenidos los indicadores de rendimiento en ambos escenarios, se realizó el análisis comparativo de los tres indicadores evaluados: latencia, pérdida de paquetes y disponibilidad, los resultados se presentan en las siguientes tablas comparativas.

Tabla 10*Comparación de latencia entre escenario IPv4 e IPv6*

Métrica de latencia	IPv4	IPv6 (Dual Stack)
Latencia mínima (ms)	51.5 ms	87.5 ms
Latencia máxima (ms)	54.3 ms	87.6 ms
Latencia promedio (ms)	52.6 ms	87.5 ms
Variación (ms)	2.8 ms	0.1 ms

En cuanto a la latencia, se observa que el escenario IPv6 registra valores promedio de 87.5 ms superiores a los 52.6 ms obtenidos bajo IPv4, este incremento de aproximadamente 34.9 ms se explica principalmente por la diferencia en el destino de las pruebas: en el escenario IPv4 se realizaron pings hacia direcciones dentro de la red troncal, mientras que en IPv6 el destino fue un servidor externo global (2001:4860:4860::8888), lo que introduce la latencia propia del recorrido hacia Internet. No obstante, la variabilidad de la latencia en IPv6 es notablemente menor (rango de 0.1 ms frente a 2.8 ms en IPv4), lo que indica mayor consistencia y estabilidad en la transmisión.

Tabla 11*Comparación de pérdida de paquetes entre escenario IPv4 e IPv6 (Dual Stack)*

Métrica de pérdida	IPv4	IPv6 (Dual Stack)
Total de paquetes enviados	2500	2500
Total de paquetes recibidos	2493	2500
Paquetes perdidos	7	0
Pérdida promedio (%)	0.28 %	0.00 %

La comparación de pérdida de paquetes reveló que hubo una gran mejora en el escenario IPv6 mientras que bajo IPv4 se perdieron 7 paquetes de un total de 2500 enviados, estos paquetes perdidos representan el 0.28 % del total, mientras que en el escenario IPv6 no se registró ningún paquete perdido. Este resultado evidencia que la implementación Dual Stack no genera degradación en la integridad de la transmisión de datos, sino que por el contrario esto permite alcanzar una entrega perfecta de paquetes hacia destinos IPv6 globales.

Tabla 12*Comparación de disponibilidad entre escenario IPv4 e IPv6 (Dual Stack)*

Métrica de disponibilidad	IPv4	IPv6 (Dual Stack)
Paquetes enviados	2500	2500
Paquetes recibidos	2493	2500
Disponibilidad (%)	99.72 %	100.00 %

En términos de disponibilidad, el escenario IPv6 alcanza el 100.00% frente al 99.72% registrado bajo IPv4, si bien ambos valores se consideran altos y operativamente aceptables, la disponibilidad perfecta obtenida en IPv6 refuerza la viabilidad técnica del método Dual Stack para poder garantizar la continuidad del servicio durante y después del proceso de migración.

4.3.4. Análisis del rendimiento del equipo posterior a la implementación Dual Stack

De forma adicional a la evaluación del análisis de latencia, pérdida de paquetes y disponibilidad, se procedió a evaluar el comportamiento de los recursos del equipo MikroTik CCR2116-12G-4S+ antes y después de la implementación Dual Stack, esto se hizo con la finalidad de poder determinar si la coexistencia de IPv4 e IPv6 genera un impacto importante en el consumo de CPU y memoria. Los resultados obtenidos en el escenario pre- implementación (RouterOS 7.14) muestran un uso de CPU que oscilaba entre 27% y 32%, con memoria libre de 15.2 GiB sobre 16.0 GiB totales:

Figura 4.22

Estado de recursos del equipo BNG-CARAVELI en el escenario pre- implementación (RouterOS 7.14, CPU: 32%)

```
[dartelecom@BNG-CARAVELI] > /system resource print
    uptime: 1w1d15h41m36s
    version: 7.14 (stable)
    build-time: 2024-02-29 11:44:44
    factory-software: 7.8
    free-memory: 15.2GiB
    total-memory: 16.0GiB
    cpu: ARM64
    cpu-count: 16
    cpu-load: 32%
    free-hdd-space: 77.3MiB
    total-hdd-space: 128.0MiB
    write-sect-since-reboot: 41695
    write-sect-total: 577368
    bad-blocks: 0.3%
    architecture-name: arm64
    board-name: CCR2216-1G-12XS-2XQ
    platform: MikroTik
[dartelecom@BNG-CARAVELI] > █
```

La Figura 4.22 muestra la primera medición del escenario pre- implementación, el equipo CCR2116-1G-12XS-2XQ ejecutaba RouterOS 7.14 con una carga de CPU del 32%, uptime de 1 semana 15 horas, y 15.2 GiB de memoria libre sobre 16.0 GiB totales, este nivel de uso de CPU refleja la carga de procesamiento que el equipo soportaba operando únicamente con IPv4, incluyendo las sesiones PPPoE activas y el enrutamiento estático en producción.

Figura 4.23

Estado de recursos del equipo BNG-CARAVELI en el escenario pre -implementación (RouterOS 7.14, CPU: 28%)

```
[darte telecom@BNG-CARAVELI] > /system resource print
    uptime: 1w1d15h41m22s
    version: 7.14 (stable)
    build-time: 2024-02-29 11:44:44
    factory-software: 7.8
    free-memory: 15.2GiB
    total-memory: 16.0GiB
    cpu: ARM64
    cpu-count: 16
    cpu-load: 28%
    free-hdd-space: 77.3MiB
    total-hdd-space: 128.0MiB
    write-sect-since-reboot: 41695
    write-sect-total: 577368
    bad-blocks: 0.3%
    architecture-name: arm64
    board-name: CCR2216-1G-12XS-2XQ
    platform: MikroTik
[darte telecom@BNG-CARAVELI] >
```

La Figura 4.23 corresponde a una segunda medición tomada segundos después de la anterior, con una carga de CPU del 28%, esta ligera variación respecto a la medición anterior es normal en equipos con múltiples procesos activos y confirma que la carga de procesamiento en el escenario IPv4 oscilaba en el rango del 27 % al 32 %, sin estabilizarse en un valor fijo.

Figura 4.24

Estado de recursos del equipo BNG-CARAVELI en el escenario pre -i implementación (RouterOS 7.14, CPU: 27%)

```
[darte telecom@BNG-CARAVELI] > /system resource print
    uptime: 1w1d15h41m7s
    version: 7.14 (stable)
    build-time: 2024-02-29 11:44:44
    factory-software: 7.8
    free-memory: 15.2GiB
    total-memory: 16.0GiB
    cpu: ARM64
    cpu-count: 16
    cpu-load: 27%
    free-hdd-space: 77.3MiB
    total-hdd-space: 128.0MiB
    write-sect-since-reboot: 41695
    write-sect-total: 577368
    bad-blocks: 0.3%
    architecture-name: arm64
    board-name: CCR2216-1G-12XS-2XQ
    platform: MikroTik
[darte telecom@BNG-CARAVELI] >
```

La Figura 4.24 presenta la tercera medición del escenario reimplementación que registra la carga de CPU más baja del conjunto que es 27 %, este valor confirma que incluso en el punto mínimo de uso del procesador durante el escenario IPv4, la carga era considerablemente superior a la observada tras la implementación Dual Stack, estableciendo así una línea de referencia clara para la comparación posterior.

En contraste, las capturas obtenidas en el escenario post- implementación (RouterOS 7.20.7 con Dual Stack activo) muestran un uso de CPU del 4 %, con memoria libre de 15.3 GiB sobre 16.0 GiB

Figura 4.25

Estado de recursos del equipo BNG-CARAVELI en el escenario post- implementación (RouterOS 7.20.7, CPU: 4 %)

```
[dartelecom@BNG-CARAVELI] > /system resource print
    uptime: 21h24m42s
    version: 7.20.7 (long-term)
    build-time: 2026-01-08 09:40:00
    factory-software: 7.8
    free-memory: 15.3GiB
    total-memory: 16.0GiB
    cpu: ARM64
    cpu-count: 16
    cpu-frequency: 2000MHz
    cpu-load: 4%
    free-hdd-space: 87.9MiB
    total-hdd-space: 128.0MiB
    write-sect-since-reboot: 13518
    write-sect-total: 1488483
    bad-blocks: 0%
    architecture-name: arm64
    board-name: CCR2116-12G-4S+
    platform: MikroTik
```

La Figura 4.25 muestra la primera medición del escenario post- implementación Dual Stack, el equipo CCR2116-12G-4S+ opera ahora con RouterOS 7.20.7 (long-term), registrando una carga de CPU del 4 % y 15.3 GiB de memoria libre, la reducción del uso de CPU respecto al escenario pre- implementación es inmediata y sustancial, teniendo de rango de 27 %-32 % y se pasa a un 4 %, lo que representa una disminución de entre 23 y 28 puntos porcentuales.

Figura 4.26

Estado de recursos del equipo BNG-CARAVELI en el escenario post- implementación 2 (RouterOS 7.20.7, CPU: 4 %)

```
[dartelecom@BNG-CARAVELI] > /system resource print
    uptime: 21h24m11s
    version: 7.20.7 (long-term)
    build-time: 2026-01-08 09:40:00
    factory-software: 7.8
    free-memory: 15.3GiB
    total-memory: 16.0GiB
    cpu: ARM64
    cpu-count: 16
    cpu-frequency: 2000MHz
    cpu-load: 4%
    free-hdd-space: 87.9MiB
    total-hdd-space: 128.0MiB
    write-sect-since-reboot: 13516
    write-sect-total: 1488481
    bad-blocks: 0%
    architecture-name: arm64
    board-name: CCR2116-12G-4S+
    platform: MikroTik
[dartelecom@BNG-CARAVELI] > 
```

La Figura 4.26 corresponde a una segunda medición del escenario post- implementación que fue tomada instantes después de la anterior, el uso de CPU se mantiene en el 4 %, con parámetros de memoria y almacenamiento idénticos a los de la medición previa y la consistencia de este valor en dos capturas consecutivas confirma que la reducción de carga de CPU no es transitoria, sino un estado estable del equipo operando con Dual Stack y RouterOS 7.20.7.

Tabla 13

Comparación de recursos del equipo MikroTik CCR2116-12G-4S+ antes y después de la implementación Dual Stack

Recurso	Pre-implementación (IPv4 / ROS 7.14)	Post-implementación (Dual Stack / ROS 7.20.7)
Versión RouterOS	7.14 (stable)	7.20.7 (long-term)
Uso de CPU	27 % – 32 %	4 % – 6 %
Memoria libre	15.2 GiB / 16.0 GiB	15.3 GiB / 16.0 GiB
CPU count	16 núcleos	16 núcleos
Arquitectura	ARM64	ARM64

Los resultados muestran que el uso de CPU se redujo de forma significativa después de la implementación del Dual Stack pasando de un rango inicial de 27 %-32 % en el

escenario de solo IPv4 a un rango de 4%–6% en el escenario con Dual Stack activo, este comportamiento sugiere que la carga de procesamiento no fue incrementada por la habilitación de IPv6, sino que por el contrario la optimización del sistema operativo RouterOS 7.20.7 contribuyó a un manejo más eficiente de los recursos, el consumo de memoria RAM se mantuvo prácticamente constante en ambos escenarios, con variaciones despreciables.

Teniendo todos estos resultados se puede descartar que la implementación Dual Stack pueda generar una carga adicional significativa sobre los recursos del equipo, confirmando que la coexistencia de IPv4 e IPv6 en la infraestructura del ISP SERVICIOS A PUNTO S.A.C. es técnicamente viable sin comprometer el rendimiento operativo del hardware.

Capítulo V: Discusión

5.1. Evaluación del rendimiento de la red

La evaluación de la red del ISP SERVICIOS A PUNTO S.A.C. bajo el protocolo IPv4 evidenció un comportamiento estable: latencia promedio de 52.6 ms, pérdida de paquetes de apenas 0.28 % sobre 2 500 transmisiones y disponibilidad de 99.72 %, valores que establecen una línea base operativamente aceptable pero que exponen las limitaciones estructurales del protocolo ante el crecimiento sostenido de la demanda, estos resultados son coherentes con lo reportado por (Almutlaq & Elfadil, 2022), quienes midieron un retardo promedio de 61.4 ms en entornos dual-stack bajo IPv4 confirmando que la latencia en redes ISP con este protocolo tiende a mantenerse en rangos similares bajo condiciones normales de operación.

Por su parte (Boswell et al., 2024) añaden que las rutas IPv4 nativas presentan tiempos de respuesta menores en comparación con esquemas de transición basados en NAT64, lo que refuerza la validez de usar IPv4 como referencia de desempeño, pero como advierten (Rizzo & Salerno, 2024), más del 60 % de los operadores aún depende de mecanismos de transición por incompatibilidades con infraestructura heredada, situación que limita la escalabilidad y que en el caso de SERVICIOS A PUNTO S.A.C., se manifiesta en la disponibilidad finita de 64 direcciones IPv4 públicas para atender una base creciente de abonados en la provincia de Caravelí.

5.2. Implementación del método Dual Stack en la red del ISP

La implementación del método Dual Stack se ejecutó de manera exitosa sobre la infraestructura real de SERVICIOS A PUNTO S.A.C., abarcando la actualización del firmware a RouterOS 7.20.7, la configuración del direccionamiento IPv6 con prefijos /64 y /45 asignados por INTERNEXA (bloque 2803:65d0: :/32), el enrutamiento estático con 1

291 rutas activas y la habilitación de DHCPv6-PD con 409 abonados recibiendo prefijos /56. Este resultado es consistente con lo hallado por (Núñez, 2022), quien planteó para el Gobierno Regional Amazonas que el método Dual Stack con inventario de recursos, nueva topología y calendario gradual es una alternativa viable para la coexistencia de ambos protocolos sin interrumpir el servicio existente; del mismo modo, (Castro & Raez, 2023) demostraron en una red corporativa peruana que la arquitectura híbrida IPv4/IPv6 optimiza el uso de direcciones públicas y mejora la escalabilidad.

A escala internacional, los resultados se alinean con (Lencse & Bazsó, 2024), quienes validaron metodologías de benchmarking para tecnologías de transición como 464XLAT y MAP-T, confirmando que implementaciones correctamente planificadas permiten escalar desde pocas hasta millones de conexiones simultáneas, la delegación de prefijos a 409 abonados activos y la presencia de 1 291 rutas en la tabla IPv6 demuestran que la migración del ISP no se limitó a un entorno de prueba, sino que alcanzó escala productiva real, validando la viabilidad técnica del Dual Stack en redes de acceso de última milla.

5.3. Comparación de los resultados antes y después de la migración

El análisis comparativo entre los escenarios IPv4 e IPv6 revela diferencias relevantes en los tres indicadores evaluados, con respecto a la pérdida de paquetes y disponibilidad, IPv6 Dual Stack alcanzó 0.00 % de pérdida y 100.00 % de disponibilidad frente a 0.28 % y 99.72 % registrados bajo IPv4 siendo la eliminación completa de pérdidas el hallazgo más significativo; este resultado concuerda con (Shahid et al., 2024), quienes en entornos IPv6 con EIGRP reportaron pérdidas de solo 5 % y también es consecuente con (Boswell et al., 2024), quienes confirmaron que la conectividad nativa IPv6 ofrece mayor integridad de transmisión que los esquemas de traducción.

Respecto a la latencia los valores IPv6 (87.5 ms promedio) son superiores a los IPv4 (52.6 ms) el cual es una diferencia atribuible principalmente al destino de las pruebas, mientras en IPv4 se evaluaron nodos de la red troncal local, en IPv6 el destino fue el servidor DNS

global de Google (2001:4860:4860::8888, introduciendo la latencia inherente al tránsito internacional; esto concuerda con (Wnorowski & Lebkowski, 2022), quienes señalan precisamente que los mecanismos de transición pueden incrementar la latencia entre 10 % y 25 %, aunque en el caso del Dual Stack nativo este costo es sensiblemente menor que en soluciones como NAT64.

Finalmente, la reducción del uso de CPU de 27-32 % a 4-6 % tras la actualización a RouterOS 7.20.7 con Dual Stack activo evidencia que la coexistencia de protocolos no incrementa la carga de procesamiento, este hallazgo coincide con lo reportado por (Cala, 2025) al señalar que una planificación técnica adecuada permite que la transición IPv6 mejore la eficiencia operativa de la infraestructura sin comprometer la calidad del servicio a los usuarios finales.

Conclusiones y Recomendaciones

Conclusiones

- La evaluación del rendimiento de la red del ISP SERVICIOS A PUNTO S.A.C. bajo operación exclusiva en IPv4 evidenció un comportamiento estable y dentro de rangos operativos aceptables, la latencia promedio fue de 52.6 ms, la pérdida de paquetes alcanzó un 0.28 % y la disponibilidad del servicio se situó en 99.72 %, estos indicadores confirmaron que la infraestructura preexistente garantizaba la continuidad del servicio; pero la limitación de 64 direcciones IPv4 públicas disponibles representa una restricción estructural insuperable para el crecimiento sostenido de la red ante el incremento de usuarios y dispositivos, justificando técnica y operativamente la necesidad de avanzar hacia IPv6.
- La implementación del protocolo IPv6 mediante el método Dual Stack en la red del ISP SERVICIOS A PUNTO S.A.C. fue ejecutada de forma exitosa y sin interrupción del servicio IPv4, el proceso incluyó la actualización del firmware a RouterOS 7.20.7, la asignación y configuración del bloque IPv6 2803:65d0: :/32 provisto por INTERNEXA, el enrutamiento estático por zonas geográficas de cobertura y la habilitación de DHCPv6-PD que delegó prefijos /56 a 409 abonados activos a través de interfaces PPPoE. La presencia de 1 291 rutas IPv6 en la tabla de enrutamiento del router de gestión y la conectividad confirmada hacia Internet IPv6 con 0 % de pérdida de paquetes demostraron que la red alcanzó escala operativa real bajo Dual Stack..
- Se hizo la comparación de los indicadores de rendimiento antes y después de la implementación Dual Stack confirmando la hipótesis de la investigación, en pérdida de paquetes el escenario IPv6 eliminó por completo las pérdidas registradas en IPv4 pasando de 0.28 % a 0.00 %. En disponibilidad se alcanzó el 100.00 % frente al 99.72 % previo, en latencia el escenario IPv6 presentó una latencia promedio de 87.5 ms superior a los 52.6 ms de IPv4, esta diferencia es atribuible al destino externo global de las pruebas y no a una degradación del protocolo; adicionalmente la variabilidad de la latencia en IPv6 fue de apenas 0.1 ms

frente a 2.8 ms en IPv4, evidenciando mayor consistencia en la transmisión. Además, el uso de CPU del equipo de borde se redujo de 27 %–32 % a 4 %–6 % tras la actualización a RouterOS 7.20.7 con Dual Stack activo, descartando que la habilitación de IPv6 genere carga adicional sobre el hardware.

Recomendaciones

- • Se recomienda extender la implementación Dual Stack a todas las zonas de cobertura del ISP, replicando el proceso de configuración de direccionamiento IPv6, enrutamiento estático y DHCPv6-PD en las demás zonas de cobertura de SERVICIOS A PUNTO S.A.C. (Ocona, Secocha, San Juan, Ispacas, Ático), aprovechando el bloque 2803:65d0: :/32 ya asignado por INTERNEXA y la experiencia técnica acumulada durante esta implementación.
- • Se recomienda establecer un monitoreo continuo de los indicadores de rendimiento en el escenario Dual Stack, para ello se debe implementar herramientas de monitoreo automatizado como Zabbix o Grafana integrado con SNMP sobre los equipos MikroTik que permitan registrar de manera sistemática la latencia, pérdida de paquetes y disponibilidad en tiempo real, tanto en el plano IPv4 como en IPv6, para detectar oportunamente cualquier degradación del servicio durante la fase de consolidación de la migración.
- • Se recomienda evaluar la migración progresiva hacia un escenario IPv6-only en segmentos con equipos CPE compatibles, a medida que la base de usuarios actualice sus equipos domésticos a modelos con soporte nativo IPv6, planificando la transición gradual de esos segmentos hacia IPv6-only, eliminando la dependencia de IPv4 en el segmento de última milla y reduciendo la complejidad operativa del Dual Stack a largo plazo.
- • Se recomienda ampliar el alcance metodológico en futuras investigaciones incorporando métricas adicionales buscando que estudios futuros incorporen métricas de throughput, jitter y tiempo de convergencia de rutas, así como pruebas bajo carga

simultánea de tráfico IPv4 e IPv6, con el fin de obtener una caracterización más completa del comportamiento de la red en el escenario Dual Stack.

Bibliografía

- Acosta, E. (2024). Planeamiento estratégico y el proceso de transición al IPv6 en el Servicio Nacional de la Sanidad Agraria. <https://repositorio.une.edu.pe/handle/20.500.14039/10869>
- Almutlaq, W., & Elfadil, N. (2022). A Comparative Performance Evaluation of IPv4/IPv6 Using Network Simulation and Virtualization Tools. *11*, 56-65. <https://doi.org/10.47760/ijcsmc.2022.v11i10.005>
- Barraza, E., Salazar, S., & Serna, H. (2024). *Integración del Protocolo IPv6 en la Red GPON Para Mejorar la Calidad del Servicio de Internet en los Abonados de ISP Econocable Distrito de Villa El Salvador*. <https://repositorio.upci.edu.pe/handle/upci/1511>
- Bhuiyan, Z., Ullah, A., Khan, M., Morshed, S., & Islam, M. (2023). An Empirical Research Towards the State of Transition from IPv4 to IPv6. *6*, 1-6. <https://doi.org/10.1109/STI59863.2023.10464716>
- Boswell, E., McQuistin, S., Perkins, C., & Strowes, S. (2024). Measuring NAT64 Usage in the Wild. *11*. <https://doi.org/10.48550/arXiv.2402.14632>
- Cala, G. (2025). Análisis de la situación actual de la transición al protocolo IPv6 en las entidades públicas en el Perú. *6(1)*, 44-54. <https://doi.org/10.48168/innosoft.s23.a206>
- Castro, A., & Raez, J. (2023). *Arquitectura WAN en IPv4 a WAN en IPv6 para el aumento de pool público en una red corporativa en Perú*. <https://hdl.handle.net/20.500.12867/11463>
- Cervantes, P. (2024). *Diseño de la Operación lógica de los dispositivos que conforman la red de datos IPv4, desplegada en campamentos agrícolas de la sede Palmawasi - región San Martín*. <https://hdl.handle.net/20.500.12893/13834>
- Chamba, L. A. N. (2022). *PROPUESTA PARA LA IMPLEMENTACIÓN DEL PROTOCOLO IPV6 EN LA SEDE CENTRAL DEL GOBIERNO REGIONAL AMAZONAS - UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN*.

- Chen, G., Cao, Z., Xie, C., & Binet, D. (2014, junio). *NAT64 Deployment Options and Experience* (inf. téc. N.º RFC7269). RFC Editor. <https://doi.org/10.17487/rfc7269>
- Curran, J. (2008, julio). *An Internet Transition Plan* (Request for Comments N.º RFC 5211) (Num Pages: 8). Internet Engineering Task Force. <https://doi.org/10.17487/RFC5211>
- Deering, S. E., & Hinden, B. (1995, diciembre). *Internet Protocol, Version 6 (IPv6) Specification* (Request for Comments N.º RFC 1883) (Num Pages: 37). Internet Engineering Task Force. <https://doi.org/10.17487/RFC1883>
- Delgado, R. (2017). Charla magistral 4: La Adopción de Internet de las Cosas e IPv6: El Caso Perú. <https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/71367/Charla%20magistral%204%20Rosa%20Delgado%20-%20La%20Adopci%C3%B3n%20de%20Internet%20de%20las%20Cosas%20e%20IPv6%20El%20Caso%20Per%C3%BA%20%28A100%2010.08.2017%29.pdf?sequence=1&isAllowed=y>
- Dell, P. (2018). On the dual-stacking transition to IPv6: A forlorn hope? *Telecommunications Policy*, 42(7), 575-581. <https://doi.org/https://doi.org/10.1016/j.telpol.2018.04.005>
- Durdagl, E., & Buldu, A. (2010). IPV4/IPV6 security and threat comparisons [Innovation and Creativity in Education]. *Procedia - Social and Behavioral Sciences*, 2(2), 5285-5291. <https://doi.org/https://doi.org/10.1016/j.sbspro.2010.03.862>
- Gomez-Rodriguez, J., Sandoval-Aréchiga, R., Ibarra-Delgado, S., & Flores-Troncoso, J. (2016). IPv6 El tiempo ha llegado. *Difu100ci@, Revista de difusión científica, ingeniería y tecnologías*, 10(2), 12-16.
- Hamarsheh, A., Alqeerm, A., Akour, I., Alauthman, M., Aldweesh, A., Ali, M., & Alangari, S. (2023). Comparative Evaluation of Host-Based Translator Mechanisms for IPv4-IPv6 Communication Performance Analysis With Different Routing Protocols. 13. <https://doi.org/10.4018/IJCAC.332765>

- Hong, Y. G., Shin, M. K., & Kim, H. J. (2003). Application translation for IPv6 at NAT-PT. *9th Asia-Pacific Conference on Communications (IEEE Cat. No.03EX732)*, 1, 203-207 Vol.1. <https://doi.org/10.1109/APCC.2003.1274343>
- Hsu, A., Li, F., Pearce, P., & Gasser, O. (2024). A First Look At NAT64 Deployment In-The-Wild. 2. <https://doi.org/10.48550/arXiv.2311.04181>
- Hughes, L. E. (2022). Review of IPv4. En *Third Generation Internet Revealed: Reinventing Computer Networks with IPv6* (pp. 41-117). Apress. https://doi.org/10.1007/978-1-4842-8603-6_3
- itojun Hagino, J.-i. (2005). *1 - Introduction* (J.-i. itojun Hagino, Ed.). Digital Press. <https://doi.org/https://doi.org/10.1016/B978-155558318-7/50002-2>
- Jadhav, S. S., & Ballal, B. R. (2022). Review of IPv4 and IPv6 and various implementation methods of IPv6. *Arabia*, 4(783), 66.
- Lencse, G., & Bazsó, Á. (2024). Benchmarking methodology for IPv4aaS technologies: Comparison of the scalability of the Jool implementation of 464XLAT and MAP-T. 219, 243-258. <https://doi.org/10.1016/j.comcom.2024.03.007>
- Macho, T. (2012). IPv6 protocol – Base principles, deployment and industrial applications [11th IFAC, IEEE International Conference on Programmable Devices and Embedded Systems]. *IFAC Proceedings Volumes*, 45(7), 220-225. <https://doi.org/https://doi.org/10.3182/20120523-3-CZ-3015.00043>
- Manayay Ramírez, C. S., & Olivera Samamé, R. E. (2015). *Migración de IPv4 a IPv6 para mejorar la seguridad y velocidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo*.
- Núñez, L. (2022). *Propuesta para la implementación del protocolo IPv6 en la sede central del gobierno regional Amazonas - Unidad de Tecnologías de la Información*. <https://hdl.handle.net/20.500.11818/6537>
- Palma, P. (2022). *Seguridad IPv4 y los sistemas de información en trámites administrativos de los funcionarios de la Unamba región Apurímac*. <https://hdl.handle.net/20.500.12692/129083>

- Prieto, J. P. M. (2018). *PROPUESTA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A PROTOCOLO IPV6 PARA LA SECRETARIA DEL SISBEN DE LA ALCALDIA DE TUNJA*.
- Qu, J., Ma, X., Liu, W., Sang, H., Li, J., Xue, L., & Guan, X. (2024). On Smartly Scanning of the Internet of Things. 32, 1019-1034. <https://doi.org/10.1109/TNET.2023.3312162>
- Rizzo, S., & Salerno, N. (2024). Actual Reasons Involving Turn-Off Losses Improvement With Increasing Load and Gate Resistance in MOSFETs Enhanced With Kelvin Source. 71, 369-379. <https://doi.org/10.1109/TIE.2023.3243272>
- Robinson, K., Zurawski, J., & Costello, T. (2024). Designing, Constructing, and Operating an IPv6 Network at SC23. (24), 1-8. <https://doi.org/10.1145/3626203.367053>
- Sailan, K., Hassan, R., & Patel. (2009). A comparative review of IPv4 and IPv6 for research test bed. 02, 427-433. <https://doi.org/10.1109/ICEEI.2009.5254698>
- Salas, A. C. C. (2022). *MODELO DE MIGRACIÓN DE RED IPV4 AL PROTOCOLO IPV6 PARA REDES EMPRESARIALES*.
- Shahid, K., Ahmad, S., & Hussain, S. (2024). Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems. 16(9). <https://doi.org/10.3390/fi16090339>
- Streibelt, F., Sattler, P., Lichtblau, F., Gañán, C., Feldmann, A., Gasser, O., & Fiebig, T. (2023). How Ready is DNS for an IPv6-Only World? 1382, 525-549. https://doi.org/10.1007/978-3-031-28486-1_22
- Tomy Baltazar, M. A. (2017). Modelo de referencia de transición de IPv4 a IPv6 para el sector gobierno de Perú.
- Torres Sánchez, D. (2017, septiembre). *INTRODUCCIÓN Y CONFIGURACIÓN DEL PROTOCOLO IPV6* [Accepted: 2018-05-14T19:20:52Z Publisher: Universidad Autonoma del Estado de México]. Consultado el 10 de octubre de 2023, desde <http://ri.uaemex.mx/handle/20.500.11799/82865>

Wnorowski, J., & Lebkowski, A. (2022). Verification of the System for Ship Position Keeping Equipped with a Set of Anchors in Unity3d. 22(19). <https://doi.org/10.3390/s22197421>