Experimental Implementation and Validation of an IPv6-Based Web Service in a Virtualized Environment for Higher Education Institutions

Pérez-Samanamud, Miguel V., Doctor[1], Rojas-Huamaní, Daniel, Magíster[1], Cevallos-Echevarría, Alejandro N., Magíster[1]
[1] Universidad Nacional Federico Villarreal, Perú, *mperezsa@unfv.edu.pe, drojas@unfv.edu.pe, acevallosl@unfv.edu.pe*

Abstract* – The transition from IPv4 to IPv6 remains a significant challenge for higher education institutions due to infrastructure constraints, operational risks, and the need to ensure service continuity during deployment. This study presents the experimental implementation and functional validation of an IPv6-based web service within a controlled virtualized environment using open-source software as a reproducible migration strategy. A quantitative, applied, descriptive–experimental approach was adopted by designing a laboratory environment composed of virtual machines implementing an authoritative DNS server, a web server, and a client configured with IPv6 addressing. Functional validation was performed through DNS name resolution using AAAA records and verification of web service accessibility over IPv6. The experimental results confirmed the correct integration of IPv6 addressing, DNS configuration, and HTTP services, enabling successful domain name resolution and retrieval of the corresponding IPv6 address by the client. The proposed methodology demonstrated the technical feasibility of deploying IPv6-based web services in a reproducible and low-cost virtualized environment without affecting institutional production infrastructures. The study contributes a practical and replicable migration strategy that can support higher education institutions in planning, validating, and progressively adopting IPv6 services while reducing operational risks associated with real-world deployment.

***Keywords*-- IPv6, DNS, Web Service, Virtualized Environment, IPv6 Migration**

Implementación y validación experimental de un servicio web basado en IPv6 en un entorno virtualizado para instituciones de educación superior

Pérez-Samanamud, Miguel V., Doctor[1], Rojas-Huamaní, Daniel, Magíster[1], Cevallos-Echevarría, Alejandro N., Magíster[1]

[1] Universidad Nacional Federico Villarreal, Perú, *mperezsa@unfv.edu.pe, drojas@unfv.edu.pe, acevallosl@unfv.edu.pe*

Resumen: ***La migración de IPv4 hacia IPv6 constituye un desafío para las instituciones de educación superior debido a la necesidad de garantizar la continuidad de los servicios de red y reducir los riesgos asociados a su implementación. En este contexto, la presente investigación tuvo como objetivo implementar y validar experimentalmente un servicio web basado en IPv6 en un entorno virtualizado, proponiendo una estrategia de migración reproducible mediante herramientas de software libre. Se desarrolló un estudio con enfoque cuantitativo, de tipo aplicado y alcance descriptivo–experimental, utilizando un laboratorio virtual compuesto por un servidor DNS autoritativo, un servidor web y un cliente configurados con direccionamiento IPv6. La validación funcional se realizó mediante la resolución de nombres utilizando registros AAAA y la verificación del acceso al servicio web desde el cliente. Los resultados confirmaron la correcta integración del direccionamiento IPv6, la configuración del servicio DNS y el funcionamiento del servidor web, permitiendo resolver satisfactoriamente el nombre de dominio y obtener la dirección IPv6 correspondiente al servicio publicado. Se concluye que la metodología propuesta constituye una estrategia técnica viable, reproducible y de bajo costo para validar implementaciones de servicios web basados en IPv6 antes de su despliegue en infraestructuras institucionales, contribuyendo a facilitar procesos de migración progresiva hacia IPv6 en instituciones de educación superior.***

Palabras clave: ***IPv6, DNS, Web Service, Virtualized Environment, IPv6 Migration***

I. INTRODUCCIÓN

La importancia del uso de servicios basados en IPv6 radica en superar el agotamiento de direcciones IPv4, dado que IPv6 ofrece una cantidad de 2 elevado a 128 direcciones [1], las cuales son adecuadas para la masificación de servicios, satisfacen el auge del Internet de las Cosas (IoT), dispositivos inteligentes, entregas masivas a dispositivos conectados a través de redes móviles de 5G, 6G y futuros consumidores de IPv6 [1]. El crecimiento del IoT y de las aplicaciones industriales incrementa la demanda de conectividad [2]. Aunque IPv6 fue estandarizado hace décadas, su adopción continúa siendo heterogénea [3]. Diversos estudios recientes indican que numerosas universidades han postergado la transición debido a restricciones presupuestarias, riesgos operacionales, compatibilidad con infraestructuras heredadas y preocupaciones relacionadas con la continuidad de los servicios académicos. En respuesta a esta problemática, se han propuesto marcos de despliegue gradual que permiten planificar la migración minimizando el impacto sobre las actividades institucionales [4].

Las principales ventajas de la nueva versión del protocolo IPv6 respecto del protocolo IPv4 son:

1.- Espacio de direcciones de 2 elevado a la 128 (versus 2 elevado a la 32 de IPv4) [1]. Ello es vital para nuevos servicios y conexión de los miles de millones de dispositivos del Internet de las Cosas (IoT), tales como sensores, electrodomésticos y cámaras, etc.

2.- Mayor eficiencia y procesamiento, dado que IPv6 utiliza un encabezado base simplificado y favorece la conectividad de extremo a extremo al reducir la dependencia de la traducción de direcciones [1].

3.- Seguridad integrada, dado que IPv6 admite el uso de IPsec; sin embargo, la seguridad no es automática y depende de la configuración, visibilidad y controles durante la transición [5].

4.- Configuración automática, permitiendo que, los dispositivos generen su propia dirección IPv6 y se conecten a la red automáticamente. IPv6 permite autoconfiguración; el mecanismo y la necesidad de DHCPv6 dependen del diseño y de las políticas de administración.

5.- En resumen, el uso de servicios basados en IPv6 es una necesidad técnica para garantizar la estabilidad, seguridad y escalabilidad de la infraestructura digital global.

El crecimiento sostenido de aplicaciones basadas en computación en la nube, Internet de las Cosas (IoT), inteligencia artificial y redes de nueva generación ha incrementado la necesidad de infraestructuras nativas IPv6 capaces de soportar un mayor número de dispositivos y servicios distribuidos [5]. No obstante, diversos estudios evidencian que la transición desde IPv4 continúa siendo un proceso complejo debido a la coexistencia de ambos protocolos, la presencia de aplicaciones heredadas, las restricciones presupuestarias y la necesidad de garantizar la continuidad de los servicios institucionales durante la migración. En educación superior, el despliegue por fases permite evaluar la infraestructura antes de intervenir en la red [4]. En particular, las instituciones de educación superior enfrentan el reto de modernizar sus redes sin afectar las actividades académicas y administrativas, por lo que se recomienda validar previamente las configuraciones IPv6 en entornos controlados [4].

En este contexto, los mecanismos de transición y las implementaciones experimentales en entornos controlados han adquirido especial relevancia, ya que permiten validar configuraciones de red, servicios DNS y aplicaciones antes de su despliegue sobre infraestructuras institucionales. Este enfoque reduce el riesgo operativo y facilita la identificación temprana de problemas de interoperabilidad, de configuración y de resolución de nombres asociados a IPv6.

Para el sector industrial, especialmente en el contexto de la Industria 4.0 y del IIoT (Internet Industrial de las Cosas), IPv6 ofrece ventajas críticas que van mucho más allá de simplemente contar con más direcciones. los beneficios industriales más importantes:

1. Conectividad Masiva de Activos (Escalabilidad), en una fábrica inteligente, no solo las computadoras necesitan una dirección IP. Sensores, brazos robóticos, válvulas, motores y productos en inventario requieren conexión propia.

2. Capacidad ilimitada: IPv6 permite asignar una dirección única a cada componente individual de la cadena de producción sin inconvenientes de agotamiento ni el uso de NAT/PAT.

3. Visibilidad y Gestión de “Extremo a Extremo", IPv6 restaura el modelo original de Internet donde cada dispositivo puede hablar directamente con otro.

4. Trazabilidad total, en logística, permite rastrear cada unidad de producto individualmente con su propia identidad digital en toda la cadena de suministro.

5. Seguridad Industrial Nativa, la ciberseguridad es la mayor preocupación en la industria.

Un registro AAAA asocia un nombre con una dirección IPv6 [6], pero la resolución IPv6-only también exige que funcione la cadena de delegación, incluidos servidores autoritativos y registros glue [7].

A pesar de los importantes avances reportados durante los últimos años, la mayoría de las investigaciones recientes se han concentrado en el análisis de adopción de IPv6, mecanismos de transición, estudios de rendimiento o despliegues a gran escala. Son menos frecuentes los trabajos que documentan, de forma reproducible, la implementación experimental de servicios web IPv6 utilizando entornos **co**mpletamente virtualizados y herramientas de software libre, particularmente en instituciones de educación superior latinoamericanas. Esta brecha científica justifica la realización del presente trabajo, cuyo propósito es proporcionar una estrategia práctica de migración que pueda ser reproducida por otras instituciones académicas [7], [8].

En este contexto, el presente trabajo tiene como objetivo implementar experimentalmente un servicio web basado en IPv6 en un entorno virtualizado, utilizando herramientas de software libre, y proponer una estrategia de migración reproducible para instituciones de educación superior. La investigación valida el funcionamiento del servicio mediante la resolución de nombres utilizando registros AAAA y demuestra la viabilidad técnica de la propuesta en un ambiente controlado, proporcionando una guía práctica que puede servir como referencia para futuros procesos de migración hacia infraestructuras IPv6.

II. MÉTODO

La presente investigación corresponde a un estudio de enfoque cuantitativo, de tipo aplicado y alcance descriptivo–experimental. El diseño metodológico se basa en la implementación y validación funcional de un servicio web soportado en IPv6 dentro de un entorno virtualizado controlado, utilizando herramientas de software libre. Este enfoque permite evaluar la viabilidad técnica de una estrategia de migración sin intervenir en una infraestructura institucional en producción, garantizando la reproducibilidad del experimento y reduciendo los riesgos operacionales asociados al despliegue de nuevas tecnologías de red.

El entorno experimental fue diseñado con el propósito de reproducir de manera controlada las condiciones necesarias para la implementación de un servicio web basado en IPv6, permitiendo validar cada etapa de configuración antes de su despliegue sobre una infraestructura institucional. Este enfoque responde a las recomendaciones actuales sobre experimentación reproducible en redes de comunicación, las cuales destacan que los laboratorios virtualizados facilitan la repetibilidad de los experimentos, reducen los costos de

implementación y permiten verificar configuraciones en diferentes plataformas sin afectar ambientes de producción.

Se estableció y desarrolló una secuencia analítica, estableciéndose una línea base para las implementaciones de servicios basados en el protocolo IPv6, ofreciendo una guía de referencia para la implementación de servicios web basados en IPv6. Asimismo, se realizaron simulaciones en un entorno virtualizado controlado, se utilizó software libre o de código abierto. En el presente trabajo se utilizó los siguientes recursos de software libre e imágenes en código abierto:

1. "VirtualBox-6.1.38-153438-Win" (VirtualBox 6.1.38)
2. Imagen del sistema operativo en máquina virtual "CentOS-7-x86_64-Minimal-1908"
3. Imagen del sistema operativo en máquina virtual "ubuntu-24.04-live-server-amd64".
4. Imagen del sistema operativo en máquina virtual "ubuntu-24.04-desktop-amd64".

Se utilizó la herramienta "VirtualBox 6.1.38" para crear un entorno virtualizado controlado para el presente trabajo, permitiendo crear, configurar y conectar máquinas virtuales simulando una topología de red basada en IPv6.

Se estableció la topología de prueba para la simulación (véase la siguiente Figura N°1). El objetivo principal es que, desde algún cliente (por ejemplo, en la simulación de la topología en la Figura N°1, el cliente es la máquina virtual "Ubuntu desktop") se realice una consulta al servidor de nombres [1°] para resolver, es decir, para obtener la dirección IPv6 de un recurso de Internet, en este caso, la consulta debe resolver (devolver) la dirección IPv6 del servidor web. Una vez obtenida la dirección IPv6, el cliente podrá solicitar el servicio web basado en IPv6 [2].

La utilización de herramientas de software libre y plataformas de virtualización favorece la reproducibilidad científica del experimento, ya que permite recrear la misma topología, repetir el procedimiento bajo condiciones equivalentes y validar los resultados obtenidos sin depender de infraestructura física especializada. Asimismo, este enfoque facilita que otras instituciones puedan replicar la propuesta utilizando recursos tecnológicos de bajo costo [9].

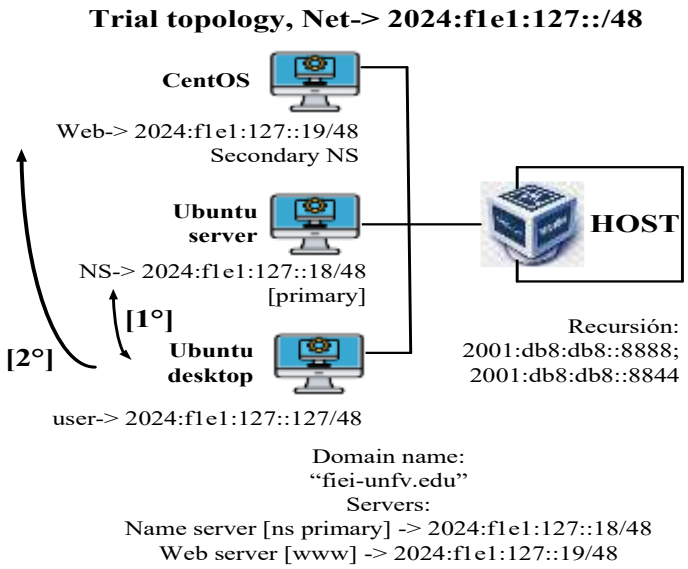


Figura N°1: Topología de prueba

La topología implementada representa una arquitectura funcional de migración hacia IPv6 conformada por un servidor DNS primario, un servidor secundario que aloja el servicio web y un cliente encargado de verificar la resolución mediante registros AAAA. Esta configuración reproduce los componentes esenciales requeridos para publicar un servicio web sobre IPv6 y permite evaluar la interacción entre los principales servicios de red en un entorno controlado y reproducible [7].

Se consideró la red IPv6: 2024:f1e1:127::/48. A título de ejemplo y solo para fines del presente documento, se consideró el nombre de dominio "fiei-unfv.edu", y los servidores: (1°) Servidor primario de nombres de dominios (NS primary): 2024:f1e1:127::18; y; (2°) Servidor web y servidor secundario de nombres de dominios (NS secondary), 2024:f1e1:127::19. Los datos utilizados en la presente simulación se consideraron solo para efectos demostrativos, lo que significa que no son datos oficiales ni obtenidos de las organizaciones competentes y legítimas. La operación de los servidores antes mencionados permitirá conseguir el objetivo desde el cliente (usuario) respecto al acceso a un servicio basado en IPv6. Con el propósito de garantizar la repetibilidad del estudio, el procedimiento experimental se organizó en etapas secuenciales, donde cada actividad constituye un requisito para la ejecución de la siguiente. Esta estructura facilita la validación progresiva de la infraestructura IPv6, la configuración del servicio DNS y la verificación del acceso al servicio web desde el cliente, permitiendo además que el experimento pueda ser reproducido por otros investigadores siguiendo la misma metodología [9]. En resumen, se realizó lo siguiente:

a) Se instaló el software virtual box en una laptop con sistema operativo Windows 10 Pro, con procesador

Intel(R) Core (TM) i7-4710HQ @2.50GHz, RAM 16.0 GB, lo que permitió disponer de la capa de virtualización con la finalizada de crear un ambiente controlado de prueba, es decir, permitió crear la topología de red mostrada en la Figura N°1.

b) Se creó la máquina virtual para el servidor secundario de nombres de dominio y servidor web asignándole 2,048 MB de memoria RAM, 20 GB fijo en disco e instalando y configurando la imagen del numeral 2 del presente ítem, lo que permitió disponer del servidor web en IPv6 para la provisión de servicio.

c) Se creó la máquina virtual para el servidor primario de nombres de dominio asignándole 2,048 MB de memoria RAM, 20 GB fijo en disco e instalando y configurando la imagen del numeral 3 del presente ítem, lo que permitió resolver o devolver al cliente la dirección en IPv6 del servidor web.

d) Se creó la máquina virtual para el cliente (usuario) asignándole 2,048 MB de memoria RAM, 20 GB fijo en disco e instalando y configurando la imagen del numeral 4 del presente ítem, lo que permitió validar la obtención de la dirección en IPv6 del servidor web.

e) Para fines demostrativos en la presente simulación se utilizó la siguiente dirección IPv6: 2024:f1e1:127::/48.

f) Se configuró la dirección IPv6 2024:f1e1:127::18/48 en el "Ubuntu server" editando el archivo /etc/netplan. En el directorio "/etc/bind" y en los ficheros de configuración (1°) named.conf.options; (2°) named.conf.default-zones; (3°) db.fiei-unfv.edu, se realizaron las configuraciones mostradas en las Figuras N°2, N°3, N°4 y N°5, con la finalidad de poner en operación el servidor primario de nombres de dominio.



Figura N°2: Configuración de la dirección IPv en el servidior primario de nombres de dominio

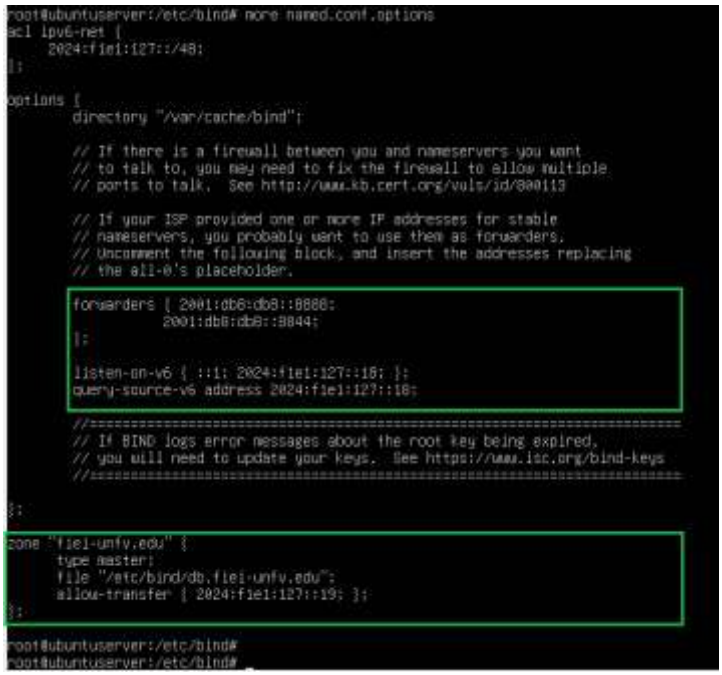


Figura N°3: Edición del archivo "named.conf.options"

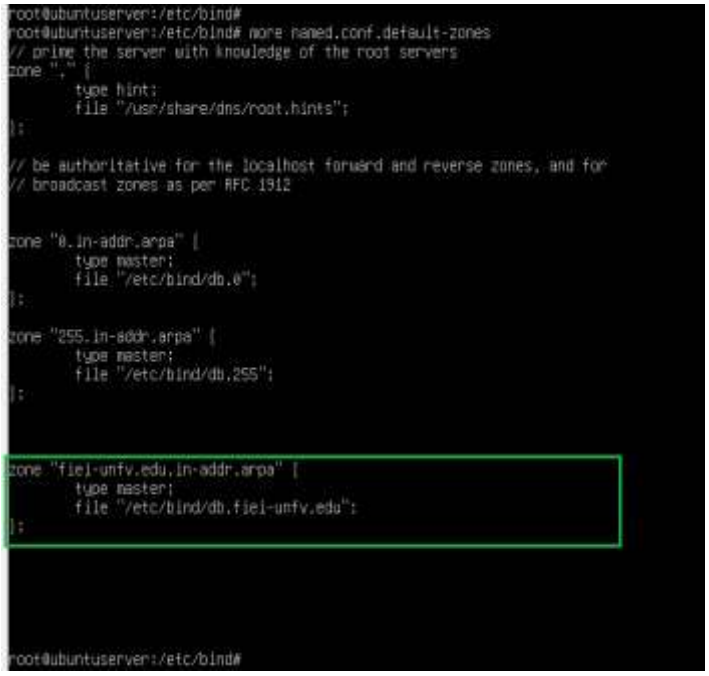


Figura N°4: Edición del archivo "named.conf.default-zones"

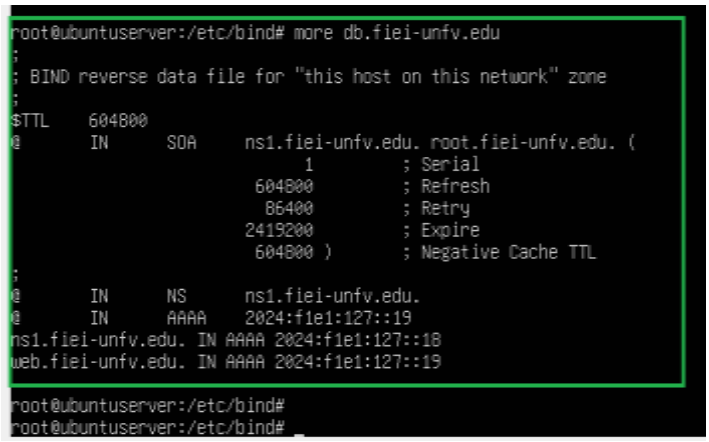


Figura N°5: Edición del archivo "db.fiei-unfv.edu"

g) En el el servidor primario de nombres de dominio (NS primary) denominado "ns1.fiei-unfv.edu" se conifgur´p los recursos en Internet "NS" y dirección 2024:f1e1:127::18. Asimismo, el servidor web llevó por nombre: "web.fiei-unfv.edu" con registro en Internet "AAAA" y dirección 2024:f1e1:127::19, lo cual permitirá al dicho servidor, resolver o devolver la dirección IPv6 (2024:f1e1:127::19) al cliente, cuando este último realice consulstas (ns) acerca del servidor web denominado "web.fiei-unfv.edu".

h) Se realizó la consulta al servidor primario de nombres de dominio (NS primary) respecto de la dirección "web.fiei-unfv.edu" y resuelvó con la IPv6 "2024:f1e1:127::19", tal como se muestra en la Figura N°6.

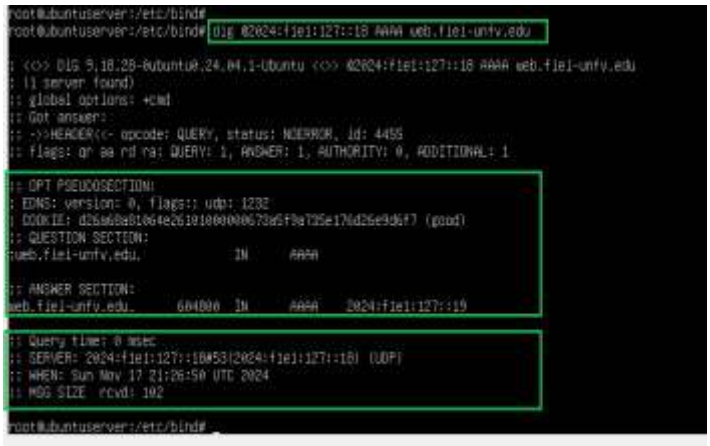


Figura N°6: Consulta al servidor de nombre primario

i) Se configuró el cliente "Ubuntu desktop" en la red 2024:f1e1:127::/48, con la dirección IPv6 2024:f1e1:127::127/48 y con servidor primario de nombres de dominio (NS primary) 2024:f1e1:127::18, tal como se muestra en la Figura N°7, con la finalidad de validar el acceso al servidor web basado en IPv6. La implementación se consideró satisfactoria cuando el cliente resolvió correctamente el nombre de dominio configurado mediante el servidor DNS autoritativo y obtuvo la dirección IPv6 correspondiente al servidor web utilizando registros AAAA. Este criterio permitió comprobar la correcta integración entre los servicios DNS y HTTP dentro del entorno virtualizado, validando funcionalmente la estrategia propuesta [7].

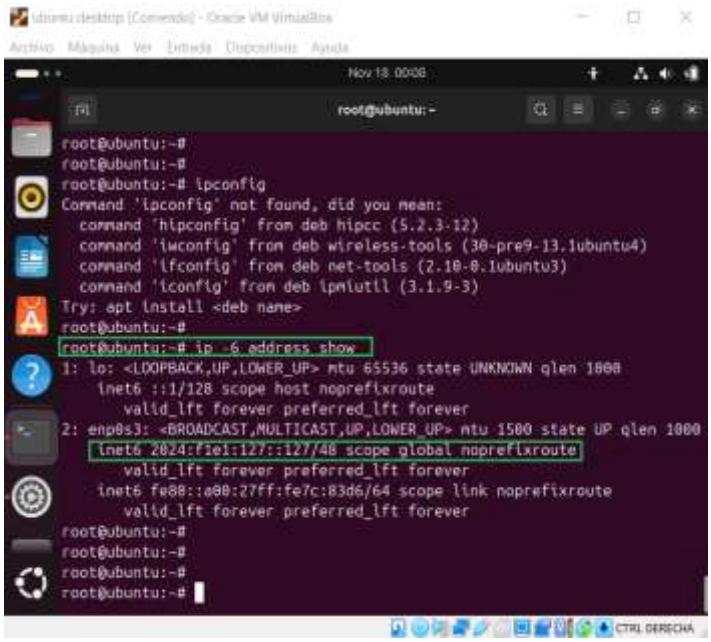


Figura N°7: Configuración del cliente "Ubuntu desktop"

El alcance de la presente investigación se limita a la validación funcional de un servicio web basado en IPv6 en un entorno virtualizado controlado. No se evaluaron métricas de rendimiento, disponibilidad, latencia, escalabilidad ni mecanismos avanzados de transición, como NAT64 o DNS64, los cuales representan oportunidades para investigaciones futuras orientadas a despliegues institucionales en ambientes de producción [10], a evaluar Dual Stack [11], NAT64 [12] y DNS64 [13], además de rendimiento, disponibilidad, latencia y escalabilidad.

III. RESULTADOS

Desde el cliente "Ubuntu desktop" se realizó la consulta al servidor primario de nombres de dominio que tiene configurado y se apreció que, el servidor primario de nombres de dominios (2024:f1e1:127::18) realizó la resolución del servidor web con nombre: "web.fiei-unfv.edu" y con dirección IPv6 2024:f1e1:127::19, tal como se muestra en la Figura N°8. Es decir, el cliente "Ubuntu desktop" obtuvo la dirección IPv6 del servidor web. Una vez obtenida

dicha dirección, podrá obtener los servicios requeridos.

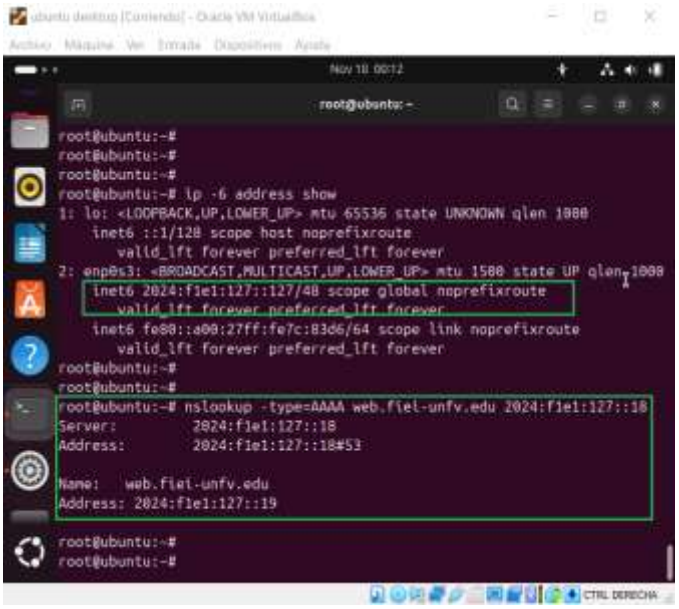


Figura N°8: Consulta desde el cliente “Ubuntu desktop” hacia el servidor primario de nombres de dominio

La Figura N.° 8 evidencia que el cliente "Ubuntu desktop" resolvió correctamente el nombre de dominio "web.fiei-unfv.edu" mediante el servidor primario de nombres de dominio, obteniendo la dirección IPv6 2024:f1e1:127::19 correspondiente al servidor web. Este resultado confirma la correcta configuración del direccionamiento IPv6, de los registros AAAA y del servicio DNS autoritativo implementado en el entorno virtualizado, verificando el funcionamiento integral de la arquitectura propuesta.

A partir de este punto, la FIEI UNFV podrá configurar y alojar contenidos en el servidor web, quedando habilitado para proveer servicios basados en IPv6. En el presente documento no se consideró las funciones de servidores recursivos de nombres de dominios ni métricas cuantitativas respecto de rendimiento en la resolución del servicio web basado en IPv6 ni tuvo por objetivo realizar una comparación entre los servicios basados en los protocolos IPv4 e IPv6.

En conjunto, los resultados obtenidos demuestran la viabilidad técnica de implementar un servicio web basado en IPv6 utilizando un entorno virtualizado y herramientas de software libre. La resolución satisfactoria del nombre de dominio y la obtención de la dirección IPv6 del servidor web constituyen la evidencia funcional del cumplimiento del objetivo de la investigación, proporcionando un entorno experimental reproducible que puede servir como base para futuras implementaciones institucionales.

IV. DISCUSIÓN

En el presente documento, en el entorno virtualizado y topología de red bajo prueba, se configuró un servidor primario de nombres de dominio, editando los archivos (1°) named.conf.options; (2°) named.conf.default-zones; (3°) db.fiei-unfv.edu, con la finalidad de resolver o devolver la dirección IPv6 del servicio web para la Faculta de Ingeniería Electrónica e Informática (FIEI) de la Universidad Nacional Federico Villarreal (UNFV). La configuración de servidor de nombre primario y secundario, es similar al trabajo realizado en “DNS IPv6 Only” [7],[13], el cual detalla la configuración de manera teórica. En el presente documento, se realizó la simulación de una implementación en un ambiente virtualizado controlado. La configuración es comparable con LACNIC [8] y utiliza registros AAAA según RFC 3596 [6].

La utilización de un laboratorio controlado facilitó la verificación progresiva de la configuración del servidor DNS, la resolución de nombres mediante registros AAAA y la publicación del servicio web, confirmando la viabilidad técnica de la arquitectura implementada antes de su posible despliegue sobre una infraestructura institucional.Se utilizó virtualización e imágenes con software libre (código abierto), desde el cliente “Ubuntu desktop” se validó el resultado esperado. Lo cual se realizó a través de la consulta realizada por dicho cliente al servidor primario de nombres de dominio que tiene configurado respecto de la dirección IPv6 del servidor web denominado “web.fiei-unfv.edu”, dicho servidor primario resolvió o devolvió al cliente la dirección IPv6 prevista (2024:f1e1:127::19).

Este resultado es consistente con lo reportado por Streibelt et al. [7], quienes señalan que el correcto funcionamiento de servicios basados en IPv6 depende no solo de la asignación de direcciones IPv6, sino también de la adecuada configuración de la infraestructura DNS y de la cadena completa de resolución de nombres. En este estudio, la obtención satisfactoria de la dirección IPv6 del servidor web confirma la correcta integración entre el direccionamiento IPv6, los registros AAAA y el servidor DNS autoritativo implementado en el laboratorio experimental. Obtenida la dirección IPv6 del servicio web por el cliente, este podrá solicitar los servicios web alojados en el servidor web, dado que ya tiene conocimiento de su dirección. Asimismo, los hallazgos obtenidos concuerdan con Abdullah [4], quien destaca que uno de los principales retos en la adopción de IPv6 consiste en garantizar la interoperabilidad entre la infraestructura existente y los nuevos servicios soportados por este protocolo.

En este contexto, el entorno virtualizado utilizado permitió validar previamente la configuración del servicio web sin afectar la infraestructura institucional, constituyéndose en una estrategia adecuada para reducir riesgos durante procesos de migración progresiva hacia IPv6.El uso de un ambiente controlado dentro de una red de área local, podría limitar la aceptación del presente documento como estrategia o guía práctica de implementación de servicios basados en IPv6. Si bien el entorno experimental representa una simplificación respecto de un ambiente de producción, su principal fortaleza radica en ofrecer una metodología reproducible basada en herramientas de software libre, permitiendo que otras instituciones de educación superior puedan replicar la propuesta como una etapa previa a la implementación de servicios IPv6 sobre infraestructura real.

Por otro lado, el presente documento no aborda las funcionalidades de servidores recursivos de nombres de dominios ni métricas cuantitativas respecto del rendimiento en la resolución del servicio web basado en IPv6. En consecuencia, los resultados deben interpretarse como una validación funcional de la estrategia propuesta y no como una evaluación integral del desempeño de la infraestructura. La incorporación de indicadores de rendimiento, disponibilidad, latencia, escalabilidad y mecanismos avanzados de transición, como NAT64 o DNS64, constituye una línea de investigación futura para ampliar el alcance de la presente propuesta.

Asimismo, en una estrategia de transición real de servicios web de IPv4 a IPv6, se deberá establecer el mismo servicio web basado en ambos protocolos: IPv4 e IPv6, con prioridad en IPv6 y, luego de aceptado el servicio web basado en IPv6 estableciendo un criterio de aceptación, se procedería a deshabilitar el servicio basado en IPv4 y tener la operación de los servicios basados solo en IPv6.

Desde una perspectiva práctica, la metodología desarrollada proporciona una estrategia reproducible para apoyar procesos de migración hacia IPv6 en instituciones de educación superior. La validación previa mediante un entorno virtualizado permite disminuir riesgos operativos, facilitar la identificación temprana de problemas de configuración y contribuir a una adopción progresiva del protocolo IPv6 conforme a las recomendaciones actuales para el despliegue de servicios de red.

V. CONCLUSIONES

En el entorno virtualizado controlado, se creó la topología de prueba utilizando la red IPv6: 2024:f1e1:127::/48 con el uso de software de virtualización e imágenes en software libre (código abierto). Desde el cliente “Ubuntu desktop” se realizó la consulta al servidor primario de nombres de dominio que tiene configurado.El servidor primario de nombres de dominio resolvió o devolvió al cliente “Ubuntu desktop” la dirección IPv6: 2024:f1e1:127::19 del servidor web con nombre: “web.fiei-unfv.edu”, con lo cual el cliente podrá obtener los servicios web desde el servidor web basado en IPv6.

Los resultados obtenidos permiten concluir que la implementación experimental cumplió satisfactoriamente el objetivo planteado, demostrando la viabilidad técnica de implementar un servicio web basado en IPv6 mediante un entorno virtualizado utilizando herramientas de software libre. La validación funcional realizada confirma que este tipo de laboratorio constituye una estrategia adecuada para verificar configuraciones antes de su implementación sobre infraestructuras institucionales, contribuyendo a reducir riesgos operativos durante los procesos de migración hacia IPv6.

Desde el punto de vista científico, la principal contribución de esta investigación consiste en presentar una metodología experimental reproducible para la implementación y validación de servicios web sobre IPv6 en instituciones de educación superior. La propuesta puede ser utilizada como referencia por otras organizaciones interesadas en iniciar procesos de adopción de IPv6 mediante ambientes virtualizados y herramientas de software libre, favoreciendo la transferencia tecnológica y la replicabilidad del experimento.

Como trabajo futuro, se recomienda ampliar la presente investigación incorporando evaluaciones de rendimiento, disponibilidad, latencia, escalabilidad y mecanismos avanzados de transición, tales como Dual Stack, NAT64 y DNS64, así como validar la estrategia propuesta en entornos institucionales de producción con el propósito de fortalecer su aplicabilidad y generalización en escenarios reales de migración hacia IPv6.

VI. REFERENCIAS

[1] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 8200, Internet Engineering Task Force, Jul. 2017, doi: 10.17487/RFC8200.

[2] B. Bolaños Bolaños, “Integración del Internet de las Cosas (IoT) en la industria: Estrategias para el monitoreo y control avanzado de procesos,” in Proc. 22nd LACCEI International Multi-Conference for Engineering, Education and Technology, San José, Costa Rica, Jul. 17–19, 2024. [Online]. Available: https://laccei.org/LACCEI2024-CostaRica/papers/Contribution_1989_final_a.pdf. [Accessed: Sep. 23,

2026].
[3] Instituto Federal de Telecomunicaciones, IPv6 Mejorado: Impulsando las redes de próxima generación de México con IPv6 Mejorado. Ciudad de México, México, Dec. 2024. [Online]. Available: https://www.ift.org.mx/sites/default/files/contenidogeneral/politica-regulatoria/whitepaperipv6terminado.pdf. [Accessed: Sep. 23, 2026].
[4] S. A. Abdullah, "A framework for deploying IPv6 at higher education institutions," International Journal on Integrating Technology in Education, vol. 13, no. 3, pp. 77–86, Sep. 2024, doi: 10.5121/ijite.2024.13306.
[5] National Security Agency, IPv6 Security Guidance, Cybersecurity Information Sheet, Fort Meade, MD, USA, Jan. 2023. [Online]. Available: https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF. [Accessed: Sep. 23, 2026].
[6] S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, "DNS Extensions to Support IP Version 6," RFC 3596, Internet Engineering Task Force, Oct. 2003, doi: 10.17487/RFC3596.
[7] F. Streibelt, P. Sattler, F. Lichtblau, C. H. Gañán, A. Feldmann, O. Gasser, and T. Fiebig, "How ready is DNS for an IPv6-only world?," in Passive and Active Measurement, Lecture Notes in Computer Science, vol. 13882. Cham, Switzerland: Springer, 2023, pp. 525–549, doi: 10.1007/978-3-031-28486-1_22.
[8] J. G. Cotúa and A. Acosta, "HowTo: Primeros pasos—DNS IPv6 Only," LACNIC Blog, Nov. 24, 2022. [Online]. Available: https://blog.lacnic.net/howto-primeros-pasos-dns-ipv6-only/. [Accessed: Sep. 23, 2026].
[9] G. Huston, A. Lord, and P. Smith, "IPv6 Address Prefix Reserved for Documentation," RFC 3849, Internet Engineering Task Force, Jul. 2004, doi: 10.17487/RFC3849.
[10] D. Eastlake 3rd and A. Panitz, "Reserved Top Level DNS Names," RFC 2606, Internet Engineering Task Force, Jun. 1999, doi: 10.17487/RFC2606.
[11] E. Nordmark and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," RFC 4213, Internet Engineering Task Force, Oct. 2005, doi: 10.17487/RFC4213.
[12] M. Bagnulo, P. Matthews, and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers," RFC 6146, Internet Engineering Task Force, Apr. 2011, doi: 10.17487/RFC6146.
[13] M. Bagnulo, A. Sullivan, P. Matthews, and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers," RFC 6147, Internet Engineering Task Force, Apr. 2011, doi: 10.17487/RFC6147.