UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TÍTULO

MIGRACIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA INFINIX INTERNET UBICADA EN LAS CIUDADES DE ATUNTAQUI Y COTACACHI

AUTOR

Fernández Catucuago, Sergio Rolando

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGÍSTER EN TELECOMUNICACIONES

TUTORA

Llerena Guevara, Lucrecia Alejandrina

Santa Elena, Ecuador

Año 2025

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA
Validar únicamente con FirmaEC

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

LUCRECIA ALEJANDRINA LLERENA GUEVARA
Firmado digitalmente por LUCRECIA ALEJANDRINA LLERENA GUEVARA
Fecha: 2025.11.26 11:02:02 -05'00'

Ing. Lucrecia Llerena Guevara, Ph.D.
TUTORA

Firmado electrónicamente por:
DANIEL ARMANDO JARAMILLO CHAMBA
Validar únicamente con FirmaEC

Ing. Daniel Jaramillo Chamba, Mgtr.
DOCENTE ESPECIALISTA

LUIS MIGUEL AMAYA FARINO
Digitally signed by LUIS MIGUEL AMAYA FARINO

Ing. Luis Amaya Fariño, Mgtr.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ
Validar únicamente con FirmaEC

Abg. María Rivera González, Mgtr.
SECRETARIA GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por el ING SERGIO ROLANDO FERNÁNDEZ CATUCUAGO, como requerimiento para la obtención del título de Magíster en Telecomunicaciones.

TUTORA

LUCRECIA ALEJANDRINA LLERENA GUEVARA

Firmado digitalmente por LUCRECIA ALEJANDRINA LLERENA GUEVARA
Fecha: 2025.11.26 11:02:36 -05'00'

Ing. Lucrecia Llerena Guevara, Ph.D.

Santa Elena, 30 de septiembre de 2025

UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **SERGIO ROLANDO FERNÁNDEZ CATUCUAGO**

DECLARO QUE:

El trabajo de Titulación, (Migración del protocolo IPv4 hacia IPv6 en la empresa INFINIX INTERNET ubicada en las ciudades de Atuntaqui y Cotacachi) previo a la obtención del título en Magíster en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 30 de septiembre de 2025

EL AUTOR

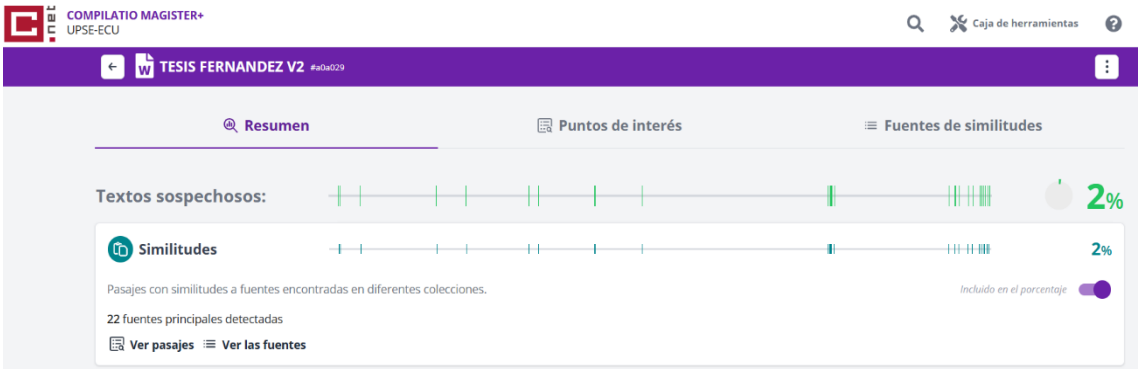
Firmado electrónicamente por:
SERGIO ROLANDO FERNANDEZ CATUCUAGO
Validar únicamente con FirmaEC

Sergio Rolando Fernández Catucuago

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Migración del protocolo IPv4 hacia IPv6 en la empresa INFINIX INTERNET ubicada en las ciudades de Atuntaqui y Cotacachi, presentado por el estudiante, SERGIO ROLANDO FERNÁNDEZ CATUCUAGO fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 2%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



TUTORA

LUCRECIA ALEJANDRINA LLERENA GUEVARA

Firmado digitalmente por LUCRECIA ALEJANDRINA LLERENA GUEVARA
Fecha: 2025.11.26 11:02:47 -05'00'

Ing. Lucrecia Llerena Guevara, Ph.D.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **SERGIO ROLANDO FERNÁNDEZ CATUCUAGO**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo con fines de difusión pública, además apruebo la reproducción de este Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 30 de septiembre de 2025

EL AUTOR

Firmado electrónicamente por:
SERGIO ROLANDO FERNANDEZ CATUCUAGO
Validar únicamente con FirmaEC

Sergio Rolando Fernández Catucuago

AGRADECIMIENTO

A Dios por brindarme sabiduría y su presencia permanente.

Al Instituto de Posgrado de la Universidad Estatal Península de Santa Elena, por brindarme la oportunidad de estudiar una maestría.

A los Docentes por el esfuerzo de sus labores en formar y enseñar.

De forma especial a mi directora de tesis PhD. Lucrecia Llerena. Por guiarme en el desarrollo de esta investigación con la enseñanza de sus valiosos conocimientos y su profesionalismo como docente.

Sergio Rolando, Fernández Catucuago

DEDICATORIA

Principalmente, a Dios, por bendecirme con los padres que tengo, por guiarme a lo largo de la vida y por permitir culminar con éxitos una etapa más de mi vida. A mis queridos padres José Leonidas y María Cruz por todo lo que me enseñaron para ser una persona correcta y por su enorme sacrificio para darme la educación.

A mis hermanos Welington y Alexander por darme la oportunidad de compartir momentos inolvidables desde la niñez y por su apoyo incondicional.

A mis familiares por los sabios consejos que me supieron compartir para seguir adelante en mis estudios. A mi novia Mónica, por estar siempre a mi lado en los buenos y malos momentos que hemos pasado, por su apoyo incondicional desde el inicio de mi vida universitaria hasta hoy en día.

Especialmente al hermoso regalo que Dios me ha brindado, a mi querido hijo Jhosuá, a quien amo con todo mi corazón, por brindarme la dicha de ser padre y por ser la motivación de cada día.

Sergio Rolando, Fernández Catucuago

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El avance acelerado en el campo de las telecomunicaciones y el incremento de dispositivos electrónicos conectados a internet han generado la necesidad de adoptar IPv6 como solución a las limitaciones del protocolo IPv4. En este contexto, la investigación plantea una migración del protocolo IPv4 hacia IPv6 en la empresa INFINIX INTERNET, con el propósito de tener una red estable y eficiente que mejore el tráfico de datos. El estudio realizado incluye un diagnóstico detallado de la infraestructura de la red, los recursos de los equipos activos, el direccionamiento IP actual y la capacidad de ancho de banda disponible. Seguidamente, se analizaron distintos mecanismos de transición, concluyendo que Dual Stack es el más idóneo para ser implementado, puesto que permite la operabilidad simultánea de ambos protocolos sin interrumpir la operabilidad del servicio. Finalmente, se determina un plan de direccionamiento IPv6, garantizando estabilidad, escalabilidad y soporte al creciente futuro del ISP.

Palabras claves: IPv6, Migración de protocolos, plan de direccionamiento.

ABSTRACT

Rapid advances in the field of telecommunications and the increase in electronic devices connected to the internet have created the need to adopt IPv6 as a solution to the limitations of the IPv4 protocol. In this context, the research proposes a migration from the IPv4 protocol to IPv6 at the company INFINIX INTERNET, with the aim of achieving a stable and efficient network that improves data traffic. The study includes a detailed diagnosis of the network infrastructure, active equipment resources, current IP addressing, and available bandwidth capacity. Next, different transition mechanisms were analysed, concluding that Dual Stack is the most suitable for implementation, as it allows both protocols to operate simultaneously without interrupting service operability. Finally, an IPv6 addressing plan was determined, guaranteeing stability, scalability, and support for the ISP's growing future.

Keywords: IPv6, Protocol migration, Addressing plan.

INTRODUCCIÓN

El internet ha sido uno de los avances tecnológicos más importantes a nivel mundial, ya que funciona como una herramienta de comunicación y acceso a la información. Su funcionamiento se implementa mediante un protocolo conocido como IP (Protocolo de Internet). En la actualidad, todos los equipos conectados a internet usan IPv4; sin embargo, la cantidad de dispositivos que pueden conectarse está limitada por la cantidad de direcciones disponibles. En total, IPv4 alcanza aproximadamente los 4.300 millones de direcciones, las cuales se están agotando rápidamente a nivel global. Según LACNIC en el 2024 da a conocer que solamente dispone de menos del 4% de este espacio de direcciones IPv4.

Las redes de telecomunicaciones han evolucionado exponencialmente, generando una mayor demanda de servicio con el aumento masivo de la tecnología. La mayoría de los proveedores de servicios de internet han empezado a implementar IPv6 o tienen planificado realizarlo de manera inmediata. En Sudamérica, Ecuador registra un 28% de adopción de IPv6, mientras que a nivel mundial Google reporta que el 49.64% del tráfico del internet ya se realiza sobre el protocolo IPv6 (IPv6-Google, 2025).

LACNIC, la entidad que se encarga de administrar las direcciones IPv4 e IPv6 en Latinoamérica y el Caribe, provee e impulsa a la transición a este nuevo protocolo, En informes previos, LACNIC señalaba que Ecuador contaba con apenas un 1.5% de direcciones IPv6 implementadas, lo que evidencia un incremento significativo en los últimos años. Este avance resalta la importancia de que los proveedores de servicio de internet continúen fortaleciendo la adopción de IPv6 con el fin de asegurar la estabilidad y eficiencia de sus redes.

Diversos estudios y reportes técnicos destacan que, aunque la adopción de IPv6 avanza, persisten brechas importantes que afectan a los ISPs, como la falta de capacidad técnica, la coexistencia prolongada entre IPv4 e IPv6 y la ausencia de políticas internas para gestionar la transición. De igual manera, se identifican riesgos operativos asociados a fallas en las configuraciones, carencia de pruebas en entornos controlados y vulnerabilidades si no se aplican buenas prácticas recomendadas por los RFC. A esto se suman los costos operativos relacionados con la actualización de equipos, soporte técnico y mantenimiento Dual Stack, lo que representa un desafío particular para proveedores

medianos. Estos elementos permiten comprender el contexto técnico y operativo en el que se plantea esta investigación, resaltando la necesidad de un modelo de transición ordenado y seguro hacia IPv6.

Conociendo el auge de la tecnología, se plantea el presente proyecto con el objetivo de desarrollar el cambio de protocolo IPv4 a IPv6 en la red de la empresa INFINIX INTERNET, considerando los mecanismos de transición para proporcionar una red más estable y eficiente que mejore el tráfico de datos. Esta iniciativa forma parte de un plan estratégico de renovación tecnológica, que contempla la implementación de los dos protocolos en los nodos de Atuntaqui y Cotacachi. De esta manera se modernizar el direccionamiento IP de la infraestructura actual de la red, buscando aumentar la disponibilidad del servicio para cada uno de sus usuarios y resolver problemas de estabilidad y rendimiento que actualmente afectan a la red.

El alcance de esta investigación comprende la elaboración de un inventario de los equipos activos de la infraestructura actual y el análisis del direccionamiento IP existente. A partir de esto, se propone un nuevo esquema de direccionamiento IP basado en las recomendaciones de los estándares internacionales expuestos en los RFC, tanto para subredes y para enlaces punto a punto. Este esquema de direccionamiento considera la coexistencia entre IPv4 e IPv6 mediante mecanismos de transición, con el fin de garantizar la compatibilidad operativa en la red de la empresa. Este plan se desarrolla en entorno de laboratorio, donde se realizan pruebas de configuración en los equipos Mikrotik. Finalmente, la respectiva validación se lleva a cabo mediante la prueba de IPv6 de Google y la herramienta de Wireshark para constatar la operabilidad del protocolo IPv4 e IPv6.

El presente trabajo sostiene que la adopción progresiva de IPv6 no solo es una necesidad técnica, sino también una estrategia de crecimiento y sostenibilidad para los proveedores de Internet. Su relevancia radica en la posibilidad de asegurar la conectividad a largo plazo, fortalecer la infraestructura tecnológica y así brindar un servicio eficiente a los usuarios. Así mismo, contribuye al desarrollo social y profesional al proveer una guía técnica replicable para otros ISPs (Proveedor de servicios de Internet) en el Ecuador, tanto en el ámbito de las telecomunicaciones como en lo científico, al documentar un modelo

de transición que puede ser utilizados como referencias en futuros proyectos académicos y técnicos.

Este trabajo de investigación busca aportar un modelo técnico de referencia para la transición de IPv4 a IPv6 en las redes de los ISPs en Ecuador, contribuyendo tanto al fortalecimiento de la infraestructura tecnológica como al desarrollo del sector de las telecomunicaciones en el país.

La estructura del presente trabajo de titulación se divide en tres capítulos. El Capítulo 1, presenta el marco teórico referencial, el cual que se compone de dos secciones fundamentales. La primera sección es la revisión de literatura. Su objetivo es sustentar conceptualmente el estudio a través de fuentes académicas relevantes. Aquí se identifica los avances, limitaciones y vacíos en investigaciones previas. La segunda parte trata sobre el desarrollo teórico, permitiendo desglosar y profundizar los conceptos que sustentan el tema de investigación.

El Capítulo 2 describe la metodología de investigación. Esta información es fundamental para garantizar un análisis técnico y estratégico del proceso de transición del protocolo IPv4 a IPv6 en la empresa INFINIX INTERNET. Los procesos metodológicos aseguran la fiabilidad de la información obtenida en el estudio y permiten establecer una transmisión de protocolo de internet, garantizando la continuidad de los servicios y la interoperabilidad de la red.

En el Capítulo 3 se muestran los resultados y discusión, desarrollando cada uno de los objetivos propuestos para encontrar una solución. El análisis se divide en tres partes. En la primera parte, se realiza el diagnóstico de la infraestructura de red llevando a cabo el levantamiento de información técnica. Este proceso describe todos los equipos activos, la evaluación de los procesos que poseen cada uno, el esquema de direccionamiento IP y la capacidad de ancho de banda disponible. Toda esta información permite determinar el estado de la red y es la base fundamental para entender cómo realizar el proceso de transición.

La segunda parte correspondiente a la selección del mecanismo de transición de IPv4 a IPv6. Es importante elegir un mecanismo de transición de protocolo que garantice la compatibilidad, permitiendo que los dos protocolos operen juntos.

La tercera parte presenta un esquema de direccionamiento IPv6. Se define un plan de direccionamiento IPv6 garantizando escalabilidad, eficiencia y compatibilidad con los servicios que ofrece el ISP, asegurando así una migración ordenada y funcional.

Finalmente, esta investigación se concreta con un conjunto de conclusiones y recomendaciones derivadas del análisis y el desarrollo de la investigación.

Planteamiento de la investigación

La empresa INFINIX INTERNET en la actualidad, ofrece sus servicios y mantiene su conectividad a internet mediante redes de telecomunicaciones que se encuentran operando bajo el protocolo IPv4. Sin embargo, esta tecnología limita la posibilidad de realizar una expansión de la red, ya que requiere de un suministro prácticamente ilimitado de direcciones IP, recursos que se encuentran en agotamiento. Frente a esta limitación, el protocolo IPv6 logrará satisfacer los requerimientos de operabilidad y expansión que IPv4 no es capaz de garantizar.

El protocolo IPv4 hoy en día presenta falencias y limitaciones. Una de ellas es que su encabezado de datagrama es el doble de tamaño que el del protocolo IPv6. Esta característica desfavorable implica que los equipos electrónicos tengan mayor procesamiento de información. Además, en IPv4 el uso del IPSec es opcional, mientras que en IPv6 constituye una implementación con soporte nativo que fortalece la seguridad de las comunicaciones. Otro aspecto crítico es que IPv4 ha dejado de ser un protocolo estable debido al crecimiento exponencial de dispositivos conectados a internet, esto lleva al agotamiento de sus direcciones públicas.

Los proveedores de servicios de internet, hoy en día se encuentran comprometidos en realizar la transición y convergencia tecnológica hacia el protocolo IPV6. Es un proceso prácticamente inevitable para garantizar un correcto desempeño y funcionalidad de las redes. En este contexto, la empresa INFINIX INTERNET, como un proveedor de servicios de internet, debe llevar a cabo en un futuro próximo la transición de sus sistemas y servicios desde el protocolo IPv4 hacia IPv6, con la finalidad de asegurar la continuidad operativa y responder a las crecientes demandas del mercado digital.

Justificación

El crecimiento acelerado de usuarios y dispositivos conectados a internet ha generado una reducción crítica en la disponibilidad de direcciones IPv4, lo que limita la expansión sostenible del servicio de acceso a internet. Esta situación obliga a implementar soluciones que respondan a los problemas de escalabilidad y eficiencia en la prestación de los servicios de internet. En este contexto, el protocolo IPv6 surge como la alternativa capaz de garantizar un tráfico de datos más adecuado frente a la creciente demanda de acceso a Internet. Este protocolo subsana las principales falencias de IPv4, al ofrecer mayor espacio de direccionamiento, lo que permite mantener una transmisión más confiable y segura, que garantiza sostenibilidad tecnológica a largo plazo.

Según datos recientes de LACNIC, aproximadamente el 20% de los usuarios en el Ecuador ya cuentan con conectividad IPv6, ubicando al país entre los líderes de adopción en Latinoamérica junto a países como Uruguay y Brasil. Esta cifra evidencia la necesidad de que más proveedores integren IPv6 para garantizar la continuidad del servicio.

El estudio de protocolo de nueva generación IPv6 incluye mejoras en su encabezado del paquete. Entre sus ventajas está la autoconfiguración de direcciones y la seguridad mejorada, gracias al soporte nativo para IPSec, de tal forma que simplifica la red al eliminar la necesidad de NAT (Traducción de Direcciones de Red). IPv6 permite una comunicación de extremo a extremo más directa, optimizando el rendimiento de nuevas aplicaciones como domótica y el Internet de las cosas (IoT). En consecuencia, la adopción de este protocolo de internet prepara a los ISP para el crecimiento continuo de los servicios digitales y asegura una base sólida para la evolución de las telecomunicaciones en el país.

Objetivo General:

Desarrollar el cambio de protocolo IPv4 a IPv6 en la red de la empresa INFINIX INTERNET mediante los mecanismos de transición para proporcionar una red más estable y eficiente que mejore el tráfico de datos.

Objetivos Específicos:

1. Realizar un levantamiento de información de la red actual mediante un diagnóstico de las configuraciones de los equipos y el direccionamiento IPv4 para determinar los cambios necesarios al nuevo protocolo de red IPv6.
2. Seleccionar el mecanismo de transición del protocolo IPv4 a IPv6 por medio de la investigación bibliográfica determinando parámetros fundamentales que establezcan la convivencia entre estos dos protocolos de internet.
3. Diseñar un esquema de direccionamiento IPv6 robusta mediante un análisis técnico y su respectiva prueba en la red con la finalidad de fortalecer el incremento de sus usuarios y satisfacer la demanda a la aparición de nuevas aplicaciones que requieran un mejor tiempo de respuesta, disponibilidad de ancho de banda y sobre todo seguridad.

Planteamiento hipotético

La presente propuesta planteada mediante los mecanismos de transición del protocolo de internet IPv4 a IPv6 permitirá un adecuado crecimiento de la infraestructura de la red, abarcando a más clientes con la finalidad de mejorar la calidad de transmisión de la información.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

El presente capítulo está estructurado en dos secciones. En primer lugar, se presenta la revisión de literatura, con la finalidad de sustentar conceptualmente el estudio a través de fuentes académicas confiables e investigaciones relevantes que aporten con temas relacionados al estudio del protocolo IP y la necesidad de migración hacia IPv6. La segunda sección aborda el desarrollo teórico y conceptual, permitiendo analizar en detalle los fundamentos técnicos del protocolo IPv6, sus mecanismos de transición y su relevancia para garantizar la continuidad y expansión de los servicios de telecomunicaciones.

1.1. Revisión de literatura

En esta sección se presenta estudios previos relacionados con la transición del protocolo de internet IPV4 hacia IPv6, así como investigaciones sobre la convivencia entre ambos protocolos en redes de telecomunicaciones. Se revisan artículos científicos y tesis recientes que aborden temas similares a lo planteado en este tramo de investigación. El objetivo es identificar enfoques relevantes y comprar los resultados obtenidos en estudios anteriores, con el fin de sustentar técnica y conceptualmente la propuesta de esta investigación.

Los autores (Zhang et al., 2024), analizan la transición de una red de IPv4 hacia IPv6 en un entorno de intranet basada en una red de campus. Proponen un esquema modular y una topología de servicio integrados que soporta el acceso a múltiples usuarios mediante el protocolo de Dual Stack. El estudio aborda las limitaciones de IPv4, como el rendimiento y los problemas de interconexión de redes. Además, se consideran las vulnerabilidades existentes durante la transición del protocolo, para la misma proponen un esquema de verificación de direcciones de origen real de IPv6 para prevenir ataques externos. Finamente, se realizan pruebas de simulación y pruebas reales, demostrando que el esquema propuesto garantiza un acceso confiable a los recursos de la intranet y facilita la coexistencia entre ambos protocolos.

Los autores (Z. Li & Qiu, 2021), dan a conocer que el crecimiento de la industria de las redes ha impulsado la popularidad de los dispositivos conectados a internet. En esta situación, las direcciones IPv4 de 32 bits se han ido agotando de manera progresiva. Ante

esta situación, surgió el desarrollo del protocolo IPv6, el cual ha sido adoptado por diferentes actores del sector, centrado la atención en los mecanismos de transición a IPv6. Con la aparición de IPv6, muchos lo consideran como una mejora de IPv4 por su amplio espacio de direccionamiento. Entre los mecanismos de transición más relevantes se encuentran Dual Stack, traducción y tunelización, los cuales permiten la convivencia entre ambos protocolos durante el proceso de migración. El principio de la transición reside en sus nuevas funciones y su amplio espacio de direcciones. Para los usuarios finales, IPv6 representa una comunicación más segura y eficientes entre aplicaciones, asegurando la continuidad de los servicios en la nueva generación de redes.

En el estudio realizado por (G. Xu, 2021), se comparan y analizan las estructuras de mensajes de IPv4 e IPv6. Este artículo revela que la dirección de red IPv4 presenta serias deficiencias, mientras que el protocolo IPv6 se caracteriza por una estructura de mensajes más eficiente. Además, ofrece un espacio de direccionamiento mucho más amplio y permite la configuración automatizada de direcciones IP. También integra políticas de seguridad y dispone de un mecanismo de descubrimiento de vecinos eficiente, entre otras características. No obstante, dada que la red IPv4 aún se utiliza ampliamente y no puede ser reemplazada por completo por la red IPv6, lo que hace necesario una etapa de transición. Este artículo también analiza la tecnología de túnel, traductor de direcciones de red y dual Stack. Finalmente, se presenta la configuración básica de la dirección IPv6 y del enrutamiento estático aplicada a un tipo específico de enrutador. Dada su relevancia, IPv6 es un protocolo de red muy importante, por lo que es fundamental investigar su aplicación en el Internet de las Cosas (IoT) en el futuro.

Los autores(Bing. Xu & Mou, 2020), realiza una investigación sobre la construcción y aplicación de redes IPv6 en centros de formación profesional superior en China. Dando a conocer que la mayoría de las redes de colegios y universidades está basada en IPv4, y que debido a las limitaciones de este protocolo se ha iniciado una transición gradual hacia IPv6. El estudio destaca que el uso del IPv6 no solo puede resolver problemas de escasez de recursos de direcciones de red, sino también elimina obstáculos para la conexión de múltiples dispositivos y servicios. Así mismo, se menciona que, en marzo de 2018, la proporción de usuarios que accedieron a sitios web de Google a través de IPv6 supero el 22.2% lo que evidencia el crecimiento y la adopción progresiva de este protocolo. Para la construcción de una red IPv6 los autores plantean un proceso en tres etapas:

1.- Primera etapa: Plantear una red de prueba IPv6 pura para que proporcione servicios de aplicaciones como web, DNS y FTP.

2.- Segunda etapa: Implementar la interconexión entre IPv4 e IPv6 dentro de la red del campus.

3- Tercera etapa: Establecer la interconexión entre la red IPv6 del campus y la red educativa, utilizando configuración de túneles para garantizar la interoperabilidad entre ambos protocolos.

En dicho contexto los autores plantean la implementación del túnel ISATAP (protocolo de direccionamiento automático de túnel intrasitio), una tecnología de tunelización automático punto a punto que permite la comunicación entre dispositivos IPv4 e IPv6. Finalmente, los autores concluyen que IPv6 es una es una versión avanzada de IPv4, pero que ambos protocolos no son compatibles, por lo cual deberán coexistir durante un periodo prolongado hasta que la transición sea completa.

Según el autor (Gallegos, 2024), plantea un proyecto de transición de IPv4 a IPv6 en una red LAN en una empresa textil de la ciudad de Ambato. El objetivo primordial es modernizar la infraestructura tecnológica de la empresa. Esta propuesta refleja el compromiso empresarial con la innovación y la modernización de tecnologías de vanguardia para garantizar un futuro sólido y eficiente. El plan de migración se desarrolla en fases concretas. El análisis de la situación actual es la primera fase donde realiza la recopilación de información técnica y un análisis de la infraestructura de la red existente. Como segunda fase plantea una selección del método de transición determinado un plan de direccionamiento y elección de estrategias más adecuadas para la migración. La tercera fase de implementación y pruebas siguiendo lineamientos técnicos y realizando pruebas de funcionalidad. Y por último la validación de operabilidad garantizando estabilidad y calidad de servicio dentro de la empresa.

Loa autores (Hu et al., 2024), en un estudio sobre la comprensión del uso de IPv6 en hogares inteligente, destacan que en los últimos años el soporte hacia IPv6 en las redes residenciales han aumentado. Actualmente, casi todos los dispositivos de red y sistemas operativos ofrecen compatibilidad con este protocolo. El artículo presenta el análisis exhaustivo de IPv6 en hogares inteligentes, considerando factores como la configuración, el DNS, así como prácticas de privacidad y seguridad.

En este contexto, para que los dispositivos IoT sean compatibles con IPv6, es necesario que cuenten con un sistema operativo y software de aplicación adaptado a este protocolo. Así mismo es indispensable que cuenten con la capacidad de resolver nombres de dominios en direcciones IPv6. No obstante, pese que la mayoría de los dispositivos IoT aún dependen de IPv4, incluso cuando cuentan con direcciones IPv6 en entornos de doble pila. Solo un número reducido de dispositivos logran operar correctamente en el protocolo IPv6, lo que refleja limitaciones técnicas y de soporte.

Unas de las principales causas identificadas en este estudio se relacionan con la falta de preparación del proveedor de servicio de internet. Estos al no ofrecer un soporte robusto en IPv6, genera dificultades de operabilidad en los disipativos IoT. En este sentido, los autores subrayan que resulta indispensable que los ISP trabajen de manera paralela con ambos protocolos para garantizar la funcionalidad y brindar escalabilidad a la demanda acelerada de equipos IoT que requieran mayor ancho de banda.

Finalmente, los autores concluyen que un cierto porcentaje de dispositivos IoT aun no funciona correctamente con el protocolo IPv6. Sin embargo, cuando se configura en Dual Stack y el ISP proporciona soporte adecuado, la operabilidad mejora significativamente. Bajo estas condiciones es posible prever que en un futuro próximo los dispositivos IoT alcanzaran una plena funcionalidad con IPv6 logrando conexiones seguras, confiables y sostenibles. En consecuencia, los autores incentivan a seguir investigando y fortaleciendo los procesos de adopción de IPv6, con el fin de asegurar una convivencia efectiva de protocolos y garantizar un futuro IoT plenamente funcional.

En conclusión, de acuerdo con los distintos estudios revisados, todos coinciden que la transición de protocolo IPv4 a IPv6 es inevitable y debe realizarse de manera gradual mediante mecanismos de coexistencias como Dual Stack, traducción y tunelización. Así mismo se evidencia que persisten desafíos, entre ellos la limitada implementación de este protocolo por parte de los ISP. Por ello, resulta indispensable consolidar una coexistencia entre ambos protocolos con el fin de asegurar la continuidad de los servicios en la nueva generación de redes.

1.2. Desarrollo teórico y conceptual

En este apartado se describe el desarrollo teórico y conceptual del protocolo IPv6, proporcionando un análisis detallado de sus fundamentos técnicos, mecanismo de transición y ventajas frente al protocolo IPv4. Además, se examina su papel estratégico con la continuidad, optimización y expansión de los servicios de telecomunicaciones.

1.2.1. Protocolo IP

El protocolo de internet (IP) está el principal protocolo de comunicación y conectividad de dispositivos de red para realizar el intercambio de paquetes. Para realizar esta comunicación el protocolo implementa funciones de direccionamiento y fragmentación de tal forma que los paquetes pueden viajar a través de la red (Ordabayeva et al., 2020).

La función básica que realiza el protocolo IP es:

- Direccionamiento: Se encarga de proporcionar una dirección IP única para identificar a un dispositivo dentro de una red.
- Enrutamiento: La implementación de múltiples niveles de jerarquía facilita la consolidación de rutas, promoviendo un enrutamiento eficiente y escalable en internet (Salcan, 2024).
- Fragmentación: Realiza la división de paquetes a través de una red.

IP se encarga de entregar paquetes desde un dispositivo origen al dispositivo destino basándose únicamente en las direcciones IP. Para ello el protocolo de internet define estructura de paquetes que encapsulan los datos que se entregarán. El protocolo de internet es un conjunto de reglas que se define como un dispositivo envía datos a otro. Básicamente se basa en el modelo de Capa de Internet en TCP/IP. Los dispositivos conectados a una red tienen una dirección IP única. Esta se utiliza para enrutar paquetes a través desde un origen hasta su destino (Ordabayeva et al., 2020).

1.2.2. Protocolo IPv6

IPv6 es un protocolo de internet más reciente que permite que los dispositivos se conecten a internet. Para esto se hace uso de direcciones IP que constan de 128 bits a diferencia de IPv4 que se conecta mediante una IP que consta de 32 bits. Dicho protocolo se ha ido tomando fuerza a nivel mundial debido al agotamiento de las direcciones IPv4 y además porque limita a la aparición de nuevas aplicaciones (Arco & Gallego, 2023).

El grupo de trabajo de la Ingeniería de Internet IETF creó el protocolo de internet versión 6 en 1998 mediante el RFC 2460 proporcionando suficiente espacio de direccionamiento para su uso futuro. Aunque IPv6 se lanzó hace 27 años, su implementación generalizada en redes IPv6 solo se ha producido en los último 7 años, el motivo de su implementación es debido a la escasez de direccionamiento IPv4 (K. H. Li & Wong, 2021).

IPv6 ofrece la posibilidad de acceder a 340 miles de trillones de direcciones IP a diferencia de IPv4 que ofrece 4.3 miles de millones de direcciones IP. De tal forma mediante IPv6 se permite priorizar paquetes a través de la implementación de calidad de servicio (QoS) de modo que se lleva a cabo una transmisión de datos de manera eficiente. IPv6 ofrece una conectividad punto a punto de manera que se descarta el NAT así tiendo transmisión de datos a altas velocidad y a muy bajas latencias (Aguirre, 2023).

A partir de noviembre de 2023 la tasa de adopción de IPv6 ha aumentado hasta alcanzar una participación de 45% del tráfico a nivel mundial. A medida que todos los proveedores de internet adopten IPv6 en sus redes podrán ofrecer un servicio con la menor tasa de pérdida de paquetes (Kasunic et al., 2024).

1.2.2.1. Características de IPv6

Las características de IPv6 abarcan aspectos técnicos y funcionales que lo convierten en el protocolo ideal para garantizar seguridad, escalabilidad y eficiencia en las redes de próxima generación**.**

- **Seguridad:** Toda infraestructura de red habilitada mediante IPv6 tiene la obligación de soportar el protocolo IPSec nativo a nivel de red, haciendo que IPv6 sea más seguro que los nodos IPv4. IPSec es un conjunto de protocolo cuya finalidad es asegurar las comunicaciones sobre el protocolo de internet autenticado, es decir que cada paquete IP es cifrado (UPN, 2022).
- **Escalabilidad:** Debido a la gran cantidad de direcciones IPv6 se tiene asegurado el crecimiento y expansión de las redes sin ninguna restricción. Esta es una característica fundamental en la nueva era del internet de las cosas, donde miles de sensores, dispositivos domésticos y otros aparatos requieren una conectividad a internet para su respectivo funcionamiento. Este protocolo IPv6 permite asignar direcciones globales únicas a cada dispositivo así eliminando la necesidad de soluciones complicadas de

overlaps de direcciones o múltiples capas de NAT para conectar a estos dispositivos (Crocetta Yanuario, 2025).

- **Autoconfiguración:** En el protocolo IPv4 los nodos están bajo una configuración estáticas mediante el cual se les asigna direcciones IPs fijas y que no cambian con el tiempo o mediante configuraciones dinámicas asignadas a un servidor DHCP. IPv6 incluye una característica denominada stateless autoconfiguración que permite a los usuarios hacer plug and play en redes sin contacto previo con el administrador de la red y obtener su dirección IPv6 (Socas & Gómez, 2023).
- **Simplificación de la arquitectura de red:** Mediante la adopción de IPv6 ya no se tiene la necesidad de NAT la cual reduce las direcciones IP públicas, pero presenta problemas de seguridad y rendimiento. IPv6 ofrece conexiones directas de extremo a extremo, configuración automática e IPSec para brindar una comunicación segura (Hossain et al., 2024).
- **Movilidad:** Una característica muy importante es la gestión de nodos IP móviles. El nodo puede moverse desde una red a otra, es decir intercambiar un enlace físico sin tener que cambiar su dirección IP.
- **Desempeño:** IPv6 ofrece rutas eficientes, menor latencia y mayor throughput, la cual redunda a una mejor experiencia para el usuario final. Esto es vital para los prestadores de servicios de telecomunicaciones ya que se puede brindar el servicio con menor latencia y pérdida de paquetes ya que evita la saturación en NAT (ITF, 2024).
- **Soporte de calidad de servicio:** La integración del protocolo IPv6 y la calidad de servicio (QoS) es fundamental para la optimización de las redes, ya que se implementan estrategias ante fallos de enlaces. Gracias a su característica de funcionalidad, IPv6 permite priorizar el tráfico de red mediante parámetros críticos de latencia, el jitter y los respectivos requerimientos de ancho de banda. La priorización de un servicio asegura que sus aplicaciones se mantengan en un óptimo desempeño, evitando la congestión y garantizando un flujo de datos más eficiente.

  La calidad de servicio mediante IPv6 posibilita una experiencia ininterrumpida del servicio al otorgar preferencia al tráfico esencial durante las transiciones de enlaces. Esto otorga que las redes tengan una mayor flexibilidad en la gestión de recursos, consolidando una infraestructura de red (Shahid et al., 2024).

- **Soporte a tecnologías emergentes y tendencias**

  Hoy en día las infraestructuras de red están viviendo una transformación hacia la virtualización, así como también el despliegue masivo de 5G. El protocolo IPv6 se integra naturalmente con estas tendencias. La tecnología 5G utiliza IPv6 para asignar identificadores únicos a cada dispositivo y aprovechar características como segmento routing sobre IPv6 para prepagar rutas inteligentes en una red (Crocetta Yanuario, 2025).

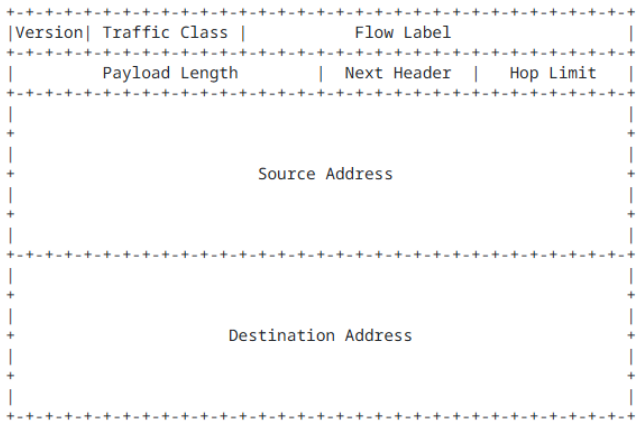
Como se analiza las características detalladas anteriormente nos dan una razón fundamental para la transición desde IPv4 a IPv6. Teniendo un beneficio en costes de operación, mejorando el rendimiento de la red y una mayor seguridad. Sin embargo, todo esto se puede relacionar directamente con la demanda de direcciones IP y la necesidad de tener una infraestructura escalable y estable.

1.2.2.2. Formato de encabezado

En el RFC 8200, documento oficial publicado por el grupo de trabajo de Ingeniería de Internet (IETF), describe las especificaciones del protocolo IPv6 y su respectivo formato de Encabezado.

El encabezado IPv6 elimina varios campos del encabezado IPv4, como se muestra en la Figura 1, con la finalidad de mantener de tamaño fijo, más simple y reduciendo el tiempo de procesamiento de paquetes.

Figura 1. Formato de encabezado IPv6



Fuente:(IETF RFC8200, 2017)

El encabezado IPv6 tiene una longitud fija de 40 octetos es decir 320 bits fijos, lo que hace el procesamiento de paquetes más eficiente.

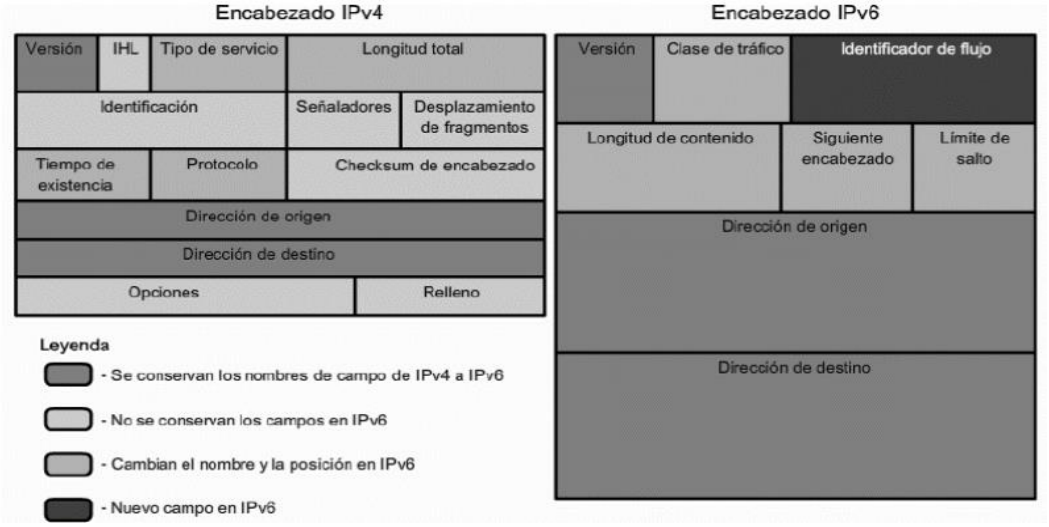
- **Versión:** Es el número de la versión del protocolo de internet; en este caso, corresponde a la versión 6 y ocupa 4 bits.
- **Clase de tráfico:** Este campo especifica la clase del tráfico. De tal forma que los valores de 0-7 están definidos para el tráfico de datos con control de la congestión y de 8-15 para el tráfico de streaming sin control. Este campo tiene 8 bits.
- **Etiqueta de flujo:** Campo determinado por 20 bits. Un flujo es definido como una secuencia de paquetes enviados desde el punto origen al punto destino. Un flujo se identifica únicamente por l combinación de una dirección origen y una etiqueta de 20 bits. El origen asigna la etiqueta a todos los paquetes que forma parte del mismo flujo (Rubio, 2022).
- **Longitud de carga útil:** Este campo especifica el tamaño del paquete incluyendo la cabecera y los datos en bytes. Este campo tiene 16 bits.
- **Siguiente encabezado:** Campo determinada con 8 bits. Identifica el tipo de encabezado inmediatamente posterior al encabezado IPv6.
- **Límites de saltos:** Campo de 8 bits. Determina el número de saltos máximos que le quedan al paquete. El límite de saltos es establecido a un valor máximo por el origen y reducido en 1 cada vez que un nodo encamina el paquete. Un nodo que sea el destino de un paquete no debe descartar un paquete con in con un salto igual a cero, debe procesar el paquete con normalidad (Viveros, 2024).
- **Dirección de Origen:** Campo de 128 bits que determina la dirección del origen del paquete.
- **Dirección de destino:** Campo de 128 bits que determina la dirección del destino del paquete(IETF RFC8200, 2017).

1.2.2.3. Diferencia de formato de encabezado de IPv4 e IPv6

El encabezado de IPv6 tiene un tamaño fijo de 40 bytes a comparación del protocolo IPv4 que tiene un tamaño variable entre 20 y 60 bytes. El protocolo de internet versión 4 incluye espacio para opciones mientras que en IPv6 estas opciones se conoce como extensiones de encabezado.

Como se muestra en la Figura 2, el protocolo IPv6 eliminan el campo IHL (Longitud de encabezado de internet), ya que el tamaño de encabezado es fijo de 40 bytes. Así mismo, se eliminan los campos de identificación y banderas presentes en el encabezado IPv4. Además, en el encabezado IPv6, el campo TTL (límite de tiempo) se renombra como límite de salto. Estos cambios reducen las sobrecargas de los equipos de telecomunicaciones y simplifica el procesamiento, optimizando el encapsulamiento de paquetes (José and Cervantes 2023).

Figura 2. Diferencia de encabezado IPv4 vs IPv6



Fuente: (Cañas, 2023)

1.2.2.4. Ventajas y desventajas del protocolo IPv6

A continuación, se presentan las principales ventajas y desventajas del protocolo IPv6, con el fin de evaluar su impacto en el rendimiento, la seguridad y la viabilidad de su adopción en entornos de telecomunicaciones.

Ventajas

- Presenta mayor escalabilidad con un gran número de direcciones IP, con esto se tendrá mayores números de dispositivos conectados a internet desarrollando un gran crecimiento tecnológico (Igulu et al., 2024).
- Seguridad en el direccionamiento IP mejorando fundamentalmente la arquitectura de telecomunicaciones y la funcionalidad al mismo tiempo que habilitan tecnologías de próxima generación (Kane, 2025).

- Uso del soporte nativo de IPSec la misma que se utiliza para asegurar las comunicaciones en redes IPv6, y su implementación es fundamental para proteger la información sensible que se transmite a través de la red (Cañas, 2023).
- IPv6 admite funcionalidad como configuración automática y plug a play. Ofreciendo un encapsulamiento más simple que IPv4 lo que aumenta la eficiencia del enrutamiento (Jadhav & Ballal, 2022).
- El protocolo IPv6 tiene una estructura de encabezado más eficiente, eso significa que los paquetes de datos puedan transmitirse más rápidamente y con menor latencia (Igulu et al., 2024).
- La calidad de servicio es implementada en la etiqueta de flujo en el encabezado del protocolo. Permitiendo dar alta prioridad a los paquetes que se envían a un destino en un cierto rango de tiempo (Piñeros et al., 2022).

Desventajas

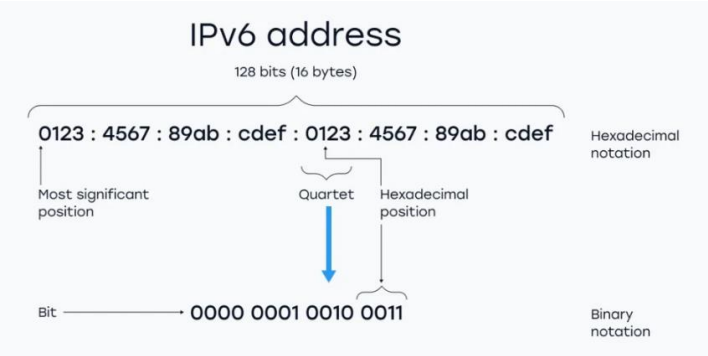
- IPv6 no es ampliamente compatible como IPv4, lo que conlleva que algunos dispositivos y redes pueden no ser capaces de aprovechar los beneficios de IPv6.
- Se deben crear nodos de soporte en IPv4 e IPv6 con el fin de tener una comunicación bidireccional. Esto debido a que existen aún aplicaciones operativas solo en el protocolo IPv4.
- Una de las principales desventajas de IPv6 es la demora en su implantación. A pesar de que el protocolo fue estandarizado hace varios años, su adopción sigue siendo limitada. Incluso con los mecanismos de transición o redes nativas IPv6, el porcentaje de despliegue aún sigue siendo bajo (Novoa, 2022).
- Para empresas pequeñas la implementación de IPv6 puede generar un costo de implementación, ya que muchos de sus equipos no podrían soportar el procesamiento de estos dos protocolos configurados simultáneamente (Torres, 2022).

1.2.3. Direccionamiento IPv6

El protocolo IPv6 proporciona un conjunto de direccionamiento más amplio gracias al uso del tamaño de direcciones de 128 bits. El grupo de trabajo de Ingeniería de Internet en 2017 determinó que IPv6 es un protocolo de internet completo (Iniobong et al., 2022).

La representación de una dirección IPv6 se detalla en la Figura 3 la misma que está compuesta con 32 dígitos hexadecimales, separados cada cuatro dígitos por un carácter de dos puntos (:). De esta forma una dirección IPv6 queda representada por 8 grupos de 4 dígitos hexadecimales. Es decir, una dirección IPv6 consta de 128 bits siendo así 4 veces más larga que una dirección IPv4. El protocolo IPv6 a diferencia de la versión anterior no usa máscara de red, si no que usan un prefijo, que se escribe en la misma barra después de la dirección. Por ejemplo, el prefijo /64 significa que, de 128 bits, los primeros 64 son a red y el resto es para el host. El prefijo en una dirección IPv6 determina cuantos bits en la dirección se usan para almacenar información de la red (Ordabayeva et al., 2020).

Figura 3. Representación de una dirección IPv6



Fuente: (Iniobong et al., 2022)

A continuación, se muestra las formas más comunes como pueden representar una dirección IPv6.

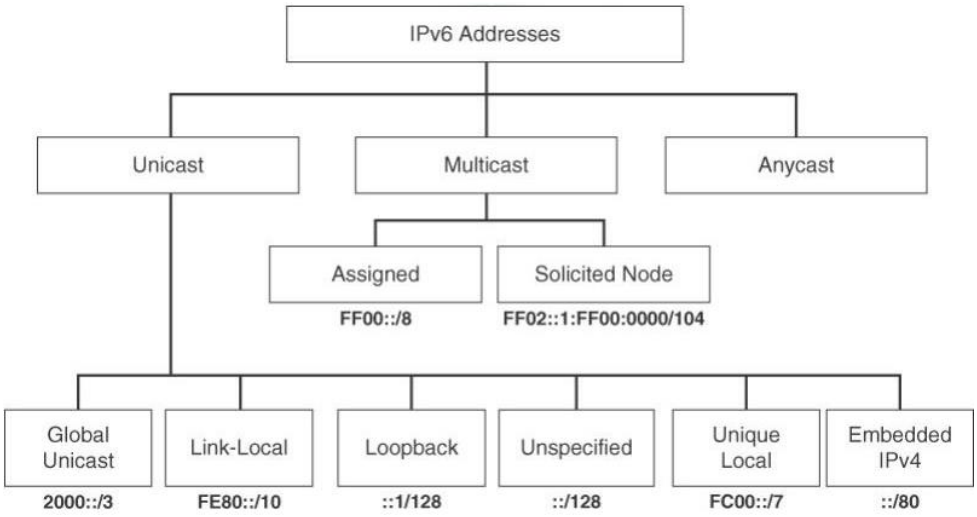
- **Formato hexadecimal con dos puntos:** Es el formato más representativo donde se muestra todos los ocho octetos completos. Cada octeto hexadecimal es separado mediante dos puntos. Por ejemplo, una dirección IPv6 de forma completa se representa como: FF02:0000:0000:abcd:0000:0000:0000:0001.
- **Formato comprimido:** Básicamente se realiza una reducción de ceros más significativos de cada grupo de 4 dígitos hexadecimales. Cuando una dirección IP contiene largas cadenas de ceros estos pueden ser reemplazados por dos características seguidas de dos puntos (::) (Castro & Raez, 2023).

Por ejemplo, la dirección IPv6 FF02:0000:0000:abcd:0000:0000:0000:0001 puede ser comprimida a FF02:0:0:abcd::1. Tomando en cuenta que el segundo y tercer octeto se reduce a un cero significativo y del quinto octeto al séptimo octeto se reemplaza por el símbolo de dos puntos consecutivos (::).

1.2.4. Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6 las mismas que están descritas en la Figura 4. Las direcciones Unicast, Multicast y Anycast. En esta versión de protocolo de internet se elimina las direcciones de broadcast(Saade et al., 2020).

Figura 4. Clasificación de direcciones IPv6



Fuente: (Saade et al., 2020)

1.2.4.1. Direcciones Unicast

Unicast es el concepto más común de la comunicación entre host. Se refiere a que en una transmisión de paquetes de información se tendrá a un emisor y a un receptor para enviar y recibir la información. Este tipo de direccionamientos está asociada a una única interfaz de host (Paucar & Jativa, 2022). Dentro de las direcciones Unicast las más destacables son las globales y las de enlace local.

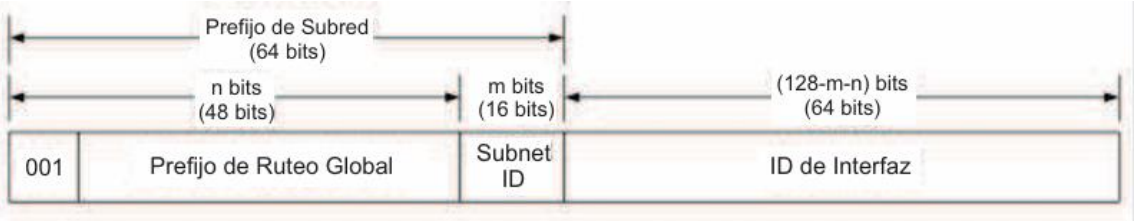
- **Direcciones Unicast Globales**

  Estas direcciones son globalmente alcanzables a internet, es decir que equivalen a las direcciones IPv4 públicas. Lo que hace distintivo de estas direcciones es que sus tres

primeros bits tiene el valor de 001 (rango del primer hexteto de 2000 a 3FFF) como se puede evidenciar en la Figura 5.

La primera porción de la dirección es denominada prefijo del ruteo global. Este prefijo es el identificador de la red y es otorgada por un Carrier o por un ISP y su tamaño es de 48 bits. Seguidamente se tiene el campo Subnet ID que es el identificador de red que consta de 16 bits. El prefijo de ruteo global y el Subnet ID componen el prefijo de subred, estos dos campos constituyen la longitud del prefijo de red. Finalmente, se tiene el campo ID de Interfaz equivalente a la dirección del nodo(Saade et al., 2020).

Figura 5. Formato de la IP Unicast global.



Fuente:(Saade et al., 2020)

Para determinar el campo ID de interfaz del formato de la IP Unicast global se utiliza un esquema de direccionamiento automático para la generación del ID de Interfaz.

Las direcciones IPv6 Unicast globales pueden configurarse de forma automática de las cuales existe dos métodos: Autoconfiguración de direcciones sin estado (SLAAC) y la DHCPv6 (Sánchez et al., 2024).

Con el direccionamiento IPv6 los nodos privados tienen configurado una dirección Unicast global. Los dispositivos privados son accesibles desde la red pública es decir no existe el concepto de direcciones públicas y privadas.

- **Direcciones Únicas de enlace Local**

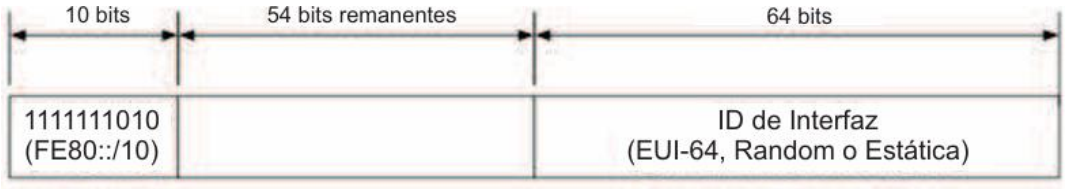
  Son direcciones unicast confinadas a un único enlace o subred, es decir, un paquete que posee una dirección de este tipo como dirección destino, no puede atravesar un router. Estas direcciones se crean automáticamente cuando se habilita el protocolo IPv6 en una interfaz (Saade et al., 2020).

  El formato de esta dirección IPv6 unicast de enlace local se puede observar en la Figura 6. El primer prefijo de 10 bits siempre comienza con FE80::/10 es la única

dirección que utilizan los dispositivos para comunicarse dentro del mismo enlace de la red. El segundo campo de 54 bits es de reserva para usos futuros y el último campo de ID de interfaz identifica de forma única la interfaz de la red y se genera mediante 3 formas:

- EUI-64 basado en la direcciona MAC.
- Random de forma aleatoria para mayor privacidad.
- Estática la cual es configurada manualmente por el administrador.

Figura 6. Formato de dirección únicas de enlace local



Fuente: (Saade et al., 2020)

1.2.4.2. Direcciones Multicast

La dirección multicast es un mecanismo de direccionamiento y difusión de paquetes. Permite que un dispositivo envié un único paquete a múltiples receptores. El formato de la dirección multicast se puede evidenciar en la Figura 7. La misma empieza con el prefijo FF::/8, luego sigue el campo del flag, de cuatro bits, que indica el tipo de direccionamiento multicast. Este tipo de dirección depende del valor que se asigne al flag y se dividen en:

- **Direcciones multicast permanentes**
  Estas direcciones son cuando el valor del flag sea 0. Estas son direcciones públicas, asignadas por la IANA.
- **Direcciones multicast transitorias o dinámicas**
  Estas direcciones son cuando el valor de flag sea 1. Estas direcciones son asignadas por aplicaciones a medida que se van creando los grupos de multidifusión.

A continuación del flag se encuentra el campo de ámbito la cual consta de cuatro bits. Este campo indica el rango de cobertura del paquete multicast. De esta forma se reemplazan los broadcast, generándose un paquete multicast dirigidos a todos los nodos de la red. Finalmente está el campo identificador del grupo de multidifusión que consta

de 112 bits de longitud así completando todo el campo del direccionamiento multicast de 128 bits como se muestra en la Figura 7.

Figura 7. Formato de direccionamiento multicast

Fuente: (Saade et al., 2020)

1.2.4.3. Direcciones Anycast

La dirección Anycast se asigna a un grupo de interfaces, generalmente ubicadas en distintos nodos de la red. Cuando un paquete se envía a una dirección Anycast, este no se entrega a todas las interfaces, sino únicamente a la que este más próximo al origen, según lo determinen las métricas de enrutamiento. En la práctica, el host envía el paquete hacia la dirección Anycast y la red se encarga de dirigirlo a la interfaz más cercana disponible (Novoa, 2022).

Las direcciones Anycast son utilizadas generalmente para:

- Balanceo de carga
- Localizar routers que provee acceso a una subred
- Redes con soporte para movilidad IPv6 para localizar los agentes de origen.

1.2.5. Comparación IPv4 vs IPv6

En la Tabla 1, se detalla el resumen de las principales diferencias entre los protocolos de internet v4 y v6. Mencionando así que estos protocolos no son compatibles, la subsistencia de estos protocoles en la red depende del mecanismo de traducción la cual permite convertir paquetes y la forma de operación a cada uno de estos (Loid Garcia et al., 2022).

Tabla 1. Comparación entre ambos protocolos

Características	IPv4	IPv6
Año de desarrollo	1981	1998
Número de direcciones	2^{32}	2^{128}
Tamaño de direcciones	32 bits	128 bits
Formato de direccionamiento	Decimales separados por puntos, 4 grupos de 8 bits.	Hexadecimales separados por dos puntos, 8 grupos de 16 bits
Autoconfiguración	No posee	Los nodos IPv6 pueden configurarse ellos mismos automáticamente una vez conectada a la red ruteada en IPv6
Notación	192.168.0.0/24	4AB8:F822:AC7F::/48
Velocidad de transferencia	Menor	Mayor
Cheksum	Si	No
Seguridad	Opcional	A través del soporte nativo para IPSec.
QoS	Mejora la identificación de calidad de servicio	Sin identificación de QoS
Tamaño de paquete	Admite un tamaño de 576 bytes	Admite un tamaño de 1280 bytes
Configuración	Manual	Automática

Fuente: (Esteban et al., 2020)

Los protocolos de internet presentan diferencias significativas que desempeñan un papel fundamental en la habilitación de la comunicación y las transmisiones de datos. IPv4 es

ampliamente utilizada durante varias décadas; sin embargo, tiene limitaciones en cuanto a espacio de direccionamiento y características de seguridad. Por otra parte, IPv6 es un protocolo más reciente que ofrece mucho más espacio de direccionamiento y seguridad (Ashraf et al., 2023). A medida que la demanda de servicios de internet continúe creciendo, se espera que IPv6 se consolide como el protocolo dominante para las comunicaciones. No obstante, es probable que ambos protocolos coexistan durante muchos años más, debido a la transición gradual (AlEnezi & AlDhamen, 2023).

1.2.6. Mecanismos de transición de IPv4 a IPv6

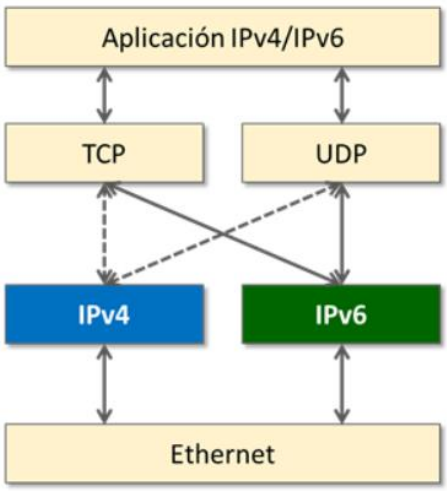
Lo mecanismos de transición demuestran un potencial significativo para facilitar la adopción gradual a IPv6. Entre los mecanismos más utilizados son Dual Stack, Tunelización y Traducción. Estos permiten que la conectividad IPv4 se entregue a través de redes IPv6 permitiendo el acceso a continuo a los recuerdos de la red (Al-Azzawi & Lencse, 2024).

1.2.6.1. Dual Stack

La transición mediante el mecanismo doble pila consiste en la operabilidad de forma simultánea de IPv4 al protocolo IPv6. Cada protocolo de enrutamiento debe llevar los prefijos correspondientes a cada tecnología de forma transparente para el usuario. Es la técnica de transición más utilizada, ya que es fácil de implementar y es compatible con la mayoría de los sistemas operativos. En Dual Stock, los protocolos IPv4 e IPv6 funcionan en paralelo; sin embargo, la red IPv6 se implementa sobre una red IPv4 existente. Este método es común para empresas que buscan convertir gradualmente sus dispositivos IPv4 existentes a IPv6.

La estructura del Dual Stack se muestra en la Figura 8. En este esquema se observa cómo una aplicación con soporte IPv4/IPv6 pueden comunicarse a través de los protocolos de transporte TCP y UDP, la cuales interactúan de manera independiente tanto con IPv4 como con IPv6. Ambos protocolos de red funcionan en paralelo sobre la misma capa de enlace. Este mecanismo de transición Dual Stack resuelve la comunicación entre IPv4 e IPv6 de una forma sencilla (Zhang et al., 2024).

Figura 8. Estructura de un nodo funcional en Dual Stack



Fuente: (Huawei, 2024)

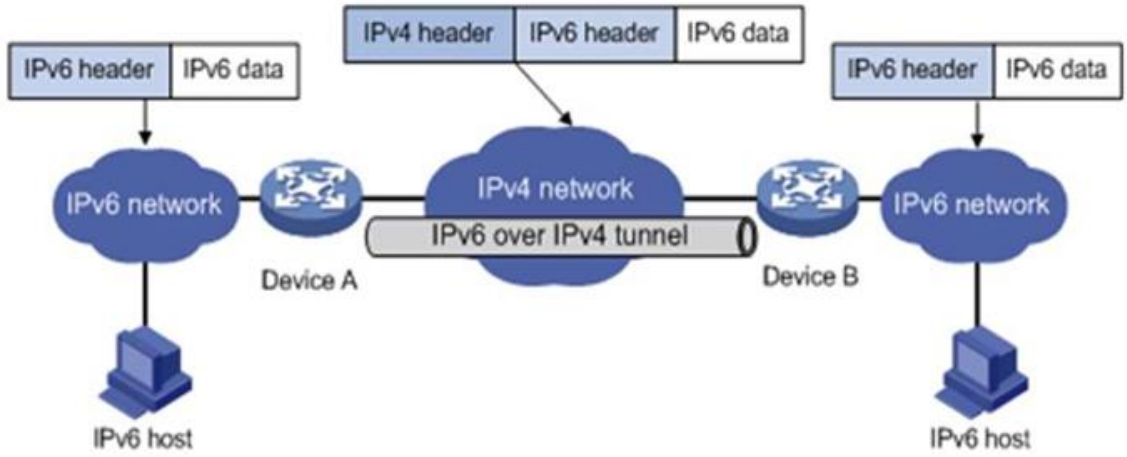
La ventaja de tener este mecanismo de transición habilitada en la central del ISP proporciona buena operabilidad y facilidad de comprensión. Sin embargo, requiere la configuración simultánea de IP para cada dispositivo, lo que es fundamental para garantizar una transición suave y eficiente hacia IPv6.

1.2.6.2. Tunelización

En la transición mediante túneles, estos permiten enviar paquetes IPv6 dentro de IPv4 y viceversa. Por lo general, hoy en día el tráfico IPv6 viaja encapsulado dentro de los paquetes IPv4; de esta forma se permite atravesar redes IPv4 existentes. Los túneles más comunes son túneles manuales y túneles automáticos. Los túneles manuales se deben configurar explícitamente en algún equipo de red mientras que los automáticos se configuran automáticamente en algunos sistemas operativos (Khadiri et al., 2023).

Los túneles manuales se configuran de manera estática entre dos extremos del túnel, lo que asegura control y estabilidad en la comunicación. Este mecanismo se utiliza para las conexiones entre sitios IPv6 separados por una red IPv4 como muestra la Figura 9.

Figura 9. Tunelización manual



Fuente: (Khadiri et al., 2023)

1.2.6.3. Traducción de direcciones

Es un mecanismo de transición que convierte los encabezados de los paquetes IPv6 en encabezado IPv4 y viceversa. Una puerta de enlace, conmutador o enrutador ya sea de software o hardware, puede actuar como un elemento de difusión. El método de traducción más conocido es NAT64, que permite que dispositivos IPv6 funcionen con dispositivos IPv4. Sin embargo, este esquema tiene una característica, la cual tiene una necesidad de compatibilidad adicional con el sistema de nombre de dominios DNS. Especialmente para este mecanismo de traducción, se desarrolló DNS64, que reemplaza la dirección IPv4 en la respuesta DNS por la dirección IPv6 sintetizada, la cual es comprensible tanto para el cliente como para el traductor del protocolo NAT64 (Ordabayeva et al., 2020).

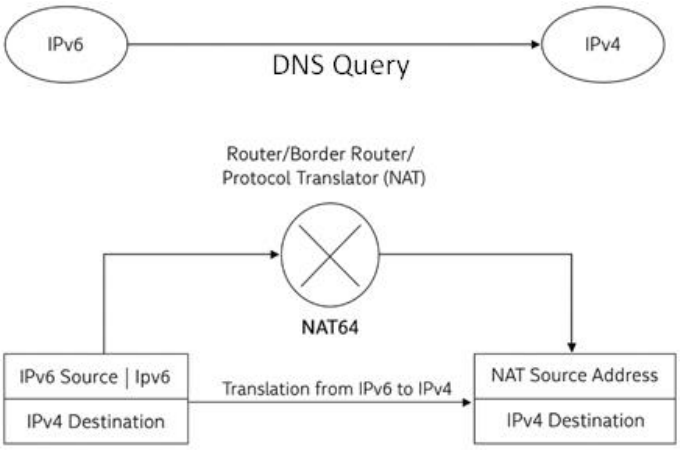
- **NAT64**

NAT64 (Network Address Translation 64) es un componente importante para la implementación de IPv6. Proporciona una traducción de dirección IPv6 y direcciones IPv4, permitiendo que dispositivos con IPv6 se comuniquen con dispositivos que tienen solo IPv4 (Qaid & Ertug, 2021). La implementación de NAT64 es fundamental cuando los usuarios o dispositivos finales cuentan solo soporte de configuración IPv4. NAT64 garantiza accesos a contenidos y servicios que solo están disponibles a través de IPv4.

Este protocolo de transición facilita la coexistencia de ambos protocolos y garantiza la conectividad en entornos mixtos (Cañas, 2023).

Según (Hsu et al., 2024), NAT64 aprovecha las resoluciones de DNS64 para mapear direcciones IPv4 a direcciones IPv6 como se muestra en la Figura 10. El DNS64 se encarga de adaptar registros IPv4 para que los clientes IPv6 puedan acceder a través del NAT64. Hasta la fecha NAT 64 no se ha explorado impuramente en internet ya que si existen por lo general equipos que soporten IPv4 e IPv6 de manera simultánea

Figura 10. Protocolo de transición NAT64 con interacción de DNS64



Fuente: (Cañas, 2023)

El desarrollo del capítulo del marco teórico referencial permite comprender los fundamentos conceptuales y técnicos necesarios para establecer la migración de IPv4 a IPv6. La revisión de los temas planteados proporciona una base sólida que respalda el diseño de la solución planteada. De esta manera, el análisis teórico no solo conceptualiza la importancia de la adopción de IPv6, sino que también justifica las decisiones técnicas consideradas en la propuesta, para garantizar compatibilidad, eficiencia y continuidad en la red de la empresa.

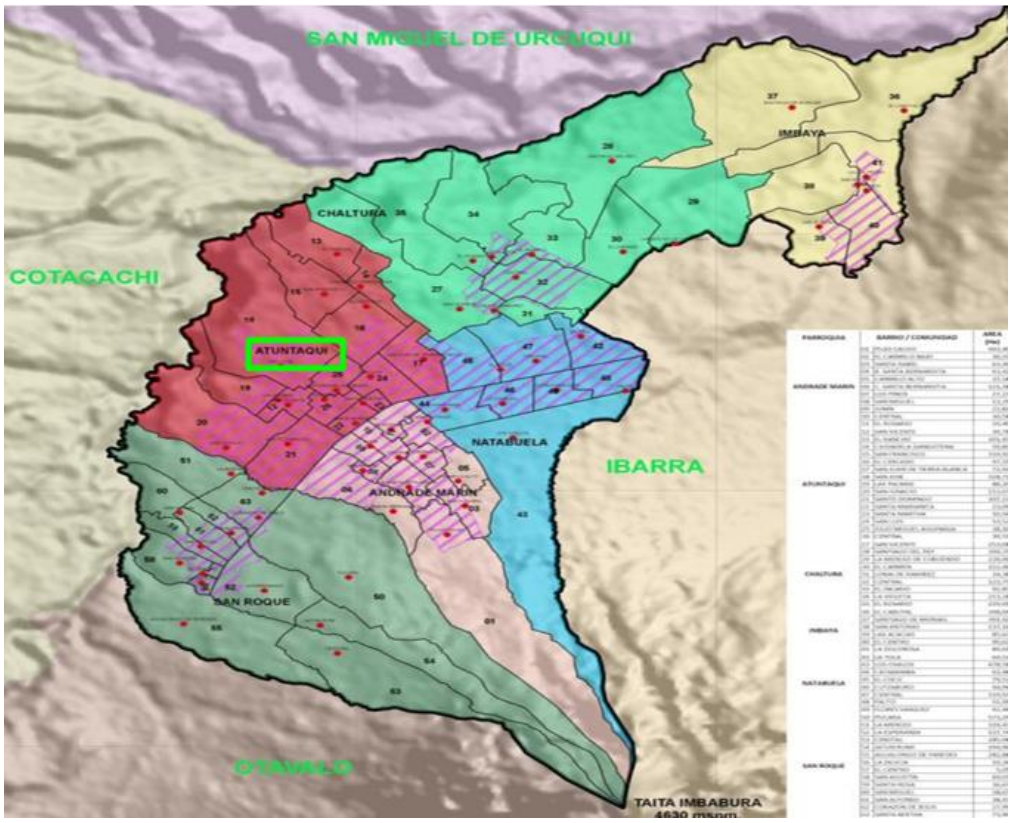
CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

El presente trabajo de investigación está definido a realizar en la empresa INFINIX INTERNET, la misma que brinda servicio de internet en las ciudades de Atuntaqui y Cotacachi, ubicadas en los cantones Antonio Ante y Cotacachi respectivamente, pertenecientes a la provincia de Imbabura.

El cantón Antonio Ante cuenta con seis parroquias, de las cuales dos son urbanas y cuatro rurales, como se muestra en la Figura 11. El primer nodo de telecomunicaciones de la empresa INFNIX INTERNET está situado en Atuntaqui una de las parroquias urbanas y determinada como cabecera cantonal.

Figura 11. Cantón Antonio Ante y sus parroquias



Fuente: (GAD Antonio Ante, 2024)

La infraestructura de telecomunicaciones implementada con tecnología GPON parte desde la cabecera cantonal de Atuntaqui y se extiende hacia las demás parroquias vecinas, tal como muestra la Figura 12. Su ubicación es seleccionada considerando criterios de

accesibilidad, escalabilidad eléctrica y condiciones de seguridad, lo que permite garantizar la operabilidad de la red.

Figura 12. Despliegue de la red desde el nodo Atuntaqui

Fuente: Elaborado por el autor en Google Earth

El rack principal del primer nodo de telecomunicaciones de la empresa INFINIX INTERNET se encuentra instaladas en las coordenadas geográficas 0°19'49.53"N-78°12'50.74"0 y su detalle se presenta en la Tabla 2. Este nodo constituye un punto estratégico dentro de la red, ya que alberga los equipos esenciales para la distribución del servicio a distintos sectores.

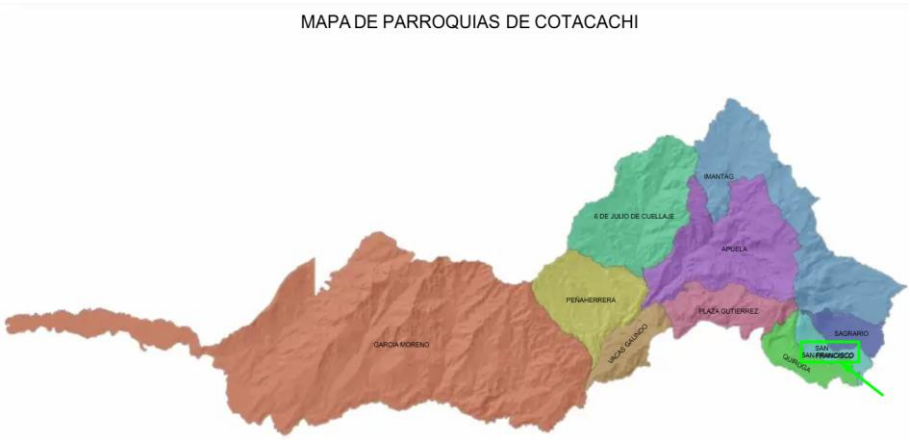
Tabla 2. Detalles de la ubicación del nodo Atuntaqui

ISP INFINIX INTERNET NODO 1	
Provincia	Imbabura
Cantón	Antonio Ante
Parroquia	Atuntaqui
Barrio	Santa Marianita
Dirección	Calle Atahualpa entre Olmedo y Av. Salinas

Fuente: Elaborado por el autor

El cantón Cotacachi cuenta con diez parroquias de las cuales dos son urbanas y ocho rurales como se muestra en la Figura 13. El segundo nodo de telecomunicaciones de la empresa INFNIX INTERNET está situada en parroquia San Francisco ciudad Cotacachi.

Figura 13. Cantón Cotacachi y sus parroquias

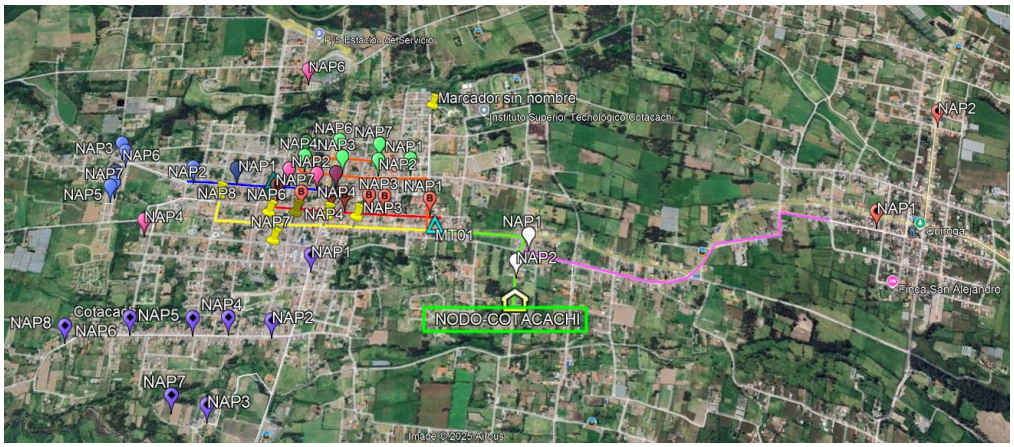


Fuente: (GAD Municipal Santa Ana de Cotacachi, 2023)

La infraestructura de telecomunicaciones del nodo Cotacachi, también está basada en la tecnología GPON. Se encuentra situada en la parroquia San Francisco, desde donde la red se despliega hacia las demás parroquias vecinas, tal como se observa la Figura 14. Este lugar es un punto estratégico, ya que no se trata de zona de alto tránsito, lo que reduce el

riesgo de daños de enlaces troncales, así mismo permite garantizar la operabilidad de la red.

Figura 14. Despliegue de la red desde el nodo Cotacachi



Fuente: Elaborado por el autor en Google Earth

El segundo rack del nodo de telecomunicaciones la empresa INFINIX INTERNET se encuentra instaladas en las coordenadas geográficas 0°17'48.18"N-78°16'31.45"0 y descrita en la Tabla 3. Este nodo constituye un punto clave en la red, al concentrar los equipos de telecomunicaciones que permite la distribución eficiente del servicio a los diferentes sectores del Cantón.

Tabla 3. Detalles de la ubicación del nodo Cotacachi

ISP INFINIX INTERNET NODO 2	
Provincia	Imbabura
Cantón	Cotacachi
Parroquia	San Francisco
Barrio	El Ejido
Dirección	Calle Filemón Proaño y Av. Manuel Larrea

Fuente: Elaborado por el autor

2.2. Diseño y alcance de la investigación

La presente investigación es de carácter experimental y explicativo, ya que integra una revisión bibliográfica del protocolo IPv6 y de los mecanismos de transición existentes, junto a la ejecución de pruebas de configuración en la red con el propósito de comprobar su funcionalidad. La migración planteada se desarrolla mediante una producción controlada, lo que permite implementar el nuevo protocolo IPv6 por fases y garantiza la continuidad de los servicios durante el proceso. Para mantener la compatibilidad con la infraestructura existente, se plantea el uso del mecanismo de transición Dual Stack, que habilita la operación simultánea de IPV4 e IPv6 en la red. De esta forma, los servicios y dispositivos pueden comunicarse utilizando indistintamente cualquiera de los protocolos, asegurando una transición gradual y sin interrupciones de operación.

2.3. Tipo y métodos de investigación

Este proyecto corresponde al tipo de investigación cualitativa, basada en el análisis bibliográfico y documentación del protocolo IPv6 y los mecanismos de transición. Su propósito es comprender sus características y determinar el mecanismo de transición más adecuado para la empresa. En cuanto al método de la investigación, se emplean los enfoques analítico y sintético: analítico, porque permite examinar de manera detallada los aspectos técnicos de los mecanismos de transición. El enfoque sintético, porque se realiza una propuesta de direccionamiento en IPv6 que facilite la transición al nuevo protocolo, garantizando el cumplimiento de los objetivos específicos planteados y así llegar a la solución establecida en el objetivo general.

2.4. Población y muestra

El estudio se ha definido con el objetivo que tiene la empresa INFINIX INTERNET en la migrar hacia un protocolo de internet que garantice la operabilidad con las tendencias tecnológicas actuales. Dicho esto, el administrador y el personal de infraestructura toman una decisión estratégica y responsable para el mejoramiento del ISP. En este contexto, la población de estudio está conformada por toda la infraestructura tecnológica de la empresa.

Para efectos del presente trabajo, se ha considerado como muestra a los equipos de red, así como administrador y al personal de infraestructura responsables del proyecto. El tipo

de muestreo es no probabilístico, ya que se centra en los recursos y actores claves que garanticen la transición de IPv4 a IPv6, contando con el conocimiento teórico y técnico necesario para alcanzar el éxito del proyecto planteado.

2.5. Técnicas e instrumentos de recolección de datos

La recolección de datos se desarrollará mediante la técnica cualitativa, basada en la revisión documental de la literatura científica y técnica relacionados con la migración de IPv4 a IPv6, así como el levantamiento de la información interna del ISP. Esta información permite analizar la situación actual de la infraestructura y estructurar el planteamiento de la red orientada a cubrir la necesidad de transición hacia el protocolo IPv6.

2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información.

La validez de los instrumentos aplicados se garantiza mediante la revisión de literatura especializada en migración de IPv4 a IPv6 y el análisis de las configuraciones de los equipos de red de la infraestructura actual de la empresa INFINIX INTERNET. De esta manera, se asegura que la información recopilada este directamente relacionado con los objetivos del estudio y permita evaluar de forma correcta la infraestructura tecnológica y el proceso de transición.

La confiabilidad se respalda a través de la verificación cruzada de los datos obtenidos en el análisis documental, las configuraciones de los equipos de red y el plan de direccionamiento vigente. Este procedimiento asegura resultados adecuados para identificar falencias en la red y sustentar la propuesta de transición a IPv6.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

En este capítulo se presentan los resultados y la discusión a partir de tres secciones principales: el diagnóstico de la infraestructura de red, donde se realiza un levantamiento técnico sobre los equipos activos, esquema de direccionamiento actual y capacidad de ancho de banda. La segunda sección en donde se determina la elección del mecanismo de transición, la misma que debe garantizar la compatibilidad entre ambos protocolos y finalmente, se define un plan de direccionamiento IPv6 que asegure escalabilidad, eficiencia y una migración ordenada y funcional para el ISP.

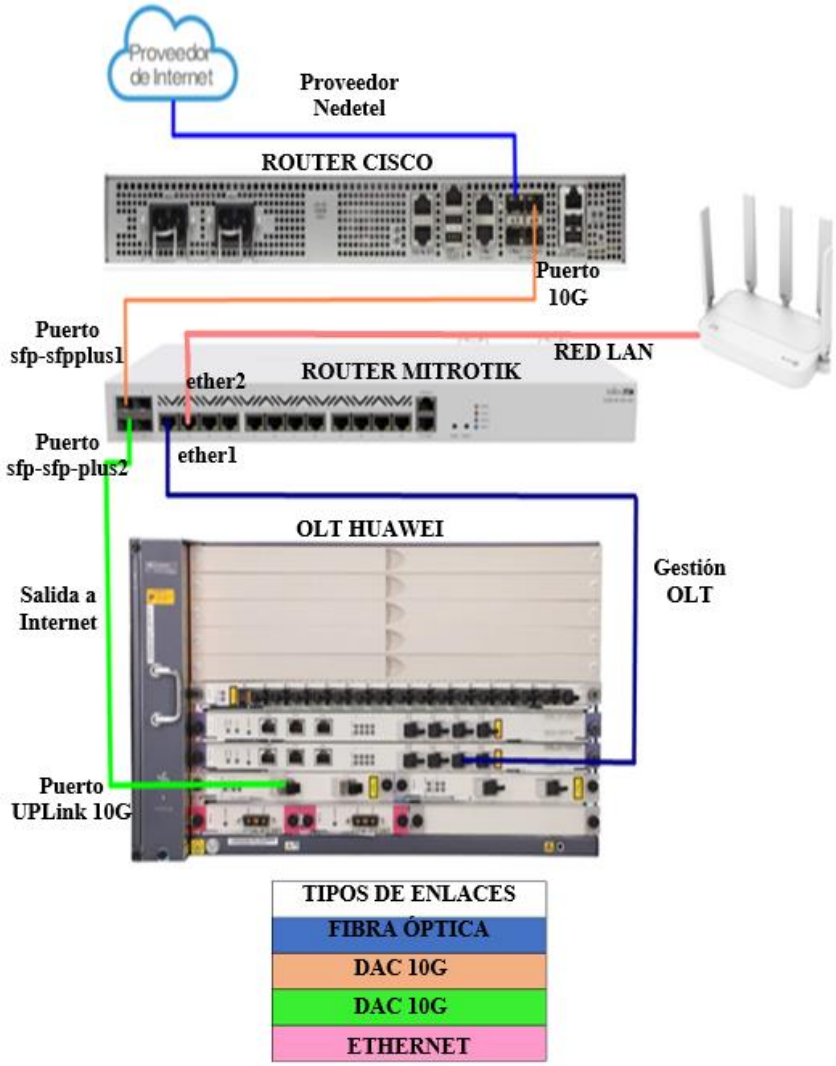
3.1. Diagnóstico y análisis de la infraestructura de la red actual

En esta sección se describe la situación actual de la empresa INFINIX INTERNET de los nodos de la ciudad de Atuntaqui y Cotacachi. Se tiene en cuenta el estado y las características de los diferentes equipos de red utilizados con la finalidad de obtener un diagnóstico real de las configuraciones y recursos en las respectivas infraestructuras de red.

3.1.1. Descripción de la red Atuntaqui

Para llevar a cabo la descripción de la red, es necesario conocer la infraestructura física, como también las conexiones de los equipos y demás componentes de red que conforman el nodo de telecomunicaciones. La Figura 15 detalla la infraestructura física del nodo Atuntaqui, la misma que está conformada por un router de marca Cisco, un router de marca MikroTik, un router destinado a la gestión de la red interna del nodo y una OLT de marca Huawei. El router Cisco permite tener salida a internet; este equipo pertenece a la empresa NEDETEL, la que brinda el servicio de Carrier. El router MikroTik es el equipo de administración utilizado para brindar el acceso a la red a los usuarios. Finalmente, se tiene una OLT de la marca Huawei, la misma que administra y distribuye la potencia óptica a toda la red GPON.

Figura 15. Topología física del nodo Atuntaqui



Fuente: Elaborado por el autor

La información de los equipos de telecomunicaciones, las características y función de cada uno de estos se detalla en la Tabla 4. Estos equipos brindan acceso a internet a 230 usuarios activos mediante la red de fibra óptica distribuida en el cantón Antonio Ante en las parroquias de Atuntaqui, Andrade Marín y Natabuela. Cada uno de los equipos activos cumple un rol esencial en la infraestructura de telecomunicaciones, permitiendo la administración del tráfico de datos. Su correcta integración asegura que los usuarios cuenten con una conectividad hacia internet.

Tabla 4. Descripción general de los equipos del nodo Atuntaqui

Equipo	Descripción	Marca	Modelo y año de fabricación
Router proveedor	NEDETEL-Carrier contratado	CISCO	ASR-920-4SZ-A Año: 2014
Router de administración	Gestiona todo el tráfico y los usuarios de la red.	Mikrotik	CCR2116-12G-4S+ Año: 2021
OLT	Es el dispositivo de concentración para múltiples conexiones de fibra óptica y administra todas las ONTs que está operando mediante la tecnología GPON	Huawei	MA5683T Año: 2015

Fuente: Elaborado por el autor

3.1.1.1. Descripción técnica del router de administración Mikrotik CCR2116-12G-4S+

Mikrotik es un enrutador de alto rendimiento, ideal para grandes proyectos de telecomunicaciones y proveedores de servicios de internet. El modelo CCR2116 está impulsado por una CPU (Unidad Central de Procesamiento) de 16 núcleos AL73400 funcionando a 2GHz, lo que destacan en el procesamiento de paquetes siendo la elección óptima para las aplicaciones de última milla. Este equipo está equipado con cuatro puertos 10G SFP+ y doce puertos Gigabit Ethernet, como se puede evidenciar en la Figura 16. Esta versión cuenta con una memoria RAM (Memoria de Acceso Aleatorio) de 16GB DDR4 lo que asegura una capacidad de procesamiento robusta. Además, cuenta con una ranura M.2 integrada para almacenamiento adicional de hasta 1TB. Su capacidad de operar bajo condiciones intensas y manejar múltiples tareas de red lo convierte en un equipo versátil y de alto rendimiento para infraestructuras de red (MikroTik, 2023).

Figura 16. Mikrotik CCR2116-12G-4s+

Fuente: (MikroTik, 2023)

En la Tabla 5 se detallan las especificaciones técnicas del equipo, que constituye una parte esencial y de alto rendimiento para los servicios de telecomunicaciones.

Tabla 5. Especificaciones técnicas del equipo Mikrotik CCR2116-12G-4s+

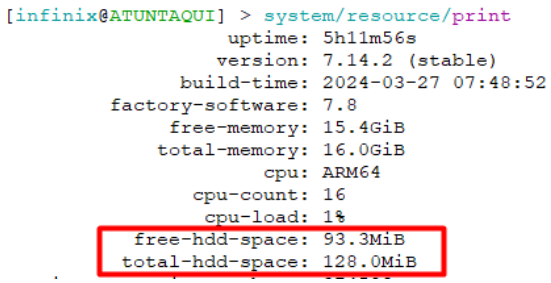
Producto	**CCR2116-12G-4S**
Arquitectura	ARM 64bit
CPU	AL73400
Núcleos	16
Frecuencia de CPU	2000 MHZ
Licencia de RouterOS	6
Sistema operativo	RouterOS v7
Compatibilidad IPv6	Si
RAM	16 GB DDR4
Almacenamiento	128 MB
Puertos SFP+	4 puertos SFP+ 10G
Puertos Ethernet	12 puertos Gigabit Ethernet
Puerto USB	1* USB 3.0 tipo A
Consumo eléctrico	65W
Refrigeración	Ventiladores integrados

Fuente:(MikroTik, 2023)

3.1.1.2. Recursos consumidos del router Mikrotik CCR2116-12G-4s+

El análisis del rendimiento actual de la red de cada dispositivo nos ayuda a determinar las características reales de operación. En la Figura 17, se comprueba el valor del almacenamiento total de 128.0 MiB expresado en megabytes y el espacio libre que queda es de 93.3MiB.

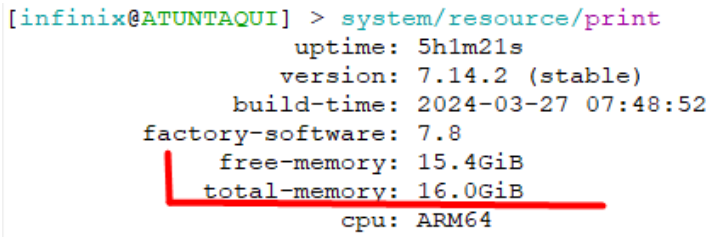
Figura 17. Almacenamiento interno del Mikrotik CCR2116-12G-4s+



Fuente: Equipo de administración de INFINIX INTERNET

La Figura 18 muestra el consumo de la memoria del equipo. Aquí se detalla todos los procesos que está ejecutando en el router MikroTik, incluyendo las configuraciones de cada interfaz y las reglas del firewall que se utiliza como seguridad para la red. El equipo tiene 16.0 gigabytes de memoria total. De esos, el 15.5 gigabytes están libres tal que significa que se está utilizando alrededor de 0.6 gigabyte es decir un 3.75% de la memoria total. Esto garantiza que es posible realizar más configuraciones sin presentar inconvenientes en su funcionamiento.

Figura 18. Memoria interna del Mikrotik CCR2116-12G-4s+



Fuente: Equipo de administración de INFINIX INTERNET

En la Figura 19 se observa que el uso actual del CPU es del 4%, valor. Este porcentaje refleja que el router apenas está utilizando una mínima fracción de su capacidad de procesamiento, manteniendo un 96% de recursos disponibles lo que garantiza un margen

suficiente para soportar configuraciones adicionales. De acuerdo con las buenas prácticas de operación en equipos de telecomunicaciones, un uso promedio de CPU debe estar por debajo del 60%; por tanto, los valores observados en la red de INFINIX INTERNET demuestra una utilización eficiente de los recursos y una amplia capacidad de crecimiento.

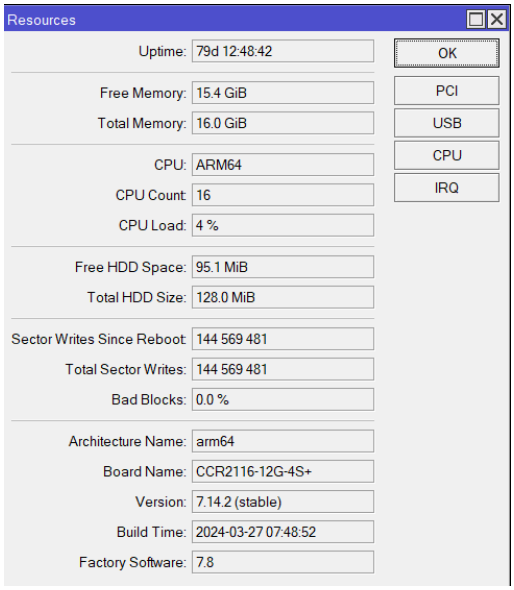
Figura 19. Estado del CPU del Mikrotik CCR2116-12G-4s+

```
[infinix@ATUNTAQUI] > system/resource/monitor
          cpu-used: 4%
  cpu-used-per-cpu: 12%,0%,4%,1%,5%,1%,5%,2%,6%,5%,10%,3%,9%,1%,7%,2%
```

Fuente: Equipo de administración de INFINIX INTERNET

Los equipos Mikrotik permiten ver sus recursos en una interfaz gráfica, así se puede observar el uso de los recursos del equipo en tiempo real. En la Figura 20 se puede ver que el uso del CPU en tiempo real es del 4%, el espacio de memoria disponible es de 15.4 GiB y 95.1 MiB de almacenamiento libre.

Figura 20. Recursos generales del CCR2116



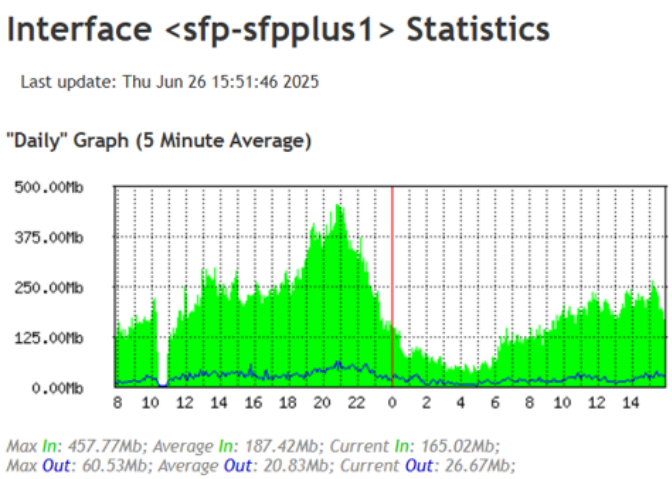
Fuente: Equipo de administración de INFINIX INTERNET

3.1.1.3 Consumo de ancho de banda

El ancho de indica la capacidad de una red para trasferir datos. Actualmente, INFINIX INTERNET tiene un contrato con la empresa Nedetel por un ancho de banda dedicado de 1Gbps. Para conocer el tráfico actual de la red, es necesario acceder a la interfaz web del

router Mikrotik, la cual debe estar previamente habilitada en la opción de servicios. La interfaz web tiene un panel gráfico que muestra el consumo del ancho de banda para cada interfaz física del equipo. En la Figura 21 se evidencia el consumo diario del ancho de banda real utilizado por los clientes en la interfaz física sfp-sfpplus1, determinada como la interfaz WAN. El máximo pico de tráfico es de 457,77 Mbps y el valor promedio es de 187.42 Mbps.

Figura 21. Consumo diario del ancho de banda

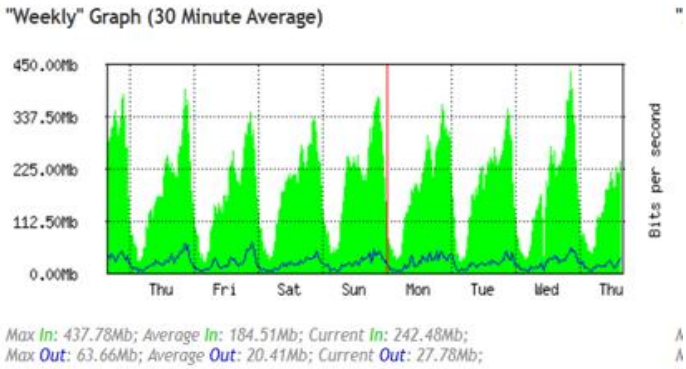


Fuente: Equipo de administración de INFINIX INTERNET

En la Figura 22 se analiza el gráfico del consumo del tráfico en un periodo de tiempo más largo. El patrón de consumo de ancho de banda es casi similar todos los días. En la gráfica de consumo semanal, los picos máximos de uso son de 437.78 Mbps y el consumo promedio por semana es de 184.51 Mbps.

En el gráfico semanal se observa que en el eje X representa los días de la semana, mientras que cada punto corresponde a un promedio de 30 minutos de tráfico. De esta manera, se puede analizar la variación del uso de la red a lo largo de los días, identificando los picos de mayor demanda.

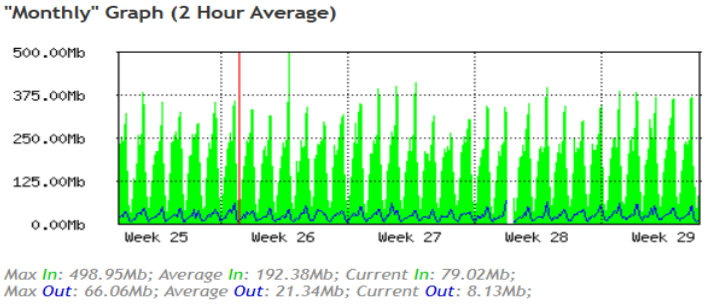
Figura 22. Consumo de ancho de banda semanal



Fuente: Equipo de administración de INFINIX INTERNET

Al igual que en el caso anterior, se puede comprobar el consumo de ancho de banda de manera mensual. Esta información nos ayuda a equilibrar el recurso de ancho de banda y a evitar que la demanda de la red aumente. En la Figura 23, se presenta un consumo mensual de 498.95 Mbps. Este valor inferior al ancho de banda contratado de 1GBps, lo que significa que aproximadamente el 50% de la capacidad permanece disponible. Esta condición no impide planificar el crecimiento y la expansión de la red, si no que representa una oportunidad para anticipar futuras necesidades de capacidad. Contar con un margen disponible del 50% garantiza estabilidad en los recursos y permite responder a picos de tráfico sin afectar el desempeño de la red.

Figura 23. Consumo de ancho de banda mensual



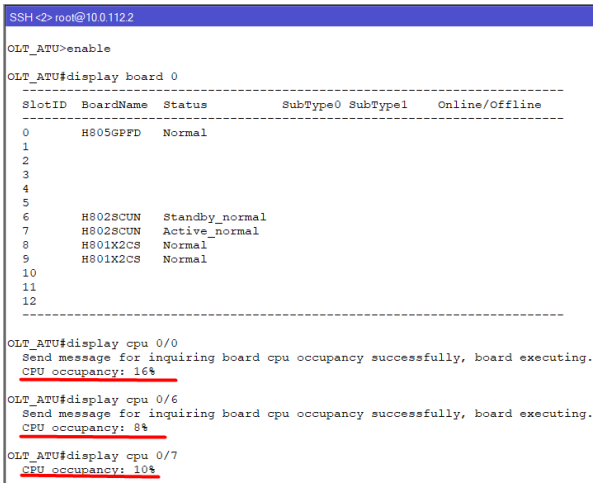
Fuente: Equipo de administración de INFINIX INTERNET

Para determinar los valores de recursos consumidos en la OLT, se realiza la conexión mediante el emulador de telnet. Para esto, se ingresa la dirección IP correspondiente a la gestión de la OLT, como también el correspondiente usuario y contraseña. La Figura 24

muestra los módulos activos y usando el comando *display cpu* más el respectivo número de interfaz para verificar el estado del CPU.

El primer módulo hace énfasis en la tarjeta de servicio GPON. Esta tarjeta soporta 1.25 Gbps de subida y 2.5 Gbps de bajada, la misma tiene un uso del CPU del 16%. El segundo y el tercer módulo que están en las ranuras 0/6 y 0/7 respectivamente son las tarjetas de control y conmutación. Estas tarjetas gestionan el control de la OLT y tiene un consumo del CPU del 8% y 10 % respectivamente.

Figura 24. Consumo del CPU de los módulos activos de la OLT

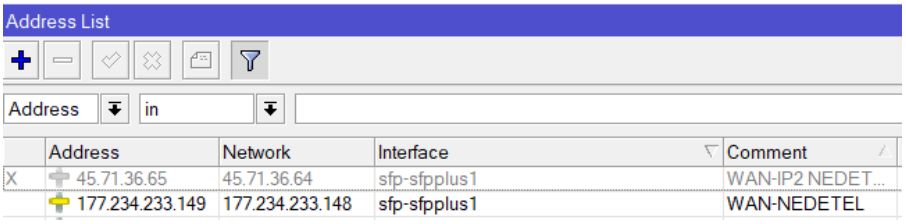


Fuente: Equipo de administración de INFINIX INTERNET

3.1.1.4. Direccionamiento IPv4 actual del Atuntaqui

La infraestructura de la red cuenta con un direccionamiento IPv4. El acceso a internet se realiza a través de dos direcciones IPs públicas asignadas por el proveedor NEDETEL. Estas direcciones están configuradas en el router de administración, específicamente en la interfaz física sfp-sfpplus1, como se muestra en la Figura 25.

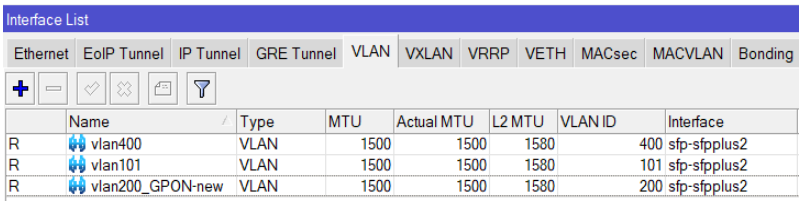
Figura 25. IPs públicas asignadas al nodo Atuntaqui



Fuente: Equipo de administración de INFINIX INTERNET

Para que los usuarios puedan acceder a la red, se tiene creadas tres redes virtuales como se puede evidenciar en la Figura 26. Estas redes virtuales ayudan a dividir el tráfico de los usuarios en la interfaz sfp-sfpplus2 del router Mikrotik. Cada VLAN (Red de Área Local Virtual) es una red distinta que cuenta con su propio direccionamiento IP. La VLAN 101 es para los clientes que se conectan mediante el protocolo DHCP, y las VLANs 200 y 400 son para clientes que tienen acceso mediante el protocolo PPPoE.

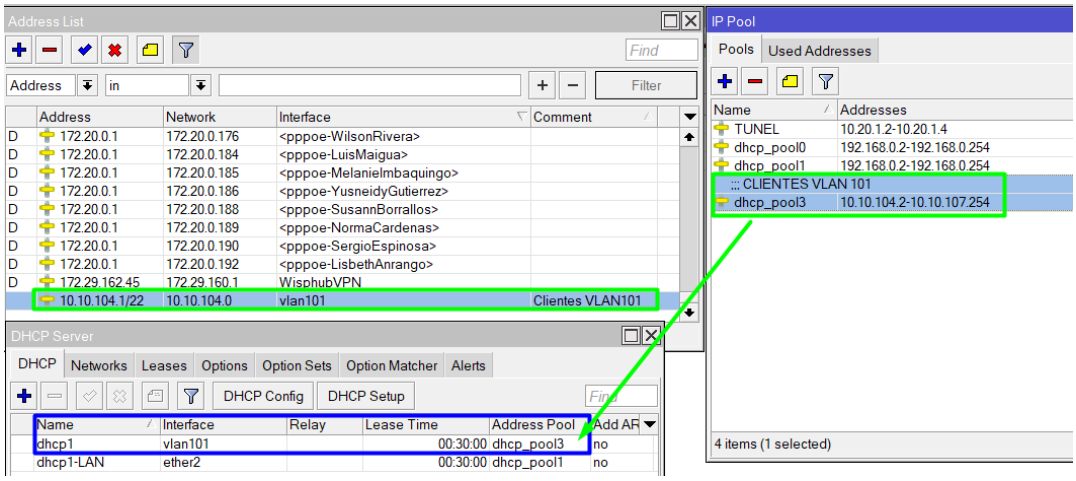
Figura 26. VLANs de acceso para los usuarios



Fuente: Equipos de administración de INFINIX INTERNET

La VLAN 101 está determinada mediante el protocolo de red DCHP la cual brinda direcciones IPs dinámicas a varios clientes. Esto significa que un servidor DHCP envía los parámetros de configuraciones específicas para cada cliente que se conecta a la red. Entre estos parámetros se encuentra la dirección IP del cliente. La dirección IP de la interfaz virtual 101 es la 10.10.104.1/22, como muestra en la Figura 27. Mediante esta dirección IP se puede tener hasta 1022 usuarios. El rango de direcciones IP se gestiona mediante en el servidor DCHP por el pool de direccionamiento (dhcp_pool3) que va desde la dirección 10.10.104.2 al 10.10.107.254. Con esta información, se evidencia notablemente que dicho direccionamiento IP esta sobredimensionado. En una VLAN es recomendable administrar hasta 254 usuarios por el tema de rendimiento de la red, si sobrepasa dicha cantidad de usuarios se genera mucho tráfico de broadcast, lo que puede saturar la red.

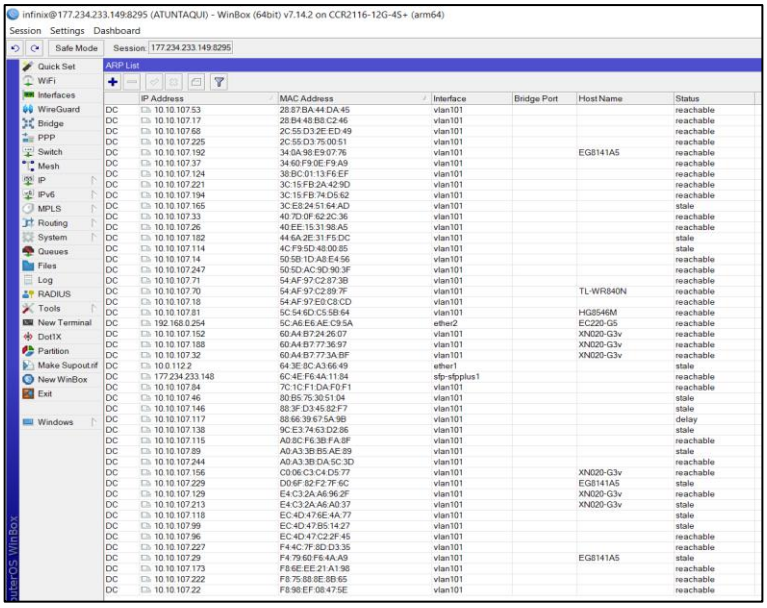
Figura 27. Direccionamiento IP de la VLAN 101



Fuente: Equipos de administración de INFINIX INTERNET

La Figura 28, muestra la sección de ARP del router Mikrotik. En este bloque, se puede ver la tabla de ARP, que muestra todas las direcciones IP de los clientes registrados en el servidor DHCP. Estas direcciones IP están asociados a la MAC Address de los equipos finales de cada cliente. Todas estas direcciones IPs están operativas mediante la VLAN 101.

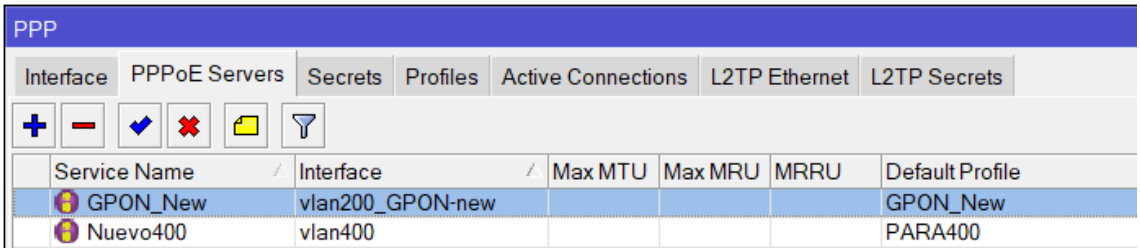
Figura 28. Lista ARP con su respectiva MAC Address



Fuente: Equipos de administración de INFINIX INTERNET

El direccionamiento IP de las VLAN 200 y 4000 como se puede observar en la Figura 29, se obtiene usando el servidor de autenticación PPPoE. Este sistema se utiliza para verificar y autenticar a los usuarios que puedan tener acceso a internet a través de una base local creada en el Mikrotik.

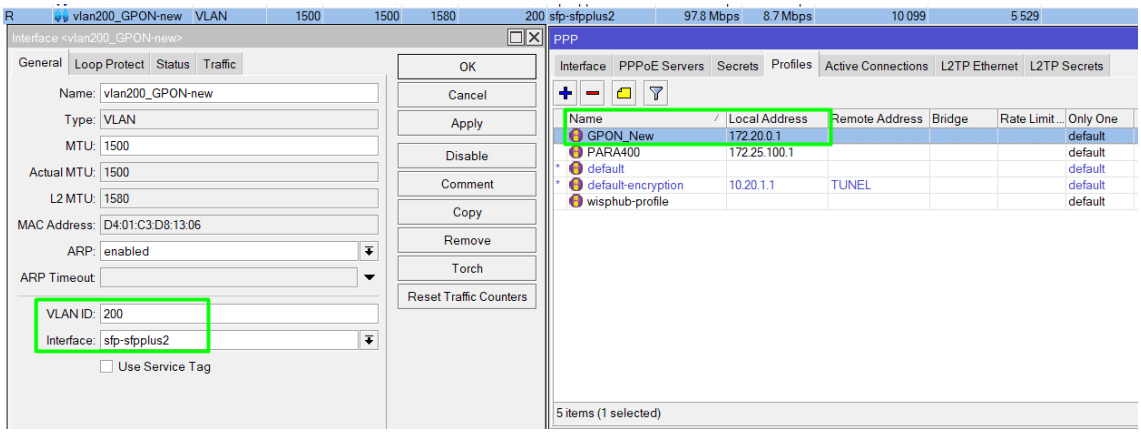
Figura 29. Servidor PPPoE



Fuente: Equipos de administración de INFINIX INTERNET

La VLAN 200 es asociada a la interfaz física sfp-sfpplus2 del router Mikrotik. El nombre es vlan200_GPONnew y en el servidor PPP se crea una profile llamado GPON_New como se muestra en la Figura 30. Se asocia una dirección local 172.20.0.1 sin delimitación de ancho de banda. La gestión del ancho de banda se lo realiza en el Simple Queues.

Figura 30. Interfaz PPPoE para VLAN 200

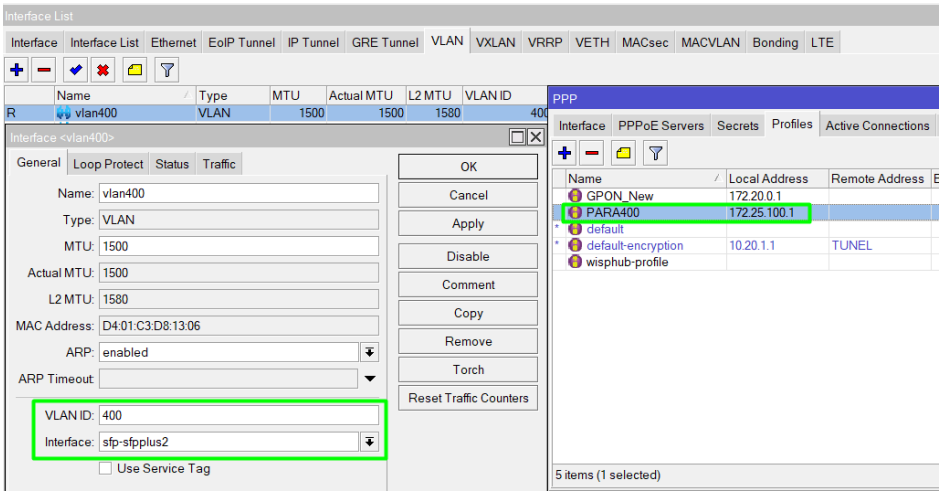


Fuente: Equipos de administración de INFINIX INTERNET

De la misma forma, la VLAN 400 está asociada a la misma interfaz física sfp-sfpplus2 del router de administración. Tiene el nombre vlan400 y en el servidor PPP, hay un profile

con el nombre PARA400, que está asociada a la dirección IP local 172.25.100.1 sin límite de ancho de banda como se muestra en la Figura 31.

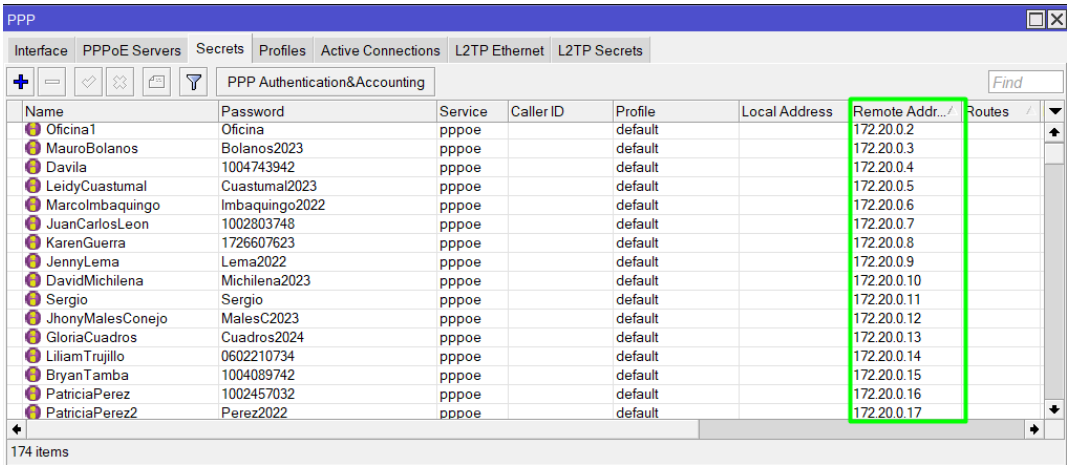
Figura 31. Interfaz PPPoE para VLAN 400



Fuente: Equipos de administración de INFINIX INTERNET

Cada usuario se autenticará de forma individual mediante su nombre y la contraseña establecida en el directorio de Secrets tal cual se evidencia en la Figura 32. También se asigna la dirección IP en el apartado de Remote Adress. Toda esta configuración se lleva a cabo de manera manual en la plataforma Winbox del router de administración.

Figura 32. Usuarios y contraseñas para la autenticación PPPoE

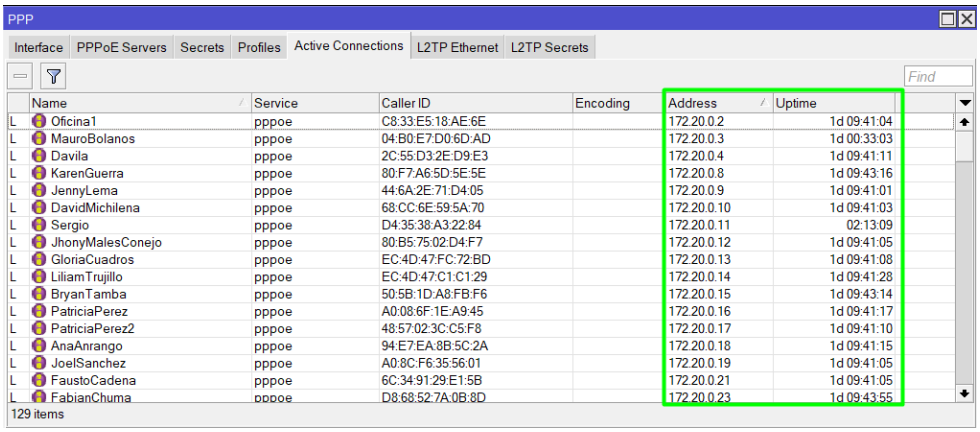


Fuente: Equipos de administración de INFINIX INTERNET

En la sección PPP de conexiones activas del respectivo router de administración, se pueden ver las conexiones de los usuarios a la red a través del protocolo PPPOE. En la

Figura 33 se muestra información como el usuario, la dirección IP y el tiempo que ha estado en línea desde que se autenticó.

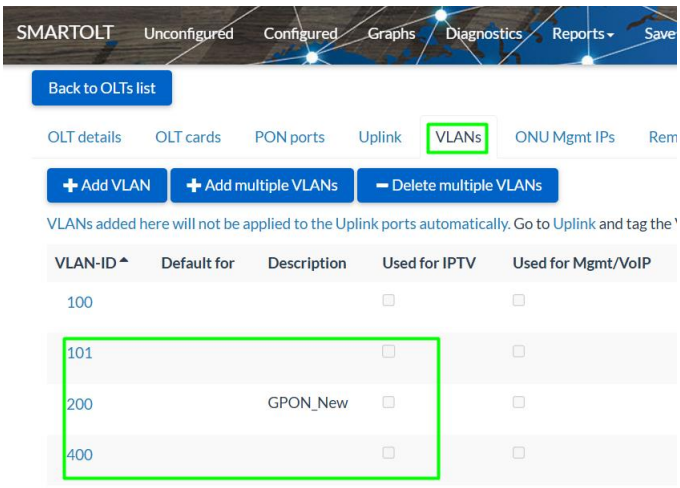
Figura 33. Conexiones activas mediante el protocolo PPPoE



Fuente: Equipos de administración de INFINIX INTERNET

La OLT es administrada mediante el software SMARTOLT. En este software se puede apreciar que se han configurado tres VLANs tal como muestra la Figura 34, de esta manera se tiene por separada el tráfico de múltiples usuarios en cada una de su red virtual.

Figura 34. VLANs configuradas en la OLT

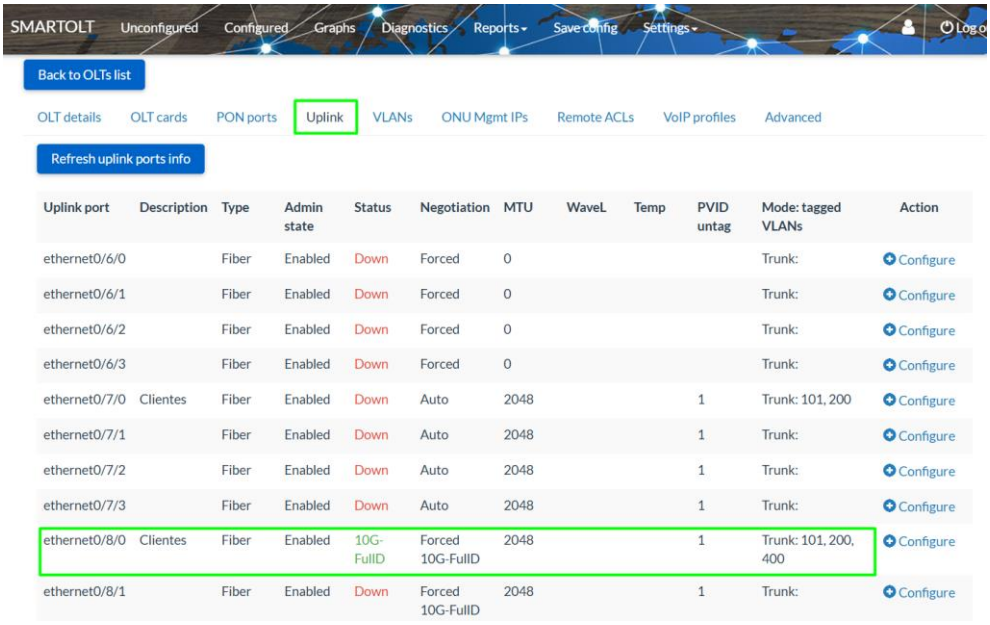


Fuente: Software de administración de la OLT

La tarjeta UPLink ethernet 0/8/0 se usa para que todos los usuarios tengan acceso a internet. Esta tarjeta tiene una capacidad de transmisión de datos hasta 10G. Como se observa en la Figura 35, en la interfaz de esta tarjeta está configurada un trunk para todas

las interfaces virtuales. El trunk es el enlace que transporta múltiples VLANs a través de un cable DAC, que es la única conexión física entre la OLT hacia el router de administración.

Figura 35. Troncalizacion de VLANs en la interfaz UPLink de la OLT



Fuente: Software de administración de la OLT

En la Tabla 6 se muestra un resumen de todas las direcciones IPv4 que están configuradas en los equipos de telecomunicaciones. Hay 2 IPs públicas y 3 IPs de direccionamiento internas para conexión de clientes una mediante el protocolo DHCP y 2 mediante el protocolo PPPOE. Estas están operativas en la interfaz sfp-sfpplus2 brindando servicio de internet a los usuarios. También hay un direccionamiento IP para la red LAN interna de la oficina central, en la interfaz ether2. Además, hay un direccionamiento IP para gestionar la OLT en el router Mikrotik, que está configurada en la interfaz ether2. Por último, hay una conexión troncal en la interfaz UPLink 10G para dar salida a internet a los usuarios, asociada a las VLANs 101, 200 y 400.

Tabla 6. Direccionamiento IP con su respectiva interfaz asociada

Equipo	Interfaz	Dirección IP	Dirección de red	Prefijo	Descripción
Mikrotik CCR2116	sfp-sfpplus1	45.71.36.65 177.234.233.149	45.71.36.64 177.234.233.148	/32 /32	IPs públicas
	sfp-sfpplus2	**VLAN 101** 10.10.104.1	10.10.104.0	/22	IP designada a los usuarios mediante la VLAN DHCP
		VLAN 200 172.20.0.1 **VLAN 400** 172.20.100.1	172.20.0.0 172.20.100.0		IPs designadas a los usuarios mediante sus respectivas VLAN PPPoE
	ether1	10.0.112.1	10.0.112.0	/30	Gestión OLT
	ether2	192.168.0.1	192.168.0.0	/24	IP para LAN
OLT Huawei	Puerto UPLink 10G	**TRUNK** VLAN 101 VLAN 200 VLAN 400			Troncalización de las VLAN salida hacia internet de los usuarios.

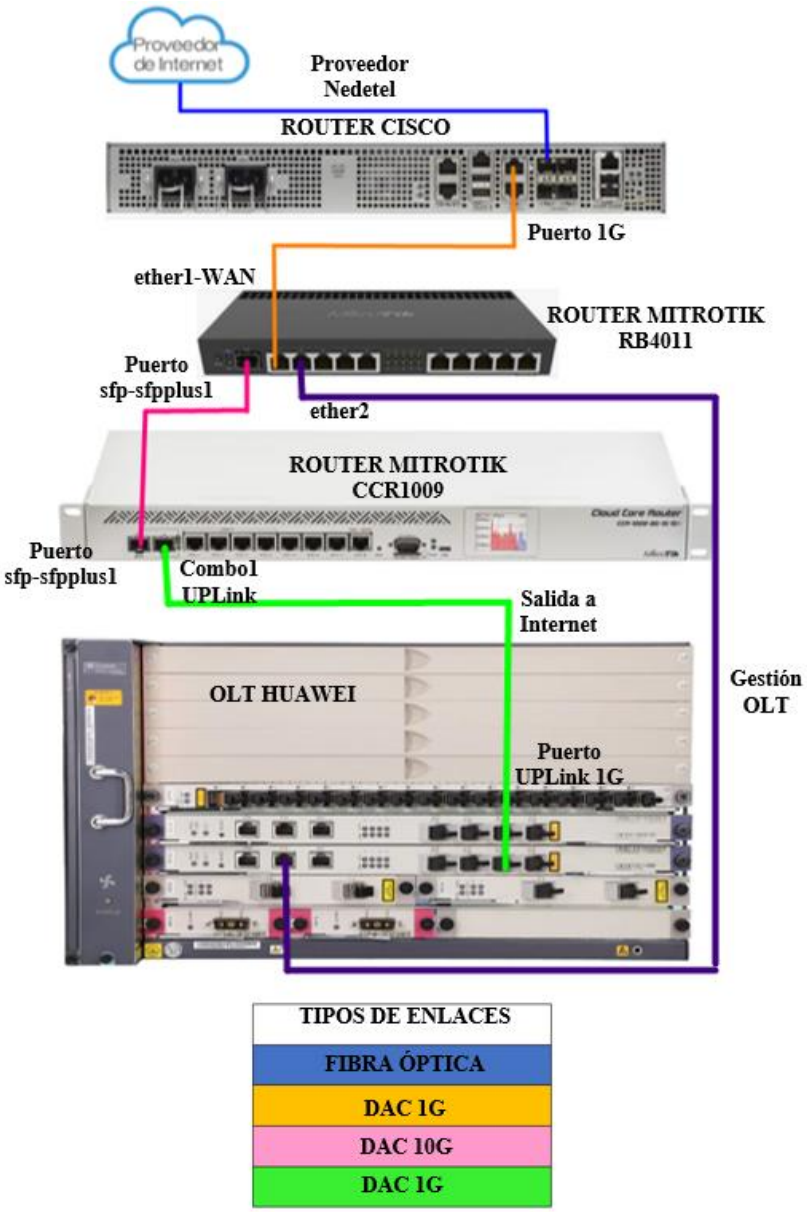
Fuente: Elaborado por el autor

3.1.2. Descripción de la red Cotacachi

Para llevar a cabo la descripción de la red, es necesario conocer la infraestructura física, como también las conexiones de los equipos y demás componentes de red que conforman el nodo de telecomunicaciones. La Figura 36 detalla la infraestructura física del nodo Cotacachi, la misma que está conformada por un router de marca Cisco, dos router de

marca MikroTik y una OLT Huawei. El router Cisco permite tener salida a internet, este equipo pertenece a la empresa NEDETEL, la que brinda el servicio de Carrier. Uno de los routers MikroTik es el equipo de borde y otro de administración utilizado para brindar el acceso a la red a los usuarios. Finalmente, se tiene una OLT de la marca Huawei, la misma que administra y distribuye la potencia óptica a toda la red GPON.

Figura 36. Topología física del nodo Cotacachi



Fuente: Elaborado por el autor

La información de los equipos de telecomunicaciones, las características y función de cada uno de estos se detalla en la Tabla 7. Estos equipos brindan acceso hacia internet a 200 usuarios activos mediante la red de fibra óptica distribuida en el cantón Cotacachi.

Tabla 7. Descripción general de los equipos del nodo Cotacachi

Equipo	Descripción	Marca	Modelo y año de fabricación
Router proveedor	Pertenece a la empresa NEDETEL, Carrier contratado	CISCO	ASR-920-4SZ-A Año: 2014
Router de borde	Gestiona la conexión de la red interna con la red externa de internet	MikroTik	RB4011iGS+RM Año: 2018
Router de Acceso	Gestión de acceso para los usuarios y gestiona el tráfico interno de la red	Mikrotik	CCR1009-7G-1C-1S+ Año: 2016
OLT	Es el dispositivo de concentración para múltiples conexiones de fibra óptica y administra todas las ONTs que está operando mediante la tecnología GPON	Huawei	MA5683T Año: 2015

Fuente: Elaborado por el autor

3.1.2.1. Descripción técnica del router de borde Mikrotik RB4011iGS+RM

El RB4011 es un routerboard diseñado para gestionar el tráfico de internet entre la red interna y la red externa. Funciona con el sistema operativo RouterOS, impulsado por una CPU ARM 1400 de 4 núcleos funcionando a una frecuencia nominal de 1400MHz. Este modelo cuenta con una memoria RAM de 1GB ideal para configuraciones de enrutamiento y firewall. Este equipo integra un puerto SFP+ de 10Gbps y 10 puertos Gigabit Ethernet como se puede evidenciar en la Figura 37. Una de las características de

este equipo es que incorpora la tecnología Power over Ethernet (Poe) en el puerto numero 10 (Mikrotik, 2022).

Figura 37. Mikrotik RB4011iGS+RM

Fuente: (Mikrotik, 2022)

En la Tabla 8 se detallan las especificaciones técnicas del equipo de borde.

Tabla 8. Especificaciones técnicas del equipo Mikrotik RB4011iGS+RM

Producto	**RB4011iGS+RM**
CPU	ARMv7
Núcleos	4
Frecuencia de CPU	1400 MHZ
Licencia de RouterOS	5
Sistema operativo	RouterOS
Compatibilidad IPv6	Si, mediante actualización
RAM	1 GB
Almacenamiento	512 MB
Puertos SFP+	1 SFP+ 10G
Puertos Ethernet	10 gigabit ethernet
Consumo eléctrico	33W
Puerto de salida PoE	Ether10

Fuente:(Mikrotik, 2022)

El router Mikrotik RB4011iGS+RM si cumple con los requisitos para soporte IPv6, ya que cuenta con el sistema operativo RouterOS. Mediante la actualización a versiones estables, es posible habilitar este soporte sin necesidad de hardware adicional.

3.1.2.2. Descripción técnica del router de acceso Mikrotik CCR1009-7G-1C-1S+

Es un router de alto rendimiento diseñado para para proveedores de servicios de internet. El CCR1009 pertenece a la familia Cloud Core Router la misma que se conoce por su CPU TILE de 9 núcleos funcionando a 1.2GHz. Ideal para aplicaciones de firewall avanzado y filtración de tráfico de alta velocidad incorporada en redes de última milla. Está equipado con un puerto SFP+ 10G, un puerto combo SFP+ 1G y siete puertos Gigabit Ethernet como se puede evidenciar en la Figura 38. Esta versión cuenta con una memoria RAM de 2GB y un almacenamiento interno de 128 MB (MikroTik, 2022).

Figura 38. Mikrotik CCR1009-7G-1C-1S+

Fuente:(MikroTik, 2022)

En la Tabla 9 se detallan las especificaciones técnicas del equipo, que constituye una parte esencial y de alto rendimiento para los servicios de telecomunicaciones.

Tabla 9. Especificaciones técnicas del equipo Mikrotik CCR1009-7G-1C-1S+

Producto	**CCR1009-7G-1C-1S+**
Arquitectura	TILE
CPU	TLR4-00980
Núcleos	9
Frecuencia de CPU	1.2 GHz
Licencia de RouterOS	6
Sistema operativo	RouterOS

Producto	CCR1009-7G-1C-1S+
Compatibilidad IPv6	Si, mediante actualización
RAM	2 GB
Almacenamiento	128 MB
Puertos SFP+	1 SFP+ 10G
Ethernet Combo ports	1 RJ45 o SFP 1G
Puertos Ethernet	7 puertos Gigabit Ethernet
Consumo eléctrico	34W
tarjeta de memoria externa	1 tarjeta inteligente microSD

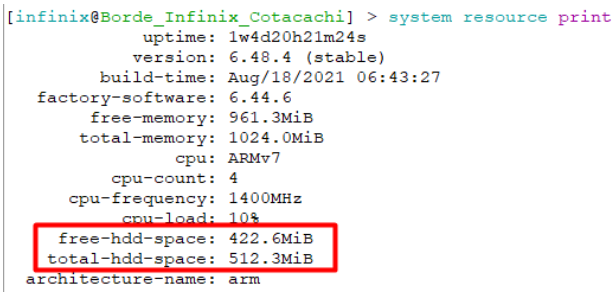
Fuente: (MikroTik, 2022)

El router equipo Mikrotik CCR1009-7G-1C-1S+ si soporta el protocolo IPv6 de manera nativa a través del sistema operativo RouterOS, el cual si incluye el paquete IPv6 siempre que el sistema este actualizado. Al mantener la actualización del equipo el mismo está apto para entornos de transición y despliegue de redes IPv6.

3.1.2.3. Recursos consumidos del router Mikrotik RB4011iGS+RM

El análisis del rendimiento actual de la red en cada dispositivo nos ayuda a determinar las características reales de operación. En la Figura 39, se comprueba el valor del almacenamiento total de 512.3 MiB expresado en megabytes y el espacio libre que queda es de 422.6 MiB.

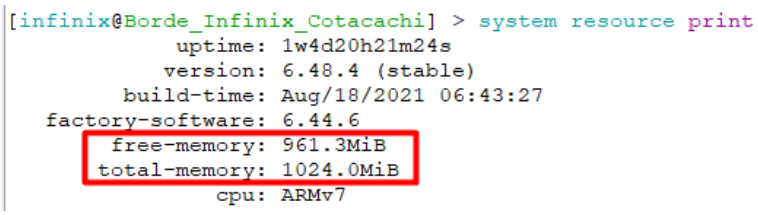
Figura 39. Almacenamiento interno del RB4011iGS+RM



Fuente: Equipo de administración de INFINIX INTERNET

La Figura 40 muestra el consumo de la memoria del equipo. Aquí se detalla todos los procesos que está ejecutando en el router MikroTik, incluyendo las configuraciones de cada interfaz y las reglas del firewall que se utiliza como seguridad para la red. El equipo tiene 1024 MiB de memoria total. De esos, el 961.3 MiB están libres. Esto nos garantiza que si se pueden realizar más configuraciones sin ningún inconveniente.

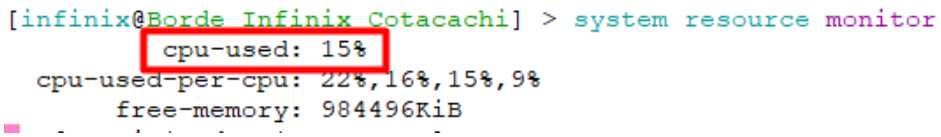
Figura 40. Memoria interna del RB4011iGS+RM



Fuente: Equipo de administración de INFINIX INTERNET

En la Figura 41, se puede ver que el uso actual del CPU es del 15%. Este uso depende de los servicios que están configurados en el equipo de administración. Dicho porcentaje muestra cuanta capacidad de procesamiento está utilizando el router para realizar todas las tareas. El uso del CPU del 15% significa que el router tiene aún una capacidad del 85% de procesamiento libre para cualquier configuración adicional.

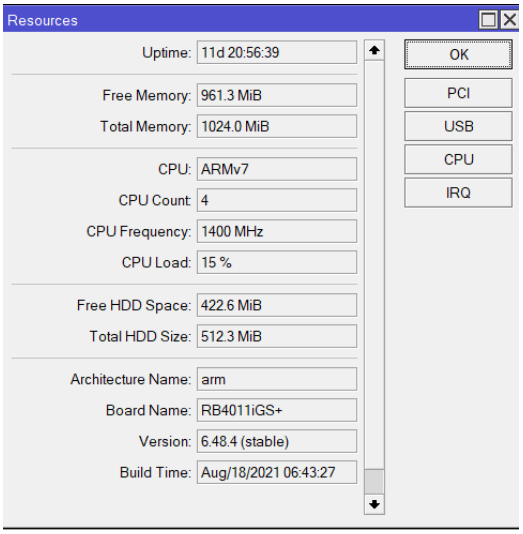
Figura 41. Estado del CPU del RB4011iGS+RM



Fuente: Equipo de administración de INFINIX INTERNET

Los equipos Mikrotik permiten ver sus recursos en una interfaz gráfica, así se puede observar el uso de los recursos del equipo en tiempo real. En la Figura 42 se puede ver que el uso del CPU en tiempo real es del 15%, el espacio de memoria disponible es de 512.3 MiB y 422.6 MiB de almacenamiento libre.

Figura 42. Recursos generales del del RB4011iGS+RM



Fuente: Equipo de administración de INFINIX INTERNET

3.1.2.4. Recursos consumidos del router Mikrotik CCR1009-7G-1C-1S+

El análisis del rendimiento actual de la red de cada dispositivo nos ayuda a determinar las características reales de operación. En la Figura 43, se comprueba el valor del almacenamiento total de 128.0 MiB expresado en megabytes y el espacio libre que queda es de 68.3MiB.

Figura 43. Almacenamiento interno del Mikrotik CCR1009-7G-1C-1S+

```
[infinix@Router_Accesos_Cotacachi] > system resource print
                   uptime: 1w4d20h35m50s
                  version: 6.48.4 (stable)
               build-time: Aug/18/2021 06:43:27
         factory-software: 6.38.5
              free-memory: 1696.4MiB
             total-memory: 1984.0MiB
                      cpu: tilegx
                cpu-count: 9
            cpu-frequency: 1200MHz
                 cpu-load: 5%
           free-hdd-space: 68.3MiB
          total-hdd-space: 128.0MiB
        architecture-name: tile
                board-name: CCR1009-7G-1C-1S+
                  platform: MikroTik
```

Fuente: Equipo de administración de INFINIX INTERNET

La Figura 44 muestra el consumo de la memoria del equipo. Aquí se detalla todos los procesos que está ejecutando en el router MikroTik, incluyendo las configuraciones de cada interfaz y las reglas del firewall que se utiliza como seguridad para la red. El equipo

tiene 1984 MiB de memoria total. De esos, el 1696.4 MiB gigabytes están libres. Esto nos garantiza que si se pueden realizar más configuraciones sin ningún inconveniente.

Figura 44. Memoria interna del Mikrotik CCR1009-7G-1C-1S+

```
[infinix@Router_Accesos_Cotacachi] > system resource print
                   uptime: 1w4d20h35m50s
                  version: 6.48.4 (stable)
               build-time: Aug/18/2021 06:43:27
         factory-software: 6.38.5
              free-memory: 1696.4MiB
             total-memory: 1984.0MiB
                      cpu: tilegx
```

Fuente: Equipo de administración de INFINIX INTERNET

En la Figura 45, se puede ver que el uso actual del CPU es del 14%. Este uso depende de los servicios que están configurados en el equipo de administración. Dicho porcentaje muestra cuanta capacidad de procesamiento está utilizando el router para realizar todas las tareas. El uso del CPU del 14% significa que el router tiene aún una capacidad del 86% de procesamiento libre para cualquier configuración adicional.

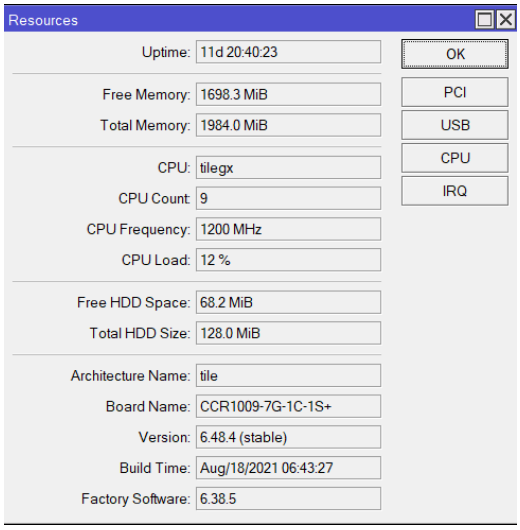
Figura 45. Estado del CPU del Mikrotik CCR1009-7G-1C-1S+

```
[infinix@Router_Accesos_Cotacachi] > system resource monitor
               cpu-used: 14%
  cpu-used-per-cpu: 6%,18%,1%,17%,28%,12%,36%,3%,5%
       free-memory: 1739328KiB
```

Fuente: Equipo de administración de INFINIX INTERNET

Los equipos Mikrotik permiten ver sus recursos en una interfaz gráfica, se puede observar el uso de los recursos del equipo en tiempo real. En la Figura 46 se puede ver que el uso del CPU en tiempo real es del 12%, el espacio de memoria disponible es de 128 GiB y 68.2 MiB de almacenamiento libre.

Figura 46. Recursos generales del Mikrotik CCR1009-7G-1C-1S+

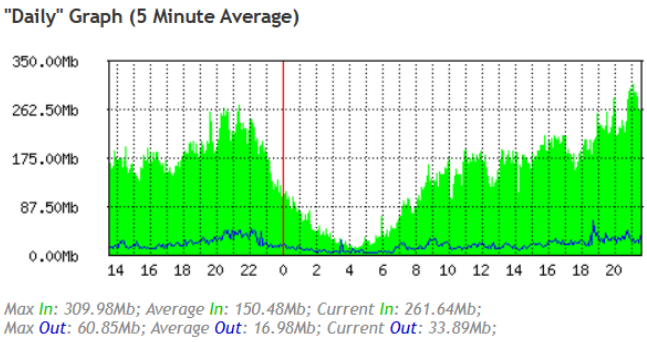


Fuente: Equipo de administración de INFINIX INTERNET

3.1.2.5. Consumo de ancho de banda

El ancho de banda determina la velocidad de trasferencia de datos. Actualmente, INFINIX INTERNET tiene un contrato con la empresa Nedetel por un ancho de banda dedicado de 1Gbps. Para conocer el tráfico actual de la red, se accede a la página web del router Mikrotik la misma que debe estar habilitado en el apartado de servicio. La interfaz web tiene un panel gráfico que muestra el consumo del ancho de banda para cada interfaz física del equipo. En la Figura 47 se evidencia el consumo diario del ancho de banda real utilizado por los clientes en la interfaz física sfp-sfpplus1 determinada como la interfaz WAN. El máximo pico de tráfico es de 309.98 Mbps, mientras que el valor promedio es de 150.48 Mbps.

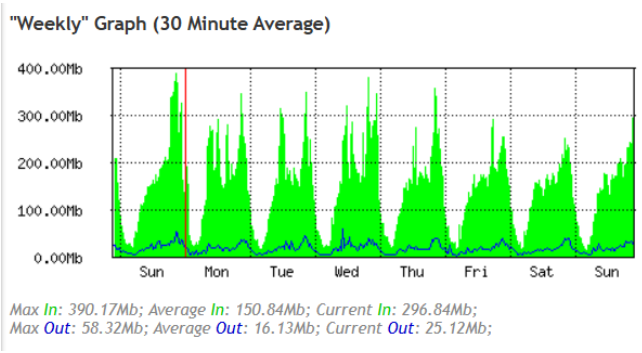
Figura 47. Consumo diario del ancho de banda



Fuente: Equipo de administración de INFINIX INTERNET

En la Figura 48 se analiza el gráfico del consumo del tráfico en un periodo de tiempo más largo. El patrón de consumo de ancho de banda es casi similar todos los días. En la gráfica de consumo semanal, los picos máximos de uso son de 390.17 Mbps y el consumo promedio por semana es de 150.84 Mbps.

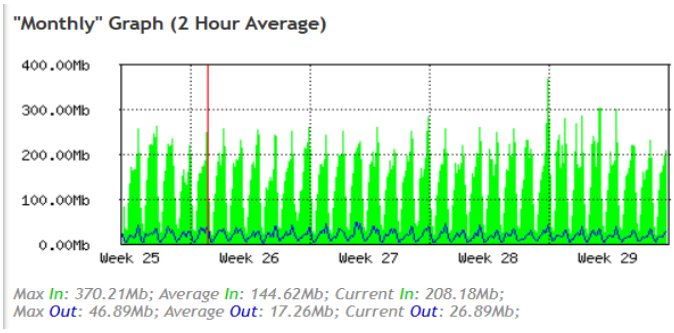
Figura 48. Consumo de ancho de banda semanal



Fuente: Equipo de administración de INFINIX INTERNET

Al igual que en el caso anterior, se puede comprobar el consumo de ancho de banda de manera mensual. Este dato nos ayuda a equilibrar el recurso de ancho de banda y a evitar que la demanda de la red aumente. En la Figura 49, se presenta un consumo mensual de 370.21 Mbps. Esto es menos que el ancho de banda que se tiene contratado de 1GBps, lo que significa que hay un 63% de ancho de banda libre. Esto no impide planificar el crecimiento y la expansión de la red.

Figura 49. Consumo de ancho de banda mensual

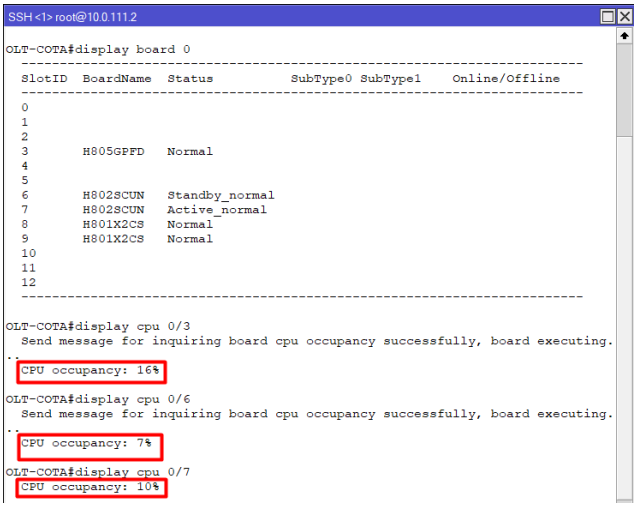


Fuente: Equipo de administración de INFINIX INTERNET

Para determinar los valores de recursos consumidos en la OLT, se realiza la conexión mediante el emulador de telnet. Para ello, se ingresa la dirección IP de la gestión de la OLT, como también el correspondiente usuario y contraseña. La Figura 50 muestra los módulos activos y usando el comando *display cpu* más el respectivo número de interfaz para verificar el estado del CPU.

El primer módulo hace énfasis en la tarjeta de servicio GPON. Esta tarjeta soporta 1.25 Gbps de subida y 2.5 Gbps de bajada, la misma tiene un uso del CPU del 16%. El segundo y el tercer módulo que están en las ranuras 0/6 y 0/7 respectivamente son las tarjetas de control y conmutación. Estas tarjetas gestionan el control de la OLT y tiene un consumo del CPU del 7% y 10 % respectivamente.

Figura 50. Consumo del CPU de los módulos activos de la OLT del nodo Cotacachi

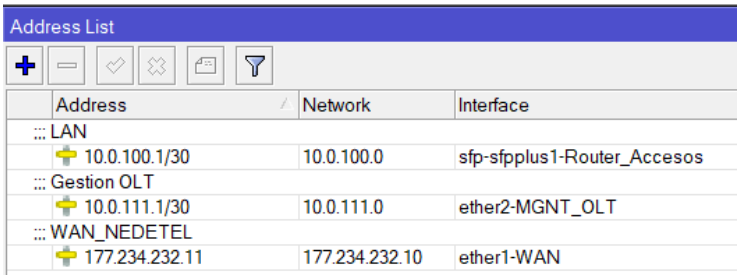


Fuente: Equipo de administración de INFINIX INTERNET

3.1.2.6. Direccionamiento IPv4 actual del nodo Cotacachi

La infraestructura de la red del nodo Cotacachi cuenta con un direccionamiento IPv4. El equipo de borde encargado de la conexión hacia internet dispone de una dirección IP pública asignada por el proveedor NEDETEL, la misma que está configurada en la interfaz ether1. Para la red LAN que interconecta al equipo de acceso de clientes, se ha configurado una dirección IP privada en la interfaz sfp-sfpplus1. Finalmente, en la interfaz ether2 se encuentra configurada el direccionamiento IP para la gestión de la OLT, tal como se muestra en la Figura 51.

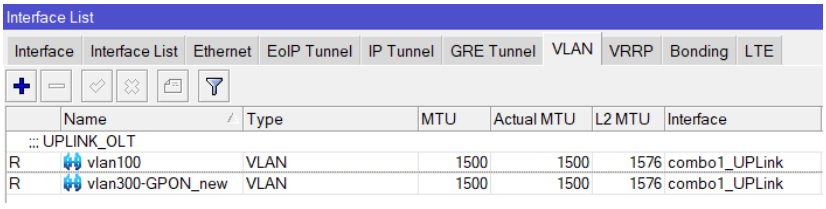
Figura 51. IP pública asignadas al nodo Cotacachi



Fuente: Equipo de borde de INFINIX INTERNET

En la red LAN está el equipo Mikrotik CCR1009-7G-1C-1S+ denominado router de acceso. Para que los usuarios puedan acceder a la red, se tiene creadas dos redes virtuales como se puede evidenciar en la Figura 52. Estas redes virtuales ayudan a dividir el tráfico de los usuarios en la interfaz combo1 del router de acceso. Cada VLAN es una red distinta que cuenta con su propio direccionamiento IP. La VLAN 100 es para los clientes que se conectan mediante el protocolo DHCP, y la VLAN 30 son para clientes que tienen acceso mediante el protocolo PPPoE.

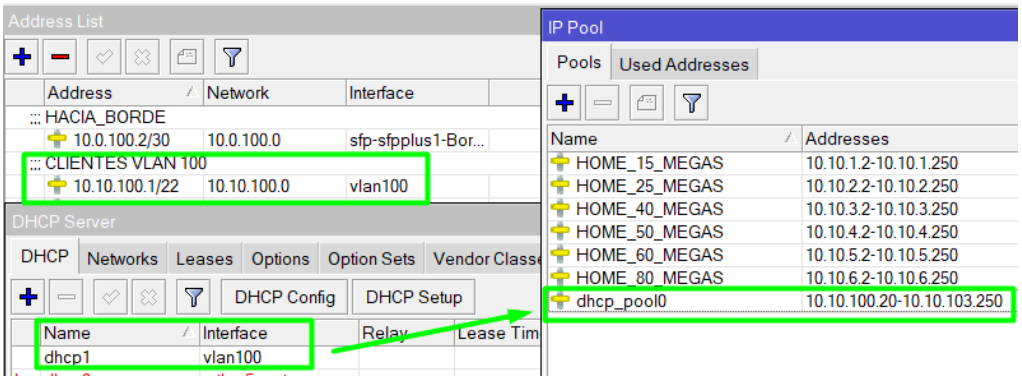
Figura 52. VLANs de acceso para los usuarios



Fuente: Equipos de acceso de INFINIX INTERNET

La VLAN 100 está determinada mediante el protocolo de red DCHP la cual brinda direcciones IPs dinámicas a varios clientes. Esto significa que un servidor DHCP envía los parámetros de configuraciones específicas para cada cliente que se conecta a la red. Entre estos parámetros se encuentra la dirección IP del cliente. La dirección IP de la interfaz virtual 100 es la 10.10.100.1/22, como muestra en la Figura 53. Mediante esta dirección IP se puede tener hasta 1022 usuarios. El rango de direcciones IP se gestiona mediante en el servidor DCHP por el pool de direccionamiento (dhcp_pool0) que va desde la dirección 10.10.100.20 al 10.10.103.250. Con esta información, se evidencia notablemente que dicho direccionamiento IP esta sobredimensionado. En una VLAN es recomendable administrar hasta 254 usuarios por el tema de rendimiento de la red, si sobrepasa dicha cantidad de usuarios se genera mucho tráfico de broadcast, lo que puede saturar la red.

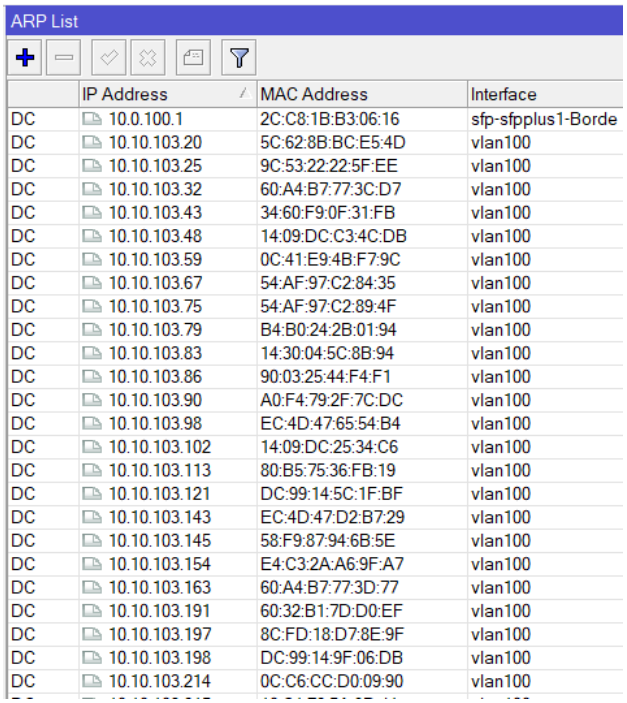
Figura 53. Direccionamiento IP de la VLAN 100



Fuente: Equipos de acceso de INFINIX INTERNET

La Figura 54 muestra la sección de ARP del router Mikrotik. En este bloque, se puede ver la tabla de ARP, que muestra todas las direcciones IP de los clientes registrados en el servidor DHCP. Estas direcciones IP están asociados a la MAC Address de los equipos finales de cada cliente. Todas estas direcciones IPs están operativas mediante la VLAN 100.

Figura 54. Lista ARP con su respectiva MAC Address

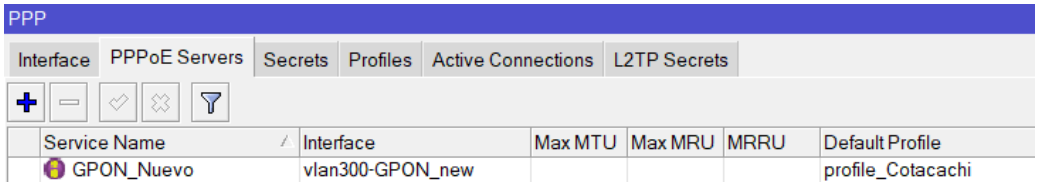


	IP Address	MAC Address	Interface
DC	10.0.100.1	2C:C8:1B:B3:06:16	sfp-sfpplus1-Borde
DC	10.10.103.20	5C:62:8B:BC:E5:4D	vlan100
DC	10.10.103.25	9C:53:22:22:5F:EE	vlan100
DC	10.10.103.32	60:A4:B7:77:3C:D7	vlan100
DC	10.10.103.43	34:60:F9:0F:31:FB	vlan100
DC	10.10.103.48	14:09:DC:C3:4C:DB	vlan100
DC	10.10.103.59	0C:41:E9:4B:F7:9C	vlan100
DC	10.10.103.67	54:AF:97:C2:84:35	vlan100
DC	10.10.103.75	54:AF:97:C2:89:4F	vlan100
DC	10.10.103.79	B4:B0:24:2B:01:94	vlan100
DC	10.10.103.83	14:30:04:5C:8B:94	vlan100
DC	10.10.103.86	90:03:25:44:F4:F1	vlan100
DC	10.10.103.90	A0:F4:79:2F:7C:DC	vlan100
DC	10.10.103.98	EC:4D:47:65:54:B4	vlan100
DC	10.10.103.102	14:09:DC:25:34:C6	vlan100
DC	10.10.103.113	80:B5:75:36:FB:19	vlan100
DC	10.10.103.121	DC:99:14:5C:1F:BF	vlan100
DC	10.10.103.143	EC:4D:47:D2:B7:29	vlan100
DC	10.10.103.145	58:F9:87:94:6B:5E	vlan100
DC	10.10.103.154	E4:C3:2A:A6:9F:A7	vlan100
DC	10.10.103.163	60:A4:B7:77:3D:77	vlan100
DC	10.10.103.191	60:32:B1:7D:D0:EF	vlan100
DC	10.10.103.197	8C:FD:18:D7:8E:9F	vlan100
DC	10.10.103.198	DC:99:14:9F:06:DB	vlan100
DC	10.10.103.214	0C:C6:CC:D0:09:90	vlan100

Fuente: Equipos de acceso de INFINIX INTERNET

El direccionamiento IP de las VLAN 300 como se puede observar en la Figura 55, se obtiene usando el servidor de autenticación PPPoE. Este sistema se utiliza para verificar y autenticar a los usuarios que puedan tener acceso a internet a través de una base local creada en el Mikrotik.

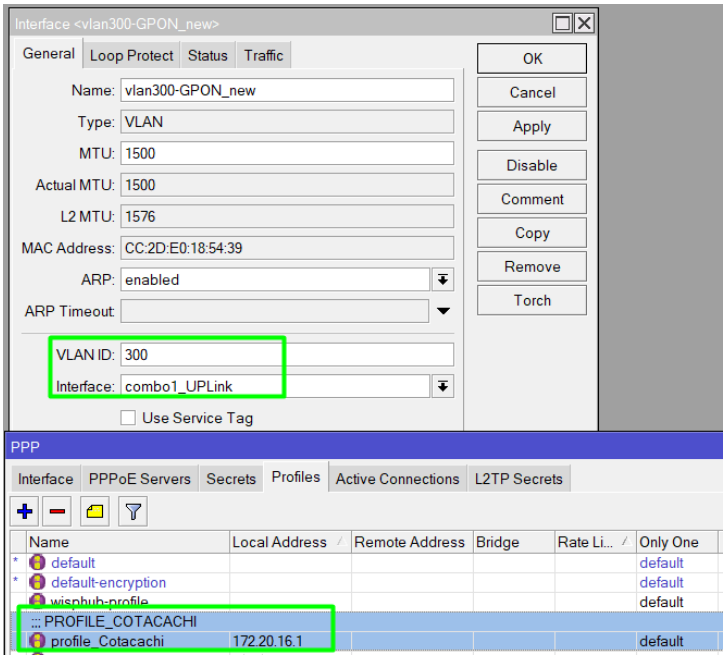
Figura 55. Servidor PPPoE



Fuente: Equipos de administración de INFINIX INTERNET

La VLAN 300 es asociada a la interfaz física denominada combo1 del router de acceso. El nombre es vlan300-GPON_new y en el servidor PPP se crea una profile llamado GPON_New como se puede observar en la Figura 56. Se asocia una dirección local 172.20.16.1 sin delimitación de ancho de banda. La gestión del ancho de banda se lo realiza en el Simple Queues.

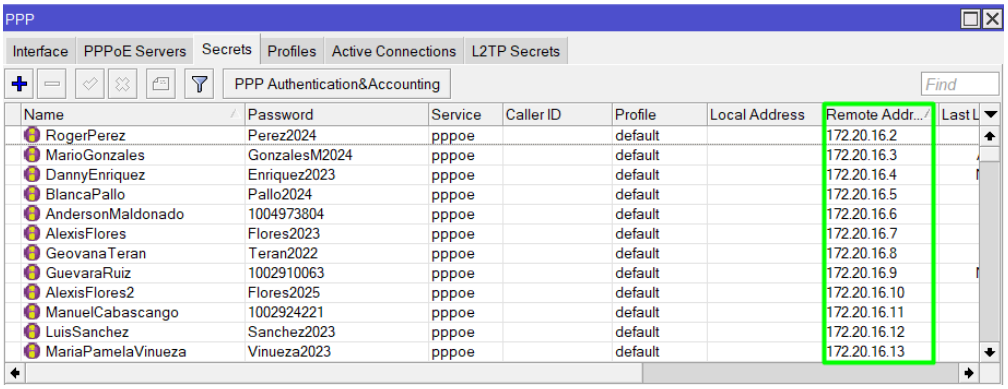
Figura 56. Interfaz PPPoE para VLAN 300



Fuente: Equipos de acceso de INFINIX INTERNET

Cada usuario se autentica de forma individual mediante su nombre y la contraseña establecida en el directorio de Secrets como se muestra en la Figura 57. También, se asigna la dirección IP en el apartado de Remote Adress. Toda esta configuración se lleva a cabo de manera manual en la plataforma Winbox del router de acceso.

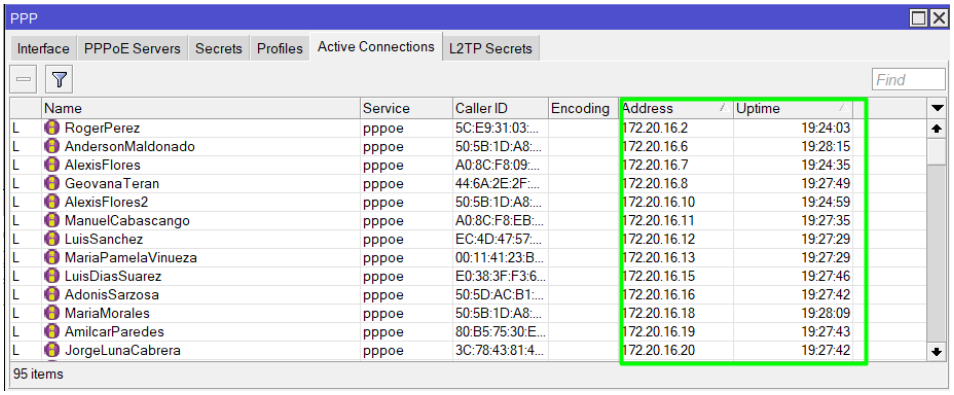
Figura 57. Usuarios y contraseñas para la autenticación PPPoE



Fuente: Equipos de acceso de INFINIX INTERNET

En la sección PPP del router de acceso, es posible visualizar las conexiones activas de los usuarios a la red mediante el protocolo PPPOE. En la Figura 58 se muestra información como el usuario, la dirección IP y el tiempo que ha estado en línea desde que se autenticó.

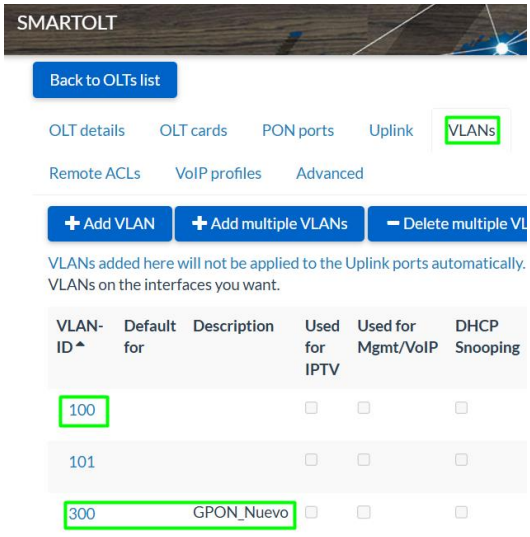
Figura 58. Conexiones activas mediante el protocolo PPPoE



Fuente: Equipos de acceso de INFINIX INTERNET

La OLT del nodo Cotacachi es administrada mediante el software SMARTOLT. En este software se puede apreciar que se han configuradas las VLANs tal como muestra la Figura 59, así tenido por separada el tráfico de múltiples usuarios en cada una de su red virtual.

Figura 59. VLANs configuradas en la OLT

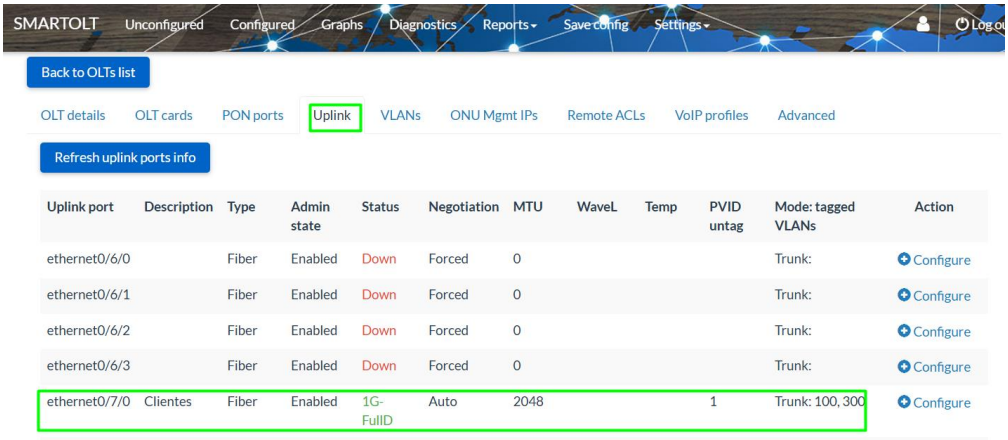


Fuente: Software de administración de la OLT

La tarjeta UPLink ethernet 0/7/0 se usa para que todos los usuarios tengan acceso a internet. Esta tarjeta tiene una capacidad de trasmisión de datos hasta 1G. Como se

observa en la Figura 60, en la interfaz de esta tarjeta está configurada un trunk para las interfaces virtuales. El trunk es el enlace que transporta múltiples VLANs a través de un cable DAC, que es la única conexión física entre la OLT hacia el router de acceso.

Figura 60. Troncalizacion de VLANs en la interfaz UPLink de la OLT



Fuente: Software de administración de la OLT

En la Tabla 10 se muestra un resumen de todas las direcciones IPv4 que están configuradas en los equipos de borde y de acceso del nodo Cotacachi. En el equipo de borde está configurada una IP pública, una IP para la red LAN que se conecta al router de acceso y un direccionamiento IP para la gestión de la OLT. En el router de acceso a clientes está configurada una VLAN mediante el protocolo DHCP y otra mediante el protocolo PPPOE. Estas están operativas en la interfaz combo1 brindando servicio de internet a los usuarios. Por último, hay una conexión troncal en la interfaz UPLink 1G de la OLT para dar salida a internet a los usuarios, asociada a las VLANs 100 y 300.

Tabla 10. Direccionamiento IP de los equipos del nodo Cotacachi

Equipo	Interfaz	Dirección IP	Dirección de red	Prefijo	Descripción
Mikrotik RB4011 iGS+RM Router de Borde	Ether1	177.234.323.11	177.234.232.10	/32	WAN- IP pública
	Ether2	10.0.111.1	10.0.111.0	/30	Gestión OLT
	sfp-sfpplus1	10.0.100.1	10.0.100.0	/30	Red LAN a router de acceso
Mikrotik CCR1009-7G-1C-1S+ Router de acceso	sfp-sfpplus1	10.0.100.2	10.0.100.0	/30	Conexión al equipo de borde
	combo1	**VLAN 100** 10.10.100.1	10.10.100.0	/22	IP designadas a los usuarios en la VLAN DHCP
		VLAN 300 172.20.16.1	172.20.16.0		IP designadas a los usuarios en la VLAN PPPoE
OLT Huawei	Puerto UPLink 1G	**TRUNK** VLAN 100 VLAN 300			Troncalización de las VLAN salida hacia internet de los usuarios.

Fuente: Elaborado por el autor

Discusión general del objetivo 1

Realizar un diagnóstico general de la red es muy importante para cualquier proceso de migración tecnológica. Este procedimiento ayuda a determinar de manera detallada la situación actual de la infraestructura de red y detectar posibles limitaciones de los recursos de cada equipo de telecomunicaciones. Este análisis inicial facilita la identificación de los recursos disponibles, el consumo del ancho de banda y la forma en que se encuentran configurados los equipos de telecomunicaciones de cada nodo. Sin este levantamiento de información, cualquier cambio en la red podría ejecutarse de manera improvisada, aumentando el riesgo de errores durante la transición.

El diagnóstico evidenciado en la red de los nodos Atuntaqui y Cotacachi se encuentra operando bajo el direccionamiento IPv4, el cual, aunque funcional, presenta limitaciones importantes. Entre ellas destacan la baja escalabilidad, ya que la cantidad de direcciones IPv4 es insuficiente frente al crecimiento proyectado de usuarios, y la deficiente segmentación de VLANs, que incrementa el riesgo de tráfico de broadcast, lo que aumenta la carga del trabajo de la red.

El análisis de la red permite identificar varios aspectos que requieren atención. Entre ellas se encuentra la dependencia total del protocolo IPv4, lo que limita la capacidad de expansión frente al incremento de usuarios y servicios. Así mismo, se evidencia la falta de un esquema de direccionamiento con proyección futura, lo que dificulta la organización y gestión eficiente de los recursos de red. A esto se suma el riesgo de saturación en la administración de usuarios debido al agotamiento de direcciones públicas. En general, estas limitaciones reflejan que la infraestructura actual carece de sostenibilidad a largo plazo y presenta vulnerabilidades técnicas que podrían comprometer la continuidad del servicio.

Finalmente, el diagnóstico de la red no se limitó a describir el estado de la infraestructura, sino que evidencia problemas técnicos como falta de escalabilidad del IPv4 y la subutilización de los recursos de la red que afecta la calidad del servicio. Esta situación justifica la propuesta de migración hacia el protocolo IPv6, asegurando escalabilidad, eficiencia y crecimiento sostenible para la empresa INFINIX INTERNET, ofreciendo de esta forma un servicio más estable y confiable a sus usuarios.

3.2. Selección del mecanismo de transición IPv4 a IPv6

La selección de un mecanismo de transición requiere un análisis detallado de las características, ventajas y desventajas que ofrece cada alternativa de transición, con el fin de asegurar una buena convivencia entre infraestructura existente y el nuevo protocolo. Dado que no es posible realizar una migración drástica hacia IPv6, principalmente porque muchos servicios y aplicaciones aún no cuentan con soporte completo para este protocolo. Es necesario implementar soluciones de transición que permitan mantener la operación bajo IPv4 mientras se habilita gradualmente la adopción de IPv6.

En la Tabla 11, se detallan las principales características de los distintos mecanismos de transición, las cuales constituyen un factor determinante para identificar cuál de ellos resulta más adecuado para su implementación en la infraestructura actual de la empresa INFINIX INTERNET.

Tabla 11. Características de los mecanismos de transición

Característica	**Mecanismos de Transición**		
	Dual Stack	**Tunelización**	**Traducción**
Principio de operación	Doble pila	Encapsulamiento de paquetes IPv6 dentro de IPv4	NAT64/DNS64 Traducción con mapeo algorítmico.
Backbone del proveedor	Doble pila	IPv4 o IPv6 según la implementación del túnel	IPv6 Only
Conserva direcciones IPv4	Si	Si	Si
IPv6 nativo para el usuario	Si	No, IPv6 viaja encapsulado en IPv4	Si

Característica	Mecanismos de Transición		
	Dual Stack	**Tunelización**	**Traducción**
Alcanzan sitios IPv6-Only	Si	Si, con limitaciones	Si, con limitaciones
Red de transporte	Dual Stack	IPv4 más el túnel	IPv6 Only
Diseñado para	Para clientes de un ISP que puedan acceder a interne IPv4 e IPv6 usando doble pila de protocolo	Usuarios que tienen conexión mediante IPv4 pero necesitan acceder a servicio IPv6	Para clientes con IPv6 que establezcan conexión a servidores IPv6 desde una IPv4 y usando DNS64

Fuente: (Aguirre, 2023)

3.2.1. Ventajas y desventajas del mecanismo de transición

A continuación, se presentan las ventajas y desventajas del mecanismo de transición Dual Stack, con el fin de evaluar su idoneidad para la migración de IPv4 a IPv6.

Ventajas de Dual Stack

- La principal ventaja del método de transición dual Stack radica en su simplicidad, ya que no es necesario utilizar las técnicas de túneles ni de procesos de encapsulado.
- No se elimina el direccionamiento IPv4, dicho protocolo puede seguir operando sin realizar ninguna adaptación adicional.
- Dual Stack permite la coexistencia prolongada de IPv4 e IPv6. Esta característica posibilita que las aplicaciones y servicios realicen una migración progresiva hacia IPv6 sin interrumpir la operación (Aguirre, 2023).
- Los host o equipos terminales pueden resolver DNS tanto en IPv4 e IPv6.

Desventajas de Dual Stack

- La implementación de Dual Stack implica tener doble planificación, administración y supervisión de la red.
- No es adecuado para redes telefónicas celular, debido a lo que requiere el doble de recursos.

Se detallan a continuación las ventajas y desventajas de la tunelización como mecanismo de transición entre IPv4 e IPv6, considerando su aplicabilidad en redes de telecomunicaciones.

Ventajas de Tunelización

- Permite la comunicación entre dominios de enrutamiento IPv6 sin problemas de configuración generalizados.
- Puede realizar una configuración de manera remota
- No requiere modificación de la capa de enlace

Desventajas de Tunelización

- La transición entre Ipv4 a Ipv6 utilizando solo túneles IP, puede llevar a problemas de escalabilidad debido a que algunas redes requieren la declaración explicita de las direcciones origen y destino.
- Algunas conexiones no responden bien a esta técnica por limitantes de hardware en los routers.

A continuación, se exponen las ventajas y desventajas del mecanismo de traducción NAT64, destacando su papel en la interoperabilidad entre redes IPv4 e IPv6.

Ventajas de traducción

- Al traducirlas direccionesIPv6 a direcciones IPv4, NAT64 permite a las direcciones IPv6 comunicarse con las redes IPv4, conservando las direcciones IPv4.
- En el nodo de un ISP necesita mantener una sola pila de protocolo es decir IPv6 nativo lo que puede reducir uso de recursos en la infraestructura de telecomunicaciones.

Desventajas de traducción

- Mediante este mecanismo de traducción el NAT64 requiere la traducción de las direcciones IP, lo que puede crear problemas de rendimiento y compatibilidad.
- Diversas aplicaciones que incrustan direcciones IP en el contenido del paquete pueden tener problemas de comunicación.
- En traducción de direcciones NAT64 necesita trabajar en combinación con DNS64 para crear direcciones IPv6 sintéticas, lo que añade una capa adicional de complejidad.
- No todos los protocolos son fácilmente traducibles entre IPv4 a IPv6. Esto puede causar problemas de interoperabilidad (Academy, 2023).

3.2.2. Mecanismo de transición a implementar

Para seleccionar un mecanismo de transición más adecuado en la migración del protocolo IPv4 a IPv6, nos apoyamos en una matriz de decisión que permite comparar varias alternativas frente a un conjunto de criterios técnicos previamente definidos, como ventajas y características de cada mecanismo, asignando valores ponderados a cada criterio. La Tabla 12 facilita un análisis estructurado de alternativas como Dual Stack, tunelización y traducción.

Los criterios de evaluación se relacionan con aspectos fundamentales de eficiencia, escalabilidad, compatibilidad, complejidad de implementación y sostenibilidad a largo plazo. Cada criterio recibe una ponderación de acuerdo con su nivel de importancia dentro del proyecto, asignado valores del 1 al 5, donde 1 representa la puntuación más pobre y 5 un desempeño óptimo.

La ponderación total de cada mecanismo se obtiene mediante el producto entre el peso asignado y la puntuación obtenida en cada criterio. De este modo, la matriz de decisión constituye una herramienta técnica y objetiva que permite determinar qué alternativa garantiza mejor la operabilidad de la red, asegurando la continuidad del servicio y una migración ordenada hacia IPv6.

Tabla 12. Matriz de decisión de los mecanismos de transición

Criterio	Peso	Mecanismos de transición		
		Dual Stack	**Tunelización**	**Traducción**
Escalabilidad	0.25	5	2	4
Compatibilidad	0.20	5	3	3
Facilidad de implementación	0.15	4	4	3
Seguridad	0.12	4	2	3
Rendimiento	0.12	5	3	4
Gestión de operación	0.10	3	2	3
Costo	0.06	5	3	4
Total ponderado	1	4.53	2.68	3.37

Fuente: Elaborado por el autor

En la evolución realizada a través de la matriz de decisión, en las cuales se compararon los mecanismos de transición. Cada uno de ellos presenta ventajas y limitaciones que influye en su aplicabilidad dentro de la infraestructura de un ISP.

- Dual Stack obtiene la puntuación más alta con 4.53 ofreciendo máxima compatibilidad con excelente rendimiento. Este mecanismo es la opción más preferida para implementación en un ISP ya que se caracteriza por permitir la coexistencia entre IPv4 e IPv6.
- El mecanismo de tunelización obtiene una puntuación de 2.68 son las soluciones de transición menos deseables en producción en un ISP. Son rápidos para establecer pruebas de funcionalidad entre enlaces punto a punto, pero menos escalables con mayor latencia y gestión compleja.

- Por último el mecanismo de traducción obtenido una puntuación de 3.37. Este ofrece una solución práctica para facilitar la conexión de usuarios IPv6 hacia servicios IPv4; sin embargo, presenta limitaciones al no solucionar casos de interoperabilidad.

Una vez realizada el análisis de cada uno de los mecanismos de transición. Se determina que el más adecuado para la implementación dentro de la infraestructura de telecomunicaciones de la empresa INFINIX INTERNET es Dual Stack. Este mecanismo ofrece un cambio progresivo y seguro hacia IPv6, permitiendo la convivencia entre ambos protocolos en una misma red. Según las recomendaciones del (IETF RFC 4213, 2018), Dual Stack constituye la forma más natural de transición, ya que habilita de manera nativa la interoperabilidad entre IPv4 e IPv6 sin requerir traducción o encapsulamiento de los datos. De igual forma, el (IETF RFC 6180, 2011) señala que Dual Stack debe ser considerado como la primera opción de despliegue en los ISPs. debido a los beneficios que brinda asegurando continuidad operativa y reduce riesgos asociados a otros mecanismos temporales como tunelización o la traducción.

Con la implementada el mecanismo Dual Stack, el enrutador puede gestionar de manera simultánea conectividad en IPv4 e IPv6. De esta forma, cuando se establece una conexión hacia un destino que tenga configurado IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6. Este enfoque garantiza compatibilidad con servicio que aún no han adoptado IPv6 y asegura una transición transparente sin pérdida de conectividad. En caso de que el destino tenga configurada ambos protocolos normalmente se conecta primero por IPv6 y en segunda instancia por el protocolo IPv4.

Discusión general del objetivo 2

El análisis comparativo de los mecanismos de transición evidencia que Dual Stack ofrece mayor ventaja, ya que proporciona una conectividad nativa tanto en IPv4 como en IPv6, garantizando al usuario un acceso sin limitaciones a servicios y sitios disponibles en IPv6. Esto lo convierte en la alternativa más robusta y adaptable frente a los demás mecanismos de transición. Por otro lado, el mecanismo de tunelización presenta limitaciones al encapsular los paquetes, lo que reduce eficiencia y desempeño en la red. Finalmente, el

mecanismo de traducción puede presentar posibles restricciones de acceso a ciertos servicios, ya que no todos los protocolos son fácilmente traducibles de IPv4 a IPv6.

Desde una perspectiva operativa, la gestión de Dual Stack implica que los administradores deben mantener configuraciones paralelas de IPv4 e IPv6, lo que requiere un monitoreo constante de las tablas de enrutamiento, políticas de seguridad y el uso eficiente del direccionamiento IP. Este enfoque disminuye riesgos de pérdida de conectividad durante la transición, ya que permite seguir operando con IPv4 mientras se adopta gradualmente IPv6. Además, reduce la dependencia de mecanismos temporales que suelen incrementar la latencia y limita la compatibilidad en ciertos servicios.

En este sentido, las recomendaciones del RFC 4231 destacan la relevancia de la implementación del mecanismo Dual Stack para garantizar interoperabilidad y continuidad del servicio durante el periodo de transición. De manera complementaria, la recomendación del RFC 6180 establece que Dual Stack es el mecanismo primordial para ISPs, ya que permite un despliegue ordenado en IPv6. La interacción de estas recomendaciones impuestas por el Grupo de Trabajo de la Ingeniería en Internet refuerza la decisión técnica, ya que alinean la solución planteada con las mejores prácticas internacionales, asegurando sostenibilidad, escalabilidad y compatibilidad a largo plazo en la infraestructura de la empresa.

3.3. Diseño del esquema de direccionamiento IPv6

El diseño del esquema de direccionamiento IPv6 es esencial para garantizar una migración ordenada y escalable. En esta sección se define la asignación de prefijos y subredes, optimizando el uso de recursos y asegurando la compatibilidad con los mecanismos de transición implementados.

3.3.1. Recursos y soportes de IPv6 en equipos activos

El primer punto consiste en verificar el soporte del protocolo IPv6 en los equipos activos de la red de la empresa INFINIX INTERNET y evaluar sus recursos de hardware, con el fin de determinar si cuentan con los recursos necesarios para implementar el direccionamiento de red en IPv6. En la Tabla 13 se presentan las características técnicas de cada uno de los equipos activos de los diferentes nodos del ISP, detallando tanto

recursos actuales en uso como también la disponibilidad del CPU, memoria y almacenamiento.

Tabla 13. Recursos de equipos activos

Recursos	**Equipos activos**		
	Mikrotik CCR2116	**Mikrotik RB4011**	**Mikrotik CCR1009**
Almacenamiento Interno	Total: 128.0MiB	Total: 512.3 MiB	Total: 128.0 MiB
	Libre: 95.1 MiB	Libre: 422.6 MiB	Libre: 68.3 MiB
Memoria Interna	Total 16.0 GiB	Total: 961.3 MiB	Total: 1981.0 MiB
	Libre 15.4 GiB	Libre: 1024 MiB	Libre: 1696.0 MiB
CPU	En uso 4%	En uso: 15%	En uso: 14%
	Libre 94%	Libre: 85%	Libre: 86%
Versión IOS	7.14.2 estable	6.48.4 estable	6.48.4 estable
Soporte IPv6	Si	Si mediante actualización	Si mediante actualización
Nodo	Atuntaqui	Cotacachi	Cotacachi
Cumple requerimiento	SI	SI	SI

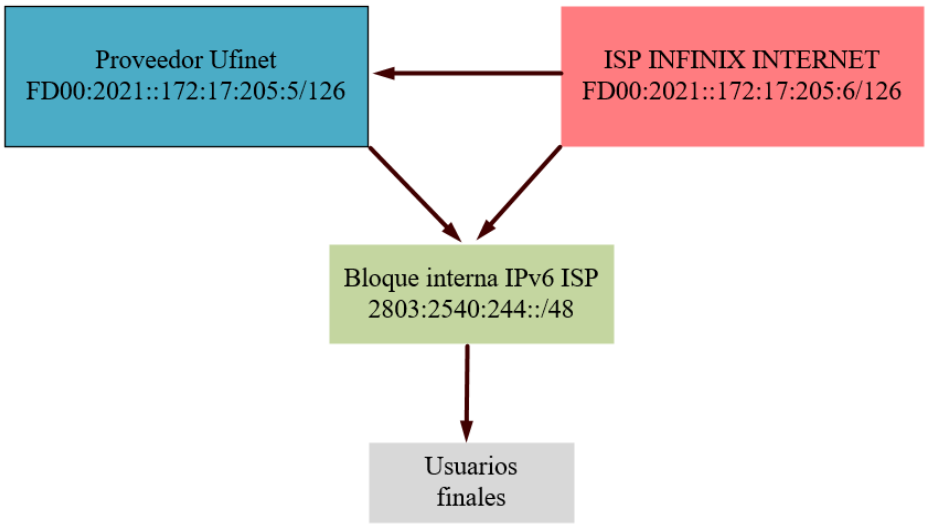
Fuente: Elaborado por el autor

Una vez verificado los recursos disponibles de cada equipo activo, se confirma que cumplen con los requerimientos necesarios para habilitar el protocolo IPv6. Del análisis realizado, los routers Mikrotik CCR1009 y RB4011 operan actualmente en la versión de RouterOS 6.48.4, por lo que para implementar IPv6 será necesario activar el paquete correspondiente y reiniciar el equipo, garantizando así la compatibilidad de dicho protocolo. Esta información constituye la base para analizar la viabilidad de la transición a IPv6 y será como referencia en el diseño del esquema de direccionamiento de red.

3.3.2. Solicitud de una dirección IPv6

El proveedor Ufinet Nedetel asigna un esquema de direccionamiento IPv6 compuesto por un enlace punto a punto con prefijo /126 y un bloque de ruta /48 para la red interna del ISP, como se muestra en la Figura 61. La dirección FD00:2021::172:17:205:5/126 corresponde al lado del proveedor, mientras que el ISP debe utilizar la dirección contigua en el mismo rango para el router de administración. La dirección de ruta 2803:2540:244::/48 es anunciada por el proveedor a través del enlace punto a punto y corresponde al bloque asignado para la red interna del ISP. A partir de este bloque se realiza la división en subredes, con el fin de asignar IPv6 organizadamente y garantizar su correcta administración y escalabilidad.

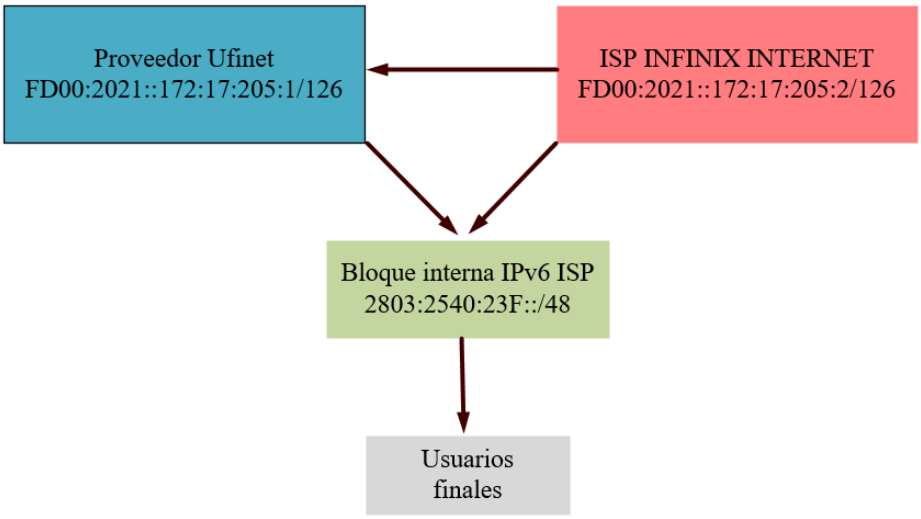
Figura 61. Asignación de prefijos nodo Atuntaqui



Fuente: Elaborado por el autor

De la misma forma, el proveedor Ufinet Nedetel asigna un esquema de direccionamiento IPv6 conformada por un prefijo /126, destinado para el enlace punto a punto entre el proveedor y el ISP, y un bloque de ruta /48, delegado para el ISP realice el respectivo subneteo y lo utilice en la red interna misma que se muestra en la Figura 62.

Figura 62. Asignación de prefijos nodo Cotacachi



Fuente: Elaborado por el autor

3.3.3. Planificación de direccionamiento en entorno Dual Stack

En el marco de la migración al protocolo IPv6, según el (IETF RFC 6177, 2011), establece que la asignación de prefijos a los ISPs es de un bloque /48, ya que este tamaño de direccionamiento constituye el estándar recomendado para ISPS con proyección a crecimiento. En este sentido, la empresa INFINIX INTERNET recibió del proveedor UFINET un bloque del prefijo 2803:2540:244::/48, el cual constituye el espacio de direccionamiento IPv6 asignado para su operación en el nodo de Atuntaqui.

A partir de este bloque se lleva a cabo el procedimiento de subneteo, dividiendo la dirección IPv6 global unicast en subredes más pequeñas con la finalidad de optimizar los recursos del direccionamiento IP. Dicho esquema se estructura conforme a las recomendaciones impuestas en el (IETF RFC 4291, n.d.), que establece la utilización de prefijo /64 para VLANs de clientes finales. En la operación de la red, el equipo OLT cuenta con una tarjeta GPON activada de 16 puertos PON, por lo que se define una VLAN para cada puerto PON. A cada VLAN se le asigna un direccionamiento IPv4 e IPv6, permitiendo que la red opere bajo el mecanismo Dual Stack, como se encuentra detallado en la Tabla 14.

Tabla 14. Direccionamiento Dual Stack Nodo Atuntaqui

Equipo	Interfaz	VLAN	Dirección IPv4	Dirección IPv6	Definido para
Mikrotik 2116	sfp-sfpplus1	ENLACE WAN	45.11.36.65 177.234.233.149	fd00:2021::172:17:205:6/126	Enlace punto a punto
	sfp-sfpplus2	VLAN 110	172.16.0.0/24	2803:2540:0244::/64	Puerto GPON 0
		VLAN 111	172.16.1.0/24	2803:2540:0244:1::/64	Puerto GPON 1
		VLAN 112	172.16.2.0/24	2803:2540:0244:2::/64	Puerto GPON 2
		VLAN 113	172.16.3.0/24	2803:2540:0244:3::/64	Puerto GPON 3
		VLAN 114	172.16.4.0/24	2803:2540:0244:4::/64	Puerto GPON 4
		VLAN 115	172.16.5.0/24	2803:2540:0244:5::/64	Puerto GPON 5
		VLAN 116	172.16.6.0/24	2803:2540:0244:6::/64	Puerto GPON 6
		VLAN 117	172.16.7.0/24	2803:2540:0244:7::/64	Puerto GPON 7
		VLAN 118	172.16.8.0/24	2803:2540:0244:8::/64	Puerto GPON 8
		VLAN 119	172.16.9.0/24	2803:2540:0244:9::/64	Puerto GPON 9
		VLAN 120	172.16.10.0/24	2803:2540:0244:a::/64	Puerto GPON10
		VLAN 121	172.16.11.0/24	2803:2540:0244:b::/64	Puerto GPON11
		VLAN 122	172.16.12.0/24	2803:2540:0244:c::/64	Puerto GPON12
		VLAN 123	172.16.13.0/24	2803:2540:0244:d::/64	Puerto GPON13
		VLAN 124	172.16.14.0/24	2803:2540:0244:e::/64	Puerto GPON14
		VLAN 125	172.16.15.0/24	2803:2540:0244:f::/64	Puerto GPON15
	ether1	No asignada	10.0.112.1	No asignada	Gestión OLT
	ether2	No asignada	192.168.0.0/24	2803:2540:0244:10::/64	Red LAN
OLT	Puerto UPLink 10G	**TRUNK**			Todas las VLANS

Fuente: Elaborado por el autor

El proveedor Ufinet Nedetel, siguiendo las recomendaciones del (IETF RFC 6177, 2011), ha asignado a la empresa INFINIX INTENRET en el nodo de Cotacachi el bloque IPv6 2803:2540:23f::/48 destinado a la red interna. A partir de este bloque se realiza el correspondiente subneteo. En primer lugar, se determina un enlace punto a punto entre el router de borde Mikrotik RB4011 y el router de acceso Mikrotik CCR1009, utilizando para ello un direccionamiento /127, conforme a lo que indican las recomendaciones del (IETF RFC 6164, 2011). Posteriormente, se realiza la asignación de subredes /64 para cada uno de las 16 VLAN, correspondiente a los puertos PON activos de la tarjeta GPON de la OLT Cotacachi. De esta forma, la estructura de direccionamiento bajo el mecanismo Dual Stack para el nodo de Cotacachi queda definida como se muestra en la Tabla 15.

Tabla 15. Direccionamiento Dual Stack Nodo Cotacachi

Equipo	Interfaz	VLAN	Dirección IPv4	Dirección IPv6	Definido para
Mikrotik RB4011 Router de Borde	Ether1	**ENLACE WLAN**	177.234.323.11	Fd00:2021:172:205:2/126	Enlace Punto a punto
	Ether2	No asignada	10.0.111.1	No asignada	Gestión OLT
	sfp-sfpplus1	Enlace punto a punto a LAN	10.0.100.1	2803:2540:23f:ff01::/127	Red LAN hacia router de acceso
Mikrotik CCR1009 Router de acceso	sfp-sfpplus1	Enlace punto a punto con Borde	10.0.100.2	2803:2540:23f:ff02::/127	Conexión al equipo de borde
	sfp-sfpplus2	VLAN 210	172.21.0.0/24	2803:2540:23f::/64	Puerto GPON 0
		VLAN 211	172.21.1.0/24	2803:2540:23f:1::/64	Puerto GPON 1
		VLAN 212	172.21.2.0/24	2803:2540:23f:2::/64	Puerto GPON 2
		VLAN 213	172.21.3.0/24	2803:2540:23f:3::/64	Puerto GPON 3
		VLAN 214	172.21.4.0/24	2803:2540:23f:4::/64	Puerto GPON 4
		VLAN 215	172.21.5.0/24	2803:2540:23f:5::/64	Puerto GPON 5
		VLAN 216	172.21.6.0/24	2803:2540:23f:6::/64	Puerto GPON 6
		VLAN 217	172.21.7.0/24	2803:2540:23f:7::/64	Puerto GPON 7
		VLAN 218	172.21.8.0/24	2803:2540:23f:8::/64	Puerto GPON 8
		VLAN 219	172.21.9.0/24	2803:2540:23f:9::/64	Puerto GPON 9
		VLAN 220	172.21.10.0/24	2803:2540:23f:a::/64	Puerto GPON10
		VLAN 221	172.21.11.0/24	2803:2540:23f:b::/64	Puerto GPON11
		VLAN 222	172.21.12.0/24	2803:2540:23f:c::/64	Puerto GPON12
		VLAN 223	172.21.13.0/24	2803:2540:23f:d::/64	Puerto GPON13
		VLAN 224	172.21.14.0/24	2803:2540:23f:e::/64	Puerto GPON14
		VLAN 225	172.21.15.0/24	2803:2540:23f:f::/64	Puerto GPON15
OLT	UPLink 10G	**TRUNK**			Todas las VLANS

Fuente: Elaborado por el autor

3.3.4. Conexión de IPv6 en la interfaz WAN

El proceso de implementación empieza en la habilitación del soporte IPv6 en el router. La configuración mostrada mediante el comando *ipv6 settings /print* evidencia que el soporte IPv6 está habilitado y que el equipo funciona en modo enrutador, al tener habilitado el reenvío tráfico IPv6. Además, se establece que el router no aceptará mensajes de redireccionamiento ni anuncios de enrutadores externos cuando actúan como router, lo que refuerza la seguridad de red. Estos aspectos son fundamentales y se reflejan en la configuración presentada en la Figura 63.

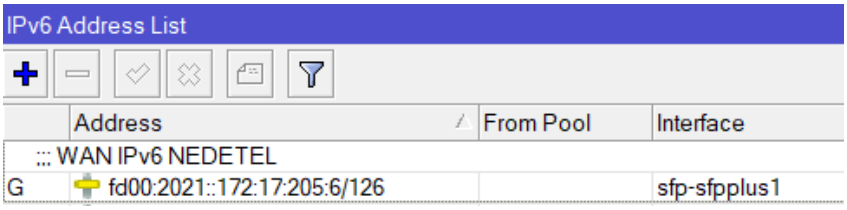
Figura 63. Verificar el soporte IPv6 en el router MikroTik

```
[infinix@ATUNTAQUI] > ipv6 settings/print
                    disable-ipv6: no
                         forward: yes
                 accept-redirects: yes-if-forwarding-disabled
  accept-router-advertisements: yes-if-forwarding-disabled
           max-neighbor-entries: 16384
```

Fuente: Equipos de administración de INFINIX INTERNET

En el router de administración se configura el enlace WAN IPv6, tal como muestra la Figura 64. Para ello, se asigna a la interfaz sfp-sfpplus1 la dirección IPv6 proporcionada para el ISP, estableciendo de esta manera la comunicación punto a punto entre la red del ISP con el equipo del proveedor. Esta configuración resulta esencial, ya que constituye la puerta de enlace hacia internet y permite garantizar la conectividad mediante el protocolo IPv6.

Figura 64. Dirección IPv6 correspondiente al router de administración



Fuente: Equipos de administración de INFINIX INTERNET

La Figura 65 muestra la configuración la ruta por defecto en IPv6. Esta configuración es fundamental para establecer que todo el tráfico destinado a redes externas sea enviado a

través del Gateway por defecto fd00:2021::172:17:205:5, correspondiente a la dirección del equipo del proveedor NEDETEL. Esta ruta asegura que el router tenga una vía definida hacia internet para cualquier dirección IPv6 que pertenezca a la red interna del ISP.

Figura 65. Configuración de la ruta por defecto en IPv6

```
[infinix@ATUNTAQUI] > /ipv6 route add dst-address=::/0 gateway
=FD00:2021::172:17:205:5 comment="Default IPv6 hacia Ufinet"
[infinix@ATUNTAQUI] >
```

Fuente: Equipos de administración de INFINIX INTERNET

En la Figura 66, se muestra la configuración del DNS en IPv6, la cual se implementa con el fin de garantizar el correcto funcionamiento la red y permitir que los usuarios finales accedan a los servicios mediante nombres de dominio.

Figura 66. Configuración de DNS en IPv6

```
[infinix@ATUNTAQUI] > /ip dns set servers=2001:4860:4860::8888
,2001:4860:4860::8844 allow-remote-requests=yes
```

Fuente: Equipos de administración de INFINIX INTERNET

Una vez concluida la configuración de IPv6 en el router, se procede a realizar una prueba de conectividad mediante el comando ping hacia la dirección IPv6 que está configurada en el equipo del proveedor. En la Figura 67 se evidencia que la respuesta de conectividad es satisfactoria, por lo que confirma que el enlace WAN está correctamente operativo. Con esta validación se asegura que el protocolo IPv6 esté activo y que los clientes del ISP dispondrán de la salida a internet a través de IPv6.

Figura 67. Prueba de conectividad del enlace WAN

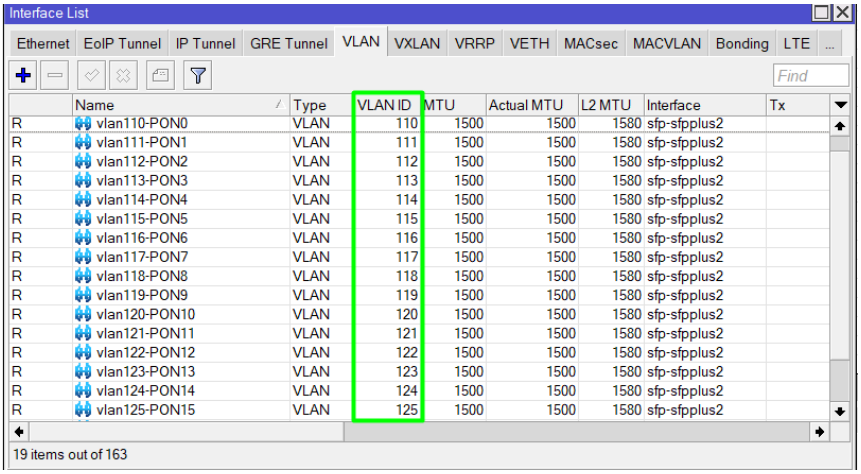
```
[infinix@ATUNTAQUI] > ping fd00:2021::172:17:205:5
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 fd00:2021::172:17:205:5                    56  64 1ms223us   echo reply
    1 fd00:2021::172:17:205:5                    56  64 1ms79us    echo reply
    2 fd00:2021::172:17:205:5                    56  64 1ms119us   echo reply
    3 fd00:2021::172:17:205:5                    56  64 1ms89us    echo reply
    4 fd00:2021::172:17:205:5                    56  64 1ms198us   echo reply
    5 fd00:2021::172:17:205:5                    56  64 1ms129us   echo reply
    6 fd00:2021::172:17:205:5                    56  64 1ms93us    echo reply
    7 fd00:2021::172:17:205:5                    56  64 1ms98us    echo reply
    8 fd00:2021::172:17:205:5                    56  64 1ms416us   echo reply
    9 fd00:2021::172:17:205:5                    56  64 1ms559us   echo reply
   10 fd00:2021::172:17:205:5                    56  64 1ms207us   echo reply
   11 fd00:2021::172:17:205:5                    56  64 1ms117us   echo reply
    sent=12 received=12 packet-loss=0% min-rtt=1ms79us avg-rtt=1ms193us max-rtt=1ms559us
```

Fuente: Equipos de administración de INFINIX INTERNET

3.3.5. Configuración de mecanismo Dual Stack

El uso de las VLANs constituye un aspecto fundamental en el diseño de la red, ya que se permite segmentar el tráfico y administrar de manera eficiente los recursos disponibles. En este caso, la OLT cuenta con una tarjeta GPON activa de 16 puertos PON, por lo que se asigna una VLAN a cada puerto como muestra la Figura 68. Estas VLANs se asocian a la interfaz sfp-sfppuls2, que mantiene la conexión directa con la OLT, permitiendo un control centralizado del tráfico. De esta manera se optimiza la administración de la red, y se mejora la seguridad al evitar tráfico cruzado entre diferentes clientes.

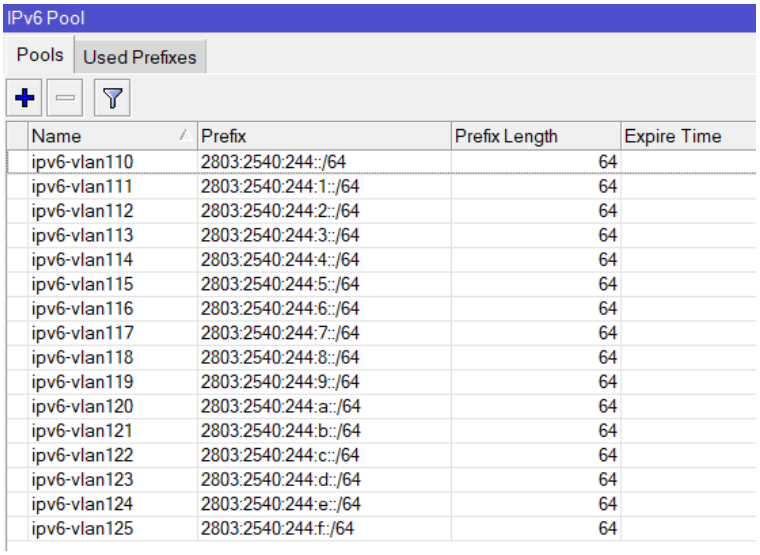
Figura 68. Crear VLANs para cada puerto PON



Fuente: Equipos de administración de INFINIX INTERNET

El direccionamiento de IPv6 se establece tomando como referencia los parámetros detallados en la Tabla 13. Se configura un pool al que se asigna un nombre identificativo y se le asocia un bloque con un prefijo /64, el cual es el estándar recomendado para las redes de acceso a cliente. Así mismo, se ajusta la longitud del prefijo /64 como muestra en la Figura 69 según los requerimientos de la infraestructura, lo que permite garantizar la correcta asignación de subredes y mantener escalabilidad de la red bajo el esquema de direccionamiento propuesto.

Figura 69. Direccionamiento IPv6 para cada VLAN

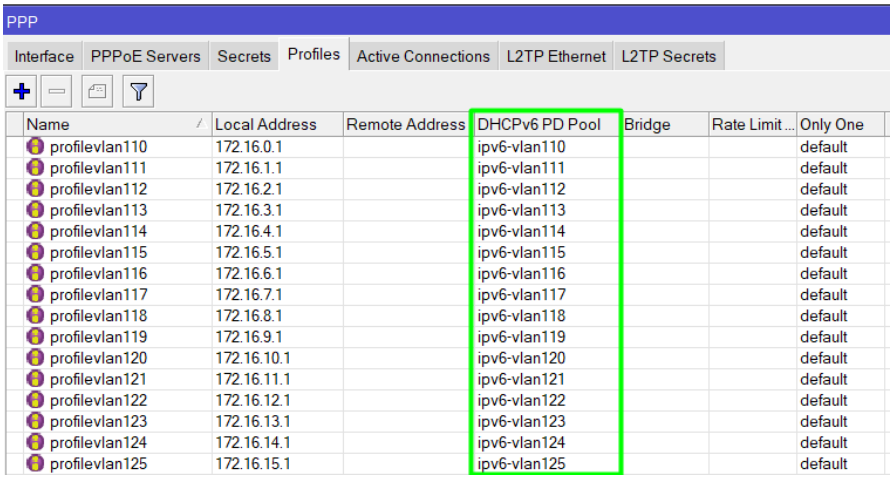


Name	Prefix	Prefix Length	Expire Time
ipv6-vlan110	2803:2540:244::/64	64	
ipv6-vlan111	2803:2540:244:1::/64	64	
ipv6-vlan112	2803:2540:244:2::/64	64	
ipv6-vlan113	2803:2540:244:3::/64	64	
ipv6-vlan114	2803:2540:244:4::/64	64	
ipv6-vlan115	2803:2540:244:5::/64	64	
ipv6-vlan116	2803:2540:244:6::/64	64	
ipv6-vlan117	2803:2540:244:7::/64	64	
ipv6-vlan118	2803:2540:244:8::/64	64	
ipv6-vlan119	2803:2540:244:9::/64	64	
ipv6-vlan120	2803:2540:244:a::/64	64	
ipv6-vlan121	2803:2540:244:b::/64	64	
ipv6-vlan122	2803:2540:244:c::/64	64	
ipv6-vlan123	2803:2540:244:d::/64	64	
ipv6-vlan124	2803:2540:244:e::/64	64	
ipv6-vlan125	2803:2540:244:f::/64	64	

Fuente: Equipos de administración de INFINIX INTERNET

A continuación, se procede con la configuración del servidor PPPoE, comenzando con la creación de los profiles correspondientes para cada VLAN tal cual detalla la Figura 70. En dichos profiles se definen los parámetros de direccionamiento IPv4 y se incorpora el direccionamiento IPv6 mediante la asociación de los pools configurados en IPv6 para cada VLAN, lo que permite establecer la conectividad en modo Dual Stack. De esta manera, queda determinado el esquema de direccionamiento IPv4 e IPv6 que recibirán los clientes finales, asegurando la coexistencia de ambos protocolos y garantizando compatibilidad con las aplicaciones y servicios actuales.

Figura 70. Creación de profile en Dual Stack

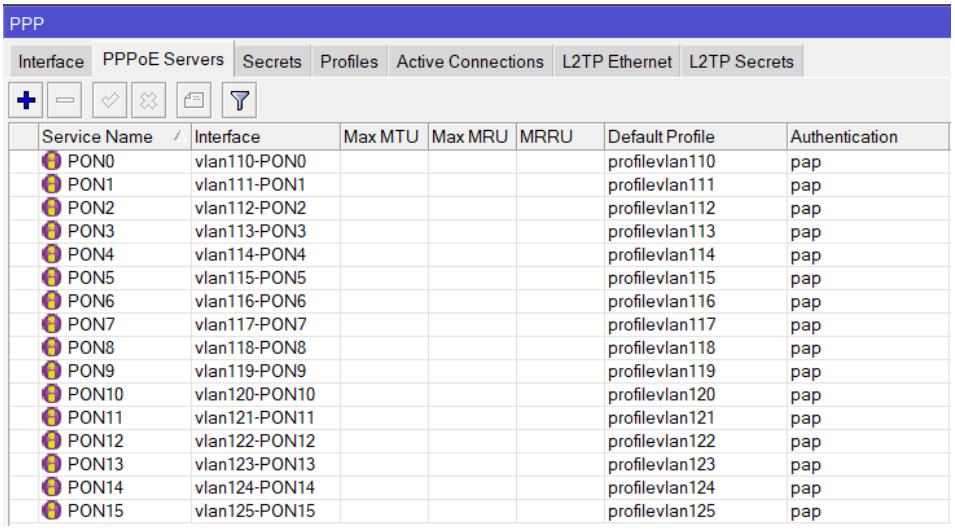


Name	Local Address	Remote Address	DHCPv6 PD Pool	Bridge	Rate Limit ...	Only One
profilevlan110	172.16.0.1		ipv6-vlan110			default
profilevlan111	172.16.1.1		ipv6-vlan111			default
profilevlan112	172.16.2.1		ipv6-vlan112			default
profilevlan113	172.16.3.1		ipv6-vlan113			default
profilevlan114	172.16.4.1		ipv6-vlan114			default
profilevlan115	172.16.5.1		ipv6-vlan115			default
profilevlan116	172.16.6.1		ipv6-vlan116			default
profilevlan117	172.16.7.1		ipv6-vlan117			default
profilevlan118	172.16.8.1		ipv6-vlan118			default
profilevlan119	172.16.9.1		ipv6-vlan119			default
profilevlan120	172.16.10.1		ipv6-vlan120			default
profilevlan121	172.16.11.1		ipv6-vlan121			default
profilevlan122	172.16.12.1		ipv6-vlan122			default
profilevlan123	172.16.13.1		ipv6-vlan123			default
profilevlan124	172.16.14.1		ipv6-vlan124			default
profilevlan125	172.16.15.1		ipv6-vlan125			default

Fuente: Equipos de administración de INFINIX INTERNET

Una vez definidos los profiles en modo Dual Stack, se procede a la creación del servidor PPPoE. Para ello, se asigna un nombre identificativo que corresponde a cada puerto PON y se especifica la interfaz asociada, en este caso, las VLANs creadas para cada puerto como muestra la Figura 71. Finalmente, se vincula el profile previamente configurado, en el cual se establece el direccionamiento IPv4 e IPv6 que será entregado a los clientes finales.

Figura 71. Configuración del servidor PPPoE



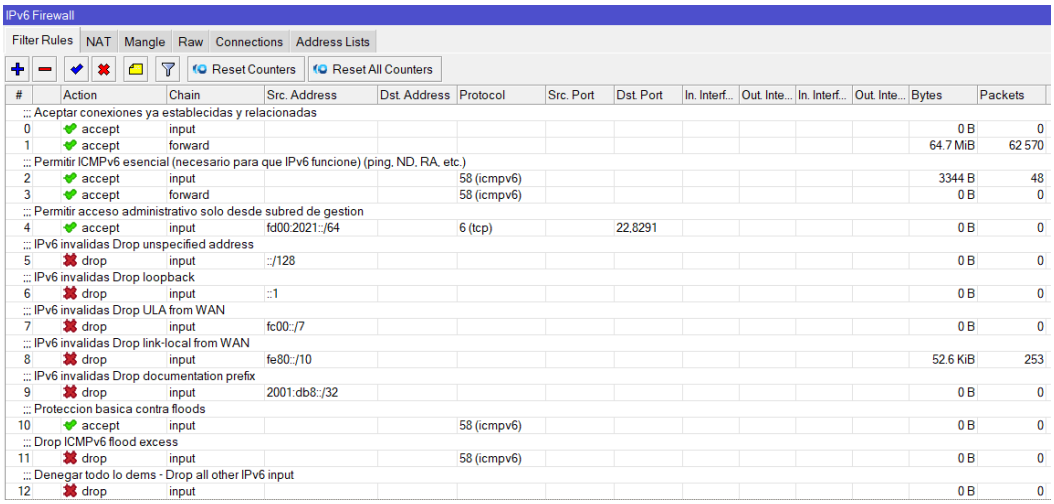
Service Name	Interface	Max MTU	Max MRU	MRRU	Default Profile	Authentication
PON0	vlan110-PON0				profilevlan110	pap
PON1	vlan111-PON1				profilevlan111	pap
PON2	vlan112-PON2				profilevlan112	pap
PON3	vlan113-PON3				profilevlan113	pap
PON4	vlan114-PON4				profilevlan114	pap
PON5	vlan115-PON5				profilevlan115	pap
PON6	vlan116-PON6				profilevlan116	pap
PON7	vlan117-PON7				profilevlan117	pap
PON8	vlan118-PON8				profilevlan118	pap
PON9	vlan119-PON9				profilevlan119	pap
PON10	vlan120-PON10				profilevlan120	pap
PON11	vlan121-PON11				profilevlan121	pap
PON12	vlan122-PON12				profilevlan122	pap
PON13	vlan123-PON13				profilevlan123	pap
PON14	vlan124-PON14				profilevlan124	pap
PON15	vlan125-PON15				profilevlan125	pap

Fuente: Equipos de administración de INFINIX INTERNET

Con la configuración en modo dual Stack, es fundamental brindar la seguridad en la transmisión de datos, proteger la red y garantizar una comunicación eficiente. Dicho esto, el firewall es determinado como una buena práctica de seguridad, ya que protege la red contra accesos no autorizados, evitando fugas de información, bloquea ataques comunes y permite únicamente el tráfico legítimo, contribuyendo así a mantener la integridad y la confiabilidad de los datos.

En la Figura 72 se detallan las reglas de seguridad implementadas, las cuales permiten conexiones válidas, habilitan el ICMPv6 para el correcto funcionamiento de IPv6. En cuanto a las restricciones, nos muestra que bloquea el acceso a equipos de administración de la red desde cualquier IPv6 no reconocida. Además, se bloquean direcciones inválidas para prevenir ataques. En cuanto a la protección del equipo, se determina una protección básica para sobrecarga del CPU y finalmente, se descarta todo el tráfico no definido, reforzando así la seguridad de la red.

Figura 72. Firewall en IPv6



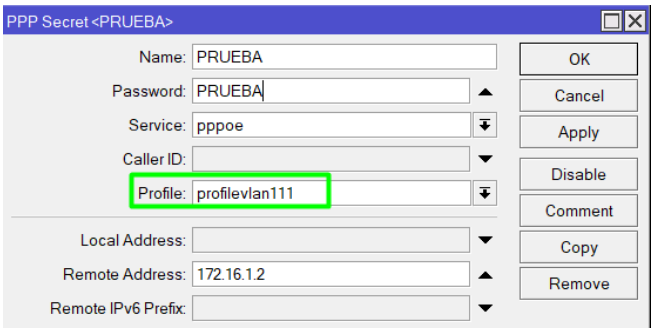
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interf...	Out. Inte...	In. Interf...	Out. Inte...	Bytes	Packets
;;; Aceptar conexiones ya establecidas y relacionadas													
0	accept	input										0 B	0
1	accept	forward										64.7 MiB	62 570
;;; Permitir ICMPv6 esencial (necesario para que IPv6 funcione) (ping, ND, RA, etc.)													
2	accept	input			58 (icmpv6)							3344 B	48
3	accept	forward			58 (icmpv6)							0 B	0
;;; Permitir acceso administrativo solo desde subred de gestion													
4	accept	input	fd00:2021::/64		6 (tcp)		22,8291					0 B	0
;;; IPv6 invalidas Drop unspecified address													
5	drop	input	::/128									0 B	0
;;; IPv6 invalidas Drop loopback													
6	drop	input	::1									0 B	0
;;; IPv6 invalidas Drop ULA from WAN													
7	drop	input	fc00::/7									0 B	0
;;; IPv6 invalidas Drop link-local from WAN													
8	drop	input	fe80::/10									52.6 KiB	253
;;; IPv6 invalidas Drop documentation prefix													
9	drop	input	2001:db8::/32									0 B	0
;;; Proteccion basica contra floods													
10	accept	input			58 (icmpv6)							0 B	0
;;; Drop ICMPv6 flood excess													
11	drop	input			58 (icmpv6)							0 B	0
;;; Denegar todo lo dems - Drop all other IPv6 input													
12	drop	input										0 B	0

Fuente: Equipos de administración de INFINIX INTERNET

Una vez finalizada la configuración en el equipo de administración, se procede a establecer la conexión con el usuario final. Para ello, se crea un PPP Secret destinado al usuario en el servidor PPPoE, tal como se muestra en la Figura 73. En esta configuración se define un profile que corresponde al puerto físico al cual está conectado el usuario final. Este profile proporciona una dirección IPv6, mientras que la dirección Remote

Address corresponde a la IPv4 del usuario. Esto confirma que la conexión está configurada en modo Dual Stack.

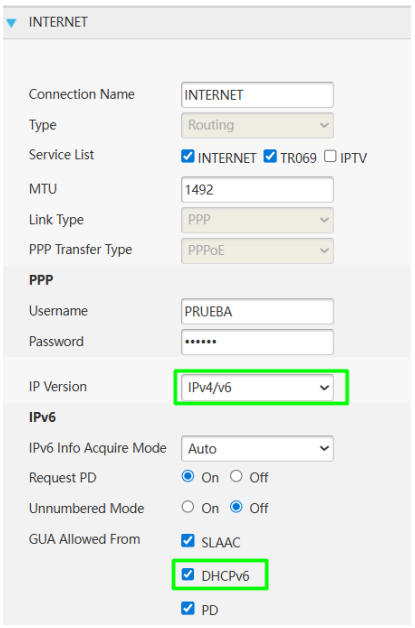
Figura 73. Crear usuario y contraseña para el usuario final



Fuente: Equipos de administración de INFINIX INTERNET

En el equipo del usuario final, se establece la conexión mediante PPPoE, utilizando el nombre de usuario y contraseña previamente configurados. Esta conexión permite enlazar el router de administración del ISP con el dispositivo terminal del usuario. En la Figura 74 se detalla esta configuración, así como la habilitación de los protocolos IPv4 e IPv6, lo que garantiza la convivencia entre estos dos protocolos de internet.

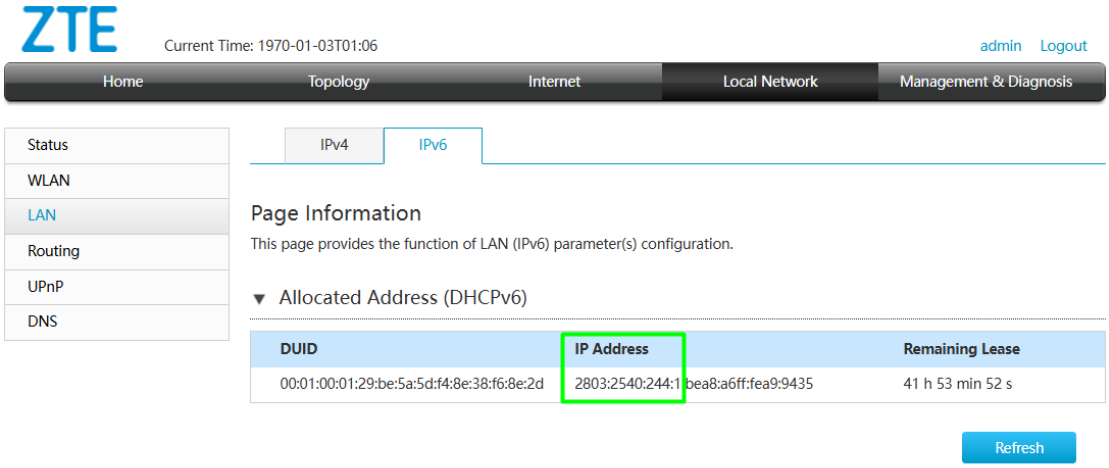
Figura 74. Configuración del interfaz internet en el equipo del usuario final



Fuente: Elaborado por el autor, pruebas de conectividad en el equipo del usuario

Una vez establecida la conexión, se verifica que el protocolo IPv6 mantiene una conexión de manera correcta. Tal como se muestra en la Figura 75, el direccionamiento configurado en el profile asignado al puerto PON1 se refleja correctamente en el equipo del usuario final. Esto conforma que cada usuario recibe una dirección IPv6 global única, válida para acceder a internet, garantizando así una comunicación directa sin necesidad de traducción de direcciones como ocurre en IPv4.

Figura 75. Dirección IPv6 en el equipo del usuario final

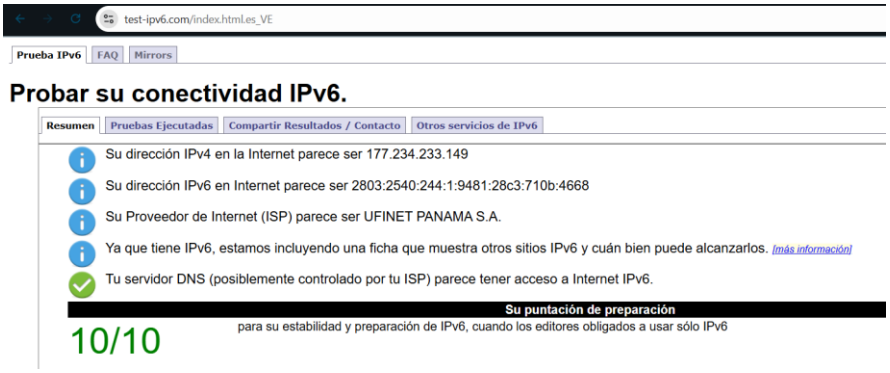


Fuente: Elaborado por el autor, pruebas de conectividad en el equipo del usuario

3.3.6. Resultados de conectividad en Dual Stack

Una vez finalizada la configuración, se procede a verificar la conectividad mediante la herramienta test-ipv6 en cualquier página web, la cual confirma la operabilidad del protocolo IPv6 junto A IPv4 tal como se muestra en la Figura 76. El resultado obtenido muestra una calificación de 10/10, lo que evidencia que la red cuenta con soporte completo para ambos protocolos y garantiza la transición adecuada hacia IPv6 sin afectar la conectividad existente.

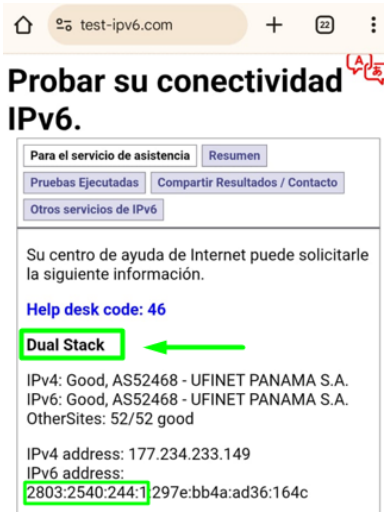
Figura 76. Test de conectividad a IPv6



Fuente: Elaborado por el autor, pruebas de conectividad en el ISP

La prueba de conectividad confirma que la red está operando en modo Dual Stakc tal como muestra la Figura 77, lo que significa que existen conectividad funcional tanto IPv4 como en IPv6 de forma simultánea. Los resultados muestran que ambos protocolos se encuentran activos bajo el proveedor UFINET. Así mismo, se evidencia la asignación de una dirección IPv6 pública del bloque 2803:2540:244::/64 lo que demuestra que el direccionamiento implementado en la red es reconocido y validado exitosamente. Estos resultados validan la correcta configuración del esquema Dual Stack y garantía la interoperabilidad de los servicios en la infraestructura del ISP.

Figura 77. Resultados de configuración Dual Stack



Fuente: Elaborado por el autor, pruebas de conectividad en el ISP

Los resultados de la configuración realizada confirma que la red de la empresa INFINIX INTERNET cuenta con soporte operativo en Ipv4 como e IPv6 bajo un esquema Dual Stakc. En la Figura 78 se muestra que el DNS responde correctamente en ambos protocolos, priorizando IPv6 en ambientes Dual Stack, y se comprobó la capacidad de transicion de paquetes grandes sin ningun inconveniente. Asi mismo, se evidencia que tanto IPv4 e IPv6 se encuentra asociado al ASN 52468 lo que garantiza soporte nativo y continuidad operativa en el proceso de migración hacia IPv6.

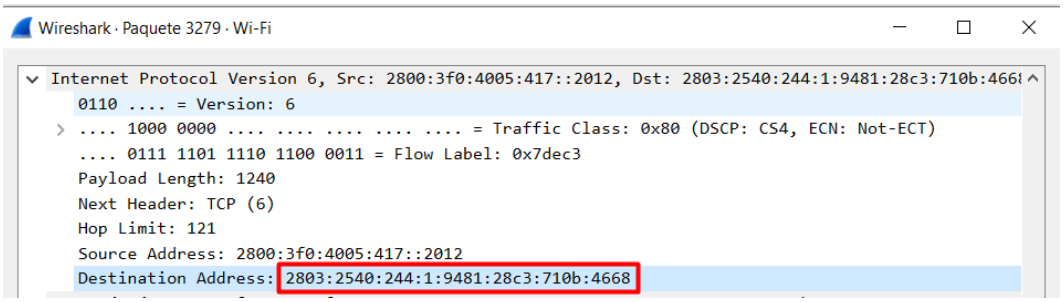
Figura 78. Resultados de transición al protocolo IPv6

Prueba con el registro DNS IPv4	**okey** (0.545s) usando ipv4
Prueba con el registro DNS IPv6	**okey** (0.534s) usando ipv6
Prueba con registro de doble pila DNS	**okey** (0.543s) usando ipv6
Prueba de doble pila DNS y paquete grande	**okey** (0.472s) usando ipv6
Prueba paquete grande de IPv6	**okey** (1.184s) usando ipv6
Prueba si el servidor DNS de su ISP utiliza IPv6	**okey** (0.616s) usando ipv6
Encontrar proveedor de servicios IPv4	**okey** (0.650s) usando ipv4 ASN 52468
Encontrar proveedor de servicios IPv6	**okey** (0.436s) usando ipv6 ASN 52468

Fuente: Elaborado por el autor, pruebas de conectividad en el ISP

Las capturas realizadas en el software de Wireshark permiten comprobar la presencia y correcta transición de paquetes bajo el protocolo IPv6. A través de esta herramienta se puede identificar el encabezado de IPv6 tal como se muestra en la Figura 79, donde nos muestra las direcciones de origen y destino, así como verificar que la comunicación se realiza de manera eficiente mediante el protocolo dual Stack. De esta forma, Wireshark se convierte en una evidencia técnica confiable que respalda la implementación del direccionamiento IPv6 en la red del ISP.

Figura 79. Capturas realizadas en Wireshark de paquetes IPv6



Nota: Fuente: Elaborado por el autor, pruebas de conectividad

Cada campo del paquete de datos nuestra información acerca de la comunicación IPv6/TCP, mostrando claramente los parámetros relevantes para el análisis de la red como:

- **Tipo de paquete:** IPv6 con protocolo de capa superior TCP (Next Header:6).
- **Dirección origen:** 2800:3f:4005:417::2012 dirección establecido a un dispositivo conectado a la red del usuario final.
- **Dirección destino:** 2803:2540:244:1:9481:28c3:710b:4668 dirección del equipo del usuario de acuerdo con el bloque establecido para el ISP.
- **Longitud de carga útil:** 1240 bytes es el tamaño de la carga útil en IPv6.
- **Hot Limit:** equivalente a TTL en IPv4 : 121
- **Clase de tráfico:** 0x80 que indica prioridad de tráfico IPv6 usado para garantizar un mejor tratamiento en la red frente a tráficos estándares como IPv4.
- **Etiqueta de flujo**: 0x7dec3, indica que los paquetes pertenecen a un flujo especifico de tráfico IPv6, lo que permite a los routers intermedios tratarlos con una política mejorada de calidad de servicio, así optimizando el rendimiento para aplicaciones sensibles al retardo.

La información confirma la plena operabilidad mediante el protocolo IPv6, así evidenciado una mayor flexibilidad y control en comparación con IPv4. Estos datos refuerzan la importancia de validar los campos comunicación en pruebas de laboratorio como parte del proceso de transición y despliegue en producción.

En el análisis del desempeño de la red es fundamental considerar parámetros de operabilidad que permitan evaluar de manera objetiva la calidad de servicio que se ofrece al usuario. Estos parámetros permiten identificar posibles problemas de rendimiento, garantizar la escalabilidad de las comunicaciones y validar la calidad de la comunicación. Entre los parámetros más relevantes a analizar son:

- **Latencia:** determina el tiempo que tarda el paquete de información en desplazarse desde el origen hacia el destino. Una latencia baja asegura una comunicación fluida y eso se evidencia en servicios de streaming.

- **Jitter:** Es la representación de la variación en los tiempos de llegada de los paquetes. Si el jitter es alto puede provocar pérdidas de comunicación.
- **Pérdidas de paquetes:** Es el porcentaje de paquetes enviados que no llegan a su destino. Este parámetro refleja directamente la confiabilidad de la red. Si el valor es alto compromete la calidad del servicio, afectando la transmisión de datos.

Para este estudio, se realizaron mediciones de cada uno de estos parámetros en diferentes días y horarios, para verificar el comportamiento de la red. Tal como se detalla en la Tabla 16 en la operabilidad del protocolo IPv4 se establecieron 5 muestras independientes para cada parámetro, de las cuales se calcula un promedio con el fin de analizar el comportamiento de la red.

Tabla 16. Parámetros de operabilidad de la red en IPv4

Periodo de muestra en IPv4	**Latencia**	**Jitter**	**Pérdida de paquetes**
1	12 ms	1.62 ms	0%
2	10 ms	1.83 ms	2%
3	9 ms	1.41 ms	1%
4	9 ms	1.33 ms	2%
5	11 ms	1.57 ms	0%
Promedio	**10.2 ms**	**1.55 ms**	**1%**

Fuente: Elaborado por el autor

En la Tabla 17 se muestra los parámetros de operabilidad correspondiente al protocolo IPv6 aplicando el mismo procedimiento utilizado en el análisis de IPv4. También se realiza cinco mediciones de cada parámetro en diferentes intervalos de tiempo con el fin de obtener datos consistentes y representativos del comportamiento de la red.

Tabla 17. Parámetros de operabilidad de la red en IPv6

Periodo de muestra en IPv6	Latencia	Jitter	Pérdida de paquetes
1	6 ms	1.27 ms	0%
2	7 ms	1.18 ms	0%
3	7 ms	1.15 ms	1%
4	8 ms	1.21 ms	0%
5	5 ms	1.23 ms	1%
Promedio	**6.6 ms**	**1.20 ms**	**0.4%**

Fuente: Elaborado por el autor

Los resultados obtenidos establecen que bajo el protocolo IPv6 los parámetros de operabilidad representan un desempeño más favorable en comparación con IPv4. La latencia promedio en IPv6 es 6.6 ms frente a 10.2 ms en IPv4, lo que refleja que se tiene mejor tiempo de respuesta. De igual forma, el jitter muestra mayor estabilidad con 1.20 ms en comparación con 1.55 ms que se obtiene en la red IPv4. En cuanto a la pérdida de paquetes, el valor disminuye a 0.4% en IPv6 frente a 1% en IPv4, lo que determina una mayor confiabilidad en la entrega de la información. El análisis de estos resultados demuestra de manera concreta que la red, al operar con el protocolo IPv6, alcanza un mejor rendimiento y estabilidad.

Por otra parte, en cuanto a la resolución del DNS, en la red IPv6 el tiempo de respuesta promedio es de 38 ms, mientras que en IPv4 varía entre 20 a 60 ms. En muchos casos, la resolución mediante IPv4 puede ser más eficiente debido a la mayor disponibilidad de servicios que operan bajo este protocolo, mientras que el soporte IPv6 continúa en un proceso de consolidación.

3.3.7. Riesgos y contingencias en la transición de IPv4 a IPv6

La migración hacia IPv6 conlleva diversos riesgos técnicos y operativos que deben ser gestionados de manera ordenada para asegurar la continuidad del servicio. A continuación, se detallan los principales riesgos y las medidas de contingencias correspondientes para mantener la operabilidad de la red:

- **Compatibilidad de equipos:** Uno de los mayores riesgos es tener operativos equipos que no soportan de manera nativa el protocolo IPv6. Esto podría provocar interrupciones en la red y limitar la adopción del protocolo.
  Medida de contingencia: Antes de realizar cualquier configuración, se procede a elaborar un inventario de equipos, verificar la compatibilidad del protocolo IPv6 y por última instancia, sustituir equipos obsoletos antes de la migración.
- **Errores de configuración:** La mala asignación de direcciones IP a las interfaces o a los equipos no correspondientes puede causar pérdida de conectividad hacia internet.
  Medida de contingencia: Implementar pruebas de laboratorio, aplicar el mecanismo de transición de manera gradual, documentar todas las configuraciones y disponer un plan de operabilidad mediante IPv4.
- **Fallas en mecanismos de transición:** El mecanismo de transición puede generar latencias o problemas de acceso a ciertos servicios si no están bien implementados.
  Medida de contingencia: Realizar un monitoreo constante de la red en entornos de producción y ajustar prioridades de enrutamiento para favorecer IPv6 siempre que sea posible.
- **Riesgos de seguridad:** Las reglas de firewall establecen un mecanismo de seguridad de la red, la ausencia de estas puede exponer la red a vulnerabilidades.
  Medida de contingencia: Establecer políticas de seguridad específicas para IPv4 e IPv6, aplicando un monitoreo activo con herramientas como Wireshark y realizar audiencias periódicas de las configuraciones de la red.
- **Sobrecargas de recursos en los equipos:** La coexistencia de dos protocolos puede aumentar el consumo del CPU y la memoria en routers.

Medida de contingencia: Supervisar el uso de los recursos en tiempo real, optimizar tablas de enrutamiento y planificar la migración de manera escalonada para distribuir la carga progresivamente.

- **Impacto en los usuarios finales:** Algunos dispositivos de los usuarios finales pueden no ser compatibles con IPv6 o pueden requerir ajuste de configuración adicional.

  Medida de contingencia: Realizar prueba piloto con un grupo reducido de usuarios, mantener la coexistencia de IPv4 e IPv6 y tener guías claras de la configuración de la red.

Discusión general del objetivo 3

El desarrollo del esquema de direccionamiento IPv6 para la red de la empresa INFINIX INTERNET permitió verificar la disponibilidad de los recursos en los equipos activos existentes, los cuales validan la compatibilidad de hardware asegurando la viabilidad de la transición. La solicitud de bloques de direccionamiento IPv6 al proveedor Ufinet Nedetel fue un paso fundamental, ya que esto garantiza que la red cuente con un bloque de direccionamiento oficial y estable. Por lo tanto, se constituye un plan de direccionamiento basado en el mecanismo de transición Dual Stack, el cual asegura la coexistencia eficiente de IPv4 e IPv6 durante el proceso de migración.

La implementación del esquema de direccionamiento adoptó como referencia las recomendaciones de los estándares internacionales, en particular el RFC 4291, que indica la estructura general de las direcciones IPv6 y su asignación para subredes el prefijo /64, así como el RFC 6164, que recomienda el uso del prefijo /127 en enlaces punto a punto. Estas recomendaciones impuestas por el Grupo de Trabajo de la Ingeniería en Internet (IETF) garantizan que el direccionamiento propuesto sea sostenible, estandarizado y alineado con las buenas prácticas de la ingeniería en telecomunicaciones.

De igual forma, se detalla un plan de riesgos y contingencias que permite anticipar posibles fallos durante la transición. Dicho plan establece medidas correctivas y preventivas que fortalecen la confiabilidad del proceso y asegura una transición controlada y segura. Además, las pruebas de parámetros de operabilidad evidenciaron que la red bajo el protocolo IPv6 ofrece mejor rendimiento, menor latencia, menor jitter y

menor pérdida de paquetes en comparación con IPv4, confirmando que el nuevo protocolo garantiza mayor confiabilidad en la prestación del servicio.

En general, todo lo especificado en el objetivo 3 justifica la necesidad de adoptar IPv6, no solo por la escasez de direcciones IPv4, sino también por las ventajas técnicas y operativas que aporta. La implementación de este protocolo brinda un espacio de direccionamiento prácticamente ilimitado, facilitando organizar la red de manera jerárquica mediante subredes claras, optimizando la gestión de recursos. Por lo tanto, el objetivo planteado se cumple plenamente, ya que la empresa contará con una red más estable, preparada para el crecimiento de sus usuarios y servicios, y con la capacidad de responder a las demandas de nuevas aplicaciones que requieran mayor estabilidad y rendimiento.

Conclusiones generales del Capítulo 3

El desarrollo del capítulo permitió cumplir los objetivos planteados. El diagnóstico de la red actual evidenció limitaciones de direcciones IPv4, como baja escalabilidad y riesgos de saturación, lo que justifica la necesidad de migrar a IPv6 para garantizar sostenibilidad a largo plazo. En segundo lugar, la selección de mecanismo de transición se fundamenta en la investigación teórica, técnica y en las recomendaciones de los principales RFCs. De tal forma, se concluye que Dual Stack es la opción más viable, ya que permite la coexistencia ordenada de ambos protocolos y asegura la continuidad en los servicios durante la transición.

Finalmente, el diseño del esquema de direccionamiento IPv6 se plasma como una propuesta robusta y escalable, probada en un entorno de laboratorio validando la configuración en equipos de telecomunicaciones. La implementación con prefijos adecuados para las subredes y las pruebas de conectividad confirma el correcto funcionamiento del mecanismo Dual Stack evidenciando estabilidad y capacidad de crecimiento de la red.

La migración hacia IPv6 en la empresa INFINIX INTERNET resulta técnicamente viable y aporta beneficios en escalabilidad, seguridad y expansión de la red frente a las demandas tecnológicas presentes y futuras.

CONCLUSIONES

- El constante avance tecnológico y la masiva conexión de dispositivos a internet en hogares y empresas hacen que IPv6 se convierta en una necesidad fundamental para los ISPs. Sus características permiten responder a los crecientes requerimientos de las comunicaciones, asegurando escalabilidad, eficiencia y soporte para la evolución de los servicios digitales.
- Un proceso adecuado de transición de protocolo requiere un levantamiento detallado del estado de la red y de los equipos de telecomunicaciones, con el propósito de verificar que cuenten con el soporte necesario para la integración del protocolo IPv6.
- En el desarrollo del proyecto se estudiaron los diferentes mecanismos de transición para la implementación del protocolo IPv6, lo que permitió concluir que la transición debe realizarse de manera gradual. En este proceso, los protocolos IPv4 e IPv6 deben coexistir con el fin de no interrumpir la operabilidad de la red de la empresa INFINIX INTERNET.
- El mecanismo de transición más adecuado para la implementación en la infraestructura actual es Dual Stack, ya que permite el uso simultáneo de los protocolos IPv4 e IPv6, evitando así problemas de conectividad hacia internet.
- La escalabilidad de la red constituye un beneficio importante en la implementación del protocolo IPv6, ya que facilita el diseño del plan de direccionamiento. Al contar el proveedor con un bloque de direcciones /48, se dispone de un amplio conjunto de direcciones IPv6 asignables a los clientes, lo que permite un crecimiento eficiente de la red.

RECOMENDACIONES

- En la actualidad, un buen porcentaje de servicios y aplicaciones continúan operando únicamente sobre el protocolo en IPv4 y aún no disponen de soporte IPv6. Por ello, resulta recomendable mantener la coexistencia de ambos protocolos hasta que la migración se complete, proceso que probablemente tomará un par de años más.
- Es fundamental realizar el proceso de verificación del soporte IPv6 en todos los equipos de telecomunicación, tanto en los servidores del ISP como en los equipos de los usuarios finales. La finalidad de esto es garantizar su correcta funcionalidad y evitar conflictos de operabilidad. En los casos en que los equipos no cumplan con el soporte IPv6, se recomienda actualizar el IOS o, en última instancia, reemplazarlos por dispositivos compatibles con IPv6.
- La implementación del mecanismo de transición Dual Stack constituye una alternativa viable, ya que permite configurar y realizar pruebas de conectividad en IPv6 sin afectar la operabilidad de la red basada en IPv4.
- Se recomienda aprovechar el bloque /48 asignado al ISP para estructurar un esquema de direccionamiento IPv6 organizado, que facilite la administración de la red y permita su crecimiento futuro de manera ordenada.
- Documentar las configuraciones, el plan de direccionamiento y los procesos de cambios en la red, con el fin de facilitar el mantenimiento y agilizar la resolución de problemas en caso de alguna eventualidad que pase en la red.

REFERENCIAS

Academy. (2023, May 22). *NAT y la transición a IPv6: ¿Seguirá siendo relevante el NAT en el futuro? - abcXperts*. https://abcxperts.com/nat-y-la-transicion-a-ipv6-seguira-siendo-relevante-el-nat-en-el-futuro/?srsltid=AfmBOoozxdYV_-yYRh8uBLUP3AaOUB_1dxwWOtnZnWHM6fH9ADNB543j

Aguirre, V. (2023). *DIAGNÓSTICO Y PERSPECTIVAS DE LA IMPLEMENTACION DE IPV6 EN EL ECUADOR*. Escuela Politécnica Nacional.

Al-Azzawi, A., & Lencse, G. (2024). *Methodology for the security analysis of IPv4-as-a-Service IPv6 transition technologies*.

AlEnezi, A. G., & AlDhamen, M. F. (2023). A Comparative Study between IPv4 and IPv6. *IJARCCE*, *12*(3). https://doi.org/10.17148/ijarcce.2023.12310

Arco, J., & Gallego, J. (2023). *Instalación y Mantenimiento de Redes para Transmisión de Datos*. https://www.google.com.ec/books/edition/CFGB_Instalaci%C3%B3n_y_mantenimiento_de_red/G0HGEAAAQBAJ?hl=es&gbpv=1&dq=IPv6+2023&pg=PA16&printsec=frontcover

Ashraf, Z., Sohail, A., Latif, S., Hameed, A., & Yousaf, M. (2023). Challenges and Mitigation Strategies for Transition from IPv4 Network to Virtualized Next-Generation IPv6 Network. *International Arab Journal of Information Technology*, *20*(1), 78–91. https://doi.org/10.34028/iajit/20/1/9

Cañas, R. (2023). *COMPARATIVO DE RENDIMIENTO EN PROTOCOLOS - ANALISIS COMPARATIVO DE RENDIMIENTO EN PROTOCOLOS IPv4 e IPv6 COMO ESTRATEGIA PARA MEJORAR LA CALIDAD DEL SERVICIO EN LA RED INALAMBRICA DE LA UNIVERSIDAD DE LA COSTA*.

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. Universidad Tecnológica del Perú*.

Crocetta Yanuario, V. R. (2025). Protocolo IPv6 como solución estratégica en la administración de redes. *Revista Multidisciplinar Epistemología de Las Ciencias*, *2*(3), 1–27. https://doi.org/10.71112/G5DR6M65

Esteban, J., Santiago, S., Sistemas, I., Andrés, C., Venegas, S., Camilo, J., Velásquez, H., Santiago, C. P., & Gestión De Información, M. (2020). Proposal for the implementation of IPv6 in an operational IPv4 infrastructure. *Industry, Innovation, And Infrastructure for Sustainable Cities and Communities*, 24–26. https://doi.org/10.18687/LACCEI2019.1.1.300

GAD Antonio Ante. (2024). *Gobierno Autonomo Descentralizado Municipal de Antonio Ante*. https://www.antonioante.gob.ec/AntonioAnte/

GAD Municipal Santa Ana de Cotacachi. (2023). *GAD Municipal Santa Ana de Cotacachi*. https://cotacachi.gob.ec/

Gallegos, K. (2024). *Plan de transición de IPv4 a IPv6 en una red LAN*.

Hossain, Md., Binti, J., & Uddin, Md. (2024). A Review Paper on IPv4 and IPv6: A Comprehensive Survey. *American Journal of Computer Science and Technology*, *7*(4), 170–175. https://doi.org/10.11648/j.ajcst.20240704.14

Hsu, A., Li, F., Pearce, P., & Gasser, O. (2024). *A First Look At NAT64 Deployment In-The-Wild*. http://arxiv.org/abs/2311.04181

Hu, T., Dubois, D. J., & Choffnes, D. (2024). *IoT Bricks Over v6: Understanding IPv6 Usage in Smart Homes*. 17. https://doi.org/10.1145/3646547

Huawei. (2024). *Pila dual IPv4/IPv6*. https://info.support.huawei.com/hedex/api/pages/EDOC1000053358/YEF0907R/25/resources/en-us_concept_0133037101.html

IETF RFC 4213. (2018, April). *RFC 4213 - Mecanismos básicos de transición para hosts y enrutadores IPv6*. https://datatracker.ietf.org/doc/html/rfc4213

IETF RFC 4291. (n.d.). *RFC 4291- Arquitectura de direccionamiento IP versión 6*. Retrieved September 7, 2025, from https://datatracker.ietf.org/doc/html/rfc4291

IETF RFC 6164. (2011). *RFC 6164 - Using 127-Bit IPv6 Prefixes on Inter-Router Links*. https://doi.org/10.17487/rfc6164

IETF RFC 6177. (2011). *RFC 6177-Asignación de direcciones IPv6 a sitios finales*. https://datatracker.ietf.org/doc/html/rfc6177

IETF RFC 6180. (2011, May). *RFC 6180: Directrices para el uso de mecanismos de transición de IPv6 durante la implementación de IPv6*. https://www.rfc-editor.org/rfc/rfc6180.html

IETF RFC8200. (2017). *Internet Engineering Task Force (IETF). Internet Protocol, Version 6 (IPv6)*. 42. https://datatracker.ietf.org/doc/html/rfc8200#section-3

Igulu, K., Onuodu, F., & Singh, T. P. (2024). IPV6: Strengths and Limitations. In *Internet of Things: Vol. Part F2482* (pp. 147–172). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-97-0052-3_8

Iniobong, A. M., Ibitoye, A., Odesanya, A. &, & Idowu, O. (2022). Analysis and Optimization of IPv4 and IPv6 Transition Technologies. In *International Journal of Innovative Science and Research Technology* (Vol. 7, Issue 3). www.ijisrt.com388

IPv6-Google. (2025, September 16). *IPv6 – Google*. https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

ITF, (Instituto Federal de Telecomunicaciones). (2024). *IPv6 Mejorado: Impulsando la redes de próxima generación de México con IPv6 mejorado.* https://www.ift.org.mx/sites/default/files/contenidogeneral/politica-regulatoria/whitepaperipv6terminado.pdf

Jadhav, S. S., & Ballal, B. R. (2022). Review of IPv4 and IPv6 and various implementation methods of IPv6. *International Research Journal of Engineering and Technology*, *09*(12 DEC 2022). www.irjet.net

Kane, A. (2025). Navigating the Transition: Challenges and Benefits of Shifting from IPv4 to IPv6 in a Rapidly Evolving Internet Landscape. *International Journal of*

Internet and Distributed Systems, *07*(02), 21–34. https://doi.org/10.4236/ijids.2025.72002

Kasunic, N., Mitrovic, O., & Tadic, V. (2024). Empirical Analysis of IPv4 and IPv6 Protocol Performance in End-user Environment. *2024 47th ICT and Electronics Convention, MIPRO 2024 - Proceedings*, 795–799. https://doi.org/10.1109/MIPRO60963.2024.10569599

Khadiri, K., Kamoun, N. EL, Labouidya, O., Khadiri, K. EL, Ouaham, S. EL, Smahi, K., & Hilal, R. (2023). PERFORMANCE AND SCALABILITY OF IPV4/IPV6 TRANSITION MECHANISMS FOR REAL-TIME APPLICATIONS. *Article in Journal of Theoretical and Applied Information Technology*, *15*(23). https://www.researchgate.net/publication/377408314

Li, K. H., & Wong, K. Y. (2021). Empirical analysis of ipv4 and ipv6 networks through dual-stack sites. *Information (Switzerland)*, *12*(6). https://doi.org/10.3390/info12060246

Li, Z., & Qiu, J. (2021). Internet Protocol Version 6 Migration. *Proceedings - 2021 5th International Conference on Imaging, Signal Processing and Communications, ICISPC 2021*, 77–82. https://doi.org/10.1109/ICISPC53419.2021.00022

Loid Garcia, M., Rizal Ext West Rembo, J., City, M., Marie Espares, A., Forfieda, J., Nicole Garcia, A., Loid Serdina, M., & Rey, J. (2022). *A Comparative Study of IPv4 and IPv6 Protocols UNIVERSITY OF MAKATI A Comparative Study of IPv4 and IPv6 Protocols*. https://www.researchgate.net/publication/361108744

MikroTik. (2022). *CCR1009-7G-1C-1S_210502*. https://i.mt.lv/cdn/product_files/CCR1009-7G-1C-1S_210502.pdf

Mikrotik. (2022). *RB4011-RM_180930, The 4011 series fuel your network.*

MikroTik. (2023). *CCR2116-12G-4S+ 10G networking meets the unparalleled power of a modern ARM CPU*.

Novoa, J. (2022). *Transición de una red IPv4 a IPv6 manteniendo la coexistencia de los protocolos*.

Ordabayeva, G. K., Othman, M., Kirgizbayeva, B., Iztaev, Z. D., & Bayegizova, A. (2020, September 14). A systematic review of transition from IPV4 to IPV6. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3410352.3410735

Paucar, P., & Jativa, A. (2022). *DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACION DE IPV6*.

Piñeros, J., Ortiz, J., & Serrato, Y. I. (2022). *Analysis of the level of implementation in Information Security of the IPv6 protocol in a Government Entity*. https://repository.libertadores.edu.co/server/api/core/bitstreams/a2c1cafa-7bc9-47e3-a270-089f05d8cd47/content

Qaid, A., & Ertug, O. (2021). Transition from IPv4 to IPv6 Mechanisms by GNS3 Emulation: YPTC as a Case Study. *2021 International Symposium on Networks, Computers and Communications, ISNCC 2021*. https://doi.org/10.1109/ISNCC52172.2021.9615647

Rubio, S. (2022). *IMPLEMENTACIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) PARA LA PRESTACIÓN DE ALGUNOS SERVICIOS WEB EN LA UNIVERSIDAD DE CÓRDOBA.* https://repositorio.unicordoba.edu.co/server/api/core/bitstreams/cd994d69-2c47-4854-98b1-0edce93ac34b/content

Saade, S., Paraván, C., Lutz, F., & Bilbao, J. (2020). *Protocolo IPv6: fundamentos y aplicaciones*.

Salcan, C. (2024). *Prototipo de un Sistema en GNS3 con la Integración de Asterisk y Postgre SQL sobre IPv6 para Consulta de notas académicas*.

Sánchez, E., Arias Figueroa, D., & Alves De Godoy, H. (2024). *Análisis de Seguridad del Proceso de Configuración Automática de Direcciones IPv6 Sin Estado (SLAAC)*. https://sedici.unlp.edu.ar/bitstream/handle/10915/176653/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Shahid, K., Ahmad, S. N., & Rizvi, S. T. H. (2024). Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems. *Future Internet*, *16*(9). https://doi.org/10.3390/fi16090339

Socas, R., & Gómez, L. (2023). *Redes de ordenadores; principios y aplicaciones para la Ingeniería del Software*. 232.

Torres, K. (2022). *PLAN DE MIGRACIÓN DE IPV4 A IPV6 DE REDES INALAMBRICAS PARA PEQUEÑAS Y MEDIANAS EMPRESAS*.

UPN. (2022). POLÍTICAS DE SEGURIDAD IPv6. *Universidad Pedagógica Nacional*.

Viveros, J. (2024). *REDISEÑO DE LA RED DE DATOS DE LA ALCALDÍA MUNICIPAL DE EL CERRITO VALLE, QUE PERMITA PARA LA MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6*. https://red.uao.edu.co/server/api/core/bitstreams/ed8b54f5-1e26-4df4-800b-d81ee860547b/content

Xu, Bing., & Mou, Kefen. (2020). *Research on IPv6 network construction and application in Higher Vocational Colleges -Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2020) : June 12-14, 2020, Chongqing, China*. IEEE Press.

Xu, G. (2021). Research on the application of the IPv6 network protocol. *Journal of Physics: Conference Series*, *2031*(1). https://doi.org/10.1088/1742-6596/2031/1/012040

Zhang, Y., Fu, Y., & Wang, Q. (2024). IPv4 to IPv6 Transition Strategy Based on Dual Stack Protocol. *Advances in Transdisciplinary Engineering*, *47*, 428–435. https://doi.org/10.3233/ATDE231216

ANEXOS

Anexo 1: Solicitud al proveedor de la habilitación IPv6 en el nodo Atuntaqui

TICKET:359464 HABILITACIÓN IPV6 CLIENTE:FERNANDEZ CATUCUAGO SERGIO

Ricardo P. Gomez Salcedo <rgomezs@ufinet.com>
para mí, Grupo, Alexander, Joao

Parece que este mensaje está en inglés
Traducir al español

@srfernandezc@gmail.com buen día,

Se informa que se ha habilitado IPv6 en su servicio, se asigna el prefijo 2803:2540:244::/48.

Pruebas previas al enrutamiento con el prefijo asignado:

Salida a Internet:

```
ECIMATNEGARCPUFNEGALLEGO1#ping 2001:4860:4860::8888 sou 2803:2540:244::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4860:4860::8888, timeout is 2 seconds:
Packet sent with a source address of 2803:2540:244::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/24/28 ms
ECIMATNEGARCPUFNEGALLEGO1#ping 2001:468:D01:33::80DF:3367 sou 2803:2540:244::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:468:D01:33::80DF:3367, timeout is 2 seconds:
Packet sent with a source address of 2803:2540:244::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 156/188/200 ms
```

Respuesta desde Internet

```
route-views>ping 2803:2540:244::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2803:2540:244::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 153/153/154 ms
```

Anexo 2: Solicitud al proveedor de la habilitación IPv6 en el nodo Atuntaqui

TICKET:359444 HABILITACIÓN IPV6 CLIENTE:FERNANDEZ CATUCUAGO SERGIO

Ricardo P. Gomez Salcedo <rgomezs@ufinet.com>
para mí, Grupo, Alexander, Joao

Parece que este mensaje está en inglés
Traducir al español

@srfernandezc@gmail.com buen día,

Se informa que se ha habilitado IPv6 en su servicio, se asigna el prefijo 2803:2540:23F::/48.

Pruebas previas al enrutamiento con el prefijo asignado:

Salida a Internet:

```
ECIMCOTEGARCPUFNEGALLEG01#ping 2001:4860:4860::8888 source 2803:2540:23F::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:4860:4860::8888, timeout is 2 seconds:
Packet sent with a source address of 2803:2540:23F::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/20 ms
ECIMCOTEGARCPUFNEGALLEG01#ping 2001:468:D01:33::80DF:3367 source 2803:2540:23F::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:468:D01:33::80DF:3367, timeout is 2 seconds:
Packet sent with a source address of 2803:2540:23F::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/152/152 ms
```

Respuesta desde Internet:

```
route-views>ping 2803:2540:23F::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2803:2540:23F::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 177/201/215 ms
```