UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRANSICIÓN DE IPV4 A IPV6 DE DOS APLICACIONES DEL SISTEMA INTEGRADO DE LA UNIVERSIDAD TÉCNICA DEL NORTE

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTOR: BRAYAN DANIEL CARANQUI VALENZUELA

DIRECTOR DE TRABAJO DE GRADO: ING. CARLOS VÁSQUEZ MSc.

IBARRA - ECUADOR

Autorización de uso y publicación a favor de la Universidad Técnica del Norte

1.- Identificación de la obra

La Universidad Técnica del Norte dentro del proyecto del repositorio digital institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

Por medio del presente documento dejo sentada mi voluntad de participaren este proyecto, para lo cual pongo a disposición la siguiente información.

Datos del contacto.	
Cedula de identidad.	0401313366
Apellidos y nombres.	Caranqui Valenzuela Brayan Daniel.
Dirección.	Chontahuasi y la Capilla - Mira.
Email.	bdcaranquiv@utn.edu.ec
Teléfono.	0991341267

Datos de la obra.	
Título.	TRANSICIÓN DE IPV4 A IPV6 DE DOS APLICACIONES DEL SISTEMA INTEGRADO DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Autor.	Caranqui Valenzuela Brayan Daniel
Fecha.	Julio 2017
Programa.	Pregrado
Titulo por el que opta.	Ingeniería en Electrónica y Redes de Comunicación
Director.	Ing. Carlos Vásquez

2.- Autorización de uso a favor de la universidad

Yo Brayan Daniel Caranqui Valenzuela con C.I. 040131336-6 en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la biblioteca de la universidad con fines académicos. Para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión en concordancia con la Ley de Educación Superior, artículo 144.

3.- Constancia

Yo, BRAYAN DANIEL CARANQUI VALENZUELA, manifiesto que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que soy el titular de los derechos patrimoniales, por lo que asumo la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, julio 2017

EL AUTOR:

.....

Brayan Daniel Caranqui Valenzuela

CI: 040131336-6

Cesión de derecho de autor del Trabajo de Grado a favor de la Universidad Técnica del Norte

Yo Brayan Daniel Caranqui Valenzuela, con cedula de identidad Nro. 040131336-6, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, articulo 4, 5 y 6 en calidad de autor del trabajo de grado denominado: "TRANSICIÓN DE IPV4 A IPV6 DE DOS APLICACIONES DEL SISTEMA INTEGRADO DE LA UNIVERSIDAD TÉCNICA DEL NORTE.", que ha sido desarrollado para optar por el título de: Ingeniería en Electrónica y Redes de Comunicación, quedando la Universidad Técnica del Norte facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi consideración de autor reservo los derechos morales de la obra antes citada.

En concordancia suscribo este documento en el momento en que hago la entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

Firma: .....

Brayan Daniel Caranqui Valenzuela.

C.I. 040131336-6

Ibarra, julio 2017

Certificación

Certifico que el presente trabajo de titulación: "TRANSICIÓN DE IPV4 A IPV6 DE DOS APLICACIONES DEL SISTEMA INTEGRADO DE LA UNIVERSIDAD TÉCNICA DEL NORTE.", fue realizado en su totalidad por el Sr. Brayan Daniel Caranqui Valenzuela, bajo mi supervisión.

.....

Ing. CARLOS VÁSQUEZ

Director de tesis.

Declaración de autoría

Yo, Brayan Daniel Caranqui Valenzuela, con cedula de identidad Nro. 040131336-6, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, y que este no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual y normativa vigente de la universidad Técnica del Norte.

Brayan Daniel Caranqui Valenzuela.

C.I. 040131336-6

Autor.

Agradecimiento

Agradezco en primer lugar a Dios por brindarme un día más de vida para cumplir mis objetivos, a mi hijo por ser el motor de mi vida y ser la razón para continuar con los proyectos planteados, a mi familia por el apoyo que me han brindado día a día para superar cada uno de los objetivos propuestos para mi vida profesional y también agradecer a Nicole Proaño por ese apoyo incondicional en el transcurso del desarrollo de este nuevo proyecto.

Un agradecimiento especial al Ing. Carlos Vásquez y al Ing. Vinicio Guerra por ser parte de este proyecto de titulación, por otro lado, a todos mis maestros universitarios por darme las herramientas necesarias para desenvolverme en mi carrera profesional y al Ing. Carlos Obando por el apoyo durante todo el desarrollo del proyecto.

Dedicatoria

El presente proyecto de titulación es dedicado a mi hijo Arley Caranqui, a mis Padres Luis Caranqui y Gladys Valenzuela, a mis hermanos Lilian, Eric y Roger Caranqui, y a la persona que me ha dado todo su apoyo durante todo el desarrollo del Proyecto de Tesis a Nicole Proaño.

Resumen

El trabajo de titulación que se presenta a continuación, consiste en la implementación de un mecanismo de transición de IPv4 a IPv6 de dos aplicaciones del Sistema Integrado de la Universidad Técnica del Norte.

Para el desarrollo del proyecto, se realizó una fundamentación teórica, situación actual, diseño, implementación y pruebas de funcionamiento. El fundamento teórico, permite tener un conocimiento concreto sobre todos los requerimientos para el uso del nuevo protocolo; además, mediante el levantamiento de información dentro de la Universidad, permitió saber los equipos de red que no cuentan con un sistema que admita la utilización de IPv6.

Uno de los equipos de red que no tienen un sistema para trabajar con el nuevo protocolo, es el Switch 3750, se realizó una actualización del ISO; también, se instaló Linux Centos 6.5 y Oracle Linux 6.8, se implementó un servidor de Base de Datos, Aplicaciones y DNS64/NAT64.

El servicio DNS, es el encargado de traducir las peticiones de registros A y AAAA en la red de la Universidad; se cuenta con un NAT que permite la traducción del pool de direcciones de la UTN, los equipos de red manipulados durante la transición de las dos aplicaciones, han sido configurados mediante el mecanismo Doble Pila, para su correcta operación.

Finalmente, se realizó las pruebas de funcionamiento en el Laboratorio 4 de la Facultad de Ingeniería en Ciencias Aplicadas.

Abstract

The degree project consists in the implementation of a mechanism of the transition between IPv4 and IPv6 of two applications of the integrated system of the University ¨Técnica del Norte¨.

For the development of the project, a theoretical basis, current situation, design, implementation and performance test was described. The theoretical basis allows to have a concrete knowledge about all the requirements for the use of the new protocol, furthermore, through the collection of information within the University go along with the network equipment that do not have a system that supports the use of IPv6.

One of the network host doesn't have the system to work with the new protocol, is the Switch 3750, that was created a new updated of the ISO, in addition, the installation of the Linux Centos 6.5 and Oracle Linux 6.8, also, a Server of Data Base, Application and DNS64/NAT64 were implemented.

The DNS service is responsible of translate the request of the records A and AAAA in the network of the University, the NAT allows the translation of the address pool of the UTN, the network equipment manipulated during the transition of the two applications have been configured using the Double Stack mechanism for its correct operation.

Finally, the functionality test had been made in the Laboratory #4 of the faculty of Engineer in Applied Science.

Presentación

En el capítulo uno se realizará el planteamiento del problema, realizando un análisis de acuerdo a la situación actual que se tiene en la Universidad, se planteará los objetivos del desarrollo del Proyecto, lo que se va a realizar es decir un alcance de tal manera que se pueda limitar lo que se quiere implementar.

En el capítulo dos se hará un estudio de los conceptos, características, ventajas y desventajas del protocolo IPv4 e IPv6, se realizará un estudio para la transición de protocolos y sobre todo para tener la coexistencia de dos aplicaciones del Servicio Integrado.

En el capítulo tres se realizará un estudio de los equipos y servidores que se tienen en la Universidad para que puedan soportar el mecanismo de transición para tener la coexistencia de protocolos en las dos aplicaciones, además la implementación del software de transición de protocolos para tener coexistencia, se realizará con la utilización de servidores y equipos de la Universidad Técnica del Norte.

En capítulo cuatro se realizará las conclusiones de todo el desarrollo del proyecto de tal manera que se tenga una clara visión del proyecto realizado, además de las recomendaciones para evitar posibles percances en el desarrollo del proyecto.

Índice General

Índice de figuras

Índice de tablas

Capítulo I

Antecedentes

En este capítulo se realizará el planteamiento del problema, realizando un análisis de acuerdo con la situación actual que se tiene en la Universidad, se planteará los objetivos del desarrollo del Proyecto, lo que se va a realizar es decir un alcance de tal manera que se pueda limitar lo que se quiere implementar.

1.1 Problema

En la actualidad, las tecnologías de la información y comunicación son una parte muy importante en las vidas de cada uno de los usuarios de Internet, siendo éste un avance tecnológico para la sociedad ya que se han venido desarrollando cada día nuevas tecnologías y servicios que permiten a las personas poder comunicarse, uno de los requerimientos más importantes a nivel de protocolos, es el IP, siendo específicamente el Protocolo IPv4 el más actual.

El agotamiento de direcciones IPv4 ha llegado a un proceso de migración urgente, ya que la cantidad de usuarios y requerimientos de los mismos ha incrementado exponencialmente de tal manera que se ha saturado la cantidad de direcciones IPv4 asignadas para cada una de las entidades pertinentes, este proceso de migración ya se lo veía venir desde hace algunos años atrás.

Anteriormente ya se empezaron a realizar estudios sobre el proceso de migración al protocolo conocido como IPv6, para de esta manera poder reemplazar al antiguo protocolo y

así obtener la cantidad de direcciones IP suficientes para abastecer a todos los dispositivos que cuenten con una dirección IP en todo el mundo, una de las razones para realizar este cambio es que los usuarios de la Internet cada vez requieren nuevos servicios y aplicaciones ya que la tecnología avanza increíblemente.

Existen varios mecanismos para poder realizar este proceso de migración tanto para aplicaciones como para servicios brindados por la Universidad Técnica del Norte, de tal manera que se requiera de una coexistencia de protocolos para que así los usuarios puedan tener accesibilidad a cada una de las aplicaciones tanto desde IPV4 como de IPv6, con la utilización del nuevo protocolo IP se puede tener muchas ventajas tales como son calidad de servicio, Multicast y Anycast, además de la movilidad IP y también por el hecho de que muchas veces en su cabecera no se va a necesitar de examinar cada una de ellas sino más bien solo hop by hop lo que permitirá que se tenga una mejor velocidad de transmisión.

1.2 Objetivos

1.2.1.- Objetivo General

Realizar la transición de dos aplicaciones del sistema integrado de la Universidad Técnica del Norte, mediante la utilización de las herramientas necesarias para garantizar y permitir la coexistencia de las redes tanto en IPv4 como en IPv6.

1.2.2.- Objetivos Específicos

- Recopilar información mediante una investigación bibliográfica de los mecanismos de transición del Protocolo IPv4 a IPv6 para tener un conocimiento claro sobre las causas de este proceso.

- Analizar las ventajas y desventajas que pueden traer estos procesos de migración para que los usuarios y administradores puedan afrontar los requerimientos generados.
- Implementar dos aplicaciones del Servicio Integrado de la Universidad Técnica del Norte mediante el protocolo IPv6, utilizando los mecanismos necesarios para la transición.
- Desarrollar pruebas de verificación de acceso a las aplicaciones mediante el protocolo IPv6 ya sea internamente o externamente para poder tener un servicio adecuado en cada una de las aplicaciones.

1.3 Alcance

El siguiente proyecto se encuentra enfocado en el estudio del Protocolo IP actual que es el IPv6 en la Universidad Técnica del Norte, permitiendo realizar la coexistencia de dos aplicaciones del Servicio Integrado, teniendo en cuenta que este proceso se dejará establecido para que en un futuro pueda ser implementado en las demás aplicaciones y con los servicios necesarios para de esta manera lograr que la Universidad tenga un proceso de cambio muy amplio hacia un avance tecnológico en cuanto a redes de comunicación se refiere, la implementación de este proceso de transición es muy importante ya que permitirá realizar este cambio de una manera paulatina, teniendo en un futuro una infraestructura completamente migrada hacia IPv6, además de que esta institución es parte del Consorcio Ecuatoriano de Desarrollo de Internet Avanzado (CEDIA), lo que implica que se aplicará un mecanismo que es solicitado por CEDIA de tal manera que se pueda utilizar las nuevas prestaciones de la red avanzada.

Se realizará una comparación entre el IP versión 4 e IP versión 6, de tal manera que se pueda identificar las ventajas de utilizar este tipo de protocolo para implementarlo en las dos aplicaciones planteadas y dejar establecida la idea de migrar toda la red de la Universidad Técnica del Norte hacia IPv6.

Para la implementación del proyecto se tendrá en cuenta que no todos los usuarios tienen una dirección IPv6 para lo cual se realizará un estudio del mejor método para realizar este tipo de transición, se puede tener el caso de hacer una transición extremo a extremo, uno de estos puede ser mediante Doble Pila, el cual permite soportar tanto IPv4 como IPv6, otro de los métodos es aplicando Túneles mediante la encapsulación de paquetes IPv6 en IPv4, siendo un tipo de camuflaje para la red IPv4 y por último un método de traducción, que permitirá el acceso tanto desde IPv4 como desde IPv6 a las aplicaciones.

Para la culminación del proyecto se verificará el correcto funcionamiento de las dos aplicaciones con el nuevo Protocolo IP en versión 6, sabiendo que se debe tener acceso desde cualquier otro dispositivo, teniendo en cuenta que se contará con usuarios IPv4 que podrán acceder al servicio de estas aplicaciones en IPv6, así uno de los requerimientos que se implementará será un servidor DNS64 con un mecanismo de Dual-Stack permitiendo que se puedan enviar peticiones tanto de nombres como de direcciones en IPv6.

Se realizará pruebas de funcionamiento de las dos aplicaciones con el nuevo protocolo de tal manera que se deje establecido como un ejemplo esta transición para que se realice el mismo proceso con las demás aplicaciones de tal manera que se logre tener una transición completa de todas las aplicaciones y servicios de la red de la UTN.

Finalmente se desarrollará tanto las conclusiones como las recomendaciones de todo el proceso de transición de las Aplicaciones.

1.4 Justificación

La Universidad Técnica del Norte es una de las instituciones que han logrado formar gran cantidad de profesionales, con el paso de los años ha ido mejorando en cuanto a tecnología se refiere, por esta razón la Universidad debe contar con los recursos necesarios para poder dar el acceso a las redes de Internet para ayudar al desarrollo académico de cada uno de los usuarios dentro de la Institución.

Debido a la gran demanda de direcciones IP que se tiene en la actualidad, y sabiendo que la Universidad cuenta con un Pool de direcciones IPv6, se ha visto la necesidad de migrar o realizar la transición de dos aplicaciones del Servicio Integrado de la institución, de tal manera que sea un incentivo y sobre todo que la Universidad en sí sea pionera en la transición del direccionamiento en la zona norte del país, teniendo en cuenta que la UTN pertenece a CEDIA.

"CEDIA fue creada para estimular, promover y coordinar, por medio del Proyecto de Redes Avanzadas, el desarrollo de las tecnologías de información y las redes de telecomunicaciones e informática que están enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador." (CEDIA, 2015)

Para la realización de este proyecto se ha tomado en cuenta el análisis de la transición de las aplicaciones en el servidor para así garantizar que los usuarios puedan acceder ya sea

dentro de la Universidad o fuera de la misma con un direccionamiento en IPv4 o IPv6, llegando a tener un acceso total hacia estas dos aplicaciones.

De esta manera se podrá tener tanto un beneficio social, académico y por ende tecnológico ya que será un gran avance para la Universidad tener este tipo de migración y sobre todo tener como ejemplo para poder transicionar toda la red hacia el nuevo direccionamiento IPv6.

Capítulo II

2. Fundamento de protocolo IPv4 e IPv6

2.1 Introducción

Las redes de comunicaciones al igual que los hosts se encuentran conectados de diferentes maneras, requiriendo diferentes protocolos para establecer una conexión segura, uno de los protocolos que permite que diferentes redes de todo el mundo se puedan conectar es el TCP/IP, el cual mediante organizaciones gubernamentales ha logrado que en la actualidad se de lo que se conoce como Internet.

En el presente capítulo, se describen algunos protocolos que permiten la conexión de diferentes redes a nivel mundial, tales como son; El Protocolo de Internet versión 4 y el Protocolo de Internet versión 6, además; también se establece los organismos de asignación de direccionamiento para que cada subred creada en las diferentes regiones del mundo, puedan tener acceso a Internet.

Por otra parte, se explicará también acerca del Consorcio Ecuatoriano de Internet Avanzando, quien es el encargado de la asignación de direcciones IPv4 e IPv6 en Ecuador, el Internet avanzado ha sido de gran relevancia dentro de las telecomunicaciones, es así que dentro de cada una de las instituciones a nivel nacional han ido trabajando en la mejora de sus redes de datos, actualizando cada uno de los protocolos de Internet en los cuales se trabaja para el acceso a las redes.

Actualmente se ha venido implementando IPv6 a nivel nacional, es así que para poder usar este protocolo se debe tener primero una asignación de direccionamiento, lo cual existen organizaciones encargadas para este tipo de trámites, siendo en Ecuador CEDIA[1] el encargado de la asignación de rango de direcciones, hace algunos años atrás se realizó una reunión en la ciudad de Guayaquil con la finalidad de la creación del Consorcio Nacional para el Desarrollo de Internet Avanzado.

El objetivo de esta creación del Consorcio era impulsar la creación de una red de alta velocidad, de esta manera poder unirse a las redes académicas internacionales, pudiendo ser parte de la red de telecomunicaciones que permitan crear nuevas generaciones de científicos e investigadores, dotándolos de mejores e innovadoras herramientas tecnológicas y así, poder permitirles acceder a aplicaciones científicas y educativas de alta tecnología a nivel mundial.

CEDIA busca la creación de una red de telecomunicaciones con capacidades avanzadas, fomentar y coordinar el desarrollo de proyectos y aplicaciones relacionados con la nueva generación de Internet y que demandan la utilización de tecnologías de redes de telecomunicaciones y cómputo, enfocadas al desarrollo científico y educativo de la sociedad ecuatoriana (Marcelo Jaramillo, 2011).

2.1.1 Características de CEDIA

Dentro de lo que CEDIA tiene como características se puede nombrar que cuenta con un total de 24 Universidades y centros de investigación que ayudan a conformar redes de

[1] CEDIA: Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado

científicos ecuatorianos, de tal manera que se pueda interactuar con las contrapartes internacionales.

Se puede asegurar beneficios para tener acceso a infraestructura que pudiera no existir en Ecuador como un acelerador de partículas, un telescopio con características determinadas, entre otras cosas, de tal manera que todo esto se lo puede hacer a través de la conexión entre redes. Cabe recalcar que los organismos conectados tendrán otros beneficios agregados al servicio como el tener acceso a educación en línea a bajo costo.

CEDIA en Ecuador se encuentra agrupada por 26 organismos y universidades que en la actualidad se encuentran interconectadas entre sí, pero que además ya pueden acceder a otras redes tales y como son Clara, Internet 2 y Greant.

En Latinoamérica Clara conecta a un total de más de 800 instituciones a las que ahora Ecuador ya se encuentra integrada, teniendo en cuenta que tanto Bolivia, Cuba y Paraguay no tiene acceso a esta red.

2.1.2 Beneficios de CEDIA

Con la aparición de CEDIA, todas las instituciones que pertenezcan a este Consorcio pueden tener varios beneficios como el acceso a publicaciones científicas y bibliotecas digitales, pudiendo realizar sus investigaciones mediante bibliotecas virtuales de manera internacional.

Además, podrán hacer uso de recursos de computación avanzada de altas prestaciones de tal manera que, cada miembro del consorcio logrará tener las mejores tecnologías en

cuanto a Internet se refiere, además, de pasar a formar parte del uso de IPv6, realizando una migración de protocolos, es decir pasar de Protocolo IPv4 a IPv6.

Una de las ventajas más importantes de formar parte de la Red CEDIA es, poder hacer uso del servicio en la nube, actualmente se está trabajando mucho en plataformas con la nube ya que de esta manera se puede tener una gran cantidad de almacenamiento digital, facilitando el acceso a la información sin necesidad de tener en un ordenador la información que se requiera utilizar.

CEDIA permite tener muchos beneficios en los cuales la mayoría de Instituciones del país debería formar parte, ya que de esta manera podrían mejorar toda la infraestructura Tecnológica de cada una de sus localidades ofreciéndoles una gran variedad de servicios para investigadores académicos que trabajen en temas afines dentro y fuera del país, haciendo que esta Red sea Internacional.

2.2 Protocolo TCP/IP

2.2.1 Definición de Arquitectura TCP/IP

La arquitectura TCP/IP fue desarrollado por ARPANET, ésta fue creada por el Departamento de Defensa de los Estados Unidos, con la finalidad de brindar conectividad a universidades e instalaciones gubernamentales de ese país. Con el paso de los años, ésta red se liberó, de tal manera que fue permitiendo que diferentes redes de todo el mundo se pudieran conectar entre sí, dando lugar a lo que actualmente se conoce como Internet.

La Arquitectura TCP/IP recibe este nombre ya que sus dos principales protocolos son tanto el Protocolo de Control de Transmisión (TCP) como el Protocolo de Internet (IP). (Nuria Oliva, 2013).

2.2.2 Características de Arquitectura TCP/IP

Una de las características de la Arquitectura TCP/IP es un conjunto que define la manera de dirigir y enviar datos entre dos equipos, de tal manera que se lo conoce como un protocolo, es decir, múltiples protocolos que se agrupan pueden formar un conjunto de protocolos y estos a su vez trabajar juntos como una pila de protocolos.

La estructura del modelo TCP/IP está definida por cuatro capas, siendo la primera capa no definida en esta estructura, pero a continuación, se explicará cinco capas de manera que se tenga una idea más clara sobre TCP/IP.

2.2.2.1 Capa Física

Es aquella que define la interfaz física entre el host y el medio de transmisión o red. Se ocupa de la especificación de las características del medio de transmisión, de la naturaleza de las señales, de la velocidad de datos y cuestiones similares.

2.2.2.2 Capa de Acceso a la Red

Es la que permite el intercambio de datos entre el sistema final (equipo, terminal, estación de trabajo, etc.) y la red a la cual está conectado. Por una parte, el emisor debe proporcionar a la red la dirección destino, para así poder realizar el encaminamiento adecuado de los datos hacia su destino.

El software seleccionado en esta capa dependerá del tipo de red que se disponga, es decir, que existirán diferentes estándares para redes LAN, por ejemplo: Ethernet, Token Ring, Token Passing.

2.2.2.3 Capa de Internet

La función de la capa Internet es seleccionar la mejor ruta mediante un direccionamiento lógico para conectar los sistemas finales a través de diferentes redes, mediante el direccionamiento se puede permitir que los datos atraviesen redes que se encuentran interconectadas. En esta capa el protocolo utilizado es el Protocolo Internet brindando un servicio de encaminamiento a través de las redes.

2.2.2.4 Capa Transporte

Está diseñada para permitir que las entidades en el host de origen y destino puedan llevar a cabo una conversación, es decir que se tendrá una comunicación extremo a extremo definiendo dos protocolos de transporte como son tanto TCP como UDP.

Protocolo de Control de Transmisión o TCP

Es un protocolo orientado a conexión por lo tanto se puede decir que es un protocolo confiable, que permite que un flujo de bytes que se origina en un host se entregue sin errores en cualquier otro host de la intranet. Este protocolo confirma que un paquete ha alcanzado su destino de tal manera que se establece una conexión punto a punto entre los hosts de envío y recepción.

La principal característica que posee este protocolo es que tiene tres pasos importantes para su transmisión; el primer paso, es el punto de partida en el cual se establece la conexión; el segundo paso, es la transmisión de los datos; por último, se cierra la conexión.

Protocolo de Datagrama de Usuario o UDP

Es un protocolo no orientado a conexión, es decir, elimina los procesos de establecimiento y verificación de las conexiones, por lo tanto, se lo considera como un protocolo no confiable. Este protocolo es ideal para las aplicaciones en tiempo real tales como voz y video.

2.2.2.5 Capa Aplicación

Contiene todos los protocolos de nivel superior, siendo éstos utilizados por aplicaciones como navegadores, correo electrónico, entre otras. Además, se puede especificar que la capa aplicación provee a los usuarios la interfaz para poder interactuar con la aplicación, siendo éstas mediante línea de comandos o una interfaz gráfica. (ORACLE, 2010)

A continuación, la figura 1 muestra cada una de las capas del modelo de referencia TCP/IP, así como un ejemplo de los protocolos que pertenece a cada capa.

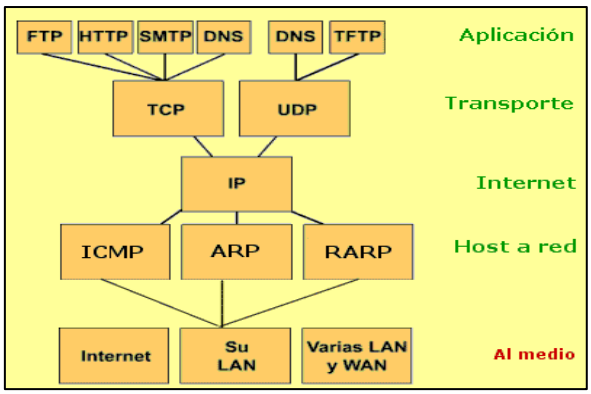


Figura 1. Estructura del Modelo de Referencia TCP/IP
Fuente: ANGELFIRE. (2012). *REDES3.* Recuperado de Comparación OSI-TCP/IP http://www.angelfire.com/empire/beraca/redes3.html

2.2.4 Direccionamiento IP

La interconexión de redes se percibe como una gran red física, se puede decir que se trataría de una estructura virtual que se define por los creadores de la red de manera lógica definiendo libremente la estructura y tamaño de los paquetes, dentro del direccionamiento se puede recalcar que el usuario no percibe en lo absoluto la presencia o la transferencia a través de distintas redes, siendo este un proceso transparente ante el usuario.

Para tener una idea más clara, la dirección IP es aquella que identifica de manera lógica y única, a un host dentro de un segmento de red específico. Existen dos tipos versiones de direcciones en la actualidad siendo: IPv4 que viene codificada en 32 bits, además de IPv6 viniendo codificada en 128 bits.

Para entender el direccionamiento se puede poner como ejemplo que, si se tiene un ordenador portátil y se lo desplaza desde una red hacia otra, será necesario proceder al cambio de su dirección IP ya sea en versión 4 como en versión 6, ya que la dirección que tenía anteriormente no encontraría una parte del identificador de red.

En IPv4 e IPv6 existen ciertas clases de direcciones, es así que, por procesos explicativos, a continuación, se detallará la clasificación del Protocolo de Internet versión 4, teniendo cinco clases de direcciones. Las direcciones de clase A, en las que el bit de mayor significación, es decir, el bit 0 es igual a 0 y el número de red, llega hasta el bit 7, a partir de éste, es decir, desde el bit 8 hasta el 31, se utiliza para denotar el número de host; las direcciones IP de clase B, en las que el bit cero es igual a 1 y el bit uno será siempre 0, llegando el número de red, hasta el bit 15, y el número del host, desde el bit 16 hasta el 31. En las direcciones IP de clase C, los bits 0 y 1 valdrán siempre 1, y el bit 2 tomará el valor 0.

El número de red en las direcciones de clase C, siempre llegará hasta el bit 23, y el número de host será a partir del bit 24. Las direcciones de clase D son utilizadas para transmisiones multicast y las de clase E agrupan un conjunto de direcciones reservadas para uso futuro (Alex, 2008).

En la figura 2 se puede identificar cada una de las clases que existen en cuanto al direccionamiento se refiere, de tal manera que se tenga una idea clara de la porción de red y la porción de host que se usa para cada una de las clases.

Figura 2. Identificación de la porción de Red y de Host
Fuente: GUÍAS PARA ARMAR UNA RED. Recuerado de http://goo.gl/GcVxet

Anteriormente se ha mencionado que existen diferentes clases de direccionamientos, para lo cual también se debe conocer que hay organismos de asignación de direccionamiento, a continuación, se explicará cada una de las organizaciones que son encargadas del plan de direccionamiento a nivel nacional.

2.3 Organismos de asignación de direccionamiento

La responsabilidad de la asignación, administración y distribución del espacio de direcciones IP está dada globalmente de acuerdo con la estructura jerárquica descrita en el

RFC[2] 2050, en donde especifica cada una de las entidades que pertenecen al plan de direccionamiento a nivel mundial, de tal manera que vaya desde la organización que realiza la asignación, hasta los usuarios finales que son quienes utilizan dicho direccionamiento.

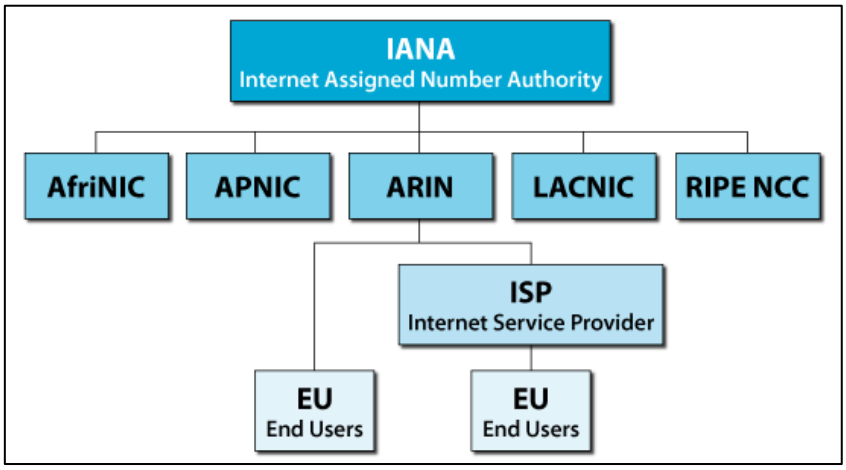


Figura 3. Jerarquía de Distribución de Direcciones IP
Fuente: ARIN. (2016). *ARIN NUMBER RESOURCE POLICY MANUAL*. Recuperado de Definitions: https://www.arin.net/policy/nrpm.html

A continuación, se podrá dar una explicación breve de cada una de las entidades que se han mostrado en la figura 3:

2.3.1 Internet Assigned Numbers Authority (IANA)

La Internet Assigned Numbers Authority (IANA) es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

En la actualidad la IANA es un departamento de la ICANN[3] que es la responsable de la coordinación de algunos de los elementos clave que mantiene el funcionamiento del

[2] RFC: Request for Comments
[3] ICANN: Corporación para asignación de nombres y números de Internet

Internet sin problemas, uno de estos es la resolución de DNS[4], en sí la IANA asigna y mantiene códigos únicos de sistemas de numeración que se utilizan en las normas técnicas, es decir en los protocolos que impulsan Internet.

Existen algunas actividades que la IANA realiza en este caso se lo puede mencionar en tres tipos, la primera que es nombres de dominio, después se tiene el número de recursos coordinando de manera global el conjunto de direcciones IP y números AS, y por último se tiene El Protocolo de Asignación de sistemas de numeración que lo hacen conjuntamente con los organismos de normalización.

"El equipo de IANA es responsable de los aspectos operativos de la coordinación de los identificadores únicos de Internet y mantener la confianza de la comunidad de proporcionar estos servicios de una manera imparcial, responsable y eficaz." Es así que en la figura 5 se puede observar el logo de esa organización. (IANA, 2015).

Figura 4. Organización de Asignación de Direcciones
Fuente: GALEON (2008). *ORGANIZACIONES REGENTES DE LOS DOMINIOS DE INTERNET*. Recuperado de http://galeon.com/losdominios/organizaciones.html

2.3.2 Regional Internet Registry (RIR)

Los Regional Internet Registry o Registros Regionales de Internet (RIR) son establecidos y autorizados por las comunidades regionales respectivas, teniendo en cuenta que deben ser reconocidos por la IANA, de tal manera que cada una de estas Organizaciones pueda servir y representar a grandes regiones geográficas.

[4] DNS: Sistema de Nombres de Dominio

En total a nivel mundial se tiene 5 Registros Regionales de Internet (RIR), los cuales se encuentran distribuidos de la siguiente manera y se los puede observar en la figura 5:

- African Network Information Centre (AFRINIC) para la Región de Africa.
- Asia-Pacific Network Information Centre (APNIC) para las Regiones de Asia y el Pacífico.
- American Registry for Internet Numbers (ARIN) para las regiones de Canadá, Islas del Caribe y Atlántico Norte, y los Estados Unidos.
- Latin American and Caribbean Internet Address Registry (LACNIC) para América Latina y parte del Caribe.
- RIPE Network Coordination Centre (RIPE) para Europa, el Oriente Medio y Asia Central.

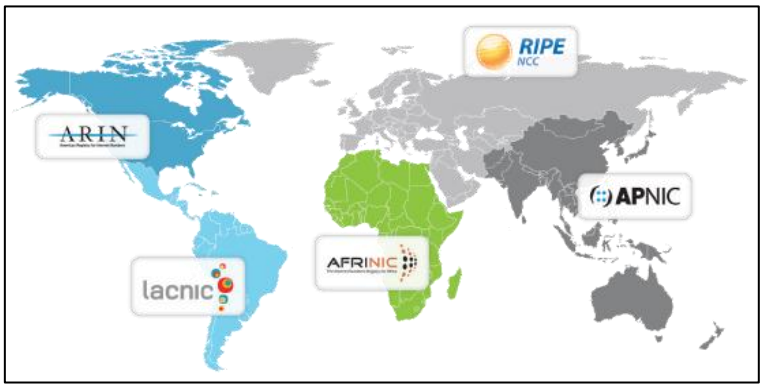


Figura 5. Distribución de RIRs a nivel mundial
Fuente: LACNIC (2015). *WORLD IPV6 LAUNCH*. Recuperado de http://ipv6.ar/quien.html

2.3.3 Local Internet Registry (LIR)

El Local Internet Registry (LIR) es un Registro de Internet local que asigna recursos de Internet a usuarios de los servicios de red que éste provee. Los LIRs son generalmente Proveedores de Servicios de Internet (ISP), cuyos clientes son principalmente usuarios finales y posiblemente pueden ser también otros ISPs.

2.3.4 Usuarios Finales

El usuario final es un suscriptor que tiene una relación de negocios o legal, de tal manera que pueda tener una misma entidad o ser una asociación de entidades con un ISP, que involucra al proveedor de servicios transportando el tráfico del usuario final.

2.4 Protocolo de Internet versión 4 (IPv4)

El Protocolo de Internet versión 4 (IPv4) es el responsable de transferir la información del usuario por la red, viene definido en el RFC 791 publicado en 1981, de esta manera IPv4 ha demostrado ser robusto, fácil de implementar y sobre todo interoperable.

Este protocolo presenta una función importante como es el direccionamiento; usándose las direcciones ubicadas en las cabeceras de internet para la transmisión de datagramas a cada uno de sus destinos por medio de la función de encaminamiento, la cual hace la selección de un camino para realizar la transmisión. (Boulevard, 1981).

2.4.1 Características de Protocolo IPv4

El Protocolo IPv4 es el más utilizado actualmente por los usuarios de Internet, ya que su funcionamiento y proceso no es complejo; éste es un protocolo no orientado a conexión, por lo tanto, es un protocolo no confiable.

IPv4 posee muchas características, las principales se listan a continuación:

- Establece un direccionamiento lógico de la red, de tal manera que los equipos puedan establecer un proceso de comunicación entre ellos.
- Es el encargado de entregar datagramas a través de la red, es decir que la entrega de paquetes la realiza mediante un proceso conocido como el mejor

esfuerzo; además, para el envío de información cuenta con un proceso conocido como encapsulado y desencapsulado.

Se puede decir que cada dirección contiene la información necesaria para que un paquete pueda ser enrutado a través de la red, las direcciones tanto origen como destino contienen una dirección de 32 bits (IPv4), cuando un paquete va a ser enviado, se debe tener en cuenta que el campo de dirección origen contiene la dirección IP del dispositivo, de tal manera que sepa quien envió el paquete y por último el campo destino debe contener la dirección IP del dispositivo que recibirá el paquete. (Boronat Seguí, 2013).

2.4.1.1 Cabecera IPv4

La cabecera que utiliza IPv4 contiene la información de control del protocolo dividiéndose en dos partes, una parte que es fija de 20 bytes existente en todos los datagramas y otra variable, múltiplo de 32 bits. La información que es transportada por el protocolo IP está contenida por los datos, teniendo por lo general la información que pasa por el nivel de transporte. (Miranda, 2014).

En la figura 6, se puede observar la cabecera IPv4 con cada uno de los campos.

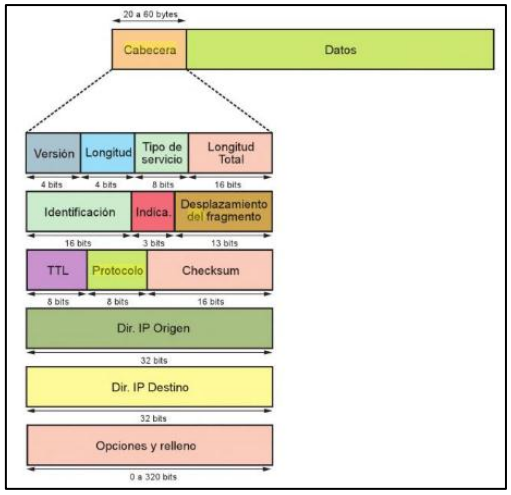


Figura 6. Cabecera IPv4
Fuente: CARLOS VALDIVIA MIRANDA (2014). *REDES TELEMÁTICAS.* Obtenido de https://goo.gl/nEuSvF

En donde:

Versión

Indica la versión del protocolo, como en este caso se está explicando sobre el protocolo IPv4, contendrá el valor 4.

Longitud de la cabecera

Indica la longitud de la cabecera en byte, se puede tener un máximo de 2^{16} con un total de 16 bytes.

Tipo de servicio

Indica el tipo de servicio que se ha solicitado siendo este un campo que no es muy utilizado, la IETF redefinió su uso como ECN (Explicit Congestion Notification) para enviar información sobre la congestión de la red.

Longitud total

En este campo se especifica el tamaño en bytes de todo el datagrama, de tal manera que se incluye a los datos. El tamaño máximo del datagrama es de 2^{16} con un total de 65.535 octetos.

Identificación

En caso de que exista fragmentación se lo utiliza para identificar el datagrama. La fragmentación se produce cuando la MTU de una red es menor que la de la red que originó el datagrama.

Indicadores

Los indicadores se utilizan únicamente para labores de fragmentación siendo un valor único asignado al datagrama por el emisor permitiendo identificar a que datagrama pertenece el fragmento.

Desplazamiento del fragmento

Se utiliza para identificar la posición de un fragmento respecto al datagrama original, si el valor es 0 indica que es el primer o único fragmento además es medido en unidades de 8 bytes.

TTL (Tiempo de Vida)

Indica el número de saltos de un datagrama. El origen especifica un valor inicial y cada vez que el datagrama atraviesa un router, este valor decrementa. El paquete es descartado el momento que el campo llega a 0 de tal manera que elimina el datagrama.

Protocolo

Indica el tipo de protocolo de nivel superior utilizado para de esta manera poder entregar un paquete, existen algunos tipos de protocolos como lo son TCP, UDP, ICMP, EGP, etc.

Checksum

Es un código de redundancia que se utiliza para determinar si se han producido errores en la cabecera, en caso de que el checksum de la cabecera no concuerde, se descarta el datagrama, de tal manera que se realiza un control de la información.

Dirección de Origen

Es aquella que identifica el origen de la comunicación, es la dirección IP origen del datagrama, siento la dirección que quiere realizar la comunicación.

Dirección de Destino

Es aquella que identifica el destino de la comunicación, es decir es la dirección destino del datagrama, cuando se requiere hacer una comunicación, la dirección destino es importante para conocer hacia dónde va dirigido el datagrama.

Opciones

El campo de Opciones IP se utiliza en caso de enviar información adicional.

2.4.2 Direccionamiento IPv4

El esquema de direccionamiento IP se puede decir que es de tipo jerárquico de tal manera que se tiene una porción destinada a la identificación de la red y una porción destinada a la identificación de un host de dicha red. Las direcciones IP constan de 4 campos separados por un punto entre cada uno de ellos, es decir tiene un total de 4 bytes de longitud, de tal manera que se puede representar tanto de manera decimal y como alternativa se tiene la binaria. Para tener una idea más gráfica se puede observar en la figura 7 como se encuentra representada una dirección IP de manera binaria.

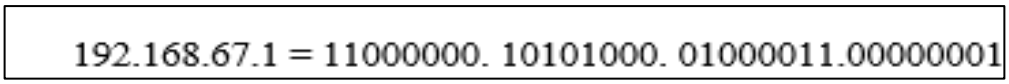


Figura 7. Representación dirección IPv4 por campos
Fuente: GONZALES (2012). *REDES TELEMÁTICAS.* Recuperado de: http://redestelematicas.com/direccionamiento-ipv4/

Anteriormente se ha mencionado que existen diferentes clases de direcciones IP, para lo cual se explicará de manera rápida la cantidad de direcciones que se puede tener en cada caso, se debe tener en cuenta que la que más utilizada es clase C como se observa en la figura 8.

Dirección	Número de redes	Número de hosts por red
Clase A:	126	16777214
Clase B:	16384	65534
Clase C:	2097152	254

Figura 8. Cantidad de Host y Redes en cada clase
Fuente: USERSHOP (2013). *REDES CISCO.* Recuperado de https://goo.gl/UVotJX

2.4.3 Ventajas del Protocolo IPv4

El protocolo IPv4 ha sido el más utilizado en los últimos años, tanto es así que su manejo y adaptamiento para los usuarios se ha hecho más sencillo, empezando por una gran

ventaja que la notación de sus direcciones es en decimal, siendo cuatro octetos que pueden ser representados como cuatro secuencias de números.

El uso de diferentes métodos de codificación ha sido importante en este protocolo de tal manera que la IETF ha adoptado el uso de: CIDR[5], VLSM[6] y NAT[7], CIDR y VLSM trabajando juntas para poder dar un mejor direccionamiento.

Las codificaciones utilizadas han hecho del protocolo una mejora bastante notable, tanto es así que por ejemplo CIDR que fue una mejora de VLSM permite tener varias subredes cada una con una cantidad de host distintos.

El protocolo IPv4 presenta dos tipos de enrutamiento siendo el uno estático y por otro lado dinámico, de tal manera que, para los Administradores de una Red sea más factible poder realizar el direccionamiento de una red, es decir si la red es demasiado grande lo mejor es utilizar un direccionamiento dinámico para así poder ahorrar tiempo y sobre todo economizar recursos en cuanto a su enrutamiento se refiere. (Juárez, 2015)

2.4.4 Problemas del Protocolo IPv4

La versión actual IPv4 presenta algunos problemas a pesar de ser el más utilizado en la actualidad a nivel mundial, sin embargo los problemas que presenta este protocolo se han ido identificando conforme los requerimientos de los usuarios han ido incrementando, es

---

[5] CIDR: Enrutamiento entre Dominios sin Clase

[6] VLSM: Máscaras de subred de tamaño variable

[7] NAT: Traducción de Direcciones de Red

decir, la cantidad de direcciones IPv4 han ido agotándose debido a la cantidad de dispositivos electrónicos que se tienen conectados a la red, por lo que el número de direcciones disponibles en IPv4 ya no va a satisfacer las necesidades de los usuarios.

Cuando se habla de agotamiento IPv4, se refiere a que se entra en una etapa de reservas donde las asignaciones son restringidas en tamaño y periodicidad. Dichas restricciones fueron definidas por las políticas que se presentaron para discusión de la comunidad en el Foro Público de Políticas. Gracias a estas políticas se provee una mejor administración de recursos para un agotamiento gradual de IPv4, así como también el permitir acceso a nuevos actores que quieran iniciar sus actividades de Internet en un futuro. Cuando se dice agotamiento, entonces, se refiere a que LACNIC no va a tener suficientes direcciones para cubrir las necesidades de direccionamiento IPv4 de sus miembros. (LACNIC, 2016)

La escasez de direcciones no es igual en todos los puntos de la red; por ejemplo, es casi inapreciable por el momento en Norteamérica, pero en zonas como en Europa y Asia, la situación es crítica. Este problema es creciente, debido principalmente al tremendo avance de la telefonía móvil celular y la inminente aparición de la tercera generación de comunicaciones móviles o UMTS[8]. Los móviles se convertirán en dispositivos siempre conectados a Internet y será necesario asignarlos una dirección IP fija y única.

En la actualidad se cuenta con un total de direcciones IPv4 de 1408512 disponibles, en la gráfica de la figura 9 que se presenta a continuación se puede observar el grado de decrecimiento de la cantidad de direcciones IPv4.

[8] UMTS: Sistema Universal de Telecomunicaciones Móviles

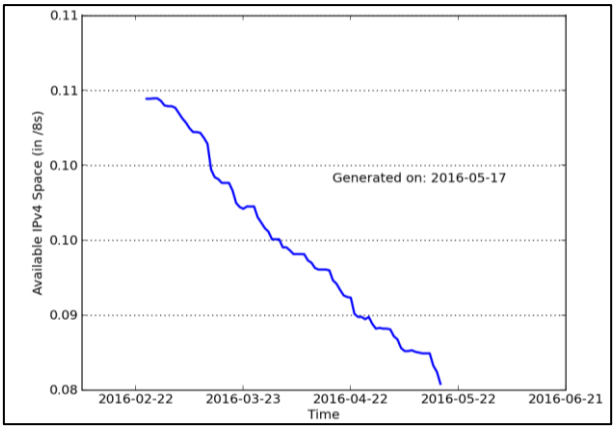


Figura 9. Cantidad de direcciones IPv4
Fuente: LACNIC (2016). *AGOTAMIENTO IPv4.* Recuperado de http://goo.gl/BDpXFw

Debido a las diferentes clases de direccionamiento de redes (clase A, B, C, D y E) cuando la cantidad de host crece a un número mayor del soportado por el tipo de red, entonces se presenta el problema de pasar a otro tipo de red o segmentar la red, es decir se necesita realizar ciertos tipos de mecanismos o configuraciones de codificación para poder abastecer esta cantidad de direccionamiento, no es un proceso muy complejo y que en la actualidad la mayoría de instituciones lo utilizan, sin embargo se puede requerir de uso de recursos no programados en la implementación de una red.

Debido a todos los problemas que se han venido dando en el Protocolo de Internet versión 4, se ha visto la necesidad de migrar a un nuevo protocolo conocido como Protocolo de Internet versión 6.

2.5 Protocolo de Internet IPv6

IPv6 surge con el crecimiento de cantidad de usuarios con IPv4, ya que con el agotamiento de las direcciones IPv4, el IETF ha comenzado un desarrollo de este nuevo protocolo en el año de 1993, de tal manera que ya se tenía prevista una limitación del

protocolo IPv4. A mediados del año 1995 se tuvo el diseño final de IPv6, que ha sido definido en el RFC 2460.

Steve Deering de Xerox PARC y Craig Mudge, han sido los diseñadores del nuevo protocolo que ha venido a reemplazar al IPv4. El nuevo protocolo que se quiere implementar no solo debía contar con un mayor número de direcciones IP, ya que se necesitaba conectar la mayor cantidad de dispositivos a la red global, sino tambien debería solucionar algunas falencias detectadas en su predecesor, de tal manera que, pueda satisfacer los requerimientos de algunas áreas de la industria que en la actualidad estaban comprometidas con su utilización. (Gerometta, 2011)

2.5.1 Definición de Protocolo IPv6

IPv6 (Internet Protocol Version 6) se ha diseñado para poder manejar la tasa de internet y realizar los requisitos de calidad de servicio, movilidad y seguridad de extremo a extremo. Es una evolución del protocolo IPv4, pero no posee ningún cambio del mismo, ya que las funciones se mantienen simplemente fueron mejoradas y las funciones que ya no tienen validez fueron eliminadas, cabe mencionar que como una característica importante es la reducción de tablas de ruteo. En la actualidad forma parte del soporte IP o IPng (IP siguiente generación) que incluye en los principales sistemas operativos del ordenador.

El servicio que proporciona a los usuarios y proveedores puede ser actualizado independientemente, sin tener que coordinarse entre sí. El mejoramiento del IPv4 al IPv6 son las direcciones IP que se alargan de 32 a 128 bits.

Para poder seguir un modelo de IPv6 se debe establecer reglas de tres tipos:

- Unicast (de un host a otro)
- Anycast (de un host a un host más cercano)
- Multicast (de un host a múltiples host)

IPv6 es aquel que permite extensiones para un paquete que especifique un mecanismo para autenticar su origen, de tal manera que, se pueda garantizar la integridad e intimidad de datos. Además, optimiza el encabezado lo que causa que sea más eficiente en la comunicación de sistemas de comunicaciones. Incluso provee nuevas funcionalidades como autentificación y seguridad. Este organiza cada datagrama como secuencia de encabezados proseguida de datos.

2.5.2 Características del Protocolo IPv6

Existen algunas características dentro de IPv6, entre las cuales se puede mencionar que; IPv6 cuenta con direcciones más largas, es decir, de tener un número formado por 32 bits (4,294,967,296 direcciones en IPv4), pasa a tener un número formado por 128 bits (aproximadamente 340 sextillones de direcciones), esto cuadruplica el tamaño de bits para generar cada dirección viéndose beneficiada la cantidad de direccionamiento que IPv6 puede soportar.

Con esta cantidad de direcciones IP se puede abastecer tranquilamente a todas las necesidades que presentan los usuarios al querer acceder a la red Internet, de tal manera que, cada uno de los dispositivos electrónicos que cuenten con una característica para acceder a una red, podrá conectarse sin ningún problema, así mismo, en la actualidad se presenta nuevas situaciones y estudios como lo es el Internet de las Cosas en donde se busca que cada dispositivo eléctrico (cocina, refrigerador, etc) pueda conectarse a la red de tal manera que con diferentes factores de programación pueda pasar a ser un dispositivo inteligente, evitando al usuario realizar algunos trabajos extras el momento de poner en funcionamiento el dispositivo.

2.5.2.1 Notación IPv6

IPv6 cuenta con tres tipos de notaciones, de tal manera que, el nuevo formato para este protocolo queda estructurado por 8 grupos de cuatro dígitos hexadecimales con un tamaño de 16 bits, separados por dos puntos ":", por ejemplo:

ABCD:BEBE:1234:BEBE:ABCD:EF01:1234:5443

Como la dirección IPv6 es demasiado extensa, se puede encontrar también, grupos en los cuales cuentan con el valor cero, de tal manera que estos grupos de ceros pueden simplificar la notación indicando el caracter "::", esta notación indica que existe uno o más grupos de 16 bits de ceros, por ejemplo:

Para la dirección IPv6:

2001:1001:0000:0000:0000:0000:0000:DACA

Como ya se explicó anteriormente, se puede comprimir la dirección de tal manera que, se suprima los ceros haciendo que la notacion quede representada de la siguiente forma:

2001:1001**::**DACA

Es importante recalcar que el caracter "::" sólo puede aparecer una sola vez en toda la dirección, ya que si se utilizan dos o más, no se podría conocer el número de grupos que cuentan con ceros, por ejemplo, la siguiente dirección no es válida.

2001**::**1001**::**DACA

Otra manera de indicar los ceros del anterior ejemplo es reemplazando los cuatro dígitos de ceros por uno solo, como se puede observar a continuación:

2001:0448:0:0:0:0:0:2474

2.5.2.2 Formato de Encabezado

El formato de encabezado IPv6 se encuentra diseñado para minimizar el procesamiento de la información, eliminando campos que no eran necesarios y consumían memoria y procesador en el protocolo IPv4, así como algunas opciones que eran utilizadas sólo en procesos específicos y que rara vez son utilizados, pero sí son procesados en cada salto del paquete, IPv6 no suprime por completo las opciones, sino más bien las agrega cuando sean necesarias en forma de extensiones.

La cabecera de IPv6 se encuentra en los primeros 40 bytes (tamaño fijo) del paquete, en el que están las direcciones de origen y destino con 128 bits cada una, de tal manera que tendría el doble de tamaño con la que cuenta la anterior versión. (Pérez Nava Juan Carlos, 2011)

Anteriormente se manejaban 12 campos en la cabecera del protocolo, como ya se mencionó para el nuevo protocolo solo se usan 8 campos teniendo el nuevo formato de cabecera como muestra la figura 10:

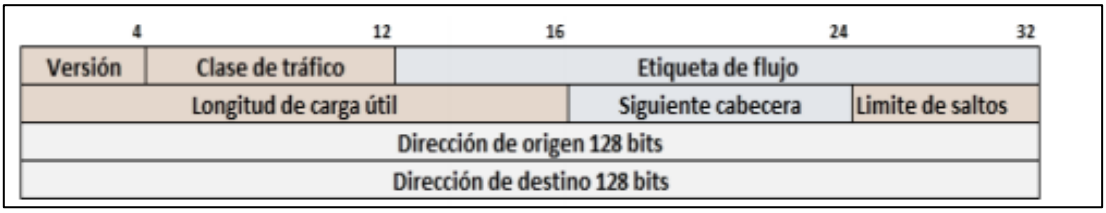


Figura 10. Formato de cabecera IPv6
Fuente: DENNYS R (2013). *CABECERA IPv6.* Recuperado de http://goo.gl/vD2oiO

A continuación, se dará una breve explicación de cada uno de los campos de la cabecera IPv6 de tal manera que se tenga una idea concisa del concepto de cada uno de ellos.

Versión

Como en el caso de IPv4 simplemente identifica el protocolo para este caso será 6.

Traffic Class o Clase de Tráfico: 8 bits

El campo clase de tráfico se utiliza para identificar y distinguir las diferentes clases o prioridades de los paquetes IPv6.

Flow Label o Etiqueta de flujo: 20 bits

La información que contiene este campo por el momento es experimental y se usa para aprovechar las ventajas de una subred de datagramas y una subred de circuitos virtuales, ya que se creará una pseudoconexión entre el origen con el destino para que exista un flujo continuo de datos, a su vez aprovechando las tablas de ruteo permitiendo una flexibilidad para establecer un camino.

Payload Length o Longitud de carga útil: 16 bits

Indica la longitud del paquete en bytes, es decir que indica la longitud de los datos o información que siguen a la cabecera, incluyendo las cabeceras de extensión (extension header), la máxima longitud puede ser de 65.536 bytes o 2^16 posibilidades.

Next Header o Encabezado siguiente: 8 bits

Este campo indica qué cabecera de extensión sigue a la cabecera principal.

Hop Limit o Límite de saltos: 8 bits

Se encarga de evitar que los paquetes se queden permanentemente en la red, delimitando un tiempo de vida por “saltos” que debe realizar el paquete para llegar a su destino, en cada salto que realiza el paquete se decrementa una unidad, en caso de que el valor llegue a 0, se dice que éste se ha descartado.

Source Address o Dirección de origen: 128 bits

Contiene la dirección desde donde es enviada la información, es decir indica el origen del paquete dentro del formato de IPv6 de 128 bits.

Destination Address o Dirección de destino: 128 bits

Contiene la dirección hacia donde es enviada la información, es decir indica el destino del paquete dentro del formato de IPv6 de 128 bits.

2.5.2.3 Cabeceras de Extensión de IPv6

La información adicional es codificada en cabeceras, de tal manera que, es colocada en el paquete entre la cabecera IPv6 y la de la capa transporte. Las extensiones de cabeceras son identificadas por un valor distinto en el campo siguiente cabecera. Las cabeceras de extensión pueden ser opcionales siendo éstas codificadas aparte.

Las cabeceras de extensión tienen una longitud múltiplo de 8 bits como se muestra en la figura 11, cuando se tiene más de una cabecera de extensión en un mismo paquete, existen diferentes cabeceras de extensión que a continuación se explicará cada una de ellas.

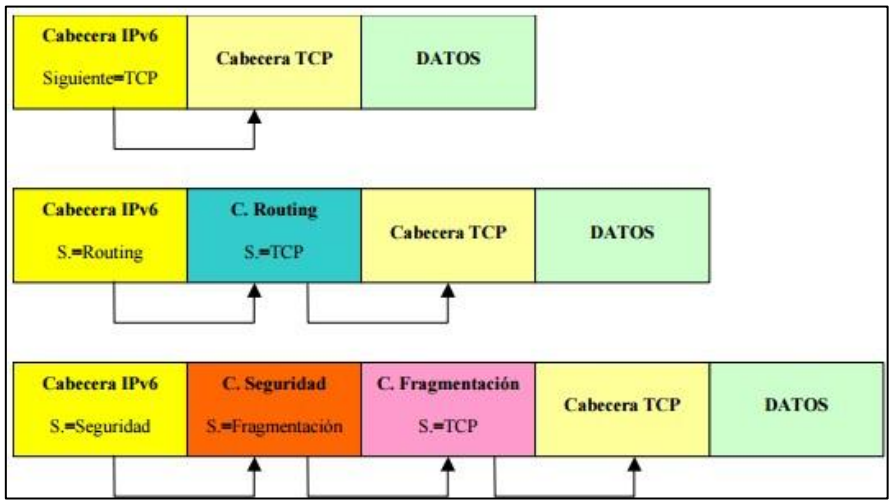


Figura 11. Cabeceras de Extensión
Fuente: S6S (2014). *EL PROTOCOLO IPv6* Recuperado de http://goo.gl/358NgF

Cabecera de Encaminamiento (Routing Header)

Esta cabecera se utiliza en el encaminamiento de origen, contiene una lista de direcciones de todas o de algunas pasarelas a lo largo de la ruta deseada. El datagrama que se

enruta de una puerta a la siguiente se modifica de acuerdo a la dirección destino que contiene la cabecera.

Cabecera de Fragmentación (Fragment Header)

En el origen se fragmenta la información de tal manera que los routers no intervendrían en esa tarea, esta cabecera se utiliza solo cuando los datos originales no tienen espacio en la unidad de transferencia máxima de cualquiera de las redes de la ruta. (Lahera Pérez J. A., 2012).

Cabecera de nodo-por-nodo (Host-by-Host Options Header)

Este tipo de cabecera se emplea en opciones de procesado de los paquetes que demandan un tratamiento salto a salto, es decir transporta la información que debe ser examinada por cada uno de los dispositivos de encaminamiento a lo largo de la ruta que sigue el paquete en donde la carga útil supere los 2^{16} octetos. (Boquera, 2003)

Cabecera de Autenticación (Authentication Header)

Contiene información para verificar la autenticación de la mayor parte de los datos del paquete, en esta cabecera se puede definir quien envió la información, es decir el origen del envío de información.

Cabecera de Opciones de Destino

La información que es transmitida solo será examinada por el destino, de tal manera que las otras cabeceras no tendrán que verificar nada, haciendo que las otras cabeceras simplemente dejen pasar la información.

2.5.3 Direccionamiento IPv6

De acuerdo al direccionamiento del Protocolo actual se puede encontrar tres tipos de direcciones de tal manera que se las explicará a continuación:

2.5.3.1 Direcciones Unicast o Unidifusión

Este tipo de direcciones son aquellas que identifican una única interfaz, es decir que los paquetes enviados a una dirección unicast, se entregan solo por la dirección identificada.

Dentro de las direcciones Unicast se puede encontrar tres tipos de direcciones que se las mencionará a continuación:

Local de Enlace

En estos tipos de enlace se puede identificar las interfaces dentro de un enlace de la misma red local, es utilizada para el descubrimiento de vecinos configurándose de manera automática.

Local de sitio

Para este tipo de direcciones, se dice que son aquellas que permiten encontrar interfaces dentro de un mismo sitio.

Global

En el caso de las direcciones global, son aquellas que permiten identificar una interfaz en el internet, siendo su equivalente las direcciones públicas dadas en IPv4.

2.5.3.2 Direcciones Anycast

Este tipo de direcciones permiten identificar un grupo o conjunto de interfaces, en donde los paquetes enviados a una dirección anycast, éste será entregado a cualquiera de las direcciones asociadas, existe un protocolo de media distancia en donde especifica que el

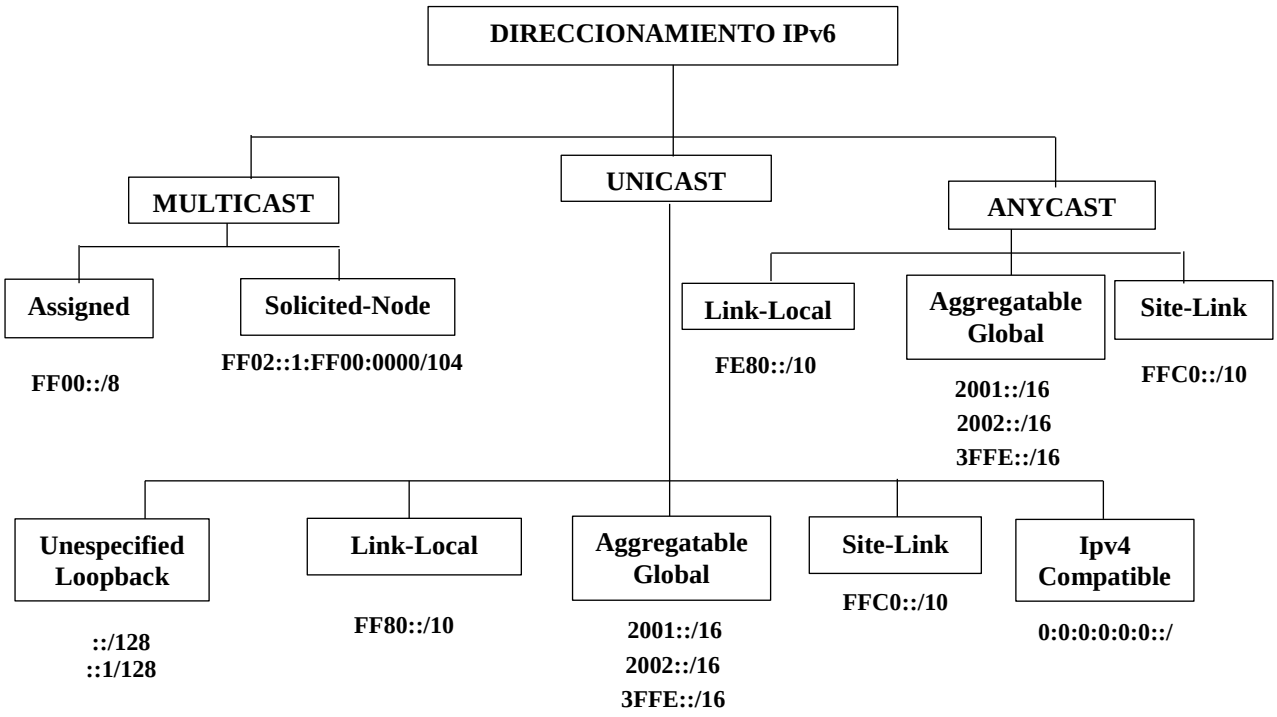
paquete será entregado al más cercano, además cabe recalcar que este tipo de agrupación no existe en IPv4.

2.5.3.3 Direcciones Multicast

Las direcciones multicast al igual que las direcciones anycast agrupan un conjunto de puntos finales de destino, con la diferencia de que cuando un datagrama es enviado a una dirección multicast, éste será entregado a un conjunto de destinos que forman parte de un mismo grupo, es decir no asocia el protocolo de media distancia.

A continuación, en la tabla 1 se muestra las direcciones de función destino.

Tabla 1. Direcciones en Función del Destino



Anteriormente se mencionó un poco sobre lo que es el alcance y del protocolo de media distancia, en realidad dentro de la clasificación de direcciones IPv6 también se puede encontrar en función del alcance como se observa en la figura 12, teniendo las siguientes:

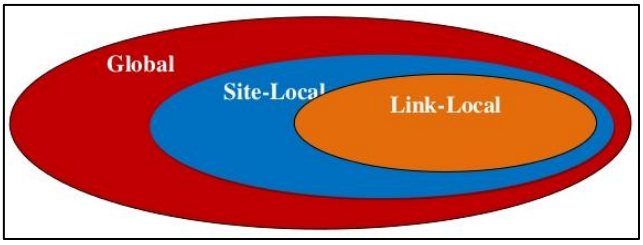


Figura 12. Direcciones IPv6 según el alcance
Fuente: UBIDIA A.(2007). *INTRANET IPv6.* Recuperado de http://goo.gl/QXaHPQ

Siendo:

- **Link-Local:** Estas tienen sentido solamente en el ámbito del enlace.
- **Site-Local:** Tienen sentido en el ámbito de una organización.
- **Global:** Estas en cambio son de manera global, abarcando las dos anteriores.

2.5.4 Enrutamiento IPv6

El enrutamiento IPv6 es un proceso tal y como se lo ha hecho en IPv4, en donde se mantiene una tabla de enrutamiento de manera actualizada, pudiendo ser ésta configurada manualmente o dinámicamente. Cuando se requiere enviar un paquete o información más allá de una red local, se requiere de enrutadores que verifican la dirección destino del paquete IPv6, buscando el prefijo que le corresponde dentro de su tabla de enrutamiento. Cuando el prefijo es encontrado, se envía el paquete a un nuevo nodo conocido como el siguiente salto, se repite el mismo proceso planteado anteriormente de tal manera que llegue a su destino, en caso de que el prefijo no sea encontrado, el paquete es desechado.

2.5.4.1 Enrutamiento Estático

Las rutas estáticas son utilizadas para hacer el enrutamiento forzado de algunos prefijos a través de enrutadores específicos. Cuando la configuración del enrutamiento es de

manera estática, estas tienen la mayor preferencia en una tabla de enrutamiento sobre las rutas aprendidas por los protocolos dinámicos, es decir siempre que exista en una red configurada los dos tipos de enrutamientos, la lógica de la topología será utilizar primero el enrutamiento estático.

Las rutas estáticas contienen la dirección IP del enrutador y el prefijo del paquete que va a ser enrutado, es conocido como el siguiente salto, existe una ruta estática que viene por defecto en IPv6 que es "::/0". Es importante mencionar que este tipo de enrutamiento no es conveniente en redes grandes debido a que si se hace un cambio de direccionamiento se puede tener problemas y sobre todo requeriría demasiado tiempo en poder actualizar las tablas de enrutamiento. (Cal, 2009)

2.5.4.1 Enrutamiento Dinámico

El enrutamiento dinámico se lo realiza por medio de mensajes de actualización, esta información se la procesa en las tablas de enrutamiento, siendo el enrutamiento dinámico el más utilizado para la implementación en redes grandes. Se tiene dos protocolos para el enrutamiento dinámico que son IGP y EGP.

Protocolo de Gateway Interior (IGP)

Se utiliza para el enrutamiento dentro de un sistema autónomo. También se lo denomina "routing interno de AS". En las diferentes organizaciones, instituciones e incluso los proveedores de servicios utilizan un IGP en sus redes internas. Dentro del Protocolo IGP se tiene los siguientes protocolos de enrutamiento dinámico:

RIP Next Generation (RIPng)

Este protocolo es utilizado generalmente en redes de tamaño mediano, en general mantiene las características de RIPv2 utilizado en IPv4, con algunas mejoras, ya que utiliza el algoritmo de Bellman-Ford para el vector distancia, el cual se basa en un intercambio de información entre routers para poder encontrar la ruta más adecuada de manera automática, las actualizaciones en su tabla de enrutamiento se lo hace cada 30 segundos, además posee métricas fijas y tiene un alcance de saltos con un máximo de 15 saltos, es basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

RIPng solo podrá ser implementado en routers, en cada router se incluirá una entrada para cada destino accesible por el sistema, teniendo algunos parámetros importantes en cada una de las entradas como son: El prefijo IPv6 de destino, la dirección IPv6 del siguiente router y la ruta para llegar a él, un indicador relativo al cambio de ruta y varios contadores asociados con la ruta. (Rivera, 2013)

Cada entrada de la tabla de enrutamiento contiene la siguiente información:

- El prefijo IPv6 al cual se requiere llegar (destino).
- Una métrica representando el número de saltos máximo que se tiene desde el router hacia su destino.
- La dirección IPv6 del siguiente router o siguiente salto y la ruta hacia el destino.
- Una bandera para indicar si existe un cambio de ruta.
- Varios contadores asociados con la ruta.

OSPFv3 (Open Shortest Path First Version 3)

OSPFv3 es un protocolo de enrutamiento de IPv4 e IPv6 que se describe en el RFC 5340. Es un protocolo de estado de enlace que se lo desarrolló en 1988 por la IETF en oposición a un protocolo de vector de distancia. La función de este protocolo es responder de manera muy rápida a todas las actualizaciones o cambios que se vayan desarrollando en la red, los protocolos de estado de enlace toman decisiones de enrutamiento basado en los estados de los enlaces que conectan las máquinas de origen y de destino. El estado de un enlace es una descripción de la interfaz y su relación con sus dispositivos de red vecinos.

La información de interfaz incluye el prefijo IPv6 de la interfaz, la máscara de red, el tipo de red; esta información se propaga en varios tipos de anuncios de estado de enlace (LSA). La colección de un dispositivo de datos de LSA se almacena en una base de datos de estado de enlace. El contenido de la base de datos, cuando se somete al algoritmo de Dijkstra, resultan en la creación de la tabla de enrutamiento OSPF. La diferencia entre la base de datos y la tabla de enrutamiento es que la base de datos contiene una colección completa de los datos en bruto; la tabla de enrutamiento contiene una lista de los caminos más cortos a destinos conocidos a través de los puertos de interfaz de dispositivo específicas. (CISCO, IP Routing: OSPF Configuration Guide, Cisco IOS Release 15SY, 2010).

Existen algunas similitudes entre OSPFv2 y OSPFv3 ya que muchos de los algoritmos son los mismo, haciéndose algunos cambios en OSPFv3, principalmente se ha manejado el aumento de tamaño de la dirección en IPv6 haciendo que se ejecute directamente en IPv6. Se tiene algunas características semejantes que se las conocerá a continuación:

Tipos de paquetes en OSPFv3

- **Hello:** Se identifican con el tipo 1 siendo enviados de manera periódica en cada una de las interfaces de la red de tal manera que se pueda establecer y mantener vecindades.
- **Data Base Description DBD:** Los paquetes DBD son identificados con el tipo 2. Estos son utilizados en el establecimiento de la adyacencia, conteniendo y describiendo la base de datos de la topología.
- **Link State Request LSR:** Son de tipo 3, una vez que se culminó con el intercambio de paquetes con DBD con un router vecino, los LSR son intercambiados para de esta manera poder actualizar la información de rutas.
- **Link State Update LSU:** Son de tipo 4, la función de estos paquetes es aplicar el envío de los LSR llevando cada LSU un grupo de paquetes a un salto más allá de su origen. (CISCO, 2013)

EIGRP para IPv6

EIGRP (Enhanced Interior Gateway Routing Protocol) para IPv6. Este protocolo es una versión mejorada del protocolo IGRP que fue desarrollada por Cisco. Es un protocolo basado en el vector distancia mejorada que trabaja con Diffused Update Algorithm (DUAL), éste permite calcular el trayecto más corto hacia un destino que se encuentre dentro de la red, EIGRP trabaja de la misma manera que se lo hace en IPv4 de tal manera que pueden ser configurados y además ser mejorados por separado. (CISCO, 2015)

EIGRP posee una rápida convergencia ya que cuando un router ejecuta EIGRP, guarda en sus tablas de enrutamiento a sus vecinos para que de esta manera puedan adaptarse de manera rápida a los cambios de la red. En caso de que una ruta no sea apropiada en la tabla de enrutamiento local y no exista una copa de seguridad apropiada en la tabla de

topología, el protocolo solicita a sus vecinos que descubran una nueva alternativa, de manera que se propaga la nueva ruta hasta determinar que ya no existe una ruta alternativa.

Además, EIGRP envía actualizaciones parciales desencadenadas en lugar de hacerlas periódicamente. Estas actualizaciones se envían únicamente cuando la ruta o la métrica de una ruta cambia. Una de las ventajas que posee este protocolo es que contiene la información solo del enlace que se cambió en lugar de toda la tabla de enrutamiento, haciendo que se consuma significativamente una menor cantidad de ancho de banda.

El proceso de enrutamiento de EIGRP es una función de la capa transporte. El paquete que transporta la información tiene el número de protocolo 88 en su cabecera IP, este proceso se lo realiza de la misma manera como en el Protocolo de Control de Transmisión (TCP), que tiene como número de protocolo 6 y UDP con un número de protocolo 17, tal y como se puede observar en la figura 13.

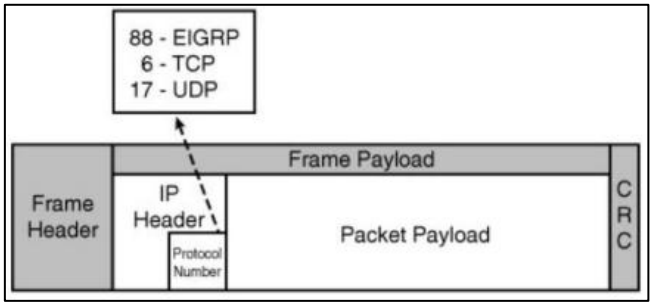


Figura 13. EIGRP para IPv6 con número de protocolo
Fuente: CISCO.(2011). *EIGRP IPv6.* Recuperado de https://goo.gl/FHAbaX

El protocolo EIGRP para IPv6 no realiza una sumarización automática como es en el caso de IPv4. Para la configuración en equipos Cisco se debe utilizar la palabra IPv6 antes del comando. (Calahorrano, 2014)

IS-IS para IPv6

Es un protocolo de encaminamiento que ha sido diseñado para soportar el protocolo CLNP (Connection Less Network Protocol), siendo éste un protocolo de la capa de red similar a IP. Actúa de manera directa sobre la capa Enlace, siendo independiente de la capa 3 que se ha utilizado, de esta manera se facilitó el trabajo para extender el soporte a otros protocolos de Red como IPv4 e IPv6 descrito en el RFC 5308.

IS-IS es un protocolo de Estado de Enlace como ya se lo había mencionado anteriormente que calcula la mejor ruta mediante el algoritmo SPF (Shorted Path First), permitiendo además dividir la red en distintas áreas, es así que se establecen dos niveles jerárquicos, Level 1 y Level 2, tal y como se observa en la figura 14.

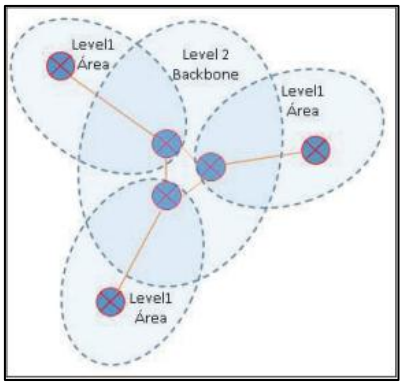


Figura 14. Niveles del Protocolo IS-IS
Fuente: CISCO.(2011). *IS-IS IPv6.* Recuperado de https://goo.gl/FHAbaX

Existen dos maneras de implementar el Protocolo IS-IS cuando se lo aplica tanto en IPv4 como en IPv6 al mismo tiempo.

Single Topology: IPv4 e IPv6 comparten el cálculo de rutas, de esta manera las interfaces tanto de IPv4 como de IPv6 deben ser las mismas.

Multitopology: Definido en el RFC 5120, para este caso el cálculo de las rutas es independiente para IPv4 e IPv6 habiendo la posibilidad de hacer dos topologías para los dos protocolos, a diferencia del anterior, las interfaces pueden ser diferentes.

IS-IS no utiliza un Router ID de 32 bits como los otros protocolos, para poder identificar de forma única los routers con IS-IS se usa un direccionamiento propio de tal manera que se conozca únicamente a los routers y las áreas de cada topología de red. (Baus, 2016)

Protocolo de gateway exterior (EGP)

Son protocolos de enrutamiento dinámico que se utilizan entre los sistemas autónomos, de tal manera que, puedan intercambiarse información de las rutas entre sí, de esta forma, cada sistema autónomo anuncia a los demás, los prefijos que tienen interiormente y además reenvían la información de prefijos de otros sistemas autónomos, aplicándose tanto para prefijos IPv4 como IPv6. El protocolo de gateway fronterizo (BGP) es el único EGP viable actualmente y es el protocolo de enrutamiento oficial utilizado por Internet, para la utilización en IPv6 hay que utilizar Multi Protocol BGP (MBGP) que soporta el envío de información de routing en IPv6 tales como unicast, multicast VPN de nivel 3, entre otros.

2.6 Mecanismo de transición

Las redes en la actualidad necesitan trabajar tanto en IPv4 como en IPv6, para esto ambos protocolos deben existir dentro de una red, de tal manera que, exista una coexistencia de protocolos o incluso se pueda trabajar como un IPv6 nativo, por esta razón se han

implementado tres tipos de mecanismos que poseen diferentes características, más adelante se detallará cada uno de dichos mecanismos.

Es importante tomar en cuenta que, para realizar la migración o transición, las aplicaciones IPv4 deben ser capaces de operar o funcionar con las aplicaciones IPv6, es decir que los equipos que se encuentran configurados con el protocolo antiguo, tengan las características necesarias para trabajar sin ningún problema con el nuevo protocolo.

2.6.1 Integración de un nuevo protocolo

Cuando se habla de integración de un nuevo protocolo se refiere a que tanto IPv4 como IPv6 deben aprender a convivir durante algunos años, ya que el proceso de transición no se lo puede realizar de un día para otro. Para esto se puede realizar la implementación del protocolo IPv6 como una actualización de software en nodos IPv4 actuales, o de igual manera poder transicionar paulatinamente diferentes servicios o aplicaciones dentro de una red.

La integración del nuevo protocolo ya se lo ha venido realizando hace algunos años atrás, pero es muy difícil saber cuándo las operadoras de Internet podrían migrar a IPv6 toda la red ya que la mayoría de operadoras utilizan IPv4, además en las instituciones públicas es un poco más difícil por cuanto muchos de los equipos que trabajan dentro de una red no soportan actualmente el nuevo protocolo, y poder adquirir equipos nuevos con características que soporten el nuevo protocolo sería muy costoso.

2.6.2 Coexistencia de Aplicaciones y Servidores

La estructura de red en La Internet está basada en el protocolo IPv4, un cambio inmediato de protocolo es inviable debido al tamaño y la proporción que posee la red, se ha

realizado una adopción de IPv6 pero que se debe implementar de una forma gradual, existiendo un periodo de transición y coexistencia entre los dos protocolos.

Las redes que posean IPv4 necesitarán comunicarse con las redes en IPv6, de igual manera las IPv6 con las IPv4, este proceso se lo puede realizar mediante el desarrollo de algunas técnicas que buscan mantener una compatibilidad de las redes que están desplegadas en IPv4 con el actual protocolo IPv6.

Tanto las aplicaciones como los servicios se verán obligados a utilizar los diferentes mecanismos que existen para tener coexistencia en ambos protocolos, es así que se pueden nombrar las diferentes técnicas o metodologías de transición que ayudarán a tener una coexistencia en la topología de la red. (Alonso, 2014)

2.7 Metodologías de transición

Existen tres tipos de metodologías o técnicas que se utilizan para la transición de los protocolos, cada una tiene sus propias características de acuerdo a las necesidades que requiera el administrador de la red para el funcionamiento: Doble Pila, Tunelling, DNS64 y NAT64.

2.7.1 Método de transición Doble-Pila

Se ha conseguido introducir IPv6 de una manera más fácil en una red, este proceso se lo conoce como “mecanismo de Doble Pila”, el cual está descrito en el RFC 2893. Por este método se logró que un host o un router alcancen ambas pilas de protocolos (IPv4 e IPv6) provistas como un componente del sistema operativo. Por lo tanto, las dos pilas envían y

reciben datagramas que pertenecen a ambos protocolos y así podrán comunicarse con cada nodo IPv4 e IPv6 en la red.

Para que tenga un buen funcionamiento este método, se lo realiza mediante la convivencia del campo que indica el tipo de “payload” para la capa de acceso al medio, ya que es distinta para ambos protocolos (0x0800 y 0x86dd, para IPv4 e IPv6 respectivamente), de esta manera los paquetes que llegan al host dual stack son desencapsulados y entregados al stack correspondiente dependiendo de dicho valor, dentro del sistema operativo. Existe un desafío en el despliegue de una red IPv6/IPv4 con pila doble, lo cual es la configuración del ruteo tanto para interno como para externo.

Se debe tomar en cuenta que cuando se está usando OSPFv2, el ruteo entre sitios antes de agregar IPv6 a la Capa 3 de la red, se debería hacer la transición a un protocolo que sea capaz de encaminar ambos protocolos IPv4 e IPv6 como IS-IS u OSPFv3 en vez de OSPFv2.

Otro de los desafíos es la interacción entre estos dos protocolos, y de saber cómo manejarla; suponiendo que una red con doble pila generalmente se vinculará con redes solo IPv4 externas. No existe un mecanismo de transición real usado en el escenario de doble pila, debido a que integra en sí mismo el soporte IPv6. Para construir un nodo de doble pila, solo es necesario habilitar en el sistema operativo el soporte IPv6, de este modo, el nodo se convierte en "híbrido" y dependiendo de la resolución de nombres, también conocido como DNS será el protocolo adecuado para cada requerimiento en particular.

2.7.2 Método de transición Tunelling

Este es un método que permite transmitir paquetes IPv6 por medio de una infraestructura que ha sido configurada en IPv4, este método cumple con encapsulamiento del contenido del paquete IPv6 en un paquete IPv4.

Para explicar el funcionamiento de este método se dice que el nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, poniéndolo en el campo de datos de un paquete IPv4, este paquete tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que conforma el túnel. Los nodos IPv4 del túnel encaminan el paquete, sin tener constancia de que el paquete IPv4 que están manejando contiene un paquete IPv6, es un proceso transparente. Finalmente, cuando el paquete llega al extremo del receptor IPv6 del túnel, determina que el paquete IPv4 contiene un IPv6 que debe ser desencapsulado.

Existen dos tipos de túneles que son tanto manuales como automáticos, los túneles manuales son cuando el paquete IPv6 es encapsulado en un paquete IPv4, de tal manera que sea encaminado sobre una infraestructura con un enrutamiento IPv4, siendo estos túneles punto a punto que deben ser configurados manualmente; los túneles automáticos pueden utilizar diferentes tipos de direcciones compatibles con IPv4, IPv6 o 6to4, es un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4, se pueden hacer configuraciones de routers y host con sus diferentes combinaciones.

2.7.3 Mecanismo DNS64 y NAT 64

El mecanismo NAT64 está definido en la RFC 6146, es una técnica para traducción de paquetes y puertos IPv6 a IPv4, permite simultáneamente el uso compartido de direcciones

IPv4. El DNS64 está definido en la RFC 6147, éste en cambio es una técnica auxiliar de mapeo para nombres de dominio, conocido como resolución de nombres de dominio, que se utiliza en conjunto con NAT64.

La utilización de NAT64 y DNS64 permite que los usuarios reciban únicamente direcciones IPv6 desde el proveedor, pero puedan acceder a dispositivos IPv4 en Internet, es así que parecería que todos los sitios y servicios en Internet fueran IPv6 y que todas las conexiones se originasen en un usuario IPv4 con una IP compartida.

Todas las direcciones IPv4 son mapeadas en prefijo IPv6 que es predefinido con un tamaño de 96 bits, para el mapeo se puede utilizar cualquier prefijo del proveedor, a pesar de que existe un bloque de direcciones reservado específicamente para ese fin, que viene dado en el RFC 6052 con 64:ff9b::/96. Un ejemplo sería si se tiene la dirección 192.168.2.1 en Internet se traduciría y mapearía a la dirección 64:ff9b::192.168.2.1 en la red del proveedor.

DNS64 funciona como un recursivo común, pero en caso de que el nombre consultado no tenga originalmente un registro, este registro se agrega a la respuesta, utilizando la misma regla de mapeo de direcciones definida para la traducción NAT64. Si la respuesta original llegase solamente con el registro, no habría más nada que hacer, ya que en la red del usuario solo hay conectividad IPv6.

Una de las desventajas del uso de DNS64 y NAT64 es que actualmente existen aplicaciones o equipos que no soportan IPv6, es por eso que si el equipo o la aplicación no puede trabajar en el nuevo protocolo IPv6 de nada serviría las técnicas de traducción, por esa razón, actualmente es un poco inviable la implementación inmediata de dicha técnica, a pesar

de que a un plazo no muy lejano se convierta ya en un uso común el nuevo protocolo. (Juárez, 2015)

2.8 Servicios y aplicaciones

La capa de Aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el tratamiento de los datos. Un único programa ejecutable debe utilizar los tres componentes e inclusive el mismo nombre. Por ejemplo: cuando se analiza “Telnet” se puede referir a la aplicación, el servicio o el protocolo.

2.8.1 Definición de Servicios y Aplicaciones

Los servicios y las aplicaciones como ya se lo había nombrado anteriormente se encuentran dentro de la capa Aplicación que se establece en el modelo de referencia TCP/IP, de esta manera tanto los servicios como las aplicaciones podrán ser transicionadas al nuevo protocolo, determinando que cada una de las aplicaciones o de los servidores acepten el nuevo protocolo, es decir que posean las características necesarias para trabajar sin ningún problema tanto en IPv4 como en IPv6.

2.8.2 Servicios y Aplicaciones que se pueden transicionar

Dentro del análisis que se ha realizado anteriormente se puede decir que las aplicaciones que serán transicionadas en la Universidad Técnica del Norte están dentro de un servidor como lo es el Chasis Blade.

El Chasis Blade cuenta con diferentes servidores ubicados en cada una de sus cuchillas, dentro de estos servidores se puede tener tanto aplicaciones, como servicios de tal manera que la transición puede realizarse ya sea de los servidores como de las aplicaciones, siendo factible poder transicionar los servicios que se encuentran dentro de cada uno de los servidores ubicados en el Chasis Blade.

Se ha determinado que tanto el Servidor de Aplicaciones como el servidor de la Base de Datos serán transicionados al nuevo protocolo, este análisis se lo ha podido verificar una vez que se estudió las características de los equipos, llegando a la conclusión de que el soporte para IPv6 es aceptable.

2.8.3 Sistema Informático Integrado de la Universidad Técnica del Norte

Los Sistemas Informáticos Integrados son herramientas de control y apoyo para la gestión de empresas haciendo que se pueda automatizar los procesos de negocio desde un enfoque global.

El Sistema Informático Integrado de la UTN está formado por un Portal Web de donde se desglosan tanto los portafolios académicos como los portafolios administrativos, en el portal web se tiene un planificador de recursos empresariales, de esta manera se tiene una organización de la Institución derivándose en diferentes gestiones como pueden ser: Académica, de Investigación, de Vinculación, de Seguridad, Administrativa, Financiera, Bienestar Universitario y Estado del Proyecto, la clasificación de estos portafolios se puede observar en la figura 15.

Figura 15. Sistema Informático Integrado UTN
Fuente: UTN (2016). SII. Recuperado de DDTI[9]

En la Gestión Académica se tiene todo el proceso de educación de tal manera que se encuentra la biblioteca con sus respectivas derivadas, es decir se puede encontrar diferentes sugerencias bibliográficas, la hemeroteca e incluso se tiene también un seguimiento de las tesis de los estudiantes que han culminado los estudios en dicha Universidad, facilitando de manera considerable el acceso a la información.

Dentro de este bloque también se tiene la Gestión de Investigación, en donde se realiza todos los procesos investigativos de la Universidad, además se tiene también la Gestión de Vinculación en donde se hace un seguimiento de todos los estudiantes egresados y graduados de la Universidad, y también las extensiones universitarias, de modo que se dé un seguimiento de las actividades que realiza el estudiante para complementar el proceso de titulación.

[9] DDTI: Dirección de Desarrollo Tecnológico e Informático

Se tiene la Gestión Administrativa en donde se realiza toda la estructura de una planificación estratégica para que lo planificado se pueda cumplir de acuerdo a un proceso establecido anteriormente, se dice que la parte administrativa es una de las gestiones más importantes de una empresa ya que se encarga de gestionar y controlar diferentes aspectos de la institución, por ejemplo, control de asistencia, roles de pago con sus respectivas nóminas, los convenios universitarios, entre otros.

La Gestión Financiera trata sobre el análisis y toma de decisiones financieras de una institución tratando de utilizar los recursos óptimos para la consecución de los objetivos, dentro de la Universidad se tiene el presupuesto, adquisiciones, recaudación, inventarios, etc.

El Bienestar Universitario es uno de los beneficios que mejor puede tener el estudiante debido a que se encuentra la situación socio-económica estudiantil, se cuenta con atención médica e incluso con atención odontológica.

Gestión de Seguridad se refiere a la parte de protección de la información que se tiene en la Universidad, realizando una auditoría de la Base de Datos para que no exista problemas en la infiltración de personas no autorizadas al manejo de cierta información que puede tener la Universidad.

Por último, se tiene el Estado del Proyecto que es en donde se tiene la inicialización, construcción, transición y producción; todo el proceso anteriormente descrito se lo realiza mediante una Intranet, teniendo todo en una Gestión Documental.

2.8.4 Aplicaciones en la Universidad Técnica del Norte

La Universidad Técnica del Norte cuenta con dos servidores de aplicaciones ubicados en dos cuchillas del Chasis Blade que se encuentra en el Data Center de la Dirección de Desarrollo Tecnológico e Informático, en el una de las cuchillas se encuentra el Servidor de Aplicaciones Forms y en otra el Servidor de Aplicaciones Reports.

El Servidor de Aplicaciones Forms se encuentra implementado con un Sistema Operativo Oracle Linux 5, el cual tiene un soporte sobre IPv6, es un software que forma parte de la suite Oracle Fusion Middleware agrupado dentro del área de herramientas de desarrollo.

El paquete de software está orientado a facilitar la creación de pantallas, de tal manera que utiliza la metodología RAD[10], en cual consiste en la mejora del despliegue de las formas en entornos web permitiendo una mejor interacción con la base de datos Oracle. Es un software que no requiere demasiada codificación ya que cuenta con muchos complementos y con la facilidad de integrar tanto JAVA como JavaScript obteniendo la creación de aplicaciones web robustas y con un tiempo moderado.

El Servidor de Aplicaciones Reports también se encuentra implementado con un Sistema Operativo Oracle Linux 5, este se encuentra categorizado dentro de las áreas de inteligencia de negocios, una de las carácterísticas es que cuenta con estabilidad en el servidor, es decir, que se crea una característica con la base de datos en caso de que existan algunos errores, tiene una alta disponibilidad ya que como cuenta con la base de datos, permite que las tareas programadas no se pierdan, y además tiene una facil administración ya

[10] RAD: Desarrollo Rápido de Aplicaciones

que dispone de una ventana de administración pudiendo visualizar gráficamente la cola de impresión, número de reportes programados, en ejecución, terminados, etc. (Cañar & Cordero, 2013)

Capítulo III

3. Análisis de requerimientos, implementación y pruebas del método de transición

En el presente capítulo se detalla el desarrollo práctico del proyecto, el cual consta de cuatro secciones: Situación actual, es el análisis de los equipos, requerimientos y una introducción de la manera que se encuentra constituida la red de la Universidad Técnica del Norte; Diseño, se necesita una metodología o procesos para cumplir con la transición de IPv4 a IPv6 de los servicios planteados en el presente proyecto, basado en el rango de direccionamiento IPv6 que dispone la Universidad, configuraciones de los servicios tanto de la Base de Datos, como de Aplicaciones y también el servicio de DNS64/NAT64 a nivel general; Implementación, aquí se tendrá toda la implementación del mecanismo Doble Pila, configuración del Equipo ASA 5520, equipos de conmutación de Core y Distribución hasta llegar hacia los usuarios finales, que se les asignará una dirección IPv6 para comprobar el método de transición planteado; Finalmente, se tendrá pruebas de funcionamiento de la transición propuesta en el presente proyecto de tesis, pudiendo tener acceso a los diferentes servidores tanto en IPv4 como en IPv6.

3.1 Situación actual

La Universidad Técnica del Norte (UTN) cuenta con un rango de direccionamiento IP asignado por CEDIA, en IPv4 dispone del rango 190.95.216.x/26 y en IPv6 tiene el rango 2800:68:19::/48 .

La UTN dispone de un equipo de borde de la red, el cual es suministrado y gestionado por el proveedor de Servicios de Internet “Telconet”, este equipo tiene habilitado el mecanismo de doble pila. El acceso a este equipo de borde por parte de la UTN es únicamente en modo lectura, es decir, no se tiene permisos para realizar cambios en la configuración del equipo.

La arquitectura de red de datos de la UTN cuenta con un Equipo Cisco 3750 conectado entre el equipo de borde de red y el equipo Cisco ASA 5520 que cumple las funciones de Firewall para la administración y control de red.

El switch Cisco 3750 tiene configurado vlans para el acceso al segmento de red Público proporcionado por Telconet, además tiene habilitado el mecanismo doble pila, así como enrutamiento estático, para permitir conectividad entre el segmento Público y el segmento de red privado con soporte para IPv6 e IPv4.

3.1.1 Topología de red de la UTN

La Universidad Técnica del Norte cuenta con un cuarto de equipos ubicado en el Edificio Central de la institución; en este cuarto de equipos es donde se interconectan cada una de las subredes de las dependencias de la Universidad. En la figura 16 se muestra la topología lógica de la red de datos del Cuarto de Equipos de la UTN; se debe mencionar que el direccionamiento IP utilizado en esta topología es ficticio por motivos de seguridad.

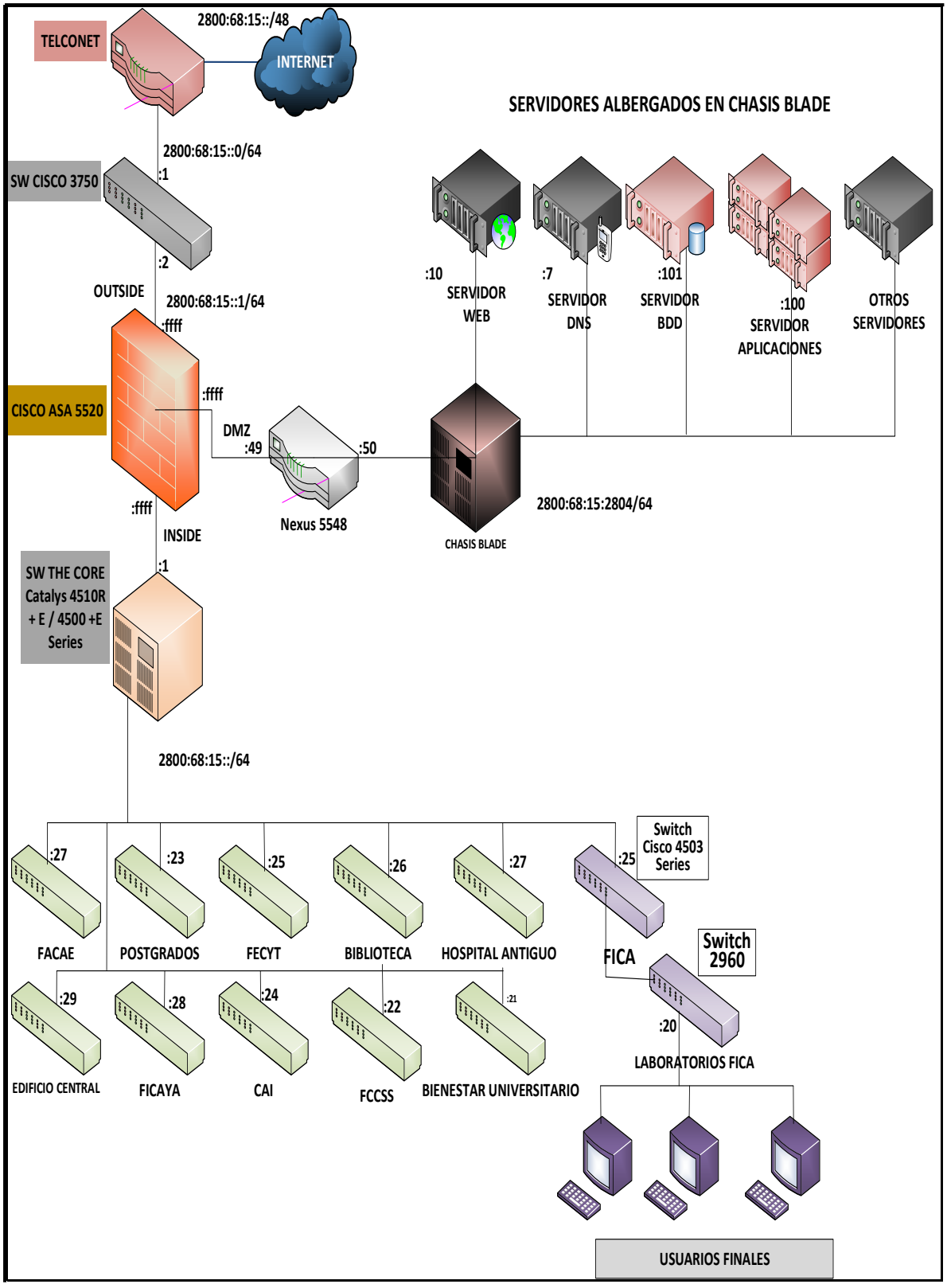


Figura 16. Topología Lógica de Red UTN
Fuente: Dirección de Desarrollo tecnológico e informático

3.1.2 Cuarto de equipos de la UTN

La Universidad Técnica del Norte posee equipos para brindar diferentes servicios de telecomunicaciones, este equipamiento se encuentra ubicado en la Dirección de Desarrollo Tecnológico e Informático, teniendo: Router de TELCONET, Switch 3750, Cisco ASA 5520, Switch de Core Catalyst 4510R + E / 4500 +E Series, Nexus 5548, Proliant BL460c G1, Servidor para DNS64 y NAT64 PROLIANT ML150; Además, cada una de las dependencias universitarias cuenta con equipos de conmutación, por ejemplo, en la Facultad de Ingeniería en Ciencias Aplicadas se tiene un Switch Cisco 4503 Series y en el Laboratorio de la FICA un Switch 2960.

A continuación, se describe de manera detallada, las características de uno de los equipos que serán manipulados directamente en el desarrollo del proyecto, teniendo en cuenta que, este equipo alberga servidores en cada una de sus cuchillas.

3.1.3 Análisis y características del Chasis Blade

En la figura 17 se observa un equipo servidor Hp Proliant BL460c G1, en donde se tiene algunos servidores de la red de la UTN, dentro de los cuales albergará a los servidores IPv6 tanto de Aplicaciones como el de la Base de Datos, cuenta con un soporte para poder operar en diferentes sistemas operativos como son Windows, Linux y NetWare.

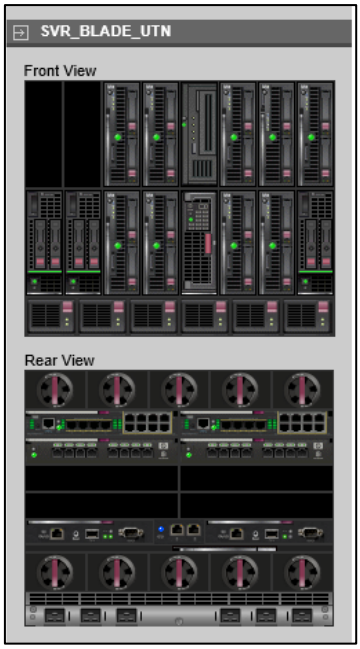


Figura 17. Servidor Blade Hp Proliant BL460c G1
Fuente: Departamento de Desarrollo Tecnológico e Informático UTN

3.1.3.1 Procesador

® 5300 procesadores de secuencia Hasta dos Quad-Core Intel® Xeon, tolera máximo dos procesadores de doble núcleo Intel ® Xeon ® 5100 o 5000.

Soporta hasta 1.86 GHz 1066 MHz FSB-2x4 MB de caché de nivel 2, 3,0 GHz 1333 MHz o 1066 MHz.

FSB-4 MB Nivel 2 la memoria caché o 3.2MV GHz Nivel 1 066 MHz.

FSB-2x2MB memoria caché de 2 Chipset Intel 5000P soporta hasta un Frente MHz Bus 1333.

3.1.3.2 Memoria

Hasta 32 GB de memoria, con el apoyo de los módulos DIMM (8) ranuras de PC2-5300 búfer completo a 667 MHz Soporte de memoria ECC avanzada.

Apoya el intercalado de memoria (2x1); la duplicación de memoria y la capacidad de reserva en línea.

3.1.3.3 Controlador de almacenamiento

Tiene integrado HP Smart Array E200i controlador RAID con 64 MB de caché (con batería opcional para respaldo caché de escritura con un actualizar a 128 MB de caché (BBWC)). Soporta RAID 0,1

3.1.3.4 Soporte de controlador interno

Hasta 2 unidades de disco duro de conexión en caliente (SFF) SAS o SATA pequeño factor de forma Controlador de red:

Dos puertos únicos (2) integrado NC373i multifunción adaptadores Gigabit Server Un (1) adicional 10/100 NIC dedicada a iLO 2 Gestión

3.1.3.5 Soporte Mezzanine

Dos (2) ranuras de expansión de E / S adicionales a través de tarjeta intermedia. Soporta hasta (2) tarjetas intermedias Doble puerto de canal de fibra Mezzanine (4 Gb) opciones para conectividad SAN (Elección de Emulex o QLogic). Ethernet opciones NIC Mezzanine para los puertos de red adicionales Adaptador de servidor Gigabit HP NC325m PCI Express de cuatro puertos para BladeSystem clase C Adaptador de servidor HP 1Gb NC326m PCI Express de doble puerto para BladeSystem clase C Adaptador de servidor Gigabit multifunción HP NC373m PCI Express de doble puerto 4X DDR InfiniBand (IB) Mezzanine (20 Gb / s) opciones para baja interconectividad servidor de latencia.

3.1.3.6 Soporte USB interno

Un (1) conector interno USB 2.0 para dispositivos clave de seguridad y llaves de unidad USB.

3.1.3.7 Administración

Dentro de la administración del equipo se tiene la siguiente característica para su administración que es Integrated Lights-Out 2 (iLO 2) Standard Hoja Edición (incluye KVM virtual y consola remota gráfica).

3.1.3.8 Características del Chasis Blade

El Switch interno del Chasis Blade es un Cisco 3320, en la actualidad no se puede realizar una actualización para el IOS del Protocolo IPv6, es decir que, para la administración del Switch solamente se lo puede hacer mediante el Protocolo IPv4, pero para conmutación trabaja sobre ambos protocolos, pudiendo ser administradas cada una de sus cuchillas siempre y cuando el sistema operativo de cada uno de los servidores albergados en el Chasis sea apto para trabajar en IPv6, ese es el caso tanto del servidor de aplicaciones como el servidor de base de datos.

3.1.3.9 Requerimientos para implementación IPv6

Entre los requerimientos que se necesitan para la implementación se tiene los siguientes: analizar los equipos que se van a transicionar, de tal manera que soporten el nuevo protocolo, una vez que se determine que los equipos puedan trabajar sobre el protocolo IPv6, se procede a determinar el proceso de configuración de cada uno de los equipos, detallando los diferentes lenguajes de configuración de cada uno de ellos. Cabe destacar que se ha realizado un análisis más profundo del Chasis Blade ya que es en este equipo en donde se alberga los servidores que se realizará la transición, también se ha realizado un análisis en el cuál se pueda determinar si cada uno de los equipos son o no son aptos para el proceso de transición, concluyendo que cada uno de los equipos si cumplen con las características necesarias para este proceso.

3.1.4 Aplicaciones a transicionar

Se ha realizado la investigación para poder realizar la Transición de las dos Aplicaciones que se van a implementar en donde se ha decidido que tanto el Servidor de Aplicaciones Form y el Servidor de Base de Datos, serán las elegidas para el proceso de transición, de esta manera a continuación se presenta las características que posee cada uno de estos servidores, teniendo en cuenta que en los dos casos se acepta IPv6.

3.1.4.1 Servidor de base de datos

El servidor de la base de datos se encuentra albergado en una de las cuchillas del Chasis BladeSystem c7000 Enclosure, este servidor soporta IPv6 ya que posee un sistema operativo Oracle Linux 5, por lo que no se tendría ningún problema el momento de realizar la transición de este servidor, tiene características que en la tabla 2 se las presenta.

Tabla 2. Información general de Servidor de Base de Datos

CARACTERÍSTICA	DESCRIPCIÓN
Sistema Operativo	Oracle Linux 5, tiene compatibilidad con el protocolo IPv6.
Alergue del Servidor	El servidor que alberga a la Base de Datos es el ProLiant BL460c G7
Número de Nodos o Servidores Actuales	1 Servidor
Versión de Base de Datos Actual	Oracle 11g R2
Memoria Actual	Cuenta con un espacio de memoria de 32GB
Número de Procesadores y Cores Actuales	1 Procesador Intel(R) Xeon(R) CPU E5620 2.40GHz - 4Cores

Tamaño de Base de Datos en Storage	Espacio Total 3.6 TB de los cuales se tiene usado 600GB
Esquemas de Alta Disponibilidad o Contingencia	No se dispone de equipos de contingencia

Fuente: Dirección de Desarrollo tecnológico e informático

3.1.4.2 Servidor de Aplicaciones Forms

El servidor de Aplicaciones Forms se encuentra albergado en otra de las cuchillas del Chasis BladeSystem c7000 Enclosure, este servidor soporta IPv6 ya que posee un sistema operativo Oracle Linux 5, a continuación, en la tabla 3 se presenta las características que posee este servidor.

Tabla 3. Información general de Servidor de Aplicaciones Forms

CARACTERÍSTICA	DESCRIPCIÓN
Sistema Operativo	Oracle Linux 5, tiene compatibilidad con el protocolo IPv6
Alergue del Servidor	El servidor que alberga a la Base de Datos es el ProLiant BL460c G7
Número de Nodos o Servidores Actuales	1 Servidor de Aplicaciones
Versión de IAS o Weblogic	Weblogic 11g
Versión de Forms	Forms 11 - Version 11.1.2.0.0
Memoria Actual de Equipo	40GB
Número de Procesadores y Cores Actuales	1 Procesador Intel(R) Xeon(R) CPU E5620 2.40GHz - 4 Cores

Tamaño de Base de Datos en Storage	Espacio Total 296 GB Instalación 174GB, Formas y Reportes 4GB
Esquemas de Alta Disponibilidad o Contingencia	No se dispone de equipos de contingencia

Fuente: Dirección de Desarrollo tecnológico e informático

3.1.4.3 Requerimientos de Transición de Servicios

Los dos equipos tienen las mismas características, de tal manera que serán implementados con el mismo sistema operativo. A continuación, se presenta en la tabla 4 si cada uno de los equipos que serán manipulados dentro del proceso de transición, soporta o no soporta IPv6:

Tabla 4. Requerimientos de Implementación de Transición IPv4 a IPv6

EQUIPO	REQUERIMIENTO
Servidor de Aplicaciones	Sistema Operativo Oracle Linux 6.8 ya cuenta con un soporte sobre IPv6 ya que el IOS soporta configuraciones sobre el nuevo Protocolo.
Servidor de Base de Datos	Sistema Operativo Oracle Linux 6.8 ya cuenta con un soporte sobre IPv6 ya que el IOS soporta configuraciones sobre el nuevo Protocolo
Proliant BL460c G1	Es un equipo que no tiene compatibilidad sobre IPv6 ya que no permite actualización del IOS, para la transición no hay problema que no soporte IPv6 ya que solo cumple como función de encaminamiento hacia los servidores albergados en su Chasis.
Cisco ASA 5520	Tiene compatibilidad sobre IPv6, estando configurado con el mecanismo de transición doble pila, permite redes de acceso de la Universidad.

Switch De Core Catalyst 4510R + E / 4500 +E Series	Es un equipo que está configurado mediante el mecanismo de transición doble pila, tiene compatibilidad con IPv6, además, permite la conectividad y acceso a las diferentes VLAN de la Universidad.
Nexus 5548	Se encuentra configurado con mecanismo doble pila, se encuentra conectado para salir desde al firewall. Tiene compatibilidad sobre IPv6.
Servidor para DNS64 y NAT64 PROLIANT ML150	Este es el equipo en donde se realizará la configuración tanto del DNS64 como del NAT64 permitiendo la traducción de direccionamiento IP como la resolución de nombres de dominio. Este equipo tiene una versión del sistema operativo que ya tiene compatibilidad con IPv6, por lo tanto, es apto para el funcionamiento de resolución de nombres y nateo de IPv4 e IPv6.
Switch Cisco 4503 Series	Tiene soporte sobre IPv6 y se encuentra configurado con metodología Doble Pila, es un equipo que se encuentra ubicado en la Facultad de Ingeniería en Ciencias Aplicadas.
Switch 2960	Equipo que trabaja sobre IPv6, se encuentra configurado con mecanismo Doble Pila.
Usuarios Finales	Equipos que pueden ser configurados con IPv6, ya que su tarjeta de red lo permite y tienen un IOS con este soporte.

Fuente: Dirección de Desarrollo tecnológico e informático

3.2 Diseño y configuración de servicios

Para el diseño y la configuración de servicios se definió cinco etapas, las cuales se dividen así: primero, se va a realizar una distribución y un direccionamiento tanto en IPv4 como en IPv6, segundo, la instalación de los servidores tanto para Base de Datos, para

Aplicaciones y además para el DNS64/NAT64; tercero, configuración del fichero de la interfaz de red del servidor de Base de Datos; cuarto, configuración del fichero de la interfaz de red del servidor de Aplicaciones; por último, la configuración de la interfaz de red del servidor DNS64/NAT64.

3.2.1 Distribución y Direccionamiento en IPv4 e IPv6

La distribución de subredes se encuentra segmentada por VLANs, con la finalidad de administrar de manera más eficiente cada una de las dependencias en la red de la UTN.

La información del direccionamiento IP solamente la debe conocer el administrador de red de la Universidad, siendo así, la información es confidencial, es por eso que en la tabla 5 se muestra la Distribución del Direccionamiento IPv4 ficticio.

Tabla 5. Direccionamiento IPv4 y segmentos de VLANs de la red UTN

DISTRIBUCIÓN DE SUBREDES (VLANS) IPv4					
N°	DESCRIPCIÓN	VLAN	DIRECCIÓN IP	PREFIJO	GATEWAY
1	EQUIPOS-ACTIVOS	1	192.168.1.0	/24	192.168.1.1
2	DMZ	2	10.5.7.0	/24	10.5.7.1
3	EQUIPOS-ACTIVOS-WIRELESS	3	192.168.3.0	/24	192.168.3.1
4	CCTV	4	192.168.4.0	/24	192.168.4.1
5	RELOJES-BIOMETRICOS	5	192.168.5.0	/24	192.168.5.1
6	TELEFONIA-IP-ELASTIX	6	192.168.6.0	/24	192.168.6.1
7	TELEFONIA-IP-CISCO	7	192.168.7.0	/24	192.168.7.1
8	AUTORIDADES	8	192.168.8.0	/24	192.168.8.1
9	DDTI	9	192.168.9.0	/24	192.168.9.1
10	FINANCIERO	10	192.168.10.0	/24	192.168.10.1
11	COMUNICACION-ORGANIZACIONAL	11	192.168.11.0	/24	192.168.11.1
12	ADMINISTRATIVOS	12	192.168.12.0	/24	192.168.12.1
13	ADQUISICIONES	13	192.168.13.0	/24	192.168.13.1
14	U-EMPRENDE	14	192.168.14.0	/24	192.168.14.1
15	AGUSTIN-CUEVA	15	192.168.15.0	/24	192.168.15.1
16	BIENESTAR-DOCENTES	16	192.168.16.0	/24	192.168.16.1
17	BIENESTAR-ADMINISTRATIVOS	17	192.168.17.0	/24	192.168.17.1
18	PROYECTO-INDIA	18	192.168.18.0	/24	192.168.18.1

19	NATIVA	19	-----		-----
20	FICA-LABORATORIOS	20	192.168.20.0	/24	192.168.20.1
21	FICA-WIRELESS	21	192.168.21.0	/24	192.168.21.1
22	FICA-ADMINISTRATIVOS	22	192.168.22.0	/24	192.168.22.1
23	FICAYA-LABORATORIOS	23	192.168.23.0	/24	192.168.23.1
24	FICAYA-ADMINISTRATIVOS	24	192.168.24.0	/24	192.168.24.1
25	FECYT-LABORATORIOS	25	192.168.25.0	/24	192.168.25.1
26	FECYT-ADMINISTRATIVOS	26	192.168.26.0	/24	192.168.26.1
27	FACAE-LABORATORIOS	27	192.168.27.0	/24	192.168.27.1
28	FACAE-ADMINISTRATIVOS	28	192.168.28.0	/24	192.168.28.1
29	FCCSS-LABORATORIOS	29	192.168.29.0	/24	192.168.29.1
30	FCCSS-ADMINISTRATIVOS	30	192.168.30.0	/24	192.168.30.1
31	POSTGRADO-LABORATORIOS	31	192.168.31.0	/24	192.168.31.1
32	POSTGRADO-ADMINISTRATIVOS	32	192.168.32.0	/24	192.168.32.1
33	CAI-LABORATORIOS	33	192.168.33.0	/24	192.168.33.1
34	CAI-ADMINISTRATIVOS	34	192.168.34.0	/24	192.168.34.1
35	BIBLIOTECA-LABORATORIOS	35	192.168.35.0	/24	192.168.35.1
36	BIBLIOTECA-ADMINISTRATIVOS	36	192.168.36.0	/24	192.168.36.1
37	COLEGIO-LABORATORIOS	37	192.168.37.0	/24	192.168.37.1
38	COLEGIO-ADMINISTRATIVOS	38	192.168.38.0	/24	192.168.38.1
39	WIRELESS-DOCENTES	39	192.168.39.0	/24	192.168.39.1
40	WIRELESS-ADMINISTRATIVOS	40	192.168.40.0	/24	192.168.40.1
41	EDUROAM	41	192.168.41.0	/24	192.168.41.1
42	WIRELESS-EVENTOS1	42	192.168.42.0	/24	192.168.42.1
43	WIRELESS-EVENTOS2	43	192.168.43.0	/24	192.168.43.1
44	WIRELESS-ESTUDIANTES	44	192.168.44.0	/24	192.168.44.1
45	COPIADORA	45	192.168.45.0	/24	192.168.45.1
46	BANCO-PACIFICO	46	192.168.46.0	/24	192.168.46.1

Fuente: Dirección de Desarrollo tecnológico e informático

A continuación, en la tabla 6 se presenta el direccionamiento IPv6 de la red de la UTN, el tercer octeto de la dirección IPv4 tiene la misma asignación de dirección que el quinto hexteto de la dirección IPv6.

Tabla 6. Direccionamiento IPv6 y segmentos de VLANs de la red UTN

DISTRIBUCIÓN DE SUBREDES (VLANS) IPv6					
N°	DESCRIPCIÓN	VLAN	DIRECCIÓN IP	Prefijo	GATEWAY
1	EQUIPOS-ACTIVOS	1	2800:68:19:x:1::	/xx	2800:68:19:x:x::1
2	DMZ	2	2800:68:19:x:2::	/xx	2800:68:19:x::1
3	EQUIPOS-ACTIVOS-WIRELESS	3	2800:68:19:x:3::	/xx	2800:68:19:x:3::1

4	CCTV	4	2800:68:19:x:4::	/xx	2800:68:19:x:4::1
5	RELOJES-BIOMETRICOS	5	2800:68:19:x:5::	/xx	2800:68:19:x:5::1
6	TELEFONIA-IP-ELASTIX	6	2800:68:19:x:6::	/xx	2800:68:19:x:6::1
7	TELEFONIA-IP-CISCO	7	2800:68:19:x:7::	/xx	2800:68:19:x:7::1
8	AUTORIDADES	8	2800:68:19:x:8::	/xx	2800:68:19:x:8::1
9	DDTI	9	2800:68:19:x:9::	/xx	2800:68:19:x:9::1
10	FINANCIERO	10	2800:68:19:x:10::	/xx	2800:68:19:x:10::1
11	COMUNICACION-ORGANIZACIONAL	11	2800:68:19:x:11::	/xx	2800:68:19:x:11::1
12	ADMINISTRATIVOS	12	2800:68:19:x:12::	/xx	2800:68:19:x:12::1
13	ADQUISICIONES	13	2800:68:19:x:13::	/xx	2800:68:19:x:13::1
14	U-EMPRENDE	14	2800:68:19:x:14::	/xx	2800:68:19:x:14::1
15	AGUSTIN-CUEVA	15	2800:68:19:x:15::	/xx	2800:68:19:x:15::1
16	BIENESTAR-DOCENTES	16	2800:68:19:x:16::	/xx	2800:68:19:x:16::1
17	BIENESTAR-ADMINISTRATIVOS	17	2800:68:19:x:17::	/xx	2800:68:19:x:17::1
18	PROYECTO-INDIA	18	2800:68:19:x:18::	/xx	2800:68:19:x:18::1
19	NATIVA	19	-----	----	----
20	FICA-LABORATORIOS	20	2800:68:19:x:20::	/xx	2800:68:19:x:20::1
21	FICA-WIRELESS	21	2800:68:19:x:21::	/xx	2800:68:19:x:21::1
22	FICA-ADMINISTRATIVOS	22	2800:68:19:x:22::	/xx	2800:68:19:x:22::1
23	FICAYA-LABORATORIOS	23	2800:68:19:x:23::	/xx	2800:68:19:x:23::1
24	FICAYA-ADMINISTRATIVOS	24	2800:68:19:x:24::	/xx	2800:68:19:x:24::1
25	FECYT-LABORATORIOS	25	2800:68:19:x:25::	/xx	2800:68:19:x:25::1
26	FECYT-ADMINISTRATIVOS	26	2800:68:19:x:26::	/xx	2800:68:19:x:26::1
27	FACAE-LABORATORIOS	27	2800:68:19:x:27::	/xx	2800:68:19:x:27::1
28	FACAE-ADMINISTRATIVOS	28	2800:68:19:x:28::	/xx	2800:68:19:x:28::1
29	FCCSS-LABORATORIOS	29	2800:68:19:x:29::	/xx	2800:68:19:x:29::1
30	FCCSS-ADMINISTRATIVOS	30	2800:68:19:x:30::	/xx	2800:68:19:x:30::1
31	POSTGRADO-LABORATORIOS	31	2800:68:19:x:31::	/xx	2800:68:19:x:31::1
32	POSTGRADO-ADMINISTRATIVOS	32	2800:68:19:x:32::	/xx	2800:68:19:x:32::1
33	CAI-LABORATORIOS	33	2800:68:19:x:33::	/xx	2800:68:19:x:33::1
34	CAI-ADMINISTRATIVOS	34	2800:68:19:x:34::	/xx	2800:68:19:x:34::1
35	BIBLIOTECA-LABORATORIOS	35	2800:68:19:x:35::	/xx	2800:68:19:x:35::1
36	BIBLIOTECA-ADMINISTRATIVOS	36	2800:68:19:x:36::	/xx	2800:68:19:x:36::1
37	COLEGIO-LABORATORIOS	37	2800:68:19:x:37::	/xx	2800:68:19:x:37::1
38	COLEGIO-ADMINISTRATIVOS	38	2800:68:19:x:38::	/xx	2800:68:19:x:38::1
39	WIRELESS-DOCENTES	39	2800:68:19:x:39::	/xx	2800:68:19:x:39::1
40	WIRELESS-ADMINISTRATIVOS	40	2800:68:19:x:40::	/xx	2800:68:19:x:40::1
41	EDUROAM	41	2800:68:19:x:41::	/xx	2800:68:19:x:41::1
42	WIRELESS-EVENTOS1	42	2800:68:19:x:42::	/xx	2800:68:19:x:42::1
43	WIRELESS-EVENTOS2	43	2800:68:19:x:43::	/xx	2800:68:19:x:43::1
44	WIRELESS-ESTUDIANTES	44	2800:68:19:x:44::	/xx	2800:68:19:x:44::1
45	COPIADORA	45	2800:68:19:x:45::	/xx	2800:68:19:x:45::1
46	BANCO-PACIFICO	46	2800:68:19:x:46::	/xx	2800:68:19:x:46::1

Fuente: Dirección de Desarrollo tecnológico e informático

3.2.2 Instalación de Servidores

Los servidores instalados en el desarrollo del proyecto son: Base de Datos, Aplicaciones y DNS64/NAT64; a continuación, se tiene la instalación del Sistema Operativo con el que trabajan los servidores anteriormente mencionados.

3.2.2.1 Instalación de Linux Centos

Linux trabaja sobre una plataforma libre, no se requiere de permisos para la descarga ni para la instalación del sistema operativo, lo primero que se realiza es la descarga de la imagen IOS de Linux Centos en las versiones 5.5 y 6.5, y se lo genera en el medio de instalación.

Es importante tener en cuenta los requerimientos que se necesitan para la instalación de Linux Centos, puede ser un USB booteable, una unidad disco, en el cual se grabará la imagen IOS para proceder a la instalación en donde se levantarán los servicios DNS64/NAT64, el Servidor de Aplicaciones y el Servidor de la Base de Datos.

Los equipos servidores donde se alogaran los servicios, cumplen con las características que requiere Centos 6.5 y Centos 5.5 para ser instalados teniendo un procesador Quad-Core Intel® Xeon de 1,83 GHz, Memoria RAM de 16GB y un almacenamiento de 250 GB.

El procedimiento a detalle de la instalación de Linux Centos se presenta en el Anexo 1, es importante mencionar que tanto para Centos 5.5 como para 6.5, la instalación es similar; por lo que en el Anexo 1 se muestra solamente la instalación de Centos 6.5.

3.2.3 Configuración IPv6 del Servidor de Base de Datos

Como primer paso en la configuración del servidor, se debe asignar una dirección IPv6 en la tarjeta de red para esto se debe acceder al fichero mediante el comando *#nano /etc/sysconfig/network-scripts/ifcfg-eth0* como se muestra en la figura 18:

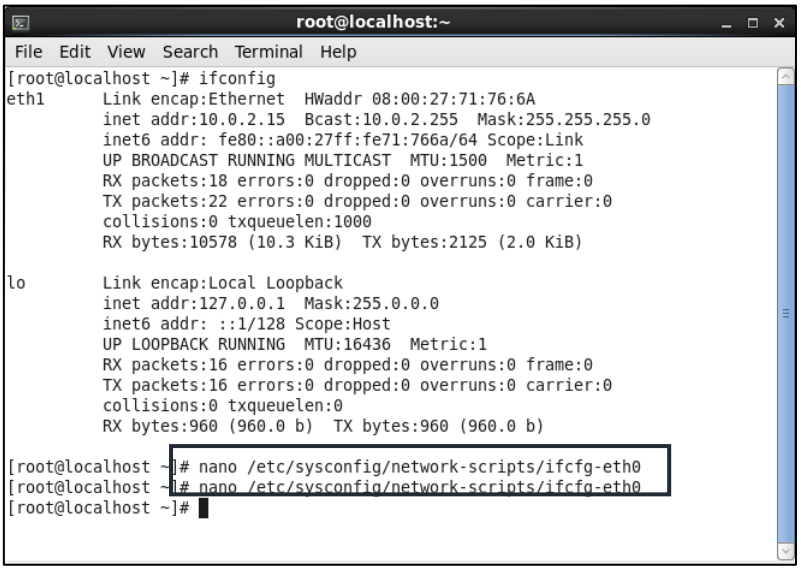


Figura 18. Ingreso Interfaz de Red
Fuente: Equipo servidor de Base de Datos

Una vez ingresado al fichero de configuración de red, se procede a asignar las direcciones IPv4 e IPv6 de interfaz para el servidor de la base de datos, tal como muestra la figura 19.

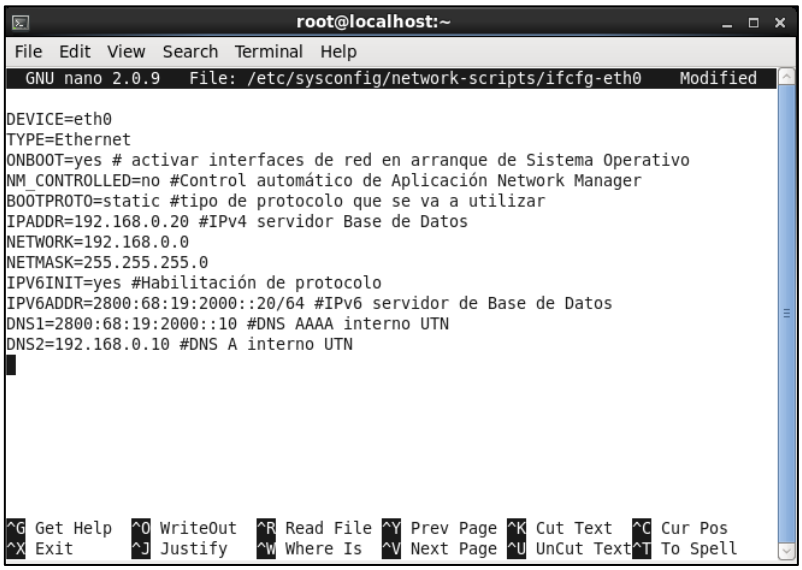


Figura 19. Configuración de Direcciones en interfaz de red
Fuente: Equipo servidor de Base de Datos

Es importante mencionar que se debe realizar la habilitación de los protocolos de internet en los cuales se va a trabajar, se ingresa al archivo de configuración de red, mediante el comando *#nano /etc/systemconfig/network, se habilita el protocolo IPv6 digitando NETWORKING_IPv6* seteado en YES como se observa en la figura 20; además, asignar la dirección del Gateway de Firewall en IPv4 y para IPv6 un Gateway por default asignado por el Administrador de red UTN.

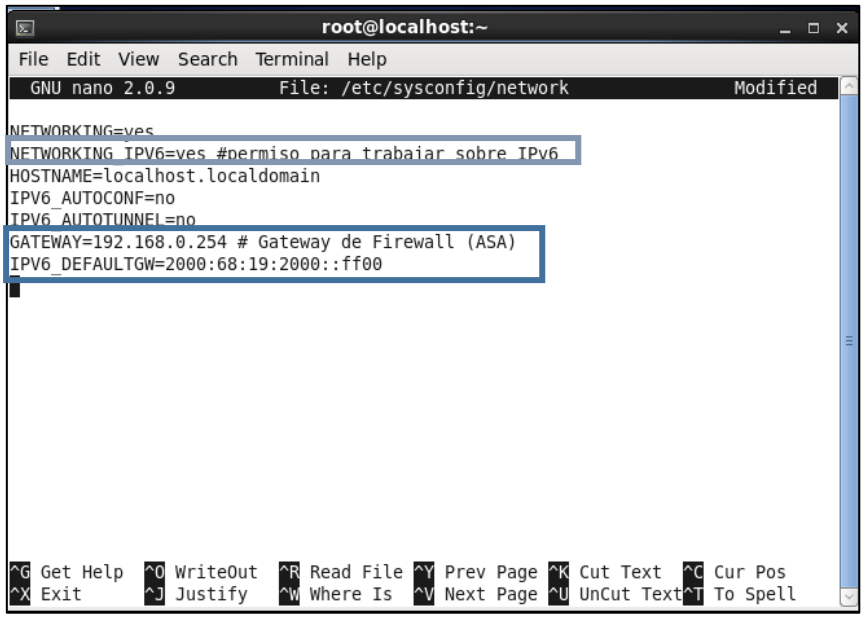


Figura 20. Habilitación IPv6 en Equipo
Fuente: Equipo servidor de Base de Datos

Para finalizar con la configuración se debe realizar reiniciar las tarjetas con el comando *service network restart.*

3.2.4 Configuración Interfaz de red del Servidor de Aplicaciones Forms

Se realiza la configuración del fichero de la interfaz de red tanto para IPv4 como para IPv6, se asigna la dirección de Gateway, además se reinicia las interfaces, a continuación, se indica paso a paso el proceso de configuración del servidor de Aplicaciones.

3.2.4.1 Configuración IPv4 del Servidor de Aplicaciones Forms

Se debe asignar una dirección IPv4 en la tarjeta de red, para esto se debe acceder al fichero mediante el comando *#nano /etc/sysconfig/network-scripts/ifcfg-eth0* como se muestra en la figura 21:

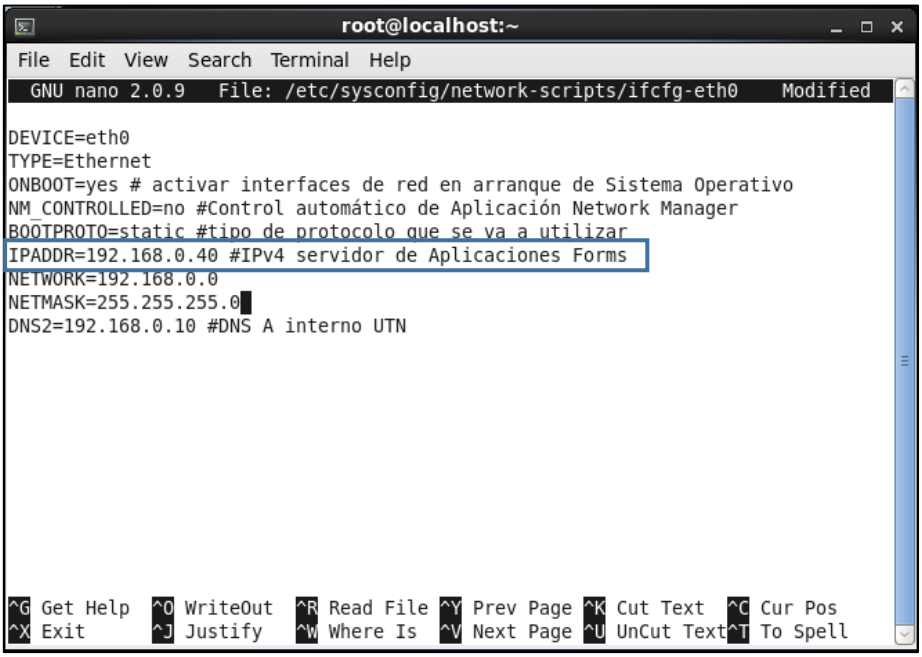


Figura 21. Configuración Nativa IPv4
Fuente: Equipo servidor de Aplicaciones

Se habilita el protocolo en el cual se va a trabajar ingresando al archivo de configuración de red, digitar *NETWORKING* seteado en YES para trabajar solamente en IPv4 como se observa en la figura 22.

Figura 22. Habilitación solo IPv4 en Equipo
Fuente: Equipo servidor de Aplicaciones

De esta manera se ha configurado IPv4 Nativo para este servidor, como se mencionó anteriormente es importante reiniciar la configuración de la tarjeta de red cuando ya se haya culminado con la configuración, esto permitirá que todas las configuraciones realizadas anteriormente se guarden de manera correcta.

3.2.4.2 Configuración de Doble Pila para Servidor de Aplicaciones Forms

En la figura 23 se muestra la configuración para trabajar en el servidor como Doble Pila, es decir, se asigna una dirección IPv4 e IPv6 en la interfaz de red.

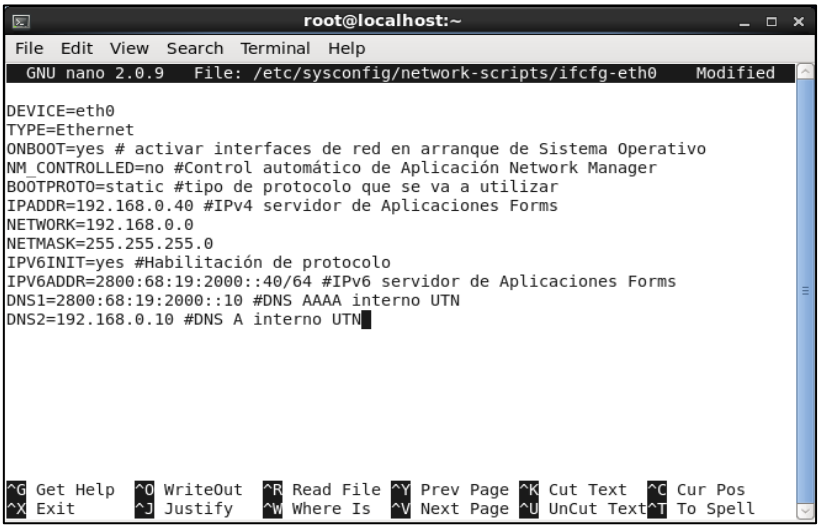


Figura 23. Configuración Interfaz con IPv6 servidor de Aplicaciones
Fuente: Equipo servidor de Aplicaciones

Es importante mencionar que se tendrá dos direcciones de DNS internos de la UTN, tomando en cuenta que DNS1 será el primario, es decir este DNS será el que trabajará como principal para la resolución de nombres.

En la figura 24 se muestra la habilitación del protocolo IPv6, configurando el Gateway del Firewall (ASA) para conocer la salida de las peticiones hacia la red de la Universidad, como también una dirección IPv6 de Gateway por default.

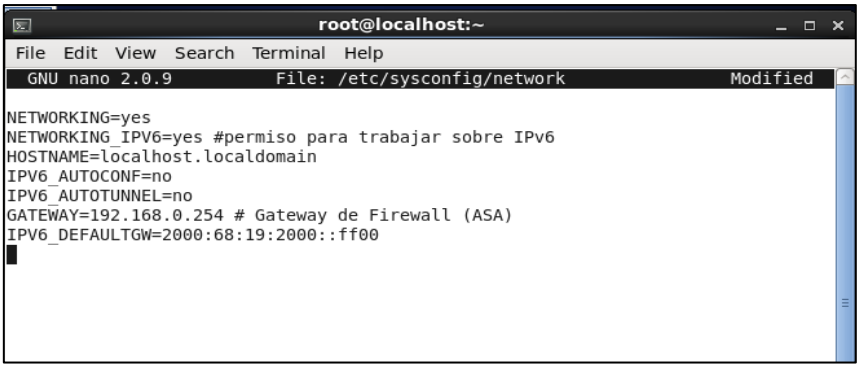


Figura 24. Habilitación IPv6 servidor de Aplicaciones
Fuente: Equipo servidor de Aplicaciones

Una vez configurado se reinicia las tarjetas con el comando *service network restart*, de tal manera que cuando se inicie de nuevo el sistema, la tarjeta de red quede con las direcciones asignadas.

3.2.5 Configuración de Mecanismo de Transición DNS64/NAT64

A continuación, se presenta la configuración de los mecanismos de traducción de direcciones para IPv4 e IPv6 y de traducción de nombres, conocidos como DNS64/NAT64.

3.2.5.1 Configuración DNS64

Para la configuración del DNS64 se asigna las direcciones IP en el archivo de configuración de la tarjeta de red, para este caso como se tendrá tanto una dirección IPv4 como una IPv6 tal y como lo muestra la figura 25.

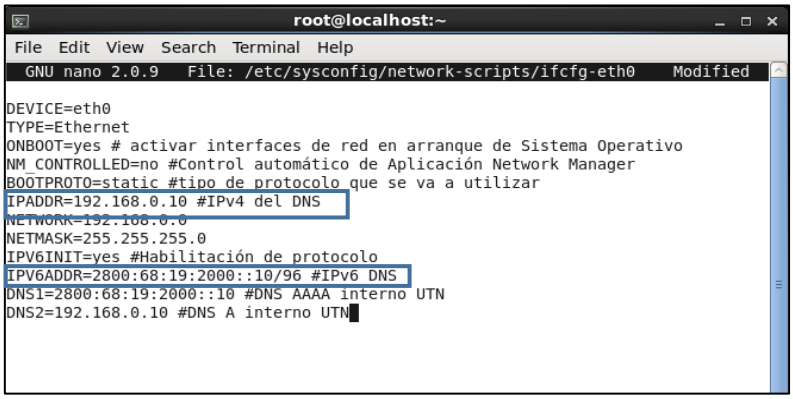


Figura 25. Configuración Interfaz de Red del DNS
Fuente: Equipo servidor DNS64/NAT64

Como se lo ha realizado anteriormente se debe habilitar y dar permiso para trabajar sobre IPv4 e IPv6 en el DNS visto en la figura 26, para lo cual se setea NETWORKING y NETWORKING_IPV6 en YES.

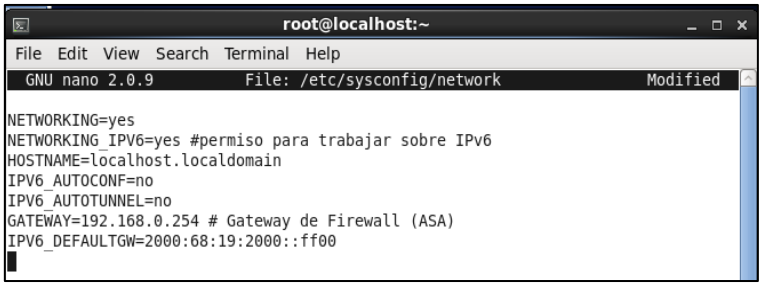


Figura 26. Habilitación para trabajar sobre IPv6 en DNS
Fuente: Equipo servidor DNS64/NAT64

Se reinicia el servicio y se ejecuta los cambios que se realizaron en las tarjetas de red para que la configuración no se modifique en el reinicio del sistema, en la figura 27 se observa que el reinicio de las tarjetas se lo ha realizado correctamente.

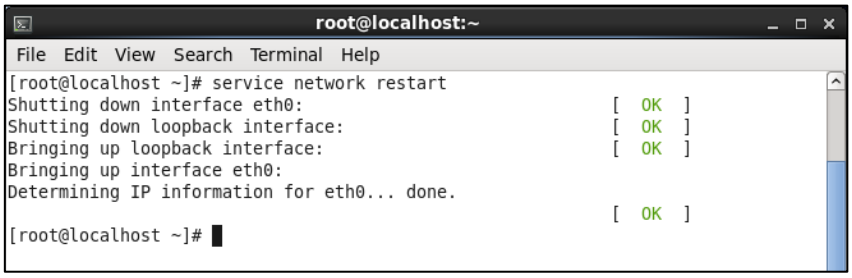


Figura 27. Reinicio de Tarjetas de Red
Fuente: Equipo servidor DNS64/NAT64

Es importante tener en cuenta que para el DNS se debe instalar la aplicación BIND (Berkeley Internet Name Domain) para lo cual se lo realiza con el comando que se observa en la figura 28 que se presenta a continuación.

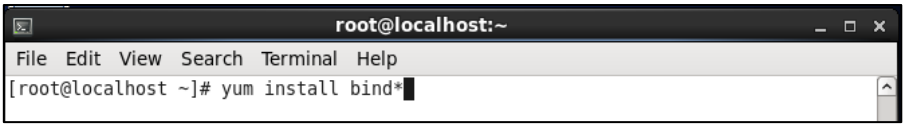


Figura 28. Instalación BIND
Fuente: Equipo servidor DNS64/NAT64

Una vez que se haya digitalizado el comando anterior, se procede aceptar la instalación de la aplicación poniendo Y en la pantalla que se despliega según se observa en la figura 29.

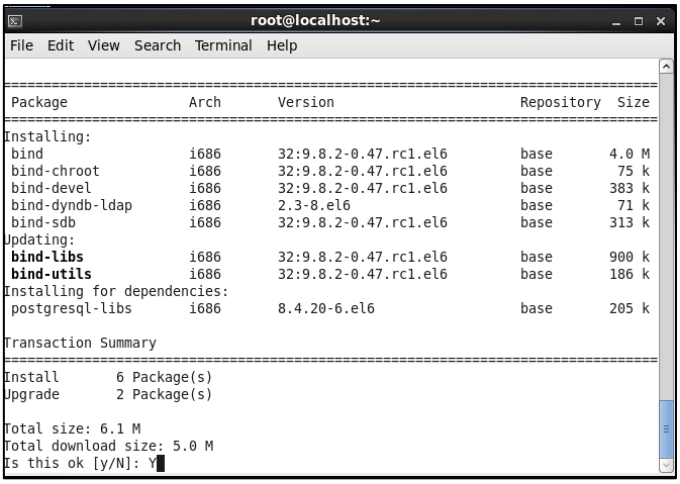


Figura 29. Aceptación de Instalación BIND
Fuente: Equipo servidor DNS64/NAT64

Una vez que se ha culminado con la instalación de la aplicación, se ingresa al archivo de configuración general BIND del DNS con el comando *nano /etc/named.conf* ya que este archivo contiene todos los parámetros que se requieren para el servidor. Hay que editar las direcciones de las cuales se escuchará las peticiones mediante el puerto 53, estás direcciones tendrán un encaminamiento y una traducción hacia su destino.

El puerto será direccionado, se agregará las direcciones del servidor, siendo IPv4 e IPv6 y además se asignarán los Forwards del proveedor de Internet, estos permiten que se envíen las consultas ya generadas hacia los servidores DNS externos, en la figura 30 se muestra todas las configuraciones mencionadas anteriormente, de tal manera que se encuentra detallado cada uno de los comandos digitados.

Un forward o reenviador es un servidor de Sistema de nombres de dominio (DNS) en una red que se usa para reenviar consultas DNS de nombres DNS externos fuera de dicha red. (Microsoft, 2016)

Figura 30. Direccionamiento servidor DNS64
Fuente: Equipo servidor DNS64/NAT64

Dentro de los Forwards se establece que primero busca en zona directa y para el DNS64 se le asigna un pool de direcciones especial para los hosts que requieran acceder en IPv4.

Ahora se procede a realizar la creación de las zonas para los registros de los cuales se quiere traducir, es decir, para el reenvío de los dominios que se tiene autoridad se crea una zona y para las redes que se tiene un control total se crea una zona inversa con el fin de resolver los dominios.

Zonas Directas

Se realiza la configuración y establecimiento de las Zonas Directas de tal manera que se define el tipo de zona y el nombre del archivo con el que se va a buscar la zona directa, a continuación, se muestra en la figura 31 que el archivo utn.edu.ec se encontrará en el directorio *var named.*

Figura 31. Zona Directa
Fuente: Equipo servidor DNS64/NAT64

Para la creación del archivo de las zonas directas se ingresa el siguiente comando *nano var/named/forward.utn.edu.ec,* de esta manera se entra al archivo de configuración como se observa en la figura 32:

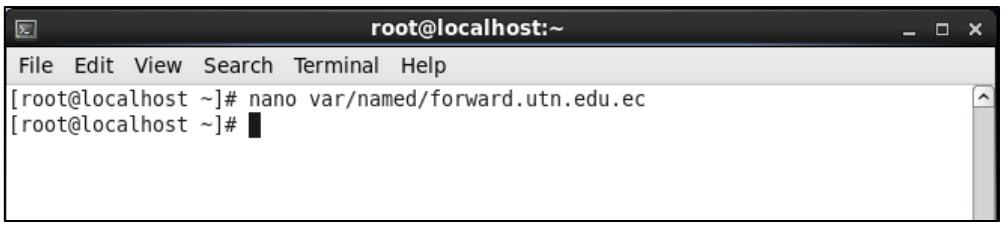


Figura 32. Creación de archivo de zonas directas
Fuente: Equipo servidor DNS64/NAT64

Dentro del fichero de la zona directa, se realiza la configuración de las aplicaciones y los registros con los que se va a redireccionar o traducir el servidor DNS64, el momento que se apunta el nombre, se traduce la dirección hacia IPv6 y de la misma manera si se apunta a la dirección IP, arrojaría el nombre de dicha dirección IP. Es importante mencionar que si se desea incluir una nueva aplicación se debe agregar a la lista con el registro y la dirección que se quiera redireccionar. Para el caso que se presenta en este proyecto se puede observar en la figura 33 que se tiene diferentes tipos de aplicaciones tales y como son: Servidor DNS, Servidor WEB, Servidor de Aplicaciones, Servidor de Base de Datos.

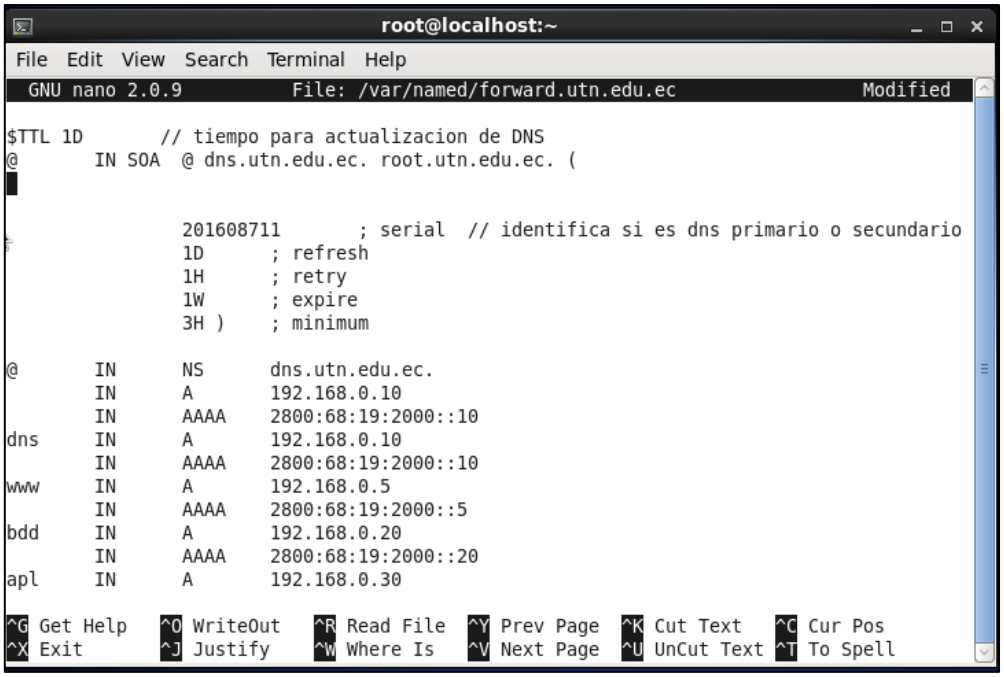


Figura 33. Configuración de Registros y Aplicaciones del DNS64
Fuente: Equipo servidor DNS64/NAT64

De esta manera se ha culminado con la configuración de la zona directa, a continuación, se procede a guardar todo lo que se encuentra en el fichero y se procede a salir del mismo, una vez que se tiene configurado las zonas directas, se procede a la configuración de las zonas inversas.

Zonas Inversas

Para la creación de las zonas inversas se debe tener en cuenta que se crea una zona para cada subred que se va a utilizar o las aplicaciones que se encuentren, es importante mencionar que se crean tanto para IPv4 como también para IPv6, además cada zona tiene su propio fichero, es decir que la dirección de protocolo versión seis no tiene el mismo fichero que la dirección de protocolo versión cuatro, como se observa en la figura 34.

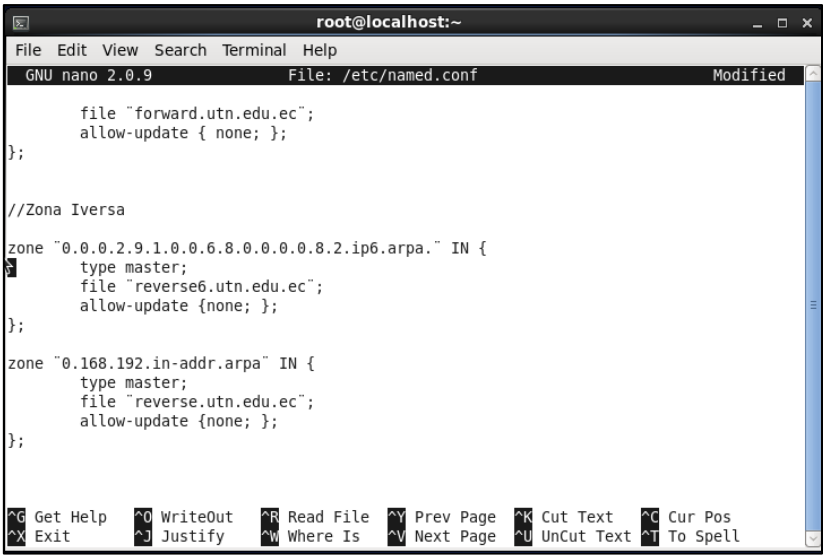


Figura 34. Zonas Inversas
Fuente: Equipo servidor DNS64/NAT64

Para la creación del archivo de las zonas inversas se ingresa el comando *nano var/named/reverse.utn.edu.ec*.

Una vez que se encuentra dentro del fichero de la zona inversa en IPv4, se realiza la asignación de los punteros de cada una de las aplicaciones, con la cual se complementa juntamente con la definición de la zona en el archivo general *named.conf* del servidor DNS, es importante mencionar que el punto que se utiliza al final del nombre por ejemplo utn.edu.ec. indica que éste es un nombre de dominio. En este fichero se tiene el serial en donde se debe tener en cuenta que entre mayor sea el serial, se podrá conocer si el DNS es primario o es secundario, como se observa en la figura 35.

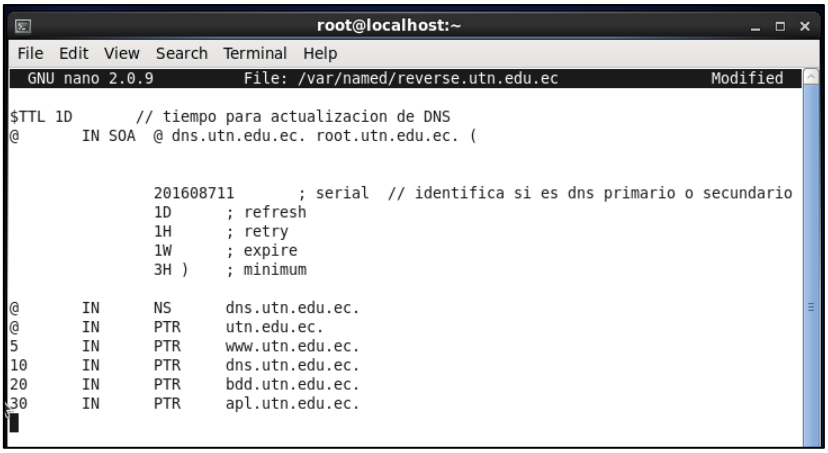


Figura 35. Zona inversa DNS64
Fuente: Equipo servidor DNS64/NAT64

De igual manera se culmina con la configuración de la zona inversa, a continuación, se procede a guardar todo lo que se encuentra en el fichero y a salir del mismo. Anteriormente se ha mencionado que la configuración de la zona inversa se la debe realizar en IPv4, es por eso que a continuación se presenta la configuración de la zona inversa para IPv6 para lo cual se debe ingresar a *nano /var/named/reverse6.utn.edu.ec*

En la figura 36 se indica la configuración de la Zona inversa para IPv6 siendo de la misma manera que se lo ha hecho con IPv4.

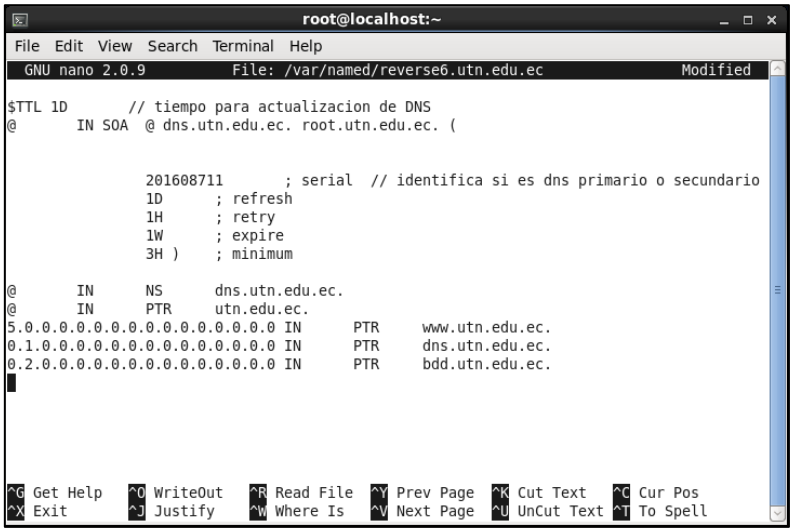


Figura 36. Zonas Inversas IPv6
Fuente: Equipo servidor DNS64/NAT64

Se reinicia el servicio del *named* para ejecutar todos los cambios realizados y poner en funcionamiento el servidor de resolución de nombres DNS64, como se observa en la figura 37, el reinicio del servicio se lo ha realizado correctamente.

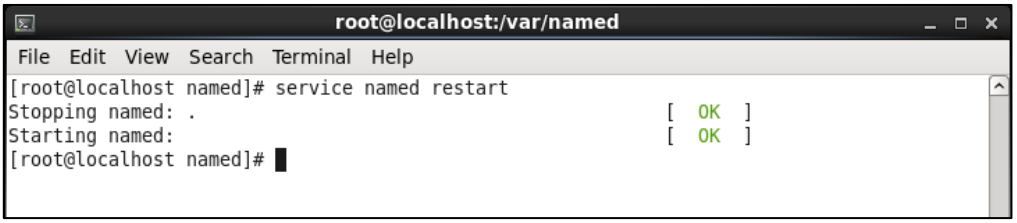


Figura 37. Reinicio de Servicio
Fuente: Equipo servidor DNS64/NAT64

Antes de realizar las pruebas de resolución de nombres se debe activar el demonio de la aplicación Bind con el comando *chkconfig named on* como se muestra en la figura 38, el cual permitirá iniciar automáticamente el arranque del sistema.

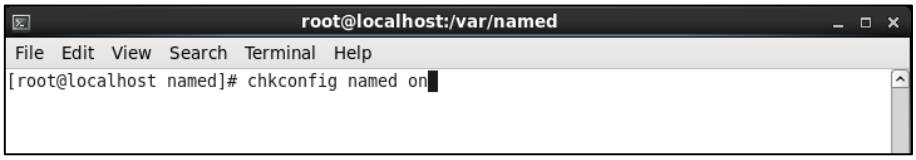


Figura 38. Activación de Demonio
Fuente: Equipo servidor DNS64/NAT64

Prueba de resolución de nombres

La primera prueba que se realiza es con el comando *dig dns.utn.edu.ec* que muestra las direcciones y nombres relacionadas con el dominio dns.utn.edu.ec. Para este caso se puede observar en la figura 39 tanto la dirección IPv4, la dirección IPv6 y además el nombre con el que está relacionado el dominio.

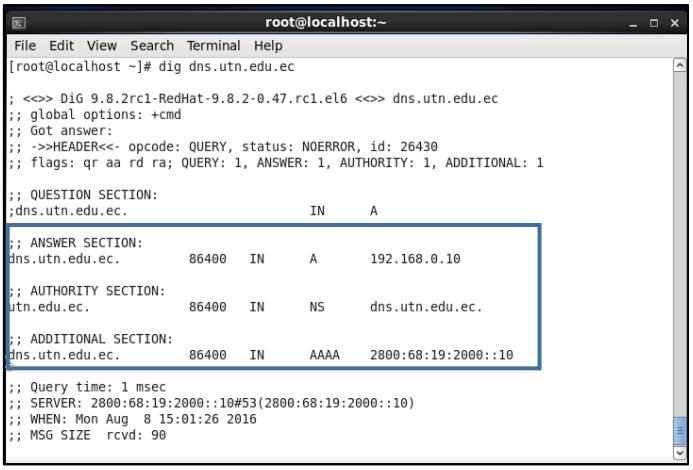


Figura 39. Prueba 1 de resolución de nombres DNS
Fuente: Equipo servidor DNS64/NAT64

Otra prueba es con el comando *dig any utn.edu.ec* que permite realizar una visualización con mayores detalles como es el tiempo de respuesta, el tipo de registro y la dirección del servidor de nombres, este proceso se lo puede realizar de cada uno de los servicios asociados al DNS64 observados en la figura 40.

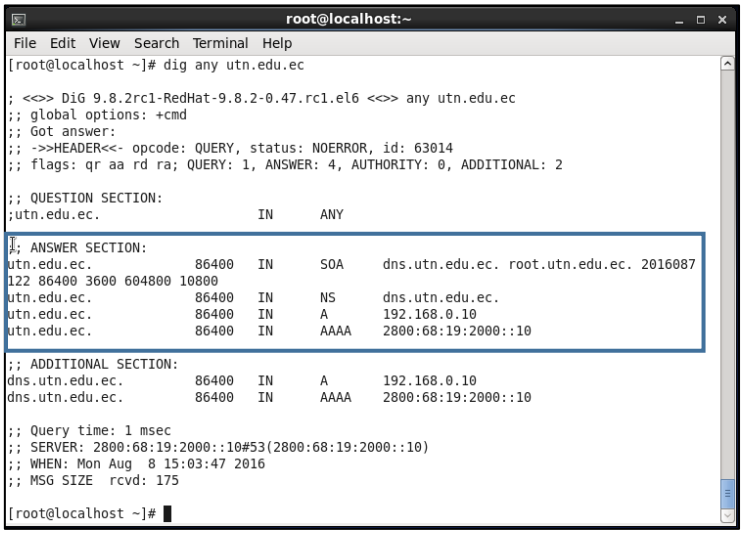


Figura 40. Prueba 2 de resolución de nombres DNS
Fuente: Equipo servidor DNS64/NAT64

La última prueba que se realiza es con el comando *nslookup utn.edu.ec* en donde se puede observar tanto el nombre del dominio como la dirección del servidor de resolución de nombres, dicha dirección se la puede observar tanto en IPv4 como en IPv6 vistos en la figura 41.

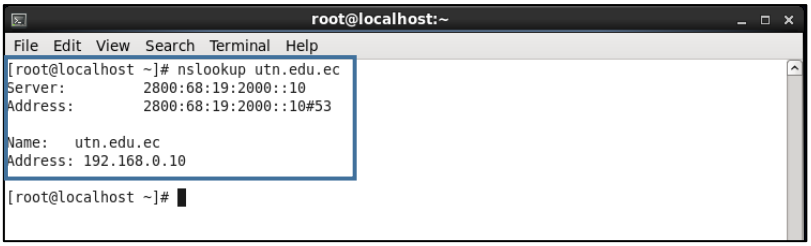


Figura 41. Prueba 3 de resolución de nombres DNS
Fuente: Equipo servidor DNS64/NAT64

3.2.6.2 Configuración NAT64

Para la configuración del NAT64 lo primero que se va a realizar es la instalación de TAYGA, se realiza la descarga de este paquete para luego continuar con el proceso, para poder realizar esto se escribe en el terminal la dirección que se observa en la figura 42 con el uso del comando *wget*.

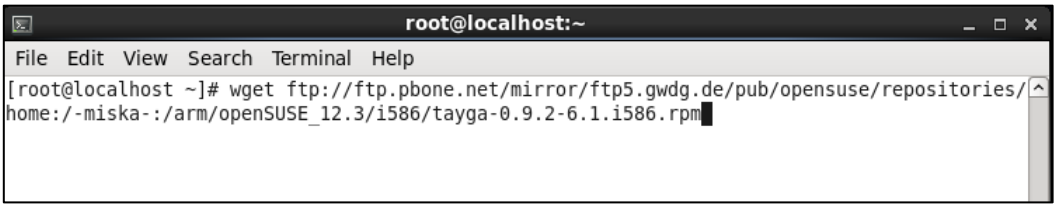


Figura 42. Descarga de TAYGA
Fuente: Equipo servidor DNS64/NAT64

Instalación de TAYGA

Una vez que se tiene descargado el paquete de TAYGA, de manera gráfica se procede a realizar la instalación, para esto simplemente se busca en el root, la instalación de este paquete y se da doble clic para continuar con la instalación, aparece un mensaje en el cual se debe poner en la opción *continue anyway* como se observa en la figura 43.

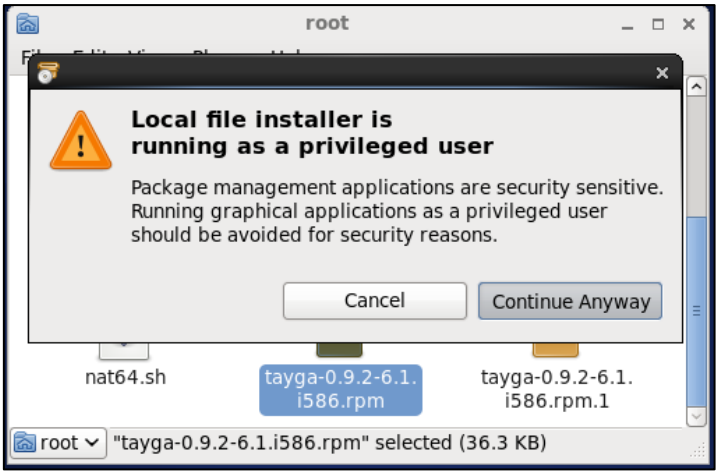


Figura 43. Instalación de TAYGA
Fuente: Equipo servidor DNS64/NAT64

Una vez que se tiene instalado el TAYGA se procede a la creación interfaz virtual NAT64 para la asignación y traducción de direcciones IPv4, de tal manera que puedan acceder todos los hosts nativos IPv6.

En la figura 44 se muestra que además de la creación de la interfaz virtual, también se crea las rutas estáticas para el encaminamiento de los paquetes de IPv6 a IPv4.

Figura 44. Rutas estáticas e Interfaz virtual
Fuente: Equipo servidor DNS64/NAT64

Se ingresa al archivo de configuración de las Iptables para crear cada una de las reglas como muestra la figura 45, lo primero que se realiza es para el enmascaramiento de las interfaces de NAT64 hacia la interfaz real eth0 para que exista comunicación con el entorno

de la red, las siguientes reglas aceptan el tráfico de los puertos de DNS, ICMP. Además, realiza el encaminamiento entre las interfaces tanto virtual como real en el proceso de la traducción.

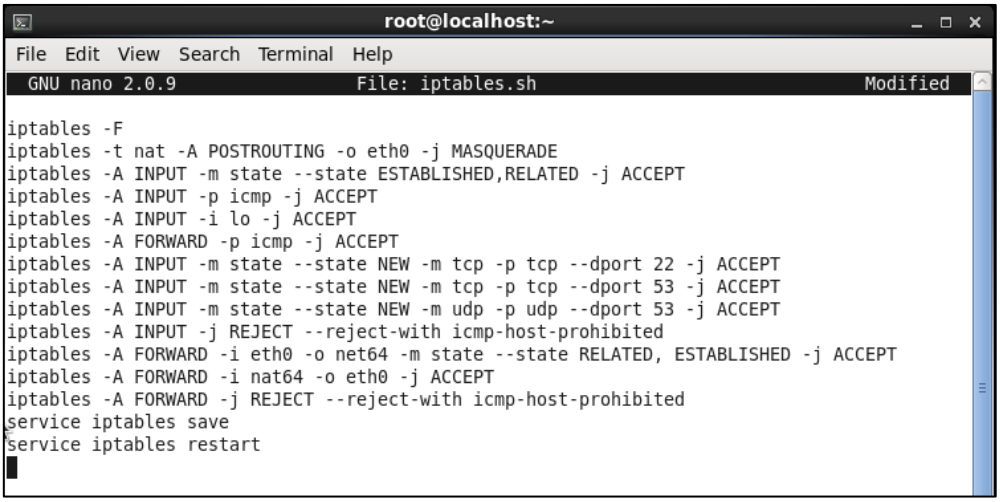


Figura 45. Configuración Iptables
Fuente: Equipo servidor DNS64/NAT64

En la figura 46 se observa la configuración para IPv6 de tal manera que, para permitir el tráfico entre los diferentes protocolos a utilizarse se debe activar y permitir el paso de ICMP6, es decir que permite aceptar el echo request para toda la topología.

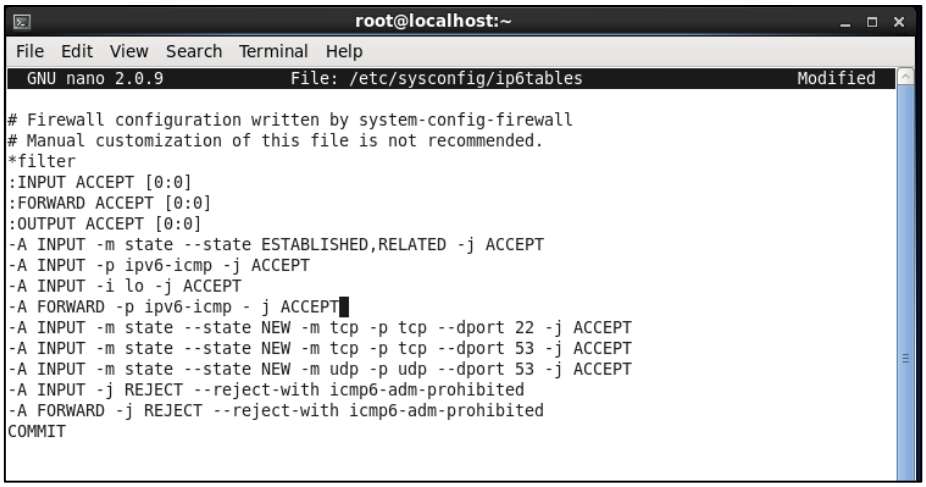


Figura 46. Configuración Iptables versión 6
Fuente: Equipo servidor DNS64/NAT64

En la figura 47, dentro del archivo de configuración, se escribe en 1 para habilitar el encaminamiento desde el servidor hacia los hosts externos.

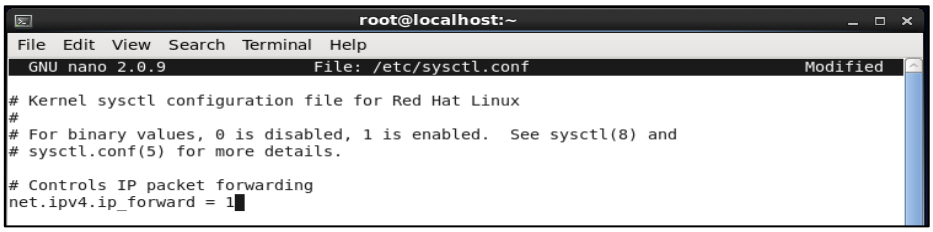


Figura 47. Encaminamiento hacia exterior
Fuente: Equipo servidor DNS64/NAT64

A continuación, se procede a realizar la configuración dentro del archivo de TAYGA, para lo cual se debe ingresar el comando *nano /etc/tayga.conf*. Una vez que se encuentra dentro del archivo de configuración se procede a dar el rango de direcciones con las que se va a realizar la traducción de direcciones tal y como se observa en la figura 48.

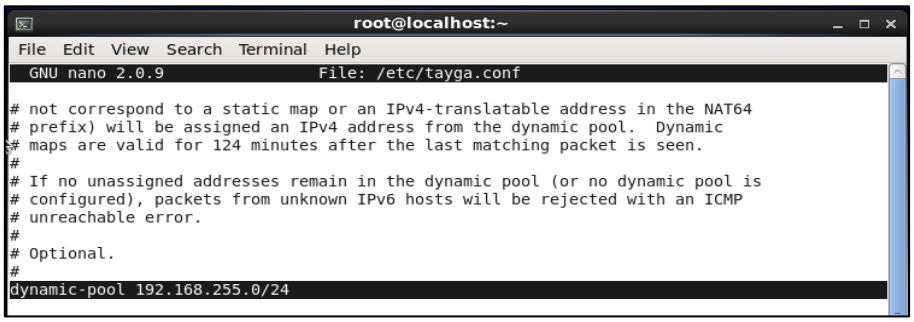


Figura 48. Rango de Direcciones para Traducción
Fuente: Equipo servidor DNS64/NAT64

Como se muestra en la figura 49, se tiene la dirección IPv4 asignada a TAYGA de la interfaz NAT64.

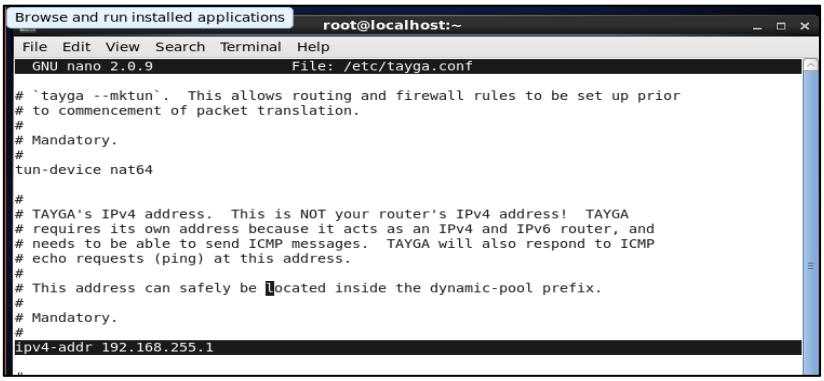


Figura 49. Asignación de Interfaz TAYGA
Fuente: Equipo servidor DNS64/NAT64

En la figura 50 se muestra el prefijo asignado para realizar la traducción de direcciones, el cual debe ser el mismo que se ha configurado en las rutas estáticas y en el fichero de configuración global del DNS64.

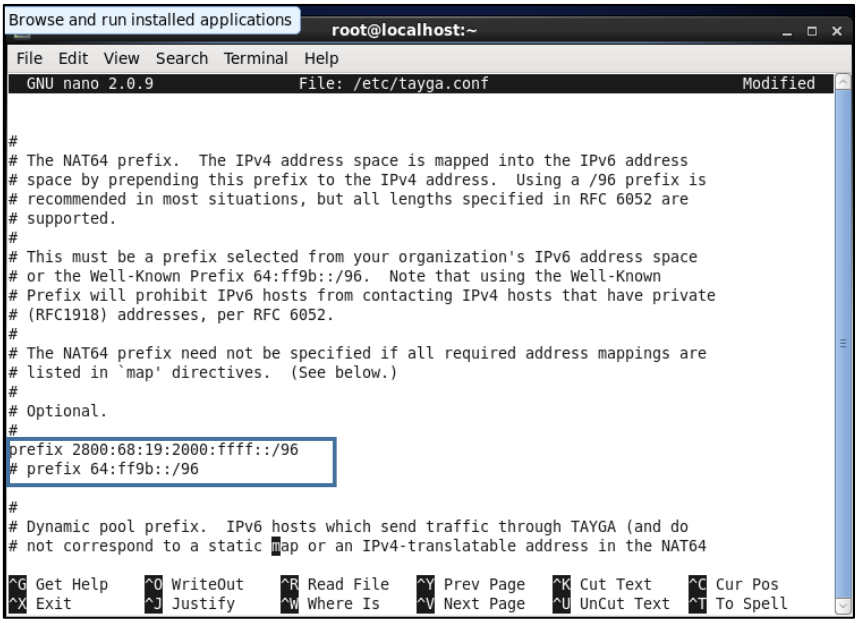


Figura 50. Prefijo de traducción de direcciones
Fuente: Equipo servidor DNS64/NAT64

Para culminar con la configuración del NAT64 se procede a inicializar la interfaz virtual del mismo y también las configuraciones previamente realizadas con los comandos que se observan en la figura 51.

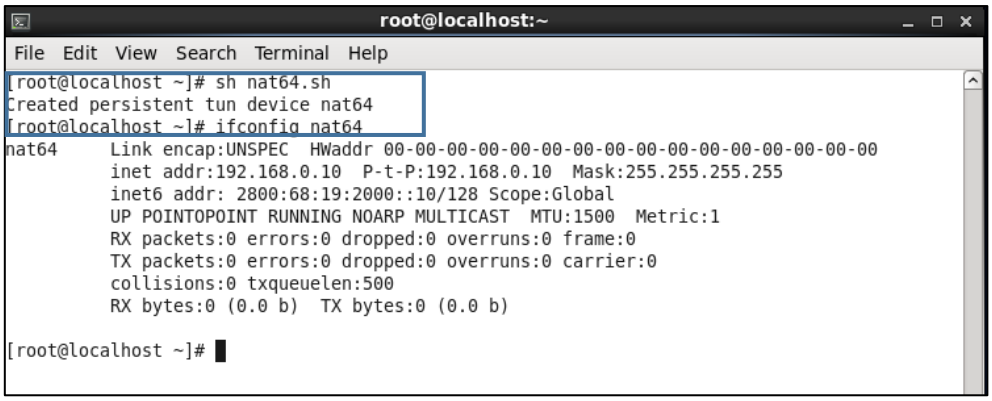


Figura 51. Inicialización de la Interfaz Virtual
Fuente: Equipo servidor DNS64/NAT64

Pruebas de funcionamiento de traducción por NAT64

Realización de Echo Request desde IPv6 hacia IPv4, entre las diferentes interfaces configuradas anteriormente (interfaz real-virtual) figura 52.

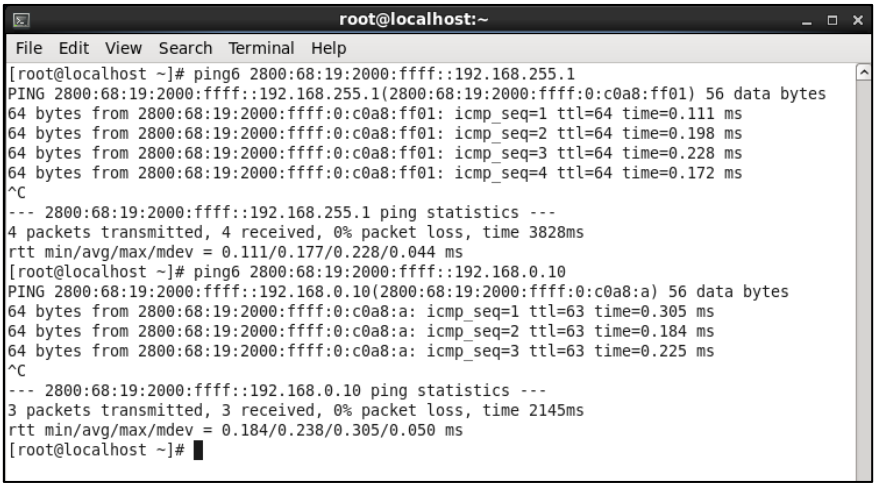


Figura 52. Ping desde IPv6 hacia IPv4
Fuente: Equipo servidor DNS64/NAT64

Como ya se demostró el echo request, en la figura 53 se procede a incluir la creación automática de la interfaz y el encaminamiento del NAT64, para lo cual se ingresa *nano/etc/rc.local.* En esta carpeta se realizará la activación para que todo lo que contenga el archivo nat64.sh, se ejecute automáticamente desde la inicialización del sistema.

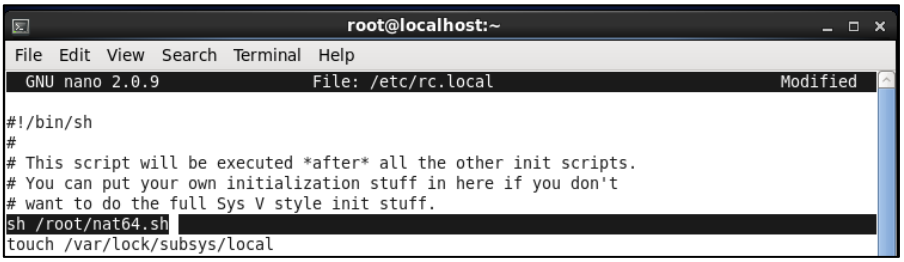


Figura 53. Ejecución Automática del archivo nat64.sh
Fuente: Equipo servidor DNS64/NAT64

3.2.6.3 Cálculo de asignación de una dirección IPv4 a IPv6

Para la asignación de una dirección IPv4 en una dirección IPv6 se lo hace de una manera muy sencilla, el proceso en si es: tomar la dirección en IPv4 y escribirla en binario, una vez que se tiene esto, se procede a convertir esta dirección que se tiene en binario, a

hexadecimal; de esta manera se tendría los últimos 32 bits de la dirección IPv6, para un mejor entendimiento se puede observar el anexo 3.

3.3 Implementación de mecanismo

3.3.1 Configuración del Mecanismo de Transición Doble Pila

La configuración del mecanismo Doble Pila como se observa en la figura 54, permitirá enviar y recibir paquetes tanto IPv4 como IPv6, teniendo en cuenta que para la comprobación de este método se realizará la configuración de uno de los servidores en IPv4, para la verificación del funcionamiento de Doble Pila.

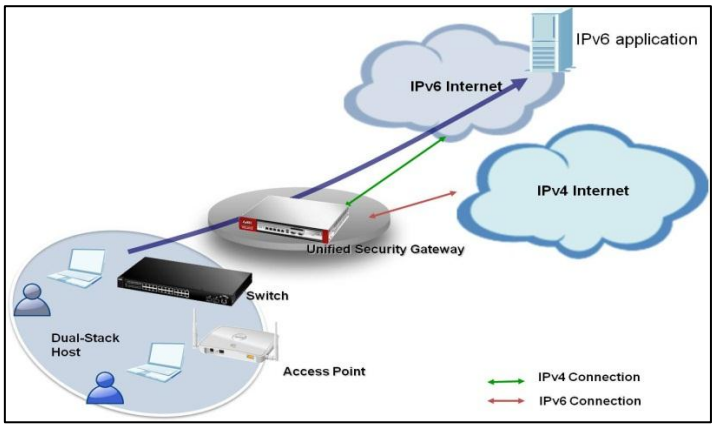


Figura 54. Metodología Doble Pila
Fuente: Recuperado de https://www.zyxel.com/solutions/solution_detail_20120424_255576_tab3.inc

Lo primero que se debe realizar para que el dispositivo final pueda acceder y enviar paquetes en IPv4 e IPv6 se digita los siguientes comandos en el fichero "*/etc/named.conf*". Como ya se conoce para realizar la modificación de un fichero se lo realiza con el comando nano quedando finalmente *nano /etc/named.conf* como se observa en la figura 55.

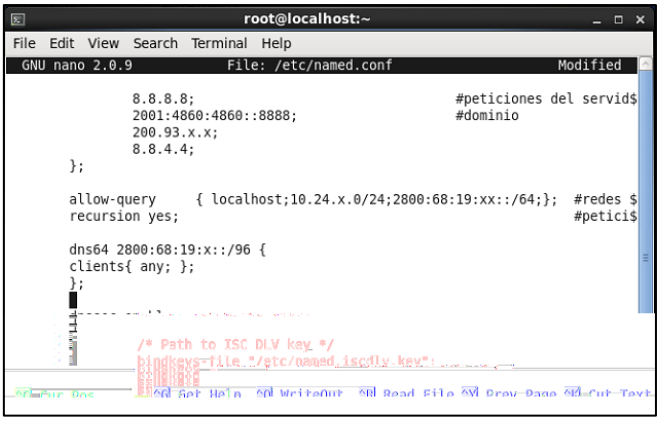


Figura 55. Configuración para Consultas IPv4 e IPv6
Fuente: Equipo servidor DNS64/NAT64

La configuración que se tiene anteriormente permite realizar consultas de usuarios que contengan solo registros A que sean entregadas a los usuarios de tal manera que se añada: 2800:68:19:x::/96 se debe reiniciar el servicio de resolución de nombres para que los cambios que se han realizado se queden guardados y empiecen a ejecutarse, para esto se lo realiza con el comando *service named restart.*

3.3.1.1 Configuración de Switch CISCO 3750

Las configuraciones que se realizarán en este equipo serán tanto el direccionamiento como el encaminamiento de las direcciones del proveedor de internet (Telconet) hacia el Cisco ASA 5520, de esta manera se procede a realizar la configuración en doble pila con los comandos que se presentan a continuación.

Lo primero que se va a realizar es la habilitación del protocolo IPv6:

Switch# configure terminal

Switch(confg)# sdm prefer dual-ipv4-and-ipv6 default

Switch(confg)# end

Switch# reload

Switch# configure terminal

Switch(confg)#ipv6 unicast-routing

```
Switch(confg)#interface vlan 400
Switch(confg-if)#ipv6 address 2800:68:19::x/y
Switch(confg-if)#enable ipv6
Switch(confg-if)#no shutdown
Switch(confg-if)#exit
Switch(confg)#ipv6 route ::/0 2800:68:19::x
Switch(confg)#ipv6 route 2800:68:19::/48 2800:68:19::x
```

Con los comandos que se digitaron anteriormente se culmina con la configuración del Switch 3750, a continuación, se procederá a realizar la configuración del Firewall o CISCO ASA 5520.

3.3.1.2 Configuración de CISCO ASA 5520

En la configuración del Cisco ASA 5520 se va a tener el enrutamiento y el control del tráfico que transita por la red, de tal manera que se establezcan las reglas de encaminamiento para todas las zonas de la red.

Compuesto de tres interfaces la One u Outside que es la interfaz con acceso tiene internet conectada, directamente conectada al switch de IPs públicas; la Inside que es la red de área local (LAN); y la zona desmilitarizada (DMZ) que es donde se encuentran los servidores tal y como es el DNS64 NAT64, el servidor de aplicaciones y el de base de datos.

Para empezar con el ingreso y configuración del equipo se debe ingresar al navegador y digitar la dirección IP que se le haya designado como se observa en la figura 56.

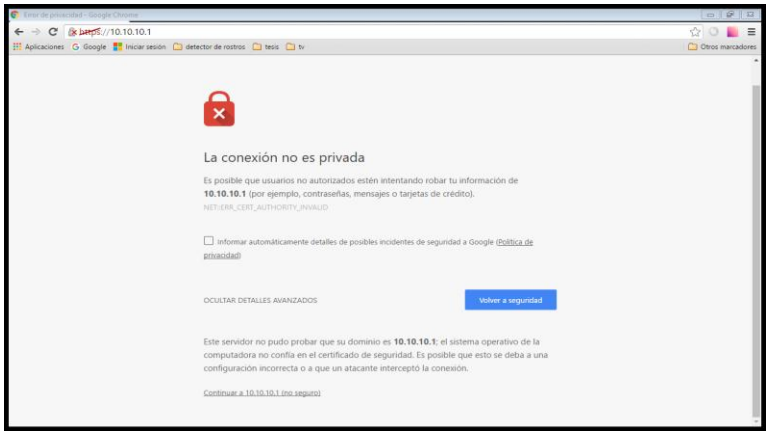


Figura 56. Ingreso CISCO ASA 5520
Fuente: Departamento de Desarrollo Tecnológico e Informático

Por motivos de seguridad aparece que la página no es segura, pero a este mensaje no se le toma mayor relevancia, por lo que se procede a realizar la autenticación mediante un nombre de usuario y una contraseña para el acceso al equipo tal y como se lo observa en la figura 57 que se presenta a continuación.

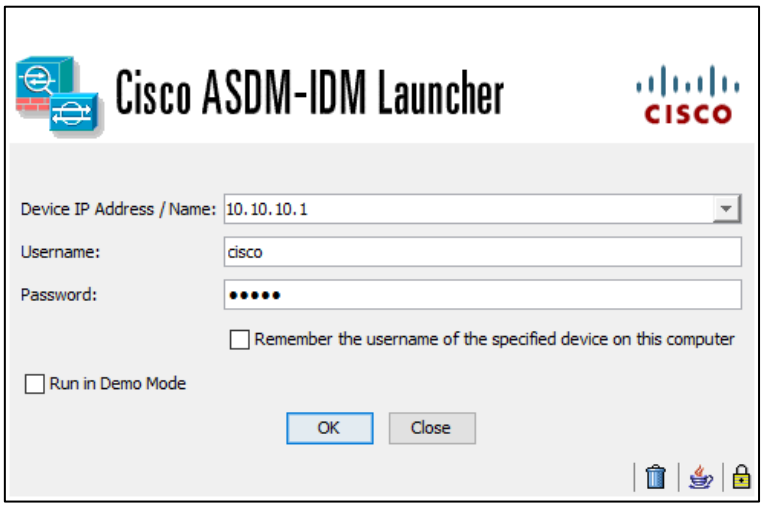


Figura 57. Cisco ASDM-IDM launcher
Fuente: Departamento de Desarrollo Tecnológico e Informático

El primer paso es la asignación de direcciones IPv4 e IPv6 de cada una de las interfaces, de esta manera se puede observar en la figura 58 la interfaz de gestión del equipo.

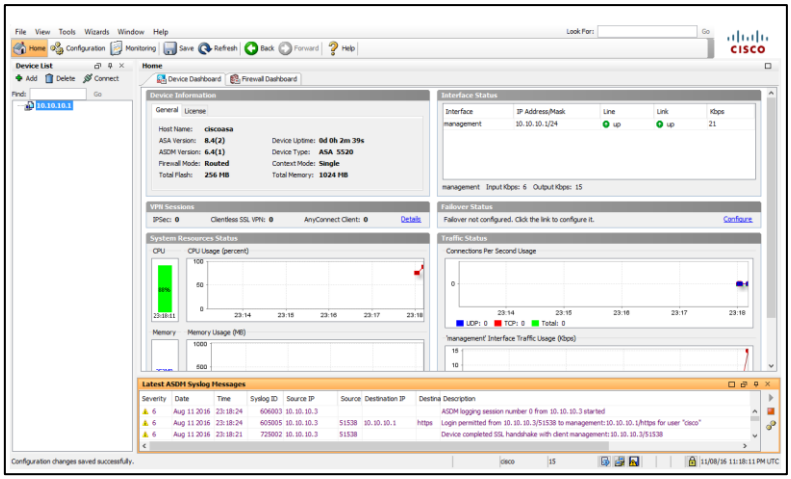


Figura 58. Interfaz de Gestión
Fuente: Departamento de Desarrollo Tecnológico e Informático

Una vez que se tiene la información con cada una de las interfaces, se procede a la asignación de la interface de red WAN u OUTSIDE, en la figura 59 y en la figura 60 se puede observar la asignación de direccionamiento IPv4 e IPv6 respectivamente a dicha interface.

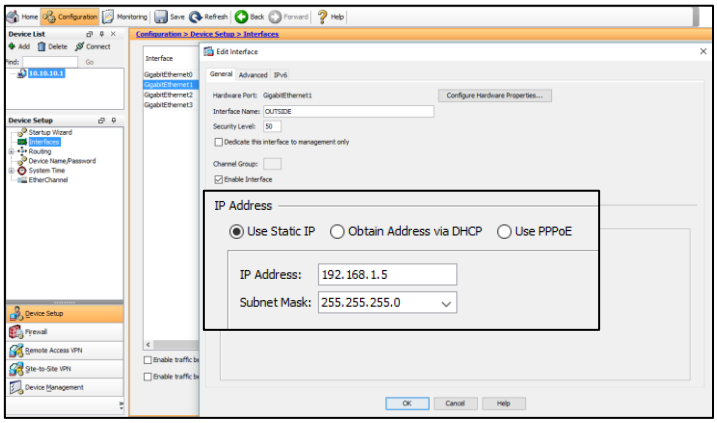


Figura 59. Dirección IPv4 interface OUTSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

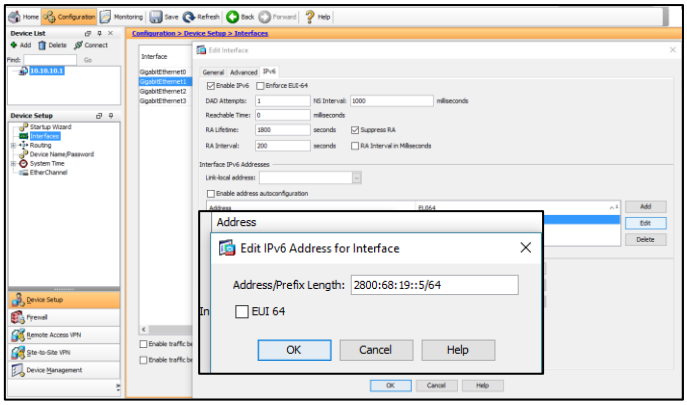


Figura 60. Dirección IPv6 interface OUTSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

De igual manera se procede a la configuración de la interface de red LAN o INSIDE, siendo estas configuradas tanto en IPv4 como en IPv6, tal y como se observa en la figura 61 y en la figura 62.

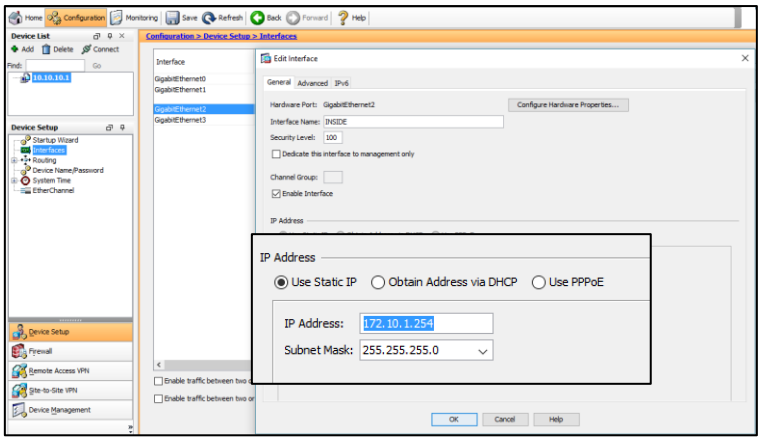


Figura 61. Dirección IPv4 interface INSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

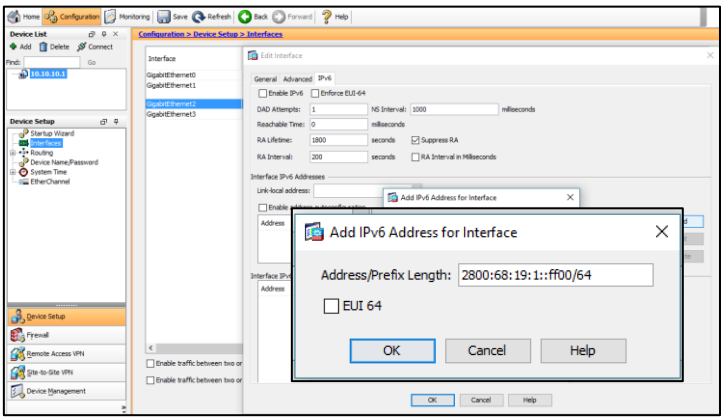


Figura 62. Dirección IPv6 interface INSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

De la misma manera que las anteriores configuraciones tanto para OUTSIDE como para INSIDE se lo realiza con la zona desmilitarizada, siendo configuradas las interfaces tanto para IPv4 como para IPv6 tal y como se observa en la figura 63 y en la figura 64.

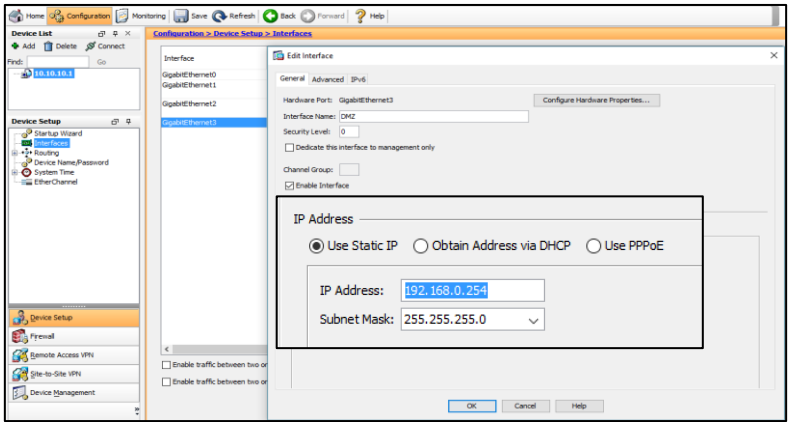


Figura 63. Dirección IPv4 interface DMZ
Fuente: Departamento de Desarrollo Tecnológico e Informático

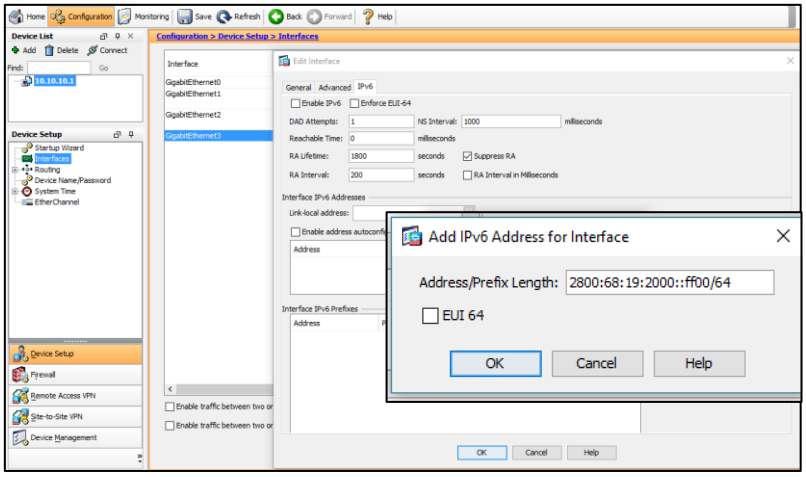


Figura 64. Dirección IPv6 interface DMZ
Fuente: Departamento de Desarrollo Tecnológico e Informático

Una vez que se ha culminado con la configuración se puede observar en la figura 65 que cada una de las interfaces ya tienen asignada una dirección IPv4 y una IPv6.

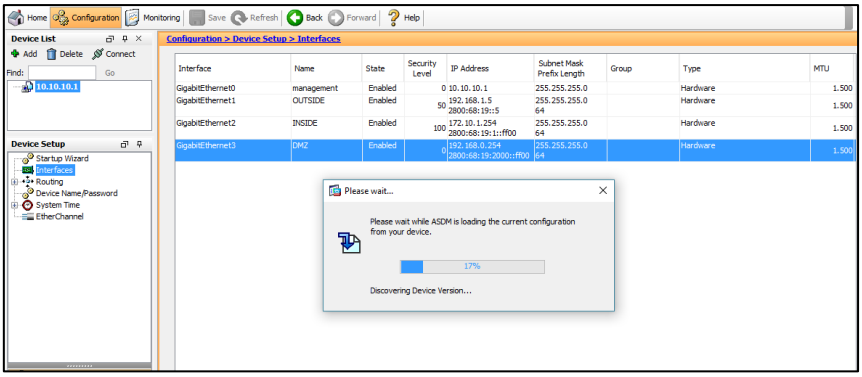


Figura 65. Direcciones de Interfaces CISCO ASA
Fuente: Departamento de Desarrollo Tecnológico e Informático

A continuación, se procede a realizar la configuración de enrutamiento, es decir, se realiza la definición de rutas estáticas en IPv4 e IPv6, una ruta estática es igual al encaminamiento hacia el router de borde de la red (Internet).

En la figura 66 y la figura 67 se muestra el direccionamiento de la ruta estática en IPv4 e IPv6 de la WAN u OUTSIDE.

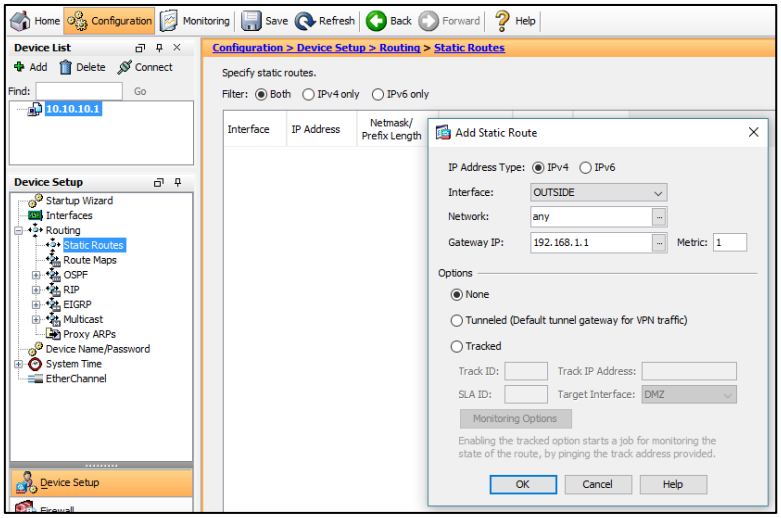


Figura 66. Direccionamiento IPv4 OUTSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

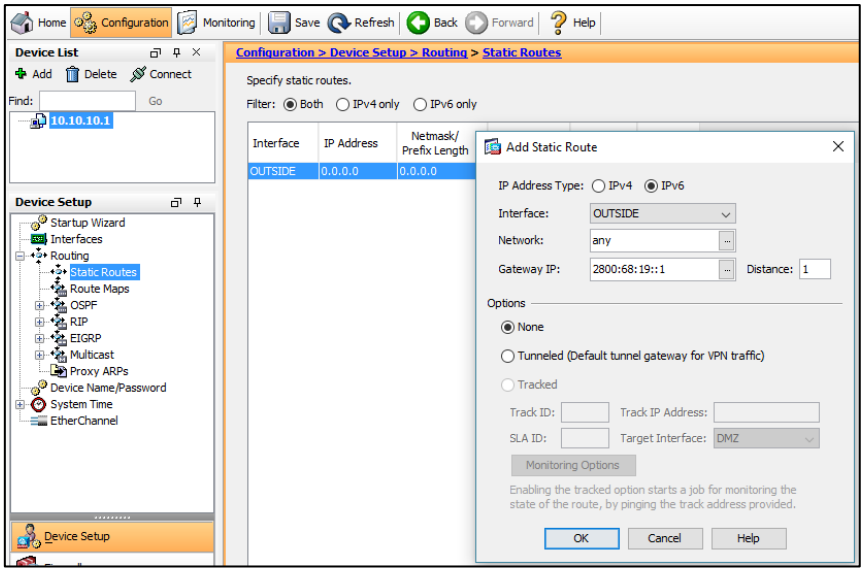


Figura 67. Direccionamiento IPv6 OUTSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

Ahora se procede a la creación de rutas estáticas en IPv4 e IPv6 de las subredes LAN o INSIDE, en la figura 68 se muestra la dirección perteneciente a esta subred con su respectivo gateway.

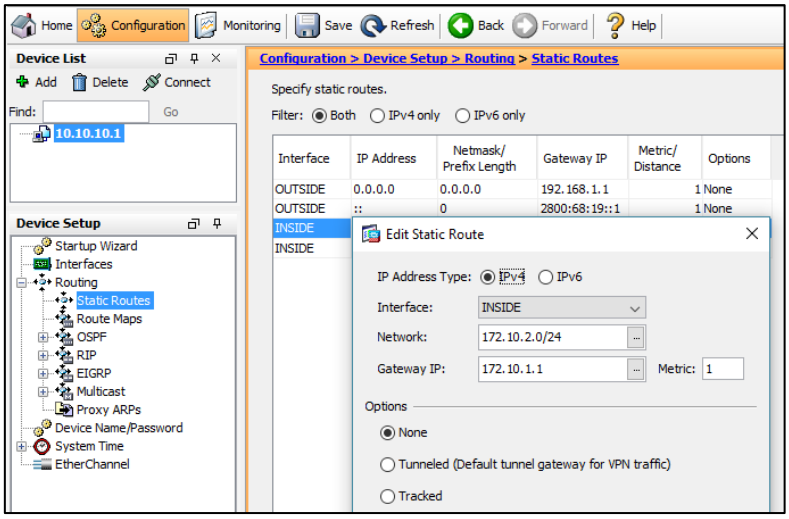


Figura 68. Direccionamiento IPv4 INSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

Una vez que se ha culminado con la asignación de las rutas estáticas se podrá observar en la figura 69, todas las subredes que han sido configuradas en el equipo CISCO ASA, de tal manera que se cuente tanto con las direcciones IPv4 como las IPv6 de las tres zonas hacia donde se quiere llevar la conectividad.

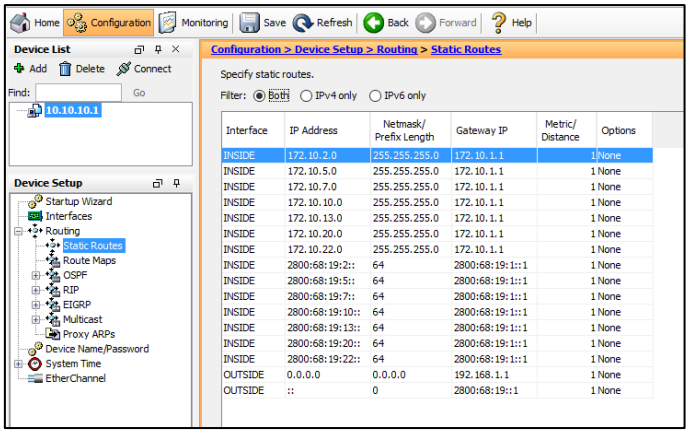


Figura 69. Direccionamiento IPv4 e IPv6 CISCO ASA
Fuente: Departamento de Desarrollo Tecnológico e Informático

A continuación, se procede a generar las reglas de acceso en el Firewall observado en la figura 70, permitiendo que la dirección 172.10.1.0/24 pueda llegar hacia cualquier destino.

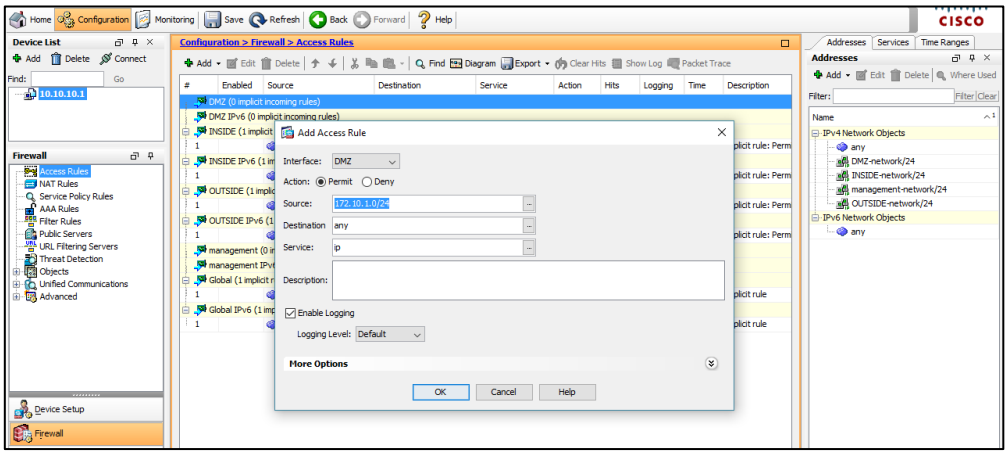


Figura 70. Reglas de tráfico de resolución de nombres
Fuente: Departamento de Desarrollo Tecnológico e Informático

La figura 71 y la figura 72 que se presenta a continuación indica que esa configuración va a permitir el tráfico entre la red LAN y DMZ, para que exista este permiso se debe tener claro que tanto el origen como el destino van a ser LAN y DMZ, es decir que como primera instancia LAN viene a ser el origen y DMZ el destino, y después se realiza la configuración en donde DMZ es el origen y LAN es el destino.

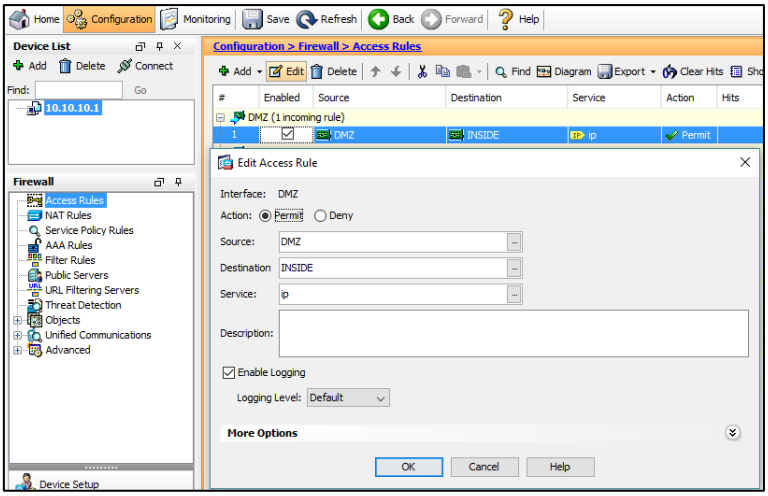


Figura 71. Permiso de tráfico desde DMZ hacia INSIDE
Fuente: Departamento de Desarrollo Tecnológico e Informático

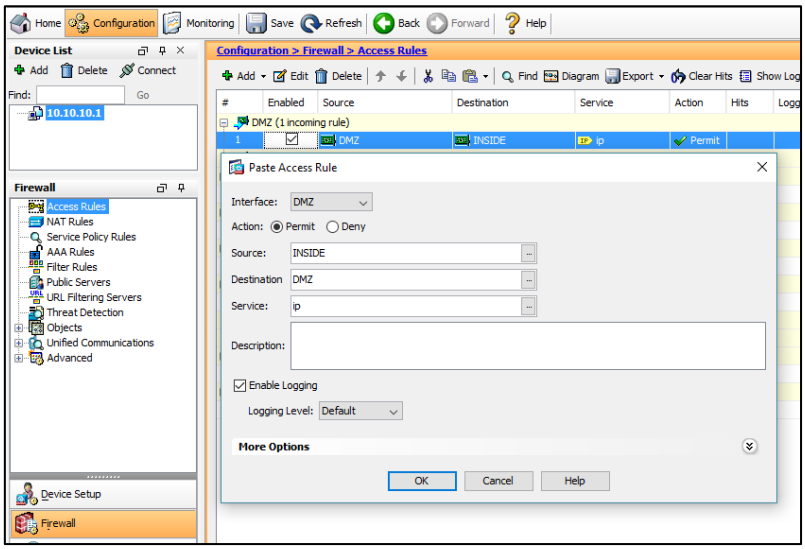


Figura 72. Permiso de tráfico desde INSIDE hacia DMZ
Fuente: Departamento de Desarrollo Tecnológico e Informático

3.3.1.3 Configuración Switch de Core FICA

Es el equipo de distribución para la red de acceso local (LAN), están definidas las VLANs y está directamente conectada a cada una de las dependencias universitarias. (FICA, BIENESTAR, FACAE, ETC.) Se debe configurar en Doble Pila, en la figura 73 se observa que primero se accede a la configuración en modo privilegiado, habilitando el equipo como un enrutador tanto para IPv4 como para IPv6, se asigna a la interfaz conectada hacia el

Firewall o ASA la dirección en los dos protocolos y se habilita la interfaz para que trabaje sobre el protocolo IPv6, finalmente se levanta la interfaz.

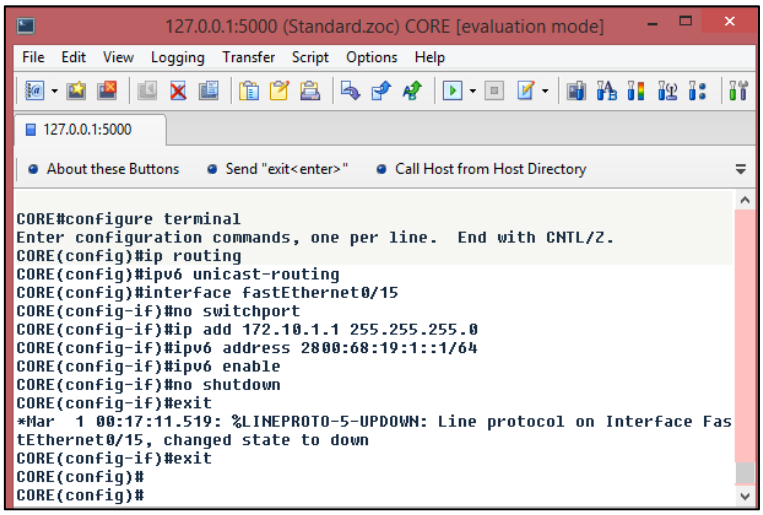


Figura 73.Configuración Switch de Core FICA
Fuente: Switch The Core FICA

Las interfaces que se encuentran conectadas directamente a los switchs de acceso de cada dependencia universitaria establecen enlaces en modo troncal como se puede observar en la figura 74.

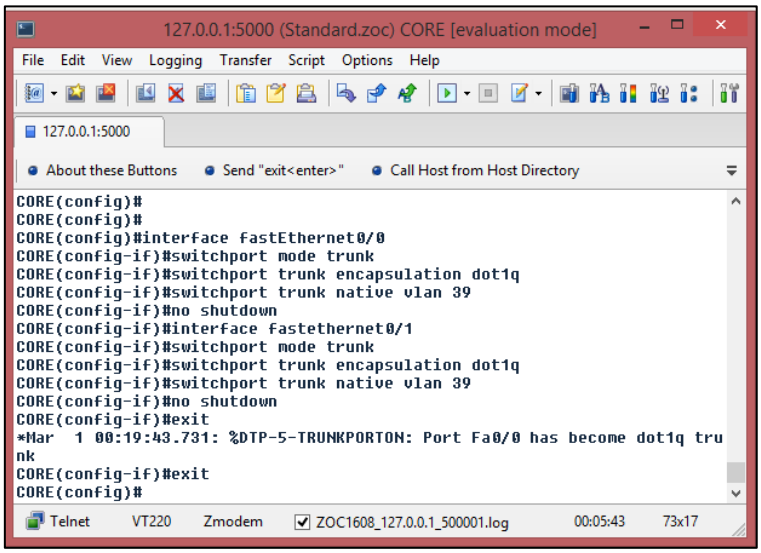


Figura 74. Configuración modo Troncal Switch de Core FICA
Fuente: Switch The Core FICA

En la figura 75 se puede observar que se asigna la dirección IP correspondiente en ambos protocolos para cada una de las VLANs asi como también la habilitación del protocolo versión 6.

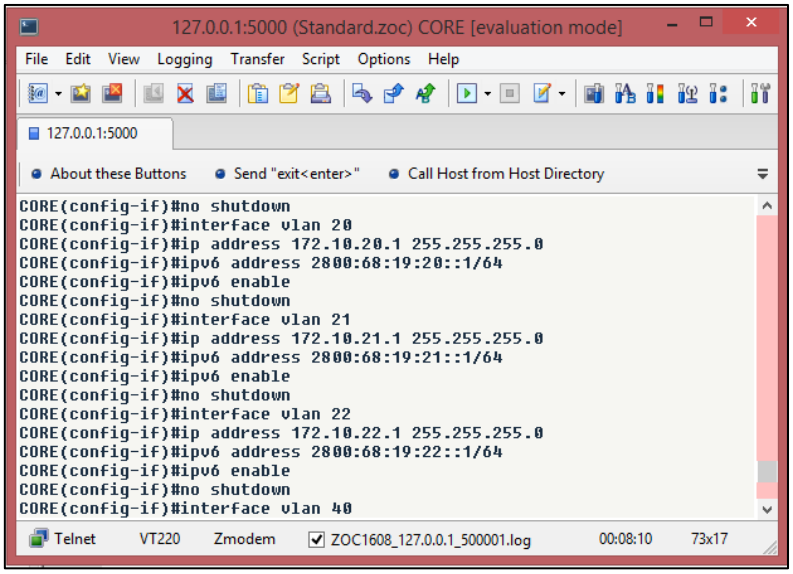


Figura 75. Asignación de direcciones IPv4 IPv6 en Switch FICA
Fuente: Switch The Core FICA

A continuación, y como muestra la figura 76 se configura las rutas estáticas en donde se encamina todo el tráfico de la red local hacia la interface del Firewall ASA 5520 tanto en IPv4 como en IPv6.

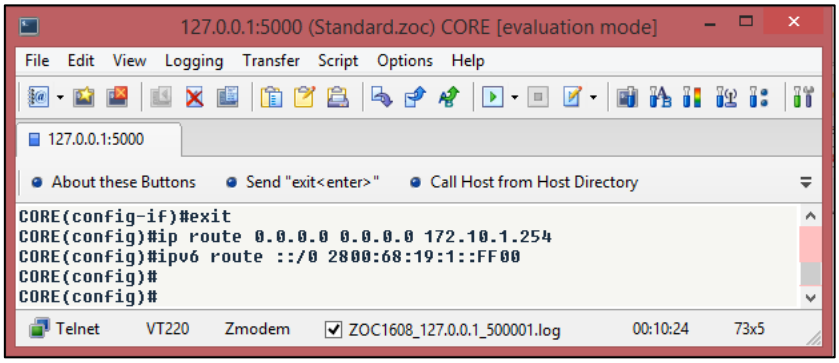


Figura 76. Configuración Rutas Estáticas hacia FIREWALL
Fuente: Switch The Core FICA

3.3.1.4 Configuración de Switch Cisco 2960 Laboratorios FICA

Para realizar las pruebas de funcionamiento correcto de la transición hay que realizar pruebas en el laboratorio de la Facultad de Ingeniería en Ciencias Aplicadas, para esto también se debe realizar la configuración de los equipos de los laboratorios, es por eso que en el Switch 2960 se realiza la habilitación de la Interfaz conectada directamente al Switch de Core en modo troncal como se observa en la figura 77.

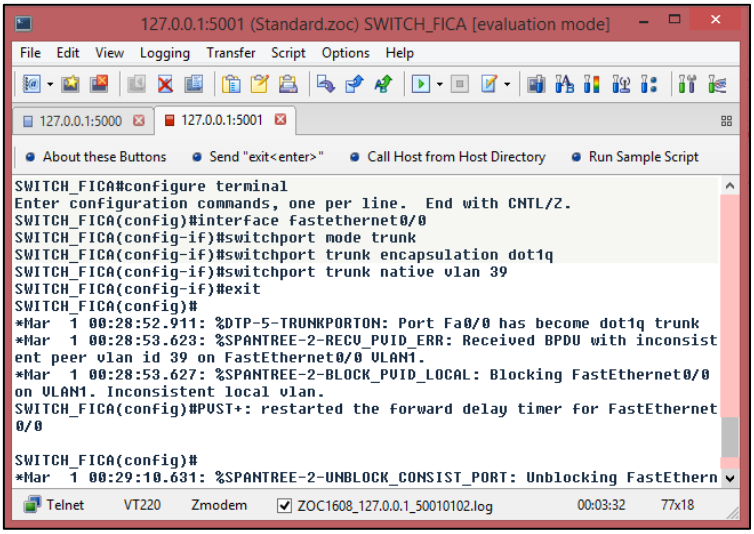


Figura 77. Habilitación Interfaz conectada al Switch de Core
Fuente: Switch Cisco 2960 - FICA

Ahora en la figura 78 se muestra la asignación de IPv4 e IPv6 en la Vlan 1 que sirve para la administración de los equipos de red, así como también la habilitación del Protocolo de Internet versión 6.

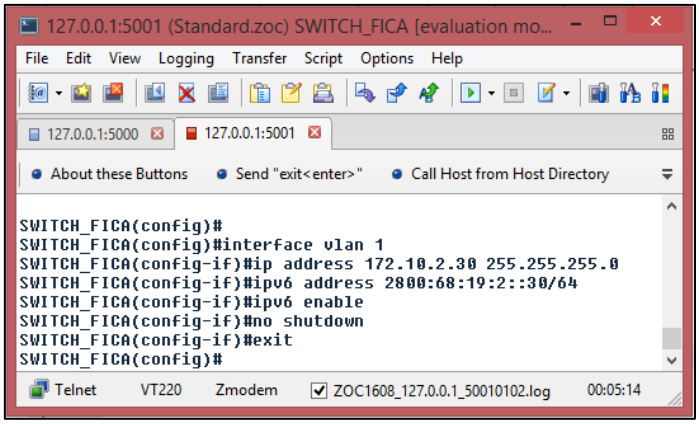


Figura 78. Asignación IPv4 e IPv6 en Vlan 1
Fuente: Switch Cisco 2960 - FICA

Una vez que se tiene configurado IPv4 e IPv6, se realiza la asignación de puertos de acceso a la Vlan de laboratorios FICA, tal y como se muestra en la figura 79.

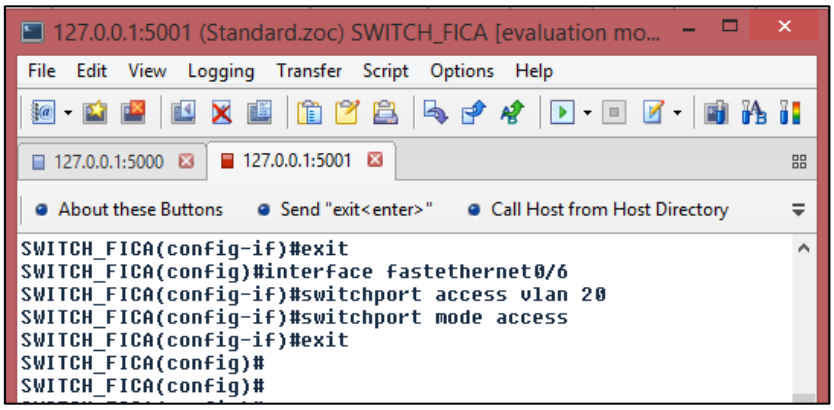


Figura 79. Asignación de puertos de acceso
Fuente: Switch Cisco 2960 - FICA

Con los comandos que se presentan en la figura 80 se realizará la asignación de la ruta por defecto o del Gateway por defecto y la deshabilitación para que el equipo no sea un enrutador sino más bien solo sea un equipo de acceso.

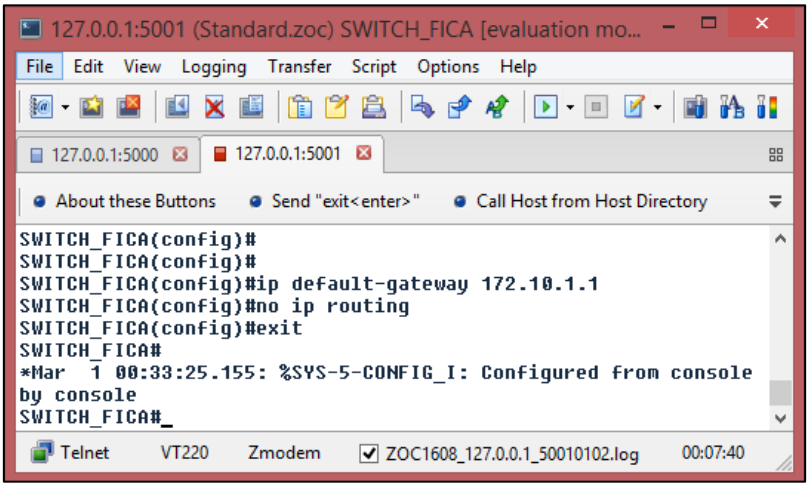


Figura 80. Asignación de Ruta por defecto
Fuente: Switch Cisco 2960 - FICA

Para comprobar la conectividad del mecanismo en Doble Pila se lo hace mediante un echo request realizado hacia el Gateway o puerta de enlace, de esta manera se demuestra que la configuración ha sido realizada de manera correcta, como se observa en la figura 81.

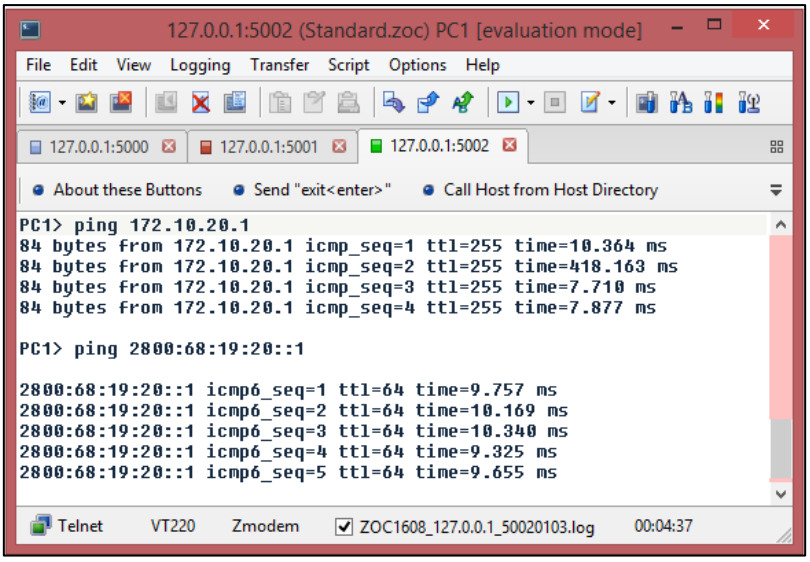


Figura 81. Ping desde Switch Lab FICA hacia su Gateway
Fuente: Switch Cisco 2960 - FICA

3.3.2 Configuración de Usuarios Finales

Para la configuración de los usuarios finales se debe tener en cuenta que se debe hacer la asignación de direccionamiento en IPv4 como en IPv6, de tal manera que se explicará el modo de asignación de cada una de las direcciones IP.

3.2.8.1 Asignación de Direcciones IPv4 e IPv6

La asignación de Direcciones IPv4 e IPv6 se lo realiza de manera gráfica en cada una de las computadoras, para explicar el procedimiento de asignación se puede ver en el anexo 4.

3.4 Pruebas de funcionamiento

Para las pruebas de funcionamiento se realizará diferentes métodos de conectividad, tanto dentro como fuera de la red de la Universidad, a continuación, se presentará de manera detallada cada prueba de acceso a los diferentes servicios.

3.3.1 Prueba de Funcionamiento de Mecanismo Doble Pila

3.3.1.1 Pruebas de conectividad

En la figura 82, se puede observar que se realiza PING6 desde el servidor DNS64 hacia los servidores de DNS UTN, Base de Datos y Aplicaciones, respectivamente. Visualizándose el NAT64 hacia dichos servidores.

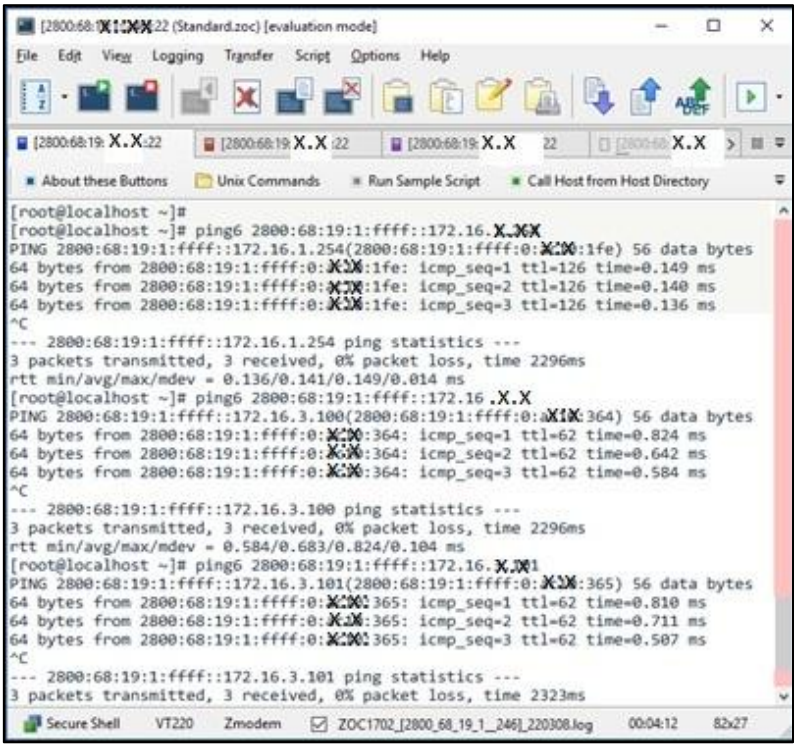


Figura 82. Conectividad NAT64
Fuente: Servidor DNS64/NAT64

En la figura 83 se puede observar que mediante la aplicación PING se tiene conectividad desde el servidor DNS hacia los servidores, se observa además que la traducción de nombres de dominio está funcionando correctamente.

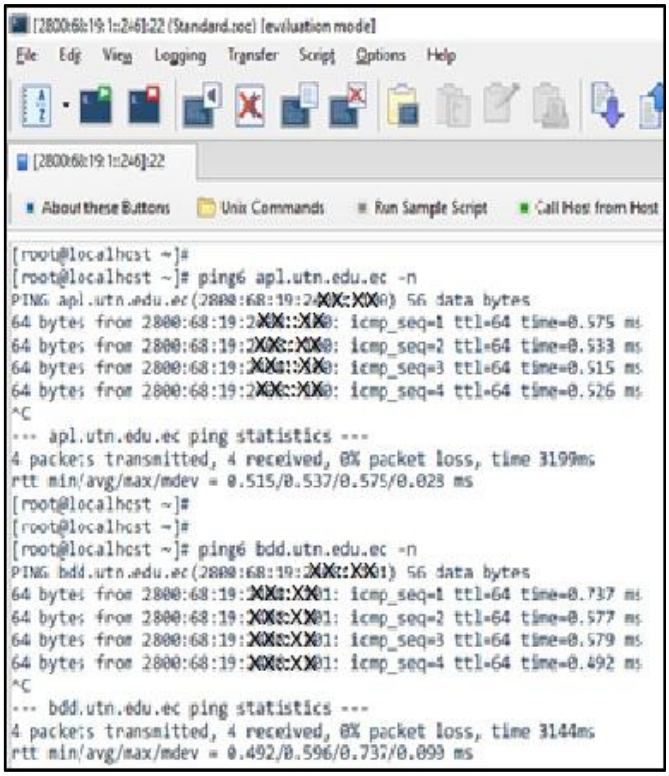


Figura 83. Ping desde DNS64 hacia servidores
Fuente: Servidor DNS64NAT64

3.3.1.2 Pruebas de acceso de red interna

En la figura 84 se puede visualizar que se tiene acceso desde la red local, de tal manera que se puede acceder al portafolio de los estudiantes y docentes de la Universidad Técnica del Norte.

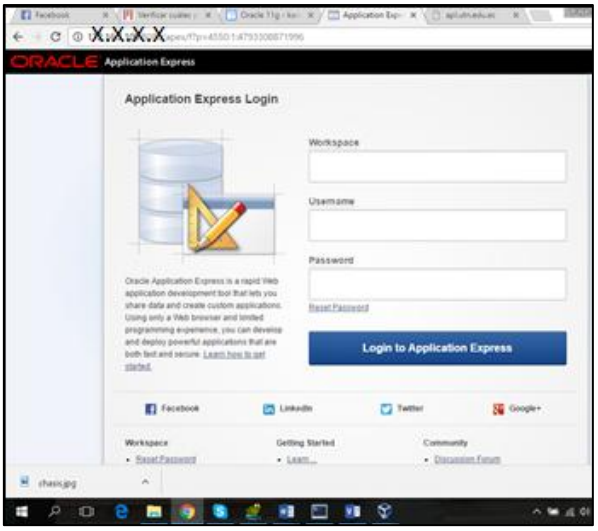


Figura 84. Acceso a Portafolio Estudiantil
Fuente: Usuario Final

En la figura 85 se puede observar el ingreso desde la red local, mediante un cliente asignado para acceder a la interfaz de control de la base de datos.

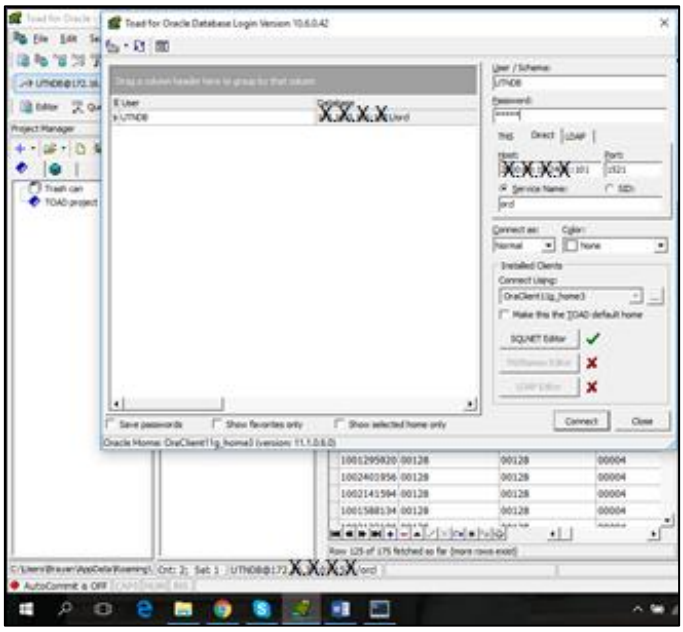


Figura 85. Ingreso Servidor de Aplicaciones
Fuente: Usuario de Base de Datos

3.3.2 Pruebas de Acceso Externo

Se cuenta con un acceso hacia el servidor de aplicaciones desde una red que se encuentra fuera de la Universidad, como se observa en la figura 86.

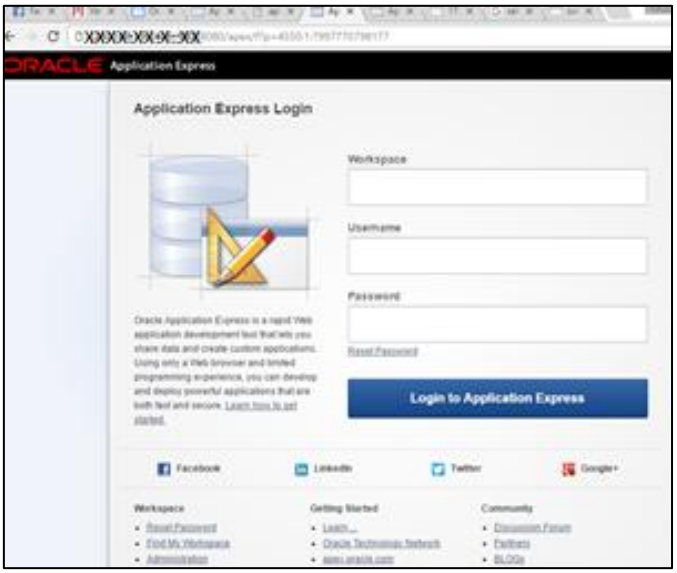


Figura 86. Acceso Externo Servidor Aplicaciones
Fuente: Usuario final red externa

Wireshark es una aplicación que permite visualizar la entrada de peticiones que realizan los usuarios, en la figura 87 se observa los parámetros del protocolo utilizado.

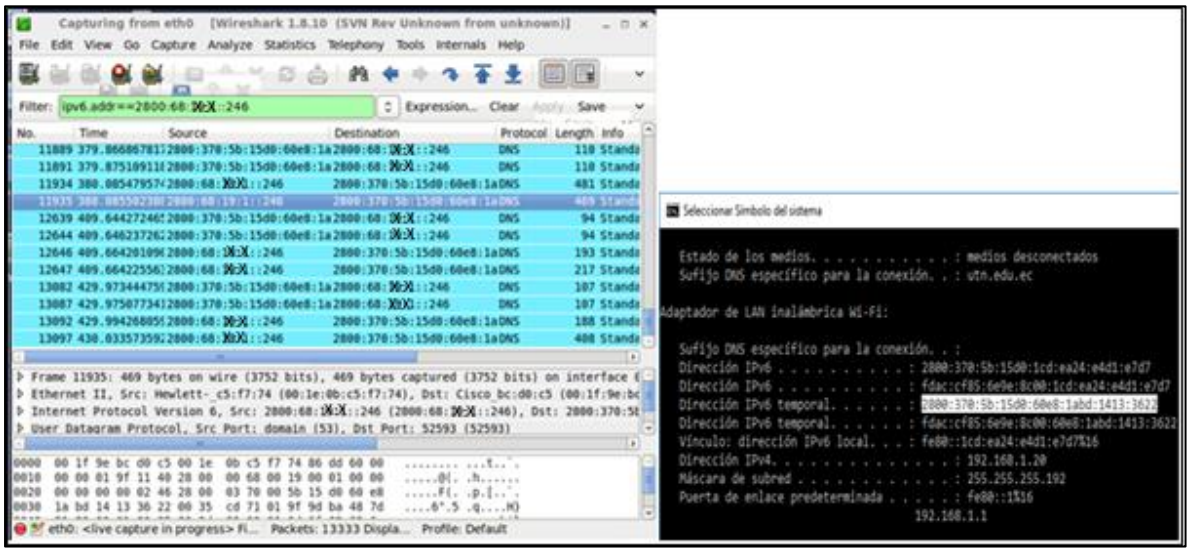


Figura 87. Captura de Wireshark paquete IPv6
Fuente: Servidor DNS64/NAT64

En la figura 88 se observa una solicitud de Echo Request desde el servidor de aplicaciones hacia el DNS64 mediante IPv6.

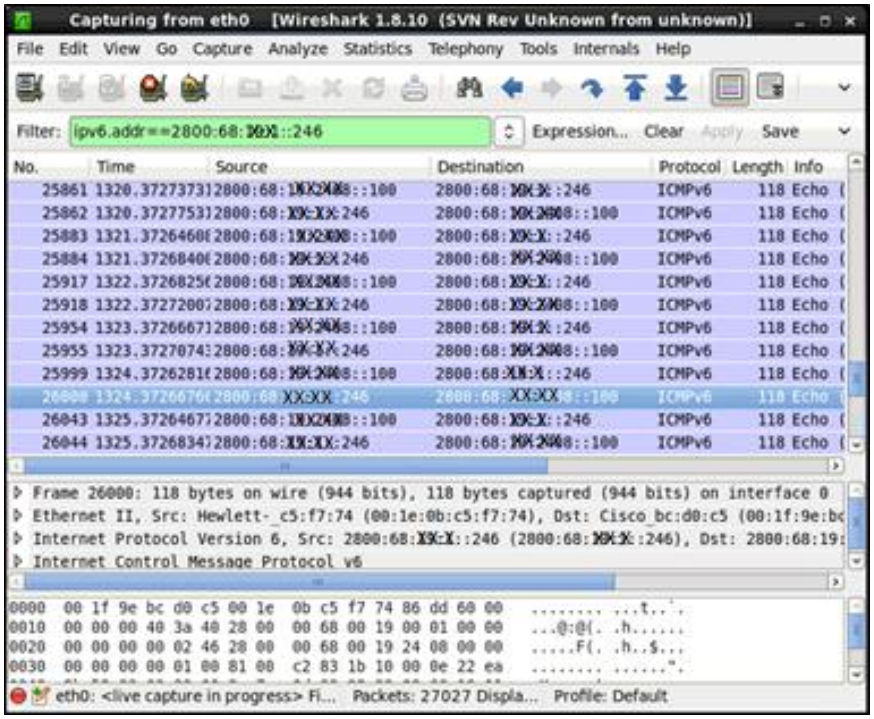


Figura 88. Echo Request desde Aplicaciones hacia DNS64
Fuente: Servidor DNS64/NAT64

Capítulo IV

Conclusiones

Para la culminación del proyecto de tesis realizado en la Universidad Técnica del Norte, se puede llegar a las siguientes conclusiones:

- Se ha realizado la transición de dos aplicaciones del Sistema Integrado de la Universidad Técnica del Norte, con el uso de mecanismos que permitan garantizar una coexistencia de las redes tanto en IPv4 como en IPv6, teniendo como resultado el acceso a los dos servidores desde usuarios IPv4 e IPv6.

- La Universidad Técnica del Norte, pasa a formar parte de la red de Internet avanzado CEDIA, siendo una de las pocas instituciones que forman parte de este consorcio, ya que cuenta con servicios y aplicaciones implementadas con el nuevo protocolo.

- El desarrollo del proyecto ha sido realizado de manera estructurada, teniendo un mecanismo ordenado para la transición, de tal manera que, se cuenta con un levantamiento de información de la red de la Universidad, un Diseño y Configuración de los Servicios, la Implementación de los Mecanismos de Transición y las Pruebas de Funcionamiento respectivas.

- Las pruebas de verificación, permitieron visualizar el desarrollo del proyecto de manera exitosa; además, se puede tener una idea clara del funcionamiento de cada uno de los servicios transicionados al nuevo protocolo.

- El desarrollo del proyecto, conlleva a realizar una investigación más profunda de lo que se ha venido aprendiendo en las aulas de la casona universitaria, de esta manera,

se logra concluir con el trabajo de tesis planteado, para desarrollarlo dentro de la universidad.

Recomendaciones

Para la culminación del proyecto de tesis realizado en la Universidad Técnica del Norte, se puede detallar las siguientes recomendaciones:

- En un futuro, se logrará tener una migración completa en la Universidad Técnica del Norte, de tal manera que, todos los hosts estén conectados mediante una dirección IPv6, pero este proceso se lo hará de manera progresiva, es decir, la migración de otros servicios será de manera transparente para los usuarios.

- Se debe tener en cuenta el sistema operativo con el que trabaja cada uno de los equipos, ya que, no todos tienen la misma metodología de configuración, muchas veces pueden variar ciertas líneas de comandos o sintaxis; además, también es importante analizar si cada uno de los equipos que se van a utilizar en el nuevo protocolo tienen soporte sobre IPv6.

- La administración de cada uno de los equipos que forman parte de la Universidad Técnica del Norte, deben ser manipulados sólo por personas autorizadas, ya que el mal uso de estos equipos, podría causar problemas muy graves en la red, además el costo de los equipos de comunicaciones es muy alto, por ende, si una persona no está capacitada para el manejo de estos equipos, podría dañarlos.

- Es importante realizar un proceso de configuración en los equipos; además, tener un respaldo de los comandos de configuración, ya que suele darse el caso que en el momento de realizar las pruebas de funcionamiento, puede fallar, de esta manera ya se tiene un respaldo de todo el proceso que se ha realizado durante el desarrollo del proyecto.

Glosario de términos

CEDIA: Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (Creada para estimular, promover y coordinar el desarrollo de las tecnologías de información y las redes de telecomunicaciones e informática)

RFC: Request for Comments (son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet)

ICANN: Corporación para asignación de nombres y números de Internet (es una organización que opera a nivel multinacional/internacional y es la responsable de asignar las direcciones del protocolo IP)

DNS: Sistema de Nombres de Dominio (Permite identificar una dirección IP mediante un Nombre dentro de la red de Internet)

CIDR: Enrutamiento entre Dominios sin Clase (Es un método para asignar las direcciones IP y el enrutamiento IP)

VLSM: Máscaras de subred de tamaño variable (Permite evitar el agotamiento de las direcciones IPv4)

NAT: Traducción de Direcciones de Red (Convierte en tiempo real las direcciones que no son compatibles para que exista comunicación y transmisión de paquetes)

UMTS: Sistema Universal de Telecomunicaciones Móviles

DDTI: Dirección de Desarrollo Tecnológico e Informático

RAD: Desarrollo Rápido de Aplicaciones

UTN: Universidad Técnica del Norte

IPV6: Protocolo de Internet Versión 6 (Diseñada para reemplazar el protocolo IPv4)

IPV4: Protocolo de Internet Versión 4 (Es el protocolo más utilizado por los usuarios de la red)

VLAN: Red de Aréa Local Virtual (Crea redes lógicas independientes en una misma red física)

IANA: Internet Assigned Numbers Authority (Supervisa la Asignación Global de direcciones IP)

LIR: Registro de Internet Local (Es una organización a la cual se le asignan bloques de direeciones IP)

RIR: Registro de Internet Regional (supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo)

IETF: Internet Engineering Task Force (Crea los estándares que se usa para la utilización de un equipo electrónico)

ECN: Explicit Congestion Notification

MTU: Unidad Máxima de Transferencia (es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones)

TTL: Tiempo de Vida (Indica la cantidad de nodos por los que puede pasar un paquete antes de ser descartado por la red)

LACNIC: Registros de Direcciones de Internet para Latinoamérica y el Caribe (Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6))

RIP: Protocolo de Información de Enrutamiento (Es un protocolo de puerta de enlace interna)

OSPF: Open Shortest Path First (es un protocolo de red para encaminamiento jerárquico de pasarela interior)

IGP: Protocolo de Gateway Interior (hace referencia a los protocolos usados dentro de un sistema autónomo)

IS-IS: Intermediate system to intermediate system (Es un protocol de estado de enlace que soporta el encaminamiento en grandes dominios)

TELNET: Telecommunication Network

A: Host IPv4(es un registro en el archivo de zona DNS de su dominio que establece la conexión entre su dominio y su dirección IP coincidente)

AAAA: Host Ipv6 (Es similar al registro A, pero le permite apuntar el dominio a una dirección Ipv6)

DHCP Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)

DMZ Demilitarized Zone (Zona desmilitarizada)

TCP Transmission Control Protocol (Protocolo de Control de Transmisión)

Bibliografía

Libros

Alonso, N. O. (2013). *Redes de comunicaciones industriales.* UNED.

Boquera, M. C. (2003). *Servicios Avanzados de Telecomunicación* . Ediciones Díaz de Santos

Cabeza, E. C. (2009). *Fundamentos de Routing.*

Comer, D. E. (1996). *Redes globales de información con Internet y TCP/IP : principios básicos, protocolos y arquitectura.* Prentice-Hall.

Dordoigne, J. (2013). *Redes Informáticas: Nociones fundamentales (Protocolos, arquitecturas, redes inalámbricas, virtualización, seguridad, IPv6).*

Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de computadoras.* Pearso Educación.

Pérez Nava Juan Carlos, H. G. (2011). *TECNOLOGÍAS Y MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6.* Mexico.

Juan Carlos Pérez Nava, E. R. (2011). *TECNOLOGÍAS Y MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6.* Mexico.

Miguel, M. V. (2011). *Instalaciones Domóticas.* Paraninfo.

Miranda, C. V. (2014). *Redes Telemáticas* . Paraninfo.

Nuria Oliva, A. (2013). *Redes de comunicaciones industriales.* UNED.

Gerometta, O. (2011). *IPv6 - Algo de Historia* .

TESIS

Alex, A. (2008). *Análisis y diseño para la instalación del protocolo IPv6 en la red.* Obtenido de http://repositorio.utc.edu.ec/bitstream/27000/1841/1/T-UTC-1332.pdf

Baus, G. A. (Julio de 2016). *Google Académico.* Obtenido de bibdigital.epn.edu.ec: http://bibdigital.epn.edu.ec/bitstream/15000/16491/1/CD-7173.pdf

Boronat Seguí, F. a. (2013). *Direccionamiento e interconexión de redes basada en TCP/IP : IPv4/IPv6, DHCP, NAT, Encaminamiento RIP y OSPF.* . Valencia: Universidad Politécnica de Valencia.

Calahorrano, F. R. (Enero de 2014). *Google Corporativo.* Obtenido de http://dspace.ups.edu.ec/: http://dspace.ups.edu.ec/bitstream/123456789/6353/1/UPS-ST001088.pdf

Cañar, P., & Cordero, S. (Septiembre de 2013). *Universidad Politécnica Salesiana.* Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/5149/1/UPS-CT002729.pdf

Rivera, D. X. (2013). *ups.edu.ec.* Obtenido de dspace.ups.edu.ec: http://dspace.ups.edu.ec/bitstream/123456789/5332/1/UPS-CT002767.pdf

REVISTAS

Awduche, D. (Noviembre de 2010). Beneficios de IPv6 para las empresas. Obtenido de http://www.verizonenterprise.com/resources/whitepapers/wp_beneficios-de-ipv6-para-las-empresas_es_xg.pdf

Cabellos, A. (2004). S6S, ipv6 servicio de información y soporte. Obtenido de Protocolo IPv6: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

URL

Alonso, J. C. (Julio de 2014). *Lacnic*. Obtenido de Lacnic: http://www.labs.lacnic.net/site/sites/default/files/ES-Transicion.pdf

anonimo. (s.f.). *Textoscientificos.com*. Obtenido de http://www.textoscientificos.com/redes/fibraoptica/tiposfibra

Boulevard, W. (septiembre de 1981). *rfc.* Obtenido de rfc: https://tools.ietf.org/html/rfc791

Cal, E. F. (Agosto de 2009). *Biblioteca.Usac.* Obtenido de Biblioteca.usac.edu.gt: http://biblioteca.usac.edu.gt/tesis/08/08_0246_EO.pdf

CEDIA. (2015). *Red Nacional de Investigación y Educación del Ecuador*. Obtenido de Red Nacional de Investigación y Educación del Ecuador: https://www.cedia.org.ec/inicio/cedia

CISCO. (2010). *IP Routing: OSPF Configuration Guide, Cisco IOS Release 15SY*. Estados Unidos: Cisco Systems, Inc.

CISCO. (29 de octubre de 2013). Obtenido de www.cisco.com/en/US/doc/security/asdm/6_1/user/guide/routing.html#wp1090636

CISCO. (25 de Agosto de 2015). *Google académico*. Obtenido de Cisco. com: http://www.cisco.com/cisco/web/support/LA/110/1108/1108948_eigrp-ipv6-00.pdf

Dye, M. A., McDonald, R., & Rufi, A. W. (2008). *Aspectos básicos de networking : guía de estudio de CCNA Exploration.* Madrid: CISCO Systems.

IANA. (Junio de 2015). *ICANN*. Obtenido de ICANN: https://www.iana.org/about

Ing. Marcelo Jaramillo, Dr. Enrique Pelaez, Ing. Otilia Alejandro. (s.f.). *nsr.org*. Obtenido de https://nsrc.org/regions/STHAM/EC/CEDIA-info-Ecuador.pdf

Juárez, M. A. (Junio de 2015). *cdigital*. Obtenido de http://cdigital.uv.mx/: http://cdigital.uv.mx/bitstream/123456789/41559/1/OrtizJuarezMiguel.pdf

LACNIC. (2016). *lacnic.net*. Obtenido de google corporativo: http://www.lacnic.net/web/lacnic/agotamiento-ipv4

Lahera Pérez, J. A. (s.f.). *IPv6. Visión general y comparativa con el actual IPv4.* Barcelona: Universidad Politécnica de Catalunya.

Lahera Pérez, J. A. (2012). *IPv6. Visión general y comparativa con el actual IPv4.* Barcelona: Universidad Politécnica de Catalunya.

Marcelo Jaramillo, E. P. (2011). *nsr.org.* Obtenido de https://nsrc.org/regions/STHAM/EC/CEDIA-info-Ecuador.pdf

Microsoft. (16 de Agosto de 2016). *technet.microsoft*. Obtenido de technet.microsoft.com: https://technet.microsoft.com/es-es/library/cc754941(v=ws.11).aspx

ORACLE. (2010). *Oracle Corporation*. Obtenido de Oracle Corporation Web site: https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0re/index.html

Anexos

Anexo 1 – Instalación Centos

1. Instalación Linux Centos 6.5

La instalación de Centos es muy sencilla, en la figura 89 se observa la primera pantalla, aparece el menú de opciones, para lo cual se elige la primera opción una vez que se inicia el asistente.

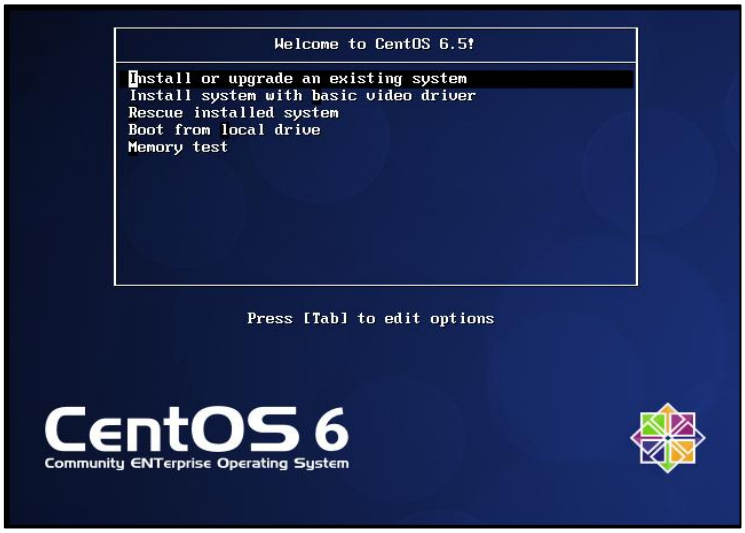


Figura 89. Pantalla de Opciones de Menú CENTOS
Fuente: Servidor DNS64/NAT64

A continuación, se debe elegir la opción Skip como se observa en la figura 90, para continuar con la instalación personalizada, en caso de realizar una evaluación de los medios de comunicación.

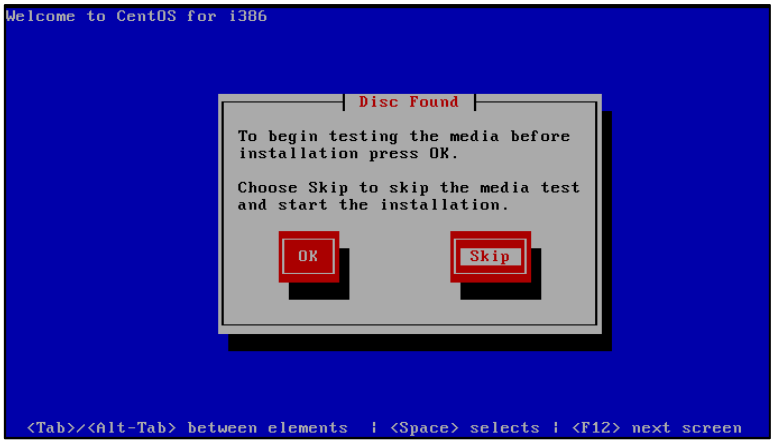


Figura 90. Análisis de Medios para Instalación
Fuente: Servidor DNS64/NAT64

El inicio de la instalación personalizada empieza desde la siguiente pantalla clic en Next como se observa en la figura 91.

Figura 91. Pantalla de bienvenida a la Instalación
Fuente: Servidor DNS64/NAT64

En la figura 92 se observa la selección del idioma, en este caso se elegirá Ingles debido a que todos los comandos a utilizar funcionan correctamente sobre este idioma, teniendo en cuenta que algunos de los comandos varían dependiendo el idioma en el que este el sistema operativo.

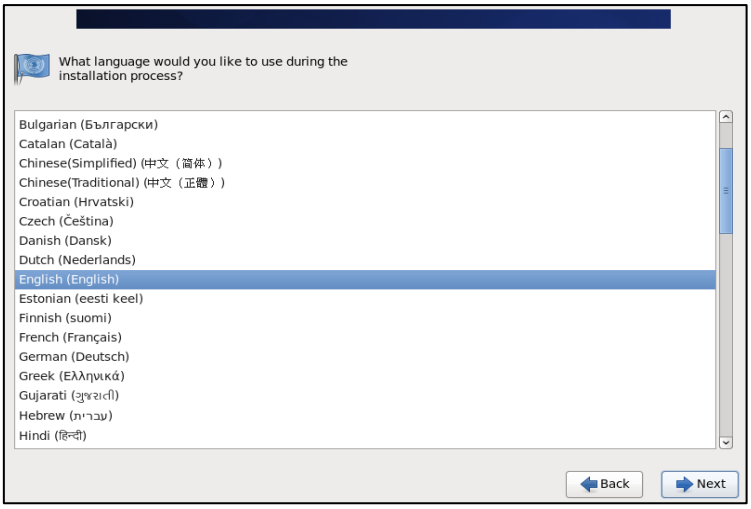


Figura 92. Selección de Idioma para Instalación
Fuente: Servidor DNS64/NAT64

Se elige la distribución del idioma del teclado que se tiene en el equipo servidor, como se observa en la figura 93.

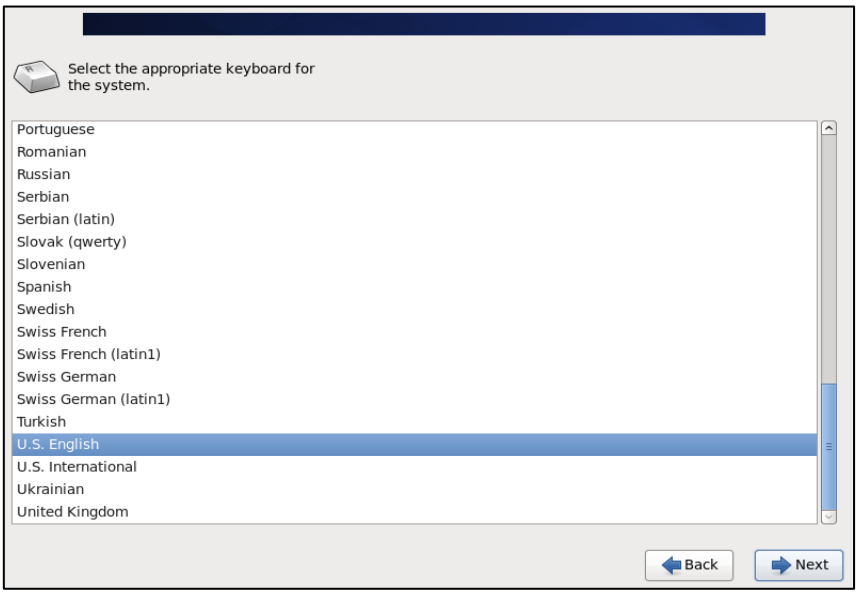


Figura 93. Selección de Idioma para el teclado
Fuente: Servidor DNS64/NAT64

La opción del tipo de almacenamiento a elegir es básica debido a que toda la información se ubica en un disco local como lo es la unidad de disco (DVD), como se observa en la figura 94.

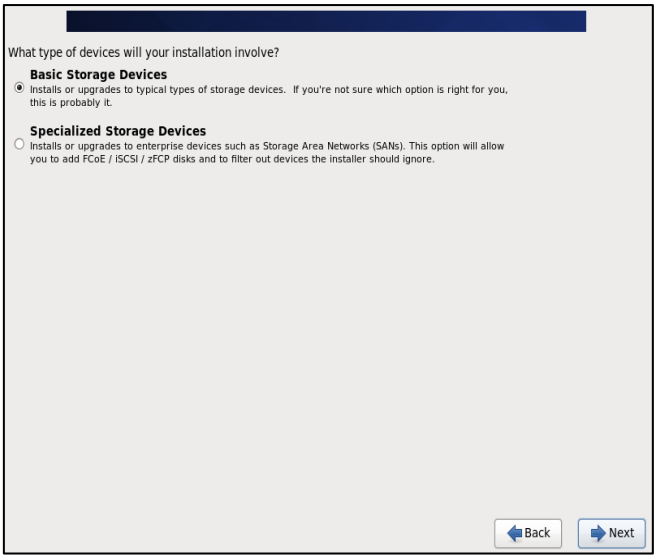


Figura 94. Selección del tipo de almacenamiento
Fuente: Servidor DNS64/NAT64

En la figura 95 se observa la ventana en la cual se coloca que si descarte todos los datos de la unidad para proceder con la instalación.

Figura 95. Descartar datos en unidad de disco
Fuente: Servidor DNS64/NAT64

Se puede dejar por defecto el nombre de localhost y si se desea después se podría cambiar como se observa en la figura 96, la configuración de red se realizará una vez Centos esté instalado, por lo tanto, solo se da clic en siguiente.

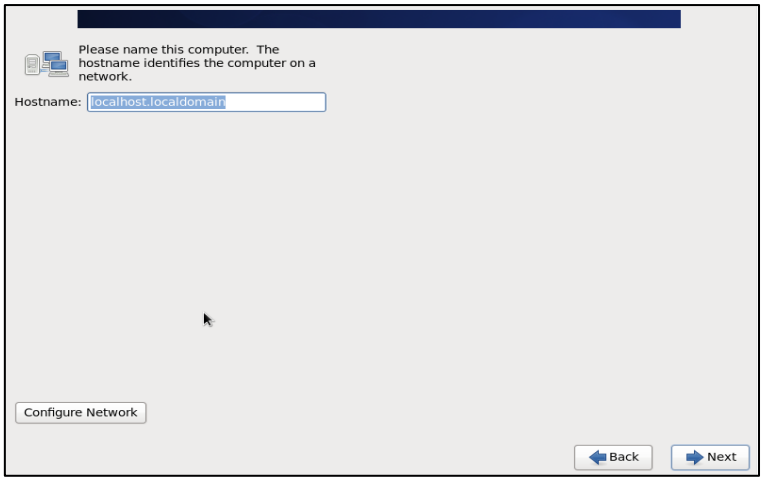


Figura 96. Nombre del Servidor
Fuente: Servidor DNS64/NAT64

En la figura 97 se observa la selección de ubicación Geográfica, en la que se selecciona la ubicación en la cual se encuentra el servidor y se da clic en siguiente.

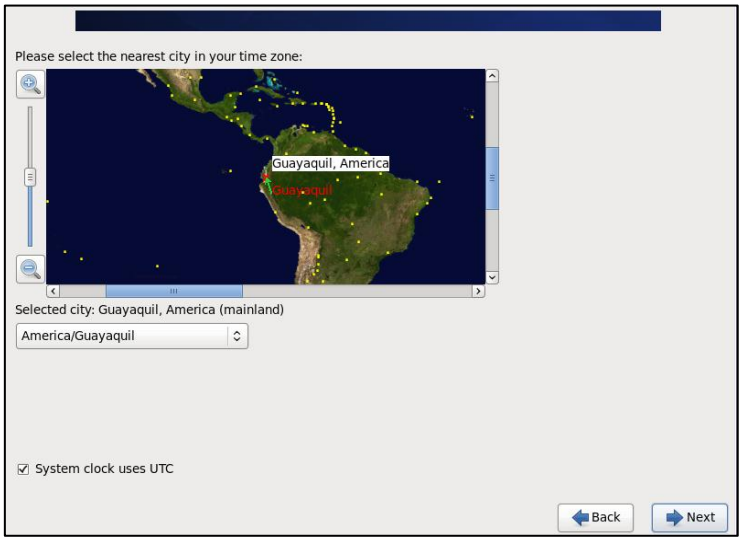


Figura 97. Definición de Zonas Horarias
Fuente: Servidor DNS64/NAT64

Escribir la contraseña de administrador, el nombre de usuario de este es root y la contraseña que se elija es muy importante ya que es con el único usuario que dé inicio se puede modificar las configuraciones del sistema, observadas en la figura 98.

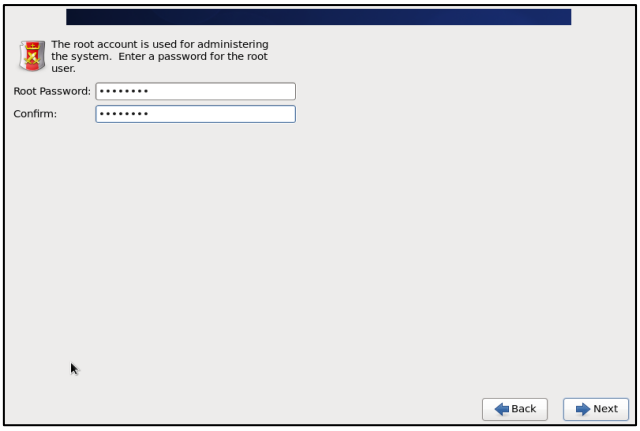


Figura 98. Inserción de contraseña de servidor
Fuente: Servidor DNS64/NAT64

Seleccionamos la forma en que se quiere configurar o crear las particiones de disco en las que va a estar ubicado Centos, como se observa en la figura 99.

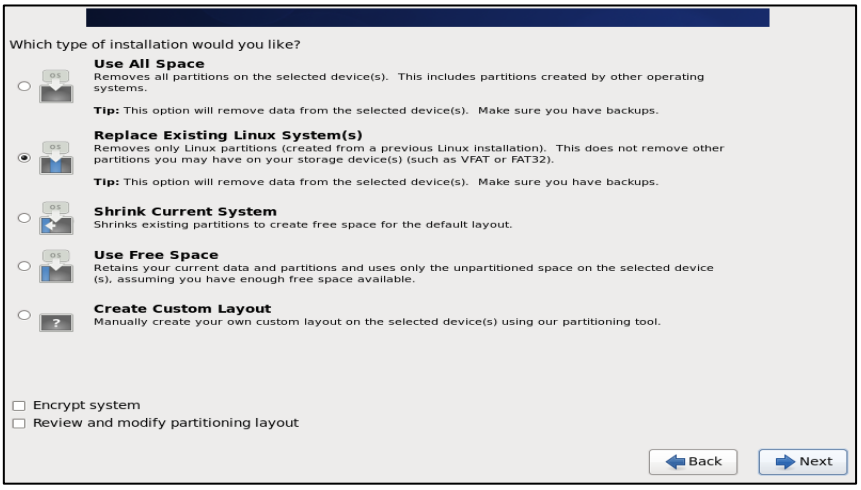


Figura 99. Selección de particiones de Discos
Fuente: Servidor DNS64/NAT64

Clic en escribir los cambios sobre el disco para continuar la instalación, figura 100.

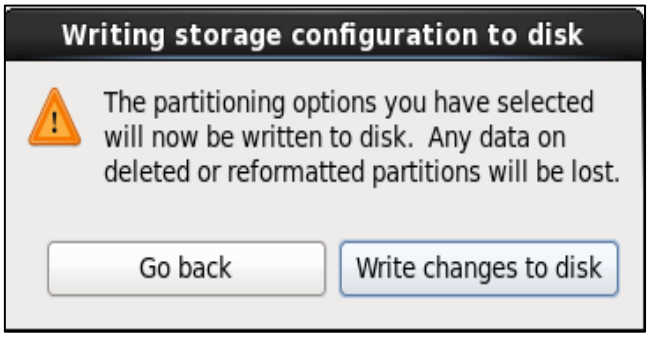


Figura 100.Confirmación de particiones de Disco
Fuente: Servidor DNS64/NAT64

En esta parte se elige cual es el tipo de entorno Linux se quiere utilizar, puede ser con escritorio o modo básico entre otras opciones, en este caso se utilizará con escritorio, figura 101.

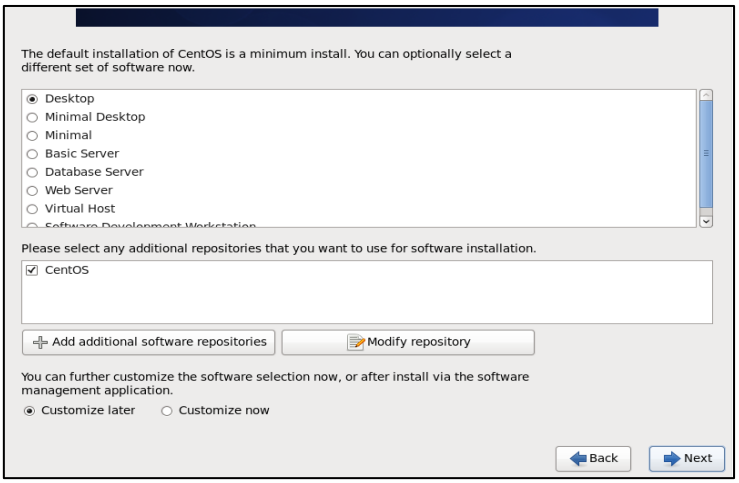


Figura 101. Elección de entorno a trabajar
Fuente: Servidor DNS64/NAT64

Instalación de Centos 6.5 en progreso, figura 102.

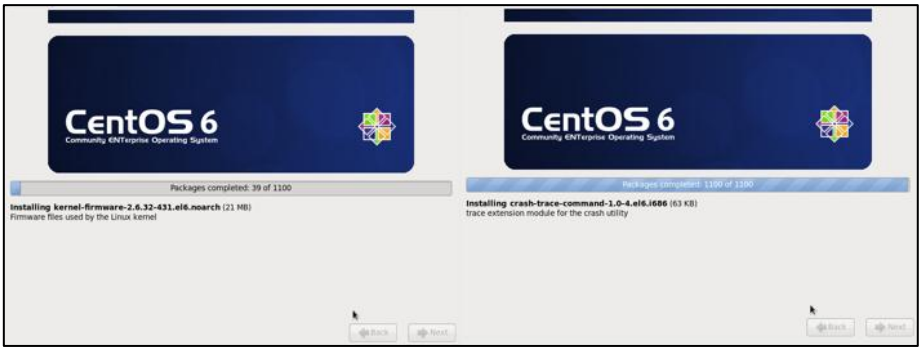


Figura 102. Progreso de Instalación Centos
Fuente: Servidor DNS64/NAT64

Reiniciar el servidor para culminar la instalación, figura 103.

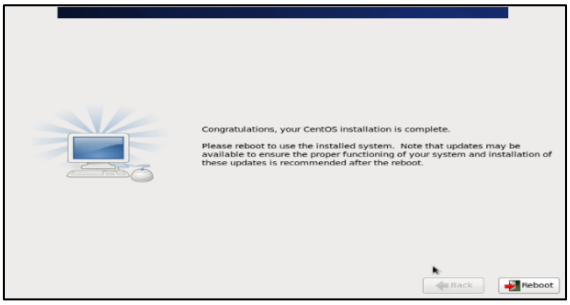


Figura 103. Reinicio del Servidor
Fuente: Servidor DNS64/NAT64

Pantalla de bienvenida cuando se inicia por primera vez el Centos, figura 104.

Figura 104. Pantalla de bienvenida
Fuente: Servidor DNS64/NAT64

Aceptación del contrato de uso del Sistema Operativo, figura 105.

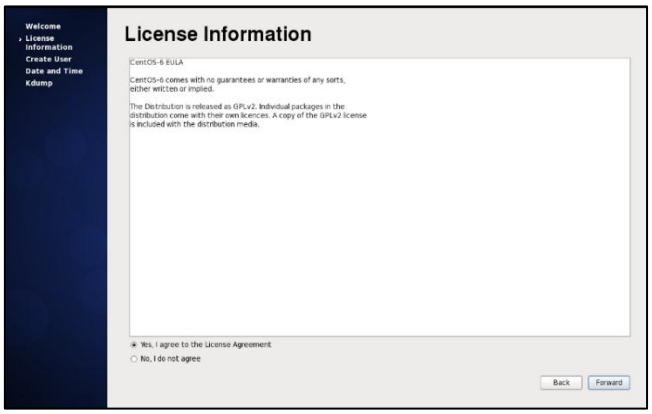


Figura 105. Aceptar términos de uso
Fuente: Servidor DNS64/NAT64

Si se desea se puede crear un usuario o solo utilizar el usuario administrador dando clic en forward, como se observa en la figura 106.

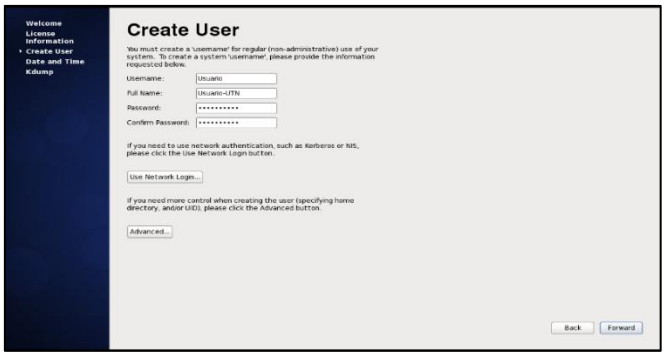


Figura 106. Creación de Usuario
Fuente: Servidor DNS64/NAT64

Seleccionar la configuración de Fecha y hora, figura 107.

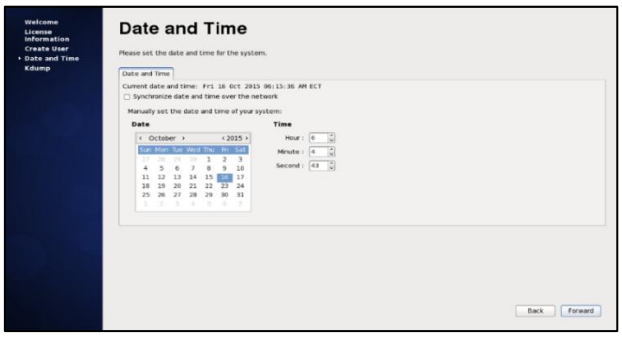


Figura 107. Definición Horaria
Fuente: Servidor DNS64/NAT64

Finalización de parámetros de inicio de sesión, figura 108.

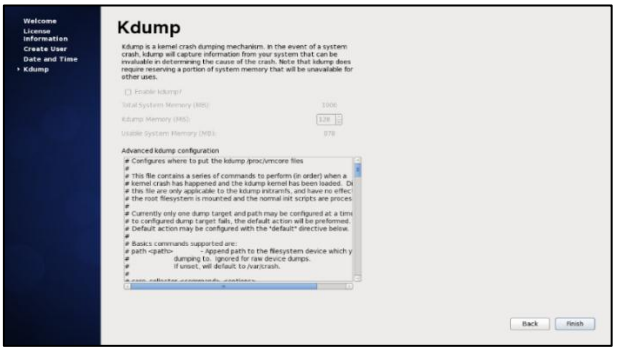


Figura 108. Finalización
Fuente: Servidor DNS64/NAT64

Inicio de sesión, se puede realizar con el usuario o con el administrador, figura 109.

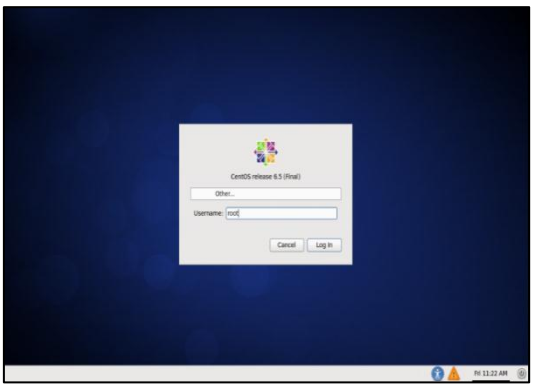


Figura 109. Inicio de sesión
Fuente: Servidor DNS64/NAT64

Anexo 2 – Instalación Oracle

Para la instalación de este sistema operativo que es con el cual trabajan los servidores que se ha implementado en el proyecto de tesis, lo primero que se debe realizar es descargarse la imagen del disco de Oracle, seguidamente se procede a arrancar y elegir la primera opción ¨Install or upgrade an existing¨ cómo se observa en la figura 110.

Figura 110. Inicio de Instalación de Sistema Iperativo
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

A continuación, en la figura 111 aparece un mensaje para ver si se quiere analizar el medio antes de empezar con la instalación, para lo cual se le da clic en Skip y se prosigue con el proceso.

Figura 111. Análisis del medio a grabar
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

En la siguiente pantalla se dará clic a ***"Next"*** y se puede elegir el idioma, en este caso inglés, figura 112.

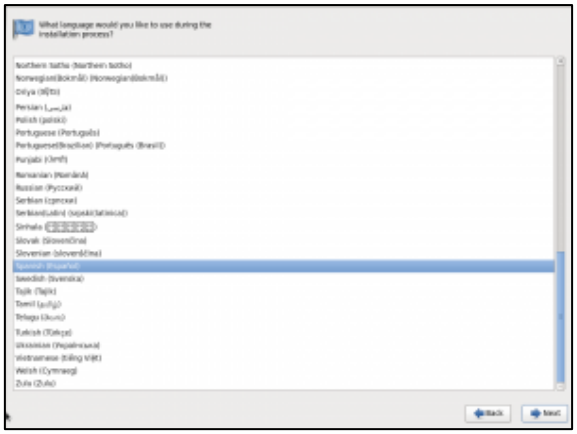


Figura 112. Idioma para la instalación del sistema operativo
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

Ahora, en la figura 113 se procede a elegir el idioma de la distribución del teclado con el cual se va a trabajar.

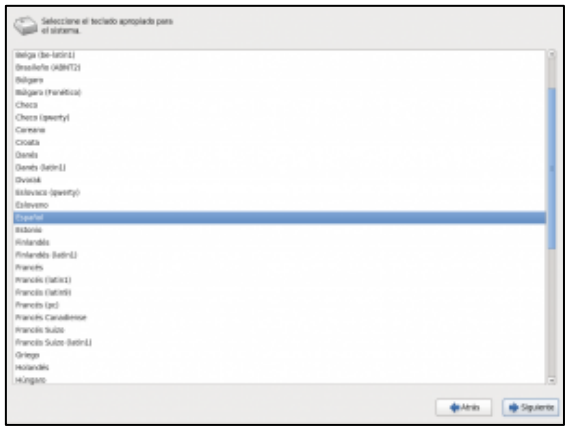


Figura 113. Idioma de distribución del teclado
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

A continuación, se procede a elegir el **tipo de dispositivo** donde se realizará la instalación, figura 114.

Figura 114. Tipo de dispositivo para instalación
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

Se le dará un nombre al equipo con el cual se va a trabajar, figura 115.

Figura 115. Determinación de nombre de máquina
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

En la figura 116 se procede a indicar la **posición geográfica** en la que se encuentre.

Figura 116.Ubicación Geográfica
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

Para tener una mejor seguridad del acceso hacia el equipo, se procede a crear una contraseña para el ingreso, figura 117.

Figura 117. Creación de contraseña
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

Ahora se procede a escoger el tipo de instalación para partición de los discos como se observa en la figura 118, para este caso se debe crear un diseño personalizado, para crear a conveniencia del usuario la cantidad de espacio en cada una de las particiones.

Figura 118. Creación de partición de Discos
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

A continuación, se procede a elegir el tipo de software que se desee utilizar, en este caso se ha elegido **Desktop,** figura 119**.**

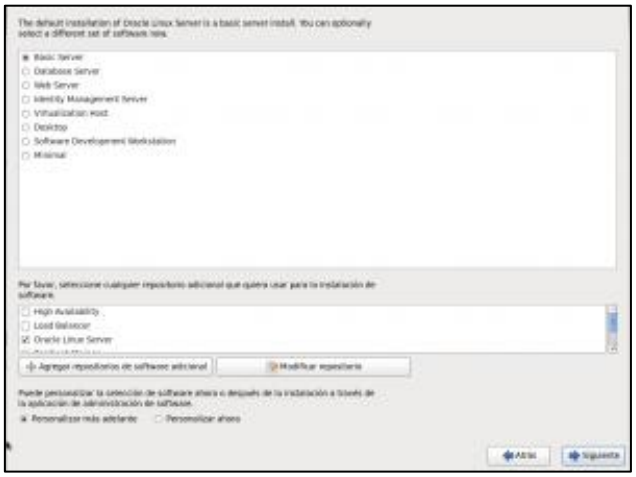


Figura 119. Elección de software de instalación
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

Una vez que se ha culminado con el proceso de instalación, se debe reiniciar el sistema, de tal manera que todas las configuraciones anteriormente mencionadas, se queden guardadas para el inicio del sistema, figura 120.

Figura 120. Reinicio del Sistema
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

De esta manera se puede observar en la figura 121 que se presenta a continuación, la pantalla de inicio del sistema operativo, para proceder a trabajar sobre el mismo.

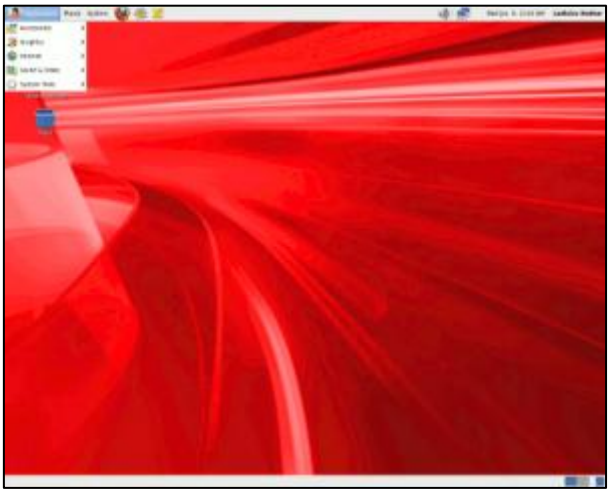


Figura 121. Pantalla de Inicio
Fuente: Recuperado de https://lignux.com/instalar-oracle-linux-6-5/

Anexo 3 – Cálculo de Asignación de una Dirección IPv4 en IPv6

Para el cálculo de la asignación de una Dirección IPv4 en una Dirección IPv6 se explicará mediante un ejemplo que a continuación se presenta:

La petición desde un usuario en IPv6 a una aplicación IPv4 o viceversa, se lo puede realizar mediante la aplicación PING. A continuación, se presenta un usuario en IPv6 nativo que realiza una petición de comunicación mediante un PING hasta una aplicación en IPv4:

- Usuario ➔2800:68:19:2408::34
- Aplicación ➔ 172.16.1.248

Existe un prefijo especial para mapear direcciones IPv4 a IPv6 el cual se puede observar a continuación: *2800:68:19:2408:ffff::/96*

Se toma los 32 bits de la dirección IPv4 y se la convierte en una dirección en binario como se observa a continuación:

- IPv4 en binario ➔ 10101100.00010000.00000001. 11111000

Una vez que se tiene esta dirección IPv4 en binario, se procede a convertirla en un número en hexadecimal, separando en cuatro bits a cada uno del binario:

- IPv4 en hexadecimal ➔ A C 1 0 0 1 F 8

De esta manera, como ya se mencionó anteriormente, se toma el prefijo especial para mapear direcciones IPv4 y se añade al final de la dirección, la IPv4 que se ha sacado en hexadecimal.

- Prefijo especial + IPv4 hexadecimal = IPv6 Asignada de aplicación
- IPV6 Asignada de Aplicación ➔ 2800:68:19:2408:ffff::AC10:01F8

Anexo 4 - Configuración de equipos de laboratorio (usuarios)

Para la configuración de los equipos de laboratorio, primero se toma en cuenta el tipo de sistema operativo que tienen instaladas las computadoras, estas computadoras cuentan con un sistema operativo Windows 10, contando con un soporte sobre IPv6, el proceso de la configuración se detallará a continuación:

Usuarios IPv4/IPv6

Primero se ubica en la parte inferior derecha de la pantalla, con clic derecho en la sección de configuraciones de red, aparece un menú en la cual se escoge abrir el centro de redes y recursos compartidos, figura 122.

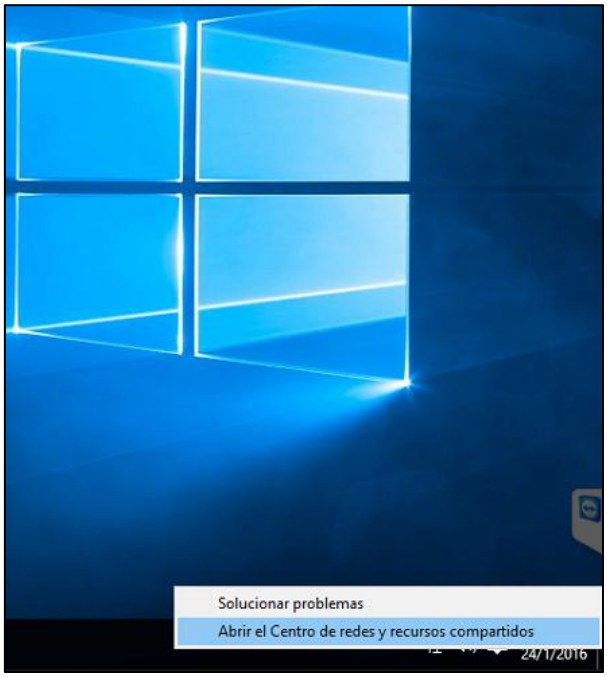


Figura 122. Abrir el Centro de redes y recursos compartidos
Fuente: Equipo de laboratorio – FICA

A continuación, se procede a elegir el adaptador de red en el cual se tiene la conexión de red de la universidad, para este caso Ethernet, como se observa en la figura 123.

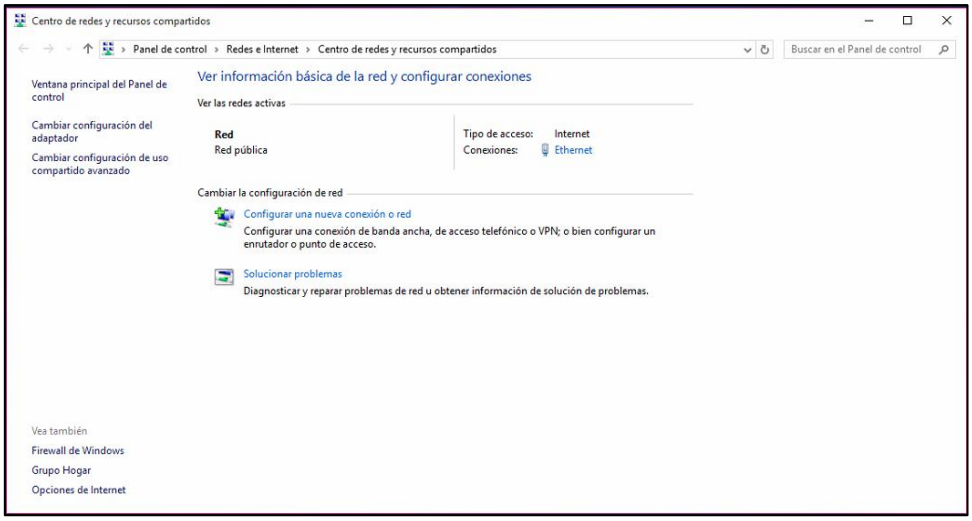


Figura 123. Selección de adaptador de red
Fuente: Equipo de laboratorio – FICA

Para configurar cada uno de los protocolos de internet, se selecciona en **propiedades,** figura 124**.**

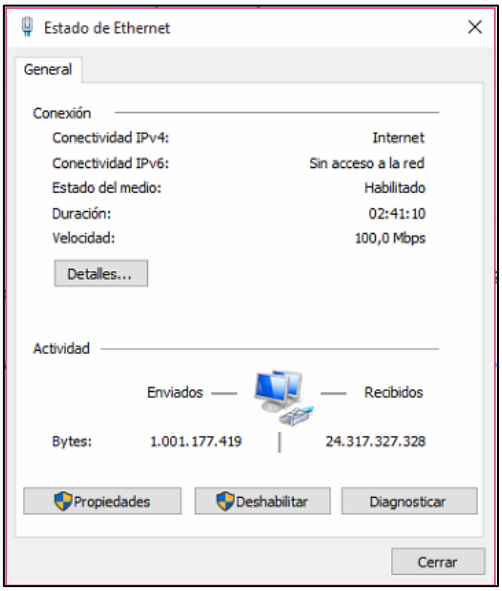


Figura 124. Estado de ethernet
Fuente: Equipo de laboratorio – FICA

A continuación, en la figura 125 se pueden observar algunas opciones, de las cuales se selecciona **protocolo de internet vesión 4 (TCP/IPv4)** y se da clic en propiedades.

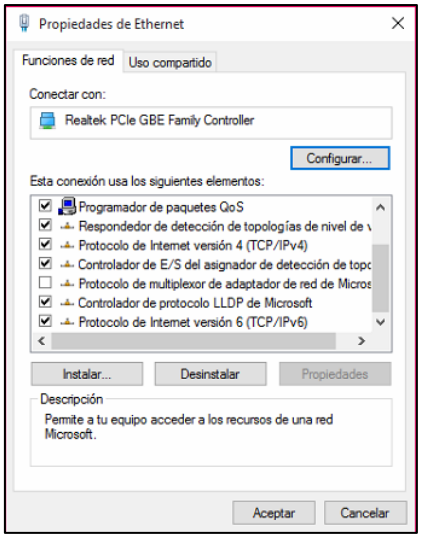


Figura 125. Propiedades Ethernet seleccion Ipv4
Fuente: Equipo de laboratorio – FICA

Ahora se presenta una imagen en la cual se observa todos los parámetros de red correspondientes a la red universitaria, como se trabaja de acuerdo a dependencias, para laboratorios FICA se asigna las direcciones correspondientes a esta dependencia y clic en aceptar para que se realicen los cambios, figura 126.

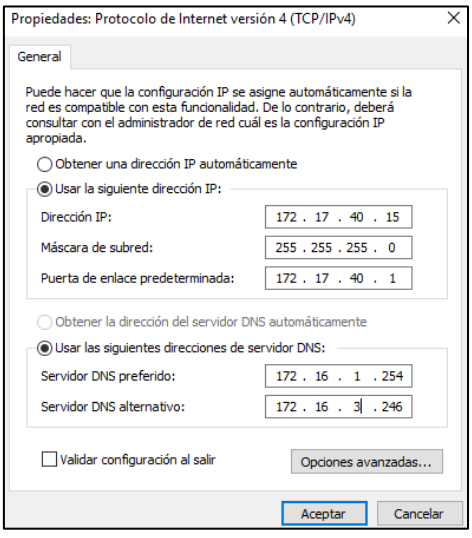


Figura 126. Parametros de red IPv4
Fuente: Equipo de laboratorio – FICA

Una vez que se ha culminado con la configuración de dirección IPv4, se procede a realizar la configuración de IPv6 para lo cual, se selecciona **protocolo de internet vesión 6 (TCP/IPv6)** y clic en propiedades, figura 127.

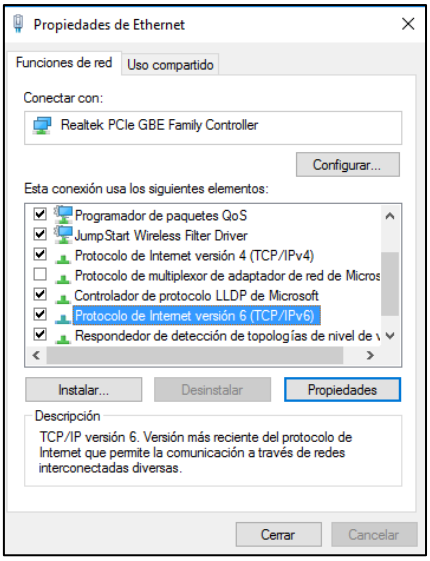


Figura 127. Propiedades Ethernet seleccion IPv6
Fuente: Equipo de laboratorio – FICA

En la figura 128 que se presenta a continuación, se procede a ingresar los campos pertenecientes a la dependencia de laboratorios FICA, tal y como se lo ha hecho en IPv4, con la diferencia que esta vez se lo realizará en IPv6, clic en aceptar para que se realicen los cambios.

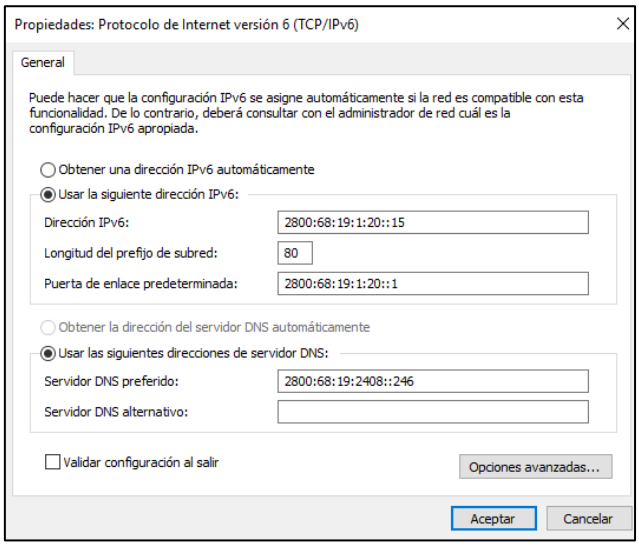


Figura 128. Parametros de red IPv6

Fuente: Equipo de laboratorio – FICA

Anexo 5 – Configuración Usuario Base de Datos

Para la configuración de los Usuarios asignados para el control de la aplicación de la Base de Datos se debe tener los instaladores de Toad para Oracle que sería la base de datos y además un cliente win32_11gR1_client para el control de la base.

En la figura 129 se observa la instalación del cliente para el control de la aplicación de la base de datos, se ejecuta el archivo de instalación setup.

Figura 129. Pantalla de Bienvenida a Instalación Cliente
Fuente: Cliente para control de Aplicación BDD

En la figura 130 se observa el directorio de Inventario en donde se realiza la instalación, se escoge el directorio y se da clic en siguiente.

Figura 130. Directorio de Inventario
Fuente: Cliente para control de Aplicación BDD

A continuación, en la figura 131 se va a seleccionar el tipo de instalación que se quiere realizar, en este caso se elige Cliente y se da clic en siguiente.

Figura 131. Tipo de Instalación de Cliente
Fuente: Cliente para control de Aplicación BDD

En la figura 132 se observa los detalles de directorio raíz, simplemente se da clic en siguiente.

Figura 132. Detalles de Directorio Raíz
Fuente: Cliente para control de Aplicación BDD

A continuación, se presenta las comprobaciones de requisitos específicos del producto, en la figura 133 se observa que aparentemente el sistema operativo no es apto, pero no tiene mayor relevancia el momento de su funcionamiento, se da clic en siguiente.

Figura 133. Comprobaciones de Requisitos Específicos del Producto
Fuente: Cliente para control de Aplicación BDD

En la figura 134 se observa un resumen de todo lo que se ha instalado hasta el momento, dar clic en instalar.

Figura 134. Resumen de Instalación de Cliente
Fuente: Cliente para control de Aplicación BDD

De esta manera se culmina con la instalación del cliente para el control de la aplicación de la base de datos como se observa en la figura 135.

Figura 135. Finalización de la Instalación
Fuente: Cliente para control de Aplicación BDD

Una vez que se ha culminado con la Instalación del cliente, se procede a realizar la instalación de la base de datos, en la figura 136 se observa los archivos de instalación que se van a ejecutar. La instalación se la hará ejecutando los archivos mostrados.

Figura 136. Archivos de Instalación de Base de Datos
Fuente: Cliente para control de Aplicación BDD

La primera aplicación que se va a instalar es *dotNetFx35setup*, se hace doble clic en el archivo y se presiona en siguiente, como se observa en la figura 137.

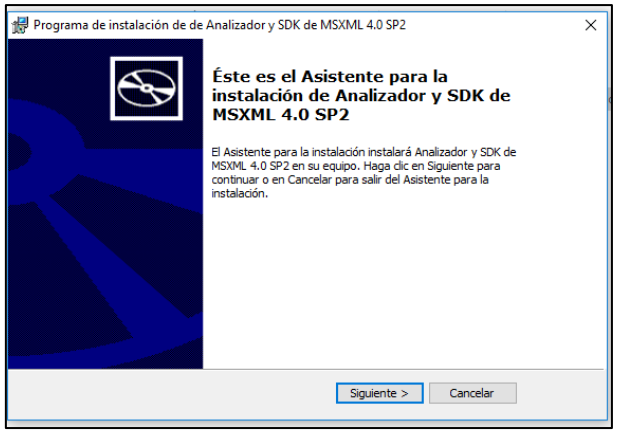


Figura 137. Asistente de Configuración MSXML 4.0 SP2
Fuente: Cliente para control de Aplicación BDD

A continuación, se presenta el contrato de licencia para usuario final, se acepta los términos y condiciones como se observa en la figura 138, clic en siguiente.

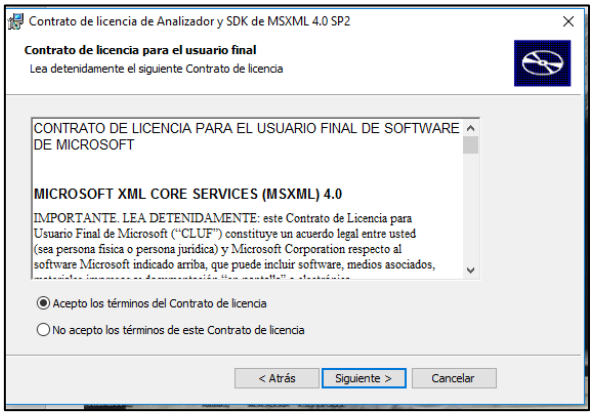


Figura 138. Contrato de Licencia para Usuario Final
Fuente: Cliente para control de Aplicación BDD

En la figura 139 se observa que el cliente debe ingresar los datos, de tal manera que tenga un identificativo, clic en siguiente.

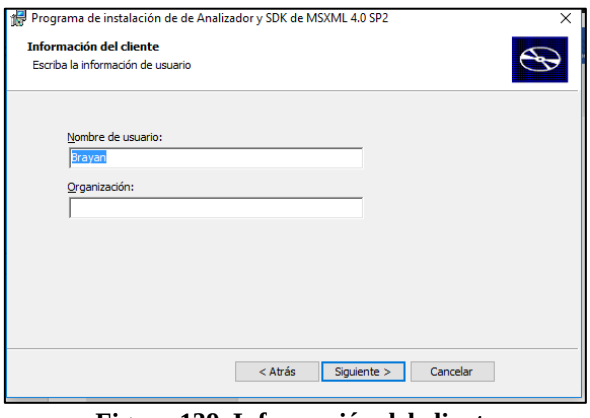


Figura 139. Información del cliente
Fuente: Cliente para control de Aplicación BDD

A continuación, se elige el tipo de instalación que se quiere realizar y se selecciona doble clic en instalar ahora, figura 140.

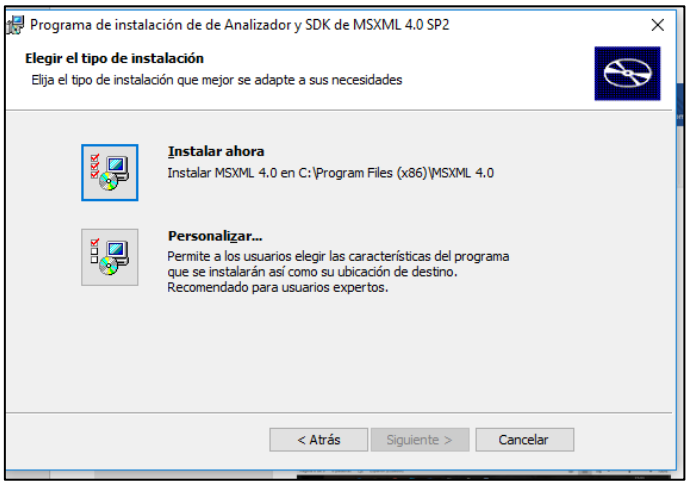


Figura 140. Tipo de Instalación
Fuente: Cliente para control de Aplicación BDD

De esta manera, se culmina con el proceso de instalación de la aplicación mencionada anteriormente, en la figura 141 se observa que la instalación se ha realizado correctamente y se da clic en finalizar.

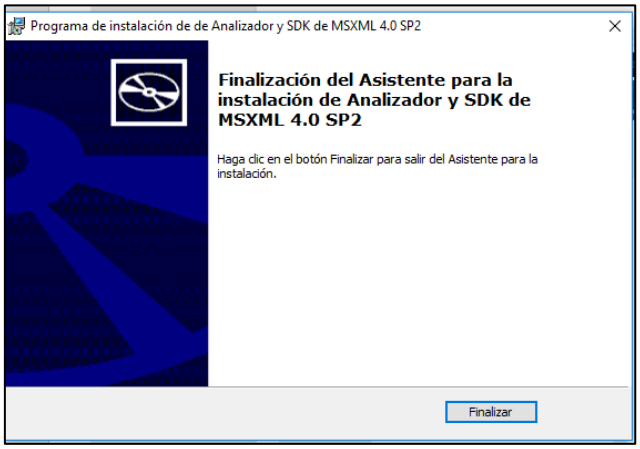


Figura 141. Finalización de Instalación MSXML 4.0 SP2
Fuente: Cliente para control de Aplicación BDD

Ahora, se procede a relizar la instalación de la aplicación *Toad Development Suite for Oracle 10.6 Commercial*, en la figura 142 se observa la pantalla de bienvenida a la instalación de la aplicación, clic en next.

Figura 142. Pantalla de Bienvenida de Instalación
Fuente: Cliente para control de Aplicación BDD

Se presenta el contrato de licencia para usuario final, se acepta los términos y condiciones como se observa en la figura 143, clic en next.

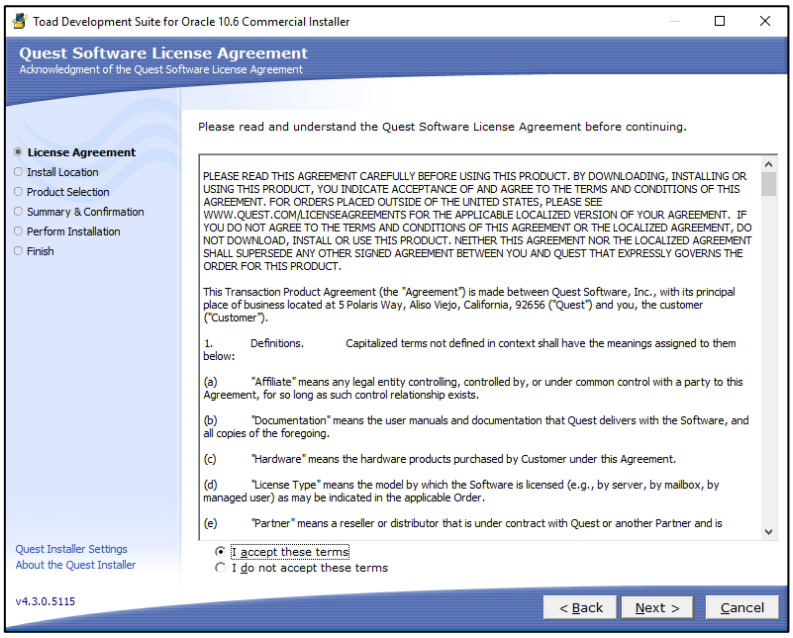


Figura 143. Aceptación de Licencia de Software
Fuente: Cliente para control de Aplicación BDD

En la figura 144 se observa la ruta de destino de instalación del software, clic en next.

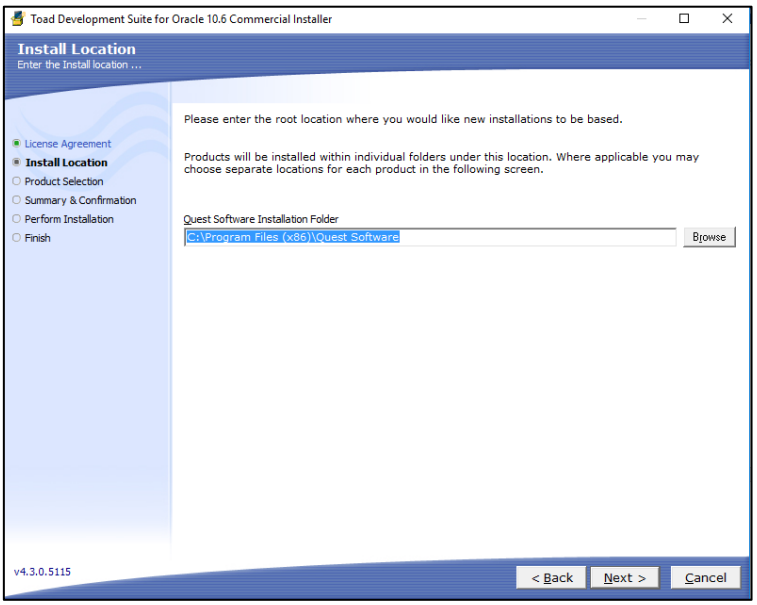


Figura 144. Directorio de Ruta de instalación
Fuente: Cliente para control de Aplicación BDD

A continuación, se presentan los productos que se van a instalar como se observa en la figura 145, clic en next.

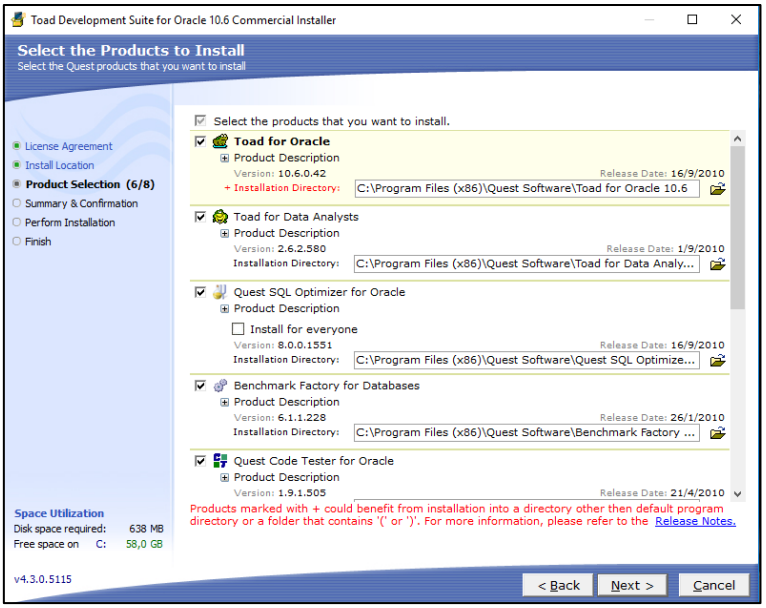


Figura 145. Selección de Productos de Instalación
Fuente: Cliente para control de Aplicación BDD

Una vez seleccionados los productos, se observa en la figura 146, que se visualizan los productos seleccionados, clic en install.

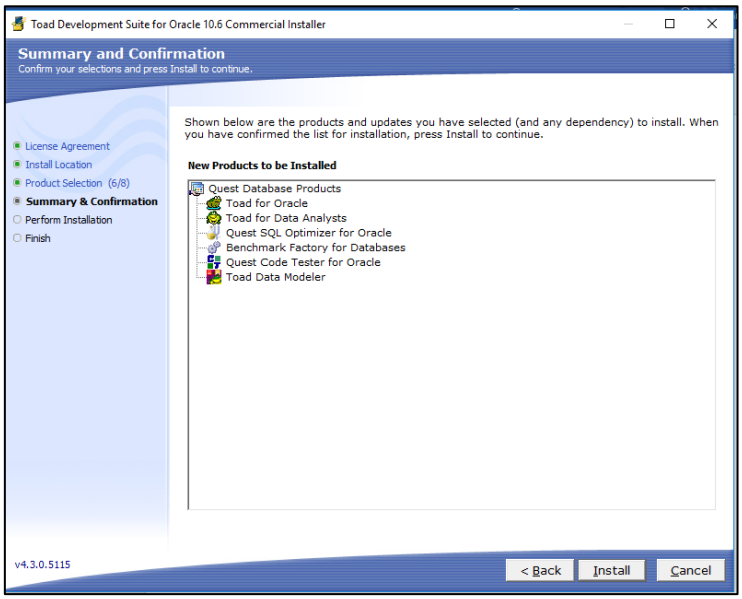


Figura 146. Resumen y Confirmación de Instalación
Fuente: Cliente para control de Aplicación BDD

En la figura 147, se visualiza la realización de la instalación de la base de datos, se tardará unos minutos, por lo que se debe esperar a su culminación.

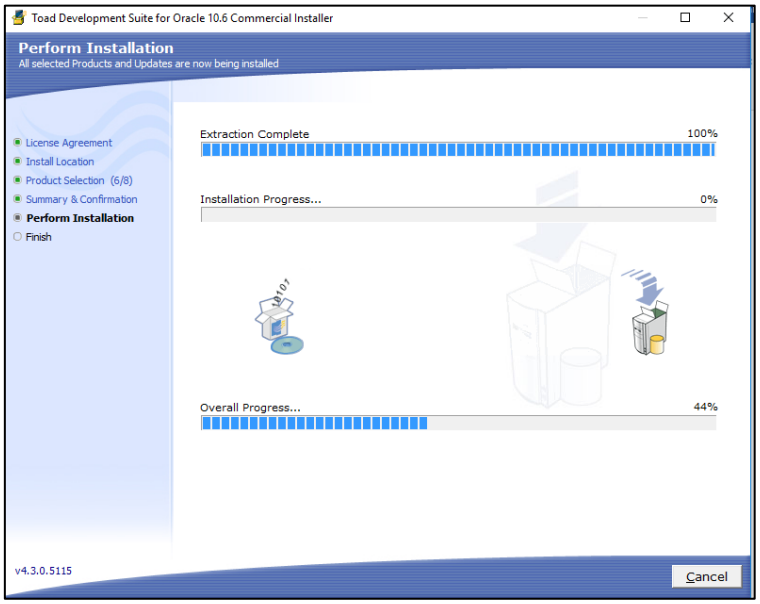


Figura 147. Instalación en curso
Fuente: Cliente para control de Aplicación BDD

Una vez finalizada la instalación, dar clic en finish, como se observa en la figura 148.

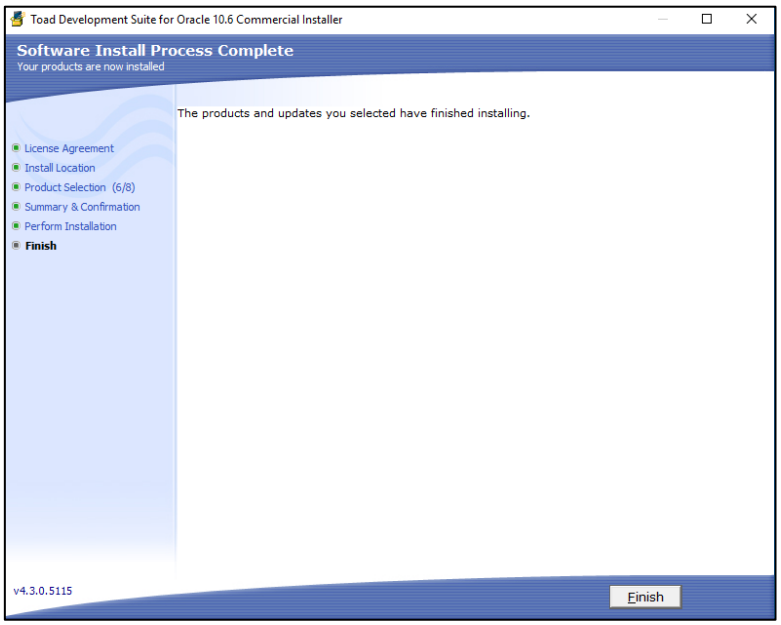


Figura 148. Culminación de Instalación Base de Datos
Fuente: Cliente para control de Aplicación BDD

Para el ingreso a la base de datos se sigue los siguientes pasos:

Se ejecuta la aplicación *Toad for Oracle 10.6* que ya se tiene instalada, aparece una ventana en la que dice si se quiere copiar los archivos de los usuarios, seleccionar no y clic en siguiente, figura 149.

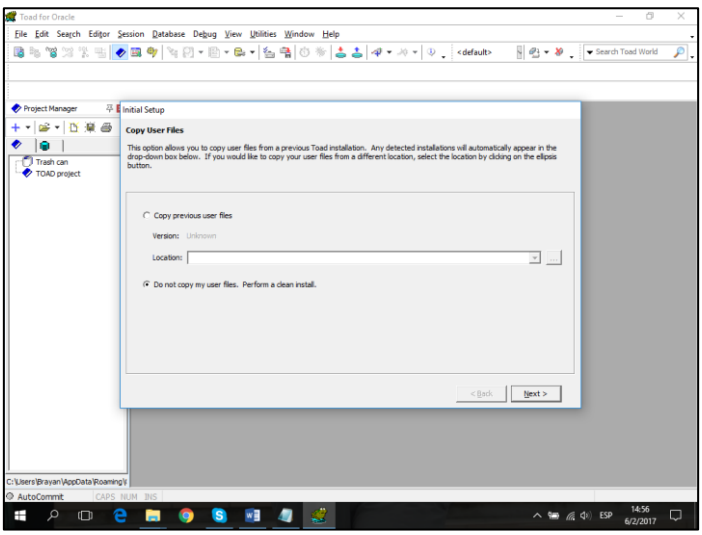


Figura 149. Copiar archivos de usuario a Base de Datos
Fuente: Cliente para control de Aplicación BDD

En la figura 150, aparece una ventana con un esquema visual de estudio, en el cual se le da clic en next.

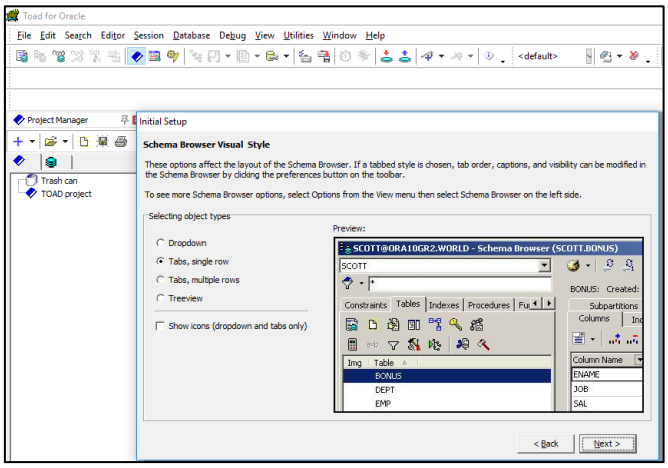


Figura 150. Estudio Visual del Esquema
Fuente: Cliente para control de Aplicación BDD

A continuación, en la figura 151 se observa las opciones generales de la base de datos, clic en next.

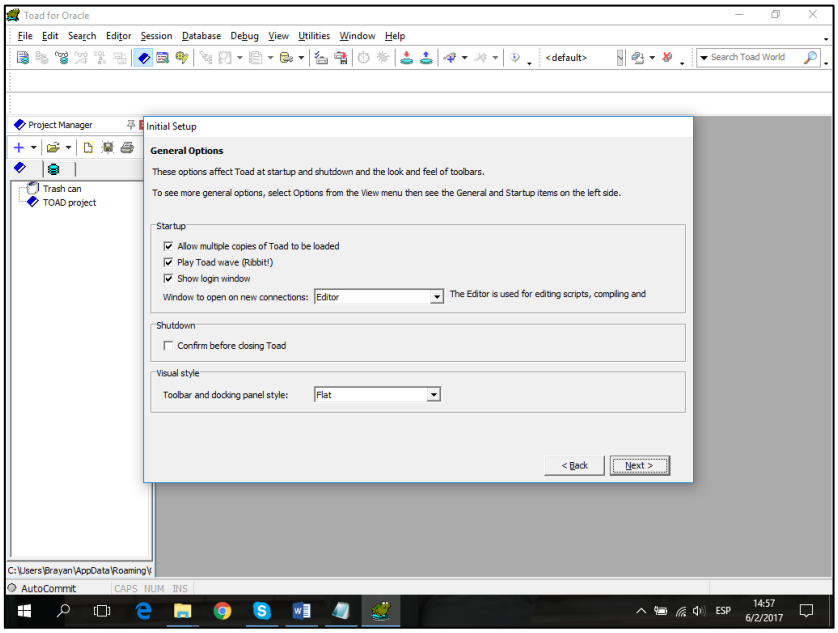


Figura 151. Opciones Generales de Base de Datos
Fuente: Cliente para control de Aplicación BDD

Finalizando con la instalación, en la figura 152 se observa la pantalla en la que se verifica que el proceso se ha realizado de manera correcta, clic en finish.

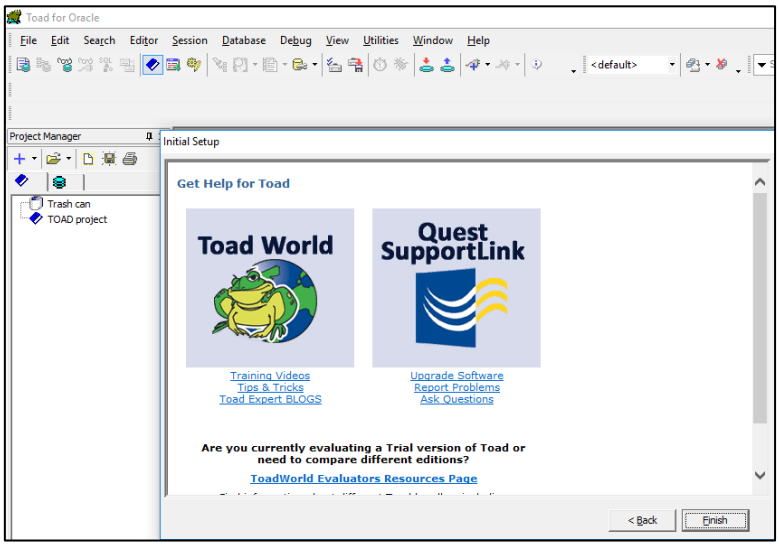


Figura 152. Finalización de la Instalación
Fuente: Cliente para control de Aplicación BDD

Para el ingreso a la base de datos, se lo puede realizar mediante el usuario de la base de datos, con una dirección IP y con la respectiva seguridad que presente la aplicación, como se observa en la figura 153.

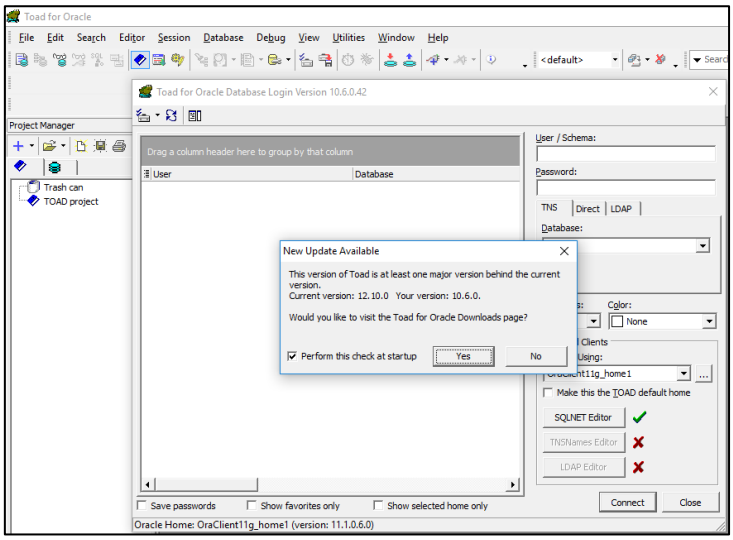


Figura 153. Ingreso a la Base de Datos
Fuente: Cliente para control de Aplicación BDD