UNIVERSIDAD NACIONAL DE LOJA

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"Despliegue del Protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja"

Tesis previa a la obtención del título de Ingeniero en Sistemas

AUTORA:

Lapo-Lapo, Kelen-Mireya.

DIRECTOR:

Ing. Torres-Carrión, Hernán-Leonardo, Mg. Sc

LOJA-ECUADOR
2018

CERTIFICACIÓN DEL DIRECTOR

Ing. Hernán Leonardo Torres Carrión, Mg. Sc

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE LOJA Y DIRECTOR DE TESIS.

CERTIFICA

Haber dirigido, revisado y corregido en todas sus partes el desarrollo del Trabajo de Titulación de Ingeniería en Sistemas titulado: **"Despliegue del Protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja",** con autoría de la egresada **Kelen Mireya Lapo Lapo**. En razón de que la misma reúne a satisfacción los requisitos de fondo y forma, exigidos para la investigación de éste nivel, autorizo su presentación, sustentación y defensa ante el tribunal designado para el efecto.

Loja, 8 de Enero del 2018

Ing. Hernán Leonardo Torres Carrión

DIRECTOR DE TESIS

AUTORÍA

KELEN MIREYA LAPO LAPO, declaro ser autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi trabajo de titulación en el Repositorio Institucional-Biblioteca Virtual.

Firma: ……

Cédula: 1105310526

Fecha: Loja, 26 de febrero de 2018

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DE LA AUTORA, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, **KELEN MIREYA LAPO LAPO**, declaro ser autora de la tesis titulada: **"DESPLIEGUE DEL PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6) PARA EL DNS AUTORITARIO Y SERVIDORES PÚBLICOS EN LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA"**, como requisito para optar el grado de **INGENIERO EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja a los ocho días del mes de enero del dos mil dieciocho.

Firma: .....

Autor: Kelen Mireya Lapo Lapo

Cédula: 1105310526

Dirección: Sozoranga, (Cdla. Julio Hidalgo).

Correo Electrónico: kmlapol@unl.edu.ec / kelitamireya@gmail.com

Teléfono: 072 660269 **Celular:** 0981754440

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

Tribunal de Grado: Ing. Jorge Iván Tocto, Mg. Sc.

Ing. Mario Andrés Palma Jaramillo, Mg. Sc.

Ing. Alfredo Vinicio Zúñiga Tinizaray, Mg. Sc.

AGRADECIMIENTO

Al padre celestial por el maravilloso don de la vida, al Divino Niño Jesús y a la Virgen del Cisne que como madre ha dirigido siempre mis pasos, ellos a quienes encomendé mis años de carrera universitaria y hoy me permiten finalizar exitosamente.

A mis padres y hermanos por entregarme su amor y apoyo incondicional para lograr culminar unas de las etapas más importantes de mi vida.

A la Universidad Nacional de Loja, a la Carrera de Ingeniería en Sistemas y a sus docentes por los conocimientos impartidos durante esta trayectoria universitaria, a la Unidad de Telecomunicaciones e Información muy especialmente a sus técnicos por la información y ayuda brindada durante el desarrollo de mi tesis, al Ingeniero Hernán Torres por dedicar parte de su valioso tiempo y con su experiencia guiar mi proyecto de titulación.

Como no agradecer a mis chiquillos de clase por el compañerismo, la paciencia y por los momentos compartidos, siempre los recordaré.

DEDICATORIA

Dedico este esfuerzo que refleja el trayecto de mi vida universitaria y me encamina a un futuro profesional al Maestro Dios, a mis adorados padres Zulema y Luis, a mis queridos hermanos Gioysi, Yohanna, Yandri, Natali y Pepin, y a ti mi pequeño Samuelito por ser mi principal inspiración para lograr culminar esta anhelada meta y continuar cosechando logros a lo largo de mi diario vivir, finalmente a mis familiares y amigos por el soporte y confianza puesta en mí.

Kelen

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. TÍTULO

“Despliegue del Protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja”

2. RESUMEN

El presente Trabajo de Titulación (TT), consiste en el despliegue de IPv6 en el DNS autoritario y servidores públicos en la red de datos de la Universidad Nacional de Loja, considerando que esta nueva versión de protocolo está en auge, lo que permitirá la innovación y crecimiento de la Red ante la inminente escases de direcciones IPv4 públicas y con ello brindar a la colectividad servicios de calidad y eficientes, puesto que el futuro de una Internet accesible depende del exitoso desarrollo e implementación de IPv6.

El TT se enfoca en el estudio del nuevo protocolo de Internet, sus características, mejoras y diferencias respecto a su antecesor IPv4 (Protocolo de Internet versión 4), para seguidamente centrarse en el análisis de la situación actual del DNS y servidores públicos, determinación del mecanismo de transición a ser utilizado para el despliegue de IPv6, esto después de haber realizado un análisis entre los mecanismos de doble pila, túneles y traducción, continuando con el diseño del esquema de direccionamiento IPv6 donde se plantea un mecanismo a ser utilizado en el direccionamiento de los servicios públicos.

Además para la ejecución del proyecto fue necesario la utilización de métodos como el inductivo, experimental y analítico que permitieron llevar a cabo el desarrollo de un trabajo ordenado y sustentado, apoyándose en técnicas como: la entrevista, la observación, investigación bibliográfica y tutorías, las mismas que fueron fundamentales para su culminación , teniendo como resultado final la implementación de doble pila (Dual stack) en los servidores públicos (servidores web), manteniendo así la convivencia de las dos versiones del Protocolo IP (IPv4-IPv6).

2.1 SUMMARY

The present work of titling (TT) consists of the deployment of IPv6 in the authoritative DNS and public servers in the data network of the National University of Loja, considering that this new version of the protocol is booming, which will allow the innovation and growth of the network before the imminent scarcity of public IPv4 addresses and thus provide the community with quality and efficient services, since the future of an accessible Internet it depends on the successful development and implementation of IPv6.

The TT focuses on the study of the new Internet protocol, its characteristics, improvements and differences with respect to its predecessor IPv4 (Internet Protocol version 4), to then focus on the analysis of the current situation of the DNS and public servers, determination of the transition mechanism to be used for the deployment of IPv6, this after having performed an analysis between double-stack mechanisms, tunnels and translation, continuing with the design of the IPv6 addressing scheme where a mechanism to be used in addressing is proposed of public services.

In addition to the execution of the project, it was necessary to the use of methods such as inductive, experimental and analytical data, enabling the development of orderly and sustained work, drawing on techniques such as: the interview, observation, bibliographical research and tutorials, which were fundamental to its culmination , taking the final result of the implementation of dual-stack (Dual stack) in the public servers (web servers), thus maintaining the coexistence of the two versions of the IP protocol (IPv4-IPv6).

3. INTRODUCCIÓN

Internet, conocido como la Red de redes, es considerado como uno de los medios de comunicación e información más extendido y para muchos un modelo de negocio; Su evolución, la gran demanda de conectividad de usuarios y de dispositivos que utilizan el protocolo TCP/IP han logrado una revolución en el desarrollo de las comunicaciones y de la información, que en conjunto con la deficiente manera en que las direcciones IP han sido asignadas han provocado una rápida escasez del sistema de direccionamiento actual (IPv4), el cual se ha quedado pequeño debido al gran auge de Internet. Otra consideración es que Pv4 no fue diseñado para ser un protocolo seguro y muchas de las aplicaciones creadas para solucionar este problema de seguridad solo protegen la información en las capas de comunicación más altas (Aplicación y Transporte) haciendo vulnerable la información a ataques en la capa de Red.

Ante los inconvenientes citados anteriormente la necesidad de un nuevo protocolo era ineludible, motivo por el cual surge IPv6 siendo la nueva versión del Internet Protocol (IP), diseñada para remplazar a la IPv4. Este nuevo protocolo dispone de un amplio espacio de direcciones, suficiente para conectar billones de nuevos dispositivos (tabletas, teléfonos móviles, y televisiones inteligentes entre otros), nuevos usuarios y tecnologías “siempre-conectadas” (cable, Ethernet en el hogar, Fibra en el hogar, redes inalámbricas, etc.) como lo menciona el portal web de LACNIC [19] “IPv6 representa quizás el cambio más importante en la historia del Internet ya que es necesario para que la red de redes pueda seguir desarrollándose de una forma segura y estable.” Razones suficientes para que en la actualidad la adopción de IPv6 sea una de las principales alternativas en las instituciones y empresas alrededor del mundo, y con ello lograr una convergencia a nivel de protocolo.

La Universidad Nacional de Loja actualmente tiene implementado direccionamiento IPv4, pero uno de las aspiraciones de la institución es implementar el protocolo de internet versión 6 en su red de datos, puesto que al no contar con esta nueva tecnología no se podría acceder a sitios de internet que estén habilitados solo para IPv6, además que la institución queda rezagada ante otras entidades educativas de nivel superior que ya han implementado IPv6.

El objetivo general del presente trabajo de titulación es: Configurar el protocolo de Internet versión 6 (IPV6) en el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja; a su vez de este objetivo principal se desglosan los siguientes objetivos específicos:

- Analizar la situación actual del DNS autoritario y Servidores públicos para la implementación de IPv6.
- Determinar el mecanismo de transición a utilizar entre IPv4 e IPv6.
- Diseñar el esquema de direccionamiento para la red pública de la Universidad Nacional de Loja.
- Establecer un escenario de pruebas de acuerdo al mecanismo de transición seleccionado.
- Realizar las configuraciones necesarias para la implementación de IPv6 en el DNS autoritario y Servidores públicos de la Universidad Nacional de Loja.

La investigación desarrollada se encuentra estructurada a lo largo de 9 secciones descritas a continuación:

Las tres primeras secciones corresponden a las fases introductorias como lo es**:** TÍTULO, RESUMEN E INTRODUCCIÓN.

En la cuarta sección correspondiente a la REVISIÓN LITERARIA se describe los diversos conceptos relacionas al Tema de investigación para ello se ha dividido en cuatro partes la información: en la primera se hace énfasis en el protocolo IPv6, su direccionamiento, ventajas, diferencias y mejoras respecto a su antecesor IPv4, seguidamente se describen los mecanismo de transición Doble Pila (Dual Stack), Túneles (Tunneling) y Traducción; en la tercera parte se describen aspectos importantes referentes al DNS e IPv6, para finalmente la cuarta parte hacer una introducción a los principales servidores web.

En la quinta sección denominada MATERIALES Y MÉTODOS se detalla los métodos y técnicas de investigación utilizados en el desarrollo del proyecto.

Seguidamente en la sexta sección se presentan los RESULTADOS donde destaca el análisis de la situación actual del DNS autoritario y servidores públicos y el análisis de los mecanismos de transición para determinar el mecanismo a ser empleado en el despliegue

de IPv6, así como la creación de un mecanismo para el direccionamiento en el DNS autoritario y servidores públicos, continuando con las configuraciones realizadas en el servidor DNS y Web como parte del escenario de pruebas y finalmente la implementación del protocolo versión 6 en los servidores públicos.

La séptima sección incluye la DISCUSIÓN donde se describe y analiza los resultados obtenidos relacionados con los objetivos del proyecto, además de realizar la valoración técnica, económica y ambiental del proyecto. Por último se presenta las CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS como soporte del trabajo realizado.

Finalmente cabe resaltar que esta memoria forma parte de un trabajo conjunto realizado con Walter Camacho y cuyo tema versa “Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja”, por lo que ambos trabajos presentan una parte común (Determinar el mecanismo de transición a utilizar entre IPv4 e IPv6) y una parte específica que se describe en cada una de las dos memorias.

4. REVISIÓN DE LITERATURA

4.1. PROTOCOLO DE INTERNET VERSIÓN 6

En la presente sección se abordará principalmente temas relacionados al protocolo IPv6, sucesor de IPv4, destacando la relevancia e importancia de la implementación de esta nueva versión de IP mediante comparativas entre estos dos tipos de direccionamiento.

4.1.1. Introducción a IPv6

En la actualidad Internet usa el protocolo IPv4, pero el drástico crecimiento de la población mundial y el persistente aumento de dispositivo electrónicos que requieren el uso de direcciones IP, conllevó a que la IANA (Internet Assigned Numbers Authority/ Autoridad para la Asignación de Números de Internet) Organismo responsable de la asignación de direcciones IP de Internet, planteara una serie de propuestas que permitieran solucionar o por lo menos aminorar este problema, por lo que enfocaron esfuerzos en un mejor aprovechamiento de las direcciones disponibles definiendo redes con un tamaño más ajustado a las necesidades de las empresas.

Para retardar el agotamiento de las direcciones se utilizaban tecnologías como el enrutamiento inter-dominio sin clase (CIDR) y el protocolo NAT (Network Address Translation – Traducción de Direcciones de Red) que promueve el uso de direcciones privadas, en lugar de públicas, para direccionar redes de área local [1]. Pero, estas alternativas no tuvieron mucho éxito, ya que en primera instancia no todos los enrutadores soportan CIDR y además hay muchas aplicaciones que requieren utilizar direcciones estáticas, por lo que NAT no ayuda en gran medida en estos casos. Otro inconveniente que presenta el uso de esta técnica es que no se puede encriptar la información en cierto tipo de comunicaciones, esto debido a que NAT reemplaza las direcciones y los puertos para realizar la traducción [2].

El número de direcciones IP públicas disponibles no es el único problema detectado en IPv4, sino que tiene otras limitaciones entre ellas: la no incorporación de mecanismos de seguridad a nivel de capa 3 y el gran tamaño de las tablas de enrutamiento, debido a la mala distribución de direcciones IP, que ralentiza los tiempos de respuesta y hace ineficaz el encaminamiento; Motivos por los cuales la organización IETF (Internet Engineering Task Force -Fuerza de Tareas de Ingeniería de Internet) durante la década de los 90 [3], vio la

necesidad de crear un nuevo protocolo de internet, al cual se le denominó versión 6 o IPng (IP next generation) definida en el RFC 2460 y llamado a ser el sucesor de IPv4 descrito en el RFC 791, este protocolo dispone de 340 billones de billones de billones (sextillos) de direcciones, lo que hace que la cantidad de direcciones IPv4 (2^{32}=4.3 millones de direciones) parezca insignificante. Al poseer un mayor espacio de direcciones, IPv6 proporciona una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes, así como podemos crear una compleja jerarquía de direcciones y conseguir un auto configuración mucho más simple [4], [5], [6]. IPv6 también proporciona un formato de cabecera eficiente y los enrutadores son capaces de procesar más rápidamente [7], entre otras características y una de ellas es la movilidad, móvil IP es un estándar de la IETF que permita a los usuarios con dispositivos Wireless estar conectados de manera transparente y moverse a cualquier sitio sin restricciones. La seguridad es otro tema importante, IPSec (IP Security) está presente en cada uno de los dispositivos IPv6.

4.1.2. Ventajas de IPv6 respecto a IPv4

IPv4 tiene ciertas limitaciones respecto a su sucesor IPv6, por lo que a continuación se describen algunas de las ventajas que este nuevo protocolo proporciona [8], [9]:

4.1.2.1. Número de direcciones IPv6 prácticamente ilimitado

IPv6 tiene 128 bits (16 bytes) que puede ser expresadas como 3.4 x 10^{38} posibles combinaciones, cuatro veces más larga que la longitud de la dirección IPv4 (2^{32}=4.3 billones), lo que en teoría significa que hay 2^{128} posibles direcciones, permitiendo con este rango facilitar una dirección IP a cada dispositivo conectado a la red.

4.1.2.2. Asignación jerárquica de direcciones

IPv6 permite que los routers de un determinado nivel de la jerarquía sólo necesitan conocer las direcciones que manejan los routers a los que está directamente conectado, generando que las tablas de encaminamiento se mantengan pequeñas, manejables y por ende se necesita menos capacidad de procesamiento para hacer el encaminamiento.

4.1.2.3. Autoconfiguración en la conexión a la red

En IPv6 la configuración automática está incorporada dentro del propio protocolo, de forma que los routers proporcionan a los demás equipos de la red una dirección IP pública y una puerta de enlace automáticamente.

4.1.2.4. Incorporación de mecanismos de seguridad

IPv6 tiene integrado el protocolo de seguridad IPSec lo que permite mantener la autenticación y la encriptación de los datos, pero esto no quiere decir que IPv4 no lo posea la única diferencia es que en IPv4 la seguridad es opcional.

4.1.2.5. Modificación de las cabeceras del protocolo para optimizar el procesamiento

Con IPv6 en lugar de incorporar en la cabecera toda la información necesaria para algunas funcionalidades, se ha creado lo que son las cabeceras de extensión, lo que permite a los equipos de enrutamiento tomar decisiones de encaminamiento en función de los datos de la cabecera principal.

4.1.2.6. Posibilidad de paquetes con carga útil (datos) de más de 60 kb

En IPv4 se limita el tamaño de los paquetes a 64 KB, IPv6 envía paquetes como mínimo de 1280 bytes e introduce un soporte opcional, los llamados jumbogramas, para que los paquetes puedan alcanzar una longitud de hasta 4 GB.

4.1.2.7. Mejora de identificación de flujos para gestionar la calidad de servicio

La Calidad de Servicio o QoS (Quality of Service) introduce mecanismos que permiten a los routers diferenciar y dar un trato especial a determinados paquetes acelerando su reenvío.

4.1.2.8. Nuevos modos de envío de paquetes

IPv6 define direcciones de multidifusión o multicast que permite el envío de un mismo paquete a un grupo de receptores, además se han definido las direcciones de difusión por proximidad o anycast para realizar el envío de un paquete a un receptor dentro de un grupo.

4.1.2.9. Movilidad de equipos entre redes diferentes

La movilidad está disponible tanto en IPv4 como en IPv6, en este último protocolo esta capacidad se construyó dentro del protocolo en lugar de ser una nueva función agregada

como en IPv4, lo que implica que cualquier nodo IPv6 puede usar un IP Móvil como lo requiera. IPv6 Móvil utiliza dos extensiones de encabezado: un Encabezado de Enrutamiento para el registro y un Encabezado de Destino para entrega del datagrama entre los nodos móviles y sus nodos fijos correspondientes.

4.1.2.10. Posibilidad de añadir nuevas funcionalidades en el futuro.

IPv6 proporciona nuevas funcionalidades sin tener que rediseñar el protocolo, esto debido a que su propia estructura permite que sea escalable según se vayan necesitando nuevos servicios.

4.1.3. Comparación de IPv4 e IPv6

En la TABLA I siguiente se describe algunas de las diferencias más significativas entre los protocolos IPv4 e IPv6 [10]:

TABLA I: DIFERENCIAS ENTRE IPV4 E IPV6

IPv4	IPv6
Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
El soporte del encabezado IPSec es opcional.	El soporte del encabezado IPSec es necesario.
Ninguna identificación del flujo de paquetes para el manejo de la entrega priorizada por parte de los routers. La calidad de servicio (QoS) es manejada por los router y no por la cabecera IPv4.	Identificación del flujo de paquetes para el manejo de entrega priorizada por los enrutadores está presente dentro de la cabecera IPv6 utilizando el Campo Etiqueta de flujo (Flow Label).
La fragmentación se realiza por el host de origen y los routers, lo que ralentiza el rendimiento del router.	La fragmentación se realiza solo por el host, ya que el paquete es procesado solo el nodo final de destino.

No tiene requisitos para el tamaño de un paquete de capa de enlace y debe ser capaz de reemsamblar un paquete de 576 bytes.	La capa de enlace debe admitir un paquete de 1.280 bytes y ser capaz de re ensamblar un paquete de 1.500 bytes.
La cabecera incluye una suma de verificación (campo checksum).	La cabecera no incluye una suma de verificación (campo checksum).
La cabecera incluye el campo opciones	Todos los datos opcionales se trasladan a los encabezados de extensión IPv6.
ICMP Router Discovery se utiliza para determinar la dirección IPv4 de la mejor puerta de enlace (gateway) predeterminada y es opcional.	ICMPv4 Router Discovery se reemplaza con los mensajes ICMPv6 Router Solicitation y Router Advertisement, y es requerido.
Las direcciones de broadcast se utilizan para enviar tráfico a todos los nodos de una subred.	No existen direcciones IPv6 de broadcast, en su lugar se usan las direcciones multicast.
En IPv4 las direcciones deben configurarse manualmente o a través de DHCP.	Las direcciones no requieren configuración manual o DHCP.
Utiliza registros A en el DNS para correlacionar nombres de host a direcciones IPv4.	Utiliza registros AAAA (“quad A”) en el DNS para asignar nombres de host a direcciones IPv6.
Utiliza registros de recursos de puntero (PTR) en el dominio DNS IN-ADDR.ARPA para asignar direcciones IPv4 a nombres de host.	Utiliza registros de recursos de puntero (PTR) en el dominio DNS IP6.ARPA para asignar direcciones IPv6 a nombres de host.

4.1.4. Diferencias en el formato de la cabecera IPV4 e IPV6

En la cabecera IPv6 se elimina o modifica varios campos de la cabecera IPv4, además de la aparición de nuevos campos, generando una cabecera más simple, flexible y eficiente lo cual implica una mayor facilidad en el procesamiento de los paquetes.

A continuación la Figura 1, nos muestra el formato de las cabeceras IPv4 e IPv6 respectivamente.

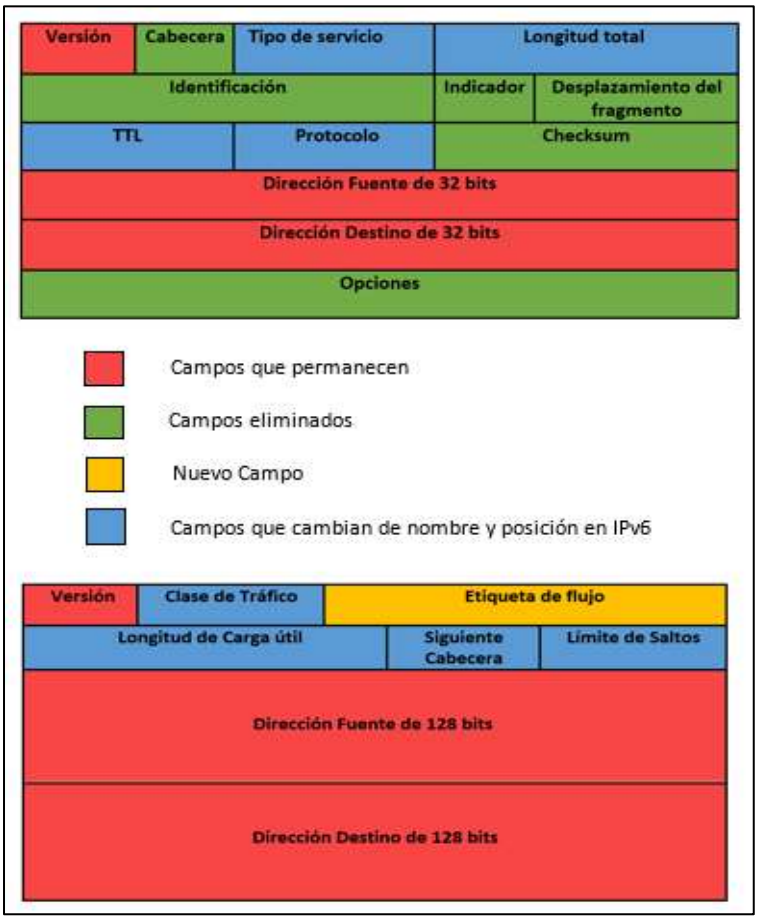


Figura 1: Formato de Cabecera IPv4 e IPv6 [Autora]

Algunas diferencias respecto a las cabeceras de IPv4 e IPv6 son las siguientes:

- La cabecera de IPv4 es de 20 bytes pudiendo llegar hasta 60 bytes si se incluyen las opciones de cabecera.
- La cabecera de IPv6 es de 40 bytes fija, por lo que no requiere de los campos de longitud y verificación de la cabecera (checksum).
- La cabecera IPv4 tiene al menos 12 campos, mientras que la cabecera ipv6 tiene 8 campos y fijos.
- IPv4 requiere de los campos identificación, banderas y desplazamiento del fragmento, porque fragmenta el datagrama mientras que IPv6 no requiere de dichos campos porque no fragmenta el datagrama.

4.1.4.2. Cambios significativos de la cabecera IPv4 a la cabecera IPv6.

A continuación se describen los campos de la cabecera IPv4 que fueron modificados, los que permanecen, los campos eliminados y los nuevos campos que conforman la cabecera IPv6 [11], [12].

TABLA II: DIFERENCIAS ENTRE LAS CABECERAS IPV4 E IPV6

Campo en IPv4	Campo en IPv6	Descripción
Versión (4)	Igual	El campo Versión especifica la versión IP del paquete y ayuda a los enrutadores intermedios a determinar cómo interpretar el paquete restante.
Longitud de Cabecera IP (4)	Desaparece	La longitud del encabezado de Internet de 4 bits especifica Longitud de la cabecera en unidades de 8 bytes incluyendo opciones. El valor mínimo es 5 y la longitud máxima será de 60 bytes porque los campos IHL son de 4 bits (15*8=60 bytes)
Tipo de servicio (ToS)	Clase de Tráfico (8)	Se utiliza para especificar los diferentes tipos de paquetes IP y proporcionar calidad de servicio (QoS).
	Etiqueta de Flujo (20)	Permite que el tráfico sea etiquetado para que se pueda manejar de manera más rápida flujo por flujo, es decir, identificar un flujo específico y hacerle un tratamiento (QoS) idéntico a todos los paquetes que pertenezcan al flujo.

Longitud Total (16)	Longitud de Carga útil (16)	El campo longitud total especifica la longitud total del paquete IP que incluye el encabezado IP en bytes y el campo longitud de carga útil especifica la longitud del paquete IP que excluye el encabezado IP. Los encabezados de extensión en IPv6 también se consideran como carga útil IP. En IPv4, con los campos longitud total y Longitud de Cabecera IP (ILH), sabemos dónde comienza la porción de datos del paquete.
Identificación (16)	Trasladado a Cabecera de extensión	Especifica un valor asignado por el remitente y ayuda a ensamblar los paquetes fragmentados.
Banderas/Indicador (3)	Trasladado a Cabecera de extensión	Especifican varios indicadores de control para la fragmentación.
Desplazamiento del fragmento	Trasladado a Cabecera de extensión	Especifica a dónde pertenece un fragmento.
Tiempo de vida (8)	Límite de saltos (8)	El campo Tiempo de vida (TTL) especifica cuánto tiempo un paquete puede permanecer en Internet. En IPv6, Hop Limit (Límite de saltos) reemplaza Time to Live (Tiempo de vida) y especifica con cuántos saltos se puede enviar un paquete.
Protocolo (8)	Siguiente Cabecera (8)	El campo Protocolo especifica el siguiente protocolo en el campo de datos de un paquete. En IPv6, se define el siguiente encabezado

		que indica el tipo de cabecera que sigue a la cabecera fija de IPv6, podría indicar por ejemplo, que el siguiente campo es TCP o UDP o podría indicar que existe una extensión de la cabecera.
Checksum (16)	Desaparece	Solo incluye la suma de verificación para la cabecera. Algunas partes de cabecera, como TTL, se pueden cambiar. Por lo tanto, el Checksum de encabezado debe ser recalculado y verificado en cada punto donde se procesa el encabezado.
Dirección Fuente (32)	Dirección de origen (128)	Especifica la dirección de origen del paquete.
Dirección Destino (32)	Dirección Destino (128)	Especifica la dirección de destino del paquete
Opción (variable)	Trasladado a Cabecera de extensión	Campo de opción en IPv4 es un campo de longitud variable, contiene datos sobre la información del paquete que no se pudieron integrar en otros campos del encabezado. Para sustituir la opción de encabezado IPv4, se definen dos encabezados de opciones en IPv6: opciones de destino y opciones salto por salto.

4.1.5. Direccionamiento IPv6

En esta sección se describe la estructura, representación de una dirección IPv6, sus usos, los prefijos IPv6, así como los tipos de direccionamiento.

4.1.5.1. Estructura de una dirección IPv6

Una dirección IPv6 consta de tres partes como se indica en la figura 3:

- → El prefijo de enrutamiento global
- → El identificador de subred
- → El identificador de interface

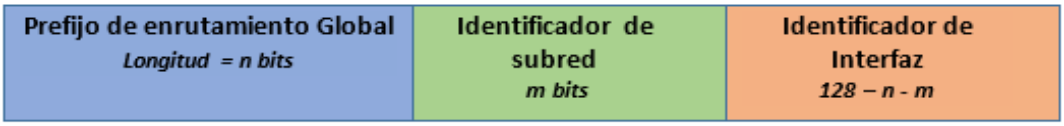


Figura 2: Estructura de una dirección IPv6 [23]

El prefijo de enrutamiento global se utiliza para identificar direcciones especiales o rango de direcciones asignadas a un sitio; El identificador de subred es utilizado para identificar un enlace dentro de un sitio; El identificador de interfaz se utiliza para identificar una interfaz en un enlace y necesita ser único en ese enlace.

4.1.5.2. Representación de una dirección IPv6

Una d diferencia respecto a IPv4 es el tamaño de las direcciones, IPv6 tiene una longitud de 128 bits y están representadas en un formato hexadecimal en lugar de la notación decimal tradicional y separada cada parte por dos puntos en lugar de uno. Teniendo de esta forma 8 campos de 16 bits cada uno. Como cada dígito hexadecimal se asocia con 4 bits, cada campo de 16 bits será de 4 dígitos hexadecimales (0-F) [12].

La notación es la siguiente:

2001:0db8:0000:0000:130f:0000:0000:140b

Puesto que no es práctico registrar todos estos ceros, pueden omitirse con ciertas convenciones:

- ✓ Los ceros a la izquierda se pueden eliminar para cualquier grupo de dígitos entre dos puntos, pero cada bloque debe tener al menos un dígito. El resultado sería entonces:

2001:db8:0:0:130f:0:0:140b

- ✓ Una serie de ceros y dos puntos también puede ser abreviado como dos puntos. El resultado es ahora:

2001:db8:0:0:130f::140b

Nota: *Formato no válido:* ***2001:db8::130f::140b*** *puesto que genera ambigüedad, por lo que no se debe eliminar grupos de ceros separados.*

- ✓ No se hace distinción entre mayúsculas y minúsculas **"DB8" es equivalente a "db8"** , tal como se indica en el ejemplo:

2001:DB8:0:0:130f::140B

2001:db8:0:0:130f::140b

- ✓ Para especificar un puerto en una determinada dirección IPv6, esta debe estar encerrada por paréntesis cuadrados en la forma **[dirección-ipv6]: puerto.**

[2001:12ff:0:4::2]:80

4.1.5.3. Prefijos IPv6

Los prefijos IPv6 se especifican en un formato similar a la notación CIDR (Classless Interdomain Routing /Enrutamiento entre dominios sin clase) de IPv4. Como muchos bits del prefijo son significativos se expresan en la notación IPv6 estándar, seguido por una barra diagonal y un recuento decimal de exactamente cuántos bits significativos hay. El

formato sería el siguiente **DirecciónIPv6 / Longitud de prefijo.** Así que las siguientes cuatro especificaciones de prefijo son equivalentes [11], [14], [15]:

2001:db8:dead:beef:0000:00f1:0000:0000/96
2001:db8:dead:beef:0:f1:0:0/96
2001:db8:dead:beef::f1:0:0/96
2001:db8:dead:beef:0:f1::/96

4.1.5.4. Uso del espacio de direcciones IPv6

Muchos rangos de direcciones IPv6 están reservados o definidos para fines especiales por los estándares IPv6 de IETF y por la autoridad asignada del número de Internet (IANA). La TABLA III presenta las principales asignaciones y los usos de cada espacio de dirección [16].

TABLA III: USOS DE LAS DIRECCIONES IPV6

Tipo de Direcciones	Prefijo Binario	Notación IPv6	Usos
Loopback	00…1 (128 bits)	::1/128	Dirección lookback (Bucle invertido) en cada interfaz [RFC 2460]
6to4	0010 0000 0000 0010	2002::/16	6to4 [RFC 3056]
Documentación	0010 0000 0000 0001 0000 1101 1011 1000	2001:db8::/32	Únicamente para efectos de documentación [RFC 3849]
Teredo	0010 0000 0000 0001 0000 0000 0000 0000	2001:0000::/32	Teredo [RFC 4380]
Multicast	1111 1111	FF00::/8	Espacio de direcciones multicast [RFC 4291]

Link-Local Unicast	1111 1110 10	FE80::/10	Link-Local Unicast
ULA(Unique Local Address)	1111 110	FC00::/7	Espacio de direcciones local únicas, unicast y anycast [RFC 4193]
No especificada		:: (todos ceros)	
Global Unicast	001	2000::/3	Asignado Global unicast y anycast [RFC 4291]
Direcciones IPv4 embebidas	00…1111 1111 1111 1111 (96 bits)	::FFFF/96	Prefijo para incrustar una dirección IPv4 en una dirección IPv6

4.1.6. Tipos de direcciones IPv6

En IPv4 se conocen direcciones unicast, broadcast y multicast. Con IPv6, desaparece la dirección de broadcast y en su lugar se utilizan direcciones de multidifusión (multicast). La dirección anycast, un nuevo tipo de dirección introducido en la RFC 1546 [20], han sido utilizadas anteriormente en el mundo IPv4 pero probablemente será utilizada sobre una base amplia con IPv6 [7].

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Una misma interfaz de un nodo puede tener asignada múltiples direcciones IPv6. Existen tres tipos de direcciones IPv6 [17]:

- Unicast
- Anycast
- Multicast

A continuación se describe de una manera más profunda cada una de las direcciones IPv6.

4.1.6.1. Unicast

Identifica a una única interfaz. Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada por dicha dirección. Es el equivalente a las direcciones IPv4 actuales. Las direcciones Unicast se pueden dividir en:

- Unicast Globales
- Unicast de Enlace Local
- Unicast de Sitio Local

Direcciones Unicast Globales

Estas direcciones han sido diseñadas para ser agregadas o resumidas de forma que produzcan una infraestructura de enrutamiento eficaz; el prefijo para las direcciones unicast globales es 2000::/3.

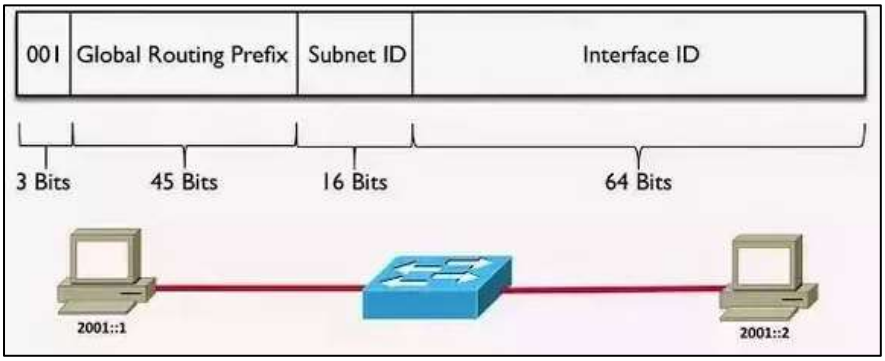


Figura 3: Esquema de una Dirección Unicast Global [24]

Cabe destacar que las direcciones únicas globales equivalen a las direcciones públicas IPv4.

Direcciones Unicast de Enlace Local (link local)

Estas direcciones han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento de vecinos, o situaciones en las que no hay routers. Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local). Tienen el siguiente formato [21]:

Figura 4: Estructura de una Dirección de enlace local [Autora]

Se trata de direcciones FE80::<ID de interfaz>/10. Las direcciones de enlace local equivalen a las direcciones IPv4 de direccionamiento privado que utilizan el prefijo 169.254.0.0/16

Direcciones Unicast de Sitio local (Site Local)

Estas direcciones permiten direccionar dentro de un "sitio" local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los encaminadores no deben de retransmitir fuera del sitio ningún paquete cuya dirección fuente o destino sea local de sitio (su ámbito está limitado a la red local o de la organización) [21].

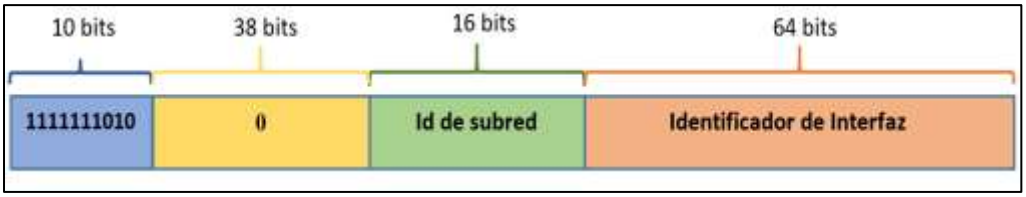


Figura 5: Estructura de una Dirección de sitio local [Autora].

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10. Las direcciones de sitio local, equivalen al espacio de direcciones privadas de IPv4: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16

Actualmente las direcciones Site-Local están siendo sustituidas por las ULA (Unique Local Address) esto debido a que el concepto de Site como tal es un concepto ambiguo y propenso a muchas interpretaciones, por ejemplo, Site es: un piso, un edificio, las oficinas en un país, toda una empresa. Las ULAs definidas en el RFC 4193 son específicamente creadas para comunicaciones entre dispositivos Internos en un ámbito (por lo general una empresa) [15].

Cabe mencionar que un dispositivo puede tener muchas direcciones IPv6 y por ello para comunicarse internamente se utiliza ULA y para comunicarse con el exterior se utilizan las

direcciones globales. Debido a lo mencionado anteriormente, las ULAs pueden ser enrutadas solo dentro de la empresa o entidad, no deben llegar a Internet. El prefijo asignado para ULAs es fc00::/7

Direcciones IPv6 con direcciones IPv4 incrustadas

Consiste en que la primera parte de la dirección IPv6 utiliza la representación hexadecimal y el otro segmento de IPv4 está en formato decimal.

La dirección se divide en dos niveles, superior e inferior y estos a su vez se subdividen. El nivel superior se fragmenta en seis campos con valores hexadecimales de 16 bits seguidos del nivel inferior compuesto de 4 campos con valores decimales de 8 bits, como lo indica la Figura 7:

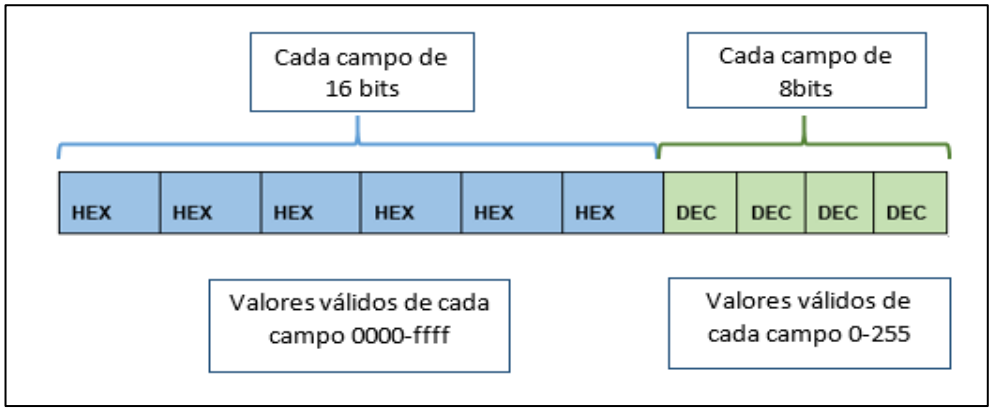


Figura 6: Direcciones ipv6 con direcciones ipv4 incrustadas [23]

Existen dos tipos de direcciones IPv6 que tienen direcciones IPv4 incrustadas:

Dirección IPv6 compatible con IPv4. La dirección compatible con IPv4 **0:0:0:0:0:0:w.x.y.z** (donde w.x.y.z es la representación de una dirección IPv4) es utilizada para establecer un túnel automático que lleva paquetes IPv6 sobre una infraestructura de enrutamiento IPv4. La representación de estas direcciones se indica en la Figura 8, donde los primeros 96 bits son rellenados con 0, y los siguientes 32 bits se componen de direcciones IPv4 [22].

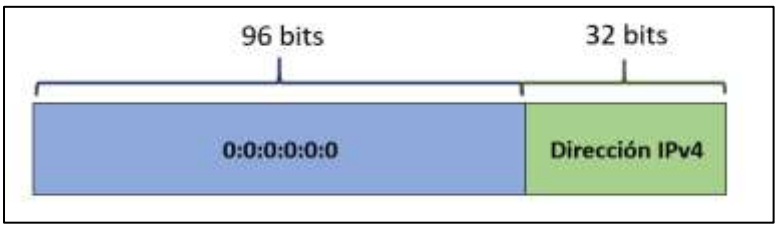


Figura 7: Direcciones IPv6 compatible con direcciones IPv4 [Autora]

Dirección IPv6 mapeada a IPv4. La dirección **0:0:0:0:0:FFFF:w.x.y.z** o **::FFFF:w.x.y.z** se utiliza para representar un nodo exclusivo de IPv4 ante un nodo IPv6. Los nodos usan direcciones IPv6 mapeadas a IPv4 de forma interna solamente. Estas direcciones no son conocidas fuera del nodo y no llegan al cable de comunicación como direcciones IPv6, es decir la dirección de IPv4 nunca se utiliza como dirección de origen o destino de un paquete IPv6 [25].

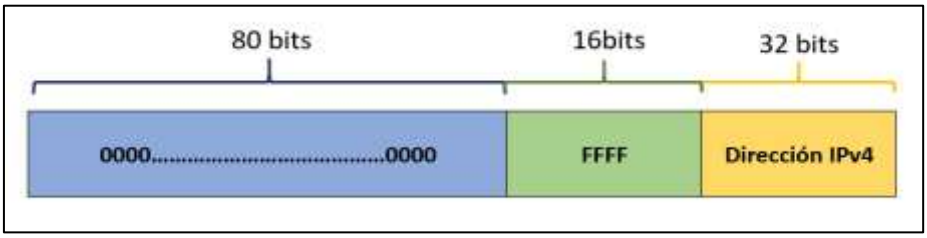


Figura 8: Direcciones ipv6 mapeadas a IPv4 [Autora]

4.1.6.2. Anycast

Identifican un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección de unidifusión se entrega a una de las interfaces identificados con dicha dirección (la "más cercana", de acuerdo con la medida de distancia del protocolo de ruteo) [13].

El RFC 1884 da una referencia sobre posibles usos para este tipo de direcciones, entre ellos destaca [11]:

- Identificación de un conjunto de enrutadores pertenecientes a un Proveedor de Servicio de Internet (ISP)
- Identificación de un conjunto de enrutadores agregados a una subred particular
- Identificación de un grupo de enrutadores que sirven como entrada a un dominio en particular.

- Utilizado en redes con soporte para movilidad IPv6 para localizar los agentes de Origen.

4.1.6.3. Multicast

Identifican un conjunto de interfaces (normalmente pertenecientes a diferentes nodos). Un paquete enviado a una dirección de multicast se entrega a todas las interfaces identificadas por esa dirección [13].

El formato de las direcciones multicast es el siguiente:

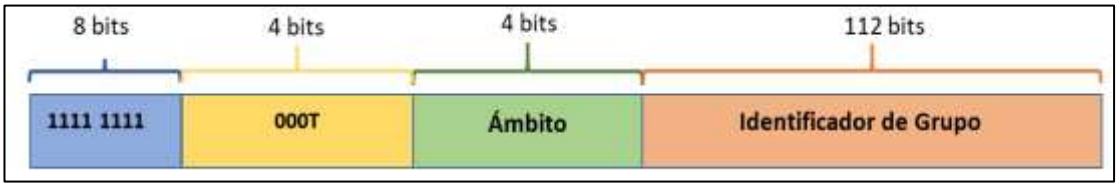


Figura 9: Formato de Direcciones Multicast

La dirección multicast comienza con el prefijo FF00::/8 (indicados por los primeros 8 bits), el bit T indica:

- ✓ Si T = 0, la dirección está asignada permanentemente, esto lo realiza autoridad de numeración global de Internet.
- ✓ Si T = 0, la dirección es temporal.

Los siguientes 4 bits indican el ámbito de una dirección, limitando cuán lejos esta dirección multicast es capaz de llegar. Los ámbitos están definidos en hexadecimal y son los siguientes:

TABLA IV: SIGNIFICADO DE LOS BITS DE ÁMBITO DE LAS DIRECCIONES MULTICAST

Valor	Ámbito
0	Reservado
1	Ámbito Local de Nodo
2	Ámbito Local de Enlace
3	No asignado
4	
5	Ámbito local de sitio
6	No asignado

7	
8	Ámbito local de organización
9	No asignado
A	
B	
C	
D	
E	Ámbito Global
F	Reservado

El identificador de grupo, identifica al grupo de multicast al que se hace referencia, sea permanente o temporal dentro de un ámbito específico.

4.2. MECANISMO DE TRANSICIÓN

Una de las premisas del diseño de IPv6, fue que pudiera realizarse una transición lenta hacia la nueva versión del protocolo IP, evitando pasar de una versión a otra en forma abrupta. El plan original para desarrollar IPv6 fue usar un mecanismo de coexistencia con IPv4 [21] razón por la cual se diseñaron varios mecanismos que permitan la convivencia entre ambas versiones, estos mecanismos son:

- Doble Pila (Dual Stack)
- Túneles
- Traducción de Direcciones

4.2.5. Doble pila (Dual Stack)

Se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red. Cuando se establece una conexión hacia un destino sólo IPv4, se utilizará la conectividad IPv4 y si es hacia una dirección IPv6, se utilizará la red IPv6, como indica la Figura 10.

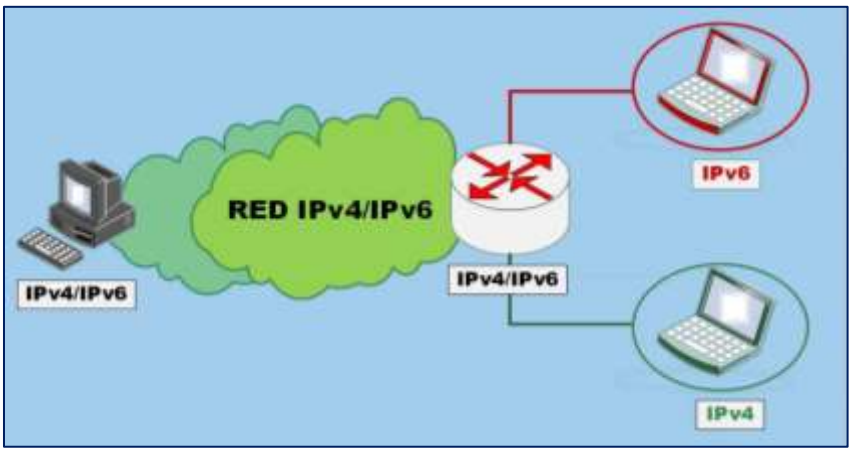


Figura 10: Esquema del Mecanismo de Doble Pila [Autora].

Un nodo que se implementa con protocolos IPv4 e IPv6, puede ser operado en uno de los tres modos siguientes [15]:

- Con la pila IPv4 habilitada pero la pila IPv6 deshabilitada.
- Con la pila IPv6 habilitada pero la pila IPv4 deshabilitada.
- Con las dos pilas habilitadas.

Nodos IPv4/IPv6 con pila IPv6 deshabilitada trabajan como un nodo IPv4 enteramente. Así mismo ocurre para los que trabajan con la pila IPv4 deshabilitada, su comportamiento será como el de un nodo IPv6.

Este mecanismo de dualidad permite a los servidores, clientes y aplicaciones moverse gradualmente hacia el nuevo protocolo provocando un mínimo impacto durante el proceso de transición [12].

Como se mencionó anteriormente una red de doble pila es una infraestructura capaz de encaminar ambos tipos de paquetes (IPv4-IPv6), razón por la cual existen algunos aspectos a tener en cuenta [13]:

- ♣ Configuración de los servidores DNS
- ♣ Configuración de los protocolos de ruteo
- ♣ Configuración de los firewalls
- ♣ Cambios en el gerenciamiento de red

4.2.6. Túneles

Considerado uno de los mecanismos más antiguos para poder atravesar redes en las que no se tiene soporte nativo del protocolo que se está utilizando. Se utiliza para conectar dos nodos de IPv6 con Redes IPv4, pero también se puede encontrar la situación inversa.

El proceso de túnel involucra tres pasos: encapsulamiento, desencapsulamiento y administración del túnel. Este mecanismo encapsula los paquetes de un protocolo a otro. En la Figura 12, se pude observar como los paquetes procedentes de un nodo IPv6 son transportados por medio de encapsulamiento IPv4 mediante un dispositivo de doble pila de protocolos (normalmente routers), se propagan a lo largo de la red IPv4, atraviesan el segmento de red que no los soporta y en el dispositivo de doble pila de destino son desencapsulados y entregados en forma de IPv6 nuevamente [26], [27].

Figura 11: Encapsulación de Datagramas [29]

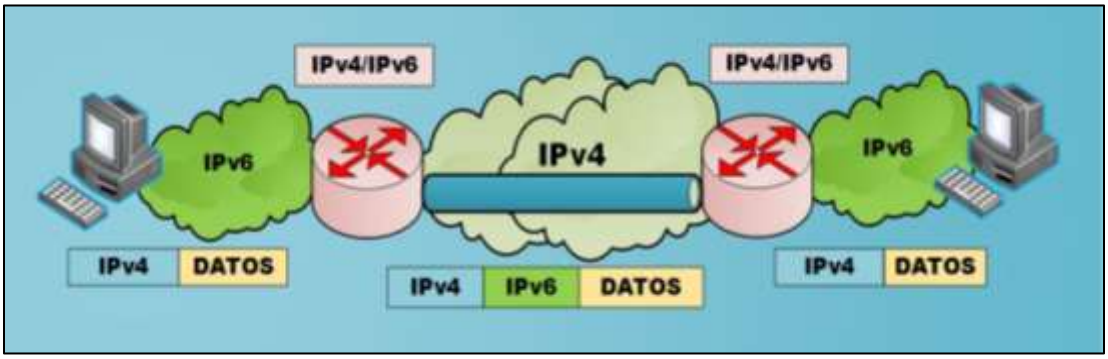


Figura 12: Esquema del Mecanismo Túneles [Autora].

Un paquete puede ser encapsulado de cuatro maneras diferentes [11]:

a. Router to Router
b. Host to Router
c. Router to Host

d. Host to Host

En los dos primeros casos (a y b), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. El extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel es determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina “túnel configurado”, describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (c y d), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina “túnel automático” [29].

Existen problemas del desempeño asociados con el “tunnelling”, como son la latencia debido a que deben realizar los procesos de encapsulamiento y desencapsulamiento. Hay un inconveniente más de desempeño debido al uso de ancho de banda adicional (payload overhead), aunque este último es normalmente marginal.

4.2.6.1. Tipos de Túneles

En la TABLA V, se describe las características, ventajas e inconvenientes de los tipos de túneles:

TABLA V: Tipos de Túneles

Mecanismo Túneles	Características	Ventajas	Inconvenientes
Túneles Configurados	- Configuración manual de los extremos del túnel. - Dos direcciones por cada extremo del túnel (Una IPv4 y una IPv6).	- Túneles soportados por muchas plataformas: Cisco, Linux, Windows, etc. - Transparente para IPv6, no requiere	- No escala, son manuales. - Overhead (Dos cabeceras)

		cambiar las aplicaciones.	
Túneles Automáticos	- Unidireccional. - Se usa cuando el destino es un nodo. - Los extremos se configuran automáticamente. - La dirección destino se deduce a partir de la IPv6. Este tipo de direcciones se las conoce como “IPv4 compatible”.	- Más fáciles de gestionar, puesto que no son manuales.	- Se necesita una dirección IPv4 por host. - Solo tiene sentido para comunicar host individuales.
Túnel Broker	- Facilita la configuración de túneles. - Encaja perfectamente en el caso de un nodo IPv6 aislado (con conectividad IPv4) que quiera acceder al mundo IPv6. - Es considerado como un ISP IPv6.	- Permite al ISP IPv6 controlar completamente el acceso. - Requieren escasa configuración, por lo que son fáciles de administrar.	- Overhead (Dos cabeceras)
Túnel 6to4	- Conexión directa entre dos redes a través de túneles dinámicos. - Los extremos del túnel son los router de cada red.	- Los túneles se configuran dinámicamente, por lo que no hace falta configurarlos. - Solo se establece un túnel cuando es necesario.	- Solo se puede usar el prefijo 2002::/16. - Se necesita de direcciones IPv4.

	- No se requiere direccionamiento IPv6. - Mediante DNS se conoce cuál es el extremo del túnel al que se va a enviar el paquete. - Los router conocen las subredes mediante "Router Advertisements".	- Cada red IPv6 solo necesita una red IPv4 global, con lo que se puede tener hasta 2^{32} redes IPv6.	

4.2.7. Traducción

Consiste en utilizar algún dispositivo en la red que convierte los paquetes de IPv4 a IPv6 y viceversa. Este dispositivo tiene que ser capaz de realizar la traducción en los dos sentidos de forma que permitir la comunicación [15].

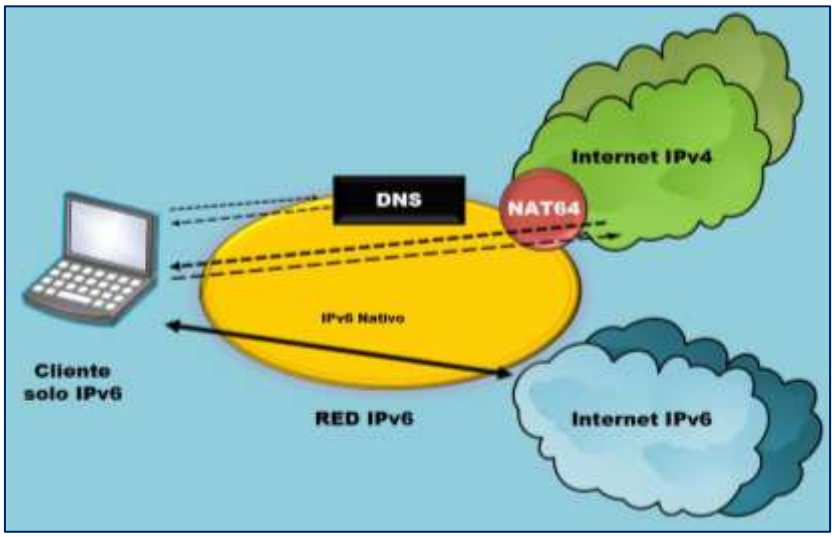


Figura 13: Esquema del Mecanismo de Traducción [Autora].

La traducción se puede implementar mediante puertas de enlace de capa de aplicación, o mediante el uso de la capa de red IPv6/IPv4, con tecnologías de traducción como IIP/ ICMP Algoritmo de traducción (SIIT) [15], Stateful NAT64 [19], DNS64 [20].

El modelo de implementación más recomendable para la traducción es una combinación de stateful NAT64 y DNS64 también conocido como NAT64/DS64 [21]: la red es IPv6 nativa y para llegar a sitios que son sólo IPv4 se realiza una traducción al estilo NAT, mediante un mapeo entre los paquetes IPv6 e IPv4. Se utiliza un prefijo especial para mapear direcciones IPv4 a IPv6: 64:ff9b::/96.

Es necesario también utilizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A) [22].

Este mecanismo de transición no es muy recomendado, ya que tiene varias limitaciones entre ellas que el protocolo de seguridad (IPSec) no puede ser usado a través de un dispositivo de traslación, además de ser considerada la peor solución, puesto que la traducción no es perfecta y requiere soporte de ALGs como en el caso de los NATs IPv4 [28].

4.3. DNS E IPV6

En la presente sección se aborda temas relacionados al DNS y su relación con el protocolo IP (IPv6), tal es el caso de la inclusión de los nuevos registros que rigen a IPv6; sin embargo previo a ello es vital conocer ciertas temáticas como lo es el concepto de DNS, su funcionamiento, tipos de servidores DNS, usos, resolución DNS con pila dual, entre otros.

4.3.5. Introducción

El DNS es la base actual del funcionamiento de internet y se encarga de traducir los nombres de dominios de la web a la IP del ordenador donde está alojada la página que estamos buscando. La comunicación en Internet sólo funciona en base a direcciones IP, resultando complicado para un usuario recordar dicha dirección, razón por la que surge el DNS que permite que usemos nombres de dominio en lugar de un número, lo que resultaría más sencillo para los usuarios en general.

Este sistema fue extendido para dar capacidad a Direcciones IP más largas como lo son las direcciones IPv6 mediante la creación de nuevos tipos de registros, y las nuevas versiones de los servidores de nombres, incluyendo BIND (Berkeley Internet Name Domain-Dominio de nombres de Internet de Berkeley) fueron lanzados para apoyar a los nuevos tipos de registro, así como el uso de IPv6 para el transporte de consultas y respuestas [41].

4.3.6. ¿Qué es un servidor DNS?

El Domain Name System, Servidor de Nombres de Dominio o simplemente DNS es denominado como una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.

Soporta tanto IPv4 como IPv6, y la información se almacena en forma de registros Resource Records (RR) de distintos tipos los cuales pueden almacenar direcciones IP u otro tipo de información. Esta información se agrupa en zonas, que corresponden a un espacio de nombres o dominio y que son mantenidas por el servidor DNS autoritativo de la misma.

4.3.7. Usos del Servidor DNS

Las principales funciones que desempeña el DNS son:

- **Resolución de nombres**: Dado el nombre completo de un host, obtener su dirección IP.

  www.unl.edu.ec → **192.16.24.2**
  → **2001:db8:7:ff02:3c:8289::e770**

- **Resolución inversa de direcciones**: Es el mecanismo inverso al anterior. Dada una dirección IP, obtener el nombre de host correspondiente.

  192.16.24.2 →
  2001:db8:7:ff02:3c:8289::e770 → www.unl.edu.ec

- **Resolución de servidores de correo**: Dado un nombre de dominio (por ejemplo gmail.com) obtener el servidor a través del cual debe realizarse la entrega del correo electrónico (en este caso, gmail-smtp-in.l.google.com).

4.3.8. Funcionamiento del DNS

El DNS para ser útil debe entregar información, en forma de respuestas a consultas, desde un servidor de nombres autoritativo para el PC del usuario o cualquier otra aplicación (como

un agente Mail SMTP o un cliente FTP) que necesita para resolver nombres a direcciones IP. La Figura 14 muestra cómo un navegador que se ejecuta en un PC usa y accede al DNS y presenta todas las piezas que componen el DNS [43].

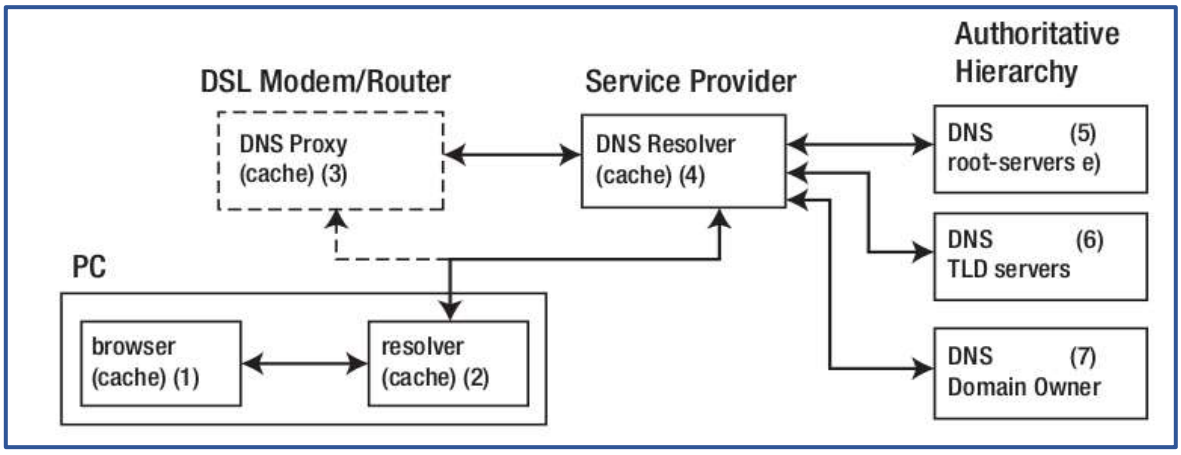


Figura 14: Funcionamiento del DNS

- Cuando los usuarios ingresan una URL, como www.ejemplo.com, en su navegador preferido, (1) primero busca en su caché interna para verificar si ya tiene los datos. Si no, el navegador llama a una biblioteca de software interna o un programa llamado resolver (2).
- Un resolver (resolución) DNS se considera como una pieza muy compleja de software, pero los estándares de DNS permiten una versión simplificada llamada stub-resolver. Los Stub-resolvers se instalan en todas las plataformas como Windows y los sistemas * nix (por ejemplo, Linux, UNIX y BSD). La mayoría de los stub-resolvers modernos también proporcionan servicios de caché, por lo que si al usuario le gusta usar descripciones largas que podría ser llamado un caché stub-resolver. Por lo tanto como era de esperar, el stub-resolver inspecciona primero su caché e inmediatamente suministra el resultado si está presente. Si no, crea una consulta DNS (una pregunta) y la envía a un router o Módem DSL (3) o directamente a un resolvedor de DNS (4) dependiendo de cómo el PC o Servidor fue configurado.
- El router normalmente proporciona un servicio Dynamic Host Configuration Protocol (DHCP). En este estilo de conexión, cuando un PC o servidor está encendido, se ejecuta a través de una secuencia de inicio durante la cual un Número de transacciones DHCP se producen. Al final de este proceso, a la

configuración se habrán suministrado los siguientes parámetros: una dirección IP y una o más direcciones DNS. Aunque en algunos casos las direcciones DNS suministradas apuntarán directamente a la resolución de DNS del proveedor de servicios (4), cada vez más la o las direcciones DNS apuntan a la DSL o router local (3), que contendrá un proxy DNS. Dependiendo de las políticas del fabricante del dispositivo y del proveedor de servicios de Internet, la funcionalidad del proxy DNS varía enormemente de una simple operación de pass-through (no se ha cambiado nada), al almacenamiento en caché y otras operaciones más intrusivas diseñadas principalmente para reducir la carga y acelerar las respuestas del usuario. No se han definido estándares para el proxy DNS, pero el RFC 5625 contiene una serie de recomendaciones destinadas a minimizar los problemas de funcionamiento. En todos los casos, si los datos no están disponibles en cualquier caché local, las consultas se reenvían para la resolución de DNS (4).

- Un PC o servidor puede acceder indirectamente a la resolución DNS (4) a través del módem/router DSL (3), como se ha descrito anteriormente, o directamente a través de la configuración manual o mediante el servicio DHCP. El resolver siempre contiene una caché que primero inspecciona las respuestas disponibles a las consultas del cliente. Resolver puede ser y con frecuencia se conoce como un servidor de nombres de caché o incluso un servidor de nombres recursivo debido a que este resolver normalmente proporciona servicios para un número muy grande de clientes y proxies, su caché es posible que ya contenga un montón de respuestas, por lo que la probabilidad de una caché "hit" (los datos requeridos existe en la caché) será alta. Sin embargo, si la respuesta no está presente en su caché, este resolver, a diferencia de todos los anteriores stub-resolver y proxies DNS perseguirá a la jerarquía autoritaria de DNS (5), (6), y (7) para obtener la respuesta autorizada a la consulta del usuario, que luego envía al usuario y coloca en su caché para su uso futuro por otras consultas.

Es importante enfatizar en este escenario el papel desempeñado por varios cachés que son en gran medida diseñados para acelerar la respuesta del usuario. Además cabe enfatizar que cualquier programa de DNS, ya sea una resolución de DNS o un servidor de nombres autoritativo, normalmente hace tres cosas:

→ Lee uno o más archivos de zona, que describen dominios de los que es responsable

o va a utilizar.

→ Dependiendo de la funcionalidad del software de DNS, lee un archivo de configuración, el cual describe distintos comportamientos requeridos (por ejemplo, almacenar en caché o no).

→ Responde a preguntas (consultas) de clientes locales o remotos (otro servidor de nombres, resolvers o proxies).

4.3.9. Tipos de Registros de Recursos (RRs) DNS

En la tabla se da a conocer los principales registros DNS, su especificación, descripción y se expone si el registro es opcional u obligatorio en un archivo de zona.

TABLA VI: PRINCIPALES REGISTROS DNS

Nombre del Registro (RRs)	Especificación	Descripción	Opcional / Obligatorio
A	RFC 1035	Se utiliza para traducir nombres de hosts a direcciones IPv4. Define la dirección IPv4 de todos los hosts (o servicios) que existen en la zona y están obligados a ser públicamente visibles. Hay cero o más registros A en un archivo de zona.	Opcional
AAAA	RFC 3596	Se utiliza para traducir nombres de hosts a direcciones IPv6. Define la dirección IPv6 de todos los hosts (o servicios) que existen en la zona y están obligados a ser públicamente visibles. Hay cero o	Opcional

		más registros AAAA (quad A) en un archivo de zona.	
CNAME (Canonical Name)	RFC 1035	El nombre canónico es un alias para un host determinado. (No define una dirección IP, sino un nuevo nombre.) Este registro permite que uno de los host se defina como el nombre alias de otro host.	Opcional
MX (Mail Exchange)	RFC 1035	Define el servidor encargado de recibir el correo electrónico para el dominio. Puede haber cero o más registros MX en un archivo de zona; si el dominio no proporciona servicios de correo electrónico no hay necesidad de un RRs MX.	Opcional
NS (Name Server)	RFC 1035	Especifica el servidor (o servidores) de nombres que es autoritativo para una zona o dominio.	Obligatorio
PTR (Pointer)	RFC 1035	Especifica un registro inverso, a la inversa del registro A, permitiendo la traducción de direcciones IP a nombres. Usado por IPv4 e IPv6	Opcional
		El registro SOA debe aparecer como el primer registro en un	

SOA (Start of Authority)	RFC 1035/2308	archivo de zona. Describe las características globales de la zona o dominio; solo puede haber un RRs en un archivo de zona.	Obligatorio
TXT (Text)	RFC 1035	Permite asociar información adicional a un dominio. Además se usa para otros fines, como el almacenamiento de claves de cifrado, DKIM) DomainKeys o SPF (Sender Policy Framework). Arbitrary text associated with a domain. Also used for SPF and DKIM antispam records.	Opcional

4.3.10. Mapeo Inverso y Directo en IPv6

Como se mencionó anteriormente los datos de un registro A corresponden a una dirección de 32 bit en formato de octetos, lo que no permite a este registro adaptarse a las direcciones IPv6 de 128 bits; motivo suficiente para que la IETF planteara una solución a este problema, el cual se describe en la RFC 1886 y consistía en un nuevo tipo de registro de direcciones: AAAA (quad A), para almacenar direcciones IPv6 de 128 bits, y un nuevo dominio IPv6 de traducción inversa ip6.int. Esta solución fue sencilla, lo suficiente como para ponerla en práctica en BIND 4. Pero está simple solución, no agradó a todo el mundo, por lo que se les ocurrió una mucho más compleja, la cual introdujo los nuevos registros A6 y DNAME y requería una completa revisión del servidor BIND a implementar. Después de mucho debate en la IETF el nuevo esquema A6/DNAME no fue aprobado y pasó a estado experimental, decayendo su uso en zonas de traducción inversa; Esto trajo el viejo RFC 1886 devuelta y por ahora, el registro AAAA es el adecuado para manejar el mapeo directo IPv6. El uso de ip6.int está en desuso, sobre todo por razones políticas, y ha sido

reemplazado por ip6.arpa, un nuevo espacio de nombres de resolución inversa para las direcciones IPv6 [42].

4.3.11. Resolución del DNS con Doble Pila

La máquina fuente hace consultas al servidor DNS para obtener la dirección IP de destino, si dicha dirección destino es IPv4 (Registro A) la máquina fuente envía datagramas IPv4. Si la dirección entregada por un servidor DNS corresponde a una dirección IPv6 (Registro AAAA), entonces la máquina fuente enviará datagramas IPv6. En caso que el destino tenga ambos protocolos, normalmente se preferirá intentar conectar primero por IPv6 y en segunda instancia por IPv4.

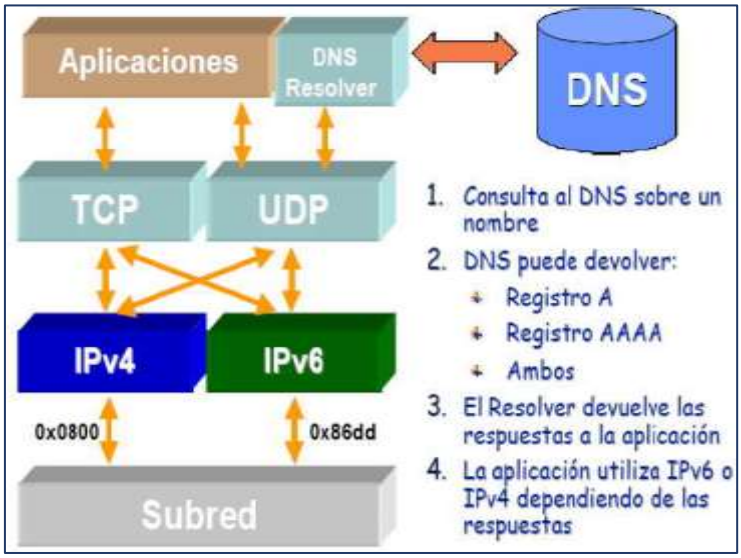


Figura 15: Resolución del DNS en Doble Pila

4.4. SERVIDOR WEB

Un servidor web es un programa encargado de atender y responder a las diversas peticiones de los navegadores, proporcionando los recursos que solicitan mediante el protocolo HTTP a través del puerto 80 o mediante el protocolo HTTPS (la versión segura, cifrada y autenticada de HTTP) a través del puerto 443.

4.4.5. Arquitectura del servidor web

La arquitectura utilizada es cliente /servidor en donde el cliente web hace una solicitud (mediante el método de petición GET) al servidor, y este atiende dicha solicitud. El Equipo Servidor atiende las peticiones recibidas desde los clientes web (navegadores) [31].

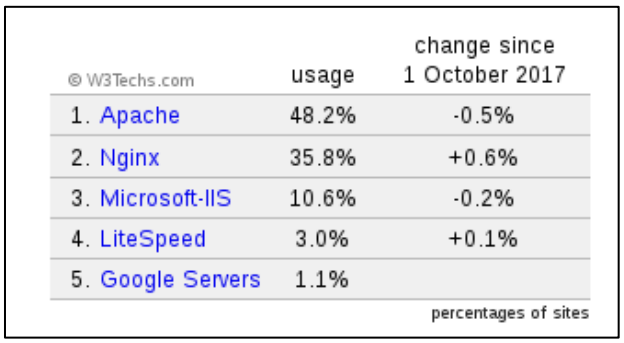
Figura 16: Arquitectura Cliente Servidor [31]

4.4.6. Funcionamiento de un servidor Web

- El usuario especifica en el cliente web la URL de la página que desea consultar.
- El cliente establece la conexión con el servidor web y solicita la página deseada.
- El servidor busca la página solicitada en su sistema de ficheros. Si la encuentra la transfiere, sino devuelve un código de error.
- El cliente interpreta el código HTML y muestra la página al usuario.
- Se cierra la conexión.

4.4.7. Principales Servidores Web

En Internet existen decenas de servidores web siendo los más utilizados: Apache, Internet Information Server (IIS) de Microsoft y Nginx de NGNIX.



© W3Techs.com	usage	change since 1 October 2017
1. Apache	48.2%	-0.5%
2. Nginx	35.8%	+0.6%
3. Microsoft-IIS	10.6%	-0.2%
4. LiteSpeed	3.0%	+0.1%
5. Google Servers	1.1%	

percentages of sites

Figura 17: Estadísticas de los principales servidores web [32]

Como se puede observar en la Figura 17, las estadísticas indican que Apache y Nginx son los servidores web más usado por los usuarios, seguido con un menor porcentaje por Microsoft-IIS.

Para conocer un poco más de cada uno de estos servidores web, se los describe a continuación:

4.4.7.1. Microsoft IIS

Es el Servidor Web de Microsoft sobre Windows, el IIS (Internet Information Server), es el motor que ofrece esta compañía a modo profesional, con él es posible programar en ASP (Active Server Pages, Páginas de Servidor Activo) las cuales vienen a ser algo similares al PHP, este servidor posee componentes programables desde ASP accediendo a cada uno de sus módulos para una función específica. IIS soporta IPv6 desde la versión 6.0.

4.4.7.2. Nginx

Nginx (motor x) es un servidor proxy HTTP y reverso, un servidor proxy de correo y un servidor proxy genérico TCP / UDP, originalmente escrito por Igor Sysoev. Según Netcraft, nginx representó el 29.43% de los sitios más activos en octubre de 2017. Estas son algunas de las historias de éxito: Dropbox, Netflix, Wordpress.com, FastMail.FM, Facebook [33]. Es un servidor web de alto rendimiento que tiene como principal característica ser sumamente ligero, lo que nos permite servir aplicaciones web con una velocidad muy superior a la de sus competidores más directos; otras de sus fortalezas es que es un software libre o abierto, lo que nos permite trabajar sin tener que realizar pago alguno por licencia de funcionamiento, además de contar con sistemas de protección y encriptado de datos que

complementan todo el paquete de software.

Características de Nginx

Entre las características del servidor Web Nginx destacan las siguientes características [34]:

- Se trata de un software que es asíncrono, a diferencia de Apache que está basada en procesos.
- Capaz de manejar más de 10.000 conexiones simultáneas con un uso bajo de memoria.
- Balanceo de carga, distribuye la carga entre los servidores que formen parte de la estructura, redirigiendo cada vez la petición hacia aquella máquina que tenga una menor carga.
- Alta tolerancia a fallos
- Soporte para TSL, SSL, FastCGI, SCGI o uWSGI, entre otros.
- Compatible con el nuevo estándar de direcciones Ipv6.
- Reescritura de URL´s, para crear URL´s amigables que nos ayuden en el proceso del posicionamiento web, aunque a diferencia de Apache, Nginx no hace uso del fichero .htaccess, sino que carga las reglas de reescritura directamente en su configuración.
- Permite limitar el número de conexiones concurrentes.
- Geolocalización basada en direcciones IP.

4.4.7.3. Apache

Es un poderoso servidor web, completamente libre, ya que es un software Open Source y con licencia GPL (General Public License). Apache es una muestra, al igual que el Sistema Operativo Linux , de que el trabajo voluntario y cooperativo dentro de Internet es capaz de producir aplicaciones de calidad profesional difíciles de igualar [35].

Características de Apache

Entre las principales características de Apache, se encuentran las siguientes [36], [37]:

- ♣ Multiplataforma: Está disponible para diferentes plataformas como: Linux, Windows, MacOs y aun así mantiene su excelente rendimiento.

- Modular: Puede ser adaptado a diferentes entornos y necesidades, con los diferentes módulos de apoyo que proporciona, y con la API de programación de módulos, para el desarrollo de módulos específicos.
- Extensible: gracias a ser modular se han desarrollado diversas extensiones entre las que destaca PHP, un lenguaje de programación del lado del servidor.
- Soporte de seguridad SSL y TLS
- Puede dar soporte a diferentes lenguajes, como Perl, PHP, Python.

En cuanto a Apache y su relación con el protocolo IPv6, será abordado con más detalle en la sección 6.4.2.3, en donde se explica las directivas a utilizar para indicarle que escuche pedidos HTTP en un socket IPv6, así como la creación de virtualhost con IPv4 e IPv6.

5. MATERIALES Y MÉTODOS

5.1. Métodos y Técnicas

Para la ejecución del presente proyecto de titulación fue conveniente y necesario la adopción de métodos y técnicas de investigación que permitieron obtener información relevante y fiable.

5.2.1. Métodos

En este apartado se describen los métodos utilizados en la ejecución del proyecto de titulación, los cuales han sido vitales durante todo el proceso de desarrollo, estos métodos se describen a continuación:

- **Método Inductivo**

  Este método fue utilizado para estructurar el marco teórico relacionado al tema, considerando que este método parte de un caso particular y se eleva a conocimientos generales, además permitió desarrollar cada uno de los objetivos específicos para así llegar a cumplir con el objetivo general.

- **Método Analítico**

  Se empleó este método para realizar el análisis de la situación actual del DNS y los servidores públicos, así como también permitió determinar el mecanismo de coexistencia entre IPv4 e IPv6 mediante un análisis a los diferentes mecanismos de transición.

- **Método Experimental**

  Este método fue empleado en el escenario de pruebas, puesto que se realizó las configuraciones a ser utilizadas en la implementación de IPv6 en el DNS y los servidores públicos.

5.2.2. Técnicas

Los métodos antes mencionados deben también tener el apoyo de algunas técnicas de investigación, para poder cumplir a cabalidad su función de permitir el desarrollo eficaz de un proyecto, razón por la cual se ha hecho uso de las siguientes técnicas:

- **Entrevista**

  Esta técnica forma parte importante para la realización y adecuado desarrollo del mencionado proyecto, ya que a través de la misma se logró obtener información acerca de los problemas a los que conlleva el no implementar el protocolo de internet versión 6, esta técnica fue aplicada al subdirector de redes y equipos informáticos de la UTI (ver ANEXO I)

- **Observación**

  La observación permite identificar la estructura de la red con la que cuenta la UNL, muy específicamente la estructura de los servidores públicos determinando que los mismos que se encuentran virtualizados en el Blade y ubicados en la DMZ.

- **Investigación Bibliográfica**

  Esta técnica permite adentrarse en información verificada y certificada, es decir, permite la obtención de información válida referente al tema, basada en investigaciones, tutoriales, tesis, libros, revistas, artículos, etc. que ayudaron a sustentar cada uno de los apartados o secciones contenidos en el proyecto.

- **Tutorías**

  La asesoría por parte del docente tutor y de los técnicos de la Unidad de Telecomunicaciones e información (UTI), constituyó un aporte fundamental para el

cumplimiento de cada uno de los objetivos del trabajo de titulación, ya que sus continuas sugerencias e indicaciones permitieron culminar con un proyecto exitoso.

6. RESULTADOS

Esta sección presenta los resultados obtenidos al culminar cada uno de los objetivos específicos y por ende se cumple con el objetivo general planteado al inicio de este proyecto.

En el primer objetivo se obtuvo información relevante relacionada a la situación actual como lo es las características hardware, software, así como también se pudo determinar los servidores que soportan IPv6. En el segundo objetivo se determinó el mecanismo de transición a ser utilizado en la implementación de IPv6; en el tercer objetivo se realizó el plan de direccionamiento IPv6 tomando como base el prefijo versión 6 asigno por ISP y se planteó una técnica para el direccionamiento en los diferentes servidores públicos; en el cuarto objetivo se realizaron las pruebas en el servidor proporcionado por la UTI en el que se configuró el DNS y el servidor web, finalmente en el quinto objetivo se implementó IPv6 en los servidores públicos, verificando la funcionalidad de la pila dual (IPv4-IPv6)

6.1. OBJETIVO 1: Analizar la situación actual del dns autoritario y servidores públicos para la implementación de IPv6.

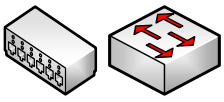
La Universidad Nacional de Loja se encuentra ubicada al sur de la ciudad de Loja en el sector “La Argelia”. Esta Institución está constituida por cinco Facultades Académico Administrativas (FAA) y una Dependencia Administrativa denominada Administración Central.

Las Facultades Académico Administrativas son: Facultad Jurídica, Social y Administrativa, Facultad Agropecuaria y de Recursos Naturales Renovables, Facultad de la Educación el Arte y la Comunicación, Facultad de Energía las Industrias y Recursos Naturales no Renovables, mismas que se encuentran localizadas en el Campus la Argelia, mientras la Facultad de la Salud Humana se encuentra ubicada en la calle Manuel Monteros detrás del Hospital “Isidro Ayora”.

En el edificio de Administración Central bloque 2, cuarto piso se encuentra la Unidad de Telecomunicaciones e Información la cual se compone de cuatro secciones: sección de desarrollo de software, sección de mantenimiento y equipos electrónicos, sección de Telecomunicaciones y la sección de Redes y Equipos Informáticos, esta última es el ente principal encargado de la administración, gestión y seguridad de la red de datos.

Para una mejor comprensión de los esquemas de redes mostrados a lo largo de este proyecto es necesario emplear la siguiente simbología:

TABLA VII: SIMBOLOGÍA DEL ESQUEMA DE RED

SÍMBOLO	DESCRIPCIÓN
	Firewall
	Internet
	Servidores
	Router
	Switch
	Fibra óptica
	UTP categoría 5e

6.1.5. Arquitectura de la red de datos de la Universidad Nacional de Loja.

La Universidad Nacional de Loja actualmente cuenta con una red LAN, con una arquitectura de red tipo estrella cuya topología es un modelo jerárquico de 3 capas: Capa de núcleo o CORE, capa de distribución y capa de acceso.

El Proveedor de Servicios de Internet (ISP) es la empresa Telconet S.A. que a través del CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado), organismo integrado por las Universidades e Instituciones de Investigación y Desarrollo de Ecuador, mantiene convenio con la UNL para brindar el servicio de internet, el mismo que llega a la institución mediante fibra óptica y cuyo ancho de banda para sus usuarios es de 450 Mbps de internet comercial y 1 Gbps de red avanzada, estos para que la institución brinde sus servicios de manera eficaz y eficiente.

La red de datos se compone de la interconexión del bloque de Administración Central con las Facultades Académico Administrativas.

La Figura 18, muestra el “backbone” de la infraestructura de la red de datos, donde se visualizan las principales conexiones tanto de la intranet como la extranet, así como los diferentes switches interconectados que transportan datos a través de las distintas dependencias, usando como medio de transmisión: fibra óptica, cable UTP categoría 5e.

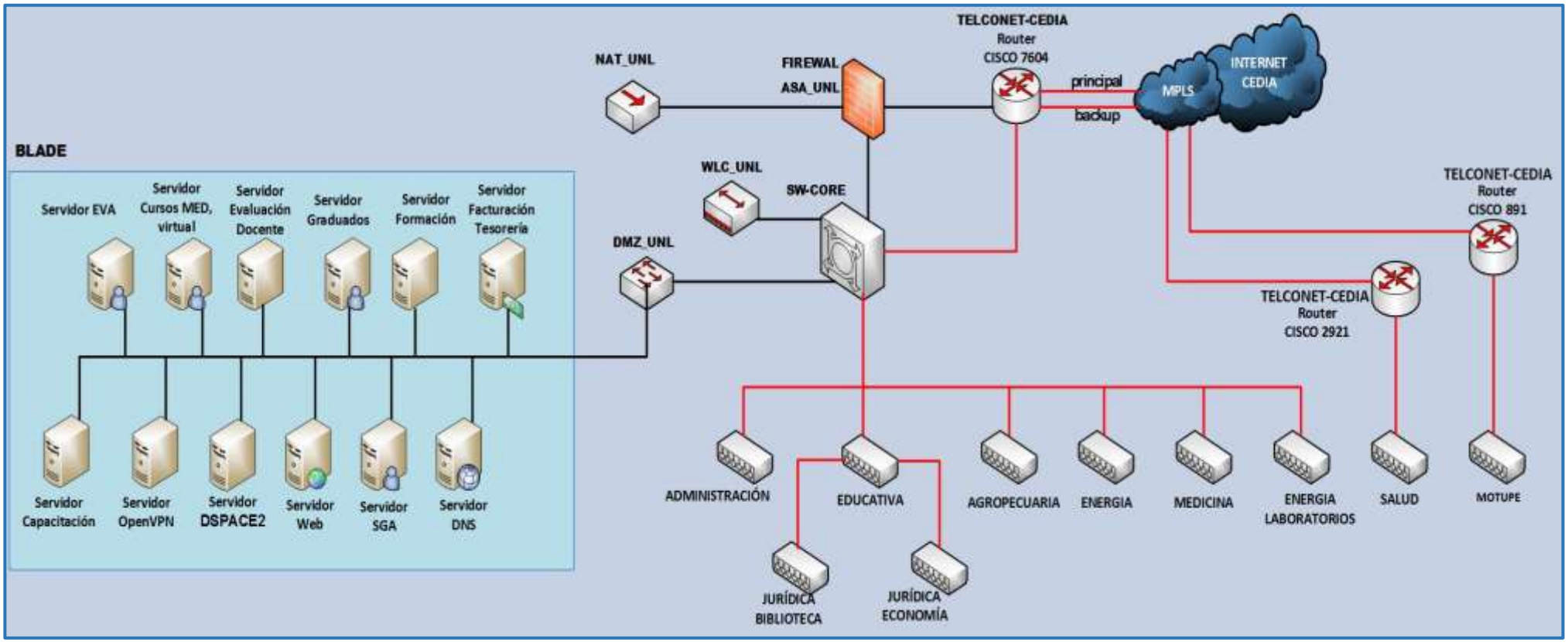


Figura 18: Backbone de la Universidad Nacional de Loja

Fuente: Unidad de Telecomunicaciones e Información (UTI)

Es importante mencionar que la facultad de Salud Humana y Motupe anteriormente estaban conectadas por radio enlace debido a la distancia a la que se encuentran ubicadas pero en la actualidad y gracias a las gestiones realizadas por la Unidad de Telecomunicaciones e Información (UTI) hay conexión mediante fibra óptica, siguiendo su conexión mediante cable UTP categoría 5e por los Switchs de Acceso que hace fácil la comunicación dentro del campus universitario a los usuarios finales.

En la actualidad la Universidad Nacional de Loja trabaja con el protocolo de internet versión 4, además tiene asignado un bloque de direcciones IPv6 prefijo /48 cuyo proveedor es el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA), pero no se encuentra en uso lo que hace que la Universidad no pueda comunicarse con aplicaciones y servicios de IPv6 que ya están dando servicio alrededor del mundo.

Como el objeto de investigación es el del DNS autoritario y los servidores públicos me centraré en el estudio de los mismos.

6.1.6. DNS autoritario y servidores públicos.

La Universidad Nacional de Loja hasta el momento dispone de 12 servidores con acceso público, los mismos que se encuentran virtualizados con el software KVM (Kernel-based Virtual Machine - máquina virtual basada en núcleo) y cuyo equipo utilizado para la virtualización es un servidor Blade. Los servidores tanto públicos como privados se encuentran ubicados en la DMZ (De-Militarized Zone - Zona Desmilitarizada) de la arquitectura de red.

Con el uso de una DMZ se crea una subred independiente (interna), para poder controlar mejor el acceso a los servidores, puesto que el objetivo de la DMZ es asegurar que los servidores de acceso público no puedan comunicarse con otros segmentos de la red interna, además es donde se establece por reglas del firewall cuales son servidores públicos y cuales privados.

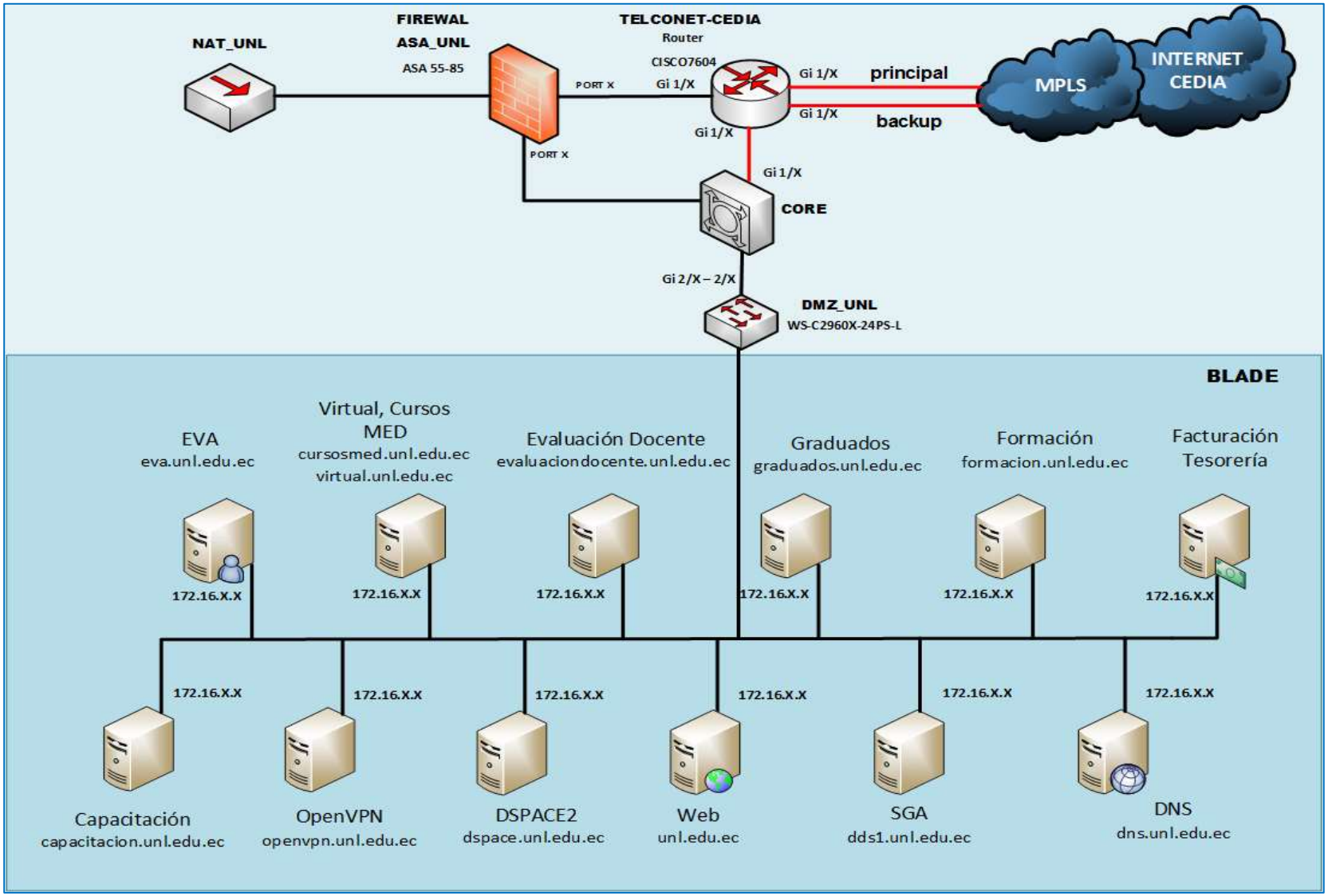


Figura 19: Topología Lógica del DNS autoritario y servidores públicos

El BLADE actualmente tiene el 70% de su capacidad ocupado, donde 6 cuchillas están totalmente copadas, de las cuales 4 son de sexta generación y 2 cuchillas de séptima generación, en las que se distribuye los servidores públicos y privados de la institución universitaria; en la siguiente figura se muestra una vista resumida del área de análisis para la implementación del protocolo IPv6:

Los servidores cuya finalidad es proporcionar servicios a los clientes, se encuentran el en el Centro de Centro de Procesamiento de Datos (CPD) ubicado en la Unidad de Telecomunicaciones e Información. En la Tabla VIII se presenta una breve descripción de la funcionalidad de cada uno de los servidores públicos.

TABLA VIII: DESCRIPCIÓN DEL SERVIDOR DNS Y SERVIDORES PÚBLICOS

Servidor	Descripción/Funcionalidad
DNS Autoritativo	Permite la resolución de Nombres a la IP, se encuentra configurado como DNS primario haciendo uso del domino unl.edu.ec con lo que facilita la resolución de nombres a los equipos finales en el campus universitario.
EVA (Entorno Virtual de Aprendizaje)	Contiene el entorno virtual de aprendizaje de la Universidad Nacional de Loja. Este servicio proporciona acceso restringido, por lo que solo está disponible para estudiantes y docentes.
Virtual, cursos (MED)	Contiene los diversos cursos virtuales que proporciona la Modalidad de Estudios a Distancia (MED)
Evaluación Docente	Contiene el sistema de evaluación de Docentes de la Universidad Nacional de Loja.

Graduados	Se encuentra alojada la página web de seguimiento a graduados, en la que consta información relacionada a los ex alumnos de la universidad.
Formación	Servidor utilizado para la impartición de cursos de computación
Capacitación	Se emplea para la capacitación en determinados momentos, es decir brinda un servicio temporal.
Open VPN	Permite Conexión remota, administración de equipos y el objetivo es poder acceder a las bases de datos científicas fuera del campus.
DSPACE2	Contiene el sistema bibliotecario en línea, se encuentran alojadas las tesis y trabajos de investigación realizados por estudiantes y docentes
Facturación Tesorería	Se emplea para la facturación en línea.
Web (unl.edu.ec)	Se encuentra el portal web de la Universidad Nacional de Loja. Además en este mismo servidor se encuentran varios subdirectorios que permiten servir con aplicaciones web información de cada una de las dependencias y Facultades Académico Administrativas, lo que permite la interacción de los usuarios con las páginas.
SGA (Sistema de Gestión Académico)	Accesible por medio de la intranet universitaria contiene la información académica tanto de estudiantes como de docentes, tales como control registro de calificaciones, asistencias, mallas curriculares, etc.

6.1.7. Características hardware del DNS autoritario y servidores públicos

En la presente tabla se describen algunas características hardware como marca, modelo, capacidad de RAM, HD, CPU y el número de la cuchilla en que el servidor se encuentra alojado en el BLADE.

TABLA IX: CARACTERÍSTICAS HARDWARE DEL DNS Y SERVIDORES PÚBLICOS

Servidor	Marca	Modelo	RAM (GB)	HD (GB)	CPU	Cuchilla (BLADE)
DNS Autoritativo	HEWLETT PACKARD	PROLIANT BL460C G7	512 MB	10	Intel(R) Xeon(R) 2.53GHz	Cuchilla 10
EVA(Entorno Virtual de Aprendizaje)	HEWLETT PACKARD	PROLIANT BL460C G8	16	450	Intel(R) Xeon(R) 2.53GHz	Cuchilla 02
Virtual, cursos (MED)	HEWLETT PACKARD	PROLIANT BL460C G9	16	400	Intel(R) Xeon(R) 2.53GHz	Cuchilla 03
Evaluación Docente	HEWLETT PACKARD	PROLIANT BL460C G15	4	111	Intel(R) Xeon(R) 2.53GHz	Cuchilla 09
Graduados	HEWLETT PACKARD	PROLIANT BL460C G16	2		Intel(R) Xeon(R) 2.53GHz	Cuchilla 09
Formación	HEWLETT PACKARD	PROLIANT BL460C G19	1	40	Intel(R) Xeon(R) 2.53GHz	Cuchilla 09
Capacitación	HEWLETT PACKARD	PROLIANT BL460C G25	512 MB	30	Intel(R) Xeon(R) 2.53GHz	Cuchilla 10

Open VPN	HEWLETT PACKARD	PROLIANT BL460C G26	512 MB	20	Intel(R) Xeon(R) 2.53GHz	Cuchilla 10
DSPACE2	HEWLETT PACKARD	PROLIANT BL460C G35	2	201	Intel(R) Xeon(R) 2.53GHz	Cuchilla 10
Facturación Tesorería	HEWLETT PACKARD	PROLIANT BL460C G37	2	27	Intel(R) Xeon(R) 2.53GHz	Cuchilla 10
unl.edu.ec	HEWLETT PACKARD	PROLIANT BL460C G38	4	151	Intel(R) Xeon(R) 2.53GHz	Cuchilla 10
SGA	HEWLETT PACKARD	PROLIANT BL460C G38	16	150	Intel(R) Xeon(R) 2.53GHz	Cuchilla 04
Fuente: Unidad de Telecomunicaciones e Información (UTI-UNL)						

6.1.8. Características software del DNS autoritario y servidores públicos

Para desplegar correctamente IPv6 es necesario conocer las características software como: versión del sistema operativo que utilizan y los servicios o aplicaciones que tienen instalados cada servidor.

TABLA X: CARACTERÍSTICAS SOFTWARE DEL DNS Y SERVIDORES PÚBLICOS

Servidor	Sistema operativo/ versión	Protocolo de acceso	Hostname (DNS)	Servicios/aplicaciones
DNS Autoritativo	CENTOS 7.0	--------	dns.unl.edu.ec	BIND
EVA(Entorno Virtual de Aprendizaje)	CENTOS 5.8	HTTP	eva.unl.edu.ec	MOODLE (APACHE)

Virtual, cursos (MED)	CENTOS 5.8	HTTP	cursosmed.unl.edu.ec virtual.unl.edu.ec	MOODLE
Evaluación Docente	CENTOS 7.0	HTTP	evaluaciondocente.unl.edu.ec	POSTGRES
Graduados	CENTOS 7.1	HTTP	graduados.unl.edu.ec	MYSQL
Formación	DEBIAN 8.2	HTTPS	formacion.unl.edu.ec	MOODLE
Capacitación	DEBIAN 8.2	HTTP	capacitacion.unl.edu.ec	POSTGRES
Open VPN	CENTOS 7.0	HTTPS	openvpn.unl.edu.ec	MYSQL
DSPACE2	DEBIAN 8.2	HTTP	openvpn.unl.edu.ec	POSTGRES
Facturación Tesorería	WINDOWS SERVER 2012 STANDARD	--------		MYSQL
unl.edu.ec	DEBIAN 7.7	HTTP	unl.edu.ec	MYSQL, APACHE
SGA	DEBIAN 6.0	HTTPS	dds1.unl.edu.ec	POSTGRES
Fuente: Unidad de Telecomunicaciones e Información (UTI)				

6.1.9. Soporte de IPv6 en el DNS autoritario y servidores públicos

Para determinar los servidores que soportan IPv6, y aquellos que requieren actualización para dicho soporte se tomó como referencia las características software proporcionadas por la Unidad de Telecomunicaciones e Información descritas en el apartado 6.1.4, puesto que la versión del Sistema Operativo con el que cuenta cada uno de los servidores es fundamental para conocer el soporte de esta versión de protocolo o si alguna de las versiones necesita alguna configuración adicional, resumiendo el resultado en la siguiente tabla:

TABLA XI: LISTA DE SERVIDORES QUE SOPORTAN IPV6

	Servidor	Soporte IPV6	¿Necesitan configuración adicional?
1	DNS Autoritativo	SI	NO
2	EVA (Entorno Virtual de Aprendizaje)	SI	NO
3	Virtual, cursos	SI	NO
4	Evaluación Docente	SI	NO
5	Graduados	SI	NO
6	Formación	SI	NO
7	Capacitación	SI	NO
8	Open VPN	SI	NO
9	DSPACE2	SI	NO
10	Facturación Tesorería	SI	NO
11	Web (unl.edu.ec)	SI	NO

12	SGA (Sistema de Gestión Académica)	SI	NO
Suma General		**12**	
Porcentaje Total		**100%**	

Como se puede apreciar en la tabla anterior de los 12 servidores públicos con los que cuenta la Universidad Nacional de Loja, 11 cuentan con sistemas operativos Gnu / Linux Centos y Debian, lo que significa que estos servidores tienen soporte IPv6 debido a que en Linux IPv6 se implementa como módulo del kernel. Así las distribuciones con kernel v.2.4.x ya vienen con este soporte y normalmente el módulo IPv6 ya está cargado. De la misma manera el servidor denominado facturación tesorería con S.O Windows Server 2012 cuenta con soporte IPv6; Como resultado de la investigación se tiene que el 100 % de los servidores públicos están disponibles para configurar e implementar IPv6.

6.2. OBJETIVO 2: Determinar el mecanismo de transición a utilizar entre IPv4 e IPv6

Para determinar el mecanismo de transición que permita la coexistencia entre IPv4 e IPv6 se tomará en cuenta los mecanismos que fueron definidos en la revisión literaria (Sección 4.2.), los mismos que se mencionan a continuación.

- Doble Pila (Dual stack)
- Túneles (Tunneling)
- Traducción (Translation)

6.2.1. Resumen de los Mecanismos de Transición

Los mecanismos de transición y coexistencia entre IPv4-IPv6 detallados anteriormente se resumen en el siguiente cuadro, en el cual se señala conectividad, ventajas y desventajas, consideraciones importantes a tener en cuenta para determinar el mecanismo idóneo que permita realizar el despliegue de IPv6.

TABLA XII: RESUMEN DE LOS MECANISMOS DE TRANSICIÓN.

Nombre	Tipo de Mecanismo	Conectividad	Descripción	Ventajas	Desventajas
Doble Pila	Dual Stack(Doble Pila)	Solo entre sistemas del mismo tipo (IPv4-IPv4 e IPv6-IPv6)	✓ Trabaja con ambos protocolos (IPv4 e IPv6). ✓ Procesa solo los encabezados IP. ✓ Uno de los más populares dentro de su tipo. ✓ Se basa en DHCP y direcciones compatibles para la asignación de direcciones. ✓ La comunicación IPv4 se hace a través de una infraestructura IPv4. ✓ La comunicación IPv6 se hace a través de una infraestructura IPv6.	✓ Fácil de implementar. ✓ La comunicación es posible entre todos los nodos de la red, sin necesidad de encapsulación o traducción. ✓ Solución inminente y accesible. ✓ Permite a los nuevos dispositivos IPv6 relacionarse rápidamente con el resto de los dispositivos.	✓ No trabaja en ambientes mixtos (IPv4 sobre IPv6 y viceversa). ✓ Si la red no es IPv6, no se ve beneficiada de las características de esta versión. ✓ No reduce la demanda de direcciones IPv4
6to4	Túneles	IPv6 a IPv6 sobre IPv4	✓ Crea túneles automáticamente. ✓ Algoritmo más popular dentro de su clase.	✓ Ayuda a conectar redes IPv6 aisladas entre sí.	

6over4	Túneles	IPv6 a IPv6 sobre IPv4	✓ Se comporta como una red virtual.	✓ Permite la autoconfiguración. ✓ Conserva todas las características de IPv6.	✓ Necesita soporte de ruteo multicast (IPv4 raramente cuenta con este soporte).
SIIT(Stateless IP/ICMP Translator)	Traducción	De IPv6 a IPv4 y de IPv4 a IPv6	✓ Para hacer dos protocolos “compatibles” realiza la traducción de encabezado. ✓ Se necesita que lleve a cabo la tarea de traducción.	✓ Permite a nodos IPv4 comunicarse con nodos IPv6. ✓ Fácil de soportar por un dispositivo. ✓ No se afecta el Checksum de la capa de transporte. ✓ Puede manejar paquetes encriptados, ya que no modifica capas superiores.	✓ Al realizar la traducción IPv6 a IPv4 se pierde muchos campos de la cabecera de IPv6 y con esto beneficios. ✓ Se ignoran la mayoría de los encabezados de extensión. ✓ Necesita utilizar dos tablas de ruteo diferentes, debido a que se manejan dos protocolos. ✓ Al trabajar con direcciones IPv4 compatibles, se reduce el campo de direccionamiento. ✓ Se reduce el tamaño del MTU lo que genera mayor fragmentación.

6.2.2. Determinación de los parámetros y criterios de evaluación

Para poder determinar el mecanismo de transición más eficiente para el despliegue de IPv6 para el DNS y servidores públicos en la red de datos de la Universidad Nacional de Loja se han planteado los siguientes parámetros:

- Escalabilidad.
- Configuración.
- Compatibilidad (hardware y software).
- Seguridad
- Interoperabilidad
- Movilidad
- Desempeño
- Aplicabilidad
- Usabilidad

A continuación se describe cada uno de los parámetros mencionados anteriormente.

Escalabilidad. IPv6 se puede ampliar fácilmente si se agregan Encabezados de Extensión tras el encabezado de IPv6. A diferencia del campo de opciones en el encabezado IPv4, el cual solo permite entre 0 y 10 palabras de 32 bits para las opciones, el tamaño de los encabezados de extensión de IPv6 solo está limitado por el tamaño del paquete IPv6.

Los encabezados de extensión se ubican entre el encabezado IPv6 y el encabezado del protocolo de la capa superior; estos garantizan soporte a las futuras aplicaciones, ya que si se requiere definir nuevas opciones, nuevas cabeceras opcionales pueden ser definidas.

Configuración. Cada mecanismo de transición tiene su propia manera de estructurar sus procedimientos de comunicación con los dispositivos que soporten la utilización de un determinado mecanismo, que varía según el Sistema Operativo. Esta información ha sido recopilada en los respectivos RFC (RFC 2893, RFC 2765, RFC 2473, etc) que describen los pasos a seguir para lograr la integración de los protocolos IPv4 e IPv6.

Compatibilidad (hardware y software):

- Hardware. Debido al avance tecnológico, los equipos de última generación incorporan funcionalidades que facilitan la configuración de los mecanismos de

transición, es decir, soportan la utilización del protocolo IPv4 e IPv6 simultáneamente.

- Software. Los Sistemas Operativos actuales incorporan el soporte necesario en sus núcleos, para facilitar la configuración del mecanismo de transición más idóneo para ambos protocolos.

Seguridad. Aunque se han definido estándares de seguridad para IPv4 ninguno de ellos es obligatorio, es por esto que se han impuesto soluciones propietarias reduciendo así la estandarización de la seguridad de Internet. En IPv6 la compatibilidad con IPSec es un requisito. IPSec proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6, aporta confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales.

Interoperabilidad. Ejecuta programas o transfiere datos entre distintas unidades funcionales de forma que se requiera el mínimo o nulo conocimiento del usuario sobre las características particulares de dichas unidades.

Este parámetro ha adquirido gran trascendencia porque la penetración de Internet a nivel universal ha hecho que se convierta en una importante necesidad la interacción entre todos los sitios conectados a la red de redes, en la actualidad se está dando una progresiva migración del protocolo IPv4 hacia IPv6 y es necesario encontrar el mecanismo de transición que cumpla esta tarea de una manera efectiva.

Movilidad. Gracias al amplio espacio de direccionamiento IPv6, es fácil asignar una dirección nueva en cada punto de conexión de los dispositivos móviles. Se introdujo la seguridad para el tráfico reencaminado y para los procesos de vinculación a las redes. La versión 6 del protocolo de internet móvil tiene una implementación más sólida que la versión 4 del protocolo de internet.

Desempeño. Se hace referencia al comportamiento que tiene un mecanismo de transición específico, una vez que cumple con todos los argumentos y/o especificaciones establecidas para su utilización. Permitiendo de esta manera, comprobar su funcionalidad en entornos de producción reales.

Aplicabilidad. Hace referencia al modo de aplicar cada mecanismo para su evaluación, cumpliendo porcentajes estandarizados de modo que al momento de implementar resulte beneficioso para manejar ambas pilas de protocolos.

Usabilidad. Se menciona en base a los equipos que se deben y pueden utilizar para la transición, infraestructura tecnológica suficientemente alta en cuanto a equipos de red, parámetro importante que debe ser analizado ya que de eso se beneficiará el mecanismo elegido al momento de desplegar IPv6.

6.2.3. Análisis comparativo de los mecanismos de transición

El análisis será realizado en base a los siguientes parámetros: escalabilidad, configuración, compatibilidad (hardware y software) seguridad, interoperabilidad, movilidad, desempeño, aplicabilidad y usabilidad y para la evaluación de los parámetros propuestos se dio una valoración a cada uno de ellos, categorizándolos de la siguiente manera: 5-óptimo, 4-satisfactorio, 3-aceptable, 2-regular y 1-inaplicable, con lo cual obtenemos una matriz con los porcentajes de cada mecanismo, llegando a la elección del mejor. A continuación se presenta la tabla matriz de los criterios de evaluación con su respectiva valoración.

TABLA XIII: CRITERIOS DE EVALUACIÓN.

Factor	Escala	Ponderación
Óptimo	5	Se cumplen los argumentos establecidos en su totalidad.
Satisfactorio	4	Se cumplen la mayoría de los argumentos establecidos.
Aceptable	3	Son cumplidos la mitad de los argumentos.
Regular	2	Cumple parcialmente ciertos argumentos.
‘Inaplicable	1	No cumple ningún argumento establecido.

Ahora se procede a evaluar cada parámetro con los mecanismos de transición seleccionados, con el objetivo de realizar un análisis específico tomando como referencia la “Matriz de Criterios de Evaluación”.

TABLA XIV: EVALUACIÓN DE PARÁMETROS.

Parámetro	Mecanismo	Factor	Escala	Justificación
Escalabilidad	Doble Pila	Óptimo	5	Encabezados de extensión garantizan soporte a futuras aplicaciones [18].
	Túneles	Aceptable	4	Necesidad de configuración manual con host individuales [18].
	Traducción	Regular	2	Debe utilizar dispositivo que convierta paquetes de IPv4 a IPv6 y viceversa [15].
Configuración	Doble Pila	Óptimo	5	Consiste en tener soporte IPv6 en el kernel para su utilización [15].
	Túneles	Satisfactorio	4	Necesita que los equipos que actúen como extremos soporten IPv4 e IPv6 [18].
	Traducción	Aceptable	3	Tedioso, requiere de muchas configuraciones en los equipos [15].
Compatibilidad (Hardware)	Doble Pila	Óptimo	5	Dispositivos de última generación soportan ambos protocolos [15].
	Túneles	Óptimo	5	Dispositivos de última generación soportan ambos protocolos [15].
	Traducción	Óptimo	5	Dispositivos de última generación soportan ambos protocolos [15].

Compatibilidad (Software)	Doble Pila	Óptimo	5	El uso de versiones de S.O. actualizadas soporta IPv6.
	Túneles	Óptimo	5	El uso de versiones de S.O. actualizadas soporta IPv6.
	Traducción	Óptimo	5	El uso de versiones de S.O. actualizadas soporta IPv6.
Seguridad	Doble Pila	Óptimo	5	Los equipos que tengan habilitado doble pila, podrán transmitir información entre sí, sin ningún tipo de problema. Asegurando la integridad y destino sin terceros en los datos que se envíen [18].
	Túneles	Satisfactorio	4	Debido a que este mecanismo hace uso de períodos de tiempo para mantener su conectividad activa. Puede darse el caso, en que durante el envío de paquetes, el tiempo de actividad para el túnel se termine, perdiéndose la información que se estaba transmitiendo [18].
	Traducción	Satisfactorio	4	Este mecanismo también hace referencia al periodo de conectividad activo, dando así un lapso de tiempo para la pérdida de paquetes en la transmisión de los mismos [18].
Interoperabilidad	Doble Pila	Óptimo	5	Cualquier dispositivo de red administrable con soporte de IPv4 e IPv6, pueden utilizar el mecanismo.
	Túneles	Óptimo	5	Cualquier dispositivo de red administrable con soporte de

				IPv4 e IPv6, pueden utilizar el mecanismo.
	Traducción	Óptimo	5	Cualquier dispositivo de red administrable con soporte de IPv4 e IPv6, pueden utilizar el mecanismo.
Movilidad	Doble Pila	Óptimo	4	Cada nodo móvil tendrá una dirección de casa [15].
	Túneles	Aceptable	4	Si un nodo no es configurado no tiene acceso a peticiones en IPv6 [15].
	Traducción	Regular	2	Debe realizar la traducción en los dos sentidos para la comunicación [15].
Desempeño	Doble Pila	Satisfactorio	4	Debe verificar el tipo de dirección que se usa [18].
	Túneles	Aceptable	4	Tiempo influye en el encapsulado y desencapsulado de paquetes [18].
	Traducción	Regular	2	Debe tener red IPv6 nativa para llegar a sitios solo IPv4 [18].
Aplicabilidad	Doble Pila	Optimo	5	Popular en su tipo, recomendado por empresas con años de experiencia en el manejo de protocolos IP [15].
	Túneles	Satisfactorio	4	Necesita tener configurado Doble Pila en los extremos del túnel creando complejidad al momento de ser aplicado [15].
	Traducción	Regular	2	No recomendado por expertos en desplegar IPv6. Obsoleto en su tipo [15].

Usabilidad	Doble Pila	Óptimo	5	Técnicamente no requiere equipos robustos, se utiliza la misma infraestructura física para ser desplegado [18] [15].
	Túneles	Aceptable	3	Si un equipo del extremo del túnel no cuenta con características físicas para soportar IPv6, la comunicación no se realiza [18].
	Traducción	Regular	2	Infraestructura física en equipos muy elevada, cada uno debe tener traductores incorporados para realizar la traducción de IPv4 a IPv6 y viceversa. Precios muy elevados de los equipos [15].

6.2.4. Resultados de la evaluación de los parámetros para determinar el mecanismo de transición a utilizar

La siguiente tabla nos muestra el valor individual obtenido al evaluar los parámetros con cada mecanismo de transición.

TABLA XV: VALORACIÓN INDIVIDUAL DE LOS PARÁMETROS ESTABLECIDOS

	Mecanismos de Transición para la coexistencia de IPv4 e IPv6 evaluados		
Parámetro	**Doble Pila**	**Túneles**	**Traducción**
Escalabilidad	5	4	2
Configuración	5	4	3
Compatibilidad (Hardware)	5	5	5
Compatibilidad (Software)	5	5	5
Seguridad	5	4	4

Interoperabilidad	5	5	5
Movilidad	4	4	2
Desempeño	4	4	2
Aplicabilidad	5	4	2
Usabilidad	5	3	2
Suma General	**48**	**42**	**32**
Porcentaje Total	**96%**	**84%**	**64%**

A continuación mediante gráficas se expone los resultados obtenidos en la tabla anterior:

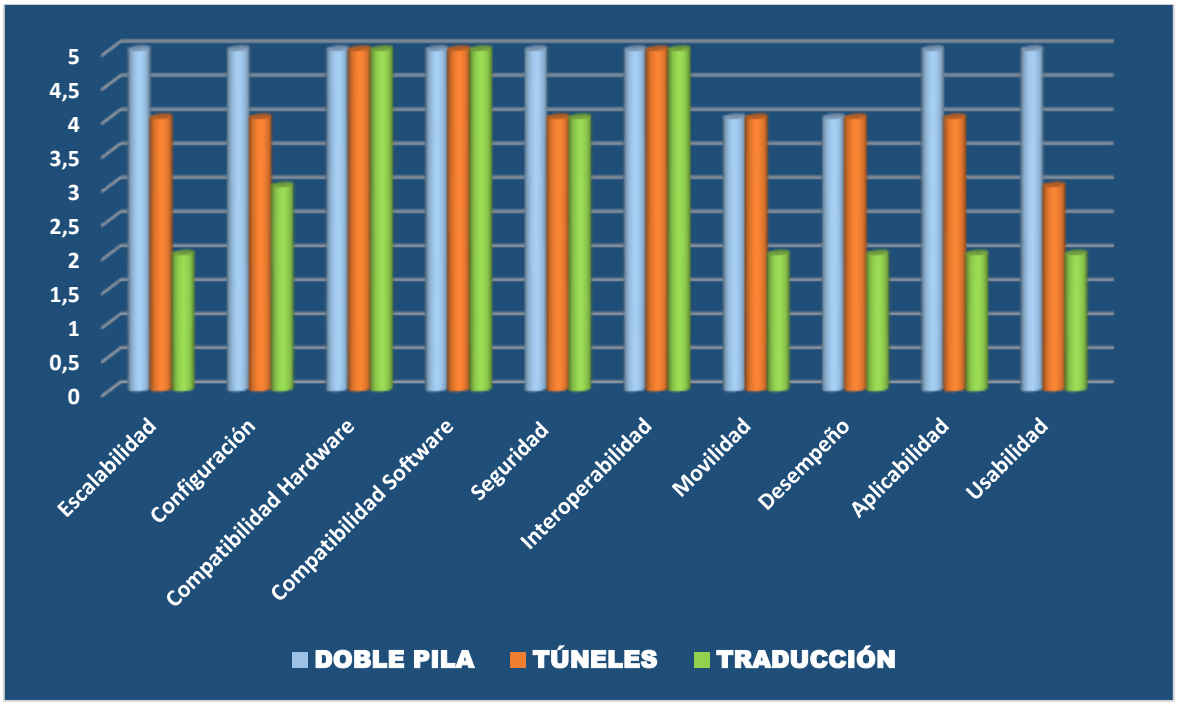


Figura 20: Valoración de parámetros de los Mecanismos de Transición.

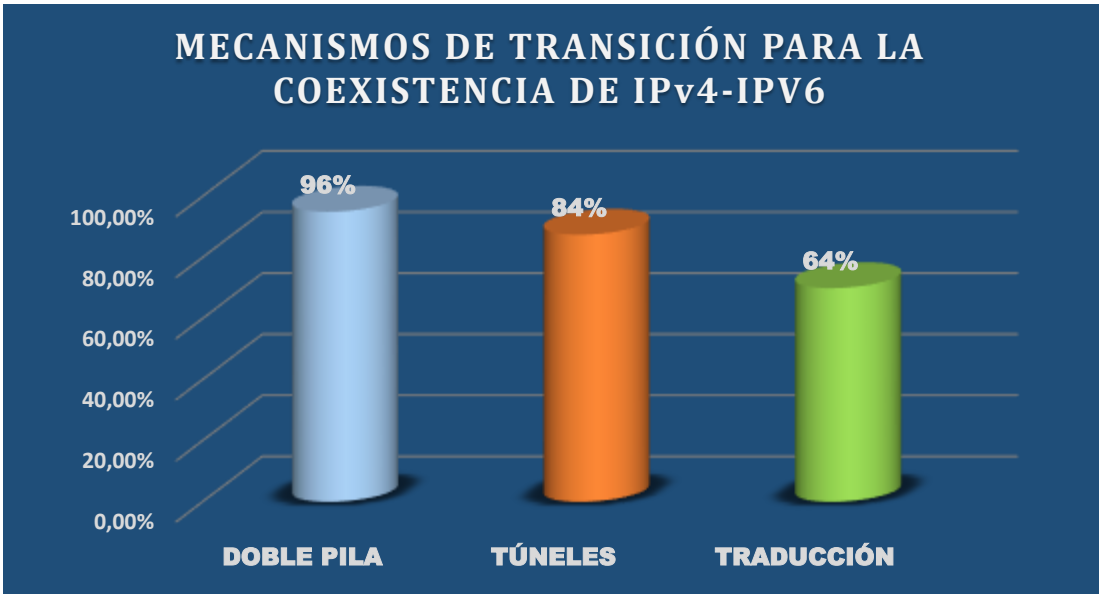


Figura 21: Porcentajes Generales de los Mecanismos de Transición.

Los resultados obtenidos de la evaluación de los mecanismos de transición a IPv6, son los siguientes:

El mecanismo doble pila presenta el porcentaje más alto con un 96%, seguido por el mecanismo de túneles con un 84%, y finalmente con un porcentaje de 64% el mecanismo de traducción. Dichos porcentajes se los obtuvo de la suma general de cada mecanismo, determinando así que Doble Pila (Dual Stack) es el mecanismo recomendado para ser aplicado en la configuración e implementación de IPv6 en la Red de Datos de la Universidad Nacional de Loja específicamente en el DNS y servidores públicos.

Con los resultados obtenidos podemos decir que:

- Los argumentos utilizados en los mecanismos de transición, cumplen con los requerimientos establecidos. Sin embargo, la diferencia está en los porcentajes totales, donde se presentó argumentos que diferencian un mecanismo del otro. Por ejemplo, en la Seguridad de los datos el mecanismo "Túneles" y “Traducción” marca una diferencia respecto a "doble pila", debido a que su utilización se basa en períodos de tiempo y si dicho período de tiempo expira, los datos que se transmiten en ese momento tienen algún grado de alteración o pérdida. Con respecto a la Configuración de cada mecanismo; "doble pila" no presenta inconvenientes, porque

para su utilización basta con tener el soporte IPv6 en el kernel, mientras que el mecanismo "Túneles" debe incorporar equipos con doble pila en sus extremos, para efectuar posteriormente la configuración que el mecanismo túneles usa y en el mecanismo “Traducción” sus configuraciones son demasiado extensas y tediosas en los equipos a utilizar.

- Se debe mencionar que la utilización del mecanismo "Doble-Pila" es apto para entornos donde se conoce explícitamente la cantidad de equipos que se usa o la infraestructura donde se realizara la implementación. Como el despliegue de IPv6 se enfoca en DNS autoritario y servidores públicos, "doble pila" cumple satisfactoriamente con lo requerido, permitiendo que ambos protocolos IPv4 e IPv6 trabajen al mismo tiempo.

6.2.5. Casos de éxito aplicando el mecanismo de transición seleccionado

En la presente tabla se puede observar algunos casos de éxito en los que se hace uso del mecanismo de transición Doble Pila por parte de algunas instituciones entre ellas de Educación Superior, lo que permite justificar además del análisis realizado anteriormente el por qué este mecanismo o técnica de transición es las más idónea a la hora de desplegar IPv6 tomando en cuenta que el protocolo predominante aun en la actualidad es IPv4 y que la mayoría de las instituciones cuenta con esta versión de IP en su estructura de Red, por lo que por el momento la transición es la mejor opción hasta llegar a obtener una Red IPv6 nativa.

TABLA XVI: CASOS DE ÉXITO – IMPLEMENTACIÓN DOBLE PILA.

Caso de éxito	Resumen
Universidad Nacional de Chimborazo (UNACH) [38]	Esta entidad de educación superior en el año 2011 – 2012, puso en marcha la ejecución de un plan de estudio e implementación para la transición de IPv4 a IPv6. Al momento de la implementación, el mecanismo Dual Stack es el idóneo logrando que los servicios y equipos trabajen con IPv4 e IPv6, sin crear impacto notable para los usuarios, debido a que trabaja de manera

	transparente, facilitando el cambio de red sin perder conectividad lo que permite mejorar la calidad de servicio (QoS). Estableciendo que el tiempo de respuesta mediante consultas IPv6 es más rápido debido a que la fragmentación se la realiza en el nodo origen y el reensamblado en los nodos finales y no en los routers como en el caso de IPv4.
Propuesta de un plan de implementación para la migración a IPV6 en la red de la Universidad Politécnica Salesiana sede-cuenca [39]	Esta propuesta si bien es cierto es un Plan de implementación pero con resultados favorables para la utilización de Doble Pila como mecanismo de transición, sus resultados fueron: 1. Simulación de toda la red de la universidad mediante doble pila utilizando Packet Tracer. 2. Factible implementación por lo que sus equipos cuentan con soporte en IPv6. 3. La migración a IPv6 debe hacerse de forma gradual, establecer un periodo de transición y coexistencia entre los protocolos con el fin de reducir el impacto sobre el funcionamiento de la red. 4. Con el plan de implementación se determinó aspectos como implementar niveles de seguridad y aspectos relevantes como la escalabilidad de la red, seguridad, configuración y administración de redes, soporte para QoS, movilidad, políticas de enrutamiento, etc.
Análisis de las técnicas de convivencia entre IPV4 e IPV6 y su implementación en los servicios: web, MAIL, FTP, PROXY, DNS y	Se implementó Dual Stack (IPv4/IPv6) dentro de la intranet de la Escuela Superior Politécnica de Chimborazo, con la finalidad de diversificar los servicios y al mismo tiempo estar preparados para el manejo del nuevo protocolo para las redes avanzadas.

DHCP de la intranet de la ESPOCH [40]	La implementación se la realizó mediante el mecanismo de transición Doble Pila, lo que permitió que el host pueda tomar decisiones de cuando se deban hacer la conexiones con IPv4 o IPv6; basándose en la disponibilidad de conectividad con IPv6 y los registros de sistema de nombres de dominio (DNS), que son completamente independientes. Con la implementación de Dual Stack se logró que los servicios trabajen con IPv4/IPv6, sin crear impacto para los usuarios, debido que trabajan de manera transparente.

6.3. OBJETIVO3: Diseñar el esquema de direccionamiento para la red pública de la Universidad Nacional de Loja.

En la presente sección se realiza la distribución y asignación de direcciones IPv6 partiendo del prefijo asignado a la Universidad Nacional de Loja por el CEDIA, así como también se explica la técnica utilizada para el direccionamiento IPv6 en el servidor DNS autoritario y servidores públicos.

6.3.1. Prefijo IPV6 asignado a la Universidad Nacional de Loja

LACNIC organismo responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6) para la región de América Latina y el Caribe, propone asignar un prefijo /32 a los Proveedores de Servicio de Internet (ISP).
Dado que el Proveedor de Servicios de la UNL es el CEDIA y de acuerdo a las políticas de asignación de direcciones por parte de LACNIC [29], CEDIA tiene delegado el prefijo **2800:68::/32 .**

De acuerdo con el plan de asignación de direcciones establecido por el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, a cada Universidad se le asigna un

prefijo /48. La UNL al ser una institución miembro recibe un prefijo **2800:68:7::/48**, esto permite utilizar 16 bits para la Institución, lo que hace un total de 65536 (2^{16}) redes internas diferentes, de prefijo /64.

6.3.2. Plan de Direccionamiento IPv6 en la Universidad Nacional de Loja

Con el objetivo de realizar una correcta distribución de las direcciones IPv6, se procedió a realizar la misma conjuntamente con los técnicos del Departamento de Redes y Telecomunicaciones, fundamentada en el direccionamiento jerárquico que considera a las diferentes Facultades Académico- Administrativas, subneteando la dirección de red principal correspondiente a un prefijo **2800:68:7::/48**, en un prefijo **/56**.

Para representar lo expuesto anteriormente, en la tabla se puede visualizar la distribución de las direcciones IPv6 desglosadas por Facultades, haciendo uso del prefijo de documentación 2001:db8::/32, el mismo que fue expuesto en la sección 4.1.5.3.; esto por políticas de seguridad de la institución.

TABLA XVII: DISTRIBUCIÓN DE LAS DIRECCIONES IPV6 EN LA UNL

Dependencia	Dirección IPv6
Administración Central	2001:db8:7:1::/56
Educativa	2001:db8:7:2::/56
Jurídica 01 (Biblioteca)	2001:db8:7:3::/56
Jurídica 02 (B10)	2001:db8:7:4::/56
Agropecuaria	2001:db8:7:5::/56
Energía	2001:db8:7:6::/56
MED	2001:db8:7:7::/56

Energía-Laboratorios (Bloque 12)	2001:db8:7:8::/56
Salud	2001:db8:7:9::/56
Motupe	2001:db8:7:a::/56
Consultorio Jurídico	2001:db8:7:b::/56
Obelisco	2001:db8:7:c::/56
Punzara	2001:db8:7:d::/56
Jardín Botánico	2001:db8:7:e::/56
Centro de Procesamiento de Datos (CPD)	2001:db8:7:ff::/56

6.3.3. Direccionamiento IPv6 en el DNS autoritario y servidores públicos

El objetivo principal de este Trabajo de Titulación es "Despliegue del Protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja", por lo que considerando el grado de seguridad que implica el utilizar una dirección IP sobre estos dispositivos, se propuso un mecanismo de asignación de direcciones IPv6, el mismo que se explica en detalle en el siguiente apartado.

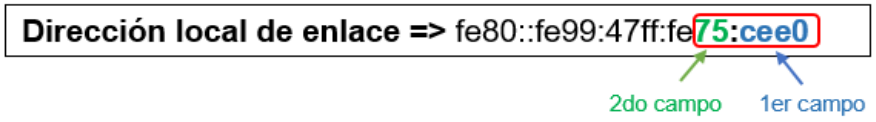
6.3.3.1. Mecanismo propuesto para el direccionamiento IPv6 en los servidores

Luego de la reunión mantenida con los técnicos de la Unidad de Telecomunicaciones e Información (UTI) para definir la distribución de direcciones IPv6, se optó por utilizar un barra 64 (/64) en la asignación de direcciones a los servidores públicos.

Para completar los 64 bits restantes de la dirección IPv6, se propuso un mecanismo el mismo que fue aprobado por la Unidad de Telecomunicaciones e Información (UTI) y el Director de este TT, dicho mecanismo se describe a continuación:

- ✓ Partimos de la dirección asignada a la DMZ, que se la obtuvo del prefijo asignado al Centro de Procesamiento de Datos (2001:db8:7:ff::/56) en un barra /64.

- ✓ Se toma los últimos 24 bits de la dirección local de enlace y se usa de la siguiente manera:
  - El segundo campo (derecha a izquierda) de la dirección es empleado para formar el quinto campo de la dirección IPv6 del servidor, y el primer campo (derecha a izquierda) formaría el sexto campo.



Nota: Para conocer la dirección local del host en GNU/LINUX se utiliza el comando **ifconfig** y en Windows **ipconfig**.

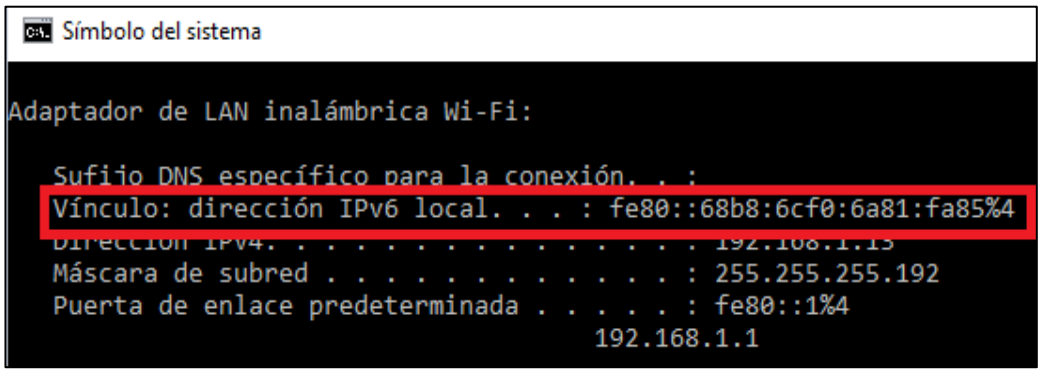


Figura 22: Dirección local de enlace en S.O Windows

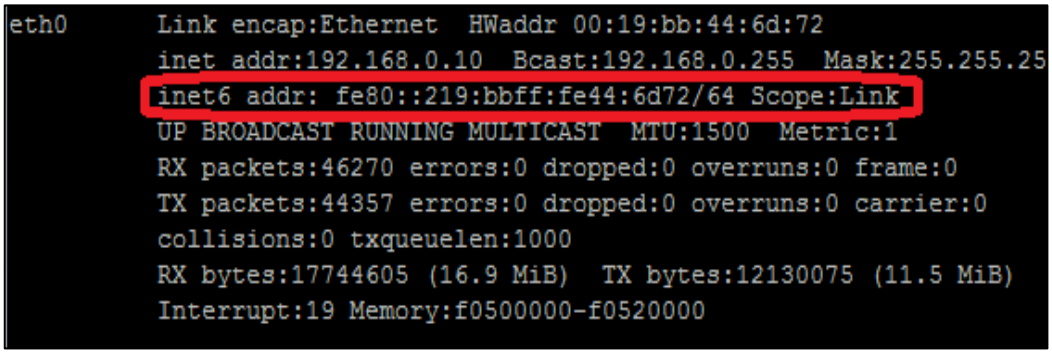
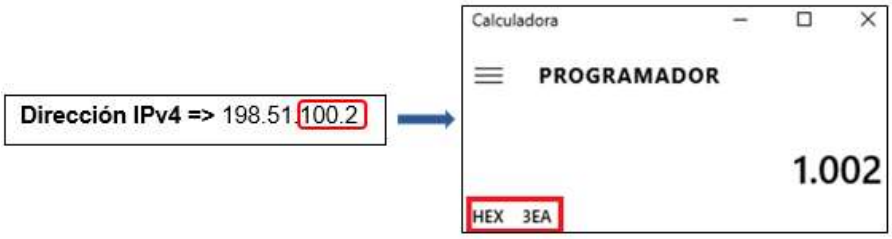


Figura 23: Dirección local de enlace en S.O Linux

- ✓ Se convierte los últimos 16 bits de la dirección IPv4 (sin considerar el punto que separa los octetos) en hexadecimal, el resultado de la conversión se agrega al octavo campo de la dirección IPv6.

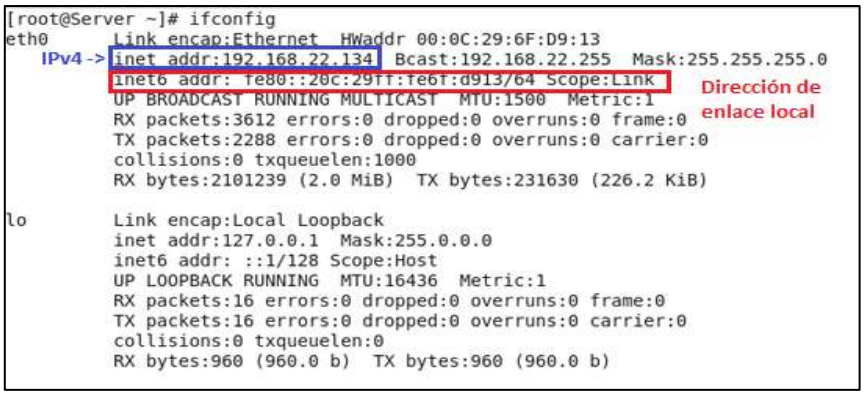


- ✓ Finalmente se concatena la dirección asignada a la DMZ, con los últimos 24 bits de la dirección local de enlace y los últimos 16 bits de la dirección IPv4 convertidos a hexadecimal como se explicó anteriormente y con esto se formaría la dirección IPv6 a ser utilizada en el direccionamiento de los servidores públicos.

2001:db8:7:ff02:75:cee0::1002

Para una mejor compresión de la técnica aplicada se representa la misma en el siguiente ejemplo:

- Ingresamos al servidor al que vamos a asignar la IPv6 y con el comando *ifconfig* (en el caso de Linux), obtenemos la dirección IPv4 y la dirección local de enlace.



Con el valor de la DMZ, más los datos que se acaba de obtener el resultado del ejemplo se ilustra en la Figura 24:

- Valor de la DMZ 2001:db8:7:ff02::/64
- Dirección IPv4 del servidor: 192.168.22.134 de la cual se toma los últimos 16 bits correspondientes a **22134** y se los convierte a hexadecimal quedando **5676**
- Dirección local de enlace fe80::20c:29ff:fe6f:d913, de la cual se toma los últimos 24 bits **6f:d913.**

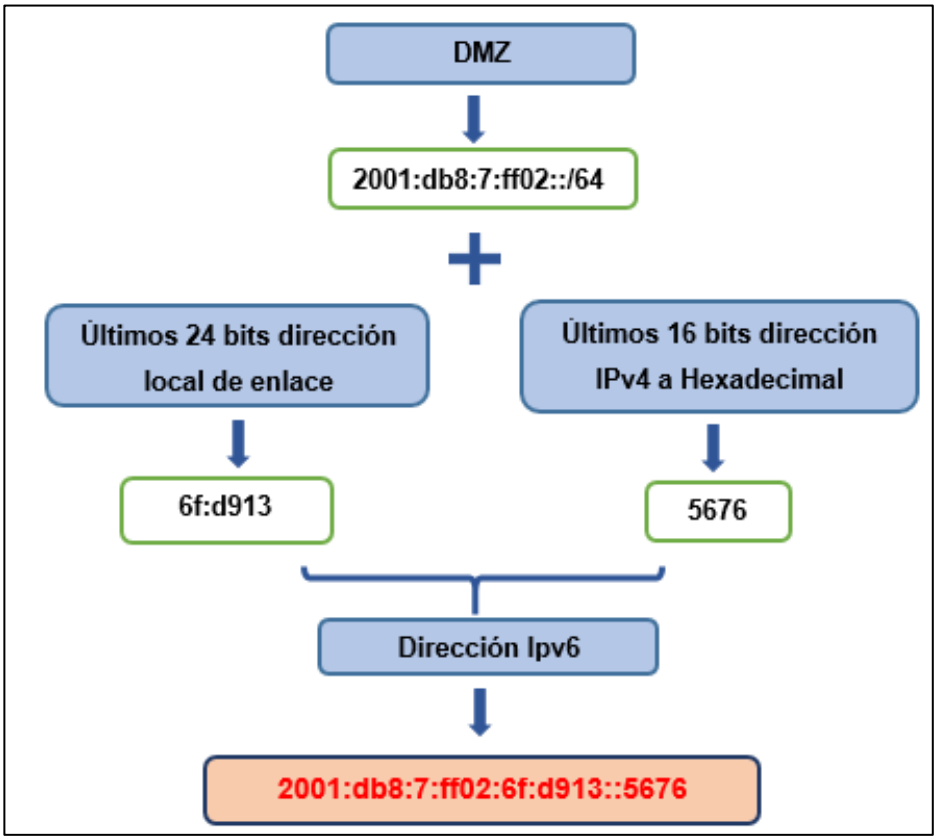


Figura 24: Ejemplo de Dirección IPv6 en servidores

En la siguiente tabla se muestra el direccionamiento IPv6 correspondiente al DNS y servidores públicos disponibles en la Universidad Nacional de Loja.

TABLA XVIII: DIRECCIONES IPV6 PARA EL DNS Y SERVIDORES PÚBLICOS

SERVIDOR	DIRECCIÓN IPv6
DNS (Sistema de Nombre de Dominio)	2001:db8:7:ff02:54:8dd9::cb3
EVA (Entorno Virtual de Aprendizaje)	2001:db8:7:ff02:b2:a056::cc3
Virtual, cursos (MED)	2001:db8:7:ff02:de:39f0::7dc7 2001:db8:7:ff02:de:39f0::7dc8
Evaluación Docente	2001:db8:7:ff02:93:4d18::7d76
Graduados	2001:db8:7:ff02:c4:b96a::cd4
Formación	2001:db8:7:ff02:d8:c1f4::c8d
Capacitación	2001:db8:7:ff02:c3:9843::cac
Open VPN	2001:db8:7:ff02:10:4ed4::cad
DSPACE2	2001:db8:7:ff02:d3:eab9::cd9
Web (unl.edu.ec)	2001:db8:7:ff02:3c:8289::e770
SGA (Sistema de Gestión Académica)	2001:db8:7:ff02:89:fb00::f6a7 2001:db8:7:ff02:89:fb00::2bd4

En la Figura 25, se puede visualizar la distribución de direcciones IPv6 correspondientes al DNS autoritativo y a cada uno de los servidores públicos, las mismas que se obtuvieron al realizar el plan de direccionamiento.

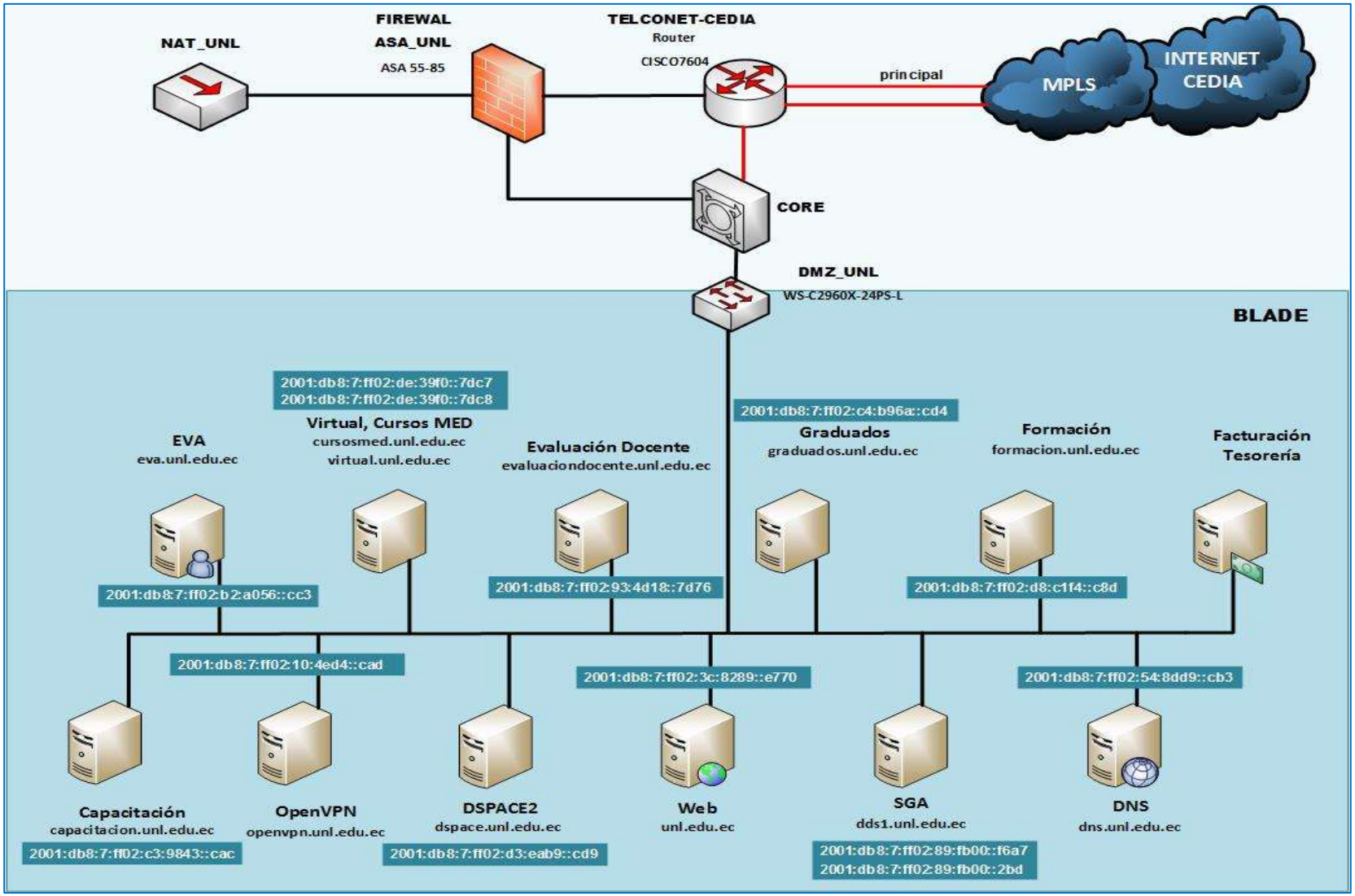


Figura 25: Direccionamiento IPv6 en el DNS y servidores públicos

6.4. OBJETIVO 4: Establecer un escenario de pruebas de acuerdo al mecanismo de transición seleccionado.

En el presente apartado se detalla el escenario a utilizar para el desarrollo de las pruebas, puesto que de estas depende la correcta implementación del mecanismo de transición Doble Pila, el cual fue determinado luego de un análisis entre los diferentes mecanismo de transición (ver sección 6.2), por lo que los servidores a configurar deben trabajar en pila dual (IPv4-IPv6). Se propone un entorno de pruebas con el objetivo de poder ejecutar acciones que no pongan en riesgo el funcionamiento de la red de datos de la UNL.

6.4.1 Escenario de pruebas

El ambiente de pruebas se desarrolló basado en un escenario con equipos físicos, donde la Unidad de Telecomunicaciones e Información (UTI), departamento para el cual se está desarrollando el presente Trabajo de Titulación, proporcionó los equipos necesarios para llevar acabo la ejecución de las pruebas. En la siguiente tabla se detalla las características hardware y software de los equipos propuesto para las pruebas:

TABLA XIX: CARACTERÍSTICAS DE LOS EQUIPOS DE PRUEBA

Características	PC1	PC2	PC3
Nombre	Dns	Web	Pc01
RAM	512 MB	512 MB	8GB
HD	50 GB	50GB	1TB
Sistema Operativo/versión	Linux Centos 7	Linux Debian 8	Windows 10
Soporte IPv6	SI	SI	SI

Los equipos funcionarán como Servidor DNS la PC1 con sistema operativo Centos, como Servidor Web la PC2 con sistema operativo Debian y PC3 como cliente con sistema operativo Windows. Así mismo se realizó un laboratorio de pruebas como indica la figura, esto para establecer comunicación entre los hosts y comprobar la correcta configuración de la pila dual tanto de los servidores como del cliente; Dichas pruebas de configuración facilitan la implementación puesto que, si estas funcionan correctamente entonces el despliegue se desarrollará de una manera eficiente.

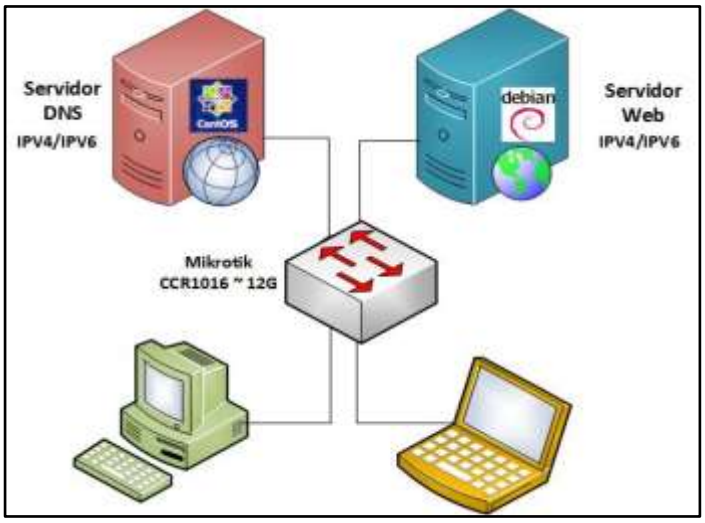


Figura 26: Laboratorio de Pruebas

6.4.2. Procedimiento de instalación y configuración de los servicios de internet (DNS y WEB)

Existen muchos servicios que se pueden ofrecer usando IPv6 como: FTP, SSH, Telnet, HTTP, DNS, Streaming, etc. Para el desarrollo de las pruebas se abordará el DNS (Sistema de Nombre de Dominio) y HTTP (Servidor Web).

6.4.2.1. Verificar Soporte IPv6

En la sección 6.1.5. se pudo comprobar que de acuerdo a las distribuciones de S.O que utilizan los servidores, estas ya soportan IPv6, pero de todas formas habrá que asegurarse, para ello abrimos el shell y escribimos **ping6 -c5 ::1** si el resultado es el siguiente:

```
kelen@kelen:~$ ping6 -c5 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from ::1: icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from ::1: icmp_seq=5 ttl=64 time=0.057 ms

--- ::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.046/0.051/0.057/0.006 ms
```

Figura 27: Verificar soporte IPv6 en Linux

Significa que nuestro GNU/Linux ya se encuentra disponible para soportar IPv6, si no se debe activar IPv6 en nuestro equipo, para lo cual verificamos que tenemos soporte en el kernel que estamos corriendo usando el siguiente comando condicional en el shell:

```
$ [ -f /proc/net/if_inet6 ] && echo 'El kernel está disponible para IPv6!' || echo 'No existe soporte IPv6! Compile the kernel!!'
```

```
kelen@kelen:~$ [ -f /proc/net/if_inet6 ] && echo 'El kernel está disponible para IPv6!' || echo
 'No existe soporte IPv6! Compile the kernel!!'
El kernel está disponible para IPv6!
```

Figura 28: Verificar soporte en el kernel

Si lo ejecutado anteriormente falla, esto implica que el módulo IPv6 no está cargado en el sistema Linux. Entonces lo que se debe hacer es ingresar con privilegios de usuario root y tipear el siguiente comando:

```
# modprobe
```

Comprobamos si el kernel fue cargado para ello digitamos:

```
lsmod | grep -w 'ipv6' && echo "El módulo fue cargado"
```

Finalmente se vuelve a hacer ping6 -c5 ::1, con lo que se comprueba que nuestro equipo ya dispone de soporte IPv6.

6.4.2.2. Configuración de las Direcciones IPv6 en los Servidores

Se debe mencionar que en los servidores se va a realizar asignación estática por lo que a continuación se explica el procedimiento para dicha asignación.

En las pruebas se utilizó direcciones IPv6 reales, además el direccionamiento IPv4 existente y para documentar las mismas se utilizó el prefijo de documentación. Es preciso acotar que los servidores no poseen ninguna configuración, por lo que será necesario configurarlos para que trabajen con pila dual, es decir, que tendrán ambas versiones de protocolo IP, acompañadas de la instalación de aplicaciones que permitan el funcionamiento de los servidores.

- **Configurar la dirección IPv6 en el Sistema Operativo Debian**

Para configurar una dirección IPv6 en el sistema Debian se debe editar el fichero **/etc/network/interfaces** y añadir una nueva definición de interfaz la family **inet6**, para lo cual ingresamos en consola:

nano /etc/network/interfaces

```
iface eth0 inet static
        address 10.10.58.252
        netmask 255.255.255.0
        gateway 10.10.58.1

iface eth0 inet6 static
        address 2800:68:7:f::4
        netmask 64
        gateway 2800:68:7:f::ffff
```

Figura 29: Configuración Dual (IPv4-IPv6) en Debian - Fichero /etc/network/interface

Donde:

- En la directiva address se va a asignar la dirección IPv6 a configurar en el equipo.
- netmask: corresponde a la máscara de red (en el caso de IPv6 un barra 64)
- gateway: la puerta de enlace IPv6

Nota: La configuración realizada anteriormente corresponde a la asignación estática de una dirección IP mediante doble pila (Dual stack).

A continuación reiniciamos la interfaz de red [eth0] para que se puedan fijar los cambios realizados:

invoke-rc.d networking restart

- **Activar dirección IPv6 en el Sistema Operativo Centos.**

  En el fichero **/etc/sysconfig/network** especificamos la información sobre la configuración de red deseada.

```
GNU nano 2.3.1                Fichero: /etc/sysconfig/network

NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=dns.unl.edu.ec
```

Figura 30: Activar IPv6 en Centos – Fichero /etc/sysconfig/network

Dónde:

- La directiva NETWORKING_IPV6 = yes habilita IPv6 en la interfaz.
- HOSTNAME: Debe ir el Fully Qualified Domain Name (FDQ), nombre de dominio cualificado completo o también el nombre del host.

- **Configurar la dirección IPv6 en el sistema Centos Dual-Stack.**

  Ingresamos al archivo de configuración **/etc/sysconfig/network-scripts/ifcfg-eth0** de la interfaz deseada en este caso [eth0] y agregamos lo siguiente:

```
GNU nano 2.3.1   Fichero: /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
NAME=eth0
UUID=62a1245c-41c0-406b-a6b7-7d81cfa2dbaa
DEVICE=eth0
ONBOOT=yes
IPADDR=172.16.32.51
PREFIX=19
GATEWAY=172.16.32.1
IPV6ADDR=2001:db8:7:ff02:54:8dd9::cb3/64
IPV6_DEFAULTGW=2001:db8:7:ff02::ffff
```

Figura 31: Configuración IPv4-IPv6 en Centos - Fichero /etc/sysconfig/network-scripts/ifcfg-eth0

Donde:

- En la directiva DEVICE: Colocamos el nombre del dispositivo físico
- ONBOOT = yes: El dispositivo debe activarse en el momento de arranque.

- IPV6INIT = yes: Habilita IPv6 en esa interfaz y permite que arranque el módulo IPv6 al iniciar el sistema.
- IPV6ADDR: Se debe colocar la dirección IPv6 que se asignará a la interfaz
- IPADDR: Dirección IP (IPv4)
- PREFIX: Prefijo de Red
- IPV6_DEFAULTGW: Especifica la puerta de enlace IPv6

Seguidamente reiniciamos la interfaz de red, para lo cual ingresamos lo siguiente:

sudo service network restart

Otra manera de agregar una dirección IPv6 es realizarlo de forma temporal (si se reinicia la interfaz o el servidor se apaga se perderá) mediante el comando **ip o ifconfig**, como se muestra en el ANEXO II.

Para verificar que en la interfaz [eth0] se agregó la dirección IPv6 [2001:db8:7:ff02:54:8dd9::cb3/64] se lo puede hacer de cualesquiera de las siguientes manera y comprobamos conectividad a la misma interfaz.

```
[kmlapol@dns ~]$ ifconfig eth0 | grep inet6
    inet6 2001:db8:7:ff02:54:8dd9::cb3 prefixlen 64  scopeid 0x0<global>
    inet6 fe80::5054:ff:fe23:9e4b  prefixlen 64  scopeid 0x20<link>

[kmlapol@dns ~]$ ip -6 addr show eth0 | grep inet6
    inet6 2001:db8:7:ff02:54:8dd9::cb3/64 scope global
    inet6 fe80::5054:ff:fe23:9e4b/64 scope link

[kmlapol@dns ~]$ ping6 -I eth0 -c 2 2001:db8:7:ff02:54:8dd9::cb3
PING 2001:db8:7:ff02:54:8dd9::cb3 (2001:db8:7:ff02:54:8dd9::cb3) 56 data bytes
64 bytes from 2001:db8:7:ff02:54:8dd9::cb3: icmp_seq=1 ttl=64 time=0.031ms
64 bytes from 2001:db8:7:ff02:54:8dd9::cb3: icmp_seq=2 ttl=64 time=0.056ms

--- 2001:db8:7:ff02:54:8dd9::cb3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.031/0.043/0.056/0.014 ms
```

Figura 32: Comprobar conectividad con la dirección IPv6

Es importante mencionar que cuando comprobamos la conectividad de la dirección IPv4 o IPv6, tanto en Windows como en Linux se utiliza el comando ping, pero en el caso de Gnu/Linux es necesario especificar la versión del protocolo con el comando ping6 y agregar lo siguiente:

- -I eth0: Dirección de la interfaz de origen.

- -c 2: Indica el número de paquetes a contabilizar.

6.4.2.2. Procedimiento de instalación y configuración del servidor DNS

- **Instalación de Bind**

Existen varios programas de servidor ¨dns¨ -que soportan IPv6, los más usados, tanto en IPv4 como en IPv6, son "Bind" para diferentes plataformas (Windows, Gnu / Linux, etc). Para la instalación se puede hacer uso de los sistemas habituales de cada distribución (apt-get, yum, up2date, rpm, etc.), en nuestro caso usamos el siguiente comando:

sudo yum install bind bind-utils

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
too slow. Less than 1000 bytes/sec transferred the last 30 seconds')
Intentando con otro espejo.
(3/3): bind-9.9.4-29.el7_2.4.x86_64.rpm                    | 1.8 MB   00:01
--------------------------------------------------------------------------------
Total                                              85 kB/s | 3.0 MB  00:35
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Instalando    : 32:bind-libs-9.9.4-29.el7_2.4.x86_64                    1/3
  Instalando    : 32:bind-9.9.4-29.el7_2.4.x86_64                         2/3
  Instalando    : 32:bind-utils-9.9.4-29.el7_2.4.x86_64                   3/3
  Comprobando   : 32:bind-9.9.4-29.el7_2.4.x86_64                         1/3
  Comprobando   : 32:bind-libs-9.9.4-29.el7_2.4.x86_64                    2/3
  Comprobando   : 32:bind-utils-9.9.4-29.el7_2.4.x86_64                   3/3

Instalado:
  bind.x86_64 32:9.9.4-29.el7_2.4     bind-utils.x86_64 32:9.9.4-29.el7_2.4

Dependencia(s) instalada(s):
  bind-libs.x86_64 32:9.9.4-29.el7_2.4

¡Listo!
```

Figura 33: Instalación del programa Bind9

Otra forma de instalar bind es descargando los ficheros fuente de **www.isc.org** y compilarlo de la siguiente manera:

```
# tar -xzvf versión del paquete-P2.tar.gz
# cd bind-versión del paquete-P2
# ./configure
# make
# make install
```

- **Configuración del Servidor DNS**

Una vez que hemos instalado el programa Bind, se procede a configurar el archivo principal el mismo que se encuentra en **/etc/named.conf,** es aquí donde vamos a realizar algunas modificaciones en ciertas directivas para el correcto funcionamiento de IPv6.

Habilitar peticiones IPv6.

Para habilitar correctamente las consultas DNS que se realicen a la dirección IPv6 del servidor de nombres, se debe agregar las siguientes directivas en el archivo de configuración principal **/etc/named.conf**.

```
GNU nano 2.3.1                                  Fichero: /etc/named.conf

acl “publicos” {
            10.10.0.0/8;
            172.16.32.0/19;
            127.0.0.1;
} ;

acl “publicos6” {
            2001:db8:7::/48;
            ::1/128;
} ;

options {
             listen-on port 53 {127.0.0.1; 172.16.32.51; };
             listen-on-v6 port 53 {::1; 2001:db8:7:ff02:54:8dd9::cb3; };
             directory           “/var/named”;
             dump-file           “/var/named/data/cache_dump.db”;
             statistics-file     “/var/named/data/named_stats.txt”;
             memstatistics-file  “/var/named/data/named_men_stats.txt”;
             allow-query       {localhost; publicos; publicos6; };

}
```

Figura 34: Fichero configuración principal del DNS - /etc/named.conf

Donde:

- Las acl (listas de control de acceso) son utilizadas para controlar el flujo de tráfico en equipos de red, en este caso vamos a tener dos acl’s, una especificando la dirección de red IPv4 y otra especificado la dirección IPv6.
- La declaración options {} contiene las especificaciones que controlan el comportamiento global del servidor, se puede usar para especificar la ubicación del directorio de trabajo (named), los puertos de escucha, entre otros.

- La opción “Listen-on”, lista las direcciones IPv4 y puertos habilitados para responder a las consultas DNS
- Las directivas listen-on-v6 port 53 {::1; 2001:db8:7:ff02:54:8dd9::cb3; }; permite indicarle al servidor Dns en que puerto escuchar para recibir peticiones de clientes Ipv6.
- La opción “directory” indica en que directorio se encuentran los archivos utilizados por el bind.
- La opción “allow-query” indica el bloque de direcciones IP que tienen permisos para realizar consultas al servidor.

Para comprobar que el servidor está escuchando en las direcciones IPv4 e IPv6 en el puerto del Dns [53] en los protocolos TCP y UDP, se lo hace ingresando lo siguiente:

netstat –anutp

Y cuyo resultado es el presentado a continuación:

```
tcp        0  0 172.16.32.51:53            0.0.0.0:*       LISTEN      27144/named
tcp        0  0 127.0.0.1:53              0.0.0.0:*       LISTEN      27144/named
tcp6       0  0 2001:db8:7:ff02:54:8d:53   :::*            LISTEN      27144/named
tcp6       0  0 ::1:53                     :::*            LISTEN      27144/named
udp        0  0 172.16.32.51:53            0.0.0.0:*       LISTEN      27144/named
udp        0  0 127.0.0.1:53              0.0.0.0:*       LISTEN      27144/named
udp6       0  0 2001:db8:7:ff02:54:8d:53   :::*                        27144/named
udp6       0  0 ::1:53                     :::*                        27144/named
```

Figura 35: Comprobar puertos e IP de escucha del servidor DNS

Netstat: Es una herramienta que nos permite verificar que puertos están abiertos y si los programas escuchan en esos puertos, es decir, permite verificar las conexiones entrantes y salientes, protocolo TCP – UDP y estado de las conexiones tanto para IPv4 e IPv6.

Configuración de las Zonas de Resolución Directa e Inversa

Los servidores DNS tienen lo que se llama ficheros de zona que contienen la información del servidor de nombre relacionado con un dominio, en este caso unl.edu.ec.

En el fichero ***/etc/named.conf*** se pueden definir directamente las zonas para las que nuestro servidor va a ser autorizado. En nuestro caso hemos establecido una zona de resolución directa (IPv4 e IPv6), una de resolución inversa para IPv4 y otra de resolución inversa para IPv6, tal como se muestra:

```
GNU nano 2.3.1      Fichero: /etc/named.conf
//Zona directa

zone “unl.edu.ec”  IN {
             type master;
             file “db.unl.edu.ec”;
             allow-update { none; };
};
```

Figura 36: Creación de Zona Directa – /etc/named.conf

```
GNU nano 2.3.1   Fichero: /etc/named.conf
//Zona reversa IPv4

zone “32.16.172.in-addr.arpa”  IN {
              type master;
              file “db.inversa4”;
              allow-update { none; };
};
```

Figura 37: Creación de Zona Reversa IPv4 – /etc/named.conf

```
GNU nano 2.3.1              Fichero: /etc/named.conf
//Zona reversa IPv6

zone “2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa”  IN {
             type master;
             file “db.inversa6”;
};
```

Figura 38: Creación de Zona Reversa IPv6 – /etc/named.conf

Donde:

- Zone: es identificada como unl.edu.ec para la resolución directa
- type master: define al servidor autoritativo para esa zona.
- File: especifica el nombre del archivo en el directorio de trabajo named que contiene información de configuración de la zona.
- Allow-update: Especifica los hosts que están autorizados para actualizar dinámicamente la información en sus zonas. Por defecto no se autoriza la actualización dinámica de la información.

En la Figura 36 la zona **“unl.edu.ec”** indica el dominio sobre el cual el servidor DNS tiene autoridad para responder consultas (type master), el servicio named se instruye para leer el archivo **/var/named/db.unl.edu.ec** y se le dice a named que no permita actualizaciones por parte de otros hosts.

De igual manera, la Figura 37 **“32.16.172.in.addr.arpa”** indica cuál es la zona de direccionamiento reverso IPv4, el servicio named se instruye para leer el archivo **/var/named/db.inversa4** y se le dice a named que no permita actualizaciones por parte de otros hosts y finalmente en la Figura 38 **“2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa”** indica cuál es la zona de direccionamiento reverso IPv6 por la(s) que el servidor responde.

Cabe mencionar que en la zona de resolución inversa para IPv6 el prefijo (2001:db8:7:ff02::/64) se divide en nibles y se concatena en orden inverso para declarar la zona al dominio **ip6.arpa.** Esta zona permitirá la resolución inversa de las direcciones IPv6 cuyo fichero es **db.inversa6.**

Creación de los ficheros de zona para la resolución directa e inversa

Los ficheros de zona se crean en el directorio **/var /named/.** Para crear los ficheros de zona podemos guiarnos en la plantilla named.localhost y editarla, para lo cual ingresamos en consola lo siguiente:

Para la resolución directa:

cp /var /named/named.localhost /var/named/db.unl.edu.ec

Para la resolución inversa:

cp /var /named/named.localhost /var/named/db.inversa4

cp /var /named/named.localhost /var/named/db.inversa6

Comprobamos que los archivos de zonas se han creado

Figura 39: Archivos de zona creados

Archivo de resolución directa

En la resolución de nombres a direcciones IPv6, existe el registro AAAA (quad A) en el DNS. El registro AAAA toma como datos de registro específico el formato textual de una dirección IPv6. Los registros A y AAAA pueden coexistir lado a lado en cualquier zona directa. Por ejemplo si el host tiene una dirección IPv4 y una dirección IPv6 (host Dual

stack), pueden conectar tanto registros A como AAAA de su nombre de dominio. En nuestra configuración editamos el fichero para resolución directa que se encuentra en **/var/named/db.unl.edu.ec** y añadimos lo siguiente:

```
GNU nano 2.3.1            Fichero: /var/named/db.unl.edu.ec
$TTL 604800
@     IN SOA  dns.unl.edu.ec.   root.unl.edu.ec. (
                              2016121601 ; serial
                              604800     ; refresh
                              86400      ; retry
                              2419200    ; expire
                              604800     ; minimum
                              )

@     IN     NS     dns.unl.edu.ec.

dns   IN     A        172.16.32.51
dns   IN     AAAA    2001:db8:7:ff02:54:8dd9::cb3
eva           IN A        172.16.32.67
eva           IN AAAA    2001:db8:7:ff02:b2:a056::cc3
cursosmed     IN A        172.16.32.199
cursosmed     IN AAAA    2001:db8:7:ff02:de:39f0::7dc7
virtual       IN A        172.16.32.200
virtual       IN AAAA    2001:db8:7:ff02:de:39f0::7dc8
evaluaciondocente   IN A       172.16.32.118
evaluaciondocente   IN AAAA    2001:db8:7:ff02:93:4d18::7d76
graduados     IN A        172.16.32.84
graduados     IN AAAA    2001:db8:7:ff02:c4:b96a::cd4
formacion     IN A        172.16.32.13
formacion     IN AAAA    2001:db8:7:ff02:d8:c1f4::c8d
capacitacion IN A        172.16.32.44
capacitacion IN AAAA    2001:db8:7:ff02:c3:9843::cac
openvpn       IN A        172.16.32.45
openvpn       IN AAAA    2001:db8:7:ff02:10:4ed4::cad
dspace        IN A        172.16.32.89
dspace        IN AAAA    2001:db8:7:ff02:d3:eab9::cd9
unl.edu.ec.   IN A        172.16.32.112
unl.edu.ec.   IN AAAA    2001:db8:7:ff02:3c:8289::7d70
www           IN CNAME    unl.edu.ec.
```

Figura 40: Fichero de resolución directa IPv4-IPv6

Archivos de Resolución Inversa

El registro empleado para la resolución inversa de una dirección IPv6 es “PTR”, igual como ocurre en la resolución inversa de direcciones IPv4, y como en cualquier zona deben contener un registro SOA (Autoridad de la zona) y uno o más registros NS (Name Server).

A continuación se configura los archivos de resolución inversa tanto para IPv4 como para IPv6.

Archivo de resolución inversa Ipv4

Editamos el fichero **/var/named/db.inversa4** y añadimos lo siguiente:

```
GNU nano 2.3.1            Fichero: /var/named/db.inversa4
$TTL 604800
@      IN SOA  dns.unl.edu.ec.   root.unl.edu.ec. (
                              2016121601 ; serial
                              604800     ; refresh
                              86400      ; retry
                              2419200    ; expire
                              604800     ; minimum
                              )

@      IN     NS      dns.unl.edu.ec.

51     IN     PTR     dns.unl.edu.ec.

67     IN     PTR     eva.unl.edu.ec.
199      IN   PTR     cursosmed.unl.edu.ec.
200      IN   PTR     virtual.unl.edu.ec.
118      IN   PTR     evaluaciondocente.unl.edu.ec.
84     IN     PTR     graduados.unl.edu.ec.
13     IN     PTR     formacion.unl.edu.ec.
44     IN     PTR     capacitacion.unl.edu.ec.
45     IN     PTR     openvpn.unl.edu.ec.
89     IN     PTR     dspace.unl.edu.ec.
112    IN     PTR     unl.edu.ec
```

Figura 41: Fichero de resolución inversa IPv4

Como se indica en la figura la zona de resolución inversa IPv4 está definida como 32.16.172.in.addr.arpa, que equivale a los primeros 3 octetos y en cada registro PTR se completa el siguiente octeto.

Archivo de resolución inversa Ipv6

El registro empleado para la resolución inversa de una dirección IPv6 es “PTR”, igual como ocurre en la resolución inversa de direcciones IPv4, y como en cualquier zona deben contener un registro SOA (Autoridad de la zona) y uno o más registros NS (Name Server), con la única diferencia que en IPv6 la representación de la dirección inversa es en nibbles.

A continuación se configura los archivos de resolución inversa para IPv6, para lo cual editamos el fichero **var/named/db.inversa6** y añadimos lo siguiente:

```
GNU nano 2.3.1                Fichero: /var/named/db.inversa6
$TTL 604800
@     IN SOA  dns.unl.edu.ec.   root.unl.edu.ec. (
                                      2016121601   ; serial
                                      604800       ; refresh
                                      86400        ; retry
                                      2419200      ; expire
                                      604800       ; minimum
                                      )

@     IN    NS    dns.unl.edu.ec.

3.b.c.0.0.0.0.0.9.d.d.8.4.5.0.0 IN    PTR     dns.unl.edu.ec.

3.c.c.0.0.0.0.0.6.5.0.a.2.b.0.0 IN    PTR     eva.unl.edu.ec.
7.c.d.7.0.0.0.0.0.f.9.3.e.d.0.0 IN    PTR     cursosmed.unl.edu.ec.
8.c.d.7.0.0.0.0.0.f.9.3.e.d.0.0 IN    PTR     virtual.unl.edu.ec.
6.7.d.7.0.0.0.0.8.1.d.4.3.9.0.0 IN    PTR     evaluaciondocente.unl.edu.ec.
4.d.c.0.0.0.0.0.9.8.2.8.c.3.0.0 IN    PTR     graduados.unl.edu.ec.
d.8.c.0.0.0.0.0.4.f.1.c.8.d.0.0 IN    PTR     formacion.unl.edu.ec.
c.a.c.0.0.0.0.0.3.4.8.9.3.c.0.0 IN    PTR     capacitacion.unl.edu.ec.
d.a.c.0.0.0.0.0.4.d.e.4.0.1.0.0 IN    PTR     openvpn.unl.edu.ec.
9.d.c.0.0.0.0.0.9.b.a.e.3.d.0.0 IN    PTR     dspace.unl.edu.ec.
0.7.7.e.0.0.0.0.9.8.2.8.c.3.0.0 IN    PTR     www.unl.edu.ec.
```

Figura 42: Archivo de resolución inversa IPv6

La zona de resolución inversa IPv6 está definida como 2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa, que equivale a los primeros 16 dígitos hexadecimales de la dirección IPv6 y en cada registro PTR se completa los siguientes 16 dígitos.

Una vez configurado cada uno de los archivos de zona, también es necesario configurar el fichero **/etc/resolv.conf** y se agrega lo siguiente:

```
GNU nano 2.3.1                Fichero: /etc/resolv.conf

search unl.edu.ec
nameserver 172.16.32.51
nameserver 2800:68:7:ff04:54:8dd9::cb3
```

Figura 43: Fichero /etc/resolv.conf

La línea “search” especifica en qué dominio buscar para cualquier nombre de máquina al que se desea conectar, “nameserver” especifica la dirección del servidor de nombres, en este caso como el mecanismo de transición utilizado es doble pila vamos a ubicar la dirección tanto IPv4 como IPv6 de nuestro servidor.

A continuación levantamos el demonio named del servidor DNS con el comando:

sudo systemctl restart named.service

Seguidamente revisamos los sucesos que se generan en el fichero ¨log¨/var/log/messages al iniciar, parar o reiniciar el demonio ¨named¨; esto nos permite verificar la correcta inicialización del DNS así como detectar posibles inconvenientes que se presenten, para ello utilizamos el siguiente comando:

sudo tail -f /var/log/messages

Pruebas de Configuración del Servidor DNS con Doble Pila

Para comprobar la correcta configuración y funcionalidad del servidor DNS se utilizará las siguientes herramientas:

Nslookup (Name System Lookup)

Es una herramienta que permite consultar un servidor de nombres y obtener información relacionada con el dominio o el host y así diagnosticar los posibles problemas de configuración que pudieran haber surgido en el DNS. Para la resolución directa o inversa con IPv6 se debe indicar que se trata de un registro quad “a” (AAA o aaaa).

Resolución directa con IPv4

```
[kmlapol@dns ~]$ nslookup dns.unl.edu.ec
Server:              172.16.32.51
Address:             172.16.32.51#53

Name:               dns.unl.edu.ec
Address:            172.16.32.51
```

Figura 44: Verificación de resolución directa con IPv4

Resolución inversa con IPv4

```
[kmlapol@dns ~]$ nslookup 172.16.32.51
Server:             172.16.32.51
Address:            172.16.32.51#53

51.32.16.172.in-addr.arpa         name = dns.unl.edu.ec.
```

Figura 45: Verificación de resolución inversa con IPv4

```
[kmlapol@dns ~]$ nslookup 172.16.32.67
Server:             172.16.32.51
Address:            172.16.32.51#53

67.32.16.172.in-addr.arpa         name = eva.unl.edu.ec.
```

Figura 46: Verificación de resolución inversa con IPv4 (Subdominio eva.unl.edu.ec)

Resolución directa con IPv6

```
[kmlapol@dns ~]$ nslookup -type=AAAA eva.unl.edu.ec
Server:             172.16.32.51
Address:            172.16.32.51#53

eva.unl.edu.ec    has  AAAA  Address 2001:db8:7:ff02:b2:a056::cc3
```

Figura 47: Verificación de resolución DNS con IPv6

Como se puede observar en la Figura 47 al realizar la consulta Dns con IPv6, se usa el comando quad “a” (AAAA), lo que indica que nuestro servidor nos arrojará como respuesta la IPv6 del dominio consultado, en este caso eva.unl.ed.ec tiene la dirección IPv6 2001:db8:7:ff02:b2:a056::cc3.

Dig (Domain Information Groper)

Otra importante herramienta que se va a utilizar es Dig, la misma que permite realizar consultas a los servidores DNS, por lo que es muy útil para comprobar si el DNS está correctamente configurado en nuestra máquina. Además permite comprobar tanto el mapeo de nombres a IP’s como el mapeo inverso de IP’s a nombres. Esta herramienta nos proporciona información más detallada de nuestro servidor DNS.

Resolución directa, utilizando el parámetro quad "a"

Al utilizar la herramienta dig seguida del parámetro aaaa, estamos comprobando si nuestro servidor resuelve el dominio unl.edu.ec con la versión 6 del protocolo IP.

```
[kmlapol@dns ~]$ dig aaaa unl.edu.ec

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.4 <<>> aaaa unl.edu.ec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30012
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;unl.edu.ec.                IN   AAAA

;; ANSWER SECTION:
unl.edu.ec.         604800   IN   AAAA        ::1

;; AUTHORITY SECTION:
unl.edu.ec.         23330    IN   NS          dns.unl.edu.ec.

;; ADDITIONAL SECTION:
dns.unl.edu.ec.     604800   IN   A            172.16.32.51
dns.unl.edu.ec.     604800   IN   AAAA         2001:db8:7:ff02:54:8dd9::cb3

;; Query time: 0 msec
;; SERVER: 172.16.32.51#53(172.16.32.51)
;; WHEN: mar dic 06 17:06:55 ECT 2016
;; MSG SIZE  rcvd: 135
```

Figura 48: Consulta DNS con la herramienta Dig – Resolución Directa IPv6

Resolución inversa, utilizando el parámetro "-x".

Al utilizar la herramienta dig seguida del parámetro -x, le estamos consultando a nuestro servidor el dominio correspondiente a esa dirección IP. En las Figuras 49 y 50 se puede observar cómo se realiza una consulta con IPv4 y con IPv6 respectivamente.

```
[kmlapol@dns ~]$ dig -x 172.16.32.51

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.4 <<>> -x 172.16.32.51
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2196
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;51.32.16.172.in-addr.arpa.           IN   PTR

;; ANSWER SECTION:
51.32.16.172.in-addr.arpa.    604800   IN   PTR   dns.unl.edu.ec.

;; AUTHORITY SECTION:
51.32.16.172.in-addr.arpa.    604800   IN   NS    dns.unl.edu.ec.

;; ADDITIONAL SECTION:
dns.unl.edu.ec.               604800   IN   A     172.16.32.51
dns.unl.edu.ec.               604800   IN   AAAA  2001:db8:7:ff02:54:8dd9::cb3

;; Query time: 0 msec
;; SERVER: 172.16.32.51#53(172.16.32.51)
;; WHEN: mar dic 06 00:14:59 ECT 2016
;; MSG SIZE  rcvd: 146
```

Figura 49: Resolución Inversa (IPv4) con la herramienta Dig

```
[kmlapol@dns ~]$ dig -x 2001:db8:7:ff02:54:8dd9::cb3

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.4 <<>> -x 2001:db8:7:ff02:54:8dd9::cb3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39599
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;3.b.c.0.0.0.0.0.9.d.d.8.4.5.0.0.2.0.f.f.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa.  IN
PTR

;; ANSWER SECTION:
3.b.c.0.0.0.0.0.9.d.d.8.4.5.0.0.4.0.f.f.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa.
604800 IN   PTR   dns.unl.edu.ec.

;; AUTHORITY SECTION:
```

```
2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa 604800     IN   NS    dns.unl.edu.ec.

;; ADDITIONAL SECTION:
dns.unl.edu.ec.               604800   IN   A     172.16.32.51
dns.unl.edu.ec.               604800   IN   AAAA  2001:db8:7:ff02:54:8dd9::cb3
;; Query time: 0 msec
;; SERVER: 172.16.32.51#53(172.16.32.51)
;; WHEN: vie dic 16 13:41:37 ECT 2016
;; MSG SIZE  rcvd: 193
```

Figura 50: Resolución Inversa (IPv6) con la herramienta Dig.

6.4.2.3. Procedimiento de instalación y configuración del Servidor Web

- **Instalación y Configuración de Apache en el Sistema Operativo Debian**

El servidor web que se encuentra en producción en la Universidad Nacional de Loja, utiliza el programa "Apache" por lo que se requiere instalar el mismo haciendo uso del siguiente comando:

apt-get install apache2

Una vez instalado Apache se crea los directorios donde se encontrará el código de la página web, tal como se muestra a continuación:

mkdir -p /var/www/html/prueba.com

y se da los permisos respectivos a las carpetas, además se debe crear el archivo index.html con el contenido de la página web que es lo que se va a visualizar en nuestro navegador.

```
  GNU nano 2.2.6          Fichero: index.html

<html>
  <head>
    <title>IPv4-ipV6</title>
  </head>
  <body>
    <h1>Bienvenidos a IPv4-IPv6</h1>
    <h2>Configurado Correctamente</h2>
  </body>
</html>
```

Figura 51: Código de la página web

En el fichero **/etc/apache2/ports.conf** se va a manipular porque interface se quiere que escuche nuestro servidor, como se indica:

```
GNU nano 2.2.6           Fichero: /apache2/ports.conf

Listen [2800:68:7:ff04:3c:8289::7d70]:80
Listen 172.16.32.112:80
```

Figura 52: IP's y puerto de escucha del servidor web

Dónde:

- Listen es la directiva utilizada para indicarle a nuestro servidor en que direcciones IP y puertos aceptar peticiones entrantes, para el caso de IPv6 es necesario que la dirección esté dentro de corchetes [] seguido por dos puntos y el puerto.

Nota: *Recordar que previo a las configuraciones que se acaban de realizar se debe haber verificado el soporte de IPv6 en el equipo que hará de servidor web, además de haber configura las direcciones IPv4 e IPv6 a utilizar.*

Para verificar los puertos en los que está escuchando apache tecleamos lo siguiente:

netstat –pan | grep apache

Configurar VirtualHost con IPv4-IPv6

Los VirtualHosts permiten que con una sola dirección IP se pueda atender varios nombres como por ejemplo www.sitio1.com, www.micompania.com, por cuestiones de práctica se creará los virtualhost para IPv4 e IPv6, aunque este no es el caso de la Universidad Nacional de Loja puesto dispone de un único dominio.

Creamos el archivo prueba.com.conf con doble pila

En el directorio **/etc/apache2/sites-available** es donde se va a creer el archivo **prueba.com.conf** que es donde vamos a configurar los virtualhost tanto para IPV4 como para IPV6.

Ingresamos por consola al archivo creado: **nano /etc/apache2/sites-available/prueba.com.conf,** y editamos agregando lo siguiente:

```
GNU nano 2.2.6      Fichero: /etc/apache2/sites-available/prueba.com.conf

NameVirtualHost [2001:db8:7:ff02:3c:8289::7d70]
NameVirtualHost  172.16.32.112

//IPv4-IPv6
<VirtualHost [2001:db8:7:ff02:3c:8289::7d70]>
        ServerAdmin webmaster@unl.edu.ec
        ServerName  www.unl.edu.ec
        DocumentRoot /var/www/html/prueba.com/
        DirectoryIndex /var/www/html/prueba.com/
</VirtualHost>

<VirtualHost [172.16.32.112]>
        ServerAdmin webmaster@unl.edu.ec
        ServerName  www.unl.edu.ec
        DocumentRoot /var/www/html/prueba.com/
        DirectoryIndex /var/www/html/prueba.com/
</VirtualHost>
```

Figura 53: VirtualHost (IPv4-IPv6) - Fichero /etc/apache2/sites-available/prueba.com.conf

La configuración de la Figura 53 permite al servidor:

- Atender peticiones sobre IPv4 a 172.16.32.112 y sobre IPv6 a 2001:db8:7:ff02:3c:8289::e770, tal es el caso de:

A continuación se explica algunas de las directivas empleadas en la configuración.

- ✓ **ServerAdmin**: Corresponde a la dirección de correo del administrador del Web server. Esta dirección de correo aparecerá en los mensajes de error generados por el servidor para páginas web, de tal manera que los usuarios pueden comunicar errores enviando correo al administrador.
- ✓ **ServerName:** Usado para configurar un nombre de servidor y un número de puerto para el servidor. El ServerName no necesita coincidir con el nombre real de la máquina.
- ✓ **DocumentRoot:** Es el directorio que contiene la mayoría de los archivos HTML que se entregarán en respuesta a peticiones. El directorio predeterminado DocumentRoot para servidores web es /var/www/html.
- ✓ **DirectoryIndex:** Es la página por defecto que entrega el servidor cuando hay una petición de índice de un directorio especificado con una barra (/) al final del nombre del directorio.

Habilitar los VirtualHost

Para habilitar los VirtualHost con las configuraciones realizadas ingresamos en consola

sudo a2ensite prueba.com.conf

y seguidamente reiniciamos apache

/etc/init.d/apache2 restart

Es importante destacar que cada vez que se realice alguna modificación en los archivos de configuración se debe reiniciar apache, para esto para que se puedan registrar los cambios realizados

Seguidamente editamos **/etc/hosts** y agregamos:

```
GNU nano 2.2.6                Fichero: /etc/hosts

127.0.0.1                       localhost
172.16.32.112                   www.unl.edu.ec
2001:db8:7:ff02:3c:8289::7d70   www.unl.edu.ec
```

Figura 54: Fichero /etc/hosts

En este fichero agregamos las direcciones IP correspondientes a los dos protocolos (IPv4 e Ipv6). Este el primer archivo que el sistema operativo lee antes de hacer una consulta DNS.

Configuración del DNS (/etc/resolv.conf)

El fichero resolv.conf especifica el dominio al que pertenece nuestra máquina y la dirección del servidor DNS. Es el cliente DNS responsable de mapear una petición de información de un programa en un host.

```
GNU nano 2.2.6                Fichero: /etc/resolv.conf

search unl.edu.ec
nameserver 172.16.32.51
nameserver 2001:db8:7:ff02:54:8dd9::cb3
```

Figura 55: /etc/resolv.conf

Comprobamos su funcionamiento

Ingresamos en el navegador lo siguiente y comprobamos que efectivamente aparece el contenido de nuestra página web, comprobando la correcta configuración del servidor web con doble pila.

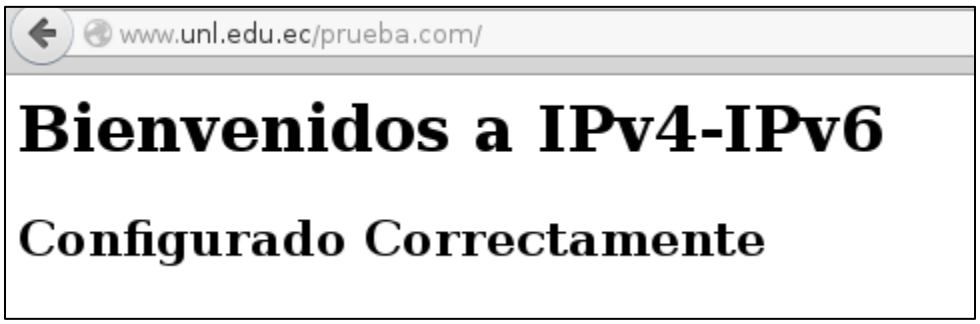


Figura 56: Página web con el dominio unl.edu.ec

Figura 57: Página Web con Doble Pila

6.4.2.4. Configuración de IPv6 en el Equipo Cliente

Para configurar el protocolo de internet versión 6 en el equipo que se usará como cliente, previamente se debe verificar si la versión de su sistema operativo dispone del protocolo IPv6 o si es necesario instalarlo o habilitarlo, en este caso nuestro equipo cliente tiene como S.O Windows 10, por lo que no es necesario hacer nada, puesto que desde versiones como: Windows XP SP1, Vista, W7 y posteriores ya viene con soporte completo.

La configuración de IPv6 se la realizará haciendo uso del entorno gráfico como se explica a continuación:

1. Se ingresa a “ver conexiones de red”
2. Seleccionar cualquier tipo de conexión
3. Clic derecho en Propiedades

4. Selecciona “Habilitar el protocolo de Internet versión 6 (TCP/IPv6)”
5. Propiedades
6. Se define qué tipo de configuración se va a realizar automática o manual.

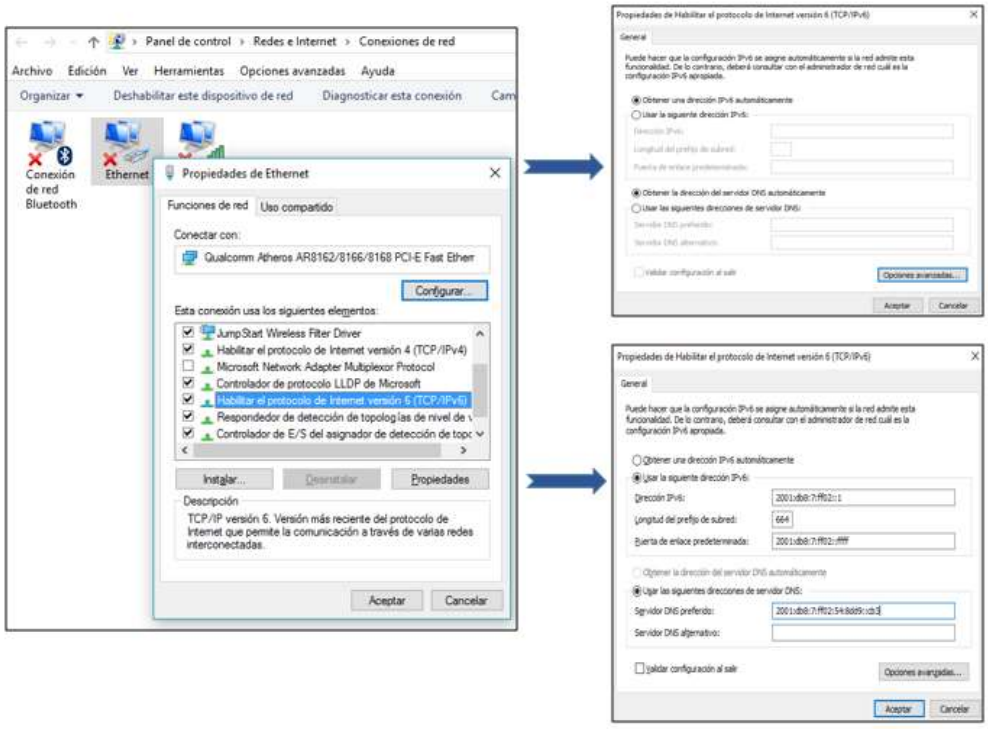


Figura 58: Configuración IPv6 en Windows

En la Figura 58, se puede observar que la configuración realizada es manual, en la que se especifica la dirección IPv6, longitud del prefijo de subred, la puerta de enlace y la dirección del servidor DNS.

7. Aceptar

Configurar equipo para que funcione con el dominio unl.edu.ec

Para configura el dominio se debe seguir los siguientes pasos:

1. En ícono de búsqueda de Windows ingresamos Configuración.
2. Ingresamos en Sistema
3. Seleccionamos “A cerca de” y si es necesario cambiamos el nombre del equipo o PC.

4. O vamos directamente a “Información del sistema” y en “Configuración de nombre, dominio y grupo de trabajo de equipo” se selecciona “Cambiar configuración”
5. Clic en “Cambiar” y agregamos el dominio

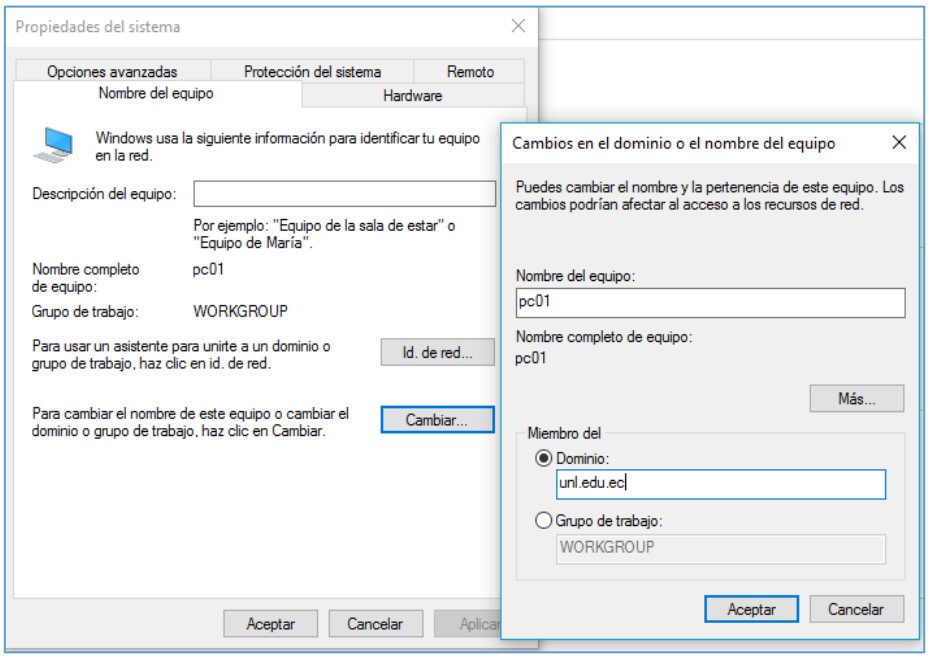


Figura 59: Configurar Dominio unl.edu.ec

6. Aceptar

Comprobar funcionamiento

Para comprobar el funcionamiento se establece conexión desde el equipo cliente al servidor dns, usando el comando ping, como se explica en las Figuras.

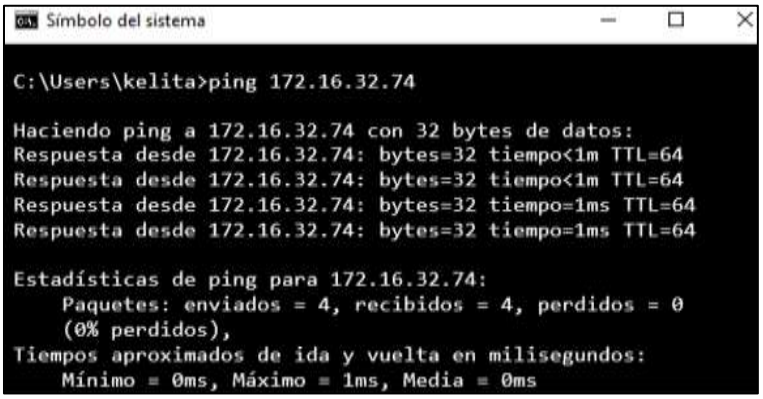


Figura 60: Prueba del comando ping con IPv4 del servidor DNS desde el Equipo Cliente

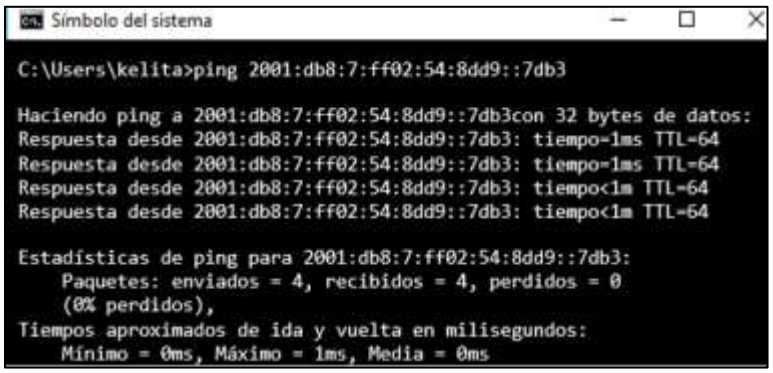


Figura 61: Prueba del comando ping con IPv6 del servidor DNS desde el Equipo Cliente

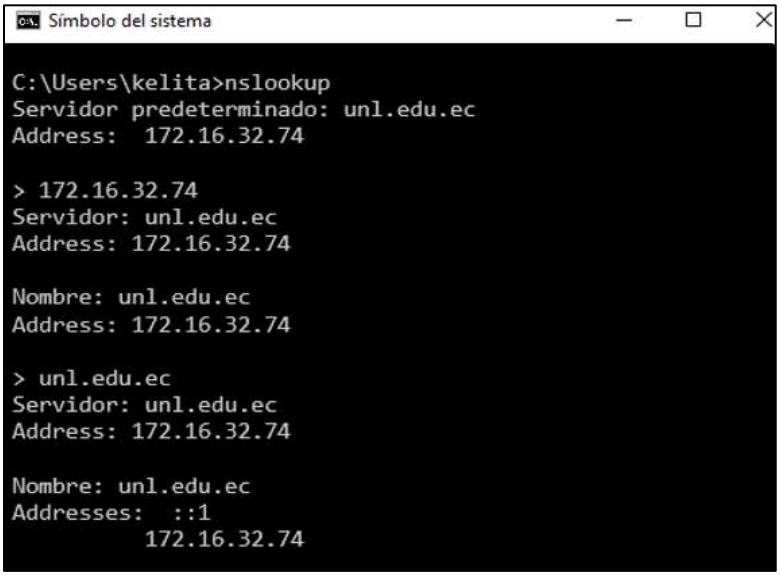


Figura 62: Prueba del comando nslookup con dominio unl.edu.ec – Equipo Cliente

Una vez realizadas las pruebas de verificación, se comprueba la correcta configuración del servidor DNS y servidor Web con pila dual (IPv4 e IPv6), como parte del escenario de pruebas, con estos resultados se puede dar inicio a la implementación de IPv6 en los servidores que actualmente se encuentran en producción.

6.5. OBJETIVO 5: Realizar las configuraciones necesarias para la implementación de IPv6 en el DNS autoritario y Servidores públicos de la Universidad Nacional de Loja.

Para llevar a cabo el desarrollo del Objetivo 5, y como se mencionó anteriormente la Red de datos de la Universidad Nacional de Loja está en funcionamiento mediante el Protocolo de Internet Versión 4 (IPv4), lo que permite que la implementación de la nueva versión de IP (IPv6), resulte un poco más cómoda. Además de que las configuraciones que se realizaron en al apartado 6.4.2 correspondiente al escenario de pruebas son de mucha importancia, puesto que las mismas fueron realizadas basándose en el direccionamiento real correspondiente a las dos versiones del Protocolo de Internet (IPv4 e IPv6), lo que facilita aún más el despliegue de IPv6.

En lo que respecta al servidor DNS autoritativo y a los servidores públicos lo que se debe hacer es agregar ciertas directivas que rigen IPv6 y la modificación y creación de algunos de los archivos de configuración.

En cuanto a la implementación del protocolo IPv6 en el DNS autoritario, queda bajo la responsabilidad de la Unidad de Telecomunicaciones e Información (ver Anexo IV) realizar dichas configuraciones, puesto que este servicio posee cierto grado de criticidad y requiere continuo funcionamiento; Por este motivo se elaboró un manual dirigido al Administrador de la Red (ver Anexo V), en el cual se detalla las configuraciones y los pasos a seguir para el despliegue de IPv6 en el DNS y su puesta en ejecución. Además se me otorgó por parte de la UTI, los ficheros de configuración del DNS en producción, para que se realice la respectiva adaptación de los parámetros y directivas IPv6, y luego de su modificación fueron devueltos a la Unidad para que realice la respectiva implementación.

6.5.1. Configuración de IPv6 en los servidores públicos

La Unidad de Telecomunicaciones e Información, dispuso realizar la implementación de IPv6 en un número determinado de servidores públicos los cuales se mencionan a continuación:

- Eva
- Capacitación

- Formación
- Graduados
- Servidor Web (unl.edu.ec)

Para acceder y configurar IPv6 en cada uno de los servidores públicos (servidores web), se lo hace mediante el protocolo SSH, con la infraestructura de clave pública (pki), mediante el usuario kmlapol como se indica en la Figura 63.

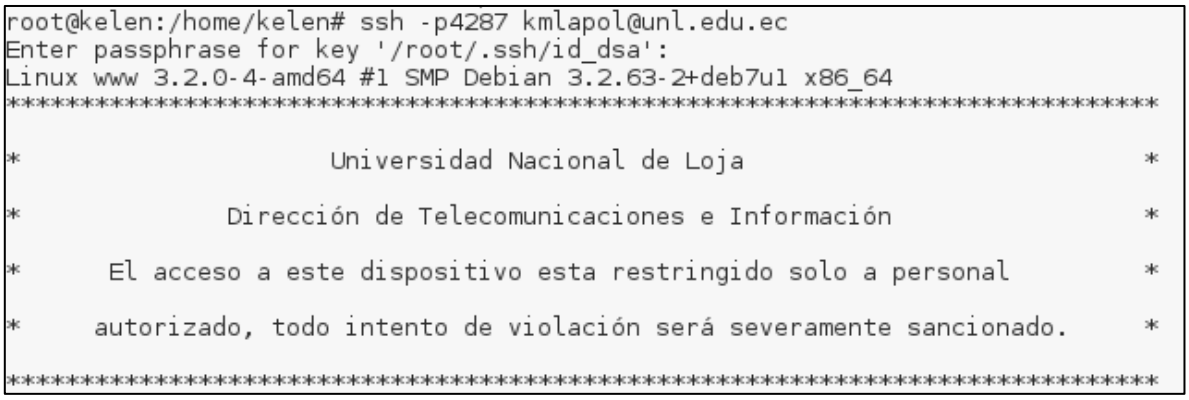


Figura 63: Interfaz de Ingreso a los servidores

Para mantener una estructura o procedimiento de asignación de la dirección IPv6 se ha establecido los siguientes pasos:

1. Acceso al servidor mediante el usuario asignado para ese servidor (SSH).
2. Verificar el soporte para IPv6
3. Ingresar al fichero /etc/network/interface (Antes de la asignación de IPv6 solo se podrá visualizar configuraciones relacionadas a IPv4).)
4. Asignar la dirección IPv6, máscara de subred, puerta de enlace o Gateway correspondiente al servidor en mención.
5. Guardar los cambios realizados (Ctrl+O).
6. Reiniciar Interfaz para hacer efectivos los cambios realizados mediante el comando:

/etc/init.d/networking restart

6.5.1.1. Servidor eva

Una vez de haber ingresado al servidor eva, se procede a realizar la verificación de soporte IPv6, haciendo ping6 a la dirección lookback de la siguiente manera:

```
kmlapol@eva:~$ ping6 -c2 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.031 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.023/0.027/0.031/0.004 ms
```

Figura 64: Comprobar soporte IPv6

Agregar dirección IPv6.

Luego de haber verificado el soporte de IPv6, se ingresa al fichero **/etc/network/interface,** que es donde se va a configurar la dirección IPv6, la máscara y el Gateway; como se puede observar en la Figura 65 la configuración existente está con el protocolo IPv4 y lo que se va a hacer es agregar lo competente a IPv6.

```
iface eth0 inet static
        address 172.[redacted]
        netmask 255.255.224.0
        network 172.[redacted]
        broadcast 172.[redacted]
        gateway 172.[redacted]
        # dns-* options are implemented by the r
        dns-nameservers [redacted]
        dns-search unl.edu.ec

#IPv6

iface eth0 inet6 static
        address 2800:68:7[redacted]c3
        netmask 64
        gateway 2800:68:7[redacted]eff
```

Figura 65: Agregar IPv6 en servidor eva - Fichero /etc/network/interface

Pruebas de conectividad

Una vez asignada la dirección IPv6 y después de haber guardado los cambios, se procede a realizar la respectiva comprobación de conectividad. Primero comprobamos conectividad a la puerta de enlace y luego comprobamos conectividad hacia Internet con IPv6 utilizando sitios que ya disponen de este nuevo protocolo como lo es google, facebook.

```
kmlapol@eva:~$ ping6 -c 4 2800:68:7:[redacted]eff
PING 2800:68:7:ff04::feff(2800:68:7:[redacted]eff) 56 data bytes
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=1 ttl=64 time=0.401 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=2 ttl=64 time=0.492 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=3 ttl=64 time=0.549 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=4 ttl=64 time=0.483 ms

--- 2800:68:7:[redacted]feff ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.401/0.481/0.549/0.055 ms
```

Figura 66: Ping6 desde el servidor eva a la puerta de enlace (gateway).

Conectividad hacia Internet con IPv6

Para establecer conexión con IPv6 a Internet se lo hará tanto con el dominio como la dirección IPv6 del sitio web.

```
kmlapol@eva:~$ ping6 www.google.com
PING www.google.com(atl14s77-in-x04.1e100.net) 56 data bytes
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=1 ttl=52 time=85.2 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=2 ttl=52 time=85.2 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=3 ttl=52 time=85.5 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=4 ttl=52 time=85.3 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=5 ttl=52 time=85.3 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=6 ttl=52 time=85.3 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=7 ttl=52 time=85.2 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=8 ttl=52 time=85.2 ms
64 bytes from atl14s77-in-x04.1e100.net: icmp_seq=9 ttl=52 time=85.3 ms
^C
--- www.google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8011ms
rtt min/avg/max/mdev = 85.270/85.334/85.557/0.253 ms
```

Figura 67: Prueba del comando ping6 en la Internet con IPv6 (www.google.com) desde el servidor eva

```
kmlapol@eva:~$ ping6 -c 4 2607:f8b0:4002:808::2004
PING 2607:f8b0:4002:808::2004(2607:f8b0:4002:808::2004) 56 data bytes
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=1 ttl=52 time=85.2 ms
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=2 ttl=52 time=85.4 ms
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=3 ttl=52 time=85.4 ms
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=4 ttl=52 time=85.4 ms

--- 2607:f8b0:4002:808::2004 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 85.293/85.400/85.447/0.062 ms
```

Figura 68: Prueba del comando ping6 en el Internet con dirección IPv6 de Google desde el servidor eva

```
kmlapol@eva:~$ ping6 www.facebook.com
PING www.facebook.com(edge-star-mini6-shv-01-iad3.facebook.com) 56 data bytes
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=1 ttl=51 time=89.2 ms
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=2 ttl=51 time=89.1 ms
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=3 ttl=51 time=89.1 ms
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=4 ttl=51 time=89.2 ms
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=5 ttl=51 time=89.3 ms
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=6 ttl=51 time=89.3 ms
64 bytes from edge-star-mini6-shv-01-iad3.facebook.com: icmp_seq=7 ttl=51 time=89.2 ms
^C
--- www.facebook.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 89.134/89.237/89.327/0.171 ms
```

Figura 69: Prueba del comando ping6 en la Internet con IPv6 (www.facebook.com) desde el servidor eva

```
kmlapol@eva:~$ ping6 -c 4 2a03:2880:f12c:183:face:b00c:0:25de
PING 2a03:2880:f12c:183:face:b00c:0:25de(2a03:2880:f12c:183:face:b00c:0:25de) 56 d
64 bytes from 2a03:2880:f12c:183:face:b00c:0:25de: icmp_seq=1 ttl=52 time=66.1 ms
64 bytes from 2a03:2880:f12c:183:face:b00c:0:25de: icmp_seq=2 ttl=52 time=66.2 ms
64 bytes from 2a03:2880:f12c:183:face:b00c:0:25de: icmp_seq=3 ttl=52 time=66.2 ms
64 bytes from 2a03:2880:f12c:183:face:b00c:0:25de: icmp_seq=4 ttl=52 time=66.2 ms

--- 2a03:2880:f12c:183:face:b00c:0:25de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 66.161/66.207/66.243/0.184 ms
```

Figura 70: Prueba del comando ping6 en la Internet con dirección IPv6 de Facebook desde el servidor eva

Nota: *Para obtener la dirección IPv6 del sitio en Internet se lo hizo mediante el comando dig como indica la Figura 71:*

```
kmlapol@eva:~$ dig aaaa www.google.com

; <<>> DiG 9.9.5-9+deb8u6-Debian <<>> aaaa www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53731
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                        IN      AAAA

;; ANSWER SECTION:
www.google.com.         3       IN      AAAA    2607:f8b0:4002:807::2004

;; AUTHORITY SECTION:
com.                    168840  IN      NS      j.gtld-servers.net.
com.                    168840  IN      NS      l.gtld-servers.net.
com.                    168840  IN      NS      a.gtld-servers.net.
com.                    168840  IN      NS      h.gtld-servers.net.
com.                    168840  IN      NS      f.gtld-servers.net.
com.                    168840  IN      NS      i.gtld-servers.net.
com.                    168840  IN      NS      b.gtld-servers.net.
com.                    168840  IN      NS      d.gtld-servers.net.
com.                    168840  IN      NS      k.gtld-servers.net.
com.                    168840  IN      NS      g.gtld-servers.net.
com.                    168840  IN      NS      e.gtld-servers.net.
com.                    168840  IN      NS      c.gtld-servers.net.
com.                    168840  IN      NS      m.gtld-servers.net.

;; Query time: 3 msec
```

Figura 71: Obtener IPv6 del sitio google – Comando dig aaaa

Como se puede observar en las figuras anteriores, al establecer conectividad IPv6, esta se genera correctamente, lo que demuestra que la configuración de IPv6 en el servidor público denominado eva es correcta.

6.5.1.2. Servidor Capacitación

Una vez de haber ingresado al servidor capacitación, se procede a realizar la verificación de soporte IPv6, haciendo ping6 a la dirección lookback:

```
kmlapol@capacitacion:~$ ping6 -c2 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.031 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.024/0.027/0.031/0.006 ms
```

Figura 72: Comprobar soporte IPv6 en servidor capacitación

Agregar dirección IPv6.

Al igual que el servidor anterior se ingresa al fichero **/etc/network/interface,** que es donde se va a configurar la dirección IPv6, la máscara y el Gateway.

```
iface eth0 inet static
        address 172.[redacted]
        netmask 255.255.224.0
        network 172.[redacted]
        broadcast 172.[redacted]
        gateway 172.[redacted]
        # dns-* options are implemented by the
        dns-nameservers [redacted]
        dns-search unl.edu.ec

#IPv6
iface eth0 inet6 static
        address 2800:68:7:[redacted]ac
        netmask 64
        gateway 2800:68:7[redacted]eff
```

Figura 73: Agregar IPv6 servidor capacitación - Fichero /etc/network/interface

Pruebas de conectividad

Se comprueba primero conectividad a la puerta de enlace y luego conectividad hacia Internet con la dirección IPv6 utilizando los sitios YouTube y facebook.

```
kmlapol@capacitacion:~$ ping6 -c4 2800:68:7[redacted]feff
PING 2800:68:7[redacted]feff(2800:68:7[redacted]feff) 56 data bytes
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=1 ttl=64 time=0.407 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=2 ttl=64 time=0.978 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=3 ttl=64 time=0.751 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=4 ttl=64 time=0.501 ms

--- 2800:68:7[redacted]feff ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.407/0.659/0.978/0.223 ms
```

Figura 74: Ping6 desde el servidor capacitacion a la puerta de enlace (gateway).

Conectividad hacia Internet con IPv6

Para establecer conexión con IPv6 a Internet, se lo hará tanto con el dominio como la IPv6 del sitio web.

```
kmlapol@capacitacion:~$ ping6 -c 4 www.youtube.com
PING www.youtube.com(mia07s49-in-x0e.1e100.net) 56 data bytes
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=1 ttl=52 time=73.9 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=2 ttl=52 time=74.2 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=3 ttl=52 time=74.2 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=4 ttl=52 time=74.3 ms

--- www.youtube.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 73.953/74.194/74.348/0.309 ms
```

Figura 75: Prueba del comando ping6 en la Internet con IPv6 (www.youtube.com) desde el servidor capacitación

```
kmlapol@capacitacion:~$ ping6 2607:f8b0:4008:803::200e
PING 2607:f8b0:4008:803::200e(2607:f8b0:4008:803::200e) 56 data bytes
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=1 ttl=52 time=73.9 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=2 ttl=52 time=74.0 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=3 ttl=52 time=74.1 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=4 ttl=52 time=74.0 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=5 ttl=52 time=74.0 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=6 ttl=52 time=73.9 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=7 ttl=52 time=74.0 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=8 ttl=52 time=74.0 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=9 ttl=52 time=74.0 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=10 ttl=52 time=73.9 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=11 ttl=52 time=73.9 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=12 ttl=52 time=73.9 ms
^C
--- 2607:f8b0:4008:803::200e ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11013ms
rtt min/avg/max/mdev = 73.964/74.019/74.152/0.318 ms
```

Figura 76: Prueba del comando ping6 en el Internet con dirección IPv6 de YouTube desde el servidor capacitación

```
kmlapol@capacitacion:~$ ping6 -c 4 www.facebook.com
PING www.facebook.com(edge-star-mini6-shv-01-mia3.facebook.com) 56 data bytes
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=1 ttl=52 time=66.1 ms
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=2 ttl=52 time=66.2 ms
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=3 ttl=52 time=66.2 ms
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=4 ttl=52 time=66.1 ms

--- www.facebook.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 66.151/66.216/66.274/0.187 ms
```

Figura 77: Prueba del comando ping6 en la Internet con IPv6 (www.facebook.com) desde el servidor capacitación

Como se puede observar en las figuras anteriores, al establecer conectividad IPv6, esta se genera correctamente, lo que demuestra que la configuración de IPv6 en el servidor público denominado eva es correcta.

6.5.1.3. Servidor Formación

Al ingresar al servidor denominado formación, se procede a realizar la verificación de soporte IPv6, haciendo ping6 a la dirección lookback:

```
kmlapol@formacion:~$ ping6 -c 2 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.057 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.028/0.042/0.057/0.015 ms
```

Figura 78: Comprobar soporte IPv6 en servidor formación

Agregar dirección IPv6.

Se ingresa al fichero **/etc/network/interface,** y se agrega la dirección IPv6, la máscara y el Gateway.

```
iface eth0 inet static
        address 172.[redacted]
        netmask 255.255.224.0
        network 172.[redacted]
        broadcast 172.[redacted]
        gateway 172.[redacted]
        # dns-* options are implemented by the r
        dns-nameservers [redacted]
        dns-search unl.edu.ec

#IPv6
iface eth0 inet6 static
        address 2800:68:7[redacted]c8d
        netmask 64
        gateway 2800:68:7[redacted]eff
```

Figura 79: Agregar IPv6 en servidor formación - Fichero /etc/network/interface

Pruebas de conectividad

Se comprueba primero conectividad a la puerta de enlace, y luego conectividad hacia Internet con IPv6 utilizando los sitios Google, Facebook, YouTube.

```
kmlapol@formacion:~$ ping6 -c 4 2800:68:7[redacted]eff
PING 2800:68:7[redacted]eff(2800:68:7[redacted]feff) 56 data bytes
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=1 ttl=64 time=0.407 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=2 ttl=64 time=0.978 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=3 ttl=64 time=0.751 ms
64 bytes from 2800:68:7:[redacted]feff: icmp_seq=4 ttl=64 time=0.501 ms

--- 2800:68:7:[redacted]eff ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.407/0.659/0.978/0.223 ms
```

Figura 80: Ping6 desde el servidor formación a la puerta de enlace (gateway).

Conectividad hacia Internet con IPv6

```
kmlapol@formacion:~$ ping6 -c 4 www.google.com
PING www.google.com(atl14s78-in-x04.1e100.net) 56 data bytes
64 bytes from atl14s78-in-x04.1e100.net: icmp_seq=1 ttl=52 time=94.9 ms
64 bytes from atl14s78-in-x04.1e100.net: icmp_seq=2 ttl=52 time=90.7 ms
64 bytes from atl14s78-in-x04.1e100.net: icmp_seq=3 ttl=52 time=90.7 ms
64 bytes from atl14s78-in-x04.1e100.net: icmp_seq=4 ttl=52 time=90.9 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 90.714/91.844/94.982/1.813 ms
```

Figura 82: Prueba del comando ping6 en la Internet con IPv6 (www.google.com) desde el servidor formación

```
kmlapol@formacion:~$ ping6 -c 4 www.facebook.com
PING www.facebook.com(edge-star-mini6-shv-01-mia3.facebook.com) 56 data bytes
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=1 ttl=51 time=71.5 ms
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=2 ttl=51 time=71.5 ms
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=3 ttl=51 time=71.5 ms
64 bytes from edge-star-mini6-shv-01-mia3.facebook.com: icmp_seq=4 ttl=51 time=71.6 ms

--- www.facebook.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 71.518/71.560/71.613/0.330 ms
```

Figura 81: Prueba del comando ping6 en la Internet con IPv6 (www.facebook.com) desde el servidor formación

```
kmlapol@formacion:~$ ping6 -c 4 www.youtube.com
PING www.youtube.com(mia07s49-in-x0e.1e100.net) 56 data bytes
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=1 ttl=52 time=79.2 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=2 ttl=52 time=79.1 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=3 ttl=52 time=79.4 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=4 ttl=52 time=79.4 ms

--- www.youtube.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 79.174/79.330/79.484/0.365 ms
```

Figura 83: Prueba del comando ping6 en la Internet con IPv6 (www.youtube.com) desde el servidor formación

Al hacer las pruebas de verificación con el comando ping6 como indica en las figuras se puede verificar la correcta asignación y configuración de IPv6 en el servidor formación.

6.5.1.4. Servidor Graduados

Luego de haber ingresado al servidor denominado graduados, se procede a realizar la verificación de soporte IPv6, haciendo ping6 a la dirección lookback:

```
kmlapol@graduados:~$ ping6 -c 2 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.028 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.024/0.026/0.028/0.002 ms
```

Figura 84: Comprobar soporte IPv6 en servidor graduados

Agregar dirección IPv6.

Similar al servidor anterior se ingresa al fichero **/etc/network/interface,** y se agrega la dirección IPv6, la máscara y el Gateway.

```
iface eth0 inet static
        address 172.[redacted]
        netmask 255.255.224.0
        network 172.[redacted]
        broadcast 172.[redacted]
        gateway 172.[redacted]
        # dns-* options are implemented by the
        dns-nameservers [redacted]
        dns-search unl.edu.ec

#IPv6

iface eth0 inet6 static
        address 2800:68:7[redacted]d4
        netmask 64
        gateway 2800:68:7[redacted]eff
```

Figura 85: Agregar IPv6 en servidor graduados - Fichero /etc/network/interface

Pruebas de conectividad

Se comprueba primero conectividad a la puerta de enlace, y luego conectividad hacia Internet con IPv6 utilizando los sitios Google, YouTube.

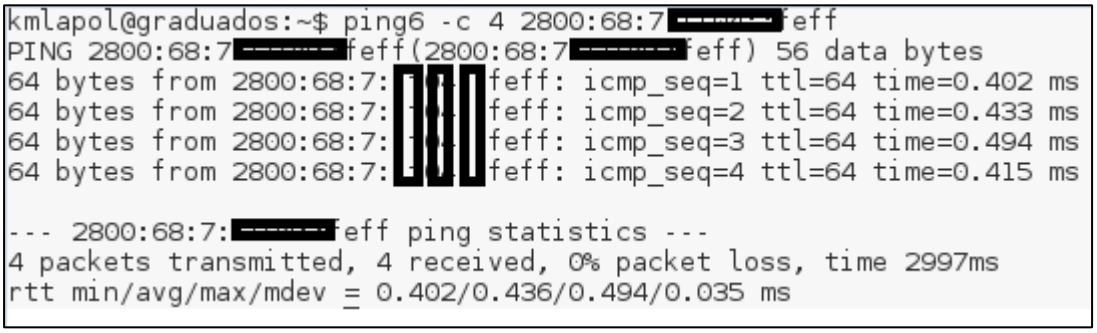


Figura 86: Ping6 desde el servidor graduados a la puerta de enlace (gateway).

Conectividad hacia Internet con IPv6

Para establecer conexión con IPv6 a Internet, se utilizará el dominio y la dirección IPv6 del sitio web.

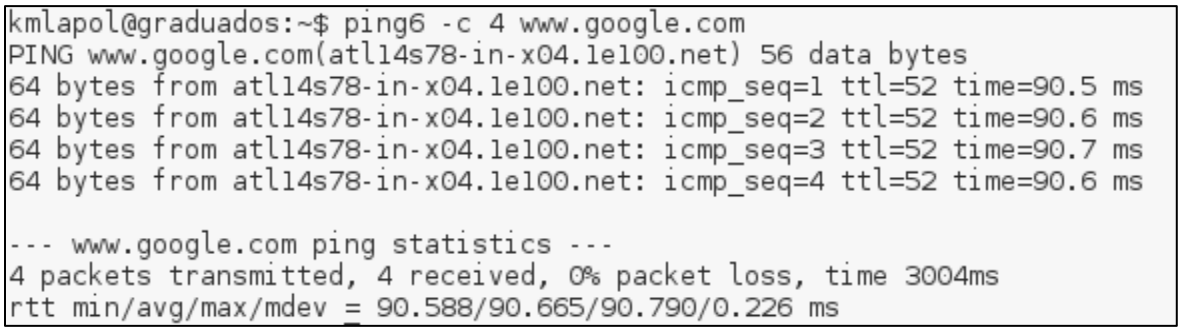


Figura 87: Prueba del comando ping6 en la Internet con IPv6 (www.google.com) desde el servidor graduados

```
kmlapol@graduados:~$ ping6 -c 4 2607:f8b0:4002:808::2004
PING 2607:f8b0:4002:808::2004(2607:f8b0:4002:808::2004) 56 data bytes
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=1 ttl=52 time=90.6 ms
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=2 ttl=52 time=91.0 ms
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=3 ttl=52 time=90.6 ms
64 bytes from 2607:f8b0:4002:808::2004: icmp_seq=4 ttl=52 time=90.9 ms

--- 2607:f8b0:4002:808::2004 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 90.614/90.810/91.037/0.346 ms
```

Figura 88: Prueba del comando ping6 en la Internet con IPv6 de Google desde el servidor graduados

```
kmlapol@graduados:~$ ping6 -c 4 www.youtube.com
PING www.youtube.com(mia07s49-in-x0e.1e100.net) 56 data bytes
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=1 ttl=52 time=79.1 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=2 ttl=52 time=79.2 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=3 ttl=52 time=79.2 ms
64 bytes from mia07s49-in-x0e.1e100.net: icmp_seq=4 ttl=52 time=79.2 ms

--- www.youtube.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 79.144/79.222/79.280/0.348 ms
```

Figura 89: Prueba del comando ping6 en la Internet con IPv6 (www.youtube.com) desde el servidor graduados

```
kmlapol@graduados:~$ ping6 -c 4 2607:f8b0:4008:803::200e
PING 2607:f8b0:4008:803::200e(2607:f8b0:4008:803::200e) 56 data bytes
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=1 ttl=52 time=79.1 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=2 ttl=52 time=79.3 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=3 ttl=52 time=79.2 ms
64 bytes from 2607:f8b0:4008:803::200e: icmp_seq=4 ttl=52 time=79.2 ms

--- 2607:f8b0:4008:803::200e ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 79.188/79.265/79.337/0.287 ms
```

Figura 90: Prueba del comando ping6 en la Internet con IPv6 de YouTube desde el servidor graduados

Las figuras que se acaban de exponer, muestran que al establecer conectividad IPv6, desde el servidor denominado Graduados a Internet esta se genera correctamente, lo que demuestra que la configuración de IPv6 en el servidor público es correcta.

6.5.1.5. Servidor Web (unl.edu.ec)

Al acceder al servidor unl.edu.ec, se procede a realizar la verificación de soporte IPv6, haciendo ping6 a la dirección lookback:

```
kmlapol@www:~$ ping6 -c2 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.031 ms

--- ::1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss,
```

Figura 91: Comprobar soporte IPv6 en servidor unl.edu.ec

Agregar dirección IPv6.

Se ingresa al fichero **/etc/network/interface,** y se agrega la dirección IPv6, la máscara y el Gateway.

```
iface eth0 inet static
        address 172.[redacted]
        netmask 255.255.224.0
        network 172.[redacted]
        broadcast 172.[redacted]
        gateway 172.[redacted]
        # dns-* options are implemented by the
        dns-nameservers [redacted]

#IPv6

iface eth0 inet6 static
        address 2800:68:7[redacted]7d70
        netmask 64
        gateway 2800:68:7[redacted]eff
```

Figura 92: Agregar IPv6 en servidor unl.edu.ec - Fichero /etc/network/interface

Pruebas de conectividad

Se comprueba primero conectividad a la puerta de enlace, al servidor eva y graduados que son dos de los servidores que se acaba de configurar, desde la PC de un usuario y luego conectividad hacia Internet con IPv6 utilizando los sitios Google, YouTube y Facebook.

Figura 93: Ping6 desde el servidor unl.edu.ec a la puerta de enlace (gateway).

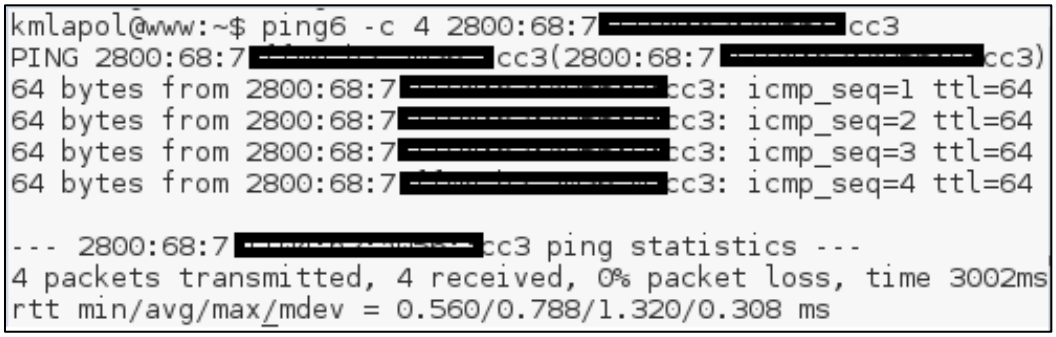


Figura 94: Prueba del comando ping6 desde el servidor unl.edu.ec al servidor eva

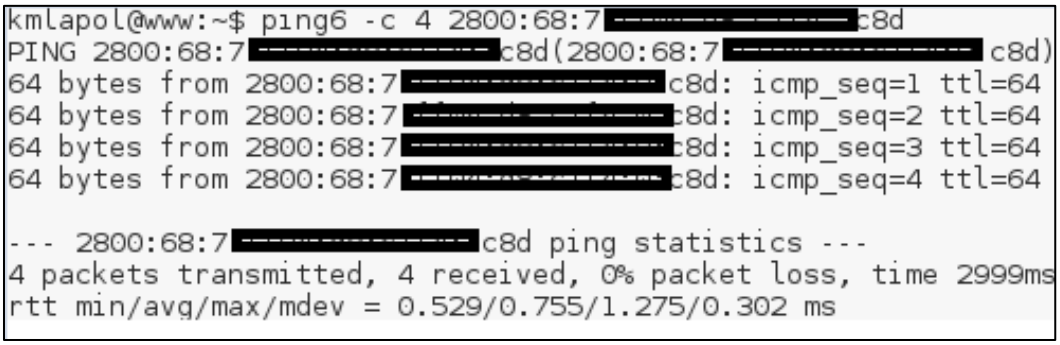


Figura 95: Prueba del comando ping6 desde el servidor unl.edu.ec al servidor formación

Conectividad desde un usuario

Se pudo comprobar la conectividad que existe desde la PC del usuario del Bloque de Administración Central Departamento UTI hacia el servidor unl.edu.ec, puesto que este bloque ya tiene salida con IPv6.

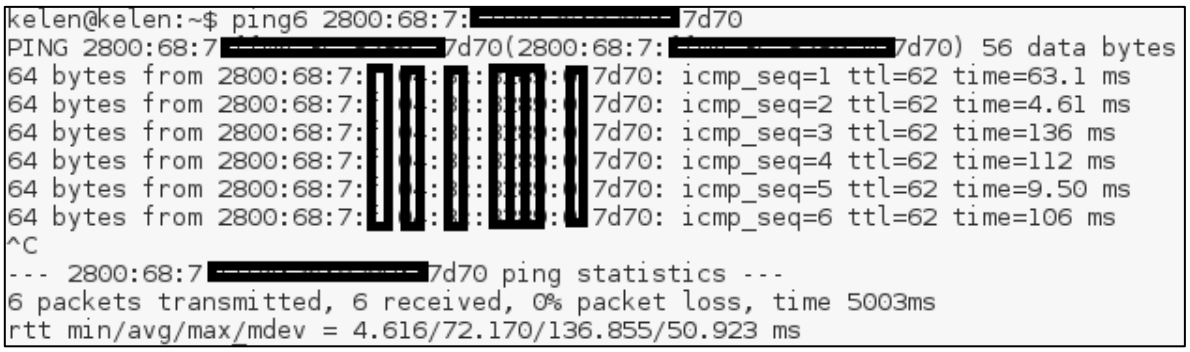


Figura 96: Prueba del comando ping6 desde un usuario (Administración Central) al servidor unl.edu.ec

Conectividad hacia Internet con IPv6

Para establecer conexión con IPv6 a Internet, se utilizará el dominio y la dirección IPv6 del sitio web.

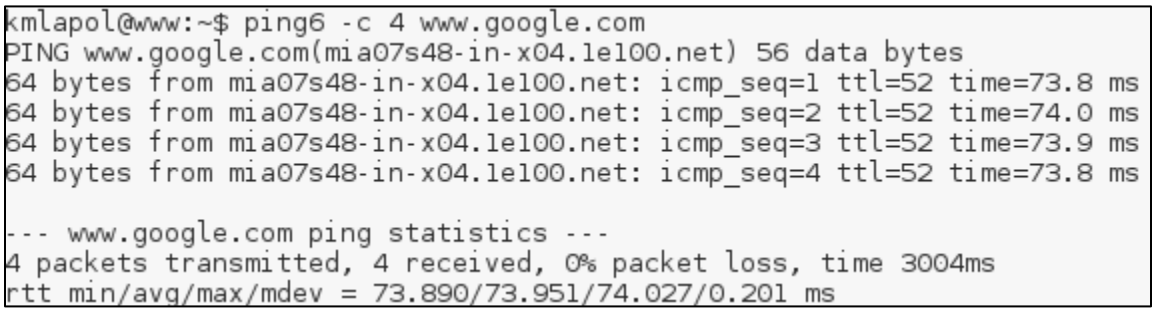


Figura 97: Prueba del comando ping6 en la Internet con IPv6 (www.google.com) desde el servidor unl.edu.ec

```
kmlapol@www:~$ ping6 -c 4 2607:f8b0:4008:803::2004
PING 2607:f8b0:4008:803::2004(2607:f8b0:4008:803::2004) 56 data bytes
64 bytes from 2607:f8b0:4008:803::2004: icmp_seq=1 ttl=52 time=73.8 ms
64 bytes from 2607:f8b0:4008:803::2004: icmp_seq=2 ttl=52 time=73.8 ms
64 bytes from 2607:f8b0:4008:803::2004: icmp_seq=3 ttl=52 time=73.8 ms
64 bytes from 2607:f8b0:4008:803::2004: icmp_seq=4 ttl=52 time=74.5 ms

--- 2607:f8b0:4008:803::2004 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 73.828/74.029/74.530/0.441 ms
```

Figura 98: Prueba del comando ping6 en la Internet con la IPv6 de Google desde el servidor unl.edu.ec

```
kmlapol@www:~$ ping6 -c 4 www.facebook.com
PING www.facebook.com(edge-star-mini6-shv-02-mia3.facebook.com) 56 data bytes
64 bytes from edge-star-mini6-shv-02-mia3.facebook.com: icmp_seq=1 ttl=52 time=66.1 ms
64 bytes from edge-star-mini6-shv-02-mia3.facebook.com: icmp_seq=2 ttl=52 time=66.2 ms
64 bytes from edge-star-mini6-shv-02-mia3.facebook.com: icmp_seq=3 ttl=52 time=66.2 ms
64 bytes from edge-star-mini6-shv-02-mia3.facebook.com: icmp_seq=4 ttl=52 time=66.1 ms

--- www.facebook.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 66.185/66.209/66.236/0.023 ms
```

Figura 99: Prueba del comando ping6 en la Internet con IPv6 (www.facebook.com) desde el servidor unl.edu.ec

```
kmlapol@www:~$ ping6 -c 4 www.youtube.com
PING www.youtube.com(mia07s47-in-x0e.1e100.net) 56 data bytes
64 bytes from mia07s47-in-x0e.1e100.net: icmp_seq=1 ttl=52 time=73.9 ms
64 bytes from mia07s47-in-x0e.1e100.net: icmp_seq=2 ttl=52 time=73.9 ms
64 bytes from mia07s47-in-x0e.1e100.net: icmp_seq=3 ttl=52 time=73.9 ms
64 bytes from mia07s47-in-x0e.1e100.net: icmp_seq=4 ttl=52 time=74.1 ms

--- www.youtube.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 73.925/73.989/74.130/0.083 ms
```

Figura 100: Prueba del comando ping6 en la Internet con IPv6 (www.youtube.com) desde el servidor unl.edu.ec

Al finalizar la configuración de IPv6 en cada uno de los 5 servidores públicos dispuestos por la UTI y luego de haber realizado las respectivas pruebas de verificación de conectividad se puede concluir que se ha configurado correctamente IPv6 en estos dispositivos.

7. DISCUSIÓN

7.2. Evaluación del Objeto de Investigación

El trabajo de titulación **denominado "Despliegue del Protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja"** arroja como resultado final la implementación de IPv6 en los servidores web públicos con los que dispone la institución.

Este trabajo se basa principalmente en el cumplimiento de todos y cada uno de los objetivos específicos, los mismos que fueron abordados tal y como se explica a continuación:

- ✓ **Objetivo Específico 1:** Analizar la situación actual del DNS autoritario y Servidores públicos para la implementación de IPv6.

Para cumplir con este objetivo se realizó una entrevista al subdirector de redes y equipos informáticos de la Unidad de Telecomunicaciones e Información, quien es el encargado de la administrar la red de datos, y por su intermedio se logró conseguir información veraz a cerca del objetivo planteado y con ello tener un conocimiento de la infraestructura de red (backbone), los servicios, tecnología empleada; Entre la información obtenida destaca las características del DNS autoritario y de los servidores públicos como lo es: capacidad de recursos, Sistema Operativo (S.O), aplicaciones, dominio web y la funcionalidad que desempeña cada uno de ellos. El S.O representa una de las características más importantes puesto que a través de las distribuciones se pudo determinar si los servidores soportan el protocolo versión 6, determinando que en su mayoría los servidores utilizan distribuciones Gnu/Linux Centos desde la versión 5 y superior y Debian desde la versión 6 y superior con lo que se confirma el soporte de IPv6, además pude conocer que los servidores públicos se encuentran en la DMZ (Zona desmilitarizada) y virtualizados en el BLADE.

- ✓ **Objetivo Específico 2:** Determinar el mecanismo de transición a utilizar entre IPv4 e IPv6.

Este objetivo fue resuelto en base a tres fases:

→ **Revisión Literaria**

En esta fase se revisó en diferentes fuentes de investigación como lo es tesis, artículos científicos, revistas indexadas, foros, etc. información relacionada a los mecanismos de transición entre IPv4 e IPv6 y con ello poder obtener los más utilizados y aquellos que permitan la coexistencia de ambas versiones del Protocolo de Internet dando como resultado los mecanismo: Doble Pila (Dual Stack), Túneles (Tunneling) y Traducción.

→ **Comparativa y Evaluación de los Mecanismos de Transición**

Al definir que los mecanismos de transición Doble Pila, Túneles y Traducción son los que serán evaluados para determinar el que esté más acorde para ser implementado en la red de datos de la UNL específicamente en el DNS autoritativo y servidores públicos, se optó por realizar un cuadro resumen donde se destaca las características, ventajas y desventajas de cada mecanismo, así como también se estableció parámetros tales como escalabilidad, configuración, compatibilidad hardware, compatibilidad software, seguridad, interoperabilidad, movilidad, desempeño, aplicabilidad y usabilidad, características importantes que fueron consideradas para marcar la diferencia entre uno y otro mecanismo, todo esto se logró asignando ciertos criterios de evaluación con una respectiva valoración que en números nos arrojó que Doble Pila con un 96% de su análisis es la técnica de transición y coexistencia propicia para ser aplicada en el proyecto.

→ **Casos de Estudio**

En esta fase se investigó casos de éxito, por parte de las Instituciones de Educación Superior que han propuesto un plan de implementación o han implementado IPv6, utilizando el mecanismo de transición Doble Pila, esto permitió conocer más a fondo el funcionamiento y despliegue de este mecanismo en base a la experiencia de estas Entidades, lo que certifica aún más que la técnica de transición apta para la coexistencia de los dos protocolos es Dual Stack.

- ✓ **Objetivo Específico 3: Diseñar el esquema de direccionamiento para la red pública de la Universidad Nacional de Loja.**

Para dar culminado este objetivo se trabajó conjuntamente con los Técnicos de la UTI y basándose en el direccionamiento jerárquico que considera a las Facultades Académico-Administrativas se empezó por subnetear el prefijo IPv6 asignado a la UNL correspondiente a 2800:68:7::/48, con el que a su vez cada Facultad obtenía un prefijo /56. Al centrarme en el direccionamiento para el DNS autoritativo y servidores públicos propuse un mecanismo que consiste en concatenar la dirección asignada a la DMZ, con los últimos 24 bits de la dirección local de enlace del servidor, más los últimos 16 bits de la dirección IPv4 convertida a hexadecimal; está técnica fue aceptada por los Técnicos de la Unidad y consensuada con el director del trabajo de titulación, con lo que quedó definido un /64 para cada servidor. Y la cual es explicada con más detalle en la sección 6.3.3.1utilizando el prefijo de documentación para una mejor comprensión.

- ✓ **Objetivo Específico 4: Establecer un escenario de pruebas de acuerdo al mecanismo de transición seleccionado.**

Para efectuar este objetivo se lo hizo en un escenario basado en equipos físicos otorgados por la UTI, tal es el caso de los equipos que sirvieron para configurar las aplicaciones necesarias para que funcione el servidor DNS y el servidor Web que representa a los servidores públicos de la institución, en estos equipos se configuró IPv6 como si de la implementación real se tratara, el motivo era que las pruebas funcionaran los más real posible, utilizando para ello los archivos de configuración y direcciones IPv4 propios del servidor DNS autoritativo y del servidor web que se encuentran en producción, así como también haciendo uso del direccionamiento IPv6 obtenido en el objetivo 3 (Sección 6.3.3.), referente al DNS y a los servidores públicos. Todo esto se lo hizo con el objeto de que la implementación sea una especie de réplica de las pruebas efectuadas.

- ✓ **Objetivo Específico 5: Realizar las configuraciones necesarias para la implementación de IPv6 en el DNS autoritario y Servidores públicos de la Universidad Nacional de Loja.**

Para realizar las configuraciones de IPv6 en cada uno de los servidores públicos se me otorgó un usuario y contraseña con los que se tenía acceso a los servidores mediante el protocolo SSH y la infraestructura de clave pública (pki), todo esto fue desarrollado bajo la supervisión del Subdirector de Redes y Equipos Informáticos de la UTI. Con estas configuraciones los servidores públicos quedan funcionando con ambas versiones de IP (IPv4 e IPv6).

La implementación de IPv6 en el DNS autoritario y como se explicó anteriormente en la sección 6.5.1 será realizada por la UTI, basándose en el manual técnico que se elaboró y fue revisado y aprobado por el Subdirector de Redes y Equipos Informáticos (ver Anexo V); En el manual se detalla paso a paso mediante imágenes el procedimiento a seguir para la configuración del servicio DNS, así como también se especifica las directivas y ficheros de configuración a ser modificados para su correcto funcionamiento.

7.3. Valoración Técnico – Económica – Ambiental

La ejecución de este proyecto contribuye enormemente al desarrollo tecnológico de la Universidad Nacional de Loja, puesto que la implementación de nuevas tecnologías como lo es el Protocolo IPv6, permite a la Institución contar con mayor velocidad y seguridad dentro de la Red de Datos, así como también le da la posibilidad de ser un referente en el despliegue de IPv6. Técnicamente es un Proyecto factible, debido a que la UNL cuenta con los equipos informáticos (servidores) necesarios para realizar tanto las pruebas como la implementación, por lo que solo se necesitó de ciertas aplicaciones y configuraciones para poner en ejecución IPv6, lo cual también es favorable en el aspecto ambiental puesto que no provoca ninguna alteración negativa para el medio ambiente. Económicamente este trabajo no acarrea muchos gastos, por cuanto las aplicaciones utilizadas son libres y gratuitas que facilitan aún más la Implementación de IPv6.

Para la realización del presente trabajo de titulación se contó con los recursos humanos, económicos y tecnológicos como hardware y software, necesarios para su culminación, los cuales se detallan a continuación:

Recursos Humanos

Recurso Humano	Cantidad	Horas	V. Unitario	V. Total	Nota
Investigadora	1	400	6,00	2,400	
Director de Tesis	1	150	10,00	1500,00	El costo del tutor lo asumirá la Universidad Nacional de Loja
			Subtotal	**2,400**	

Recursos Materiales

Descripción	Unidad	Cantidad	Costo Unitario	Subtotal
Internet/	Hora	850	0.50	400,00
Transporte	--	--	60.00	60.00
Impresiones	Unidad	400	0.05	20.00
Empastados	Unidad	3	15.00	45.00
Anillados	Unidad	3	3.00	9.00
CDs	Unidad	3	1.00	3.00
Copias		400	0.02	8.00

Refrigerio	Unidad	90	2.00	180.00
			Total	**725.00**

Recursos Técnicos/Tecnológicos

Descripción	Unidad	Cantidad	Costo Unitario	Subtotal
Memoria 8GB Kingston	Hora	1	8.00	8.00
Computador portátil Dell core i7	Unidad	1	1330.00	1330.00
Paquete de Ofimática Microsoft	Unidad	1	250.00	250.00
Sistema Operativo GNU Linux	Unidad	2	0.00	0.00
Software Libre para servicios de Internet	Unidad	8	0.00	0.00
Telefonía Celular	Unidad	--	40.00	40.00
			Total	**1628.00**

Imprevistos

Para la tasa de imprevistos se consideró el 10% de la suma total de recurso humano, material y técnico/tecnológico.

	Porcentaje costo directo	V. Total
Imprevistos (Recurso humano + materiales + técnicos)	10%	684.62
	Subtotal	**684.62**

Total de recursos

Descripción	V. Total
Recurso humano	2400.00
Recurso Material	725.00
Recurso Técnico/Tecnológico	1628.00
Imprevistos	475.30
Total	**5228,00**

8. CONCLUSIONES

En base a los resultados obtenidos durante el desarrollo y finalización del proyecto se puede concluir lo siguiente:

- El uso de las técnicas de investigación como la: bibliografía, entrevista, y observación permitieron obtener información relacionada a la infraestructura de la red, específicamente de los servidores públicos, conociendo las características software de los mismos y determinando que estos soportan IPv6, lo que facilita la configuración, implementación e integración de esta nueva tecnología.

- La mejor solución para la implementación de IPv6 es la transición, puesto que el cambio de IPv4 a IPv6 requiere de integración y evolución que permita un crecimiento escalable y simple de la Red, descartando la migración a IPv6 ya que esta requiere utilizar en algún equipo de borde alguna técnica para poder hacer la traducción.

- En base a mi investigación realizada sobre los mecanismos de coexistencia entre IPv4 e IPv6 (Doble Pila, Túneles y Traducción), se determinó que Doble Pila es el más apropiado para ser utilizado en el despliegue de IPv6 en la UNL, ya que permite a servidores, clientes y aplicaciones moverse gradualmente hacia el nuevo protocolo provocando un mínimo impacto durante el proceso de transición.

- El mecanismo que he propuesto en este TT para la asignación de direcciones IPv6 en los servidores públicos, lo desarrollé en base al grado de seguridad que implica utilizar una dirección IP sobre estos dispositivos, manteniendo la seguridad de la red y salvaguardando la información que posee un alto grado de criticidad para la Institución.

- En las pruebas establecidas en los servicios DNS y Web se visualizó el correcto funcionamiento de IPv4 e IPv6 con el mecanismo de transición seleccionado y configurado, lo cual es un indicador de que la implementación de IPv6 cumple con los objetivos planteados.

- Durante los próximos años IPv6 irá tomando mayor relevancia en Internet, por lo que el desarrollo de este proyecto permite a los servidores públicos con los que cuenta la UNL, estar preparados para las futuras necesidades de los usuarios sobre redes IPv6.

9. RECOMENDACIONES

Se recomienda:

- A las Instituciones públicas y privadas, establecer un plan de transición de IPv4 a IPv6 considerando el problema del agotamiento de direcciones IPv4, utilizando el mecanismo de Doble Pila, en vista que esta alternativa permite mantener la misma infraestructura, servicios y aplicaciones sin crear mayor impacto para los usuarios.

- El presente trabajo de titulación conjuntamente con el trabajo "Despliegue del Protocolo de Internet versión 6 (IPv6) para los dispositivos Core y Switchs de distribución en la red de datos de la Universidad Nacional de Loja" para que la implementación de IPv6 se realice en toda la infraestructura de red, y la comunidad universitaria pueda tener acceso tanto desde la Intranet como hacia Internet utilizando las dos versiones del Protocolo de Internet.

- Utilizar el mecanismo de asignación de direcciones IPv6 propuesto en este TT, en los servidores tanto públicos y privados de una Institución, ya que se ha elaborado la respectiva documentación, además el mismo ha sido implementado y probado en la UNL.

- A la Unidad de Telecomunicaciones e Información y a la Carrera de Ingeniería en Sistemas organizar conferencias que permitan una mayor difusión del Protocolo de Internet versión 6, para que estudiantes, docentes y personas interesadas en la investigación de este protocolo puedan participar y conocer de los proyectos afines que se ha realizado en la UNL.

- Realizar un estudio de herramientas de software que permitan monitorear el tráfico IPv6 en la red de datos, estado de servicios, estado de aplicaciones y obtener estadísticas de la utilización de IPv6 en los servicios de Internet públicos por parte de los usuarios finales, y determinar la que mejor se asemeje a estos requerimientos y poder utilizar en la UNL, una vez que se haya desplegado por completo IPv6.

- Realizar nuevos estudios referentes al protocolo de nueva generación IPv6, en áreas como: seguridad, video conferencia, telefonía IP, Movilidad, Internet de las Cosas (IoT), etc. y con ello aprovechar las ventajas que IPv6 aporta.

10. BIBLIOGRAFÍA

[1] "Protocolo de Internet versión 6". [En línea]. Disponible en: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6.[Accedido: 04-dic-2016].

[2] R. Llanos., *Plan de migración de IPv4 a IPv6 para una red de un proveedor de servicios de internet (ISP),* vol.12, No.36,

[3] D., Clark., *Rethinking the design of the Internet: The end to end arguments vs. the brave new world*, ACM Transactions on Internet Technology, Vol 1, No 1., 2001.

[4] Deering, S., & Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification.I In IETF (The Internet Engineering Task Force)* Request for Comments 2460

[5] IETF, « Internet Protocol,» RFC 791, 1993.

[6] G. Cicilio, et al. *IPv6 para todos*, 1a ed. Buenos Aires, Argentina, 2009, ISBN 978-987-25392-1-4.

[7] S. Hagen., *IPv6 Essentials*. 2da. ed. Estados Unidos. O´ Really.

[8] "Ventajas de IPv6 frente a IPv4-Redes locales y globales". [En línea]. Disponible en: https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/1-ventajas-de-ipv6-frente-a-ipv4. [Accedido: 04-dic-2016].

[9] "Fundamentos de IPV6", [En línea]. Disponible en: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

[10] J. Davies, *Understanding IPv6*, 3ra ed. Estados Unidos: Microsoft Corporation, 2012, ISBN: 978-0-7356-5914-8.

[11] Y. Mun and K.Lee, *Understanding IPv6*, New York: Springer, 2005, ISBN 0-387-25429-3

[12] Ariganello, E., and E. B. Sevilla, *Redes CISCO: Guía de estudio para la certificación CCNP*. México: Alfaomega, 2011.

[13] J. C. Alonso, «Introducción a IPv6,» 2012. [En línea]. Disponible en: http://www.labs.lacnic.net/site/sites/default/files/02-IPv6Introduccion-Agotamiento-Transicion.pdf. [Último acceso: 20 Diciembre 2016].

[14] «"Direccionamiento IPv6",» [En línea]. Disponible en: http://www.labs.lacnic.net/site/sites/default/files/001-Direccionamiento%20y%20Protocolo%20IPv6.pdf

[15] A. Acosta, et al. IPv6 para operadores de Red, 1a ed. Buenos Aires, Argentina, 2014, ISBN 978-987-45725-0-9

[16] «IANA,» 4 Enero 2017. [En línea]. Disponible en: https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml. [Último acceso: 10 Marzo 2017].

[17] IETF, «Internet Protocol Version 6 (IPv6) Addressing Architecture,» RFC 3513, 2003.

[18] F. Contreras, «Guía para el aseguramiento del protocolo IPv6. Seguridad y Privacidad de la Información,» Mintic, Colombia, 2015.

[19] «LACNIC,» [En línea]. Disponible en: http://portalipv6.lacnic.net/que-es/. [Último acceso: 12 Marzo 2017].

[20] IETF, « Host Anycasting Service,» RFC 1546, 1993.

[21] J. Palet, Consulintel. [En línea]. Disponible en: http://www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf. [Último acceso: 13 Enero 2017].

[22] S. Frankel, R. Graveman, P. Jhon y R. Mark, «Guidelines for the Secure Deployment of IPv6,» USA, 2010.

[23] NIC MX, IPv6 Mx. [En línea]. Disponible en: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6#. [Último acceso: 28 Abril 2017].

[24] Global Unicast Address. [En línea]. Disponible: https://www.quora.com/What-is-the-range-of-global-unicast-address-in-ipv6

[25] IETF, «IP Version 6 Addressing Architecture,» RFC 1884.

[26] López, D., Gelvez, N., & Pedraza, L. (2010). *Modelo para la integración de redes IPv4-IPv6 basado en túneles*. Bogotá, Colombia.

[27] Kalwar, S. et al. (2015). *A Survey of Transition Mechanisms from IPv4 to IPv6 – Simulated Test Bed and Analysis*.

[28] J. Palet, «Comparativa entre mecanismo de Transición IPv6,» de *FLIP6-Foro Latino Americano de IPv6*, La Habana, 2016.

[29] LACNIC, «Políticas para la Distribución y Asignación de Direcciones IPv6,» 2017.

[30] G. Martin, " Diseño de Escenarios de Transición a IPv6 utilizando la herramienta VMX: DNS, Servicios Web y Mecanismos de Transición", Tesis Maestría, Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros de Telecomunicación, 2011.

[31] C. Mateu, «Desarrollo de Aplicaciones Web,» [En línea]. Disponible en: http://libros.metabiblioteca.org/bitstream/001/591/1/004%20Desarrollo%20de%20aplicaciones%20web.pdf

[32] W3Techs, «World Wide Web Technology Surveys,» [En línea]. Disponible en: https://w3techs.com/. [Último acceso: 13 Enero 2017].

[33] «NGINX,» [En línea]. Available: https://nginx.org/en/. [Último acceso: 15 Enero 2017].

[34] «Servidor web Nginx, una clara alternativa a Apache» [En línea]. Disponible en: https://www.acens.com/wp-content/images/2013/09/servidor-web-nginx-white-paper-acens.pdf. [Último acceso: 15 Enero 2017].

[35] EcuaRed, «Ecuared,» [En línea]. Available: Servidor web https://www.ecured.cu/Servidor_Web. [Último acceso: 15 Enero 2017].

[36] «Principales características de Apache,» [En línea]. Disponible en: https://es.opensuse.org/Apache. [Último acceso: 15 Enero 2017].

[37] E. N. Talón, «Apache,» [En línea]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/Apache.pdf. [Último acceso: 15 Enero 2017].

[38] G. Moreno y C. Orozco, «Universidad Nacional de Chimborazo,» 2011. [En línea]. Disponible: http://dspace.unach.edu.ec/bitstream/51000/3119/1/UNACH-ING-ELC-TEL-2016-0035.pdf. [Último acceso: 15 Mayo 2017].

[39] D. Landy, «Universidad Politécnica Salesiana Sede Cuenca,» 2013. [En línea]. Disponible: http://dspace.ups.edu.ec/bitstream/123456789/5332/1/UPS-CT002767.pdf. [Último acceso: 16 Mayo 2017].

[40] M. Cabrera. «Escuela Superior Politécnica de Chimborazo,» 2009. [En línea]. Disponible: http://dspace.espoch.edu.ec/bitstream/123456789/169/1/38T00160.pdf [Último acceso: 16 Mayo 2017].

[41] RED DE INVESTIGACIÓN DE TECNOLOGÍA AVANZADA, «Servidor DNS BIND con soporte para IPv6». [En línea]. Disponible: http://studylib.es/doc/5958780/servidor-dns-bind-con-soporte-para-ipv6

[42] C. Liu, DNS & BIND on IPv6, USA: O'REILLY, 2011.

[43] R. Aitchison, Pro DNS and BIND 10, USA: Apress, 2011.

11. ANEXOS

ANEXO I: ENTREVISTA REALIZADA AL SUBDIRECTOR DE REDES Y EQUIPOS INFORMÁTICOS DE LA UNL

Entrevista realizada para la elaboración del Trabajo de Titulación correspondiente a desarrollar el proyecto: **"Despliegue del Protocolo de Internet Versión 6 (IPv6) en el DNS autoritario y servidores públicos en la red de datos de la Universidad Nacional de Loja"**.

Nombre: Ing. Jhon Calderón.
Institución en la que labora: Universidad Nacional de Loja.
Cargo: Subdirector de Redes y Equipos Informáticos.
Fecha de Entrevista: 04 de enero de 2016.
Objetivo: Obtener los diferentes tipos de problemas que pueden surgir al no implementar el Protocolo de Internet Versión 6 (IPv6) en la red de datos de la Universidad Nacional de Loja.

Algunos inconvenientes que se visualizan a futuro y que pueden ocurrir si se continúa utilizando direccionamiento IPv4 es el agotamiento de direcciones IPv4 Públicas, como Universidad y como ente académico no podemos hacernos a oídos sordos, por lo que debemos adaptarnos a las nuevas tecnologías y una de ellas es IPv6; de no hacerlo, no podríamos acceder a sitios de internet que tengan habilitado solo para IPv6 en vista de que los protocolos IPv4 e IPv6 no son compatibles

Es importante el despliegue de IPv6 en la Universidad Nacional de Loja porque al tener instalado IPv6 nos va a permitir como Universidad innovar en nuevos proyecto de investigación en áreas como: seguridad, temas de video conferencia, telefonía IP, entre otros.

Al tener implementado IPv6 se eliminaría la técnica que se denomina NAT (Traducción de Direcciones de Red) que utiliza IPv4; se podría tener conexiones punto a punto (end to end) con cualquier equipo en todo el mundo, pero se debería tomar medidas de seguridad al implementar IPv6 ya que algún atacante podría hacer un ingreso directamente a mi computador.

Los beneficios que ofrecerá IPv6 en el caso que se diera su implementación se basa en todos nuestros servicios institucionales (servicios públicos) sean accesibles tanto en el protocolo IPv4 e IPv6, por ejemplo si ahora mismo hay una red en cualquier parte del mundo que solo tenga implementado IPv6 y quiere acceder a nuestra página no lo podría hacer por incompatibilidad de protocolos o si quiere comunicarse lo podría hacer utilizando alguna técnica como NAT64 o túneles.

Esto queda por analizar, ya que se dice que en IPv6 la latencia es menor pero se debería realizar las pruebas necesarias para comprobarlo, lo podría ser en la actualidad porque el tráfico de internet un 90% está por IPv4 aunque el tráfico por IPv6 está en aumento datos estadísticos del 2015 afirman q están en un 10% y al no implementar IPv6 nos podríamos

estar quedando aislados de la red, pero recaería la responsabilidad en las personas que están al frente del departamento de telecomunicaciones de las universidades.

Se considera que es favorable y para iniciar hacer una transición entre los dos protocolos, es decir, que los dos protocolos estén funcionando en todos los equipos de red y servidores. En la transición de doble pila se analizaría la demanda de usuarios y ver la carga en los equipos, es decir son dos protocolos que van a estar implementados, por ende hay que tener en cuenta mayor consumo de memoria porque las peticiones serían a los dos protocolos.

La Migración a IPv6 no se tomaría en cuenta porque tocaría utilizar en algún equipo de borde alguna técnica para poder hacer la traducción.

Los dispositivos de red y los servidores con los que cuenta la Universidad Nacional de Loja soportan IPv6, el 90% si soportan IPv6 por ejemplo en servidores Debian y Centos desde varios años ya soporta IPv6, actualmente en la Universidad Nacional de Loja se está trabajando con un equipamiento CISCO y también soporta IPv6.

Los servicios de internet como Apache ya soportan IPv6 conjuntamente con el DNS, DHCP, FTP.

En la actualidad al no implementar IPv6 una de las causas sería el desconocimiento de las personas que están al frente de las redes, o tal vez porque no le ven algún beneficio o está funcionando todo bien en IPv4.

No hay que esperar a que los equipos, servicios sean accesibles a esta nueva tecnología o que tengamos algún inconveniente para recién ahí tomar medidas sino más bien ir innovando conforme avanza la tecnología.

NOTA: los datos proporcionados se utilizarán únicamente con fines académicos y en particular para la tesis denominada: **"Despliegue del Protocolo de Internet Versión 6 (IPv6) para el DNS autoritario y servidores públicos en la red de datos de la Universidad Nacional de Loja"**

Ing. Jhon Calderón
Subdirector de Redes y Equipos Informáticos.

ANEXO II: COMANDOS ÚTILES EN IPV6

- **Mostrar una dirección IPv6**

Para mostrar una dirección IPv6 se digita uno de los siguientes comandos:

```
# ip -6 addr show dev eth0
# ip -6 addr show eth0 | grep inet6
# ifconfig eth0 | grep inet6
```

- **Añadir una dirección IPv6**

```
# ip -6 addr add 2800:68:7:ff01:54:8dd9:2:7db3/64 dev eth0
# ifconfig eth0 inet6 add 2800:68:7:ff01:54:8dd9:2:7db3/64
# ip addr add 2800:68:7:ff01:54:8dd9:2:7db3/64 dev eth0
# ifconfig eth0 add 2800:68:7:ff01:54:8dd9:2:7db3/64
```

- **Añadir una ruta IPv6 a través de un gateway**

Se lo puede hacer mediante el uso de **ip o route** como indica:

```
# ip -6 route add 2800::/3 via 2800:68:7:ff01::ffff/64 dev eth0
# route -A inet6 add 2800::/3 gw 2800:68:7:ff01::ffff/64 dev eth0
# ip route add 2800::/3 via 2800:68:7:ff01::ffff/64
# route -A inet6 add 2800::/3 gw 2800:68:7:ff01::ffff/64
```

- **Eliminar una dirección IPv6 o una ruta IPv6 a través de un Gateway**

```
# ip -6 route del 2800::/3 via 2800:68:7:ff01::ffff/64 dev eth0
# route -A inet6 del 2800::/3 gw 2800:68:7:ff01::ffff/64 dev eth0
# ip route del 2800::/3 via 2800:68:7:ff01::ffff/64
# route -A inet6 del 2800::/3 gw 2800:68:7:ff01::ffff/64
```

- **Mostrar una ruta IPv6**

```
# ip -6 route show dev eth0
# route -A inet6 | grep -w “eth0”
```

ANEXO III: ACTA DE EXPOSICIÓN DE AVANCES DEL PROYECTO

UNL UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Acta de Reunión No. 035-UTI-2016

Asunto:	Exposición del proyecto de titulación: Despliegue del protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja		
Inicio:	16:30	**Duración:**	17:30
Convocado por:	Ing. Jhon Calderón	**Fecha:**	14/12/2016

AGENDA

- Ostentación de los resultados del Despliegue del protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja ante las partes interesadas.

OBSERVACIONES/RECOMENDACIONES

- Explicar la técnica de obtener las direcciones IPv6 para los servidores con el prefijo de documentación IPv6.
- Utilizar los mismos nombres de dominio para resolución directa e inversa tanto en Ipv4 e IPv6.
- Se requiere automatizar en una hoja de cálculo de Google (G-Suite) la generación de direcciones IPv6.
- Agregar descripciones más funcionales y menos técnicas en los títulos de las transparencias.

ASISTENTES:

Ing. Hernan Torres
COORDINADOR CIS

Ing. Milton Labanda
DIRECTOR UTI

Kelen Lapo
TESISTA

Ing. Rodrigo Japón
FUNCIONARIO UTI

Ing. Juan Pablo Ramón
FUNCIONARIO UTI

Ing. Jhon Calderón
SUBDIRECTOR R.E.I.

ANEXO IV: CERTIFICACIÓN DE CULMINACIÓN DEL PROYECTO

UNL
UNIVERSIDAD NACIONAL DE LOJA

Unidad de Telecomunicaciones e Información

Jhon Alexander Calderón Sanmartín

DIRECTOR DE LA UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN

Certifica

Que la señorita **Kelen Mireya Lapo Lapo** con cédula de ciudadanía número **1105310526,** egresada de la Carrera de Ingeniería en Sistemas, ha finalizado la ejecución práctica de su proyecto de titulación denominado **"Despliegue del protocolo de Internet versión 6 (IPv6) para el DNS autoritario y Servidores públicos en la red de datos de la Universidad Nacional de Loja"** en la Unidad de Telecomunicaciones de Información, bajo los lineamientos y requerimientos establecidos por esta unidad administrativa de la Universidad Nacional de Loja.

En vista que el DNS autoritario es un servicio crítico, la Unidad de Telecomunicaciones e Información realizará la implementación del protocolo IPv6 en el servicio DNS que actualmente se encuentra en producción.

Es cuanto puedo indicar en honor a la verdad, facultando al interesado hacer uso del presente documento.

Loja, 10 de Octubre del 2017.

Jhon Alexander Calderón Sanmartín
DIRECTOR DE TELECOMUNICACIONES E INFORMACIÓN

Ciudad Universitaria "Guillermo Falconí Espinosa", La Argelia, Loja - Ecuador
Teléfonos: 07 2547252 Ext.: 126, Email: direccion.uti@unl.edu.ec, Web: http://www.unl.edu.ec

ANEXO V: MANUAL TÉCNICO DE CONFIGURACIÓN DEL SERVIDOR DNS Y WEB DE LA UNL.

Despliegue del Protocolo de Internet versión 6 (IPv6) en servidor DNS y Web

Manual del administrador

Versión 1.0

DATOS GENERALES	
Código:	001
Versión:	1.0
Fecha de la versión:	26 de Junio de 2017
Páginas:	
Creado por:	Kelen Mireya Lapo Lapo
Revisado por:	Ing. Jhon Calderón
Nivel de confidencialidad:	Alto

CONTROL DE VERSIONES			
Código	**Versión**	**Fecha**	**Responsable**
001	1.0	26 de Junio de 2017	Kelen Mireya Lapo Lapo

CONTROL DE MODIFICACIONES				
Código	**Versión**	**Fecha**	**Responsable**	**Descripción**
001	1.0	26 de Junio de 2017	Kelen Mireya Lapo Lapo	

FIRMAS DE RESPONSABILIDAD			
Descripción	**Nombres y Apellidos**	**Cargo**	**Firma**
Creado por:	Kelen Mireya Lapo Lapo	Egresada de la Carrera de Ingeniería en Sistemas	
Revisado por:	Ing. Jhon Calderón	Subdirector de Telecomunicación e Información	

1. INTRODUCCIÓN

En el presente manual se detalla las configuraciones necesarias para desplegar el Protocolo de Internet versión 6 (IPv6) en el DNS autoritario y servidores públicos usando como mecanismo de transición doble-pila (IPv4 e IPv6), esto con el objetivo de ofrecer al usuario final una nueva alternativa de conexión con las características y ventajas que el nuevo protocolo de internet ofrece.

Para el correcto y rápido despliegue de IPv6 se requiere que el administrador de la Red de Datos, tenga conocimientos básicos del protocolo TCP/IP, servicios y de distribuciones Gnu / Linux, este último debido a que en el área de servidores se utilizan las distribuciones Centos y Debian.

2. DIRIGIDO A ADMINISTRADORES

El manual está dirigido a los administradores de redes del Departamento de Telecomunicaciones e Información (UTI), en él se define el proceso para el despliegue del Protocolo de Internet versión 6 en el DNS autoritario y servidores públicos.

3. OBJETIVO

Configurar el protocolo de Internet versión 6 (IPV6) en el DNS y Servidor Web de la Universidad Nacional de Loja.

4. PROCEDIMIENTO DE INSTALACIÓN Y CONFIGURACIÓN DE LOS SERVICIOS DE INTERNET (DNS Y WEB)

El manual fue elaborado para la Unidad de Telecomunicaciones e Información utilizando direcciones IP reales , pero para su respectiva documentación y vista pública se utilizará el prefijo de documentación.

CONFIGURACIONES PREVIAS

- **Comprobar soporte IPv6 en GNU/Linux**

  Antes de empezar a utilizar IPv6 en un servidor Linux, es necesario verificar si nuestra distribución tiene soporte para IPv6, para ello abrimos el terminal y escribimos **ping6 -c5 ::1** si el resultado es el siguiente:

```
kelen@kelen:~$ ping6 -c5 ::1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.046 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from ::1: icmp_seq=4 ttl=64 time=0.050 ms
64 bytes from ::1: icmp_seq=5 ttl=64 time=0.057 ms

--- ::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.046/0.051/0.057/0.006 ms
```

  Significa que nuestro GNU/Linux ya se encuentra disponible para soportar IPv6, si no se debe activar IPv6 en nuestro equipo, para lo cual verificamos que tenemos soporte en el kernel que estamos corriendo usando el siguiente comando condicional en el shell:

  $ [-f /proc/net/if_inet6] && echo 'El kernel está disponible para IPv6!' || echo 'No existe soporte IPv6! Compile the kernel!!'

```
kelen@kelen:~$ [ -f /proc/net/if_inet6 ] && echo 'El kernel está disponible para IPv6!' || echo
 'No existe soporte IPv6! Compile the kernel!!'
El kernel está disponible para IPv6!
```

  Si lo ejecutado anteriormente falla, esto implica que el módulo IPv6 no está cargado en el sistema Linux. Entonces lo que se debe hacer es ingresar con privilegios de usuario root y tipear el siguiente comando:

  # **modprobe ipv6**

  Comprobamos si el kernel fue cargado para ello digitamos:

  lsmod | grep -w 'ipv6' && echo "El módulo fue cargado"

  y finalmente se vuelve a hacer ping6 -c5 ::1, con lo que se comprueba que nuestro equipo ya dispone de soporte IPv6

CONFIGURACIÓN DE LA DIRECCIÓN IPV6 EN SERVIDORES

Se debe mencionar que en los servidores se va a realizar asignación estática por lo que a continuación se explica el procedimiento para dicha asignación.

- **Configurar la dirección IPv6 en el sistema operativo Debian (Dual-Stack)**
  Para configurar una dirección IPv6 en el sistema Debian se debe editar el fichero **/etc/network/interfaces** y añadir una nueva definición de interfaz la family **inet6**, para lo cual ingresamos en consola:

nano /etc/network/interfaces

```
iface eth0 inet static
        address 10.10.58.252
        netmask 255.255.255.0
        gateway 10.10.58.1

iface eth0 inet6 static
        address 2800:68:7:f::4
        netmask 64
        gateway 2800:68:7:f::ffff
```

Donde:

- En la directiva address se va a asignar la dirección IPv6 a configurar en el equipo.
- netmask: corresponde a la máscara de red (en el caso de IPv6 un barra 64)
- gateway: la puerta de enlace IPv6

Nota: *La configuración realizada anteriormente corresponde a la asignación estática de una dirección IP mediante doble pila (Dual stack).*

A continuación reiniciamos la interfaz de red [eth0] para que se puedan fijar los cambios realizados:

invoke-rc.d networking restart

- **Activar dirección IPv6 en el Sistema Operativo Centos.**

  En el fichero **/etc/sysconfig/network** especificamos la información sobre la configuración de red deseada.

```
GNU nano 2.3.1                Fichero: /etc/sysconfig/network

NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=dns.unl.edu.ec
```

  Donde:

  - La directiva NETWORKING_IPV6 = yes habilita IPv6 en la interfaz.
  - HOSTNAME: Debe ir el Fully Qualified Domain Name (FDQ), nombre de dominio cualificado completo o también el nombre del host.

- **Configurar la dirección IPv6 en el sistema Centos Dual-stack.**

  Ingresamos al archivo de configuración **/etc/sysconfig/network-scripts/ifcfg-eth0** de la interfaz deseada en este caso [eth0] y agregamos lo siguiente:

```
GNU nano 2.3.1   Fichero: /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
NAME=eth0
UUID=62a1245c-41c0-406b-a6b7-7d81cfa2dbaa
DEVICE=eth0
ONBOOT=yes
IPADDR=172.16.32.51
PREFIX=19
GATEWAY=172.16.32.1
IPV6ADDR=2001:db8:7:ff02:54:8dd9::cb3/64
IPV6_DEFAULTGW=2001:db8:7:ff02::ffff
```

Donde:

- En la directiva DEVICE: Colocamos el nombre del dispositivo físico

- ONBOOT = yes: El dispositivo debe activarse en el momento de arranque.
- IPV6INIT = yes: Habilita IPv6 en esa interfaz y permite que arranque el módulo IPv6 al iniciar el sistema.
- IPV6ADDR: Se debe colocar la dirección IPv6 que se asignará a la interfaz
- IPADDR: Dirección IPV4
- PREFIX: Prefijo de Red
- IPV6_DEFAULTGW: Especifica la puerta de enlace IPv6

Seguidamente reiniciamos la interfaz de red, para lo cual ingresamos lo siguiente:

sudo service network restart

Nota: *Cada vez que realice alguna modificación es importante reiniciar la interfaz de red para q se puedan registrar los cambios realizados.*

Para verificar que a la interfaz [eth0] se agregó la dirección IPv6 [2001:db8:7:ff02:54:8dd9::cb3/64] se lo puede hacer de la siguiente manera y comprobamos conectividad a la misma interfaz.

```
[kmlapol@dns ~]$ ifconfig eth0 | grep inet6
    inet6 2001:db8:7:ff02:54:8dd9::cb3 prefixlen 64  scopeid 0x0<global>
    inet6 fe80::5054:ff:fe23:9e4b  prefixlen 64  scopeid 0x20<link>

[kmlapol@dns ~]$ ip -6 addr show eth0 | grep inet6
    inet6 2001:db8:7:ff02:54:8dd9::cb3/64 scope global
    inet6 fe80::5054:ff:fe23:9e4b/64 scope link

[kmlapol@dns ~]$ ping6 -I eth0 -c 2 2001:db8:7:ff02:54:8dd9::cb3
PING 2001:db8:7:ff02:54:8dd9::cb3 (2001:db8:7:ff02:54:8dd9::cb3) 56 data bytes
64 bytes from 2001:db8:7:ff02:54:8dd9::cb3: icmp_seq=1 ttl=64 time=0.031ms
64 bytes from 2001:db8:7:ff02:54:8dd9::cb3: icmp_seq=2 ttl=64 time=0.056ms

--- 2001:db8:7:ff02:54:8dd9::cb3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.031/0.043/0.056/0.014 ms
```

Cabe mencionar que cuando comprobamos la conectividad de la dirección IPv4 o IPv6, sea en Windows o Linux se utiliza el comando ping, pero en el caso de Gnu/Linux es necesario especificar la versión del protocolo con el comando ping6 y agregar lo siguiente:

- -I eth0: Dirección de la interfaz de origen.
- -c 2: Indica el número de paquetes a contabilizar.

4.1. SISTEMA DE NOMBRES DE DOMINIO (DNS)

Procedimiento de instalación y configuración del servidor DNS

Instalación de Bind

Existen varios programas de servidor ¨dns¨que soportan IPv6, los más usados, tanto en IPv4 como en IPv6, son "Bind" para diferentes plataformas (windows, Gnu / Linux, etc). Para la instalación se puede hacer uso de los sistemas habituales de cada distribución (apt-get, yum, up2date, rpm, etc.), en nuestro caso usamos el siguiente comando:

sudo yum install bind bind-utils

Otra forma de instalar bind es descargando los ficheros fuente de **www.isc.org** y compilarlo de la siguiente manera:

```
# tar -xzvf versión del paquete-P2.tar.gz
# cd bind-versión del paquete-P2
# ./configure
# make
# make install
```

CONFIGURACIÓN DEL SERVIDOR DNS

Para la configuración del Servidor DNS, se requiere del uso y configuración de varios ficheros que permitan su correcto funcionamiento, a continuación se nombra de manera general cada uno de ellos y a medida que se va avanzando en el proceso de configuración se los va describiendo para mayor compresión.

Archivo principal del DNS

/etc/named.conf

Resolución Directa IPv4/IPv6

var/named/db.unl.edu.ec

Resolución Inversa IPv4

var/named/db.inversa4

Resolución Inversa IPv6

var/named/db.inversa6

Levantar demonio named

sudo systemctl restart named.service

Archivo log DNS

sudo tail -f /var/log/messages

Una vez que hemos instalado el programa Bind, se procede a configurar el archivo principal el mismo que se encuentra en **/etc/named.conf,** es aquí donde vamos a realizar algunas modificaciones en ciertas directivas para el correcto funcionamiento de IPv6.

Habilitar peticiones Ipv6.

Para habilitar correctamente las consultas DNS que se realicen a la dirección IPv6 del servidor de nombres, se debe agregar las siguientes directivas en el archivo de configuración principal.

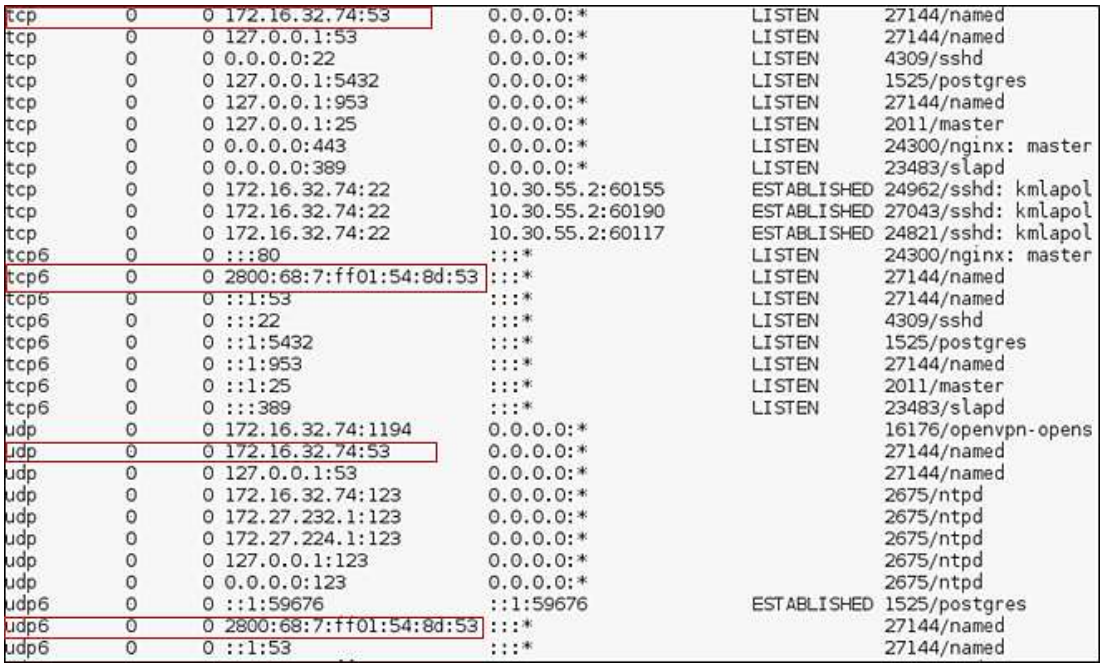
```
GNU nano 2.3.1                                  Fichero: /etc/named.conf

acl “publicos” {
           10.10.0.0/8;
           172.16.32.0/19;
           127.0.0.1;
} ;

acl “publicos6” {
           2001:db8:7::/48;
           ::1/128;
} ;

options {
            listen-on port 53 {127.0.0.1; 172.16.32.51; };
            listen-on-v6 port 53 {::1; 2001:db8:7:ff02:54:8dd9::cb3; };
            directory           “/var/named”;
            dump-file           “/var/named/data/cache_dump.db”;
            statistics-file     “/var/named/data/named_stats.txt”;
            memstatistics-file  “/var/named/data/named_men_stats.txt”;
            allow-query       {localhost; publicos; publicos6; };

}
```

Donde:

- Las acl (listas de control de acceso) son utilizadas para controlar el flujo de tráfico en equipos de red, en este caso vamos a tener dos acl's, una especificando la dirección de red IPv4 y otra especificado la dirección IPv6.
- La declaración options {} contiene las especificaciones que controlan el comportamiento global del servidor, se puede usar para especificar la ubicación del directorio de trabajo (named), los puertos de escucha, entre otros.
- La opción "Listen-on", lista las direcciones IPv4 y puertos habilitados para responder a las consultas DNS
- Las directivas listen-on-v6 port 53 {::1; 2001:db8:7:ff02:54:8dd9::cb3; }; permite indicarle al servidor Dns en que puerto escuchar para recibir peticiones de clientes Ipv6.
- La opción "directory" indica en qué directorio se encuentran los archivos utilizados por el bind
- La opción "allow-query" indica el bloque de direcciones IP que tienen permisos para realizar consultas al servidor

Para comprobar que el servidor está escuchando en las direcciones IPv4 e IPv6 en el puerto del Dns [53] en los protocolos TCP y UDP, se lo hace ingresando lo siguiente:

netstat –anutp



tcp	0	0 172.16.32.74:53	0.0.0.0:*	LISTEN	27144/named
tcp	0	0 127.0.0.1:53	0.0.0.0:*	LISTEN	27144/named
tcp	0	0 0.0.0.0:22	0.0.0.0:*	LISTEN	4309/sshd
tcp	0	0 127.0.0.1:5432	0.0.0.0:*	LISTEN	1525/postgres
tcp	0	0 127.0.0.1:953	0.0.0.0:*	LISTEN	27144/named
tcp	0	0 127.0.0.1:25	0.0.0.0:*	LISTEN	2011/master
tcp	0	0 0.0.0.0:443	0.0.0.0:*	LISTEN	24300/nginx: master
tcp	0	0 0.0.0.0:389	0.0.0.0:*	LISTEN	23483/slapd
tcp	0	0 172.16.32.74:22	10.30.55.2:60155	ESTABLISHED	24962/sshd: kmlapol
tcp	0	0 172.16.32.74:22	10.30.55.2:60190	ESTABLISHED	27043/sshd: kmlapol
tcp	0	0 172.16.32.74:22	10.30.55.2:60117	ESTABLISHED	24821/sshd: kmlapol
tcp6	0	0 :::80	:::*	LISTEN	24300/nginx: master
tcp6	0	0 2800:68:7:ff01:54:8d:53	:::*	LISTEN	27144/named
tcp6	0	0 ::1:53	:::*	LISTEN	27144/named
tcp6	0	0 :::22	:::*	LISTEN	4309/sshd
tcp6	0	0 ::1:5432	:::*	LISTEN	1525/postgres
tcp6	0	0 ::1:953	:::*	LISTEN	27144/named
tcp6	0	0 ::1:25	:::*	LISTEN	2011/master
tcp6	0	0 :::389	:::*	LISTEN	23483/slapd
udp	0	0 172.16.32.74:1194	0.0.0.0:*		16176/openvpn-opens
udp	0	0 172.16.32.74:53	0.0.0.0:*		27144/named
udp	0	0 127.0.0.1:53	0.0.0.0:*		27144/named
udp	0	0 172.16.32.74:123	0.0.0.0:*		2675/ntpd
udp	0	0 172.27.232.1:123	0.0.0.0:*		2675/ntpd
udp	0	0 172.27.224.1:123	0.0.0.0:*		2675/ntpd
udp	0	0 127.0.0.1:123	0.0.0.0:*		2675/ntpd
udp	0	0 0.0.0.0:123	0.0.0.0:*		2675/ntpd
udp6	0	0 ::1:59676	::1:59676	ESTABLISHED	1525/postgres
udp6	0	0 2800:68:7:ff01:54:8d:53	:::*		27144/named
udp6	0	0 ::1:53	:::*		27144/named

Netstat: *Es una herramienta que nos permite verificar que puertos están abiertos y si los programas escuchan en esos puertos, es decir, permite verificar las Conexiones entrantes y salientes, protocolo TCP – UDP y estado de las conexiones tanto para IPv4 e IPv6*.

Configuración de las Zonas de Resolución Directa e Inversa

En el fichero **/etc/named.conf** se pueden definir directamente las zonas para las que nuestro servidor va a ser autorizado.

```
GNU nano 2.3.1      Fichero: /etc/named.conf
//Zona directa

zone “unl.edu.ec”  IN {
             type master;
             file “db.unl.edu.ec”;
             allow-update { none; };
};
```

```
GNU nano 2.3.1   Fichero: /etc/named.conf
//Zona reversa IPv4

zone “32.16.172.in-addr.arpa”  IN {
              type master;
              file “db.inversa4”;
              allow-update { none; };
};
```

```
GNU nano 2.3.1                Fichero: /etc/named.conf
//Zona reversa IPv6

zone “2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa”  IN {
             type master;
             file “db.inversa6”;
};
```

Donde:

- Zone: es identificada como unl.edu.ec
- type master: define al servidor autoritativo para esa zona.
- File: especifica el nombre del archivo en el directorio de trabajo named que contiene información de configuración de la zona, en este caso el archivo es denominando **db.unl.edu.ec**

La zona “unl.edu.ec” indica el dominio sobre el cual el servidor DNS tiene autoridad para responder consultas (type master), la “32.16.172.in.addr.arpa” indica cuál es la zona de direccionamiento reverso IPv4 y la “2.0.f.f.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa” indica cual es la zona de direccionamiento reverso IPv6 por la(s) que el servidor responde.

Cabe mencionar que en la zona de resolución inversa para IPv6 el prefijo (2001:db8:7:FF02::/64) se divide en nibles y se concatena en orden inverso para declarar la zona al dominio **ip6.arpa.** Esta zona permitirá la resolución inversa de las direcciones IPv6 cuyo fichero es **db.inversa6.**

Creación de los ficheros de zona

Los ficheros de zona se crean en el directorio **/var /named/.** Para crear los ficheros de zona podemos guiarnos en la plantilla **named.localhost** y editarla, para lo cual ingresamos en consola.

Para la resolución directa:

cp /var /named/named.localhost /var/named/db.unl.edu.ec

Para la resolución inversa:

cp /var /named/named.localhost /var/named/db.inversa4

cp /var /named/named.localhost /var/named/db.inversa6

Comprobamos que los archivos de zonas se han creado

```
[kmlapol@labtesis1 ~]$ cd /var/
[kmlapol@labtesis1 var]$ cd named/
[kmlapol@labtesis1 named]$ ls
data         db.inversa6    dynamic   named.empty      named.loopback
db.inversa4  db.unl.edu.ec  named.ca  named.localhost  slaves
```

Archivo de resolución directa

En la resolución de nombres a direcciones IPv6, existe el registro AAAA (quad A) en el DNS. El registro AAAA toma como datos de registro específico el formato textual de una dirección IPv6. Los registros A y AAAA pueden coexistir lado a lado en cualquier zona directa. Por ejemplo si el host tiene una dirección IPv4 y una dirección IPv6 (host Dual stack), pueden conectar tanto registros A como AAAA de su nombre de dominio. En nuestra configuración editamos el fichero para resolución directa que se encuentra en **/var/named/db.unl.edu.ec** y añadimos lo siguiente:

```
GNU nano 2.3.1              Fichero: /var/named/db.unl.edu.ec
$TTL 604800
@       IN SOA  dns.unl.edu.ec.   root.unl.edu.ec. (
                                2016121601 ; serial
                                604800     ; refresh
                                86400      ; retry
                                2419200    ; expire
                                604800     ; minimum
                                )

@       IN      NS      dns.unl.edu.ec.

dns     IN      A        172.16.32.51
dns     IN      AAAA     2001:db8:7:ff02:54:8dd9::cb3
eva             IN A        172.16.32.67
eva             IN AAAA     2001:db8:7:ff02:b2:a056::cc3
cursosmed       IN A        172.16.32.199
cursosmed       IN AAAA     2001:db8:7:ff02:de:39f0::7dc7
virtual         IN A        172.16.32.200
virtual         IN AAAA     2001:db8:7:ff02:de:39f0::7dc8
evaluaciondocente    IN A       172.16.32.118
evaluaciondocente    IN AAAA    2001:db8:7:ff02:93:4d18::7d76
graduados       IN A        172.16.32.84
graduados       IN AAAA     2001:db8:7:ff02:c4:b96a::cd4
formacion       IN A        172.16.32.13
formacion       IN AAAA     2001:db8:7:ff02:d8:c1f4::c8d
capacitacion IN A        172.16.32.44
capacitacion IN AAAA     2001:db8:7:ff02:c3:9843::cac
openvpn         IN A        172.16.32.45
openvpn         IN AAAA     2001:db8:7:ff02:10:4ed4::cad
dspace          IN A        172.16.32.89
dspace          IN AAAA     2001:db8:7:ff02:d3:eab9::cd9
unl.edu.ec.     IN A        172.16.32.112
unl.edu.ec.     IN AAAA     2001:db8:7:ff02:3c:8289::7d70
www             IN CNAME    unl.edu.ec.
```

Archivos de Resolución Inversa

El registro empleado para la resolución inversa de una dirección IPv6 es “PTR”, igual como ocurre en la resolución inversa de direcciones IPv4, y como en cualquier zona deben contener un registro SOA (Autoridad de la zona) y uno o más registros NS (Name Server).

A continuación se configura los archivos de resolución inversa tanto para IPv4 como para IPv6.

Archivo de resolución inversa Ipv4

Editamos el fichero **/var/named/db.inversa4** y añadimos lo siguiente:

```
GNU nano 2.3.1              Fichero: /var/named/db.inversa4
$TTL 604800
@      IN SOA  dns.unl.edu.ec.   root.unl.edu.ec. (
                              2016121601 ; serial
                              604800     ; refresh
                              86400      ; retry
                              2419200    ; expire
                              604800     ; minimum
                              )

@      IN     NS      dns.unl.edu.ec.

51     IN     PTR     dns.unl.edu.ec.

67     IN     PTR     eva.unl.edu.ec.
199      IN   PTR     cursosmed.unl.edu.ec.
200      IN   PTR     virtual.unl.edu.ec.
118      IN   PTR     evaluaciondocente.unl.edu.ec.
84     IN     PTR     graduados.unl.edu.ec.
13     IN     PTR     formacion.unl.edu.ec.
44     IN     PTR     capacitacion.unl.edu.ec.
45     IN     PTR     openvpn.unl.edu.ec.
89     IN     PTR     dspace.unl.edu.ec.
112    IN     PTR     unl.edu.ec
```

La zona de resolución inversa IPv4 está definida como 32.16.172.in.addr.arpa, que equivale a los primeros 3 octetos y en cada registro PTR se completa el siguiente octeto.

Archivo de resolución inversa IPv6

El registro empleado para la resolución inversa de una dirección IPv6 es “PTR”, igual como ocurre en la resolución inversa de direcciones IPv4, con la única diferencia que en IPv6 la representación de la dirección inversa es en nibbles.

Editamos el fichero **var/named/db.inversa6** y añadimos lo siguiente:

```
GNU nano 2.3.1                Fichero: /var/named/db.inversa6
$TTL 604800
@     IN SOA  dns.unl.edu.ec.   root.unl.edu.ec. (
                                      2016121601   ; serial
                                      604800       ; refresh
                                      86400        ; retry
                                      2419200      ; expire
                                      604800       ; minimum
                                      )


@     IN    NS    dns.unl.edu.ec.

3.b.c.0.0.0.0.9.d.d.8.4.5.0.0 IN    PTR     dns.unl.edu.ec.

3.c.c.0.0.0.0.6.5.0.a.2.b.0.0 IN    PTR     eva.unl.edu.ec.
7.c.d.7.0.0.0.0.f.9.3.e.d.0.0 IN    PTR     cursosmed.unl.edu.ec.
8.c.d.7.0.0.0.0.f.9.3.e.d.0.0 IN    PTR     virtual.unl.edu.ec.
6.7.d.7.0.0.0.8.1.d.4.3.9.0.0 IN    PTR     evaluaciondocente.unl.edu.ec.
4.d.c.0.0.0.0.9.8.2.8.c.3.0.0 IN    PTR     graduados.unl.edu.ec.
d.8.c.0.0.0.0.4.f.1.c.8.d.0.0 IN    PTR     formacion.unl.edu.ec.
c.a.c.0.0.0.0.3.4.8.9.3.c.0.0 IN    PTR     capacitacion.unl.edu.ec.
d.a.c.0.0.0.0.4.d.e.4.0.1.0.0 IN    PTR     openvpn.unl.edu.ec.
9.d.c.0.0.0.0.9.b.a.e.3.d.0.0 IN    PTR     dspace.unl.edu.ec.
0.7.7.e.0.0.0.9.8.2.8.c.3.0.0 IN    PTR     www.unl.edu.ec.
```

La zona de resolución inversa IPv6 está definida como 2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa, que equivale a los primeros 16 dígitos hexadecimales de la dirección IPv6 y en cada registro PTR se completa los siguientes 16 dígitos.

Una vez configurado cada uno de los archivos de zona, también es necesario configurar el fichero **/etc/resolv.conf** y añadimos lo siguiente:

```
GNU nano 2.3.1                    Fichero: /etc/resolv.conf

search unl.edu.ec
nameserver 172.16.32.51
nameserver 2800:68:7:ff04:54:8dd9::cb3
```

La línea “search” especifica en qué dominio buscar para cualquier nombre de máquina al que se desea conectar, “nameserver” especifica la dirección del servidor de nombres, en este caso como el mecanismo de transición utilizado es doble pila vamos a ubicar la dirección tanto IPv4 como IPv6 de nuestro servidor.

A continuación levantamos el demonio named del servidor DNS con el comando:

sudo systemctl restart named.service

Seguidamente revisamos los sucesos que se generan en el fichero ¨log¨ /var/log/messages al iniciar, parar o reiniciar el demonio ¨named¨, esto nos permite verificar la correcta inicialización del DNS así como detectar posibles inconvenientes que se presenten, para ello utilizamos el siguiente comando:

sudo tail -f /var/log/messages

```
[kmlapol@labtesis1 ~]$ sudo tail -f /var/log/messages
Dec 16 13:37:48 labtesis1 named[26956]: zone 32.16.172.in-addr.arpa/IN: loaded s
erial 2016121601
Dec 16 13:37:48 labtesis1 named[26956]: zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 0
Dec 16 13:37:48 labtesis1 named[26956]: zone localhost.localdomain/IN: loaded se
rial 0
Dec 16 13:37:48 labtesis1 named[26956]: zone localhost/IN: loaded serial 0
Dec 16 13:37:48 labtesis1 named[26956]: zone 1.0.0.127.in-addr.arpa/IN: loaded s
erial 0
Dec 16 13:37:48 labtesis1 named[26956]: zone 1.0.f.f.7.0.0.0.8.6.0.0.0.0.8.2.ip6
.arpa/IN: loaded serial 2016121601
Dec 16 13:37:48 labtesis1 named[26956]: zone unl.edu.ec/IN: loaded serial 201612
1601
Dec 16 13:37:48 labtesis1 named[26956]: all zones loaded
Dec 16 13:37:48 labtesis1 named[26956]: running
```

PRUEBAS DE LA CONFIGURACIÓN DEL DNS

Para las pruebas se utilizará las siguientes herramientas

Nslookup (Name System Lookup)

Es una herramienta que permite consultar un servidor de nombres y obtener información relacionada con el dominio o el host y así diagnosticar los posibles problemas de configuración que pudieran haber surgido en el DNS.

Resolución directa con IPv4

```
[kmlapol@dns ~]$ nslookup dns.unl.edu.ec
Server:              172.16.32.51
Address:             172.16.32.51#53

Name:               dns.unl.edu.ec
Address:            172.16.32.51
```

Resolución inversa con IPv4

```
[kmlapol@dns ~]$ nslookup 172.16.32.51
Server:             172.16.32.51
Address:            172.16.32.51#53

51.32.16.172.in-addr.arpa         name = dns.unl.edu.ec.
```

Resolución directa con IPv6

```
[kmlapol@dns ~]$ nslookup -type=AAAA eva.unl.edu.ec
Server:             172.16.32.51
Address:            172.16.32.51#53

eva.unl.edu.ec    has  AAAA  Address 2001:db8:7:ff02:b2:a056::cc3
```

Dig (Domain Information Groper)

Permite realizar consultas a los servidores DNS, por lo que es muy útil para comprobar si el DNS está correctamente configurado en nuestra máquina. Permite comprobar

tanto el mapeo de nombres a IPs como el mapeo inverso de IPs a nombres. Esta herramienta nos proporciona información más detallada de nuestro servidor DNS.

Resolución directa, con el parámetro quad "a"

Al utilizar la herramienta dig seguida del parámetro aaaa, estamos comprobando si nuestro servidor resuelve el dominio unl.edu.ec con la versión 6 del protocolo IP.

```
[kmlapol@dns ~]$ dig aaaa unl.edu.ec

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.4 <<>> aaaa unl.edu.ec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30012
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;unl.edu.ec.                IN   AAAA

;; ANSWER SECTION:
unl.edu.ec.         604800   IN   AAAA        ::1

;; AUTHORITY SECTION:
unl.edu.ec.         23330    IN   NS          dns.unl.edu.ec.

;; ADDITIONAL SECTION:
dns.unl.edu.ec.     604800   IN   A           172.16.32.51
dns.unl.edu.ec.     604800   IN   AAAA        2001:db8:7:ff02:54:8dd9::cb3

;; Query time: 0 msec
;; SERVER: 172.16.32.51#53(172.16.32.51)
;; WHEN: mar dic 06 17:06:55 ECT 2016
;; MSG SIZE  rcvd: 135
```

Resolución inversa, utilizamos el parámetro "-x".

Al utilizar la herramienta dig seguida del parámetro -x, le estamos consultando a nuestro servidor el dominio correspondiente a esa dirección IP. En las figuras se puede observar cómo se realiza una consulta con IPv4 y con IPv6 respectivamente.

Resolución Inversa IPv4

```
[kmlapol@dns ~]$ dig -x 172.16.32.51

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.4 <<>> -x 172.16.32.51
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2196
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;51.32.16.172.in-addr.arpa.           IN   PTR

;; ANSWER SECTION:
51.32.16.172.in-addr.arpa.    604800   IN   PTR   dns.unl.edu.ec.

;; AUTHORITY SECTION:
51.32.16.172.in-addr.arpa.    604800   IN   NS    dns.unl.edu.ec.

;; ADDITIONAL SECTION:
dns.unl.edu.ec.               604800   IN   A     172.16.32.51
dns.unl.edu.ec.               604800   IN   AAAA  2001:db8:7:ff02:54:8dd9::cb3

;; Query time: 0 msec
;; SERVER: 172.16.32.51#53(172.16.32.51)
;; WHEN: mar dic 06 00:14:59 ECT 2016
;; MSG SIZE  rcvd: 146
```

Resolución Inversa IPv6

```
[kmlapol@dns ~]$ dig -x 2001:db8:7:ff02:54:8dd9::cb3

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7_2.4 <<>> -x 2001:db8:7:ff02:54:8dd9::cb3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39599
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;3.b.c.0.0.0.0.0.9.d.d.8.4.5.0.0.2.0.f.f.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa.  IN
PTR

;; ANSWER SECTION:
3.b.c.0.0.0.0.0.9.d.d.8.4.5.0.0.4.0.f.f.7.0.0.0.8.6.0.0.0.0.8.2.ip6.arpa.
604800 IN   PTR   dns.unl.edu.ec.

;; AUTHORITY SECTION:
2.0.f.f.7.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa 604800    IN   NS    dns.unl.edu.ec.

;; ADDITIONAL SECTION:
dns.unl.edu.ec.               604800   IN   A     172.16.32.51
dns.unl.edu.ec.               604800   IN   AAAA  2001:db8:7:ff02:54:8dd9::cb3
;; Query time: 0 msec
;; SERVER: 172.16.32.51#53(172.16.32.51)
;; WHEN: vie dic 16 13:41:37 ECT 2016
;; MSG SIZE  rcvd: 193
```

4.2. SERVIDOR WEB

Instalación y Configuración Apache en el Sistema Operativo Debian

El servidor web que se encuentra en producción en la Universidad Nacional de Loja, utiliza el programa "Apache", por lo que se requiere instalar el mismo haciendo uso del siguiente comando:

sudo apt-get install apache2

Asi mismo es importante la utilización de sus ficheros de configuración que es donde se van a agregar ciertas directivas y se realizará algunas modificaciones para su funcionamiento.

Archivo principal

etc/apache2/apache2.conf

Configuración IP y puerto

/etc/apache2/ports.conf

Reiniciar apache

/etc/init.d/apache2 restart

En el fichero **/etc/apache2/ports.conf** se va manipular porque interfaces se quiere que escuche nuestro servidor, como se explica:

```
GNU nano 2.2.6              Fichero: /apache2/ports.conf

Listen [2800:68:7:ff04:3c:8289::7d70]:80
Listen 172.16.32.112:80
```

Donde:

- Listen es la directiva utilizada para indicarle a nuestro servidor en que direcciones IP escuchar, para el caso de IPv6 es necesario que la dirección esté dentro de corchetes [] seguido por dos puntos y el puerto.

Nota: *Recordar que previo a las configuraciones que se acaban de realizar se debe haber seguido los pasos explicados anteriormente en el apartado configuraciones previas.*

Para verificar los puertos en los que está escuchando apache tecleamos lo siguiente:

netstat –pan | grep apache

Finalmente editamos **/etc/hosts** y agregamos

```
GNU nano 2.2.6                Fichero: /etc/hosts

127.0.0.1                       localhost
172.16.32.112                   www.unl.edu.ec
2001:db8:7:ff02:3c:8289::7d70   www.unl.edu.ec
```

En este fichero agregamos las direcciones IP correspondientes a los dos protocolos (IPv4 e Ipv6). Este es el primer archivo que el sistema operativo lee antes de hacer una consulta DNS.

Configuración del DNS (/etc/resolv.conf)

El fichero resolv.conf especifica el dominio al que pertenece nuestra máquina y la dirección del servidor DNS. Es el cliente DNS responsable de mapear una petición de información de un programa en un host.

```
GNU nano 2.2.6              Fichero: /etc/resolv.conf

search unl.edu.ec
nameserver 172.16.32.51
nameserver 2001:db8:7:ff02:54:8dd9::cb3
```

Finalmente debemos reiniciar apache mediante:

/etc/init.d/apache2 restart

Es importante destacar que cada vez que se realice alguna modificación en los archivos de configuración se debe reiniciar apache, esto para que se puedan registrar los cambios realizados.

5. CONCLUSIÓN

- Las elaboración del presente manual permitirá seguir un proceso para la correcta y exitosa implementación del protocolo de internet versión 6 (IPv6) en el DNS autoritario y servidores públicos de la red de datos de la UNL.