UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"TRANSICIÓN DE SERVICIOS WEB Y FTP DE IPV4 A IPV6 MEDIANTE EL USO DE DS-LITE (DUAL-STACK) PARA LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE"

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

AUTOR: CARLOS MARIO FERNANDO OBANDO VILLADA

DIRECTOR: ING. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA-ECUADOR

2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

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 Repositorio Digital Institucional, determinó 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 participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO	
Cédula de Identidad	108526374-3
Apellidos y Nombres	Obando Villada Carlos Mario Fernando
Dirección	Rio Chimbo - Paseo del Retorno 2 Casa 85 y Princesa Pacha
E-mail	cmobandov@utn.edu.ec
Teléfono Fijo	062951551
Teléfono Móvil	0986641487
DATOS DE LA OBRA	
Título	"TRANSICIÓN DE SERVICIOS WEB Y FTP DE IPV4 A IPV6 MEDIANTE EL USO DE DS-LITE (DUAL-STACK) PARA LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE"
Autor	Obando Villada Carlos Mario Fernando
Fecha	12 de abril del 2016
Programa	Pregrado
Título por el que se aspira:	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Carlos Alberto Vásquez Ayala

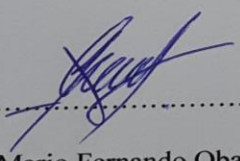
2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, CARLOS MARIO FERNANDO OBANDO VILLADA, con cédula de identidad Nro. 108526374-3, en calidad de autor y titular de los derechos patrimoniales del 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 de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

3.- CONSTANCIAS

El auto manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, al 12 día del mes de abril del 2016



.....

Carlos Mario Fernando Obando Villada

108526374-3

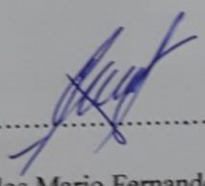
UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, CARLOS MARIO FERNANDO OBANDO VILLADA, con cédula de identidad Nro. 108526374-3, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado: "TRANSICIÓN DE SERVICIOS WEB Y FTP DE IPV4 A IPV6 MEDIANTE EL USO DE DS-LITE (DUAL-STACK) PARA LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE", que ha sido desarrollado para optar el título de Ingeniería en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, al 12 día del mes de abril del 2016



.....

Carlos Mario Fernando Obando Villada

108526374-3

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Carlos Mario Fernando Obando Villada, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste 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, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte

.....

Carlos Mario Fernando Obando Villada

108526374-3

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis "TRANSICIÓN DE SERVICIOS WEB Y FTP DE IPV4 A IPV6 MEDIANTE EL USO DE DS-LITE (DUAL-STACK) PARA LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE" ha sido realizada en su totalidad por el señor: CARLOS MARIO FERNANDO OBANDO VILLADA portador de la cédula de identidad numero:

108526374-3.

.....

Ing. Carlos Vásquez.

Director de Tesis

AGRADECIMIENTO

En el presente proyecto agradezco a mi familia por haberme dado todo el apoyo en mi etapa estudiantil y ayudarme en el cumplimiento de mis objetivos.

A mi director de trabajo de grado, Ing. Carlos Vásquez por su esfuerzo y dedicación, quien con su experiencia y conocimiento supo guiarme en la terminación de este proyecto.

A la Universidad Técnica del Norte y la Faculta de Ingeniería en Ciencias Aplicadas, por haberme brindado las herramientas necesarias y base de conocimientos para el cumplimiento de mis años de estudio y formación profesional.

Al departamento de Desarrollo tecnológico e informático por la confianza de sus dirigentes al permitir el desarrollo e implantación de mi trabajo de titulación en sus instalaciones.

Fernando Obando

DEDICATORIA

Dedico este proyecto a mis padres Sandra y Adalberto, a mis hermanas Dayana y Brighee que son mi inspiración y un motivo para siempre seguir adelante y luchar por mis metas. A toda mi familia que siempre ha estado apoyándome en mis estudios.

Fernando Obando

CONTENIDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de titulación consiste en la implementación de un mecanismo de transición de IPv4 a IPv6 utilizando una traducción que permita el acceso de los servicios Web y FTP de usuarios en la red Universitaria.

Para el desarrollo del mecanismo de transición se definió cuatro etapas de trabajo, investigación, instalación, configuración y pruebas de funcionamiento. Mediante la investigación se supo que no todos los equipos de red tienen un sistema que permita la utilización de IPv6, como fue el caso del Switch 3750, se realizó un direccionamiento de red correcto basado en las especificaciones del RFC 1884.

Durante el proceso de instalación fue necesario actualizar el ISO del Switch cisco 3750 para tener soporte de IPv6 en el equipo, la instalación de Linux Centos 6.5 y sus respectivas actualizaciones, así como también de los paquetes HTTP, APACHE y MySQL para el levantamiento del portal universitario; DHCP que permite la asignación de direcciones a usuarios de la red, VSFTPD el cual sirve para tener un servicio de transferencia de archivos el cual se asignará a dependencias universitarias y BIND para el funcionamiento del servicio DNS (servidor de nombres de dominio) quien se encargara de traducir las peticiones de registros A y AAAA en la red de la UTN.

El equipo de borde de la red Universitaria es de la empresa proveedora de servicios de internet TELCONET y está configurado con el mecanismo de doble pila. Esta configuración utiliza el recurso IPv6 asignado a la UTN por parte de CEDIA. Por ello, se realiza la configuración del mecanismo de doble pila a cada uno de los dispositivos de red y los paquetes instalados en Linux Centos, con los parámetros necesarios para su correcto funcionamiento. Finalmente se realizó las pruebas de funcionamiento en los equipos de laboratorio de la Facultad de Ingeniería en Ciencias Aplicadas.

ABSTRACT

This titling project consists of implementing a transition mechanism from IPv4 to IPv6 protocol, using a translation which allows the access of the WEB and FTP servers from students in the university network.

Four working steps has been defined, for the development of transition mechanism such as: investigation, installation, configuration and functionality tests. Through the investigation, it has become known that not all of the network devices have a system which allows the use of the IPv6 protocol, for example: Cisco Switch 3750. Also a network addressing scheme based on RFC 1884 specifications has been realized.

During the installation process, it has been necessary to update the ISO of Cisco Switch 3750 to support the IPv6 protocol. Also, Linux Centos 6.5 and its updates have been installed and HTTP, MYSQL and APACHE packages as well, all of these for the university portal web.

Other packages have been installed on the server such as: DHCP, which assigns the IP address to the network users; VSFTPD, which allows the transference of archives between the university departments and BIND, which offers the DNS service (Domain Name Server). The DNS service is that which translate the requests from A and AAAA registers in the UTN network.

The network university's edge equipment is from TELCONET internet service provider company and it is configured with dual stack mechanism. This configuration uses the UTN IPv6 resource, which is assigned from CEDIA. Thus, dual stack mechanism has been configured in each network device and Linux Centos installed packages as well. Finally, the functionality tests have been realized in the devices from FICA's network.

PRESENTACIÓN

El presente trabajo titulado "TRANSICIÓN DE SERVICIOS WEB Y FTP DE IPV4 A IPV6 MEDIANTE EL USO DE DS-LITE (DUAL-STACK) PARA LA RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE", se encuentra compuesto de los capítulos siguientes:

CAPÍTULO I: Antecedentes, Planteamiento del Problema (Antecedentes - Situación Actual – Prospectiva – Resumen), Objetivos (General y Específicos), Alcance del Proyecto y Justificación.

CAPÍTULO II: Fundamento Teórico, En este capítulo se detalla la información referente a los protocolos de internet IPv4/IPv6, DNS64, DHCP y el mecanismo DS-lite, así como también de los servicios WEB y FTP.

CAPÍTULO III: Desarrollo de la tecnología de transición, En este capítulo se presenta el análisis de equipos y servidores que soporten el mecanismo de transición DS-lite, DNS64 para la traducción de nombres de IPv6 a IPv4 y el servicio de asignación de IP a través de DHCP, además del levantamiento de servidores WEB y FTP.

CAPÍTULO IV: Implantación de Mecanismo y Pruebas de funcionamiento, En este capítulo se desarrollará la Implementación del mecanismo de transición DS-lite, mediante la utilización de equipos de laboratorios en donde se realiza las pruebas de funcionamiento, en las cuales se demuestra la confiabilidad del mecanismo de transición DS-lite en la Universidad Técnica del Norte.

CAPÍTULO V: Análisis de costo, En este capítulo se efectúa el análisis del costo de implementación de la tecnología aplicada.

CAPITULO 1

ANTECEDENTES

El presente capitulo manifiesta de manera breve la necesidad de tener un mecanismo de transición IPv4 a IPv6 en la Universidad Técnica del Norte, con la finalidad de poder aprovechar las prestaciones de la red avanzada CEDIA, reconociendo el problema y brindado una solución detallada para la coexistencia de ambos protocolos de Internet, también se especifica las áreas y campos en la UTN donde se desarrollará el presente proyecto.

1.1 PROBLEMA

Una de las principales redes de investigación en Ecuador es CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado), cuenta con una red avanzada de numerosas prestaciones permitiendo gran volumen en transferencias de información a altas velocidades, a la cual están asociadas diferentes instituciones entre ellas las de educación superior; siendo la Universidad Técnica del Norte parte de dicha entidad, brindando servicios y aplicaciones institucionales basados en el protocolo de internet versión 4 (IPv4).

En la actualidad debido al agotamiento de direcciones IPv4 el protocolo que regirá como estándar en los próximos años será IPv6, CEDIA tiene desplegado en toda la red nacional el servicio de IPv6 y actualmente universidades y organismos miembros de CEDIA se encuentran adaptándose para dar uso a esta tecnología, existe un pequeño grupo de instituciones que ya forman parte de ella estando un paso delante de aquellas instituciones que aún no cuentan con mecanismos que permitan la conectividad mediante IPv6. La red avanzada de CEDIA permite a estudiantes, profesores e investigadores de las instituciones miembro, utilizar recursos y aplicaciones de red avanzada que son difícilmente accesibles por medio de internet comercial debido a su saturación y baja disponibilidad.

1.2 OBJETIVOS

1.2.1 Objetivo General:

Emplear el mecanismo de transición DS-lite (dual-stack) IPv4 a IPv6, utilizando una traducción que permita el acceso de los servicios WEB y FTP, de usuarios en la red de la Universidad Técnica del Norte

1.2.2 Objetivos Específicos:

- Recopilar la base teórica mediante una investigación bibliográfica y documental, con la cual se sustente el proyecto en las áreas de redes avanzadas para el protocolo Ds-lite (dual-stack).

- Analizar la situación actual de red en la Universidad Técnica del Norte, de los requerimientos para la implementación del mecanismo de transición Ipv4 a IPv6 y el enrutamiento de paquetes de datos.

- Implementar mecanismo DS-lite y DNS64 para la traducción de servicios Web, Ftp y DHCP de IPv4 a IPv6.

- Ejecutar las pruebas respectivas para la verificación del correcto funcionamiento del mecanismo de traducción IPv4 a IPv6.

- Elaborar un análisis del costo que permitan justificar la implementación del mecanismo de transición tecnológica entre los protocolos IPv4 e IPv6.

1.3 ALCANCE

El presente proyecto se enfoca en el estudio de un mecanismo que permita el proceso de transición entre ambos protocolos, es decir, tener usuarios, aplicaciones y

servicios con direcciones IPv4 como con direcciones en IPv6 en la red actual de la UTN; al adoptar DS-lite (dual stack) como mecanismo de transición se cumple con el requisito que solicita CEDIA para poder utilizar las diferentes y nuevas prestaciones de la red avanzada.

La UTN al no disponer del medio para una transición de direccionamiento IPv4 a IPv6 que es inminente, se ve en la necesidad de analizar los recursos con los que cuenta la casona universitaria y así determinar cuál es la situación actual de la red en cuanto al recurso disponible, para que la implementación de DS-lite en la institución sea satisfactoria.

Se implantará el mecanismo DS-lite que está construido en túneles IPv4 en IPv6 para asegurar la coexistencia de los protocolos IP, los dispositivos IPv6 nativos se conectaran directamente de internet mediante enrutamiento IPv6 y no requieren ninguna traducción, es decir que no pasaran por el túnel proporcionado por este mecanismo. Además, presta cualquier tipo de combinaciones entre aplicaciones IPv4/IPv6; cabe señalar que al levantar un servidor DNS64 permitirá que DS-lite envié peticiones tanto de nombres como de direcciones en IPv6. Para conectar los usuarios nativos IPv6 en la red de la UTN es necesario habilitar el servicio DHCP, con la finalidad de conectar los dispositivos con el servicio WEB mediante el portal universitario y FTP a través de las carpetas de usuario de la Universidad Técnica del Norte.

Las pruebas de funcionamiento se realizarán en tres laboratorios de la UTN, organizados de la siguiente manera: El primer laboratorio dispondrá solamente direccionamiento IPv4, el segundo laboratorio en IPv6 y el tercer laboratorio una combinación de ambos protocolos IP, a través de estos se podrá acceder a los servicios WEB y FTP previamente levantados en IPv6, demostrando la coexistencia de protocolos IPv4 e IPv6 mediante el mecanismo DS-lite (dual-stack).

Finalmente se realizará un análisis en cuanto a costos de implementación que permita justificar la inversión empleada para la habilitación del mecanismo de transición DS-lite.

1.4 JUSTIFICACIÓN

El aporte que este proyecto tendría para con la sociedad es cumplir con el derecho al "el acceso universal a las tecnologías de información y comunicación" (Constitución del Ecuador, 2008), debido al agotamiento del protocolo IPv4 esto no es posible, ya que el protocolo IPv6 se ha planteado por parte de la IETF como solución al proporcionar un recurso relativamente infinito de direcciones. Además de contribuir con el propósito de la universidad técnica del Norte en cuanto a la formación de profesionales líderes, críticos, emprendedores y humanistas.

Al contar con DS-lite como mecanismo de transición IPv4 a IPv6 en la red de la Universidad Técnica del Norte se dará inicio a un proceso de renovación de la tecnología vigente actualmente en las redes de comunicación. Es aplicable la implementación de dual stack lite en la UTN ya que dispone de los recursos y herramientas necesarias para servicios y aplicaciones usando el protocolo IPv6.

El estándar que rige actualmente las redes de comunicación es el protocolo IPv6 y el cual se recomienda que su transición sea de manera progresiva mediante el uso de mecanismos. DS-lite es una solución factible para la coexistencia de los protocolos IPv4/IPv6 que garantice la conectividad e interacción de usuarios que utilizan dispositivos en ambos protocolos IP en la Universidad Técnica del Norte, siendo el mecanismo que va a permitir aportar y aprovechar las aplicaciones y recursos de la red avanzada de CEDIA.

Este tipo de proyectos permite aumentar el conocimiento en la formación como futuros profesionales de la carrera en Ingeniería Electrónica y redes de comunicación, así como también la experiencia en la implementación de nuevas tecnologías.

1.5 METODOLOGÍA

La metodología de investigación que se determina para el desarrollo del proyecto está basada en el método deductivo, haciendo énfasis en un proceso analítico sintético que presenta afirmaciones generales y particulares en los protocolos de internet versión cuatro y versión seis.

CAPITULO 2

2 FUNDAMENTO TEÓRICO

2.1 INTRODUCCIÓN

CEDIA fue oficialmente creado el 18 de septiembre del 2002, inicialmente conformada por 7 instituciones de educación superior, 2 organismos públicos y 2 instituciones. El estatuto de CEDIA es aprobado y registrado el 6 de enero de 2003 por el subsecretario de educación; ya para junio de 2003 Ecuador forma parte de la Cooperación Latinoamericana de Redes Avanzadas (red CLARA) y después de un año contrata internet comercial.

La red avanzada de CEDIA en el transcurso del tiempo ha tenido diferentes inconvenientes que se han venido superando, en un inicio existían dos inconvenientes: baja capacidad de las ultimas millas de los miembros y la falta de transparencia de la red avanzada al interior de las instituciones, la solución a la transparencia se realizó mediante la implementación de BGP en los equipos de ruteo de CEDIA y así también se aumentó de la capacidad de ultimas millas de conexión de la red avanzada.

CEDIA fue la primera red ecuatoriana en ocupar IPv6 nativo y a partir del año 2013, el consorcio cuenta con 155 Mbps en la Red Avanzada para vinculación con la Red CLARA y 22 STM-1[1] de capacidad de Internet Comercial,

[1] STM-1 Módulo de Transporte Síncrono, correspondiente al primer nivel básico y es una trama de 2430 bytes, distribuidos en 9 filas y 270 columnas.

2.1.1 CEDIA

Es el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado, es la Red Nacional de Investigación y Educación Ecuatoriana (NRENs National research and Education Networks). Su creación fue para estimular, promover y coordinar el desarrollo de las tecnologías de información y las redes de telecomunicaciones e informática, enfocándose en áreas de carácter científico, tecnológico, innovador y educativo en el Ecuador.

CEDIA ofrece una gran variedad de servicios para investigadores y fines académicos, siendo una herramienta que ayuda a la enseñanza e investigación, brindando una gran conectividad, capacitaciones, infraestructura, repositorios, proyectos, colaboración, eventos, financiamiento y publicación de resultados.

La misión del consorcio se centra en "Promover, coordinar y desarrollar redes avanzadas de informática y telecomunicaciones para impulsar, en forma innovadora, la investigación científica, tecnológica y la educación en el Ecuador." (CEDIA, s.f.) Además de trabajar por ser referente nacional en servicios de redes avanzadas con el fin de fomentar la investigación y educación en el Ecuador.

Los beneficios de formar parte de CEDIA son muchos entre los cuales se puede señalar: Acceso a publicaciones científicas y bibliotecas digitales, uso de recursos de computación avanzada de altas prestaciones, servicios en la nube, entre otros. (Figura 1)

Figura 1. Imagen institucional CEDIA

Fuente: Recuperado de http://www.cedia.org.ec/inicio/imagen-institucional

2.1.2 Red avanzada

CEDIA tiene desplegado en toda la red nacional el servicio de IPv6 y actualmente universidades y organismos miembros de CEDIA se encuentran adaptándose para dar uso a esta tecnología, existe un pequeño grupo de instituciones que ya forman parte de ella e interactúan sobre esta red, estando un paso delante de aquellas instituciones que aún no cuentan con mecanismos que permitan la conectividad mediante IPv6 o están en el proceso de empezar la adaptación de este protocolo de internet. La red avanzada de CEDIA permite a estudiantes, profesores e investigadores de las instituciones miembro, utilizar recursos y aplicaciones de red avanzada que son difícilmente accesibles por medio de internet comercial debido a su saturación y baja disponibilidad.

Un anillo de fibra óptica con capacidad de 1Gbps forma RACE (Red Avanzada de CEDIA) que está integrado por las diferentes instituciones en todo el país garantizando su calidad.

CEDIA al formar parte de la RedCLARA que está constituida por catorce países de Centro y Sudamérica, está interconecta con redes avanzadas internacionales en las que se puede mencionar a Norte América, Europa, Asia y África. Entre estas redes se cuenta Internet2, GEANT2, CANARIA, APAN y TERNA. (Figura 2)

Figura 2. Mapa de red avanzada

Fuente: Recuperado de http://www.cedia.org.ec/conectividad/red-avanzada

2.1.3 Internet

Red mundial que genera un intercambio de intereses intercomunitarios y entre grupos en temas específicos alrededor de todo el planeta, en la que se tiene acceso a todo tipo de información, a su vez transferencia y visualización de documentos, conversaciones en tiempo real, envió de correo electrónico y muchos más servicios y aplicaciones. El Internet de CEDIA permite tener acceso a todos los servicios y aplicaciones como también a: Google, Youtube, Facebook, Twitter, portales universitarios, entre otros, a muy alta velocidad.

Con el esquema de Internet de CEDIA el beneficio se encuentra en la reducción de costos muy por debajo de la media del mercado, además entrega a las instituciones miembros en capacidades de acuerdo a la necesidad de cada uno. (Figura 3)

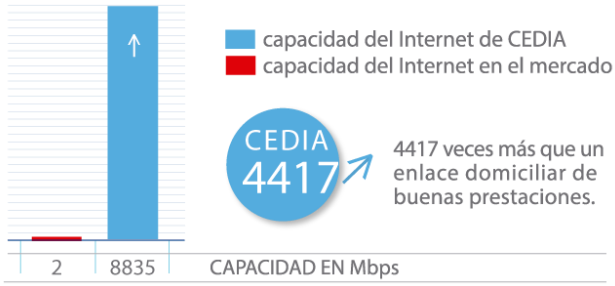


Figura 3. Internet CEDIA

Fuente: Recuperado de http://www.cedia.org.ec/conectividad/internet

2.1.4 Miembros IPv4 e IPv6

La Red Académica Avanzada de Ecuador - Red CEDIA en la que se encuentran interconectadas las principales universidades, escuelas politécnicas, institutos de tecnología y desarrollo del País, para esta red quienes cuentan con infraestructura de acceso a la red avanzada se mencionan en la tabla 1.

Tabla 1. Miembros de CEDIA

Miembro CEDIA	**IPv4**	**IPv6**
Escuela Politécnica Nacional - EPN	✓	✓
Universidad Católica Santiago de Guayaquil - UCSG	✓	✓
Universidad Politécnica Estatal del Carchi – UPEC	✓	
Universidad de las Fuerzas Armadas – ESPE	✓	✓
Universidad Estatal de Bolívar – UEB	✓	✓
Universidad Politécnica Salesiana – UPS	✓	✓
Escuela Superior Politécnica del Chimborazo – ESPOCH	✓	✓
Universidad Internacional del Ecuador – UIDE	✓	✓
Universidad San Francisco de Quito – USFQ	✓	✓
Escuela Superior Politécnica del Litoral – ESPOL	✓	✓
Universidad Nacional del Chimborazo – UNACH	✓	✓
Universidad Técnica Particular de Loja – UTPL	✓	✓
Instituto de Altos Estudios Nacionales – IAEN	✓	✓
Universidad Estatal de Milagro – UNEMI	✓	✓
Universidad Central del Ecuador	✓	
Instituto Oceanográfico de la Armada – INOCAR	✓	✓
Universidad Regional Autónoma de los Andes – UNIANDES	✓	✓
Universidad de las Américas	✓	
Pontificia Universidad Católica del Ecuador Sede Quito – PUCE	✓	✓
Universidad Técnica Equinoccial – UTE	✓	✓
Universidad Católica de Cuenca	✓	
Pontificia Universidad Católica del Ecuador Santo Domingo – PECESD	✓	✓
Universidad Tecnológica Indoamérica – UIT	✓	✓
Universidad del Azuay	✓	
Pontificia Universidad Católica del Ecuador Ibarra – PUCESI	✓	✓
Universidad Técnica del Norte – UTN	✓	✓
Universidad Nacional de Loja – UNL	✓	✓
Pontificia Universidad Católica del Ecuador Ambato	✓	
Universidad Estatal Amazónica	✓	
Universidad Técnica de Machala	✓	

Universidad Técnica de Ambato – UTA	✓	✓
Universidad de Cuenca – UC	✓	✓
Instituto Tecnológico Superior "José Chiriboga Grijalva"	✓	
Instituto Superior Tecnológico Bolivariano de Tecnología SENESCYT	✓	

Fuente: Recuperado de http://www.redclara.net/index.php/somos/miembros/asociados-plenos/ecuador, http://www.cedia.org.ec

2.1.5 NUBE (CEDIA)

La nube privada de CEDIA brinda servicios de computo en servidores virtuales, de esta manera facilita el trabajo a investigadores de las instituciones miembros del consorcio, además posibilita la instalación y servicios informáticos de diferente naturaleza.

El funcionamiento se basa en un servicio llamado IaaS (Infraestructura como un Servicio); La red avanzada de CEDIA brinda gran conectividad y velocidad de acceso a las aplicaciones y servicios que se encuentren en esta infraestructura e interactuando con la misma; la disponibilidad está respaldada con un mecanismo de protección de diferentes tipos de redundancia como energía eléctrica, almacenamiento, backups, y sitios de contingencia.

Es destacable la cantidad de servicios y aplicaciones con las que se dispone y con las cuales investigadores, profesores y estudiantes de las instituciones asociadas pueden acceder y con esto aumentar en colaboración y comunicación. Cuenta con correo electrónico, Web, intranet corporativa, repositorios Web, documentales, gestión de proyectos, compartición de archivos, entre otros.

2.1.5.1 Repositorio Multimedia

Mediante el portal Web de CEDIA se puede publicar contenidos audiovisuales tales como conferencias, cursos y capacitaciones, la principal ventaja de este portal es que permite vinculación entre las instituciones miembros, permitiendo la sociabilización entre los investigadores y académicos miembros de la red CEDIA, siendo una ayuda para un mejor manejo de información aprovechada por quienes se interesen.

2.1.5.2 Compartición de Archivos

La compartición de archivos es de gran utilidad para los miembros que deseen compartir la información ya que por medio de cualquier correo no brinda una capacidad de envió mayor a treinta megas, para los miembros de CEDIA presenta la herramienta "filesender" en la cual permite hasta 100 GB y para poder tener acceso a esta información la podrá hacer mediante su correo electrónico (correo institucional).

2.1.6 Universidad Técnica Del Norte En Ipv6

La Universidad técnica del Norte tiene disponible el recurso de direcciones IPv6 pero aún no se está utilizando, porque no se cuenta con el mecanismo de traducción de IPv4 a IPv6 que garantice la coexistencia entre usuarios de ambos protocolos IP, siendo una desventaja ya que no se aprovecha todas las prestaciones y aplicaciones que ofrece la red avanzada de CEDIA, entre las que se encuentran publicaciones científicas, bibliotecas digitales, vinculación con investigadores que trabajen en diferentes temas afines de diferentes partes del mundo, y otros servicios; razón por la cual se determina la necesidad de contar con el medio necesario para lograr la transición en dichos protocolos.

2.1.6.1 Aplicaciones con direccionamiento IPv6

En la UTN no existe servicios y aplicaciones usando el protocolo Ipv6, el presente proyecto pretende levantar un servidor Web con el portal universitario y el servidor FTP mediante el uso de carpetas de usuario con direccionamiento IPv6; el mecanismo DS-lite permitirá interactuar con la red avanzada de CEDIA.

2.2 PROTOCOLO DE INTERNET VERSIÓN 4 (IPV4)

El protocolo de internet en un principio fue diseñado para la interconexión en sistemas de redes de comunicación entre ordenadores a través de un intercambio de paquetes, proporcionando los medios necesarios para transmitir bloques de datos (datagramas) entre un punto de origen y uno de destino, es decir entre host identificados con direcciones de longitud fija. El protocolo también realiza la fragmentación y el ensamblaje de datagramas de gran tamaño si es necesario para su transmisión. (Boulevard, 1981)

El protocolo de internet versión cuatro se utilizan por protocolos host a host en internet, utilizando protocolos de redes locales para así llevar los datagramas a la puerta de enlace (gateway) y llegar al host destino. El protocolo de internet versión cuatro (IPv4) está definido en el RFC 791.

2.2.1 Estructura del protocolo

El protocolo de internet presenta dos funciones básicas de operación, direccionamiento y fragmentación; Se usan 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)

Los módulos de internet no solo utilizan la cabecera internet para el encaminamiento sino también para realizar fragmentar y re ensamblar los datagramas de ser necesario cuando la transmisión es de trama pequeña.

La operación en el protocolo de internet versión cuatro depende de cada uno de los hosts involucrados en la comunicación internet y cada Gateway que interconecta las redes, ya que existen reglas comunes para la interpretación de campos de direccionamiento, fragmentación y ensamblaje de datagramas, ya que estos son tomados como una identidad independiente que no se relaciona con ningún otro. (Marcelo, 2013)

Los mecanismos que utiliza el protocolo de internet para brindar su servicio son cuatro:

- ✓ Tiempo de servicio, el cual se utiliza para indicar la calidad de servicio y el tipo de servicio.
- ✓ Tiempo de vida, indica el máximo periodo de vida de un datagrama internet, se reduce a lo largo de la ruta donde es procesado, si este tiempo llega a cero antes de llegar a su destino el datagrama es eliminado.
- ✓ Opciones, son las funciones de control necesarias para realizar comunicaciones comunes entre la cuales incluyen marcas de tiempo, seguridad y encaminamiento especial.
- ✓ Suma de control de cabeceras, se utiliza para la verificación de que el datagrama de internet fue transmitido correctamente, si falla la suma de control el datagrama es descartado porque se detecta como error.

La relación con otros protocolos se puede presentar en una representación jerárquica de protocolos. (Figura 4)

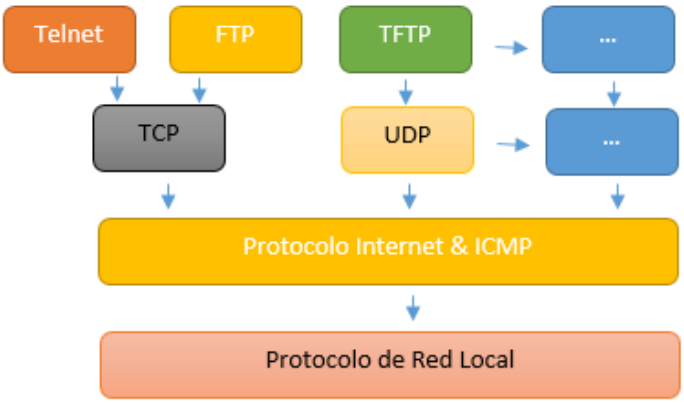


Figura 4 Relación entre Protocolos

Fuente: Recuperado de https://tools.ietf.org/html/rfc791

IPv4 es un protocolo no orientado a conexión, es decir no confiable a nivel de red, no corrige errores si los datos se envían en desorden y no da garantía sobre el tráfico, además utiliza el método del mejor esfuerzo para asegurarse que los datos lleguen a su destino.

La cabecera que se utiliza en IPv4 tiene una longitud variable, la cual se compone por una parte obligatoria de 20 bytes y una serie de opciones con longitud de múltiplo de 4 bytes. (Figura 5)

Figura 5. Cabecera de un datagrama Internet

Fuente: Recuperado de https://tools.ietf.org/html/rfc791

- Versión (4 bits): Número de versión del protocolo IP. Para el protocolo versión 4 se utiliza la constante “4”. Permite la interacción en redes similares.
- Cabecera (4 bits): Es la longitud de la cabecera IPv4. El valor oscila de 0 a 15, en bloques de 32 bits.
- Tipo de servicio (TOS) (8 bits): indica cómo se relacionan los paquetes en cuestión, priorizando unos sobre otros.
- Longitud Total (16 bits): La longitud máxima de un paquete IPv4 no debe ser mayor a 64 KB.
- Identificador: Campos usados para la fragmentación de paquetes IPv4.
- Desplazamiento de fragmentación: mecanismo para la fragmentación de paquetes.
- Tiempo de vida (TTL) (8 bits): Determina el tiempo que un paquete puede circular en la red y los saltos que puede realizar. El paquete es descartado su este campo llega a 0.
- Protocolo (8 bits): Indica el protocolo de capa superior.
- Suma de control de cabecera (8 bits): Es un control (checksum) para proteger la cabecera. Se utiliza para evitar la propagación de paquetes innecesariamente y no se protege a los datos.
- Dirección de Origen (32 bits): Indican la dirección del host origen
- Dirección destino (32 bits) Indica la dirección del host al cual va dirigido el paquete.

La anatomía de una dirección de red en IPv4 está formada por la parte de red y la parte de host, la cual se indica más calara mente por la máscara de red que está compuesta por una serie en 1 seguida por una serie en 0 con un tamaño de 32 bits; los unos indican la parte de red usada y los ceros muestran la parte de host.

La división se efectúa para evitar el costo de enrutar individualmente cada uno de los hosts para luego así poder hacer el ruteo a distintas redes. La máscara de red también indica los valores de la dirección de red y la dirección de broadcast que son el inicio y el fin de un segmento de red respectivamente. Además, la dirección de broadcast sirve para enviar un mensaje a todos los nodos de la red (Tabla 2). (Boulevard, 1981)

Tabla 2. Direcciones de red con mascara de red, dirección de red y broadcast

DIRECCIÓN IP	MASCARA DE RED	MASCARA RESUMIDA	DIRECCIÓN DE RED	DIRECCIÓN DE BROADCAST
192.16.63.1	255.255.255.252	/30	192.16.63.0	192.16.63.3
10.0.0.64	255.0.0.0	/8	10.0.0.0	10.255.255.255
64.16.10.1	255.255.240.0	/20	64.16.0.0	64.16.15.255
201.16.96.47	255.255.255.192	/26	201.16.96.0	201.16.96.63
42.16.172.1	255.255.255.0	/24	42.26.172.0	42.16.172.255
172.16.174.129	255.255.0.0	/16	172.16.0.0	172.16.255.255

Fuente: Recuperado de https://tools.ietf.org/html/rfc791

2.2.2 Limitaciones

Con el paso de los años IPv4 ha tenido diferentes actualizaciones para nuevos retos, pero los problemas que presenta son importantes y el protocolo de internet no los ha superado.

Uno de los problemas que presenta es la expansión de la tabla de enrutamiento de internet, ya que cada vez aumenta la cantidad de servidores conectados a internet también aumenta la cantidad de rutas y así el uso de más recursos de memoria y procesamiento al momento de elegir el mejor camino, haciendo que sea más lento en los tiempos de respuesta.

Otras de las dificultades que presenta IPv4 es que no se preparó para adoptar nuevas aplicaciones de red siendo la transmisión de video y audio en tiempo real, aun menos mecanismos de seguridad avanzada en la transmisión de datos.

El sorprendente número de direcciones IP requeridas en la actualidad superan la disponibilidad de direcciones que IPv4 dispone. A este problema se le ha dominado agotamiento de direcciones IP. (LACNIC, fases de agotamiento ipv4, 2015)

El agotamiento de direcciones IPv4, quiere decir que LACNIC, no tiene suficientes direcciones IPv4 para cubrir las necesidades de todos sus miembros. Por lo cual se entró a una etapa de reserva con miras a solventar los problemas presentados por la escasez de direcciones de internet del protocolo versión 4. (Castillo, 2014)

Para que el recurso en IPv4 sea gradual y no inmediato se sigue cuatro etapas (fase 0, fase 1, fase 2, fase 3), en las cuales primero se hizo una reserva de direcciones con prefijo /11. El 20 de junio de 2014 (figura 6) se pasó a la segunda fase en donde ya se alcanzó los dos últimos bloques de la reserva del pool de direcciones IPv4 de LACNIC y según el comportamiento desde esta fecha se ha hecho una proyección con la posible fecha de agotamiento. (LACNIC, fases de agotamiento ipv4, 2015)

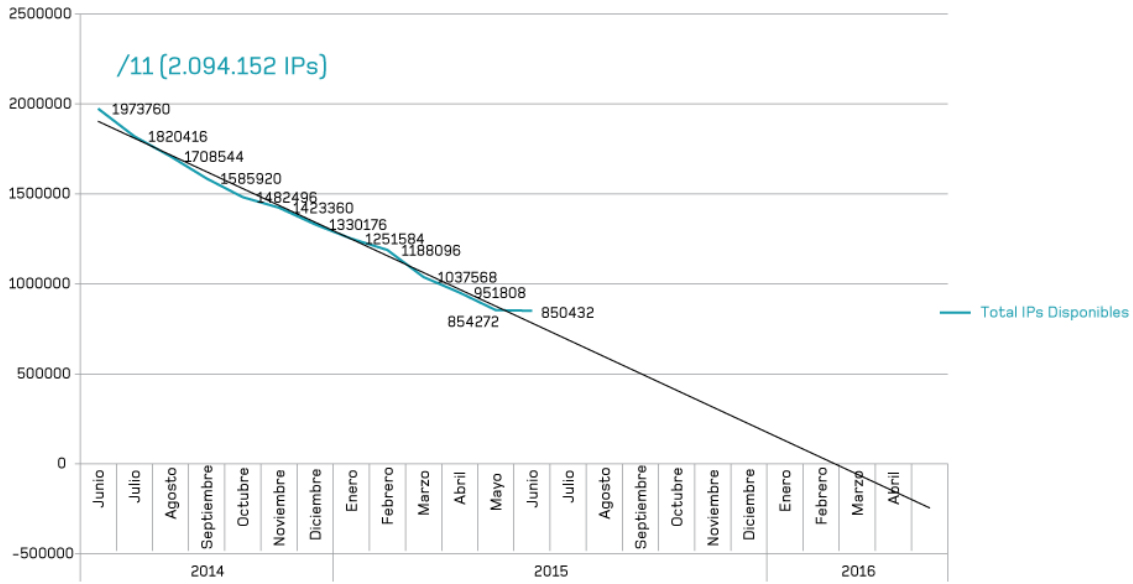


Figura 6. Proyección de agotamiento lineal -Fase 2

Fuente. Recuperado de http://www.lacnic.net/web/lacnic/agotamiento-ipv4

La etapa o fase 3 se alcanzará cuando el último bloque /11 se agote, el cual es la reserva final de la que dispone LACNIC. Y de este espacio solo serán asignados entre /22 y /24 con lo cual cada miembro solo podrá recibir una asignación inicial de este espacio. (LACNIC, fases de agotamiento ipv4, 2015)

2.3 PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6)

Actualmente las direcciones que utilizan el protocolo de internet versión 4 se ha reducido drásticamente y su finalización se acerca rápidamente, lo que significa que el sistema de direcciones mundialmente se está agotando.

La gran demanda de dispositivos que requieren sus propias direcciones IP para conectarse a internet y en algunos casos más de una dirección, ha desvanecido la idea de que por medio de tecnologías tipo NAT (Network Address Translation) resuelvan este tipo de inconveniente, y se ha determinado la necesidad de adoptar una nueva versión del protocolo de internet. (LACNIC, fases de agotamiento ipv4, 2015)

El protocolo de internet versión 6 (IPv6) con una longitud de 128 bits, tiene una disponibilidad de 340 sixtillones de direcciones aproximadamente, además este protocolo maneja términos de mayor estabilidad, flexibilidad y simplicidad en la administración de la red, conectividad extremo a extremo ya que no hay la necesidad de direcciones compartidas debido a la gran cantidad de direcciones que ofrece el protocolo IPv6 teniendo en cuenta que las direcciones se asigna por interfaz y no por nodo, un nodo puede tener más de una interfaz por lo tanto más de una dirección de internet.

El protocolo de internet versión seis está diseñado para que sea escalado conforme a las necesidades de aplicación o servicios vayan solicitando, aunque conserva la mayor parte de las características y conceptos de operación de IPv4, entre las características básicas de IPv6 se encuentra:

Formato de encabezado: El formato de encabezado de IPv6 está diseñado con la finalidad de reducir la sobrecarga en el mismo, permitiendo un procesamiento más eficaz en los enrutadores intermedio, cabe recalcar que un encabezado IPv4 no es interoperable con un encabezado IPv6 y se necesita un mecanismo que soporte ambos protocolos para poder reconocer y procesar los encabezados de ambos protocolos.

Espacio de direcciones: El protocolo IPv6 dispone de un amplio espacio de direcciones con el propósito de permitir múltiples niveles de división para subredes y en la asignación de direcciones a organizaciones que disponen de una red troncal de Internet.

Infraestructura, enrutamiento: Las direcciones IPv6 que se utilizan en Internet utilizan una infraestructura eficaz y a la vez jerárquica, las cuales se pueden resumir y usar en diferentes niveles de servicios de internet, con lo que las tablas de enrutamiento en los equipos de la red troncal sean más pequeñas.

Configuración de direcciones: IPv6 puede simplificar la configuración en los hosts, permite el uso de un servidor DHCP para las direcciones con estado, y también admite las direcciones sin estado que son las que no utilizan un servidor DHCP.

Seguridad Integrada: uno de los requisitos en los protocolos de IPv6 es la compatibilidad con IPSec, esto se basa en una solución estandarizada para las necesidades de seguridad de red.

Protocolo de interacción con nodos vecinos: Consiste en el envío de paquetes ICMPv6 para encontrar nodos que se encuentren en el mismo vínculo, este protocolo remplaza a ARP de IPv4. (Palet, 2011)

2.3.1 Estructura del protocolo

Principalmente un paquete IPv6 esté compuesto por dos partes: cabecera y datos, un paquete IPv6 es la unidad de datos del protocolo y tiene la siguiente estructura. (Figura 7)

Figura 7. Estructura paquete IPv6

Fuente: Recuperado de http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

La cabecera de IPv6 es más simple que la cabecera de IPv4 y 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. (Figura 8)

Figura 8. Cabecera IPv6

Fuente: Recuperado de http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

- Versión (4 bits): Número de versión del protocolo IP. Para el protocolo versión 6 se utiliza la constante “6”.
- Clase de Tráfico (8 bits): En este campo se puede especificar un identificador para diferenciar el tráfico.
- Etiqueta de Flujo (20 bits): La información que contiene este campo se usa por los enrutadores para asociar una determinada prioridad a los datagramas según sea su aplicación en las cuales se necesite de ciertos requerimientos como es el caso del establecimiento de una videoconferencia.
- Longitud de carga útil (16 bits): Es en si la longitud de los datos (información) la cual puede ser máximo de 65.536 bytes o 2^16 posibilidades, aproximadamente son 64000 octetos.

- Siguiente Cabecera (8 bits): No emplea cabeceras de longitudes variables sino sucesivas cabeceras encadenadas y analizadas por los enrutadores, en algunos casos solo se procesa extremo a extremo y no por los encaminadores.
- Límite de saltos (8 bits): En este campo se determina la cantidad de saltos que un paquete puede tener, a nivel de capa de red, lo cual es importante para evitar ciclos infinitos en caso de presentarse problemas de enrutamiento.
- Dirección Fuente (128 bits): Es la dirección de donde se origina un paquete.
- Dirección destino (128 bits): Puede ser la dirección destino hacia donde se dirige el paquete, pero no necesariamente ya que también puede ser una dirección intermedia que va de acuerdo a los encabezados extendidos usando.

Las cabeceras extendidas están definidas en campo de "siguiente cabecera", este mecanismo usa el concepto de encadenar las cabeceras al siguiente y al anterior si ya existe (Figura 9). (Cabellos, 2004)

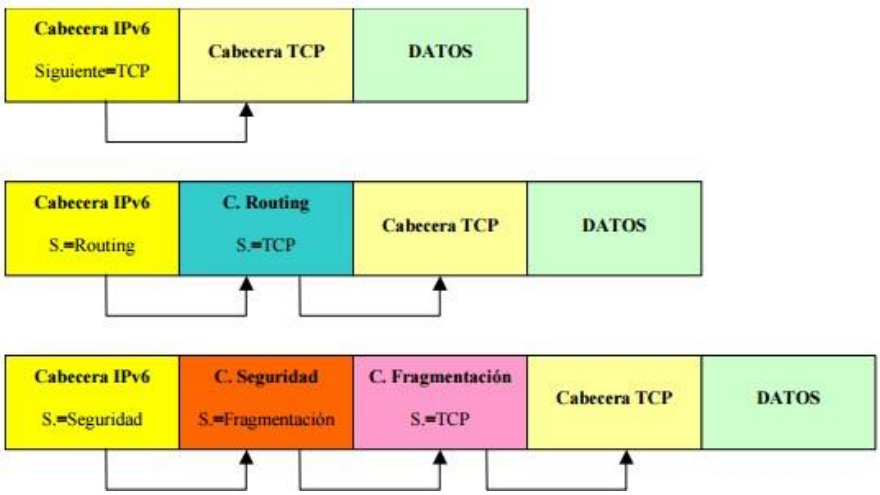


Figura 9. Extensión de cabeceras

Fuente: Recuperado de http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

2.3.2 Direccionamiento IPv6

Las direcciones IPv6 tienen una longitud de 128 bits, existen tres tipos de direcciones:

- ✓ Unicast: dirección para identificar una única interfaz, los paquetes enviados se entregan solo por la dirección adquirida.
- ✓ Anycast: Es un identificador para un conjunto de interfaces, los paquetes enviados se entregan a una de las direcciones asociadas, de acuerdo al protocolo de media distancia se entrega a la más cercana.
- ✓ Multicast: Es un identificador para un conjunto de interfaces, los paquetes enviados se entregan a todas las interfaces asociadas a la dirección.

Para cada tipo se subdivide en direcciones para resolver casos específicos de direccionamiento (Tabla 3). (ACOSTA, y otros, 2014)

Tabla 3. Subdivicio de tipo de direcciones IPv6

Tipo de dirección	Subtipos de direcciones
Unicast	Enlace local (Link-Local) Sitio Local (site-Local) Agragable Global (Aggregatable Global) Loopback Sin Especificar (Unspecified) Compatible con IPv4
Anycast	Agragable Global (Aggregatable Global) Sitio Local (Site-Local) Enlace Local (Link-Local)
Multicast	Asignada (Assigned) Nodo Solitario (Solicited Node)

Fuente: Recuperado de http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Las direcciones en IPv6 se pueden presentar en tres diferentes formas.

La primera es la manera que en general se encuentra, es en ocho partes de 16 bits de la dirección con valores hexadecimales en cada campo: x: x: x: x: x: x: x: x (en cada x se remplaza por un número hexadecimal), por ejemplo:

- ✓ EFCD: AB87:8765:4320: EFCD: AB87:8765:4320
- ✓ 1090:0:0:0:9:900:300C:528B

El segundo caso se tiene en cuenta que para las cadenas largas de cero bits se dispone una sintaxis con el fin de hacer más fácil la escritura de cero bits, consiste en el uso de "::" que indica uno o varios grupos de ceros de 16 bits y solo puede aparecer una vez en la dirección. (Tabla 4)

Tabla 4. Sintaxis de direcciones IPv6

Dirección	**Forma comprimida**	**Tipo**
1080:0:0:0:8:800:200C:417ª	1080::8:800:200C:417A	Unicast
FF01:0:0: 0:0:0: 0:101	FF01::101	Multicast
0:0:0:0:0:0:0:1	::1	Loopback
0:0:0:0:0:0:0:0	::	Dirección no especificada

Fuente: Recuperado de https://tools.ietf.org/html/rfc3513

Una tercera opción se trata cuando existe un entorno donde se encuentran nodos IPv4 e IPv6, la presentación de este tipo alternativo donde las seis primeras partes de alto orden de la dirección son en valores hexadecimales y las dos últimas partes con los 4 valores de bajo orden, es decir, con la dirección en IPv4 (Tabla 5). (R. Hiden, S. Deering, 2003)

Tabla 5. Forma alternativa en entornos mixtos de nodos IPv4 e IPv6

Dirección	Forma comprimida
0:0:0:0:0:0:192.168.1.10	::192.168.1.10
0:0:0:0:0:FECD: 172.16.18.24	::FECD:172.16.18.24

Fuente:Recuperado de https://tools.ietf.org/html/rfc3513

2.3.2.1 Plan de direccionamiento

La asignación de direcciones IPv6 está formado en un sistema de árbol invertido, es decir de arriba abajo, y el organismo principal ubicado en la parte más alta es IANA (Internet Assigned Numbers Authority) que dispone del pool Global de direcciones y se encarga de asignar a los Registros Regionales (RISRs) los cuales en sus políticas delegan los recursos a sus clientes como ISPs y estos a sus usuarios finales. (Figura 10)

Es importante tener en cuenta de no asignar bloques de direcciones consecutivos ya que se dispone de un gran espacio de dirección mediante IPv6 y se puede realizar implementaciones adicionales de manera segura.

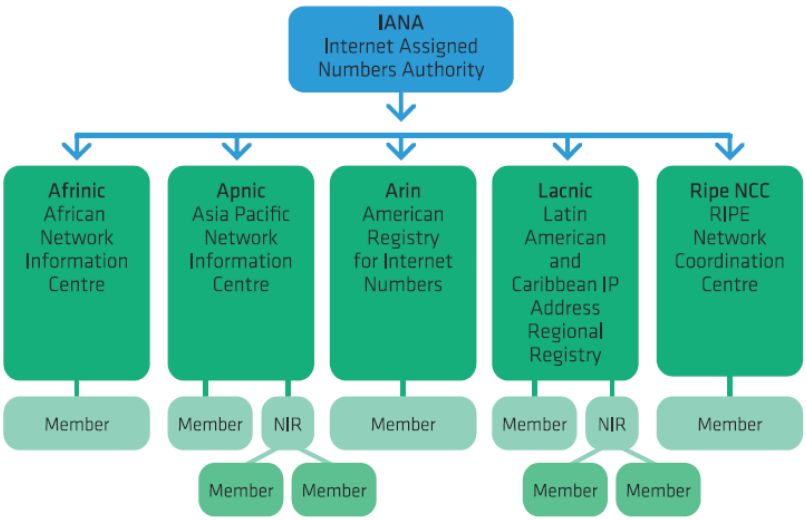


Figura 10. Modelo IANA – RIR

Fuente: IPv6 para Operadores de red

En un proceso de transición de IPv4 a IPv6 es necesario un plan direccionamiento en los que se debe de tener en cuenta la obtención del prefijo de sitio y la creación de numeración de IPv6, teniendo en cuenta que en este proceso la topología de IPv4 ya configurada es la base del esquema de red para el nuevo protocolo a implementarse. (ACOSTA, y otros, 2014)

Para la obtención del prefijo del sitio es importante consultar el soporte del protocolo por parte del proveedor de servicio de internet, ya que antes de configurar IPv6 es la red debe estar disponible dicho prefijo. Pasar de un esquema de numeración que existe para las subredes IPv4 a subredes IPv6 equivalentes teniendo en cuenta los identificadores de red y subredes, por ejemplo: (Tabla 6)

Tabla 6. Subred IPv4 a IPv6 equivalente

Prefijo de subred Ipv4	**Prefijo de subred Ipv6 equivalente**
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Fuente: Recuperado de http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-9/index.html

Para la asignación de host se puede utilizar la configuración sin estado automática de IPv6 la cual consiste en recibir el prefijo del sitio desde el enrutador más próximo, generando de forma automática direcciones IPv6 para cada interfaz de host. Las direcciones IPv6 para los servidores deben ser estables (estáticas) ya que si hay un cambio de NIC se asignara otra dirección automáticamente.

En la creación de direcciones para cada servidor se debe de tener en cuenta la asignación de identificadores de interfaz que deben ser descriptivos y estables, entre los métodos a utilizar es un sistema de numeración consecutiva a los ID de interfaz, otra forma de dar las direcciones en el caso de que la numeración ya creada de los ID de IPv4

en los enrutadores y servidores, con lo que las direcciones en IPv4 se pueden transformar en hexadecimal y el resultado aplicarlo como ID de interfaz. (Oracle, 2010)

2.3.2.2 Nomenclatura de las direcciones

Las direcciones unicast se pueden distinguir entre link local, Site local y globales de la siguiente manera:

Link local: empiezan por "FE80:" y sirven para el ID de interfaces de un mismo enlace.

Site Local: Estas direcciones empiezan por "FEC0:" sirven para identificar interfaces en la misma área de red, es decir, del mismo sitio como puede ser el campus universitario.

Global: Las direcciones de este ámbito empiezan por "2001:" o "3FFE:" y se utilizan para identificar interfaces en Internet. (Verdejo, 2000)

2.3.2.3 Enrutamiento

El uso de los protocolos de enrutamiento es para que en los router se mantenga las tablas de encaminamiento y para definir el mejor camino de un extremo a otro.

Enrutamiento Estático:

Este tipo de enrutamiento se realiza de forma manual, y no cambia su comportamiento en la red a menos que se cambien de la misma manera los parámetros,

aunque para redes grandes no es muy recomendable ya que es difícil mantener las tablas de enrutamiento si sucede algún cambio en la red, se recomienda y es eficiente en redes pequeñas. (Cabellos, 2004)

Enrutamiento Dinámico

Los protocolos de enrutamiento a través de rutas dinámicas se realizan por medio de mensajes de actualización, dicha información se procesa en las tablas de enrutamiento. En este tipo de enrutamiento los protocolos puedes ser IGP y EGP.

- IGP: es el protocolo de pasarla interna y se usa dentro de un sistema autónomo.
- EGP: protocolo de pasarla externa, se utiliza para realizar el intercambio en la información de enrutamiento, brindando información de acceso a redes internas a través de los gateways.

Enrutamiento interno (IGP)

Los protocolos de enrutamiento utilizados para IPv4 se modificaron para poder soportar IPv6, a pesar de los cambios varias de las características son las mismas de los dos protocolos de internet. Los protocolos que soportan IPv6 son:

- ✓ RIP Next Generation (RIPng)
- ✓ EIGRP para IPv6
- ✓ OSPF versión 3
- ✓ IS-IS para IPv6

RIP Next Generation (RIPng)

RIPng es un protocolo que utiliza el algoritmo de vector distancia y fue diseñado para trabajar como IGP en entornos de red moderados internos de un sistema autónomo (AS), el límite de saltos de este protocolo es de 15 saltos con un coste de 1 para cada red y utiliza métricas fijas para realizar la comparación de rutas alternativas el cual es un problema cuando las rutas necesitan ser elegidas en tiempo real, retraso controlado y fiabilidad. La métrica en RIPng de una red es un número entre 1 y 15, además cada red tendrá un prefijo de su dirección IPv6 en el destino asociado a la métrica los cuales son establecidos por el administrador del sistema de forma específica. (Malkin, 1997)

En cada una de las tablas de enrutamiento que se establece cuando un router implementa RIPng contiene información sobre la entrada para cada destino al que se puede llegar. Además, contiene el prefijo IPv6 de destino, una métrica, la dirección de router al siguiente salto, una bandera para indicar los cambios de ruta y temporizadores. Para que la información de enrutamiento se pueda proporcionar todos los routers deben utilizar el protocolo RIPng o si existen diferentes protocolos IGP al menos un router en la red debe estar programado para brindar la información entre los diferentes protocolos implementados. (Malkin, 1997)

Formato del Mensaje RIPng

Es un protocolo basado en UDP y envía y recibe datagramas a través del puerto 521 por el que se envía toda la información de enrutamiento de RIPng (Figura 11). Los mensajes de actualización se envían automáticamente y contienen el puerto de origen, destino y el puerto RIPng.

Figura 11. Mensajes Request y Response RIPng

Fuente: Recuperado de https://tools.ietf.org/html/rfc2080

La entrada definida para la tabla de enrutamiento tiene el siguiente formato: (Figura 12)

Figura 12. Formato RTE

Fuente: Recuperado de https://tools.ietf.org/html/rfc2080

El prefijo de destino, número significativos en el prefijo y el costo para llegar a un destino (métrica) se encuentra en la lista de cada RTE.

El **prefijo de destino** es de 128 bits y se ha definido en 16 octetos en el orden de bytes de la red.

La **identificación de ruta** sirve para proporcionar un método que separe las rutas internas RIPng de las rutas externas RIPng que pueden haber sido importadas de un EGP u otra red IGP.

El campo **Tamaño del prefijo** es la longitud en bits del prefijo IPv6 y su valor se encuentra entre 0 y 128.

En campo **Métrica** se marca con el valor de un destino al que se puede llegar, se encuentra entre 0 y 15 y para un destino que no se puede alcanzar se marca con infinito asignando el número 16.

Siguiente Salto: RIPng permite especificar la siguiente dirección hop IPv6 destino a la que los paquetes se pueden enviarse, especificando en la tabla de enrutamiento de cada router. El siguiente salto RTE (Figura 13) está dado por un valor de 0xFF en el campo de la métrica y en campo del prefijo se especifica la dirección IPv6 del siguiente salto. Los valores de identificación de ruta y tamaño del prefijo deberán ser cero en el siguiente salto. (Malkin, 1997)

Figura 13. RTE del siguiente salto

Fuente: Recuperado de https://tools.ietf.org/html/rfc2080

Temporizadores

Los temporizadores tiene la finalidad de enviar los mensajes de actualización de las tablas de enrutamiento completas a cada router vecino en un periodo de 30 segundos, en una red que usa como protocolo de enrutamiento RIPng estos tiempos tienden a sincronizarse para que todos los routers envíen la información al mismo tiempo, pero esto recae en un problema que puede generar colisiones innecesarias para evitar dicho problema el temporizador de 30 segundos se compensa con un tiempo aleatorio cada vez que se establece, este tiempo se da por la multiplicación de 0,5 por el periodo de actualización (30 segundos).

Los temporizadores que se asocian a cada ruta son dos, timeout (tiempo de espera) y garbage-colletion time (tiempo de recolección de basura). De esta manera se determina

que una vez se termina el tiempo de espera la ruta se tacha como no valida, mas sin embargo no se elimina de la tabla de enrutamiento esperando si algún router vecino verifique la ruta, cuando el tiempo de recolección de basura se acaba se elimina la ruta definitivamente.

La eliminación de las rutas puede ocurrir ya sea porque el tiempo de espera expira o porque la métrica se marca como infinito (16), para que la eliminación sea definitiva tiene que suceder los siguientes procesos:

- Expira tiempo de espera 180 segundos
- Métrica se marca como infinita (16)
- La bandera cambia indicando que la entrada ha cambiado
- El proceso de salida para generar una respuesta
- Expira tiempo de recolección de basura 120 segundos.

Seguridad

No especifica ningún mecanismo de seguridad y se basa en la autenticación de IP de cabecera además de la seguridad encapsulada en la dirección de carga útil. (Guillermo Cicileo, 2009)

EIGRP para IPv6

El protocolo de enrutamiento EIGRP es de propiedad de Cisco Systems, se trabaja con la misma base que con IPv4 solo que se agregó otro protocolo de capa 3 para poder utilizar IPv6 sin necesidad de hacer cambios significativos para poder tener soporte en dicho protocolo. Entre las características de EIGRP para IPv6 se pueden mencionar:

- Establecimiento de adyacencias

- Tablas de topología y de vecinos
- Ancho de banda definido en 1544 Kbps
- Distancia administrativa interna 90 y 170 externa
- Uso de algoritmo DUAL
- Actualizaciones parciales generadas por eventos.

Mensajes EIGRP: los mensajes de EIGRP se componen del siguiente contenido:

- Saludo – Hello: Sirve para detectar vecinos y formar adyacencias.
- Paquete de actualización: Difunden la información de enrutamiento.
- Paquete de reconocimiento: Identifica la recepción paquetes de actualización, consulta y respuesta.
- Paquete de consulta: Utilizados por DUAL para buscar redes y otras tareas.
- Paquete de respuesta: respuestas automáticas para el paquete consulta.

Este protocolo solo manda actualizaciones cuando existe un cambio de ruta, además las actualizaciones parciales solo se envía la información de la ruta y no toda la tabla de enrutamiento; cuando ocurre un cambio de ruta solo se notifica a los dispositivos afectados generando menor consumo de ancho de banda. (CISCO)

Open Shortest Path First Version 3 (OSPFv3)

El protocolo de enrutamiento OSPFv3 conserva la mayoría de los algoritmos usados en OSPFv2, realizando los cambios necesarios para tener soporte con el protocolo de internet versión 6. Este protocolo usa el término “link” indicado la facilidad de comunicación o el medio donde los nodos se comunican a la capa enlace; varias subredes IPv6 se pueden asignar a un solo enlace, a su vez dos nodos pueden interactuar doble un único enlace así no compartan la misma subred IPv6.

Las direcciones IPv6 no se encuentran en los paquetes OSPF, pero si en LSA de los paquetes de actualización, la inundación por LSAs esta explícitamente codificado en el campo de LS y son tres diferentes ámbitos para la inundación de LSA. (Flores, 2014)

- **Alcance de enlace local.** LSA solo se inundan solamente en un vínculo local
- **Alcance de la Zona.** La inundación de LSA solamente se realiza a través de una sola área de OSPF.
- **Alcance de Sistema Autónomo (AS).** La inundación de LSA ocurre en todo el dominio de enrutamiento, considerando el router de frontera y estableciendo su E-bit Router-LSAs en las áreas regulares.

En OSPFv3 se eliminó los campos “AuType” y “Autenticación” de la cabecera del paquete OSPF, los campos relacionados con los mismos se han retirado del área OSPF y de las estructuras de datos de la interfaz. La ejecución de OSPF se basa en la cabecera de autenticación y de la seguridad de encapsulamiento en la carga útil. Solo se envía las actualizaciones cuando se produce un cambio en la topología de red y se crea un anuncio de estado de enlace (LSA) y se envía a todos los dispositivos vecinos mediante una dirección multicast, esta información se actualiza en la base de datos de estado de enlace (LSDB). Se utiliza el puerto 89 UDP para su comunicación. (Sánches, 2006)

OSPF es un protocolo de preferencia en el uso de redes IGP, ya que no tiene desventajas considerables con respecto a otros protocolos para implementaciones a gran escala, teniendo en cuenta que las redes pequeñas son aproximadamente hasta 99 routers y medianas hasta 300 routers, para las cuales OSPF se razona adecuado. OSPF delimita la cantidad de routers y enlaces que pueden existir en una red debido a que requiere procesamiento y ancho de banda, para que esto no sea un problema el protocolo permite dividir la red en áreas, pero si la red es pequeña puede definirse en una sola área sin restricciones en la topología.

Si OSPFv2 y OSPFv3 estan configurados en un mismo router cada protocolo trabaja independientemente el uno del otro, de mismo modo el algoritmo shortest path first (SPF) se ejecuta independiente. OSPFv3 tiene sus propias características ya que está diseñado para trabajar con IPv6:

- ✓ Direcciones IPv6 de 128 bits
- ✓ Direcciones de origen Link-local
- ✓ Diferentes direcciones por interfaz e instancias OSPF
- ✓ Soporte de IPsec (seguridad)
- ✓ Funciona sobre un enlace y no una subred

En OSPF para IPv6 para cada interfaz se asigna un identificador único con el router, además de un ID de instancia que por defecto es cero (0) y que para que existan múltiples comunidades separadas en el router solo se debe cambiar esta instancia. La métrica marcada para cada interfaz en el router es una sola y representa el costo de envió de paquetes a dicha interfaz.

Estructura de datos Vecinos (Neighbor): la función en IPv6 es la misma que en IPv4, hace la recolección de información necesaria para formar adyacencias. La estructura de Neighbor está formada por:

- ✓ ID de interfaz vecino- anuncio mediante el paquete saldo para solicitar el registro
- ✓ Dirección IP de vecino- dirección de origen en OSPF de paquetes IPv6
- ✓ Router designado de vecino- elección de router vecino y codificación de ID de router.
- ✓ BDR del vecino- a diferencia de IPv4 la dirección de BDR se encuentra codificada como ID del router y no como una dirección IP.

Paquetes de OSPFv3

- ✓ **Hello:** Identificacion del tipo de paquete es 1, se envían peridocamente para establecer y mantener enlaces vecinos.
- ✓ **Data Base Description DBD:** identificación del tipo de paquete es 2, es donde está la base de datos de la topología y se utiliza cuando las adyacencias se encuentran establecidas.
- ✓ **Link State Request LSR:** identificación del tipo de paquete es 3, los paquetes LSR son intercambiados para mantener actualizada la información de las rutas.
- ✓ **Linl State Update LUS:** el tipo de estos paquetes es 4, cada LSU lleva a un grupo de paquetes LSR a un salto más allá de su origen.

OSPFv3 para el transporte utiliza IPv6 y la dirección Link-local como dirección de origen, la cabecera de OSPFv3 tiene un tamaño de 16 bytes. (Figura 14)

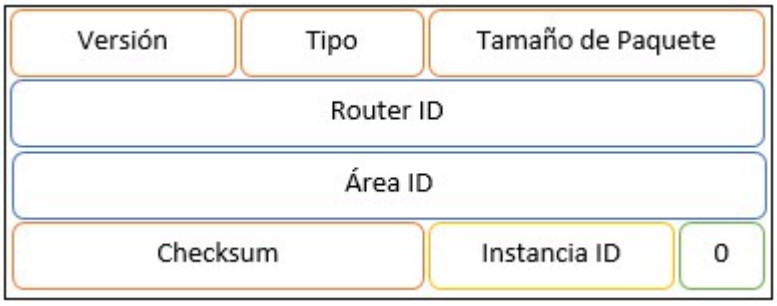


Figura 14. Cabecera de OSPFv3

Fuente: Recuperado de https://tools.ietf.org/html/rfc5340#section-2.6

Con el uso del campo Instancia ID, OSPFv3 puede establecer varias instancias por enlace lo que permite tener separado los dominios de enrutamiento y así mismo utilizar el mismo enlace. Ahora en cuanto a la autenticación no forma parte del protocolo ya que el nivel de seguridad de la integridad de la información es trabajo de IPv6. (N. Sheth, L. Wang, J. Zhang, 2013)

IS-IS para IPv6

El protocolo de IS-IS es de intra-dominio donde cada router que se encuentra en el dominio de enrutamiento emite su información relativa mediante el uso de LSP (protocolo de estado de enlace). IS-IS permite enrutar tanto IP como OSI y utiliza NLPID para la identificación del protocolo de red en uso. Son dos los niveles en los que trabaja, L1 (stub), L2 (Backbone) y la interconexión de los mismos L2/L1.

Para poder trabajar sobre IPv6 no se desarrolló una nueva versión, pero si se agregaron algunos cambios que son dos nuevos TLV, "capacidad IPv6" y "dirección de interfaz IPV6", además de un nuevo identificador de protocolo IPv6 (NLPID).

Capacidad IPv6: se describe la accesibilidad a la red a través de un prefijo especificado de enrutamiento, información de la métrica, un bit para indicar si el prefijo está por debajo un nivel superior y otro para saber si el prefijo está siendo distribuido de otro protocolo de enrutamiento y un sub-TLV que permite una posterior extensión. (Figura 15)

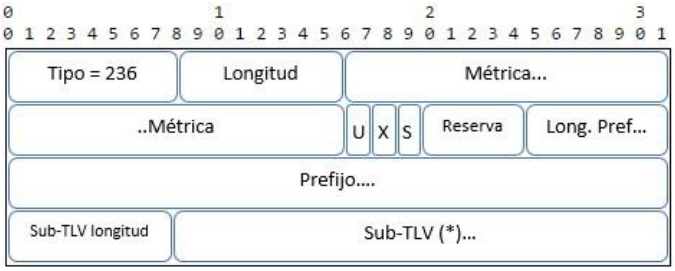


Figura 15. Estructura mensaje IS-IS

Fuente: Recuperado de https://tools.ietf.org/html/rfc5308

Dirección de Interfaz IPV6 TLV

Se modificó solo el contenido necesario y en lugar de tener de 0-63 en 4 octetos de direcciones de interfaz en IPv4 paso a ser de 0 – 15 en 16 octetos de interfaz en direcciones IPv6. Para el PDU hola, la dirección de interfaz TLV DEBE contener sólo las direcciones locales IPv6 de vínculo asignado a la interfaz que envía el Hola. (Figura 16)

Figura 16. IPv6 Interface Address TLV

Fuente: Recuperado de https://tools.ietf.org/html/rfc5308

Identificador de protocolo IPv6 NLPID

El valor en IPv6 asignado para el identificador de protocolo de capa es de 0x8E, 142 en decimal. (Hopps, 2008)

Enrutamiento externo

Para los sistemas autónomos fuera de su ámbito local se debe tener una estandarización que permita alcanzar a todos, para esto se utiliza BGP como estándar de “facto”.

Multiprotocolo BGP-4

BGP es un estándar de facto que se basa en el PVP (Path Vector Protocol) el cual es similar a el vector distancia, cada router de borde o frontera envía a sus vecinos la ruta completa a un destino y no solamente la distancia, siendo así que el camino es una secuencia de sistemas autónomos hasta el destino. BGP utiliza el puerto TCP 179 para establecer sus conexiones.

Formato de cabecera BGP

Cada mensaje tiene una cabecera de tamaño fijo, no necesariamente debe de existir una porción de datos después de la cabecera. (Figura 17)

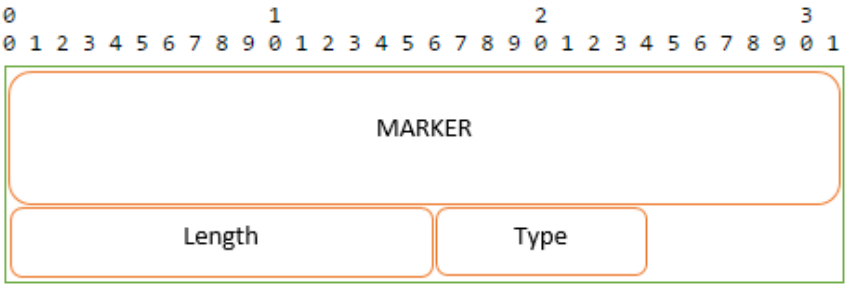


Figura 17. Formato de cabecera

Fuente: Recuperado de http://www.rfc-editor.org/rfc/rfc1771.txt

Marker- campo de 16 objetos en que el receptor pueda saber si el mensaje es abierto o si el mensaje no lleva ninguna información de autenticación, el marcador puede ser utilizado para detectar la pérdida de sincronización y para autenticar mensajes BGP entrantes.

Length- número entero sin signo de dos octetos, sirve para indicar la longitud total del mensaje, con el fin de permitir la ubicación en el nivel de transporte y transmitir los mensajes siguientes. (Sánches, 2006)

Para el intercambio de mensajes BGP utiliza TCP, entre los cuales se encuentran:

- OPEN- abre la conexión TCP. (Figura 18)

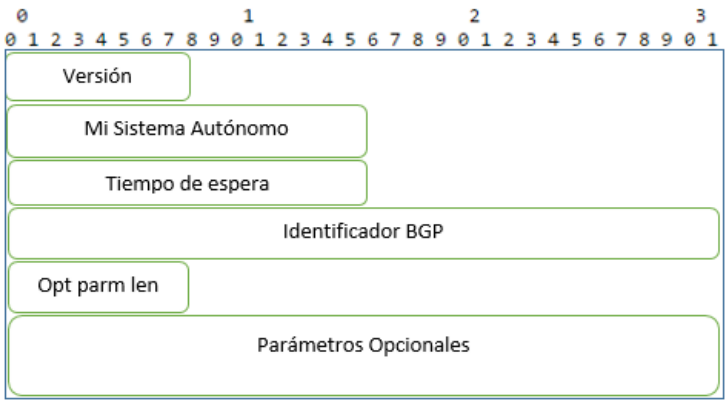


Figura 18. Mensaje OPEN

Fuente: Recuperado de https://www.ietf.org/rfc/rfc1771.txt

- UPDATE- mensaje de confirmación o aviso de un nuevo camino, compartición de información entre compañeros BGP. (Figura 19)

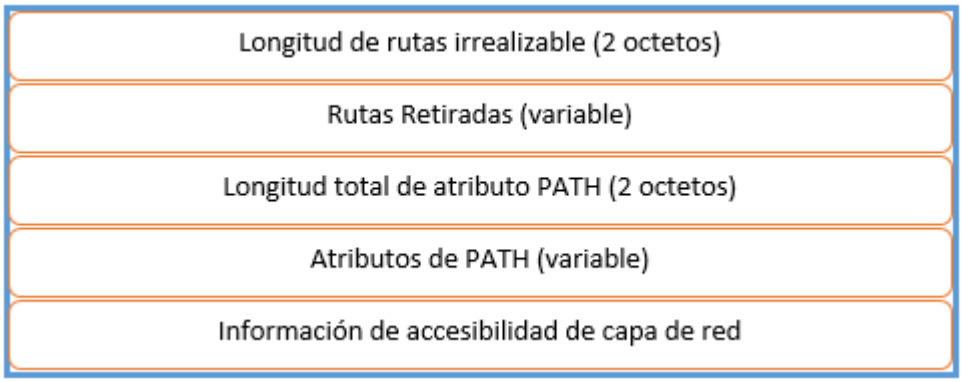


Figura 19. Mensaje de Actualización

Fuente: Recuperado de http://www.rfc-editor.org/rfc/rfc1771.txt

- KEEPALIVE- Mantiene la conexión abierta con TCP y como respuesta de un mensaje OPEN en la ausencia de UPDATES.
- NOTIFICATION- sirve para informar sobre errores en mensajes y para cerrar las conexiones.

Negociación BGP

Para abrir una conexión BGP los speakers pueden negociar la versión del protocolo haciendo múltiples intentos, comenzando con el más alto número de versión de soporte, si los compañeros o vecinos soportan uno o más versiones en común de soporte permitirá que se determine con mayor rapidez la versión común que debe de utilizar, con el fin de que en futuras negociaciones se conserve el formato de los mensajes de OPEN y de Notificaciones. (Flores, 2014)

Estados de BGP

El protocolo tiene diferentes estados en realiza sus diferentes operaciones, en los cuales se encuentra:

Idle State- el estado en reposo en BGP niega todas las conexiones entrantes BGP, en respuesta a un inicio de evento el sistema inicia todos los recursos BGP, también se inicial el temporizador connectRetry, se inicia una conexión de transporte de pares BGP y a su vez se puede escuchar una conexión iniciada por el mando a distancia de pares BGP. Dado el caso de que un transmisor detecte un error, se desconecta y cambia su estado a libre.

Connect State- es el estado en donde BGP espera a que el protocolo transporte complete la conexión, si existe se completa dicha conexión el sistema local limpia el temporizador ConnectRetry, envía un mensaje de abierto y cambia su estado a OpenSent, pero si la conexión no tiene éxito entonces se reinicia el temporizador y espera que se inicie una conexión por el par remoto de BGP y permanecer en estado conectado.

Active State- Es el estado donde BGP establece conexión con uno de los dispositivos que también están usando un sistema en común del protocolo de transporte,

si la conexión tienes éxito se limpia el temporizador ConnectRetry, escucha la conexión que fue iniciada por el par remoto de BGP y cambia su estado a Connect. Si la dirección IP del par remoto no es el parámetro esperado el sistema reinicia el temporizador y rechaza el intento de conexión, quedando en un estado activo.

OpenSent State- en este estado BGP espera un mensaje OPEN, si se recibe este mensaje todos los campos son revisados y corregidos, si se detecta un error en el encabezado o mensaje OPEN o una colisión de conexión en sistema local envía una notificación y cambia a estado libre, al no haber errores en el mensaje open BGP envía el mensaje KEEPALIVE y se establece el temporizador Keeplive. Si el valor en la espera de negociación es cero entonces los temporizadores no se inician, si el valor es igual que el del sistema autónomo local, es un sistema interno y si es diferente, es un sistema externo y se cambia al estado de OpenConfirm.

Established State- En el estado de establecimiento se pueden intercambiar mensajes de actualización, notificación y keepalive con sus pares BGP. El temporizador de espera en este estado se reinicia si recibe mensajes de actualización o keepalive, si el valor del tiempo de negociación de espera es diferente de cero. Si el sistema local recibe un mensaje de notificación cambia su estado a reposo (Idle). Si se agota el tiempo se envía una notificación y el sistema cambia su estado a libre. (P. Marques, F. Dupont, 1999)

Selección de Ruta

El proceso de selección de rutas se define por la aplicación de la base local de políticas de información (PIB) de las rutas almacenadas en Adj-RIB-IN. El resultado de este proceso de decisión es un conjunto de rutas que se anuncian a todos los pares conectados. El proceso de decisión se define en tres fases distintas. (Adriana Morales, 2010)

Fase 1- se calcula el nivel de preferencia de cada ruta recibida de un vecino del sistema autónomo y se utiliza speakers en el sistema autónomo local de rutas que tiene mayor grado de preferencia para cada destino.

Fase 2- responsable de elegir el mejor camino de los diferentes destinos disponibles, así también se realiza la instalación de cada ruta elegida en el loc-RIB indicado.

Fase 3- una vez establecido la loc-RIB se hace la difusión entre pares de sistemas autónomos vecinos, en esta fase también se puede realizar la reducción opcional de información.

El criterio de selección de ruta en el encaminamiento debe tener en cuenta las normas que se aplican a cada prefijo IP o al conjunto de prefijos IP destino, los pasos a seguir en una elección de ruta son:

1- Descartar la ruta si no existe NET-HOP
2- Eliminación de rutas con menor preferencia local (LOCAL-PREF)
3- Eliminación de rutas con AS-PATH más extenso
4- Las rutas con ORIGIN más alto se deben eliminar
5- Las rutas con mayor MED se eliminan
6- Al existir rutas aprendidas por EBGP se eliminan las rutas aprendidas por IBGP
7- Las rutas con mayor coste de NET-HOP se eliminan
8- Las rutas anunciadas por el router con el menor identificador BGP son de mayor preferencia
9- La interfaz que tiene la menor dirección para el vecino tiene mayor preferencia.

2.3.3 Beneficios de IPv6

IPv6 tiene una gran cantidad de beneficios desde diferentes aspectos, la consideración del uso de este protocolo podría reducir gastos de operación de red y en la TI, además brinda la oportunidad de expansión de dispositivos debido a la gran cantidad de direcciones disponibles. (Gerometta, 2011)

El protocolo con el que las redes de comunicación trabajan con una proyección futura es IPv6, todos los recursos he inversiones que se realizan basados en IPv6 tienen una vigencia y justificación en gastos con mayor preferencia que sistemas implementados sobre IPv4. (Awduche, 2010)

Entre los beneficios se puede destacar la flexibilidad y simplicidad de gestión de este protocolo, la eliminación de las direcciones públicas y privadas que se manejan en IPv4 elimina gastos en operaciones de dispositivos NAT, proporcionando un espacio mucho mayor de direcciones posibilita que se elimine este tipo de direcciones y dando cabida a nuevas funciones conjuntamente con la ampliable estructura de encabezamiento IPv6.

Los beneficios que proporciona IPv6 son muchos de los limitantes que tenía IPv4 y que con el tiempo pudo superar algunos, IPv6 no solo resuelve el problema del agotamiento de direcciones IP sino también proporciona los siguientes aportes en su implementación: (Guillermo Cicileo, 2009)

- ✓ Gran espacio direccionamiento
- ✓ Direcciones IP únicas en todos los dispositivos.
- ✓ Múltiples niveles de direccionamiento en la jerarquía que permite una fácil sumarización de rutas.
- ✓ Sumarización de rutas que permite la asignación de múltiples prefijos en la misma red.

- ✓ Autoconfiguración Stataless donde los dispositivos pueden estar en modo plug and play sin necesidad de que exista un servidor DHCP
- ✓ Autoconfiguración Stateful, permitiendo una configuración IP completa incluyendo servidores NTP o SIP, entre otros.
- ✓ Uso multicast ya que no existe dirección de broadcast, se configura una dirección reservada para definir todos los nodos.
- ✓ Simplicidad de encabezado.
- ✓ Eliminación de campo Checksum
- ✓ Inclusión de etiqueta de flujo para evitar que los dispositivos intermediaros accedan a la capa transporte.

2.3.4 Seguridad en IPv6

La seguridad no fue tomada en cuenta en un principio de la creación de internet, debido al crecimiento y la adopción en diferentes campos se determinó que la seguridad es una necesidad en las redes de comunicación, siendo así se optó una serie de especificaciones que garanticen la seguridad las cuales se conocen como IP Security o IPSec; en IPv6 se especifica que para evitar duplicidades y cerciorase de un sistema seguro y autentico en cada una de las capas se incluye las especificaciones en el nivel más bajo de la pila de protocolos.

Especificaciones IPSec

En los protocolos TCP.IP las especificaciones IPSec están definidas en la capa inferior de la pila, al trabajar con datagramas y siendo independiente de capas superiores IPSec se proporciona mediante los siguientes aspectos:

- ✓ **Cabecera de autenticación-** es la encargada de proporcionar autenticidad a los datos que se reciben tanto como el origen especifico del datagrama como también que los datagramas no han sido modificados.

- ✓ **Cifrado de seguridad-** la encriptación es la forma en que se garantiza que solo el destinatario legítimo al que va dirigida la información pueda descifrar el contenido del datagrama.

En IPSec la autenticidad y seguridad está dada por un algoritmo de cifrado/descifrado en una serie de parámetros que diferencian una comunicación de otra y conforman la asociación de seguridad. Cuando existe en un mismo ordenador diferentes asociaciones de seguridad se diferencian mediante el uso de un índice de parámetros de seguridad, esto permite identificar la asociación de seguridad del datagrama al que hace referencia y así poder autenticarlo o descifrarlo. (ACOSTA, y otros, 2014)

Cabecera de autenticación

Esta cabecera solo en IPv6 es designada con el número 51 y está por lo general antes de los datos con el fin de proteger la información, aunque también puede situarse antes de otras cabeceras para asegurar que todo el datagrama sea correcto, sin alterar el funcionamiento de los protocolos a nivel superior ni de routers intermedios que sirven para enrutar los datagramas a su destino. (Figura 20)

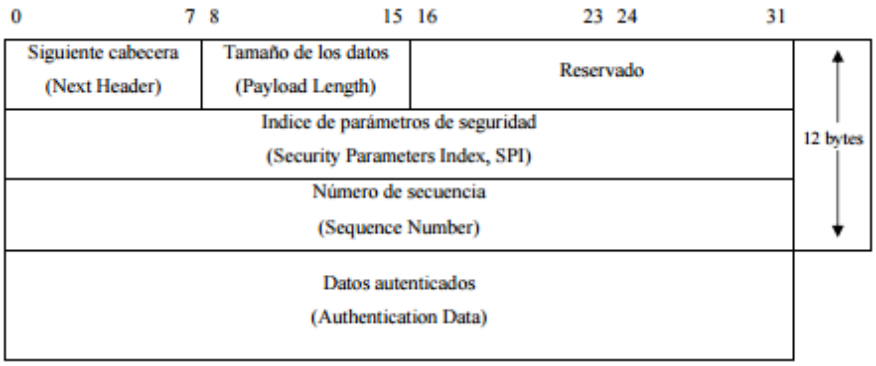


Figura 20. Cabecera de Autenticación

Fuente: Recuperado de http://www.redes-linux.com/manuales/ipv6/Memoria_del_proyecto_IPv6.pdf

- ✓ *Tamaño de datos*- en este campo se especifica longitud de datos en palabras de 32 bits
- ✓ *Índice de parámetros de seguridad (SPI)*- número (32bits) de conexiones con IPSec en un mismo ordenador.
- ✓ *Número de secuencia*- resuelve el número de datagrama de comunicación, en este campo que establece el orden y evita problemas de entrega de datagramas fuera de orden o de ataques externos.
- ✓ *Datos autenticados*- son el resultado de diversas operaciones entre algunos campos de cabecera IP, clave entre emisor, receptor y los datos enviados, además se utiliza MD5 para realizar el cálculo de datos autenticados.

Cabecera de cifrado

Se utiliza una cabecera de cifrado de seguridad para información que debe de tener acceso terceras personas, es decir información privada, esta cabecera se ubica al final de la cadena de cabeceras ya que a partir de ella se cifra todos los datos y los router intermedios serán incapaces de procesar las capas posteriores. (Figura 21)

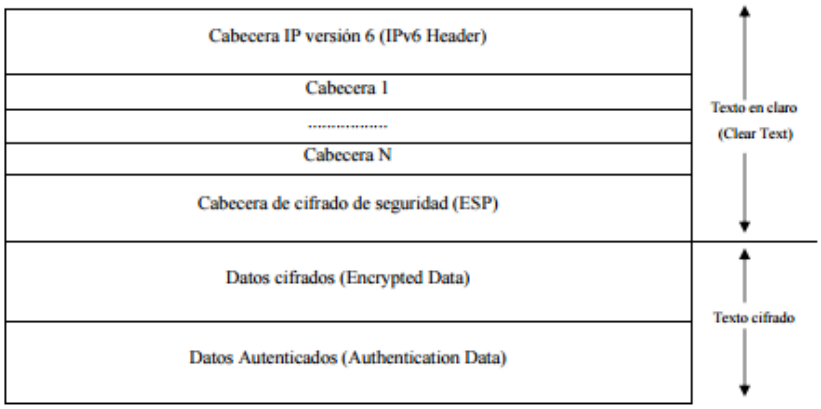


Figura 21. Escenario Cabecera de cifrado de seguridad

Fuente: Recuperado de http://www.redes-linux.com/manuales/ipv6/Memoria_del_proyecto_IPv6.pdf

Se propone DES-CBC como el algoritmo que se utiliza para la negociación con el receptor de la información, esto se hace antes de enviar un datagrama cifrado. No se

necesita especificar el tamaño de los datos cifrados a diferencia de la cabecera de autenticación. (Figura 22)

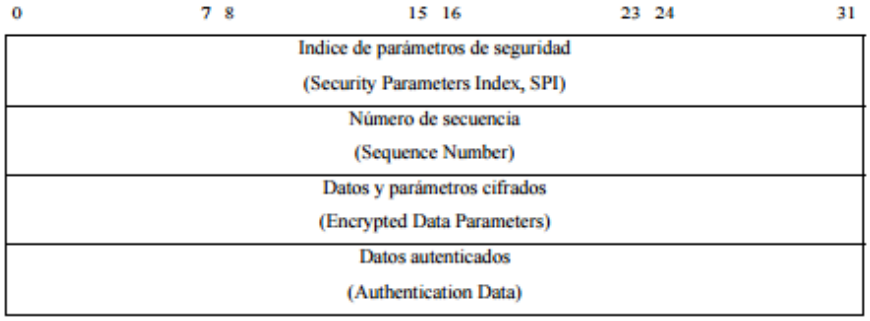


Figura 22. Cabecera de cifrado de seguridad

Fuente: Recuperado de http://www.redes-linux.com/manuales/ipv6/Memoria_del_proyecto_IPv6.pdf

IPSec brinda autenticidad y la confidencialidad de datagramas IP a través de un conjunto de algoritmos, se utiliza el protocolo IKE para el intercambio de claves, donde se aprovecha el intercambio de mensajes de ISAKMP para proporcionar un canal entre los usuarios que sea autentico y seguro. Además, IPSec facilita y mejora la seguridad en caso de existir Firewalls o VPN en un esquema de redes privadas. (Verdejo, 2000)

2.3.5 Adopción de IPv6

A partir del año 2002 empezó el despliegue de IPv6, los desarrolladores de sistemas operativos y fabricantes de equipos y dispositivos de redes ofrecían IPv6 en sus productos; ahora bien desde el año 2012 fue cuando si se empieza a operar en todo el mundo bajo el protocolo de internet IPv6, su despliegue avanza lento aunque seguro, debido a que la implantación no es tan sencilla como parece, en si prácticamente es empezar de cero si solo se quiere trabajar como protocolo de internet nativo a IPv6 y aún más complicado si se desea que tanto IPv6 como IPv4 funcionen en paralelo, un proceso de transición y coexistencia de ambos protocolos de internet es lo más apropiado hasta que IPv4 deje de utilizarse. (Guillermo Cicileo, 2009)

Entre las empresas que tienen activo sus servicios permanentes en IPv6 se encuentra Google, Yahoo! y Facebook de las más populares, en América latina la adopción es más lenta que en otras regios, pero se destaca a Ecuador con un 2% de adopción de IPv6. Actualmente la adopción mundial de IPv6 aproximadamente es del 8.65% según el seguimiento de Google al protocolo como se puede ver en la Figura23. (Cerf, 2012)

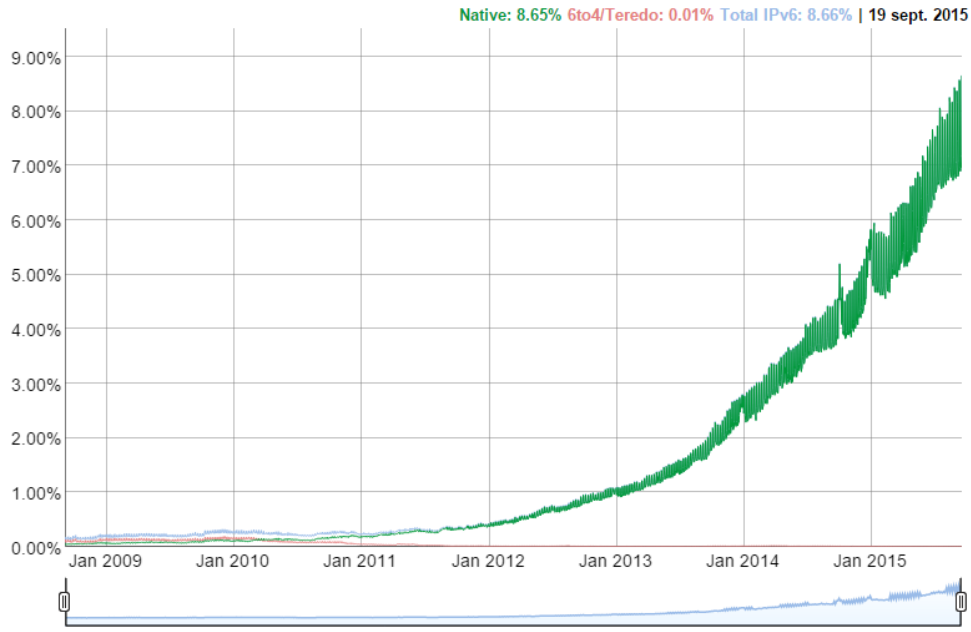


Figura 23. Porcentaje de usuarios que acceden a Google a través de IPv6

Fuente: Recuperado de http://www.google.com/intl/es/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption

Una adopción total de IPv6 llevara tiempo (Figura 24), para que esto suceda; servidores, sitios web y proveedores de internet deben realizar los cambios necesarios en sus instalaciones e infraestructuras, por lo tanto, ambos protocolos de internet IPv4 e IPv6 deberán estar funcionando hasta cuando sea necesario. (Cerf, 2012)

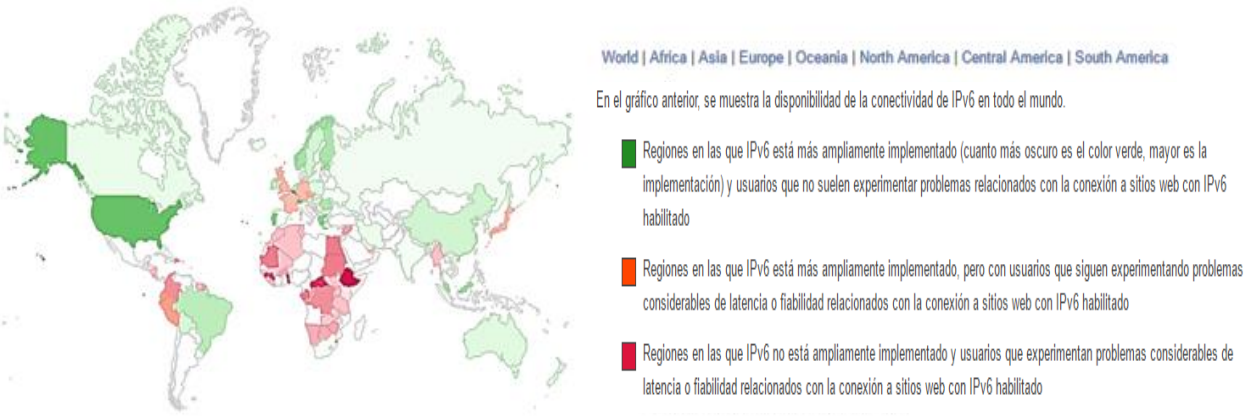


Figura 24. Adopción de IPv6 por País

Fuente: Recuperado de http://www.google.com/intl/es/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption

2.3.6 Actualidad LACNIC

Desde la aparición de IPv6 sus creadores sabían que este protocolo iba a ser la base de las comunicaciones, la realidad no es del todo cierto, debido a que existen diferentes aspectos por los que no se ha podido hacer una transición rápida, estos aspectos van desde el ámbito económico hasta la comprensión básica de funcionamiento de IPv6 en la actual y futura Internet.

A finales del 2014 según los datos proporcionados por Google el tráfico sobre IPv6 llego a un 5% y para el año 2015 en base a la misma fuente la tendencia de crecimiento es de forma ascendente, sabiendo que desde septiembre del 2014 las políticas restrictivas sobre la asignación de direcciones IPv4 entraron en vigor en los cinco registros regionales de internet, con lo que proponer crecimientos basados en IPv4 es cada vez más difícil y poco recomendable.

En la actualidad LACNIC tiene el mayor porcentaje con bloques de dirección IPv4 e IPv6 y ha realizado asignaciones de IPv6 donde la mayor parte ha sido a proveedores de servicio de internet, así como a Registros locales de internet, solo superado por Europa en este aspecto, en el caso de asignación de direcciones a organizaciones que no revenden

el servicio a terceros como los ISPs es muy diferente la situación, la región de Latinoamérica y el Caribe solo supera a la zona de África.

Teniendo en cuenta la cantidad de prefijos IPv6 en Latinoamérica y Caribe asignados, el crecimiento del empleo de este protocolo es favorable, pero también se sabe que para la integración de IPv6 a gran escala la infraestructura actual no puede realizarse únicamente con la asignación de números en internet, sino también deben colaborar diferentes sectores sociales y gubernamentales, así como también operadores de red, desarrolladores de aplicación y todos los que intervienen en la red de redes. (LACNIC, Portal Ipv6, s.f.)

LACNIC da a conocer las estadísticas de asignaciones de recursos numéricos de internet mediante las siguientes graficas: (Figura 25,26)

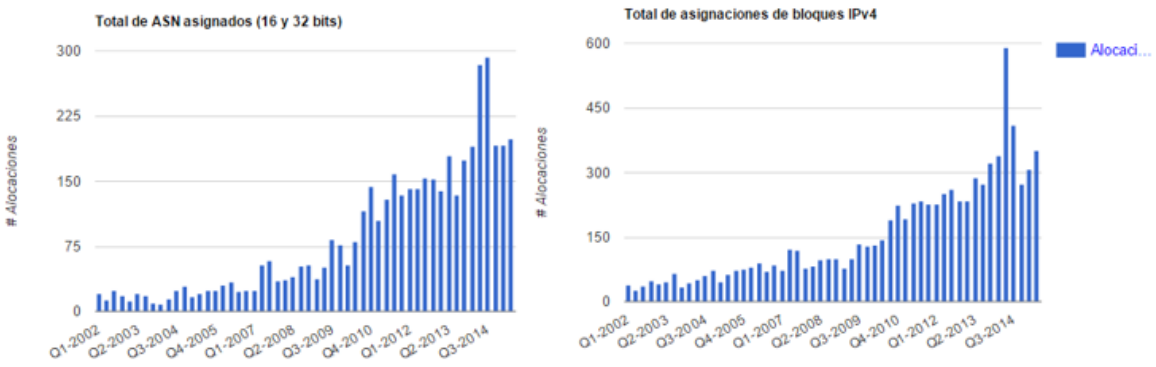


Figura 25. Total de asignaciones ASN y Bloques IPv4

Fuente: Recuperado de http://portalipv6.lacnic.net/reporte-de-terminacion-de-direcciones-ipv4/

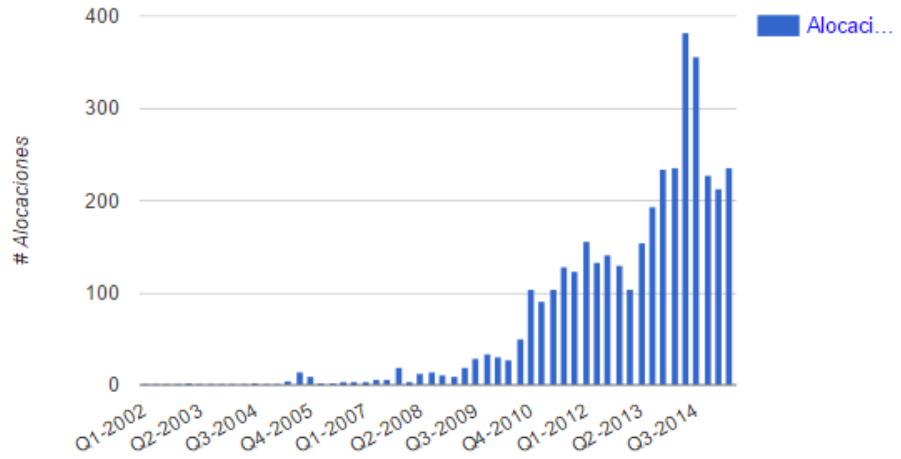


Figura 26. Total bloques asignados IPv6

Fuente: Recuperado de http://portalipv6.lacnic.net/reporte-de-terminacion-de-direcciones-ipv4/

2.3.7 Proveedores IPv6 en Ecuador

En Ecuador es AEPROVI (Asociación ecuatoriana de proveedores de valor agregado e Internet) el cual tiene como misión "Promover, proteger, masificar y desarrollar el Internet, como medio para el progreso social, económico, político y cultural en el Ecuador" (AEPROVI, s.f.). Este organismo es donde se encuentran asociados personas naturales o jurídicas en territorio ecuatoriano, entre las empresas que poseen una infraestructura que de soporte de IPv6 nativo están: (Tabla 7)

Tabla 7. Empresas con implementación IPv6

EMPRESA / INFRAESTRUCTURA	SOPORTE DE IPv6 NATIVO	COMENTARIOS
1	NAP.EC ✔	Punto de intercambio de tráfico local de Internet (IXP) del Ecuador. Administrado por AEPROVI.
2	Transnexa ✔	Proveedor de servicios portadores incluyendo tránsito internacional de Internet.

3	Telconet	✔	Proveedor de servicios portadores incluyendo tránsito internacional de Internet.

Fuente: Recuperado de http://ipv6tf.ec/quienes-estan-implementando-ipv6-en-ecuador

En la actualidad existen dos nodos Quito y Guayaquil, permitiendo la conexión entre los proveedores de internet y NAP.EC. (Figura 27)

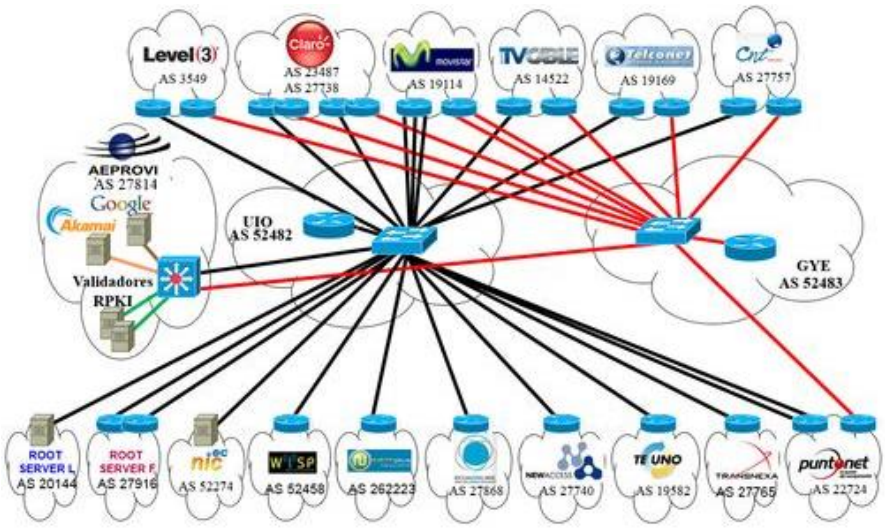


Figura 27. Topoloía de red NAP.EC

Fuente: Recuperado de http://aeprovi.org.ec/napec/topologia

Las redes ipv6 que existen en el Ecuador que han sido asignadas por LACNIC se encuentran diferenciadas en dos estados, “asignadas” son las que LACNIC asigno a ciertas entidades y “Allocated” rangos de direcciones IPv6 que se encuentran presentes en la tabla de direcciones global (Tabla 8). (AEPROVI, s.f.)

Tabla 8. Redes IPv6 Asignadas por LACNIC

Red IPv6	Institución/Empresa	Fecha de asignación	Estado
2001:13c7:6006::/48	AEPROVI	20081205	assigned

2001:13c7:6f00::/40	AEPROVI	20091009	assigned
2800:68::/32	CEDIA	20060719	allocated
2800:130::/32	UTPL	20070607	assigned
2800:2a0::/32	TELCONET	20080908	allocated
2800:2f0::/32	ETAPATELECOM	20090116	allocated
2800:370::/32	CNT CP	20090604	allocated
2800:400::/32	ETAPA	20091116	allocated
2800:430::/32	CONECEL	20100112	allocated
2800:440::/32	ECUADORTELECOM	20100121	allocated
2800:4f0::/32	EASYNET	20100803	allocated
2801:0:20::/48	ESPOL	20090102	assigned
2801:0:60::/48	NIC.EC	20100819	assigned

Fuente: Recuperado de http://ipv6.cedia.org.ec/index.php/la-realidad

En cuanto a TELCONET posee una infraestructura para manejo de IPv6 e Internet 2, en la cual la red académica avanzada del ecuador (CEDIA) opera sobre esta red nacional de nueva generación. (Figura 28)

Figura 28. Red NGN académica CEDIA sobre TELCONET

Fuente: Recuperado de http://www.telconet.net/servicios/internet2

2.3.8 Actualidad de IPv6 en la Universidad Técnica del Norte

La Universidad Técnica del Norte dispone de un pool de direcciones asignado por CEDIA, el cual comprende la red 2800:68:19::/48 y utiliza la infraestructura del proveedor de servicio de internet a la institución (Telconet) para el establecimiento de conexión con la institución.

IPv6 en la UTN es una tecnología que aún no se está utilizando, debido a que la disposición de servicios e infraestructura de red solo se encuentra disponible sobre el protocolo de internet versión 4. Además, no se ha realizado un direccionamiento del recurso y las configuraciones para el uso del protocolo son nulas.

Técnicamente el recurso IPv4 de la institución satisface la necesidad de direcciones que se utilizan en servicios y aplicaciones locales como de internet, pero la importancia que tiene la implementación de aplicaciones sobre el protocolo IPv6 y aún más de que la infraestructura de red soporte esta tecnología, ayudaran al desarrollo y crecimiento de la red, como también de aplicaciones y servicios como lo es la privacidad, VoIP, velocidad, multimedia, Internet de las cosas (IOT), transferencia de archivos, correo electrónico, videoconferencias entre otras, por tal razón es preciso que el proceso de transición IPv4 a IPv6 esté en marcha.

2.4 Transición de IPv4 a IPv6

Como ya es de conocimiento las direcciones IPv4 están agotadas y realizar una transición de protocolo de internet es inminente, debido a la incompatibilidad de paquetes entre IPv6 e IPv4 ambos protocolos deben de estar presentes hasta que sea necesario.

Existen diferentes tipos de métodos para empezar la transición de la versión 4 a la versión 6 del protocolo de internet, entre los cuales encontramos los mecanismos que se basan en encapsular paquetes IPv6 en paquetes IPv4 o de forma contraria y también están

los mecanismos de traducción, es decir, pasar paquetes de un formato a otro basándose en traducir los elementos de red.

2.5 MECANISMO DE TRANSICIÓN

Los mecanismos de transición considerados son los que se consideran de mayor utilidad para los operadores de red, se puede realizar una clasificación de acuerdo el tipo de técnica que se utiliza: Dual stack, túneles y traducción.

2.5.1 DS-Lite (dual-stack)

Esta técnica utiliza un túnel que encapsula IPv4 en IPv6 y no una doble traducción de protocolos, siendo así, el usuario se conecta con IPv6 nativo, pero también recibe una dirección IPv4 privada.

DS-Lite también es una clase de CGNAT, es decir, depende de NAT44 stateful en el proveedor de acceso. En esta técnica, el equipo responsable por el CGNAT recibe el nombre de AFTR (Address Family Transition Router). En la red del usuario, el CPE recibe el nombre de B4 (Basic Bridge BroadBand) y actúa como un bridge para el IPv4, en la terminación del túnel. (Operadores IPv6), En si DS-lite permite la asignación de direcciones IPv6 de forma nativa, pero sin dejar de dar soporte a los clientes IPv4 (Figura 29). (ACOSTA, y otros, 2014)

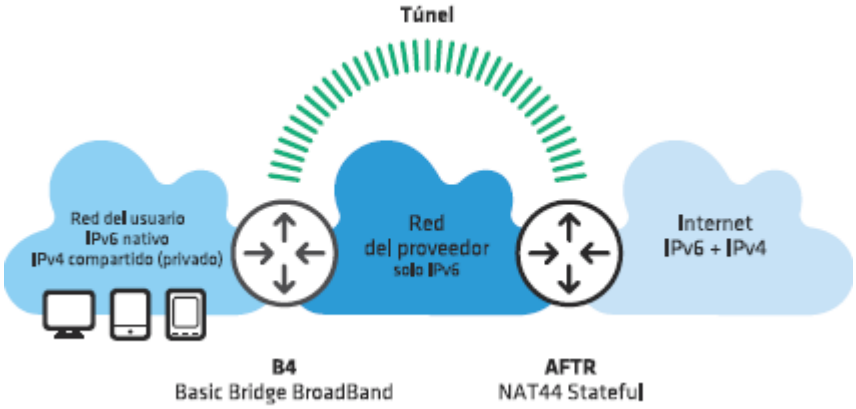


Figura 29. DS-LITE

Fuente: IPv6 para Operadores de RED, pag 142

Una red en donde se encuentra implementado DS-lite se dispone de un dispositivo con funciones de B4 (bridge), el cual asigna las direcciones privadas IPv4 en la red local del cliente, mediante B4 el AFTR tiene un puerto directamente conectado entre la red del proveedor de servicio y el usuario/cliente utilizando una dirección IPv6 en establecimiento el túnel.

Cabe mencionar que en el borde del proveedor de servicios de la red IPv6 generalmente se encuentra el AFTR y termina el túnel creado con el elemento B4 del usuario, AFTR también proporciona NAT44 para la traducción de direcciones privadas a públicas en el caso de IPv4. (DOYLE, 2009)

Procedimiento para el establecimiento de la conexión DS-lite:

1) Host con dirección IPv4 privada inicia una conexión a un recurso en la Internet pública
2) El tráfico se envía a B4, que es la puerta de enlace predeterminada
3) B4, utilizando su red de proveedores de servicios frente a las direcciones IPv6 establece el túnel con de AFTR. Dirección del de AFTR puede ser pre-configurado o puede ser descubierto usando DHCPv6
4) B4 encapsula los paquetes IPv4 en el transporte IPv6 y lo envía a través a de AFTR

5) De AFTR termina el túnel y de-encapsular el paquete IPv4
6) Dispositivo de AFTR realiza NAT44 antes de enviar tráfico a la red IPv4 destino

Los beneficios que brinda la utilización de DS-lite son muchos, entre los cuales se encuentran:

1) Una solución ligera para permitir la conectividad IPv4 sobre red IPv6
2) Evita la necesidad de múltiples niveles de NAT como en el caso de LSN
3) Permite a los proveedores de servicios para mover sus redes básicas y de acceso a IPv6 lo que les permite beneficiarse de las ventajas de IPv6
4) Permite la coexistencia de IPv4 e IPv6
5) Ayuda a IPv4 determinación problema la escasez de direcciones
6) Permite la migración gradual de ambiente nativo IPv6

Por otra parte, los retos a vencer por parte de DS-lite son: (Digani, 2012)

1) DS Lite no proporciona IPv6 y IPv4 acoge a hablar entre sí
2) Aumenta el tamaño del tráfico debido a las cabeceras de túneles - requiere la gestión de MTU para evitar la fragmentación
3) Necesidad de gestionar y mantener enlaces entre las direcciones y direcciones de clientes públicos utilizados para la traducción en el dispositivo de AFTR
4) Trae en desafíos adicionales para los DPI en la red de proveedores de servicios

2.5.2 Túneles

Existe gran variedad de técnicas que usan túneles para la transición de una red IPv4 a IPv6, aun que fueron creados en otro contexto pero que en la actualidad siguen siendo muy útiles en determinadas situaciones, en esta parte solo se consideran los que son adecuados para este proyecto. (Ralli, 2012)

Los túneles como mecanismos solo se usan donde se quiere desplegar una red IPv6 y no se tiene una infraestructura para la misma, y la base de la red es aun IPv4 la cual no podrá ser modificada a corto plazo.

El funcionamiento general es crear un paquete IPv4 que encapsule a otro paquete con IPv6, la cabecera del protocolo transportador (IPv4) contiene la dirección de fuente destino y como cuerpo o contenido el encabezado IPv6 seguido por los datos, en el nodo a la salida del túnel se elimina el encabezado IPv4 y se actualiza el encabezado IPv6, luego de esto se procesa el paquete IPv6. (Adriana Morales, 2010)

2.5.2.1 Túneles 6to4

Este mecanismo solo se incluye para comprender de mejor manera la técnica 6rd, comprendiendo los problemas de seguridad de 6to4 para los administradores de red, así como también saber que esta técnica actualmente no se utiliza mucho. Los elementos principales son:

- ✓ **Clientes 6t4:** computadores/host conectados a la red que utilizan el túnel para obtener conectividad IPv6
- ✓ **Routers 6to4:** Es aquel que sirve como extremo del túnel en la red y tiene una dirección IPv4 valida, a partir de esto utilizando un prefijo /16 más los 32 bits de la dirección IPv4, se forma un prefijo /48 de IPv6 para poder ser usado en la red. (Figura 30)
- ✓ **Relays 6to4:** son routers con conectividad nativa en ambos protocolos de internet y proveen el otro extremo del túnel, en Internet IPv6 estos routers se anuncian para el prefijo 2002::/16

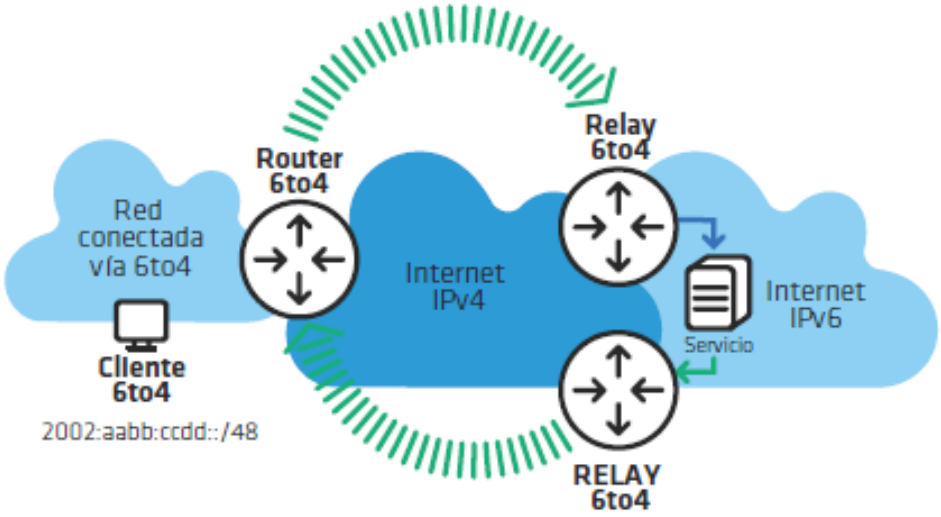


Figura 30. Túnel 6to4

Fuente: IPv6 Para Operadores De Red, pag 131.

El encapsulamiento se hace utilizando 6in4, donde el router encuentra el relay más cercano para el envío de la dirección IPv4 anycast, el cual desencapasula el paquete y lo envía a internet IPv6, el cual es enviado al relay más cercano al destino y se encapsula nuevamente para que en el paquete la dirección IPv4 forme parte de la dirección IPv6 del destino (Figura 31). Los túneles no son necesariamente simétricos y también se pueden configurar manualmente y es imposible para el usuario controlar en camino inverso. (Guillermo Cicileo, 2009)

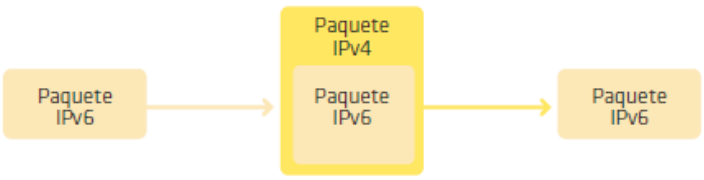


Figura 31. Diagrama de bloques de encapsulamiento

Fuente: IPv6 Para Operadores De Red, pag 131.

Entre los problemas que afectan a 6to esta que los relays son públicos y no garantizan un servicio de calidad y seguridad, en sistemas operativos como Windows desde la versión XP en adelante, una vez obtiene una dirección en IPv4 valida, el ordenador pasa a actuar como cliente y router 6to4, lo cual no es conveniente en una red

empresarial ya que los túneles pueden saltarse algunas medidas de seguridad como firewalls, así como también la iteración con otros servicios en internet de doble pila de menor calidad que la se obtiene con servicios nativos en IPv6 e IPv4. (Flores, 2014)

2.5.2.2 Túneles 6RD

Es una técnica derivada de 6to4 pero que resuelve los problemas que presenta en asimetría y control en los relays sobre los que trabaja, además presenta la ventaja de poder implementar IPv6 sin modificar el núcleo basado en MPLS IPv4. La infraestructura de que se utiliza para el acceso IPv4 sirve para poder realizar una implementación de IPv6 para llegar hasta el usuario final sin necesidad de realizar modificaciones en la misma.

Principalmente los elementos que son indispensables son el equipo local 6rd (CPE 6rd) y el relay 6rd, la diferencia entre un CPE 6rd y un router 6to4 es que utiliza un prefijo del bloque de direcciones de acceso. Generalmente se usa un prefijo de 32 bits, pero no es regla y puede utilizarse otro prefijo de mayor longitud. El relay 6rd está alojado en el proveedor de servicios y el encapsulamiento que se usa es 6in4 además de tener conectividad nativa en ambos protocolos de internet. (Ralli, 2012)

Para la resolución de los problemas de 6to4 no solo se cambia el prefijo como se mencionó anteriormente, sino también se reemplaza la dirección anycast por defecto (192.168.99.1) con una dirección escogida por el proveedor de servicios, este también actualiza o provee el Gateway 6rd utilizando uno o varios relays 6rd ya desplegados. (Figura 32)

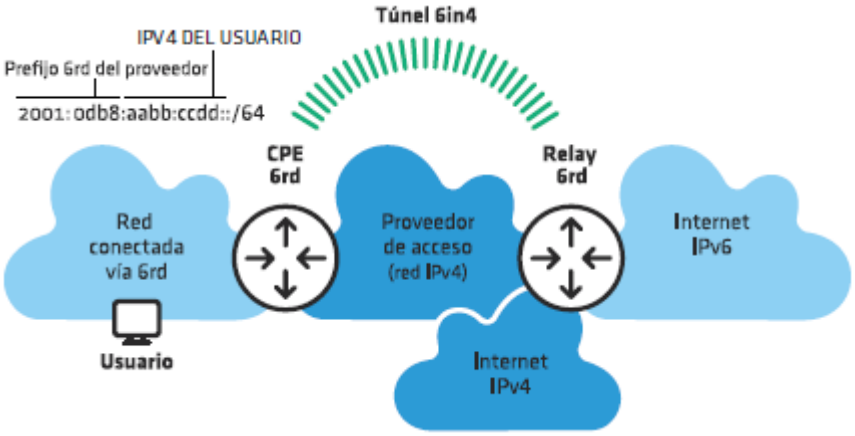


Figura 32. Túnel 6rd

Fuente: IPv6 Para Operadores De Red, pag 132.

Optar por usar túnel 6rd resuelve los problemas de falta de control de tráfico y disminuye el riesgo de ataques de seguridad, además que para los usuarios es transparente un despliegue de este tipo ya que lo hace plenamente el proveedor de servicio; pero para poder tener una implementación sin problemas solo se debe hacer en redes en las cuales el proveedor de servicios tiene direcciones IPv4 disponibles y no se van a ver afectados por el agotamiento de direcciones durante un tiempo prudencial, es decir, solo utilizar esta técnica hasta antes que el agotamiento afecte al proveedor, luego de esto se deberá utilizar otra técnica. (Guillermo Cicileo, 2009)

2.5.3 DNS64 y NAT64

NAT64 es un mecanismo que permite el uso compartido de direcciones IPv4, así como también se usa para la traducción de paquetes y puertos de IPv6 a IPv4, junto con DNS64 como técnica auxiliar de mapeo para nombres de dominio. Con el uso de ambas técnicas los usuarios posiblemente recibirán únicamente direcciones IPv6 como también acceder a servicios en IPv4, acción que para el usuario debe ser transparente y para los equipos parecerá que todos los sitios y servicios son en IPv6 nativo, en cuanto a los sitios o servicios en internet recibirán una petición de una dirección IPv4. (Figura 33)

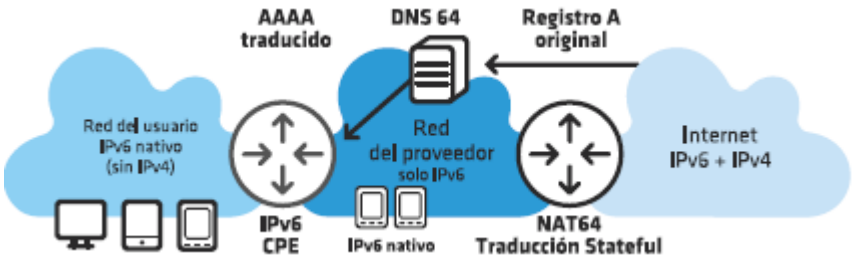


Figura 33. DNS64 y NAT64

Fuente: IPv6 Para Operadores De Red, pag 138.

Existe un bloque que se ha definido con el fin de que las direcciones IPv4 se mapeen a un prefijo IPv6, el cual se encuentra en el RFC 6052 y es 64:ff9b::/96. El primer paso para acceder a los recursos IPv4 en internet es una consulta de dominio, DNS64 se encarga de las peticiones que no tienen como un registro AAAA de origen y si de registro A, direccionar a esta petición utilizando la misma regla de mapeo de NAT64, los paquetes son encaminados a el dispositivo que realiza la traducción stateful hacia IPv4, este paquete ya traducido se dirige a internet y su dirección de origen forma parte de un pool de uso compartido, teniendo en cuenta que la traducción inversa se hace en la respuesta. (ACOSTA, y otros, 2014)

En el uso de DNS64 y NAT64 es importante saber que la desventaja está en que no todos los servicios y aplicaciones soportan IPv6, lo cual con el tiempo será irrelevante o se dé solución en un lapso corto de tiempo. Ahora bien, puede ser que el uso de este mecanismo sea el más apto para una transición de protocolos de internet, pues es la única técnica en la que los usuarios trabajan con IPv6 a diferencia de los demás mecanismos de transición, entonces si toda la red de internet y los proveedores de servicios y aplicaciones trabajen solo utilizando IPv6 todo el tráfico migra automáticamente a IPv6. (Alonso J, Martines C. , 2012)

2.5.4 Consideraciones sobre los mecanismos de transición

Hay que tener en cuenta que toda la red de internet está migrando hacia IPv6, debido al agotamiento de direcciones IPv4 y hay que considerar la importancia de elegir un mecanismo de transición adecuado teniendo en cuenta esto. (Cabellos, 2004)

Existen redes que no crecen rápidamente como son las corporativas y otras que si lo hacen como son las residenciales, más sin embargo conviene empezar con la transición y saber cualquier mecanismo que se use deben estar orientado a la utilización solamente de IPv6. Entre las opciones que se pueden elegir se encuentran técnicas de túnel, doble pila y traducción, no hay que olvidar sobre que protocolo base se quiere que la red en la que se realiza la transición trabajara. (DOYLE, 2009)

2.6 SERVIDORES

Se puede definir un servidor como un equipo capacitado y adecuado como infraestructura de hardware y software, que brinden el soporte necesario para albergar una o más aplicaciones que serán utilizadas por otras máquinas que se encuentren conectadas en un entorno de red que puede ser local o global dependiendo de la disponibilidad requerida o autorizada por los operadores de red.

En términos informáticos el servidor es el software que ofrece diferentes servicios con el propósito de que accedan diferentes usuarios/clientes y existe una gran cantidad de recursos o servicios que se pueden habilitar. (Barrios, 2015)

2.6.1 Tipos

Dependiendo de la exigencia de la red pueden existir servidores dedicados o de multiservicios, es decir, equipos que por la gran cantidad de tráfico solo realicen procesos

de una aplicación específica, o bien un súper equipo que pueda trabajar en multiplataforma dando soporte de varias aplicaciones.

En este trabajo solo se detallarán los servicios que serán utilizados, no obstante, existen diferentes tipos de servicios como: (ACOSTA, y otros, 2014)

- ✓ Telnet
- ✓ SSH
- ✓ FTP
- ✓ Mail (Correo/mensajería)
- ✓ Transmisión Multimedia
- ✓ Web
- ✓ DNS
- ✓ DHCP
- ✓ Base de Datos (BBD)
- ✓ Proxy

2.6.2 Servidor DHCP en IPv4/IPv6

Un servidor DHCP (Protocolo de configuración dinámica de Host) cumple la función de simplificar la administración de configuración de direcciones en la red, este servicio se utiliza en arquitecturas sin habilitar la configuración automática de direcciones en el caso de IPv6, en entornos de red IPv4 se realiza para la configuración automática de dispositivos en la red.

Con la disposición de un servidor DHCP se evita la configuración manual de las computadoras o diferentes dispositivos de uno en uno, este recibe las peticiones de clientes que solicitan una dirección de red y en respuesta envía los parámetros que permitirán auto configurarse. Entre los parámetros que envía están:

- ✓ Dirección IP
- ✓ Mascara de subred
- ✓ Gateway
- ✓ DNS

DHCP en IPv4, cumple con la función de asignar direcciones que están en un rango prefijado, evitando que estas generen un conflicto de IP por estar asignadas a otro equipo, cuando un cliente/usuario está configurado para acoplarse a la red mediante DHCP busca un servidor de este tipo para ser parte de la red, si no encuentra uno entonces no podrá disponer de una dirección IP que le permita comunicarse con toda la red. (Figura 34)

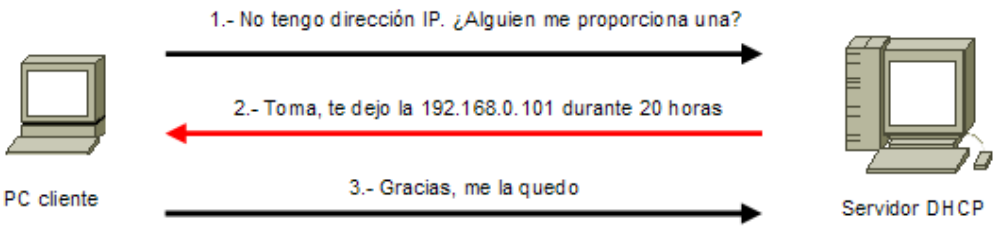


Figura 34. DHCP sobre ipv4

Fuente: Recuperado de http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dhcp.html

DHCP sobre IPv6 presenta significativas diferencias con respecto a su funcionamiento con IPv4, este tipo de servicio es stateful y es el encargado de distribuir direcciones e información de red en forma dinámica, como se sabe ambos protocolos son incompatibles y por lo ya dicho un servidor de doble pila presentaría muchos problemas de funcionamiento, por tal razón es mejor tener un servidor DHCP en IPv4 y otro diferente en IPv6.

DHCPv6 traba sobre UDP utiliza multicast en lugar de broadcast y la arquitectura empleada es cliente servidor. En IPv6 la configuración automática esta por defecto, este proceso asigna direcciones automáticamente al host cuando se conectan a la red, la dirección que utiliza se deriva desde los gatsways pero no asignan todos los parámetros

que con un servidor de direccionamiento dinámico si se puede, tales como son DNS, NTP entre otros. Los mensajes que se intercambian entre el servidor DHCPv6 y los usuarios son:

Solicit: envió de dirección multicast reservada, con el fin de encontrar un servidor DHCP, tanto agentes como servidores DHCPv6 son de tipo multicast.

Advertise: es un mensaje que se envía a todos los clientes indicando la disponibilidad del servidor para asignar una dirección.

Request: Mensaje que envía un cliente a un servidor para solicitar los parámetros de configuración de red.

Reply: mensaje enviado desde el servidor hacia la dirección de enlace local con la respuesta del mensaje request.

2.6.3 Servidor WEB en IPv4/IPv6

Cuando se habla de web se asocia a internet, a través de los navegadores disponibles en los diferentes dispositivos con acceso a la red para acceder a sitios web, que ofrecen diferentes tipos de información, archivos, enlaces a más aplicaciones, música, videos, entre otras.

Entonces un servidor web es un programa que actúa como un gestor de uno o más sitios web al que los usuarios pueden acceder por medio de un navegador que realiza el intercambio de información entre el usuario y el servidor mediante HTTP que generalmente en la navegación web usa el puerto 80 y se basa en el modelo cliente servidor. (Figura 35)

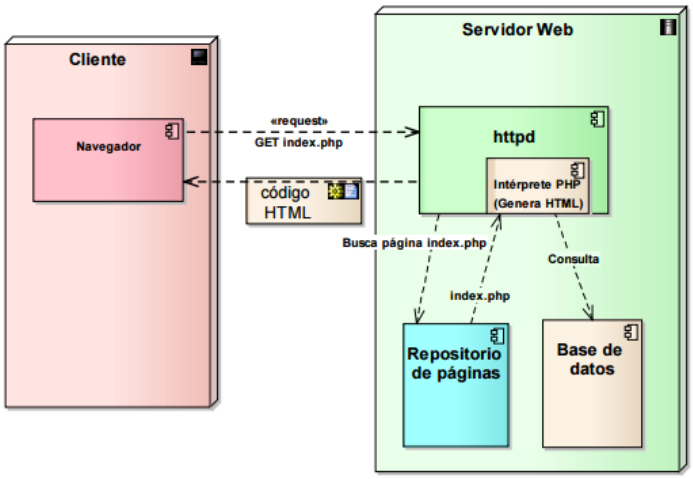


Figura 35. Esquema de Funcionamiento de servidor web

Fuente: Recuperado de http://www.fdi.ucm.es/profesor/jpavon/web/31-ServidoresWeb-Apache.pdf

Los programas más utilizados para ofrecer este servicio son Apache e IIS, donde apache es el más extendido de los servidores web y opera bajo las plataformas Linux, para tener soporto sobre IPv6 se debe utilizar versiones des de la 2.x. en adelante. IIS se usa en entornos de Microsoft Windows y para trabajar sobre IPv6 hay que habilitar y configurar la opción en el administrador IIS.

2.6.4 Servidor FTP en IPv4/IPv6

Un servidor FTP es un programa que se instala con el fin de permitir la transferencia de datos entre servidores/usuarios, proporciona movilidad de archivos entre distintos ordenadores brindado seguridad y organización de archivos, FTP usa los puertos 20 y 21 generalmente, el modelo base es cliente-servidor

Uno de los problemas de ftp era la seguridad porque su creación fue pensada en ofrecer la máxima velocidad de conexión, aunque actualmente se ha solucionado parcialmente ya que soporta diferentes protocolos de seguridad.

FTP funciona tanto en IPv4 como en IPv6 pero no al mismo tiempo bajo un mismo dominio, si se quiere trabajar bajo un mismo programa solo se debe activar un protocolo de internet, o generar dos programas que trabajen separados pero bajo el mismo ordenador. (Figura 36)

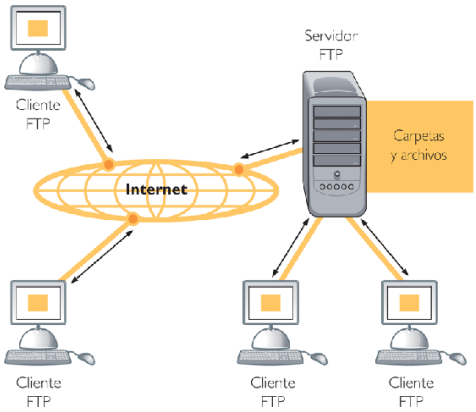


Figura 36. Funcionamiento de FTP

Fuente: Recuperado de https://serviciosenredabs8185.wordpress.com/category/ftp/

2.7 SISTEMA DE SEGURIDAD

La seguridad en la red de la Universidad Técnica del Norte se encuentra organizada bajo ciertos parámetros y con equipos en un orden determinado y con tareas específicas, se cuenta con firewall como base de la seguridad.

2.7.1 Zona Desmilitarizada (DMZ)

Mediante el uso de firewalls se puede establecer reglas entre dos redes, pero en una arquitectura de red mayor donde existen varias subredes con diferentes políticas de seguridad es necesario implementar un sistema de firewall para poder aislar las diferentes redes que existen en una institución/empresa.

Por lo general existen servidores que forman parte de la red local de una institución y que también deben ser accesibles desde el exterior, entra las cuales están servidor web, servidor de mensajería, servidor FTP, entre otros. La implementación de una DMZ de una zona aislada que alberga aplicaciones de acceso público se sintetiza en la generación de una nueva política de seguridad que permita el acceso tanto local como externo y que no comprometa la seguridad de toda la red, es decir, una DMZ es una zona intermedia entre la red interna a proteger y la red de poca seguridad propensa a ataques. (Figura 37)

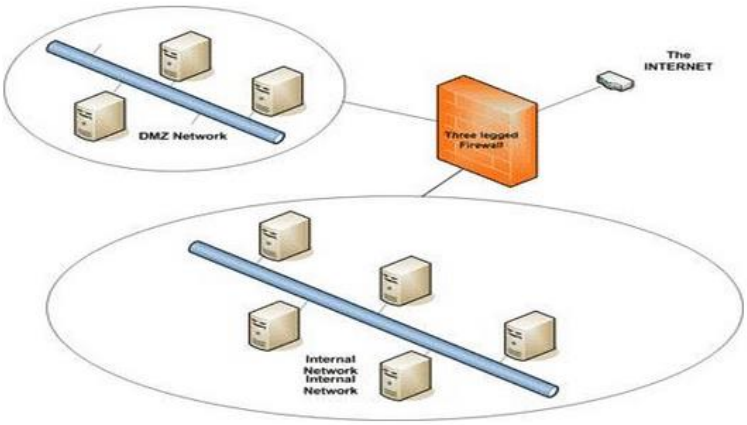


Figura 37. Representación de una DMZ

Fuente: Recuperado de http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-DMZ.php

2.7.2 Seguridad a nivel de Hardware y Software

La seguridad a nivel de hardware cuenta con equipos que posibilitan la administración segura de la red, entre los cuales se tiene:

- Cisco ASA 5520 Series
- Nexus 5548
- Swicht The Core Catalys 4510R + E

El software que provee cada uno de estos equipos sirve para monitorear el estado de la red y gestionar la misma, con lo cual se tiene control del acceso de entrada y salida como también del tráfico que existe en el entorno de red de la UTN.

2.8 SISTEMAS OPERATIVOS

Un sistema operativo es un conjunto de programas con el fin de ejecutar varias tareas para la interacción usuario máquina, así como también manejan el hardware de un dispositivo o equipo electrónico. Otra de las tareas que cumple es la administración de los periféricos de una computadora y mantiene la integridad del sistema.

Entre las tareas del sistema operativo (SSOO) están las de iniciar los procesos que se utilizaran para funcionar correctamente, además de cargar en memoria y la ejecución de los programas elegidos por el usuario, este también realiza la administración de recursos y se preocupa de que todos los componentes estén funcionando adecuadamente.

Un sistema operativo se compone de un conjunto de módulos, donde cada uno es responsable de ejecutar una función específica, entre los cuales están comúnmente:

- ✓ Núcleo
- ✓ Administrador de procesos
- ✓ Schduler
- ✓ Administrador de archivos

La lista de sistemas operativos que existen actualmente es muy extensa, pero entre los más conocidos están: (Figura 38)

- ✓ Microsoft Windows
- ✓ Windows Server (servidores)
- ✓ Linux (ordenadores/servidores)
- ✓ Mac OS

- ✓ Chrome OS (ordenadores)
- ✓ Android (SmartPhones)
- ✓ Windows Phone (para SmartPhones)
- ✓ iOS (SmartPhones)
- ✓ BlackBerry OS (SmartPhones)

Figura 38. Sistemas Operativos

Fuente: Recuperado de http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-el-sistema-operativo.php

2.8.1 Software libre

El software libre se fundamenta en la libertad y conocimiento abierto, así como también en principios éticos y la solidaridad sin dejar de lado un modelo que permita sostenibilidad económica, por tanto, hablar de software libre es referirse a libertad de elegir, compartir, utilizar las herramientas que se necesiten.

Este tipo de software no tiene tipo de restricciones políticas, geográficas o ideológicas, se puede distribuir sin problemas, generalmente el software es gratuito, pero no es obligatorio serlo, entre las condiciones principales para que sea libre, es que debe cumplir con todas las libertades y se debe entregar el código fuente e instrucciones que indican cómo funciona el programa.

2.8.1.1 Centos 6.5

Centos es un sistema operativo comunitario en base de Linux, es un programa de uso gratuito, pero se deriva de un sistema operativo comercial llamado Red Hat Enterprise Server y por su similitud en diseño es mucho más estable que otros sistemas de Linux distribuidos libremente, Centos solo ejecuta la parte más básica de los programas para evitar el bloque del sistema, por esta razón también opera con mayor velocidad que sus similares. (Figura 39)

La confiabilidad de Centos como sistema operativo es realmente buena, ya que puede ejecutar un ordenador por un largo tiempo sin la necesidad de actualizaciones adicionales, pero dado el caso las actualizaciones de hardware no hay problema ya que estas son desarrolladas para tener concurrencia con Red Hat, y el tiempo de estas es aproximadamente de 5 años mucho más de lo que otros sistemas operativos basados en Linux ofrecen, los cuales oscilan de 18 meces hasta máximo tres años.

Figura 39. Centos 6.5

Fuente: Recuperado de http://www.comoinstalarlinux.com/centos-6-5-disponible-para-descargar

Centos como requisitos de operación no es muy exigente y proporciona un buen rendimiento del ordenador o servidor, para lograr un funcionamiento correcto el mínimo que solicita es:

Entorno básico

- Memoria RAM 64MB (mínimo)
- De 1GB – 2GB de espacio en disco duro
- Procesador de 86x o 64x (32bits, 64bits)

Entorno Grafico

- Memoria RAM 2GB (mínimo)
- De 20GB – 40GB de espacio en disco duro
- Procesador de 86x o 64x (32bits, 64bits)

2.8.1.1.1 Requerimientos IPv6

Centos 6.5 tiene un soporte total sobre IPv6, los requerimientos para el uso del protocolo solo se derivan al conocimiento de implementación ya que está habilitado por defecto. Para empezar a utilizar IPv6 hay que editar los ficheros de configuración de red y adicionar la información para el uso y direccionamiento del protocolo de internet a utilizar.

Los archivos que se deben de modificar son los que contienen la información que el sistema operativo utiliza para la configuración de interfaces y direccionamiento, estos ficheros están ubicados en directorio de /etc/sysconfig/network y /etc/sysconfig/network-scripts/ifcfg-ethx respectivamente.

2.8.1.1.2 Arquitecturas

El soporte de Centos es igual al de Red Hat Enterprise Linux, y agrega dos más que no soporta su original, estas son:

- Intel x86-compatible (32 bit) (Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/II/III, AMD Duron, Athlon/XP/MP).

- Intel Itanium (64 bit).
- Advanced Micro Devices AMD64(Athlon 64, etc) e Intel EM64T (64 bit).
- PowerPC/32 (Apple Macintosh PowerMac corriendo sobre procesadores G3 o G4 PowerPC).
- IBM Mainframe (eServer zSeries y S/390).

Arquitecturas adicionales

- Alpha procesador (DEC_Alpha)
- SPARC

CAPÍTULO 3

3 DESARROLLO DE LA TECNOLOGÍA DE TRANSICIÓN

3.1 LEVANTAMIENTO DE INFORMACIÓN (SITUACIÓN ACTUAL)

La Universidad Técnica del Norte tiene a disposición el recurso desde CEDIA 2800:68:19::/48 en IPv6 y 190.95.216.x/26 IPv4, el cual llega a la red de la institución por medio de la infraestructura del proveedor de servicios Telconet. Esta empresa suministra un equipo para el borde de red de la UTN.

El equipo de borde de red dispone de una configuración de doble pila, es decir, funciona en ambos protocolos de internet (ipv4/ipv6); cabe resaltar que sobre este dispositivo de red no se tiene injerencia, pero si acceso directo como usuario.

Es por lo ya mencionado que existe otro equipo entre el borde de red y el dispositivo de administración y control de la red universitaria (ASA 5520), el switch cisco 3750 está configurado en doble pila y utiliza enrutamiento estático para permitir la conectividad entre ambos extremos de red.

(config)#ip route 190.95.196.x 255.255.x.x 190.95.196.x

3.1.1 Topología lógica de red de datos UTN

La Universidad técnica del Norte posee un cuarto de equipos ubicado en el edificio central de la institución, al cual está conectado cada una de las facultades y dependencias universitarias. (Figura 40)

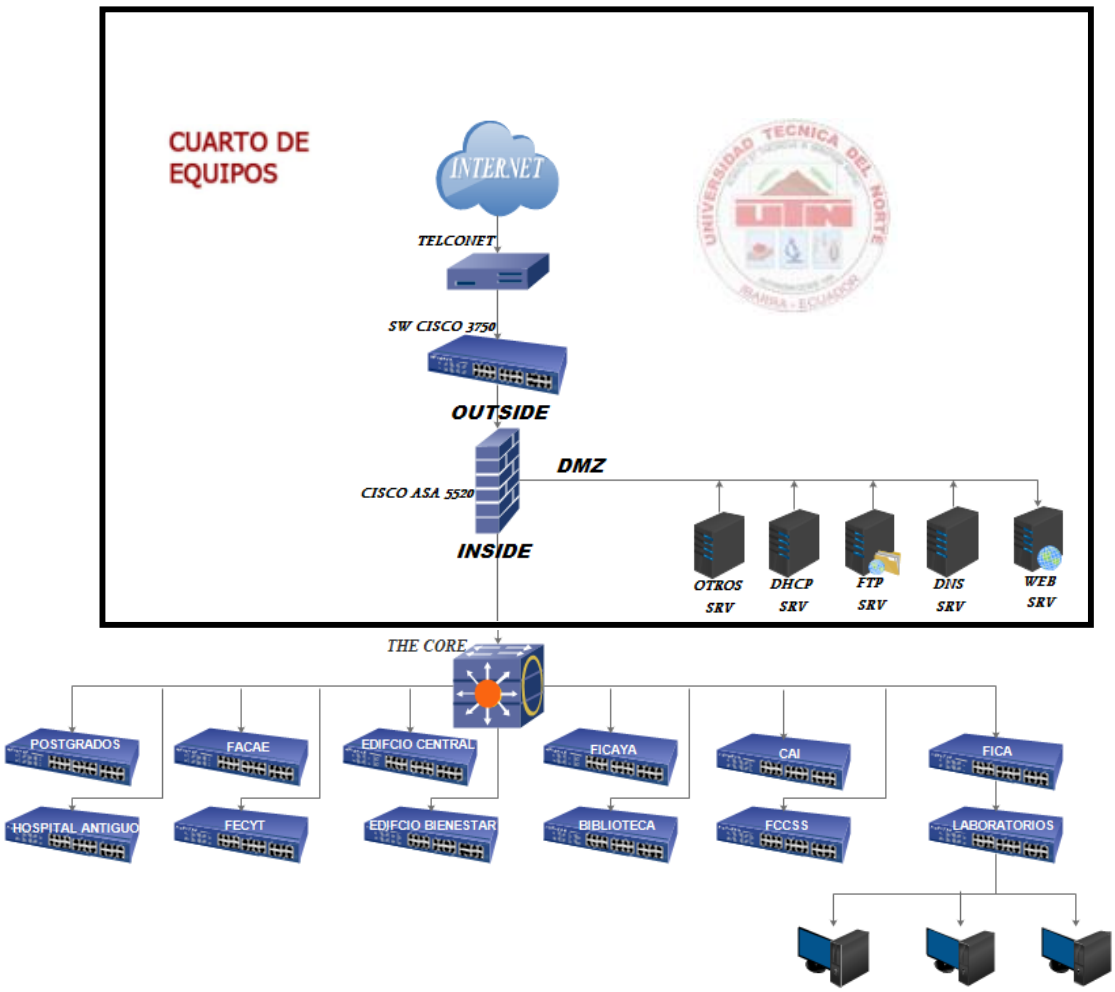


Figura 40. Topología de Red UTN

Fuente: Recuperado de Dirección de Desarrollo tecnológico e informático

3.1.2 Cuarto de Equipos

El cuarto de equipos principal en la Universidad Técnica de Norte se encuentra ubicado en el interior de la Dirección de Desarrollo tecnológico e informático, en cual se cuenta con:

- Cisco ASA 5520 Series
- Exinda 4761
- Nexus 5548
- Swicht The Core Catalys 4510R + E / 4500 +E Series
- Switch Cisco 4503 Series

- Cisco 3800 Series
- Switch Cisco 3750
- Cisco Media 7800
- Proliant BL460c G1
- Cisco Lan Controller
- Servidor Elastix
- Otros servidores

3.1.3 Características de Equipo Servidor

Hp Proliant BL460c G1 es el quipo servidor que albergara el servidor IPv6, teniendo en cuenta que también funcionan otro tipo de servicios en las diferentes cuchillas disponibles, este equipo tiene soporte para poder operar sobre Windows, Linux y NetWare. (Figura 41)

Figura 41. Servidor Blade Hp Proliant BL460c G1

Fuente: Recuperado de http://www.ebay.com/itm/HP-Proliant-C7000-Chassis-16x-BL460C-G1-Blade-Server-Barebone-/350891719510

Tabla 9. Información general de Servidor Blade Hp Proliant BL460c G1

Característica	Descripción
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
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.
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
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
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.
Soporte USB interno	Un (1) conector interno USB 2.0 para dispositivos clave de seguridad y llaves de unidad USB
Administración	Integrated Lights-Out 2 (iLO 2) Standard Hoja Edición (incluye KVM virtual y consola remota gráfica).

Fuente: Recuperado de http://www8.hp.com/h20195/v2/getpdf.aspx/c04110908.pdf?ver=7

3.1.4 Servicios WEB y FTP

La Universidad Técnica del Norte utiliza un portal web para brindar diferentes servicios a la comunidad, este está alojado en un servidor con sistema operativo Windows Server 2012 R2, el servidor no posee en encaminamiento nativo, y se encuentra ubicado en la zona desmilitarizada (DMZ).

El servidor es únicamente Web, no brinda ninguna otra aplicación para evitar saturaciones o carga innecesaria, además es muy similar con respecto a software libre en la forma de manejo de los componentes, ya que son independientes, es decir uno no depende de otro para su ejecución.

Los componentes que están instalados y configurados son: Apache, MySQL, PHP, WAF, Antivirus (proporcionado por el servidor de protección universitario), y solo tiene acceso a través de los puertos http y el puerto utilizado para la base de datos.

El gestor del portal Web es Wordpress, elegido por el administrador del mismo y justificado por el tipo de documentación existente en la comunidad y las herramientas de mantenimiento.

El direccionamiento utilizado es únicamente IPv4, aclarando que el sistema y servidor si soportan IPv6, pero los componentes con los que se encuentra el sistema operativo no soportan IPv6, con lo que parte la necesidad de actualizar el software utilizado para el levantamiento y funcionamiento del portal sobre IPv6.

Cada una de las herramientas para establecer el servidor web son desarrolladas con mayores prestaciones sobre Linux, por tal razón se decide utilizar este tipo de sistema operativo y dejar de usar Windows Server, así como también la escalabilidad de sistemas distribuidos y componentes independientes que son característicos de este tipo de sistemas.

El servidor FTP es un servicio adicional que se pretende brindar a la comunidad universitaria, por tal razón un equipo o servicio dedicado a esta actividad no existe en la institución y aún menos sobre IPv6.

3.1.5 Selección de mecanismo de transición para la UTN

La red de la Universidad Técnica de Norte trabaja localmente sobre una red basada en una infraestructura IPv4, con lo que se determina necesario empezar la transición de la misma al protocolo de internet con el cual se trabaja y será el que se utilice en la red de redes.

Teniendo en cuenta cual es la mejor opción para la implementación de IPv6 en la red de la UTN, se considera los mecanismos con los que la red no sea afectada drásticamente y cuando llegue el momento trabaje nativamente sobre IPv6. El uso de DS-lite, NAT64 y DN64 tienen la ventaja de que toda la red de acceso trabaja utilizando únicamente IPv6, siendo los mecanismos a elegir para la transición de IPv4 a IPv6 en la red universitaria.

3.2 INSTALACIÓN DEL SERVIDOR

3.2.1 Instalación de Centos 6.5

La instalación de Centos 6.5 se puede realizar a través de una unidad de disco, USB booteable o por medio de la red, al disponer al menos una de las tres opciones con el sistema operativo se puede dar inicio a la instalación, con la finalidad de tener una plataforma en donde levantar los servicios Web, FTP y los Mecanismos de NAT64/DNS64.

Entre los requisitos de instalación se necesita el DVD de Centos o el ISO del sistema operativo el cual tiene el nombre de Centos-6.5-x86-64-binDVD1.iso, la descarga está disponible en el siguiente enlace:

https://mega.nz/#!CsAFnQzb!d8CiYxvbVhPvGTDh0bg_-jNJ1Th5phiH3l9lpcza-5c

Para seguir paso a paso el proceso de instalación de Linux Centos 6.5 revisar Anexo 1.

El equipo servidor cumple con las características que requiere Centos 6.5 para ser instalado como se revisó anteriormente (página 74,75) ya que tiene un procesador Quad-Core Intel® Xeon de 1,83 GHz, Memoria RAM de 16GB y un almacenamiento de 250 GB.

3.2.2 Configuración de red IPv4/IPv6

Para realizar la configuración utilizando IPv4/IPv6 ingresamos a un terminal.

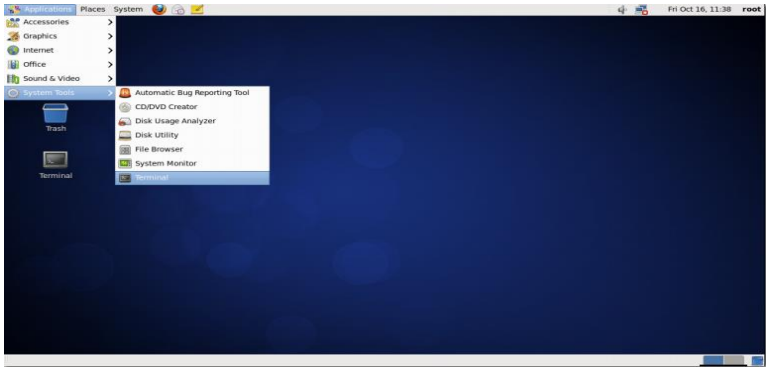


Figura 42. Ingreso a terminal/consola

Fuente: Linux Centos 6.5

Para configurar la interface de red ingresamos al fichero siguiente:

#nano /etc/sysconfig/network-scripts/ifcfg-eth0

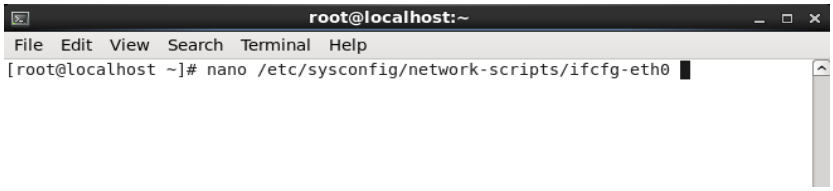


Figura 43.Comando de edición de interfaz de red

Fuente: Consola Linux Centos 6.5

El contenido de la interfaz de red está configurado de la siguiente manera, tanto con IPv4 como con IPv6, no es necesario que IPv4 este configurado, en este caso se hace debido al tipo de servicios que se brinda.

Es importante saber que el orden en que se escribe las direcciones de nombres DNS en el servidor, determinan la prioridad del protocolo de internet (IPv4/IPv6), *DNS1* establece el DNS primario y *DNS2* el secundario o alternativo.

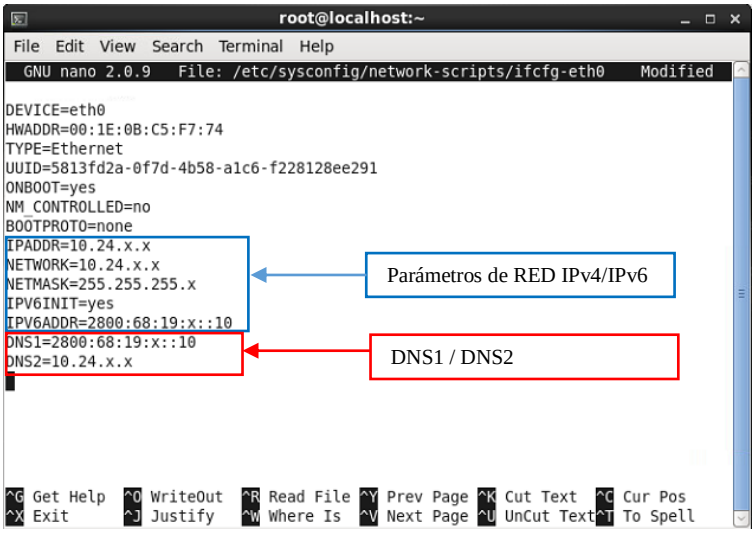


Figura 44. Configuración interfaz de red

Fuente: Archivo de configuracion network-scripts Linux Centos 6.5

Para habilitar el protocolo en la red y evitar que la dirección IPv6 sea asignada por RA se debe modificar el fichero */etc/sysconfig/network*,

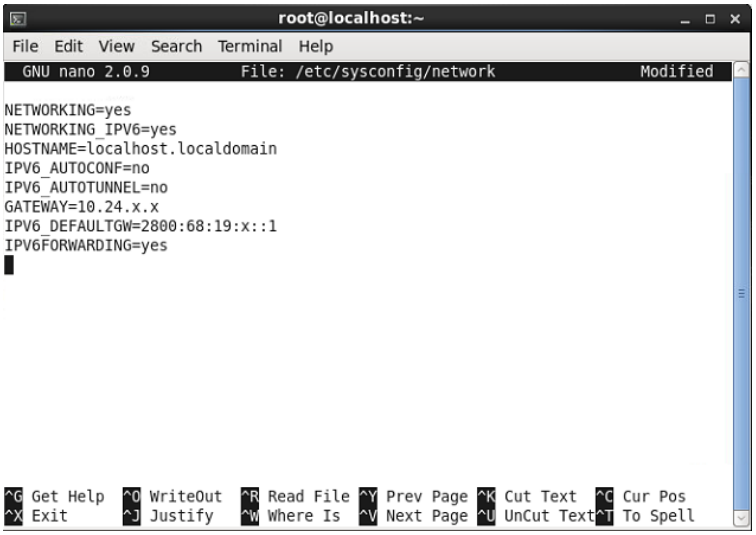


Figura 45. Habilitación de IPv6

Fuente: Archivo de configuracion network Linux Centos 6.5

Guardar la configuración, cerrar del editor y luego se debe de reiniciar el servicio.

#service network restart

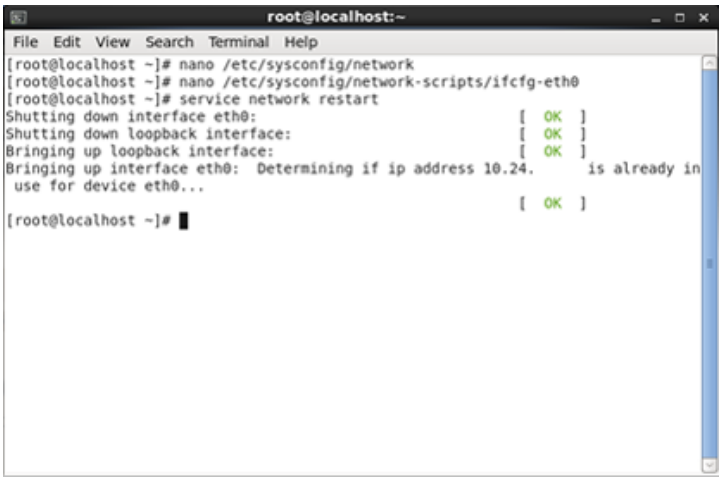


Figura 46. Reinicio de interfaz

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Para comprobar que la configuración si está funcionando se puede realizar una visualización de los parámetros de red y ping6 a la interfaz.

#ifconfig eth0 && ping6 2800:68:19:x::10

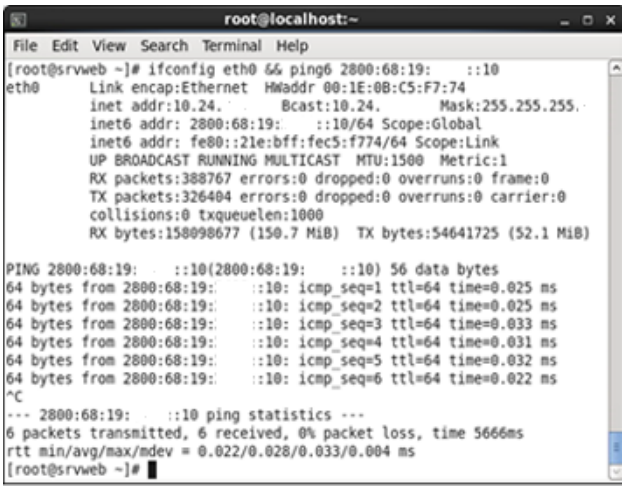


Figura 47. Comprobación de configuración de Interfaz

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

3.3 DISEÑO Y CONFIGURACIÓN DE SERVICIOS

Para empezar con el levantamiento de cada uno de los servicios se debe actualizar los repositorios del sistema, por lo que es necesario tener acceso a internet o un servidor que nos permite realizar este proceso, para ello ejecutamos el siguiente comando.

#yum update

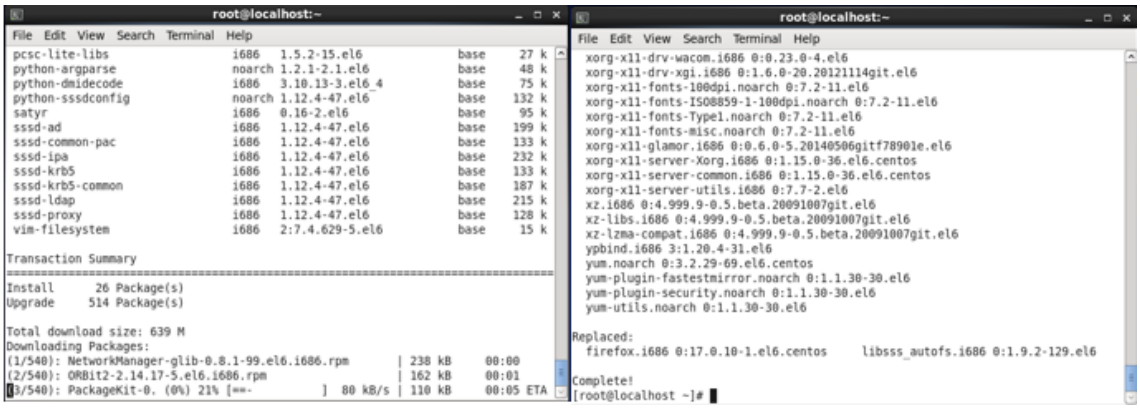


Figura 48. Actualización de repositorios paquetes de aplicaciones

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

3.3.1 Enrutamiento y Direccionamiento IPv6

La red de la UTN se encuentra segmentada por VLANs, cada una de las subredes en IPv4 está identificada con una descripción de acuerdo a la dependencia que pertenece en la institución, con esto el direccionamiento en IPv6 es acorde a la distribución existente.

Esta información es confidencial y solo la debe conocer el administrador de red de la casona universitaria, por tanto, la tabla de distribución de sub redes (vlan) IPv6 no revela la información real, pero si demuestra un correcto direccionamiento en el protocolo de internet versión 6. (tabla 10)

Tabla 10. Direccionamiento VLANs UTN IPv6

DISTRIBUCIÓN DE SUBREDES (VLANS) IPv6					
N°	DESCRIPCIÓN	VLAN	DIRECCIÓN IP	Prefijo	GATEWAY
1	EQUIPOS-ACTIVOS	1	2800:68:19:x:x::	/xx	2800:68:19:x:x::1
2	DMZ	2	2800:68:19:x::	/xx	2800:68:19:x::1
3	EQUIPOS-ACTIVOS-WIRELESS	3	2800:68:19:x:2::	/xx	2800:68:19:x:2::1
4	CCTV	4	2800:68:19:x:3::	/xx	2800:68:19:x:3::1
5	RELOJES-BIOMETRICOS	5	2800:68:19:x:4::	/xx	2800:68:19:x:4::1
6	TELEFONIA-IP-ELASTIX	6	2800:68:19:x:5::	/xx	2800:68:19:x:5::1
7	TELEFONIA-IP-CISCO	7	2800:68:19:x:6::	/xx	2800:68:19:x:6::1
8	AUTORIDADES	8	2800:68:19:x:7::	/xx	2800:68:19:x:7::1
9	DDTI	9	2800:68:19:x:8::	/xx	2800:68:19:x:8::1
10	FINANCIERO	10	2800:68:19:x:9::	/xx	2800:68:19:x:9::1
11	COMUNICACION-ORGANIZACIONAL	11	2800:68:19:x:10::	/xx	2800:68:19:x:10::1
12	ADMINISTRATIVOS	12	2800:68:19:x:11::	/xx	2800:68:19:x:11::1
13	ADQUISICIONES	13	2800:68:19:x:12::	/xx	2800:68:19:x:12::1
14	U-EMPRENDE	14	2800:68:19:x:13::	/xx	2800:68:19:x:13::1
15	AGUSTIN-CUEVA	15	2800:68:19:x:14::	/xx	2800:68:19:x:14::1
16	BIENESTAR-DOCENTES	16	2800:68:19:x:15::	/xx	2800:68:19:x:15::1
17	BIENESTAR-ADMINISTRATIVOS	17	2800:68:19:x:16::	/xx	2800:68:19:x:16::1
18	PROYECTO-INDIA	18	2800:68:19:x:17::	/xx	2800:68:19:x:17::1
19	NATIVA	19	-----	----	-----
20	FICA-LABORATORIOS	20	2800:68:19:x:18::	/xx	2800:68:19:x:18::1
21	FICA-WIRELESS	21	2800:68:19:x:19::	/xx	2800:68:19:x:19::1
22	FICA-ADMINISTRATIVOS	22	2800:68:19:x:20::	/xx	2800:68:19:x:20::1
23	FICAYA-LABORATORIOS	23	2800:68:19:x:21::	/xx	2800:68:19:x:21::1
24	FICAYA-ADMINISTRATIVOS	24	2800:68:19:x:22::	/xx	2800:68:19:x:22::1
25	FECYT-LABORATORIOS	25	2800:68:19:x:23::	/xx	2800:68:19:x:23::1
26	FECYT-ADMINISTRATIVOS	26	2800:68:19:x:24::	/xx	2800:68:19:x:24::1
27	FACAE-LABORATORIOS	27	2800:68:19:x:25::	/xx	2800:68:19:x:25::1
28	FACAE-ADMINISTRATIVOS	28	2800:68:19:x:26::	/xx	2800:68:19:x:26::1
29	FCCSS-LABORATORIOS	29	2800:68:19:x:27::	/xx	2800:68:19:x:27::1
30	FCCSS-ADMINISTRATIVOS	30	2800:68:19:x:28::	/xx	2800:68:19:x:28::1
31	POSTGRADO-LABORATORIOS	31	2800:68:19:x:29::	/xx	2800:68:19:x:29::1
32	POSTGRADO-ADMINISTRATIVOS	32	2800:68:19:x:30::	/xx	2800:68:19:x:30::1
33	CAI-LABORATORIOS	33	2800:68:19:x:31::	/xx	2800:68:19:x:31::1
34	CAI-ADMINISTRATIVOS	34	2800:68:19:x:32::	/xx	2800:68:19:x:32::1
35	BIBLIOTECA-LABORATORIOS	35	2800:68:19:x:33::	/xx	2800:68:19:x:33::1
36	BIBLIOTECA-ADMINISTRATIVOS	36	2800:68:19:x:34::	/xx	2800:68:19:x:34::1
37	COLEGIO-LABORATORIOS	37	2800:68:19:x:35::	/xx	2800:68:19:x:35::1
38	COLEGIO-ADMINISTRATIVOS	38	2800:68:19:x:36::	/xx	2800:68:19:x:36::1
39	WIRELESS-DOCENTES	39	2800:68:19:x:37::	/xx	2800:68:19:x:37::1
40	WIRELESS-ADMINISTRATIVOS	40	2800:68:19:x:38::	/xx	2800:68:19:x:38::1
41	EDUROAM	41	2800:68:19:x:39::	/xx	2800:68:19:x:39::1
42	WIRELESS-EVENTOS1	42	2800:68:19:x:40::	/xx	2800:68:19:x:40::1

43	WIRELESS-EVENTOS2	43	2800:68:19:x:41::	/xx	2800:68:19:x:41::1
44	WIRELESS-ESTUDIANTES	44	2800:68:19:x:42::	/xx	2800:68:19:x:42::1
45	COPIADORA	45	2800:68:19:x:43::	/xx	2800:68:19:x:43::1
46	BANCO-PACIFICO	46	2800:68:19:x:44::	/xx	2800:68:19:x:44::1

Fuente: Dirección de Desarrollo tecnológico e informático

3.3.2 Levantamiento de servicio DHCP en IPv6

Primero se instala el paquete que nos permitirá configurar el servicio de direccionamiento dinámico.

#yum install dhcp

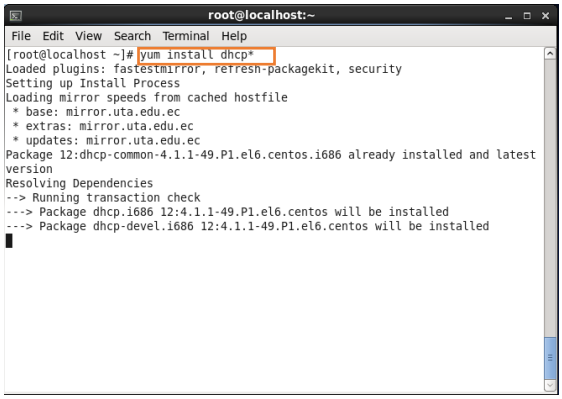


Figura 49. Instalación Paquete dhcp

Fuente: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

Colocamos Y para continuar con la Instalación

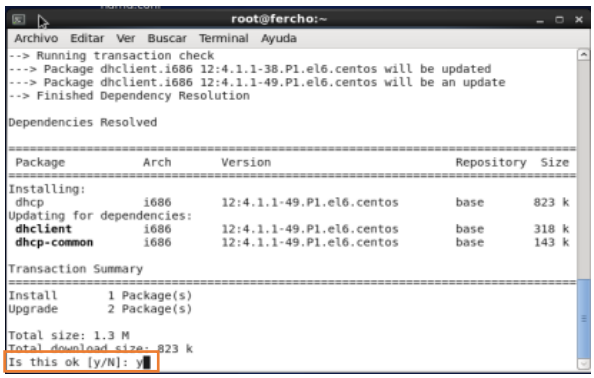


Figura 50. Aceptar instalación del paquete dhcp

Fuente: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

Una vez finalizada la instalación se precede a configurar los ficheros necesarios, en el archivo dhcpd.conf se encuentra la configuración para IPv4 pero para que coexistan los dos ficheros se debe crear en la misma ubicación un fichero llamado dhcpd6.conf

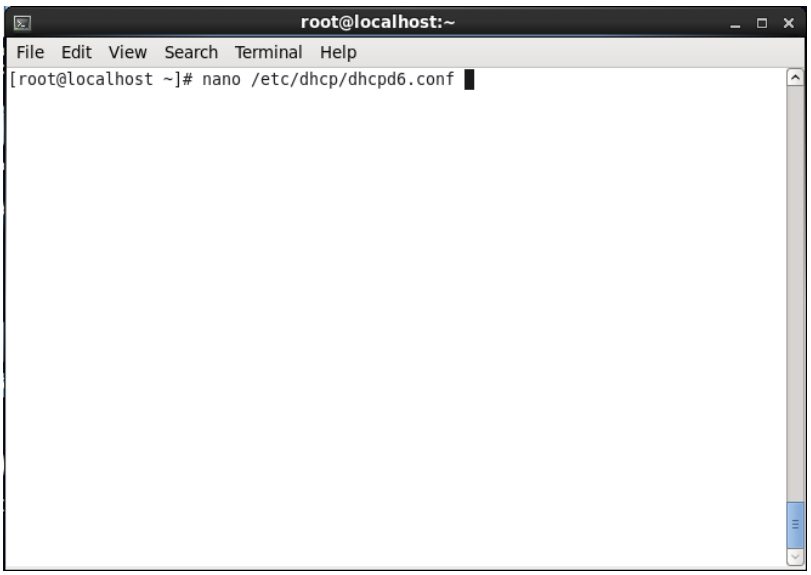


Figura 51. Comando para edición de fichero dhcpd6.conf

Fuente: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

El contenido del fichero dhcpd6.conf con los parámetros de la red asignada queda de la siguiente manera.

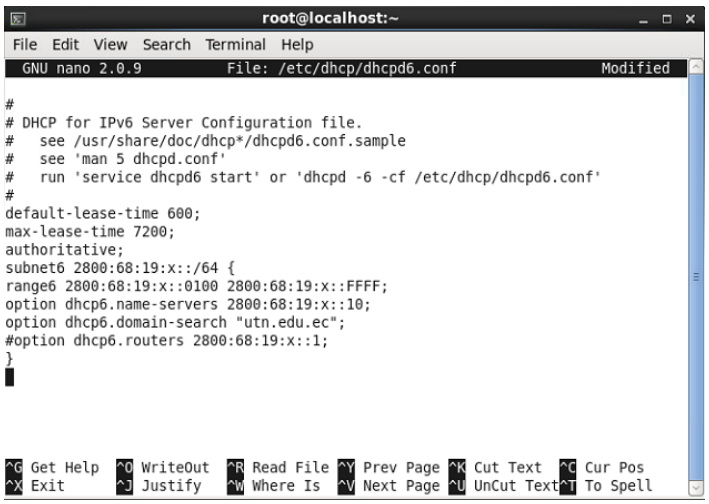


Figura 52. Fichero dhcpd6.conf

Fuente: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

Luego de configurar con los parámetros de red con los que se quiere asignar direcciones IPv6 a los dispositivos asociados a la red se debe reiniciar el servicio.

#service dhcpd6 restart

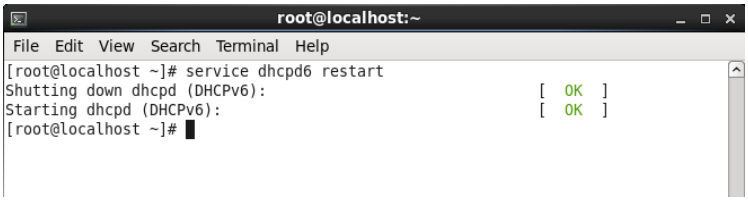


Figura 53. Reinicio de servicio dhcpd6

Fuente: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

Luego de hacer la configuracion del fichero dhcpd6.conf se debe crear un archivo donde guarde los registros de las direcciones que se esten asignando, este archovo se debe crear en el directrio /var/run con el nombre de dhcpd6.leases al cual se debe de dar los permisos necesarios para que pueda ser modificado.

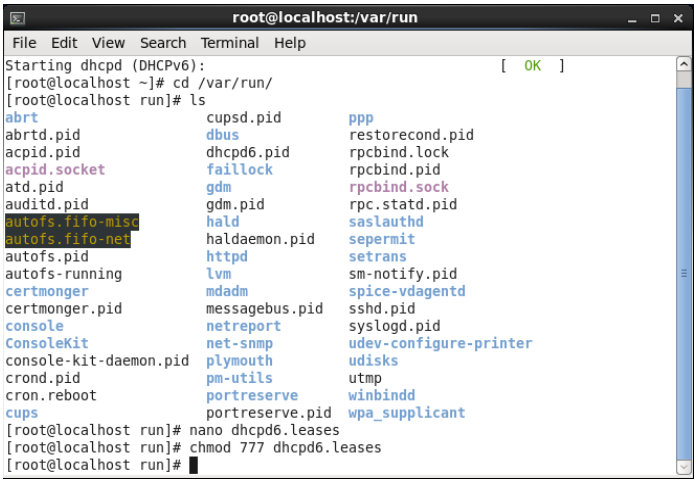


Figura 54. Creación de fichero de almacenamiento de direcciones

Fuete: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

Ahora lo que resta es iniciar el servicio y especificar el archivo de configuración y porque interfaz se escuchara las peticiones, esto se realiza mediante el comando:

 # /usr/sbin/dhcpd -6 -cf /etc/dhcp/dhcpd6.conf eth0

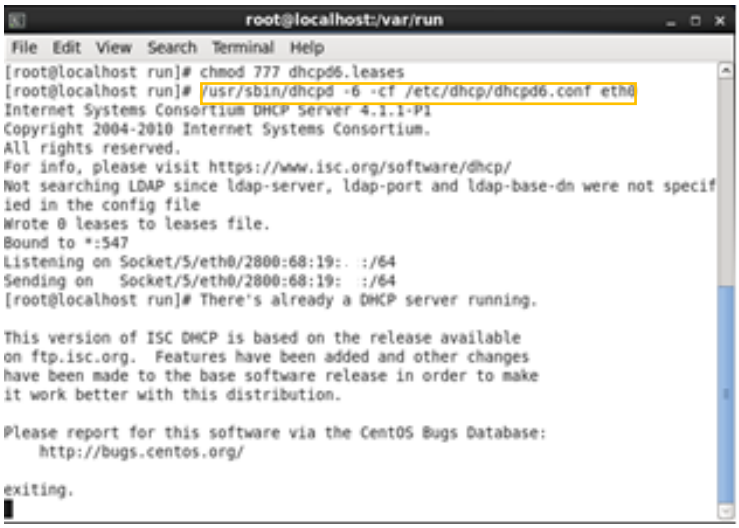


Figura 55. Iniciar el servicio dhcp en IPv6

Fuente: https://www.isc.org/wp-content/uploads/2014/08/DHCP-4.3.1-Distribution-Documentation-Aug-4-14.pdf

3.3.3 Levantamiento de servidor WEB

Para el levantamiento del servidor WEB se deben de instalar tanto el paquete de httpd como el de apache, los cuales permiten la configuración y direccionamiento del servidor.

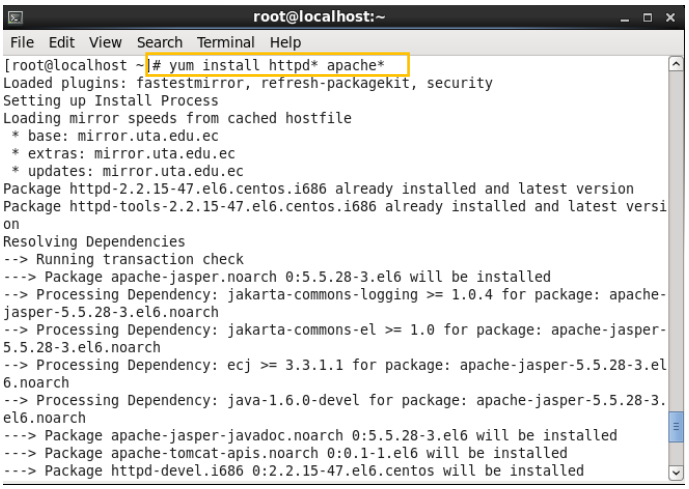


Figura 56. Instalación de httpd y Apache

Fuente: Paquete de instalacion servidor web Linux Centos 6.5

Con la instalación de estos paquetes el servidor web por defecto está activo, se debe de modificar el archivo welcome.conf como se indica en la siguiente figura:

#nano /etc/httpd/conf.d/welcome.conf

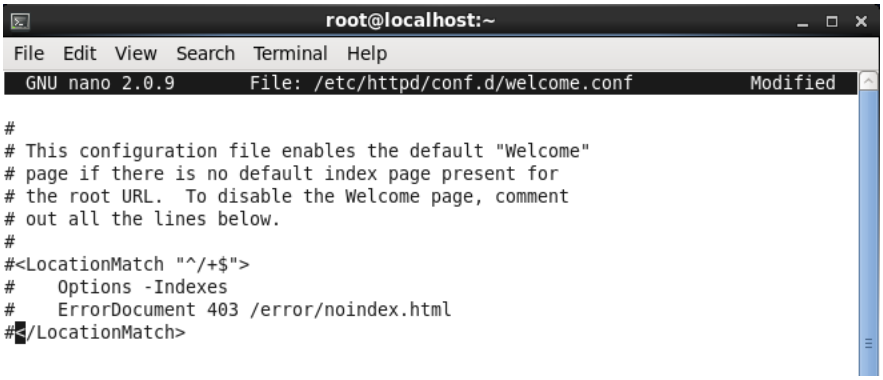


Figura 57. Archivo welcome.conf

Fuente: Archivo de configuracion welcome.conf Linux Centos

Luego crear el index.html o index.php, en si el archivo que contenga la estructura del sitio web.

#nano /var/www/html/index.html

Figura 58. Ejemplo de un index.html

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

Se reinicia el servicio y se realiza la prueba de funcionamiento mediante el ingreso al navegador y apuntando a la dirección local.

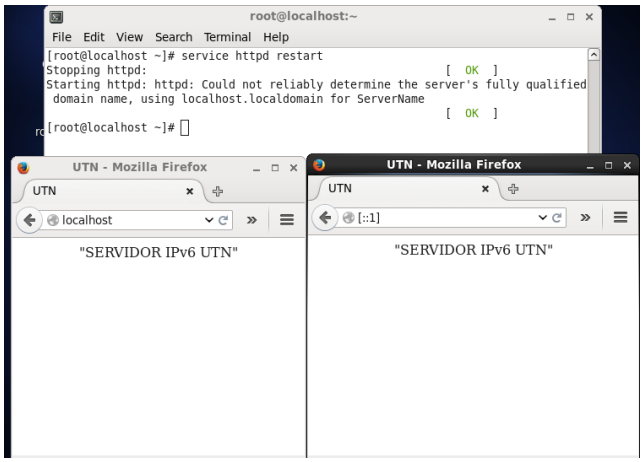


Figura 59. Prueba de funcionamiento servidor Web

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

3.3.3.1 Direccionamiento de servidor WEB en IPv6

El direccionamiento del servidor Web se realiza mediante la modificación del archivo httpd.conf, donde se especifica a que dirección se quiere asignar al portal Web.

#nano /etc/httpd/conf/httpd.conf

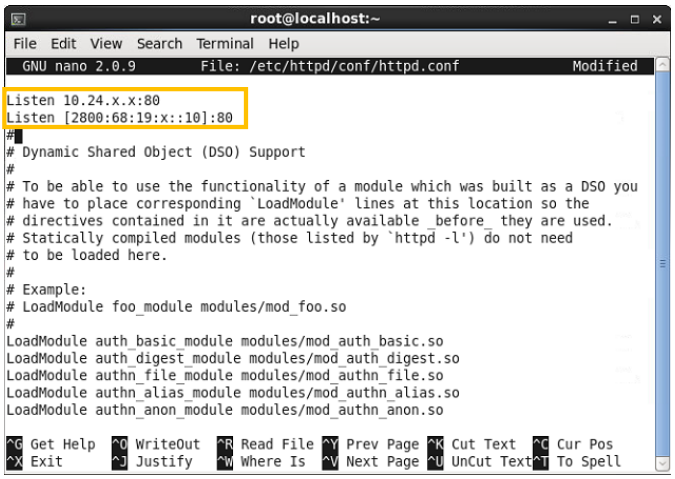


Figura 60. Direccionamiento IPv6 de servidor Web

Fuente: Archivo de configuracion Web Server - Linux Centos

Se debe salir del editor y se procede a reiniciar el servicio

#service httpd restart

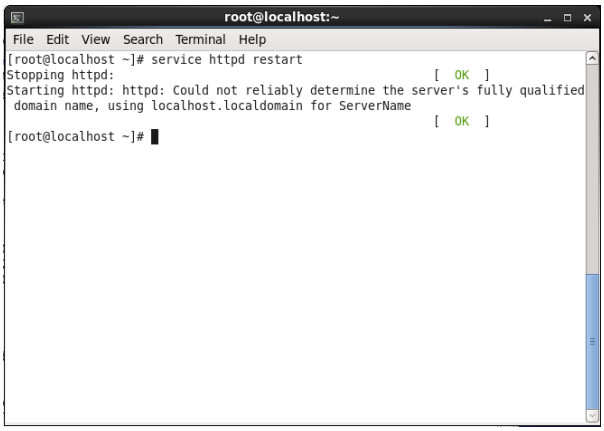


Figura 61. Reinicio de servicio httpd

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

Para verificar si está trabajando correctamente bajo el puerto 80 y el direccionamiento asignado se ejecuta el comando:

#netstat -tulpn | grep :80

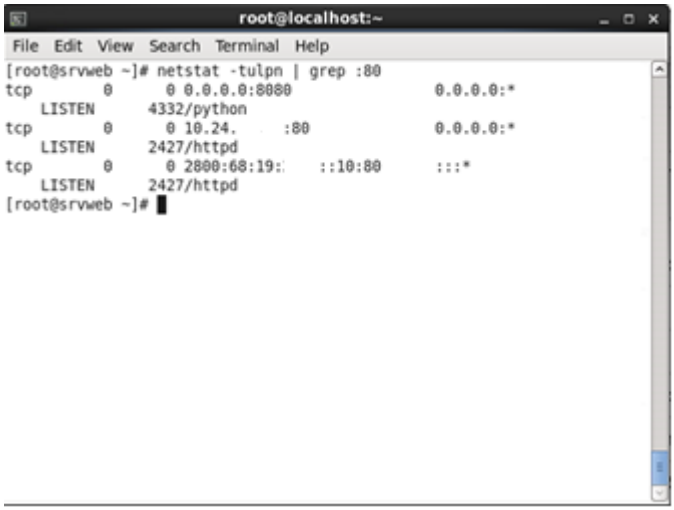


Figura 62. Verificación de puerto escuchado

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

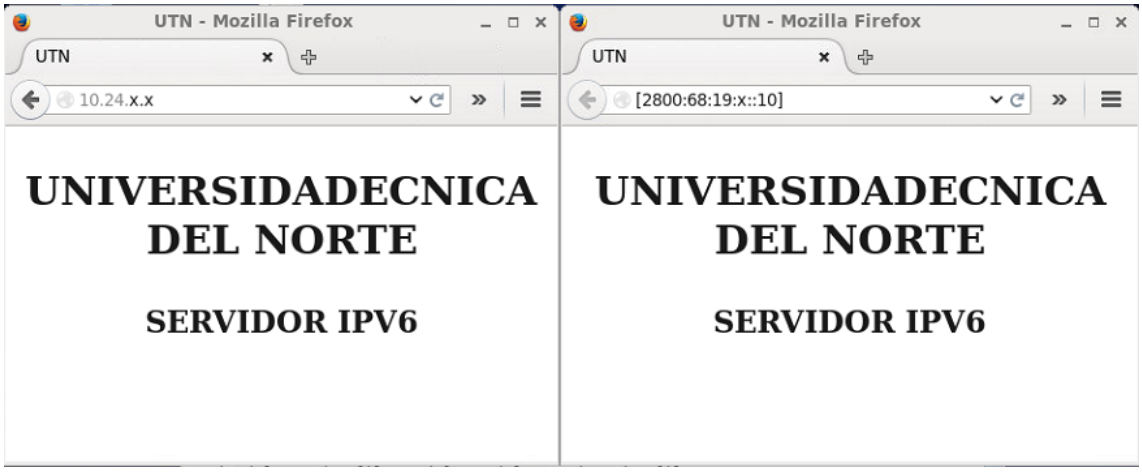


Figura 63. Prueba de funcionamiento por IP de servidor Web

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

3.3.3.2 Portal web Universidad Técnica del Norte

Entre los componentes necesarios para realizar la migración del portal universitario a Linux es muy importante la base de datos (MySQL) y otros servicios que se usa para interconectar la base de datos de un portal web, se utiliza PHP el cual tiene una gran variedad de componentes, pero solo se instala los necesarios para este proyecto.

En el Anexo 2 se puede revisar la instalación de MySQL, MySQL-Workbench (gestor de base de datos) y la especificación de los paquetes de PHP a utilizarse, como también la configuración necesaria para el funcionamiento de estos componentes de forma individual, para garantizar la escalabilidad de software utilizado en la implementación del portal universitario.

3.3.3.3 Seguridad a nivel de software WAF (APACHE)

WAF es una herramienta de protección a nivel de desarrollador de aplicación, pero cabe resaltar que no remplaza a los firewall o medidas de seguridad en la capa de red, este tipo de seguridad puede ser hardware o software, y analiza el trafico web entre el servidor y la red que realiza las peticiones, la intención es proteger al servidor de ataques como

SQL Injection, cross Site scripting, entre otros. WAF no se encarga de enrutar trafico ni tampoco realizar NAT, en si funciona haciendo dos peticiones, una que realiza el cliente al WAF y otra que hace el WAF al servidor web.

Mod_segurity es el plugin WAF que utiliza apache para brindar seguridad de este tipo, para su instalación se la puede realizar de dos maneras sobre Centos, utilizando el comando *yum install mod_ssl* o bien en la instalación completa de los componentes del servidor web al ejecutar *yum groupinstall "Web server",* como ya se instaló usando la segunda opción podemos verificar que el modulo se encuentre instalado, debe estar en el directorio /etc/httpd/modules, como se muestra en la figura 65.

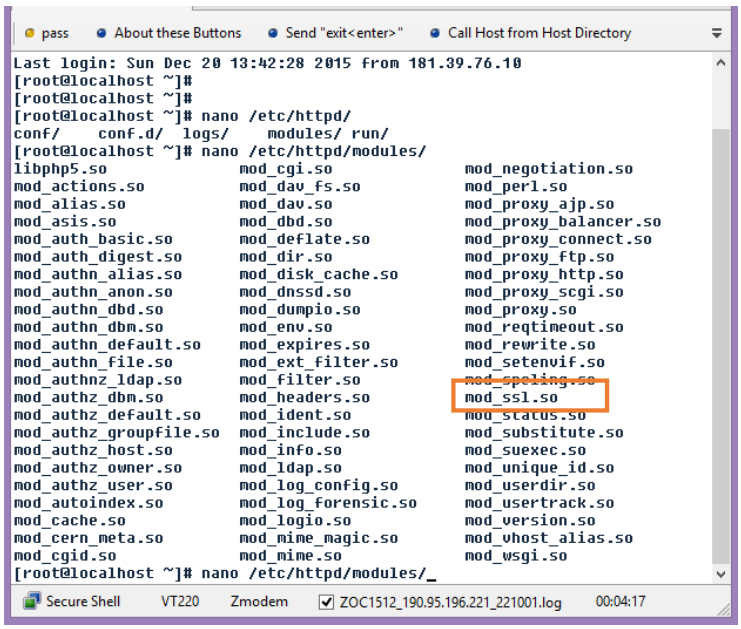


Figura 64. Modulo ssl de apache

Fuente: Contenido de directorio Web Server - Linux Centos

La configuración de Mod_segurity al instalar se encuentra en un fichero individual, el cual se debe editar para realizar el encaminamiento del portal web y que cumpla con la tarea de protección al servidor. Digitando el comando nano /etc/httpd/conf.d/ssl.conf

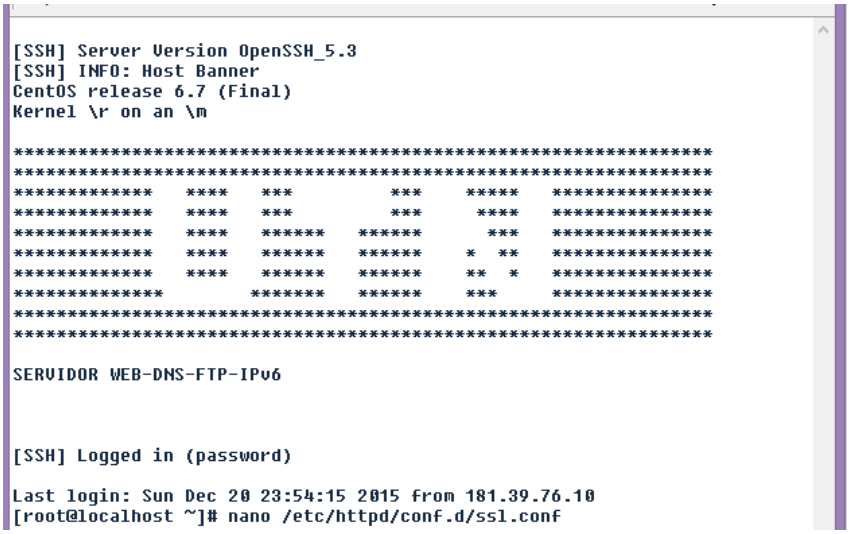


Figura 65. Fichero configuración ssl

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

En el fichero de configuración se agrega las direcciones IP del servidor web, lugar donde se encuentra almacenado el portal y el nombre de dominio del servidor.

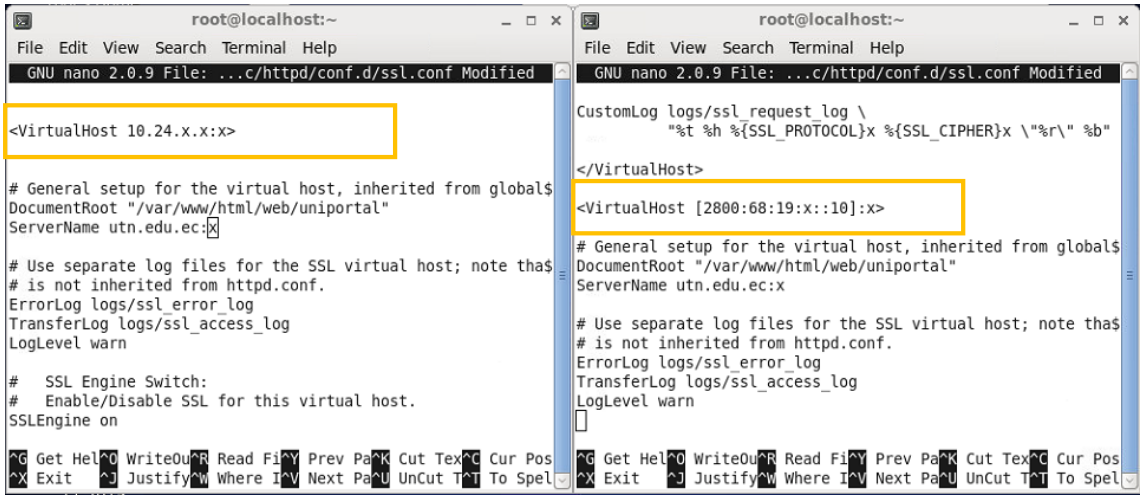


Figura 66. Configuración ssl servidor web

Fuente: Archivo de configuracion modulo ssl Linux Centos

3.3.4 Levantamiento de servidor FTP

Un servidor FTP en Centos Linux tiene varias formas de configuración, y para empezar se debe instalar uno de los paquetes disponibles para poder implementar la aplicación. Se instalará vsftpd con el siguiente comando:

#yum install vsftpd

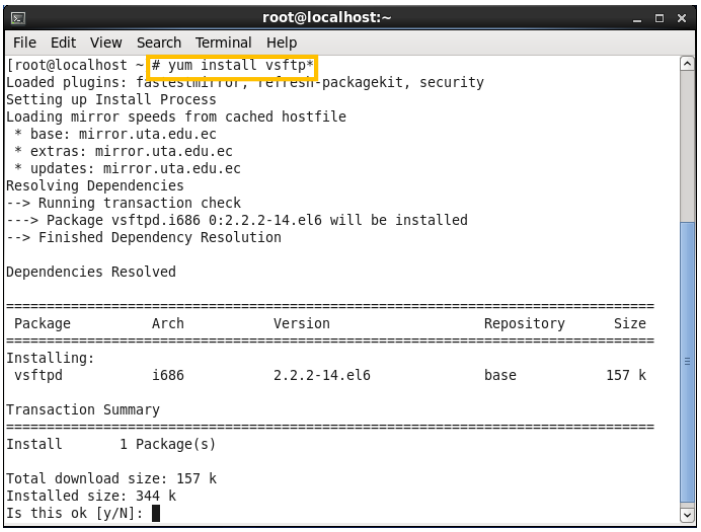


Figura 67. Instalación servidor FTP

Fuente: Paquete de servidor de transferencia de archivos Linux Centos

Inicialización del servicio ftp se hace mediante el comando

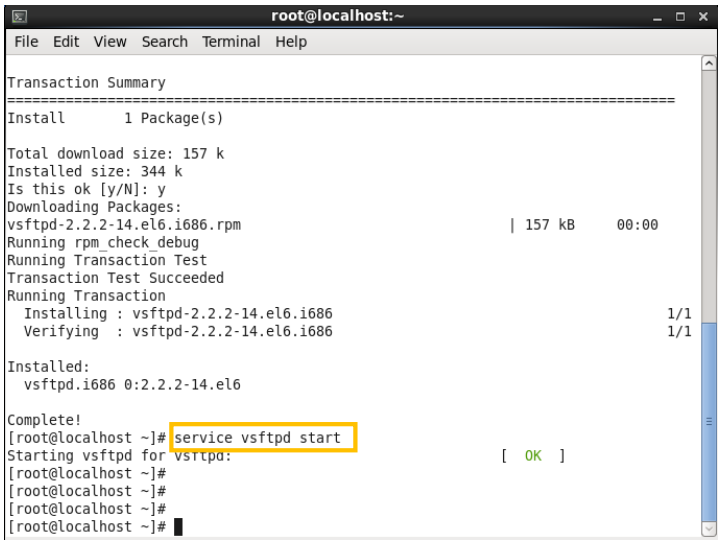


Figura 68. Inicio de servicio Ftp

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

Para el correcto funcionamiento del servicio se debe deshabilitar la línea de Selinux que se encuentra ubicada en el archivo */etc/selinux/config.*

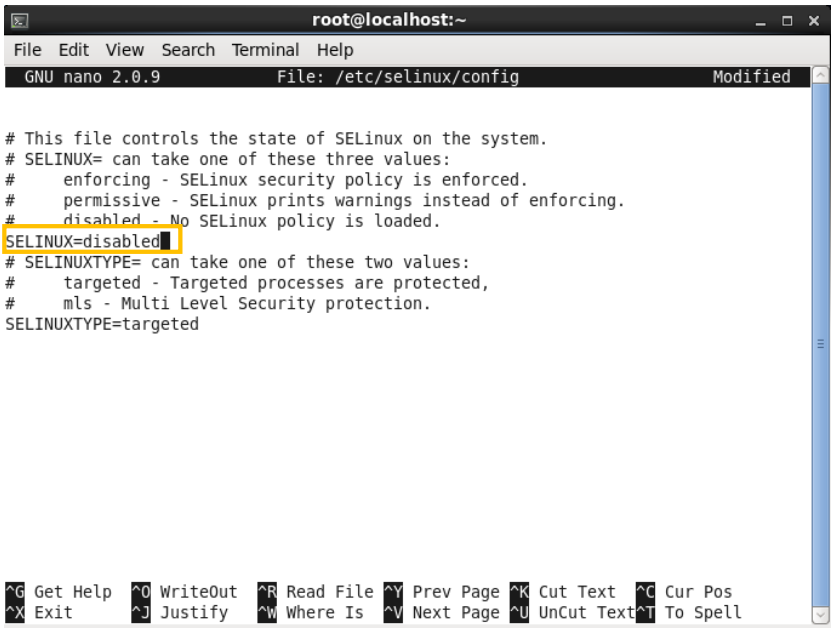


Figura 69. Archivo de configuracion Selinux

Fuente: Archivo de configuracion Selinux - Linux Centos

Para que las configuraciones tengan efecto se reinicia el servicio como también se puede revisar el puerto por el que está trabajando el servicio de Ftp.

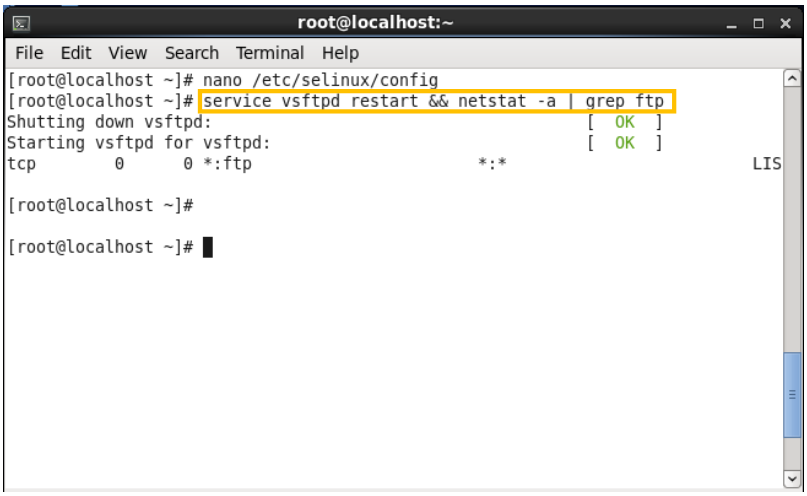


Figura 70. Reinicio y chequeo de puerto Ftp

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

Para verificar que el servicio está funcionando se puede ingresar al navegador y escribir ftp://localhost

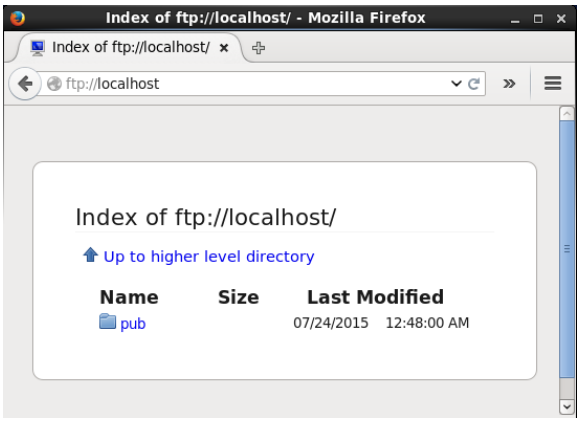


Figura 71. Acceso por ftp

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

3.3.4.1 Direccionamiento de servidor FTP en IPv6

VSFTPD es un paquete que brinda la configuración del servicio de manera muy práctica, donde hay que modificar las siguientes líneas:

- ✓ anonymous_enable=NO
- ✓ Borrar o comentar listen=YES
- ✓ ftpd_banne= “Mensaje a la entrada al servidor”
- ✓ anon_root=/var/ftp/pub
- ✓ listen_ipv6=Yes

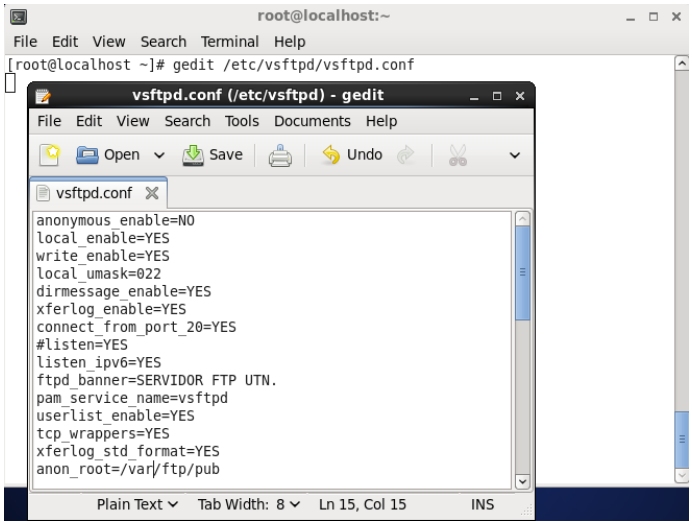


Figura 72. Configuración de archivo vsftpd.conf

Fuente: Archivo de configuracion vsftpd Linux Centos

Hay que tener en cuenta de que VSFTPD únicamente trabaja con un protocolo de internet a la vez no con ambos, listen_ipv6=Yes indica cual va a ser el protocolo con el cual funcionara el servidor Ftp, en esta línea se direcciona el servidor a que utilice la dirección IPv6 configurada en el servidor para escuchar las peticiones de quienes quieran acceder al servicio.

Para que los cambios tengan efecto y sean ejecutados se debe guardar y luego reiniciar el servicio.

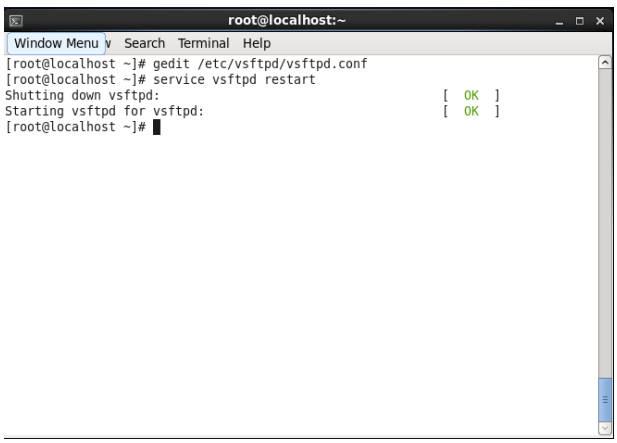


Figura 73. Reinicio de servidor vsftpd.conf

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

3.3.4.2 Asignación de dependencias universitarias

Para asignar un espacio en cual usuarios pertenecientes o asociados a la Universidad Técnica del Norte, el cual puede ser utilizado a gusto personal, se debe asignar un identificador y protegerlo con una contraseña. La creación de usuarios y asignación de contraseña se realiza mediante el comando adduser y passwd, como se mira en la figura.

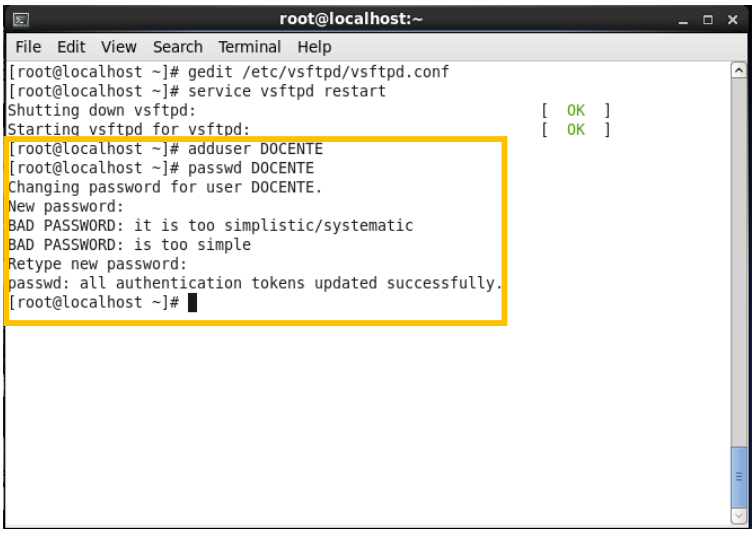


Figura 74. Creación de usuarios y asignación de contraseña

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

Uno de los métodos que se puede utilizar para acceder a la dependencia asignada es usando el navegador web o usando un programa cliente FTP. Los parámetros a ingresar son la dirección del servidor ftp, usuario y contraseña existentes en el servidor.

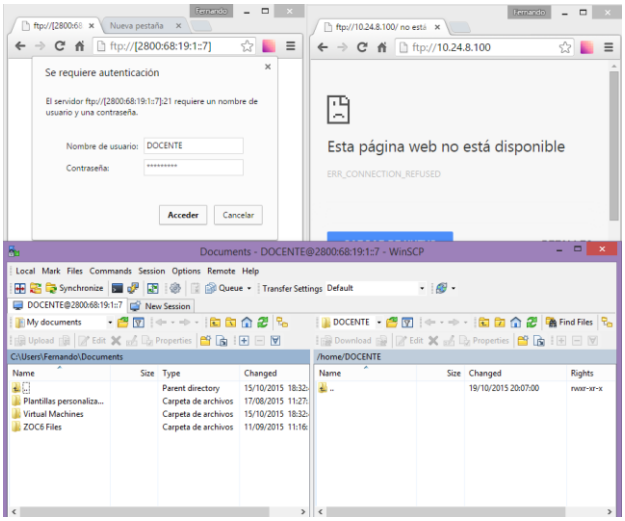


Figura 75. Acceso a servidor FTP

Fuente: Elaborado por el Autor, Curso avanzado Linux IECEIT

3.3.5 Configuración DNS64

Para la implementación del servidor de nombres de dominio sobre Centos se recurrirá a una herramienta que es muy utilizada porque es una solución robusta y estable, siendo así se procede a instalar BIND (Berkeley Internet Name Domain) mediante el siguiente comando:

#yum –y install bind

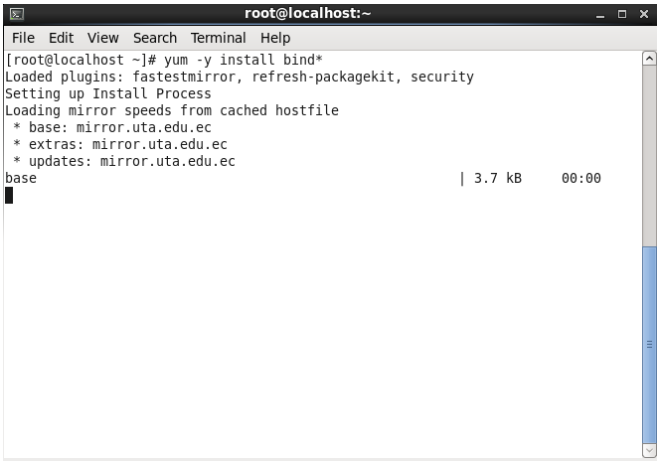


Figura 76. Instalación de Bind

Fuente: Paquete de servidor de nombres de dominio Linux Centos

3.3.5.1 Configuración de fichero principal DNS

Para empezar a configurar el DNS64 primero se edita el fichero con *nano /etc/named.conf*, este archivo contiene los parámetros por los cuales el servidor se va a regir. Teniendo en cuenta que el puerto que usa un servidor de este tipo es el 53 se edita las direcciones por las cuales va a escuchar las peticiones, mismas que después serán traducidas y encaminadas a la aplicación destino.

El primer paso es el direccionamiento del puerto, estas líneas de código se encuentran en el campo de options, y se agrega las direcciones que el servidor tendrá, tanto IPv4 como IPv6 en el lugar asignado respectivamente, así como también se asignan los renviadores (Forwarders) del proveedor de internet, mismos que se encargan de reenviar las consultas a los servidores DNS externos.

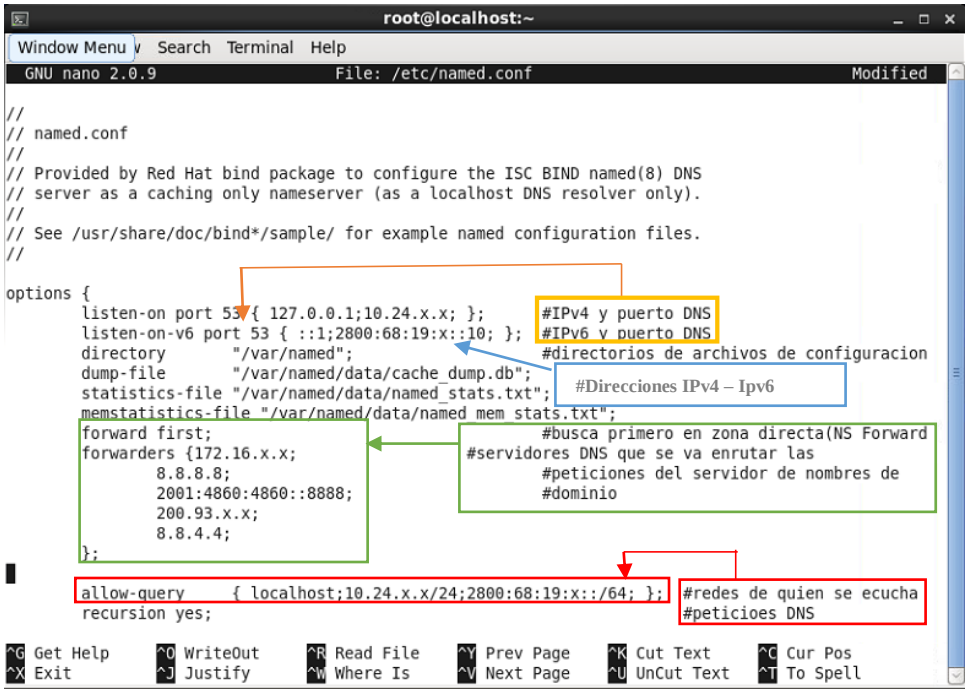


Figura 77. Direccionamiento servidor DNS64

Fuente: http://rdns6.com/zone

El siguiente paso a seguir es la creación de las zonas donde se encuentran los registros a los cuales se va a traducir, es decir, se crea una zona de reenvió por cada dominio que se tenga autoridad y una zona inversa por cada red que también se tenga un control total, estas zonas se crean con el fin de resolver el dominio.

3.3.5.2 Definición de Zona directa DNS64

En el fichero /etc/named.conf se define el nombre de la zona directa y el archivo que contendrá la información de la misma, además del tipo, es decir si es primario (master) o secundario (slave).

Si es primario quiere decir que puede recibir la transferencia de las zonas de otros servidores DNS, un DNS secundario se utiliza para tener más direcciones de un dominio.

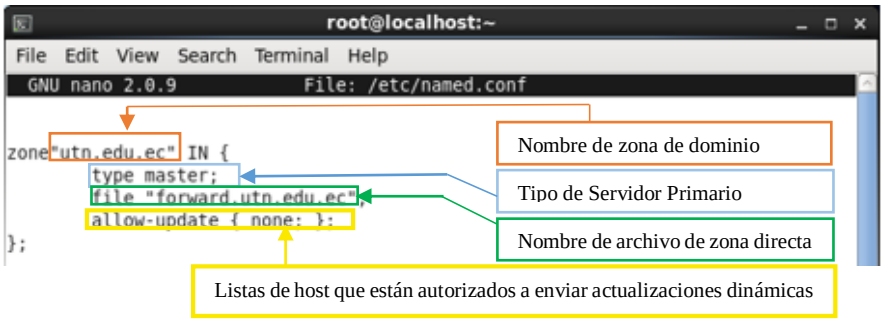


Figura 78. Zona directa en named.conf

Fuente: http://rdns6.com/zone

Después de haber definido la zona se guarda el archivo y se cierra el fichero de zonas, el siguiente paso es crear dicha zona, debe de estar en el directorio de archivos de configuración y con el nombre que se han especificado para que el funcionamiento sea el correcto. Para el cálculo de los parámetros de zona revisar Anexo 3.

La zona directa tiene el siguiente contenido y se crea utilizando el siguiente comando: *nano /var/named/forwad.utn.edu.ec*

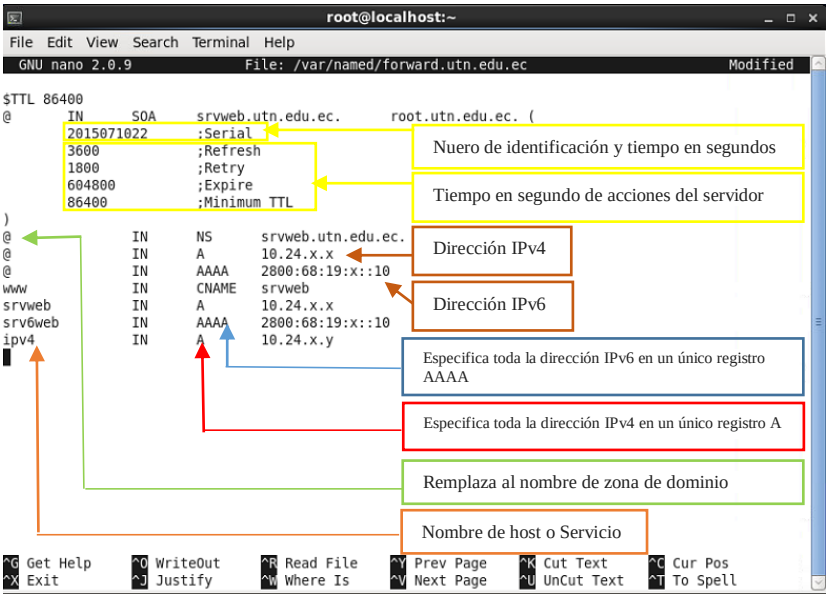


Figura 79. Zona directa DNS64

Fuente: http://rdns6.com/zone0

3.3.5.3 Definición de zonas inversas DNS64

De la misma manera que la zona directa las zonas inversas deben de ser definidas en el archivo principal de configuración */etc/named.conf*

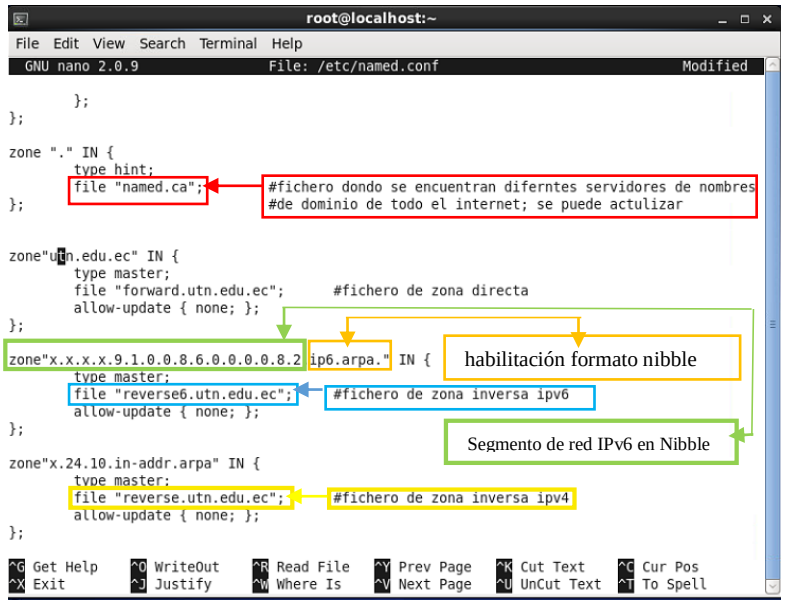


Figura 80. Zonas Inversas en named.conf

Fuente: http://rdns6.com/zone

Se guarda y se cierra sale del editor, lo siguiente es crear las zonas inversas, primero es configurar la zona inversa para ipv4 mediante el siguiente comando, sin olvidar que el nombre de esta zona ya estaba definido anteriormente. Para el cálculo de la zona inversa revisar Anexo 3.

#nano /var/named/reverse.utn.edu.ec

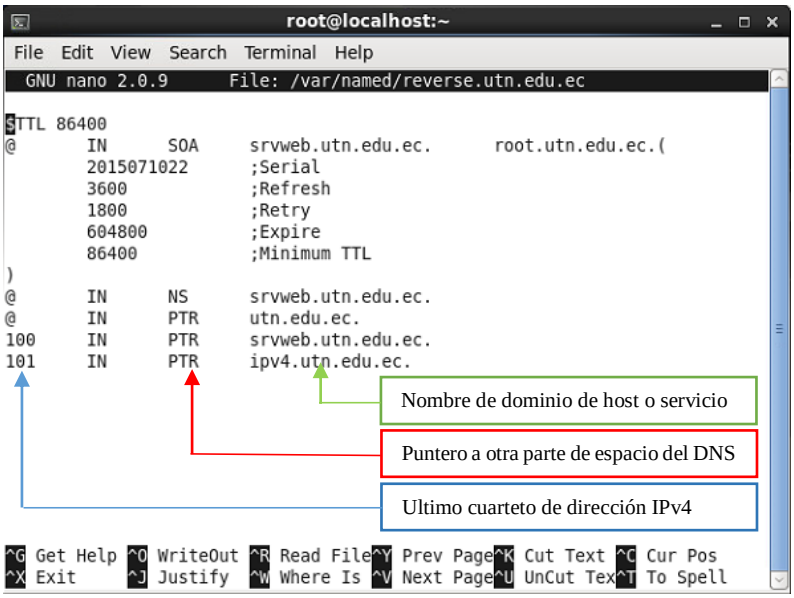


Figura 81. Zona inversa DNS64

Fuente: http://rdns6.com/zone

Guardar y salir del editor, ahora se procede a crear la zona inversa para ipv6 usando el comando: *nano /var/named/reverse6.utn.edu.ec* y utilizando el valor de la zona inversa calculada con anterioridad (Anexo 3).

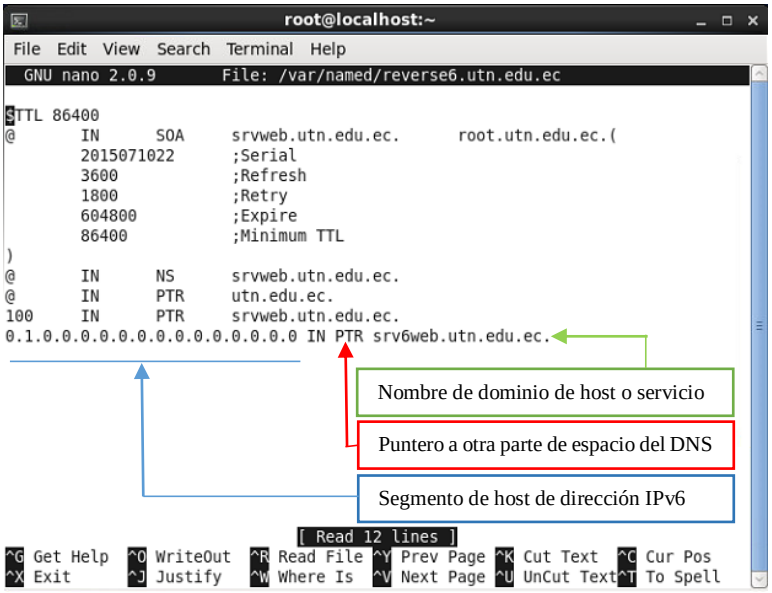


Figura 82. Zona inversa6 DNS64

Fuente: http://rdns6.com/zone

Una vez finalizado esta configuración se guarda y cierra el editor, al tener listo todos estos archivos para que los cambios tomen efecto se debe reiniciar el servicio.

#service named restart

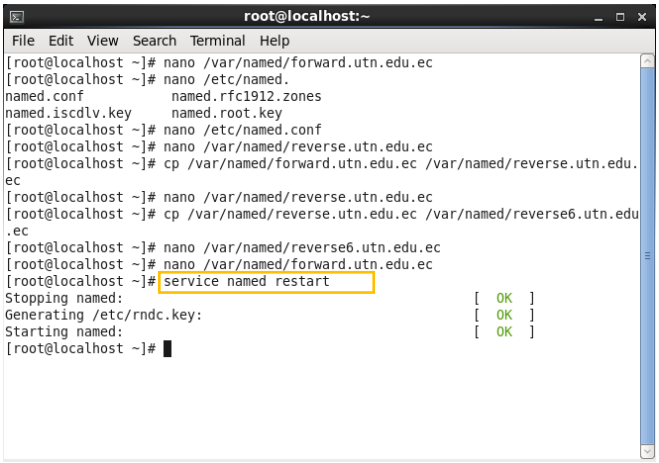


Figura 83. Reinicio de servicio DNS

Fuente: https://www.isc.org/downloads/bind/doc/bind-9-10/

3.3.5.4 Verificación de resolución de nombres IPv4/IPv6

Para verificar el funcionamiento del servidor de dominio se hace mediante los siguientes comandos, con los cuales se observa la resolución del nombre de dominio a las direcciones correspondientes.

#dig any utn.edu.ec

En lugar de especificar el tipo de registro a mostrar (A, MX, CNAME, AAAA…) con el parámetro *any* se puede pedir en una misma consulta todos los registros que se encuentren en la zona DNS del dominio

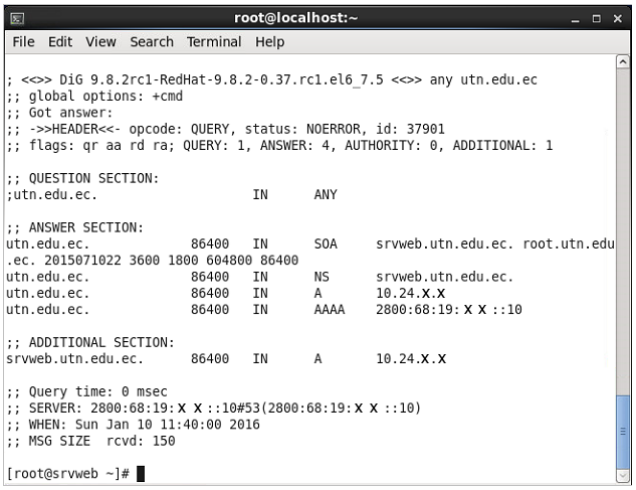


Figura 84. Diagnostico any DNS

Fuente: https://www.isc.org/downloads/bind/doc/bind-9-10/

Cuando se quiere realizar una consulta especifica de registros en IPv6 a la zona de dominios DNS se digita:

#dig AAAA utn.edu.ec

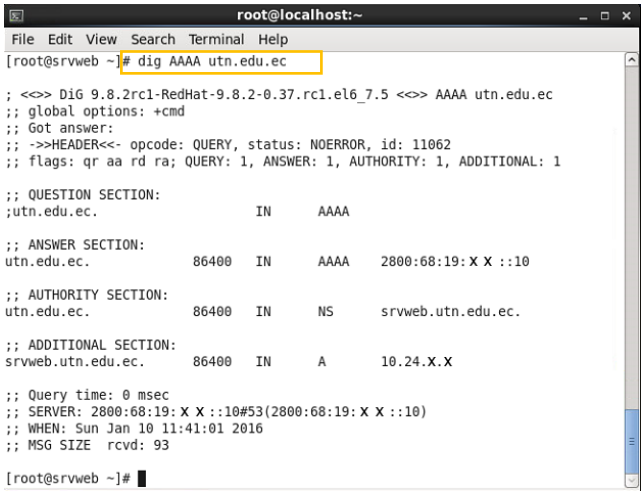


Figura 85. Diagnostico AAAA DNS

Fuente: https://www.isc.org/downloads/bind/doc/bind-9-10/

Nslookup es un comando que hace consultas dinámicamente al servidor DNS, con el cual se puede obtener la IP conociendo el nombre o traducir el dominio sabiendo la dirección IP.

#nslookup utn.edu.ec

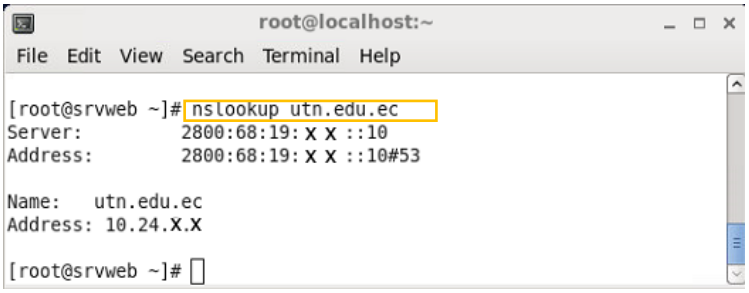


Figura 86. nslookup utn.edu.ec

Fuente: https://www.isc.org/downloads/bind/doc/bind-9-10/

Prueba de servidor de nombres dominio desde un cliente en Windows utilizando el comando nslookup en el símbolo de sistema.

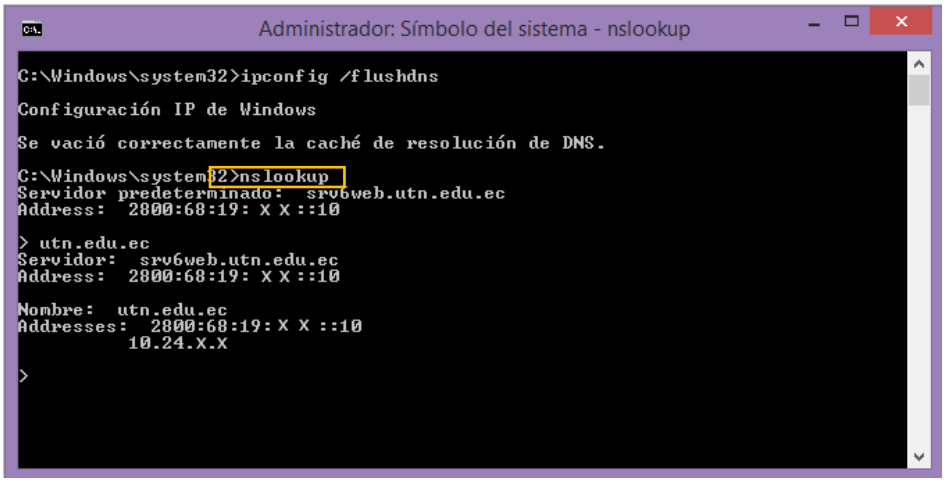


Figura 87. nslookup desde cliente

Fuente: https://technet.microsoft.com/en-us/library/cc725991.aspx

La comprobación del acceso por domino al servidor web mediante los nombres de IPv4, IPv6 y utn.edu.ec.

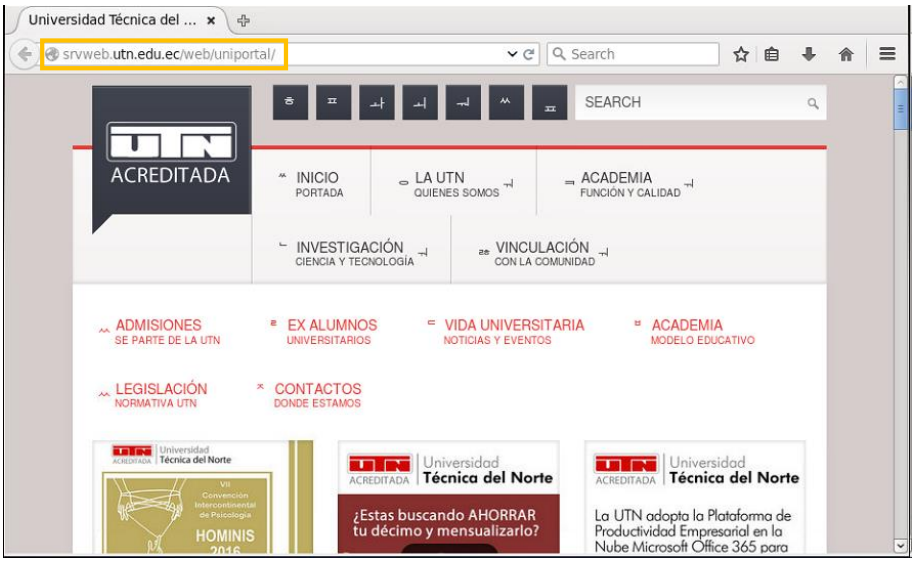


Figura 88. Acceso web por dominio IPv4

Fuente: Servidor Web Universidad Tecníca del Norte

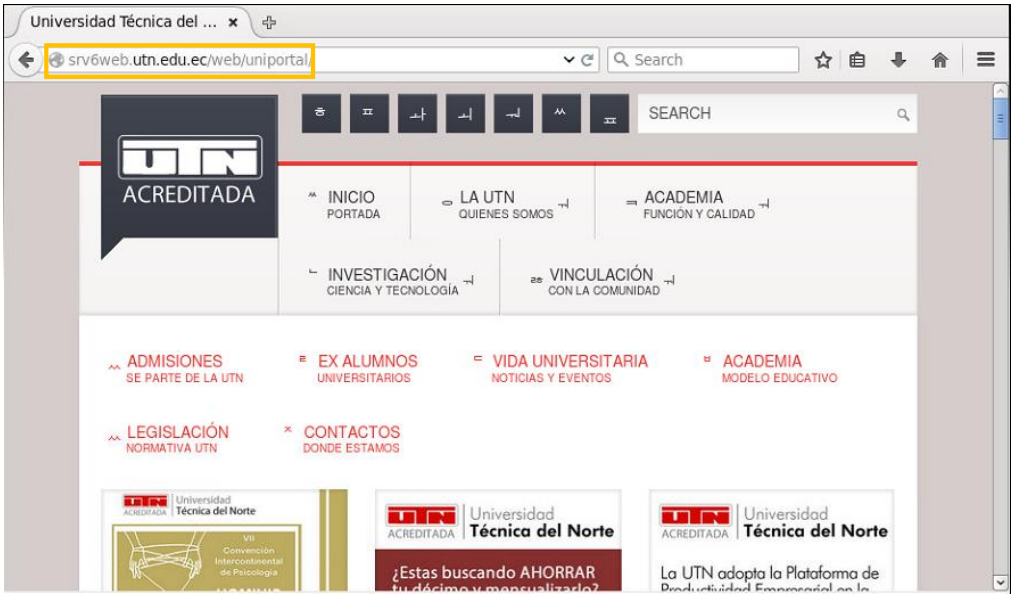


Figura 89. Acceso web por dominio IPv6

Fuente: Servidor Web Universidad Tecníca del Norte

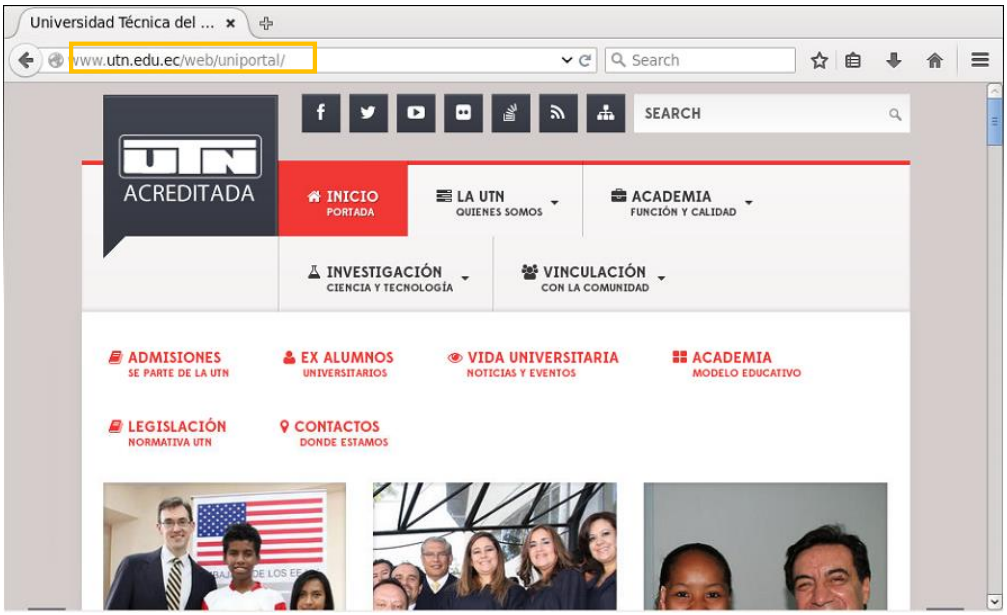


Figura 90. Acceso web por dominio universitario

Fuente: Servidor Web Universidad Tecníca del Norte

Acceso al servidor FTP usando el nombre de dominio utilizando el navegador web.

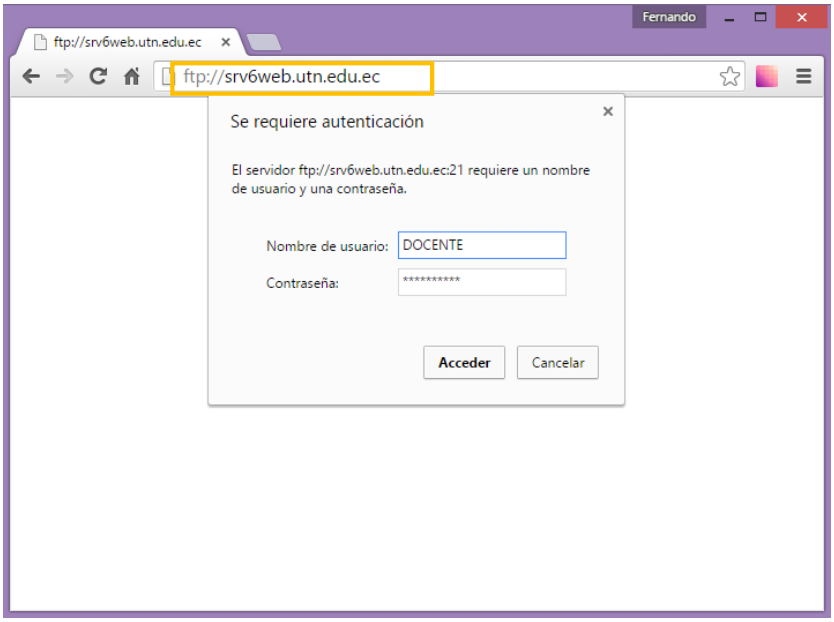


Figura 91. Acceso a FTP por dominio

Fuente: Servidor de Transferencia de Archivos de la UTN

CAPÍTULO 4

4 IMPLANTACIÓN DE MECANISMO Y PRUEBAS DE FUNCIONAMIENTO

4.1 CONFIGURACIÓN DE MECANISMO DS-LITE

El modelo DS lite (dual stack lite) que se utiliza en este proyecto consiste en la implementación de un sistema final que maneja doble pila, es decir, puede recibir y enviar paquetes IPv4 como también paquetes IPv6.

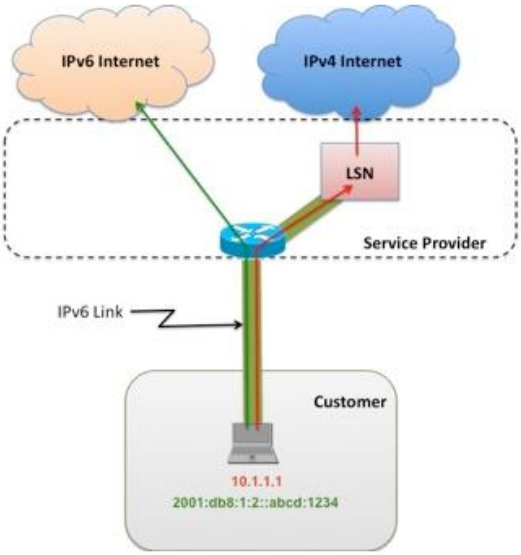


Figura 92. Modelo DS-Lite

Fuente: Recuperado de http://www.networkworld.com/article/2232181/cisco-subnet/understanding-dual-stack-lite.html

Para que el dispositivo final tenga la capacidad de recibir y enviar paquetes en ambos protocolos se debe agregar las siguientes líneas en el fichero "*/etc/named.conf*".

nano /etc/named.conf

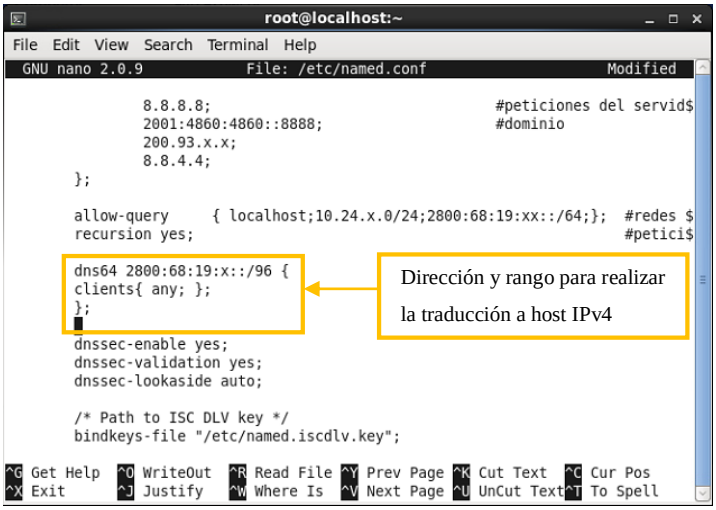


Figura 93. Configuración consultas ipv4 - ipv6

Fuente: Fichero de configuración named.conf

Con la configuración anterior se permite consultas de usuarios que no tienen registros AAAA (solo registros A), y sean entregadas a los usuarios añadiendo:

2800:68:19:x::/96

Para que los cambios tomen efecto después de salir y guardar la configuración del fichero se debe reiniciar el servicio de resolución de nombres.

#service named restart

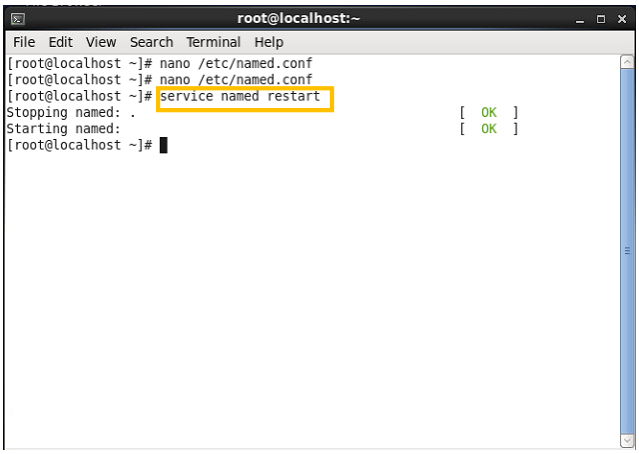


Figura 94. Reinicio de servidor de nombres

Fuente: Recuperado de http://blog.acostasite.com/2013/01/dns64-y-nat64-paso-paso-con-explicacion.html

Para comprobar que se utiliza el comando "*dig ipv4.google.com aaaa @2800:68:19:x::10",* lo importante a destacar son las direcciones que empiezan con 2800:68:19:x:: lo que indica las consultas IPv4 sobre IPv6.

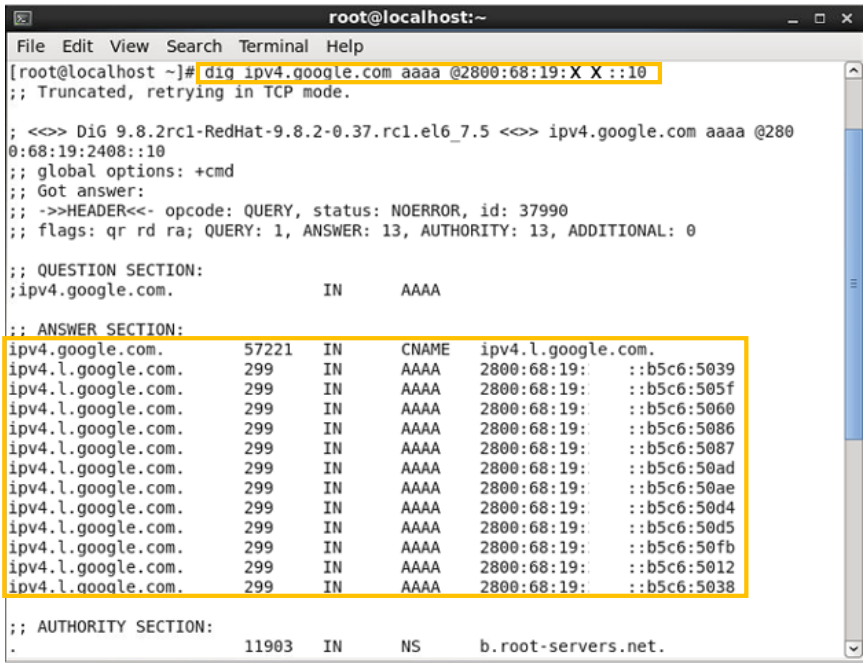


Figura 95. Consultas ipv4 sobre ipv6

Fuente: Comando de dianostico en servidor NAT64/DNS64

En este proyecto se utiliza un equipo configurado en Dual-Stack Lite, el cual realiza el proceso de NAT64 y evitará al mismo tiempo la implementación de túneles, ya que solo utiliza vínculos IPv6, es decir, todas las peticiones que hacen los usuarios IPv6 a servicios IPv4 se entregan al servicio correspondiente entre el proveedor y los usuarios. Cuando un dispositivo en la red local envía un paquete IPv6 se encapsula en un paquete IPv4 para el transporte en la red universitaria hacia el exterior obteniendo respuesta a las consultas sobre este protocolo.

Para lograr lo anteriormente dicho se usa el paquete tayga compatible con Centos 6.7. El fichero de configuración se encuentra en /etc/tayga/default, pero se debe de copiar de la siguiente manera:

#cp /etc/tayga/default.conf /etc/tayga.conf

Como resultado de esta operación se obtendrá un fichero de configuración con el nombre de tayga.conf.

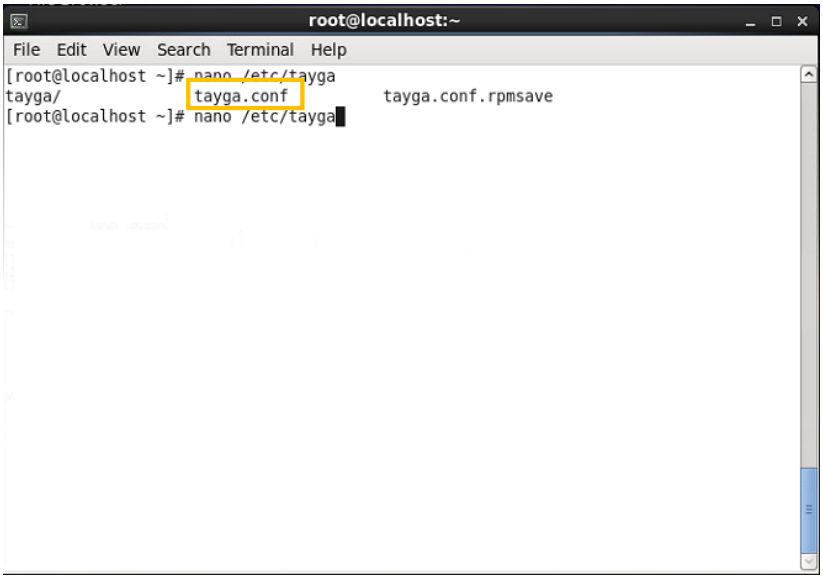


Figura 96. Ubicación de fichero taiga.conf

Fuente: Recuperado de http://blog.acostasite.com/2013/01/dns64-y-nat64-paso-paso-con-explicacion.html

La configuración del fichero tayga.conf para funcionamiento de NAT64, se realiza mediante el comando y editando la siguiente información:

#nano /etc/tayga.conf

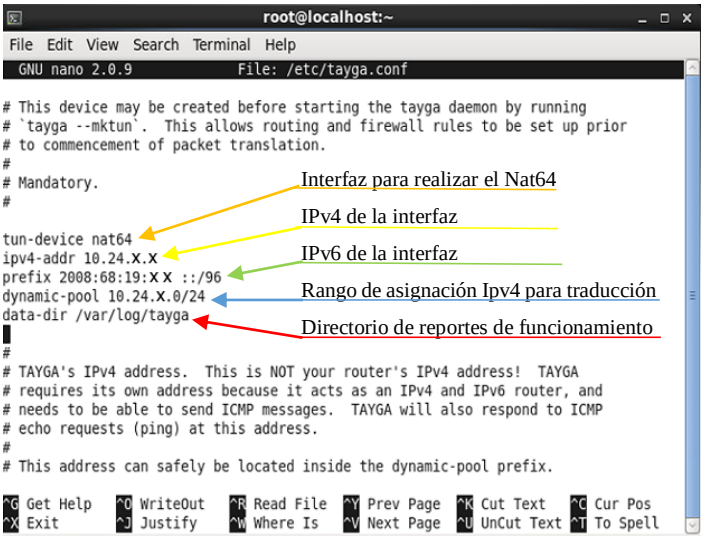


Figura 97. Configuración tayga.conf

Fuente: Fichero de confiuración tayga.conf Centos 6.5

Tayga es stateless y realiza un nat 1:1 entre IPv6 e IPv4. La configuración de la figura 96 a cada usuario IPv6 será asignado una IP del pool 10.24.x.0/24. Prefix indica el prefijo que Tayga usara para identificar los 32 bits de IPv4, es decir, cuando el destino IPv6 sea: 2800:68:19:x::/96, Tayga tomará los ultimos 32 bits para reconocer que ese es el destino IPv4. Después de guardar y cerrar el editor se debe de reiniciar el servicio para que los cambios realizados tomen efecto.

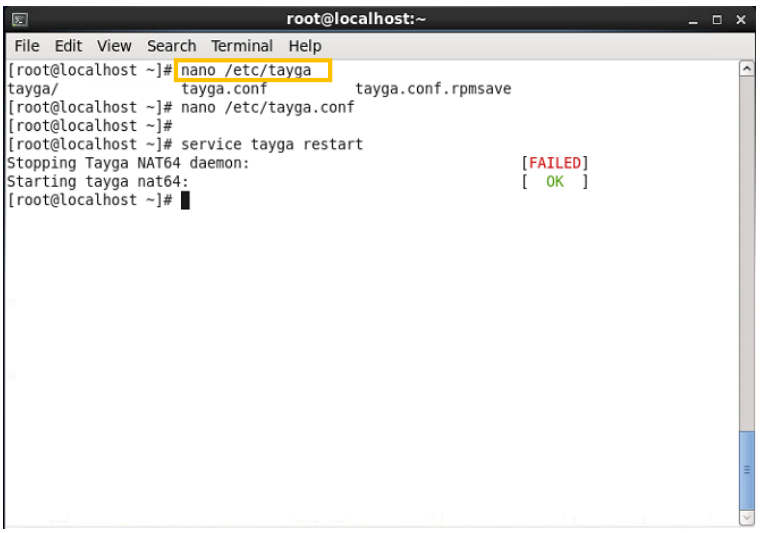


Figura 98. Rinicio de servicio nat64

Fuente: Recuperado de http://blog.acostasite.com/2013/01/dns64-y-nat64-paso-paso-con-explicacion.html

Evitar que cada vez que se reinicie el servidor tayga no se levante automáticamente con en el inicio, se ingresa:

#chkconfig tayga on

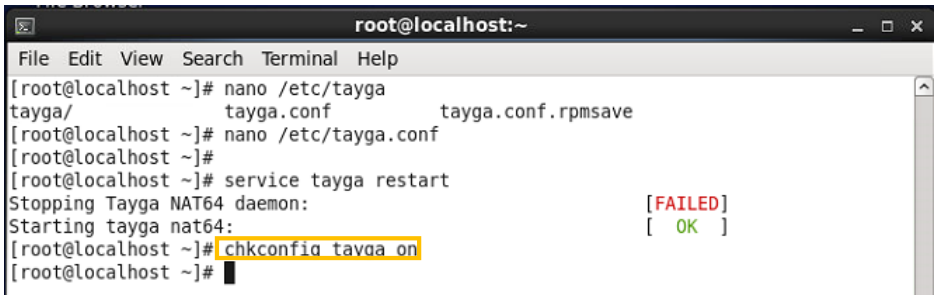


Figura 99. Inicio automatico de tayga

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

El siguiente paso a realizar es la habilitación de enrutamiento ipv6 e ipv4 en el servidor, con lo que agregamos las siguientes líneas en el terminal de Centos.

#echo "1" > /proc/sys/net/ipv6/conf/all/forwarding

#echo "1" > /proc/sys/net/ipv4/ip_forward

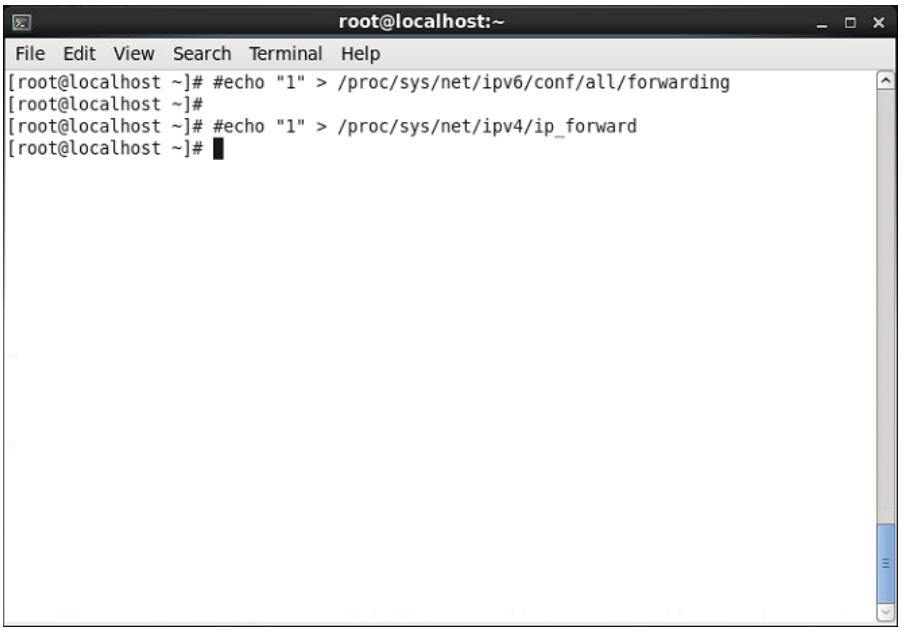


Figura 100. Habilitacion de enrutamiento ipv4 e ipv6 en servidor

Fuente: Recuperado de http://blog.acostasite.com/2013/01/dns64-y-nat64-paso-paso-con-explicacion.html

Se debe crear una interface para el NAT64 y configurar con los parámetros establecidos anteriormente con tayga, para realizar eso se agrega una interface:

#nano /etc/sysconfig/network-scripts/ifcfg-nat64

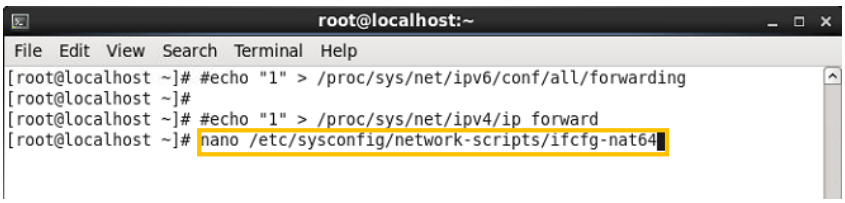


Figura 101. Creación de interface nat64

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Una vez creado el fichero de la interface NAT64 hay que configurar de acuerdo a lo establecido anteriormente.

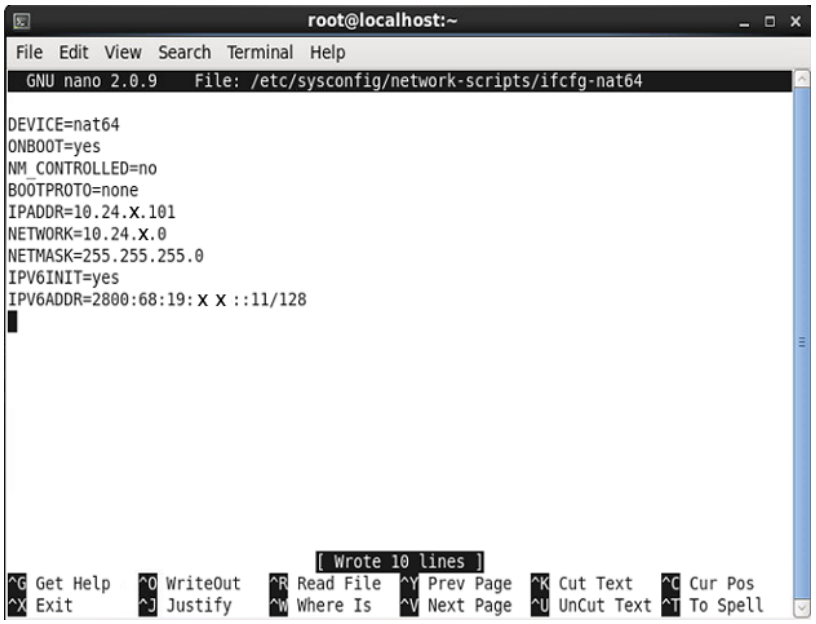


Figura 102. Interface NAT64

Fuente Elaborado por el Autor, Curso Linux Avanzado IECEIT

La configuración realizada en el fichero ifcfg-nat64 debe ser conforme con la realizada en tayga para su correcto funcionamiento. Para que los cambios tomen efecto se debe reiniciar las interfaces de red.

#service netwok restart

Si la interface NAT64 fue creada con éxito, se puede visualizar sus detalles utilizando el comando *ifconfig.*

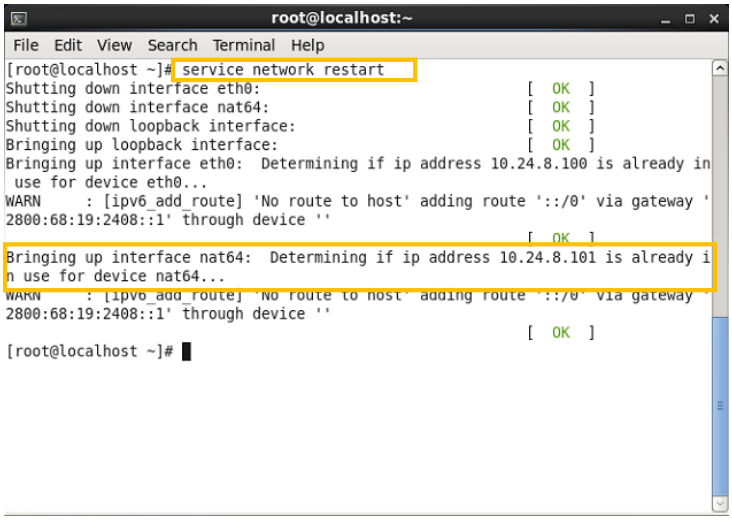


Figura 103. Reinicio de interfaces

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Por ultimo hay que crear las rutas con las que va a trabajar el servidor e iniciar tayga, la prueba de conectividad de una consulta desde ipv4 a ipv6 se puede realizar mediante un ping.

#ip route add 10.24.x.0/24 dev nat64

#ip route add 2800:68:19:xx::/96 dev nat64

#tayga

#ping6 2800:68:19:x::10.24.x.101

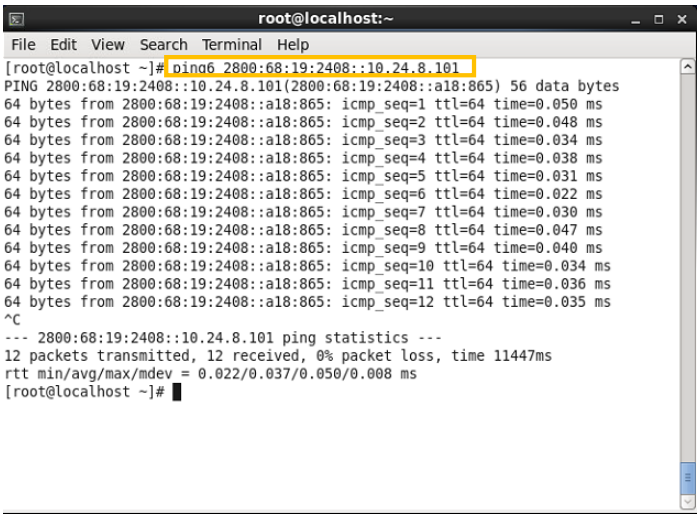


Figura 104. Ping de ipv4 a ipv6

Fuente: Recuperado de http://blog.acostasite.com/2013/01/dns64-y-nat64-paso-paso-con-explicacion.html

4.1.1 Switch cisco 3750

Las configuraciones sobre el switch cisco 3750 son el direccionamiento y encaminamiento de las direcciones del proveedor de internet hacia la el ASA 5520. El dispositivo se encontraba con una versión del sistema que no soportaba IPv6, para solucionar este problema se realizó una actualización del sistema operativo del switch.

Digitando los siguientes comandos se establece la configuración y enrutamiento en doble pila:

********** Habilitación de 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 ➔ próximo salto IPv6 ASA, la ruta estática se realiza con un /48 debido a que el recurso IPv6 de la UTN se asignó con ese prefijo, si se realizara con un /64 se estaría enrutando sobre la subred 0 y no habría tráfico de internet.

4.1.2 Configuración de Firewall CISCO ASA 5520

La configuración del CISCO ASA 5520 consiste en el enrutamiento y el control de tráfico que transita en la red, es decir, se establecen las reglas de encaminamiento para la comunicación entre las diferentes zonas de la red ouside, inside y DMZ.

El ingreso a la interfaz de configuración se realiza por medio del software proporcionado por el mismo equipo, en cual se solicitan los parámetros de la dirección IP del dispositivo como también un usuario y contraseña.

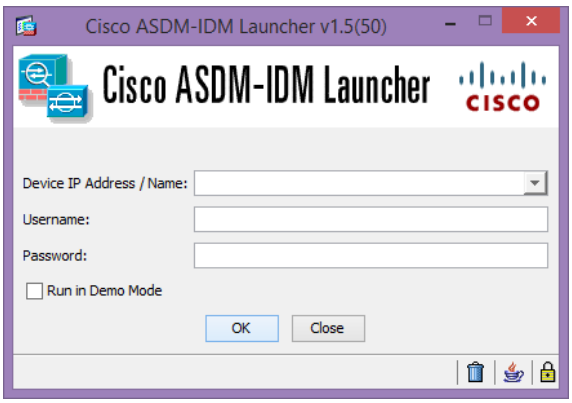
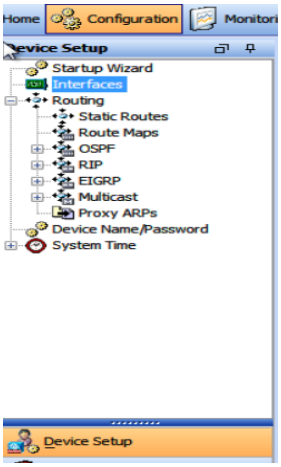
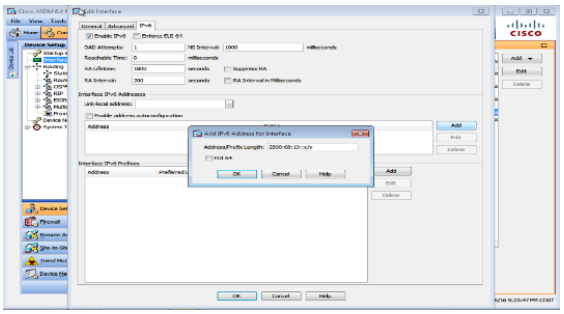


Figura 105. Cisco ASDM-IDM launcher

Fuente: Recuperado de http://www.allcustomdesign.com/cisco/

Lo primero que se debe realizar es la definición de las direcciones IPv4/IPv6 que se utilizaran en las distintas interfaces.

Tabla 11. Configuración interfaces firewall ASA csico 5520

Paso 1: definicion de interfaces, INSIDE, OUISIDE y DMZ, se entra en el menu configuration ➔ Device Setup ➔ Interfaces ➔ Add ➔ interfaces	
Paso 2: ingreso de direcciones por cada interface, 2800:68:19::x/y OUSIDE, 2800:68:19:x::/y INSIDE, 2800:68:19:x::/y DMZ. Menu IPv6 ➔ Add ➔ 2800…➔ Ok… la misma secuencia para cada una de las interfaces.	

Fuente: Departamento de desarrollo tecnológico e informático UTN

Teniendo las interfaces habilitadas con sus respectivas direcciones IPv4 e IPv6 se procede a realizar el encaminamiento de las diferentes redes, para permitir el tráfico entre la entrada del proveedor de internet hacia la red local y la zona desmilitarizada (DMZ).

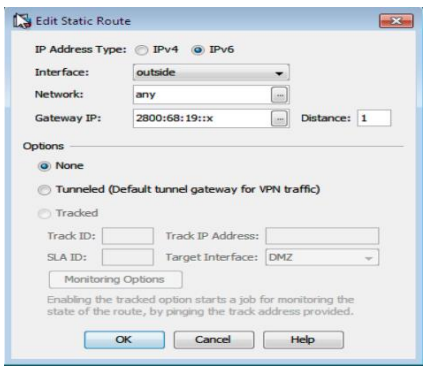


Figura 106. Direccions IPv6 OUTSIDE – INSIDE - DMZ

Fuente: Departamento de desarrollo tecnológico e informático UTN

Configuración del enrutamiento entre las diferentes VLANs de la Universidad Técnica del Norte, Donde Network es la red de acceso y Gateway ip la dirección IPv6 del switch The Core.

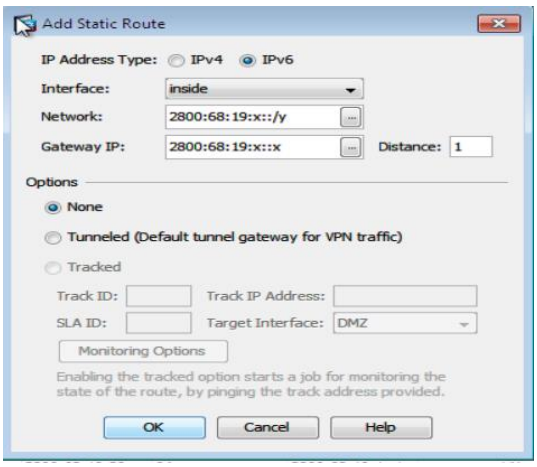


Figura 107. Enrutamiento VLANs UTN

Fuente: Departamento de desarrollo tecnológico e informático UTN

Ingreso de regla de tráfico que permiten la resolución de nombres desde el servidor DNS64 que se encuentra en la zona desmilitarizada.

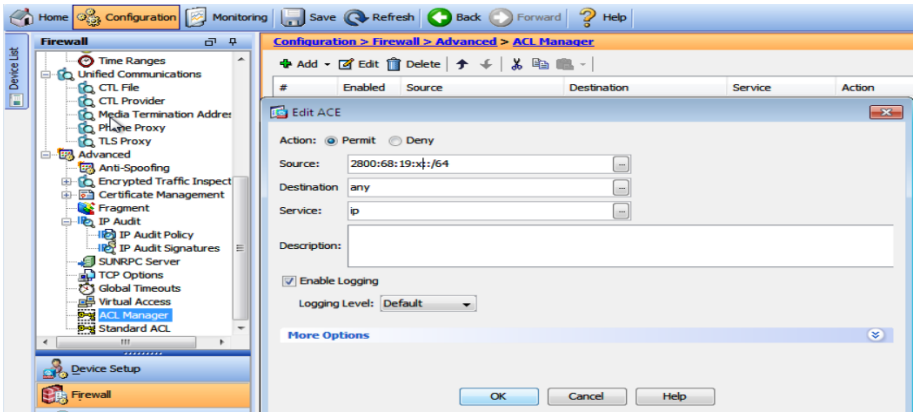


Figura 108. Reglas de trafico de resolucion de nombres

Fuente: Departamento de desarrollo tecnológico e informático UTN

4.1.3 Configuración de Switch

En la red universitaria el proveedor de servicio a internet es Telconet el cual también proporciona la conectividad directa con CEDIA, estos servicios están pre configurados en el switch de borde, el cual tiene conectividad sobre IPv4, así como también IPv6. Seguido al switch de borde se encuentra otro switch cisco 3750 en el que se definen las direcciones IP públicas de la institución y es un equipo intermedio entre el switch del proveedor y el asa 5520 de la UTN.

La red local es controlada por el switch The Core principal de cuarto de equipos, mismo que se encuentra conectado hacia el aza por medio de un control de ancho de banda (exinda), de la misma forma la zona desmilitarizada se conecta al ASA 5520 utilizando como puente al switch Nexus 5548 que también es un equipo cisco con funciones específicas.

4.1.3.1 Switch Core

La configuración de las distintas Vlans de la red local y la comunicación de las mismas hacia el ASA 5520 se realiza en el Swith The Core principal, se configurará solo las necesarias para probar el funcionamiento de este proyecto, pero el proceso es el mismo para cada una de las Vlans correspondientes.

Configuración VLAN Equipos Activos

Esta VLAN 1 está definida para equipos activos, es por interface que se realiza la administración de los equipos y para agregar funcionalidad y direccionamiento en IPv6 se digita:

```
SW-ZEUS-PRIMARIO# configure terminal
SW-ZEUS-PRIMARIO(confg)#ipv6 unicast-routing
SW-ZEUS-PRIMARIO(confg)#interface vlan 1
SW-ZEUS-PRIMARIO(confg-if)#ipv6 address 2800:68:19:x::1/y
SW-ZEUS-PRIMARIO(confg-if)#enable ipv6
SW-ZEUS-PRIMARIO(confg-if)#no shutdown
SW-ZEUS-PRIMARIO(confg-if)#exit
```

Configuración VLAN DMZ

La comunicación hacia la zona desmilitarizada de la UTN está en la VLAN 2, para agregar funcionalidad y direccionamiento en IPv6 se digita:

```
SW-ZEUS-PRIMARIO# configure terminal
SW-ZEUS-PRIMARIO(confg)#interface vlan 2
SW-ZEUS-PRIMARIO(confg-if)#ipv6 address 2800:68:19:x::1/y
SW-ZEUS-PRIMARIO(confg-if)#enable ipv6
SW-ZEUS-PRIMARIO(confg-if)#no shutdown
SW-ZEUS-PRIMARIO(confg-if)#exit
```

Configuración VLAN DDTI

El departamento de desarrollo tecnológico he informático basados en la tabla de direccionamiento definida anterior mente corresponde la VLAN 10, en la cual también se realiza los cambios para el funcionamiento de doble pila.

SW-ZEUS-PRIMARIO(confg)#interface vlan 10

SW-ZEUS-PRIMARIO(confg-if)#ipv6 address 2800:68:19:x::1/y

SW-ZEUS-PRIMARIO(confg-if)#enable ipv6

SW-ZEUS-PRIMARIO(confg-if)#no shutdown

SW-ZEUS-PRIMARIO(confg-if)#exit

Configuración VLAN FICA laboratorios

Para que los laboratorios en las facultades de la UTN tengan conectividad en doble pila se debe realizar la configuración en la VLAN correspondiente, como ejemplo de configuración se realiza en la VLAN 20 de los laboratorios FICA especificado en la tabla de direccionamiento.

SW-ZEUS-PRIMARIO(confg)#interface vlan 20

SW-ZEUS-PRIMARIO(confg-if)#ipv6 address 2800:68:19:x::1/y

SW-ZEUS-PRIMARIO(confg-if)#enable ipv6

SW-ZEUS-PRIMARIO(confg-if)#no shutdown

SW-ZEUS-PRIMARIO(confg-if)#exit

4.1.3.2 Nexus

Como se mencionó anteriormente este equipo tiene sus funciones específicas en la red de la UTN, por tanto, es necesario hacer la configuración de IPv6.

Nexus# configure terminal

Nexus(confg)#ipv6 unicast-routing

Nexus(confg)#interface g0/0

Nexus(confg-if)#ipv6 address 2800:68:19:x::3/y

Nexus(confg-if)#ipv6 enable

Nexus(confg-if)#no shutdown

Nexus(confg-if)#exit

Nexus(confg)#ipv6 route ::/0 2800:68:19:x::2

4.1.3.3 Switch Fica

La comunicación desde la facultad de ingeniería en ciencias aplicadas FICA sobre la red universitaria está establecida mediante el switch the CORE de la misma, el cual es el vínculo principal hacia los laboratorios de esta y se debe configurar para tener conectividad sobre IPv6.

SW-ARISTOTELES# configure terminal

SW-ARISTOTELES (confg)#ipv6 unicast-routing

SW-ARISTOTELES (confg)#interface vlan 1

SW-ARISTOTELES (confg-if)#ipv6 address 2800:68:19:x::31/y

SW-ARISTOTELES (confg-if)#ipv6 enable

SW-ARISTOTELES (confg-if)#no shutdown

SW-ARISTOTELES (confg-if)#exit

4.1.4 Configuración de equipos de laboratorios

El acceso para los usuarios en los laboratorios posee switch cisco 2960 de 48 puertos, los cuales también deben de configurarse con doble pila, de la siguiente manera:

Tabla 12. Configuración IPv6 en switch cisco 2960

Paso 1	configure terminal	Modo de configuración global.
Paso 2	sdm prefer dual-ipv4-and-ipv6default	Selección de SDM para tener soporte de IPv4 e IPv6.
Paso 3	end	Regresar a modo privilegiado EXEC.
Paso 4	reload	Reiniciar el sistema operativo.
Paso 5	configure terminal	Entrar al modo global de configuraciones.
Paso 6	interface*interface-id*	Ingresar a la interface a configurar.
Paso 7	ipv6 address*ipv6-address/prefixlength* ipv6 enable	Especificar una dirección global IPv6 con el prefijo correspondiente. Habilitación del procesamiento en la interface por IPv6.
Paso 8	exit	Retorno a la configuración global.
Paso 9	end	Retorno al modo privilegiado EXEC.
Paso 10	show ipv6 interface*interface-id*	Verificación de entrada de direcciones IPv6.
Paso 11	copy running-config startup-config	Guardar las configuraciones realizadas.

Fuente: Recuperado de http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-0_2_se/configuration/guide/scg2960/swipv6.html

Los equipos de laboratorio deben contener la siguiente configuración en sus respectivas tarjetas de red, tanto los equipos que solo usan IPv4, IPv6 y ambos protocolos.

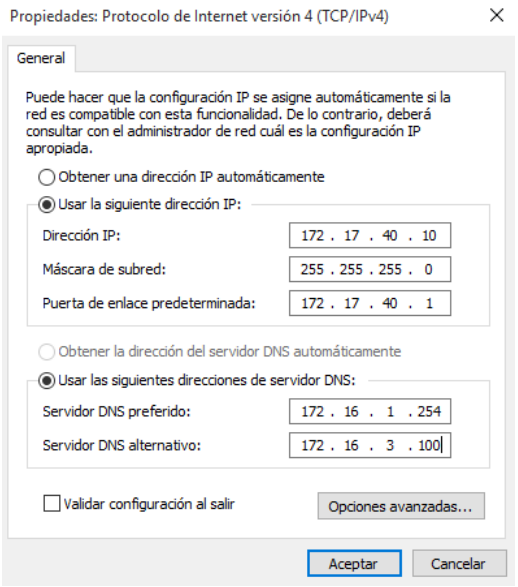


Figura 109. Configuración equipo nativo IPv4 de laboratorio

Fuente: Equipo de Laboratorio 4 – FICA

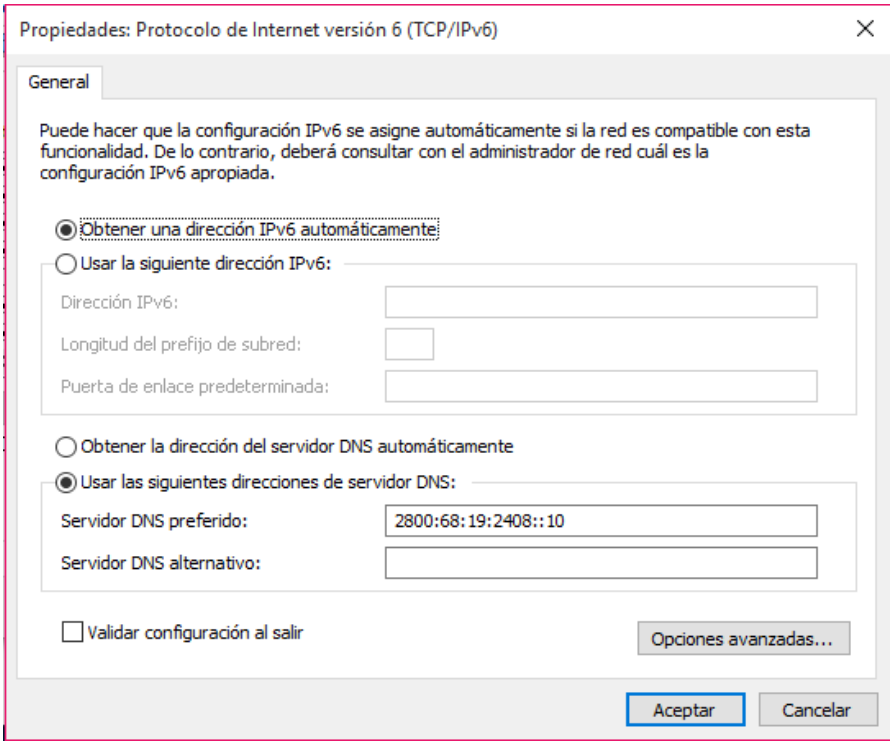


Figura 110. Configuración DNS equipo nativo IPv4 de laboratorio

Fuente: Equipo de Laboratorio 4 – FICA

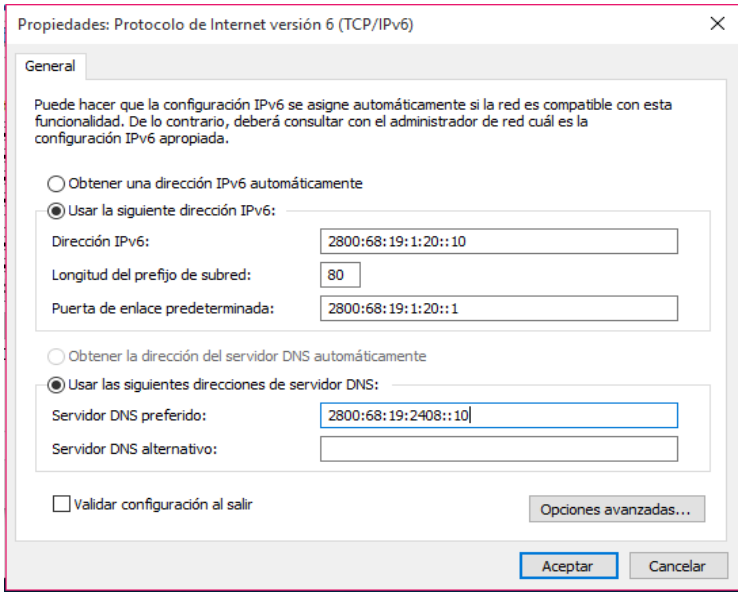


Figura 111. Configuración equipo nativo IPv6 laboratorio

Fuente: Equipo de Laboratorio 4 – FICA

En las redes actuales es necesario que ambos protocolos de internet coexistan, por tanto, los equipos y dispositivos deben de estar en la capacidad de trabajar en los mismos, debido a que no todas las aplicaciones trabajan aun sobre IPv6 como ya se mencionó anteriormente. A continuación, se configura los equipos utilizando doble pila.

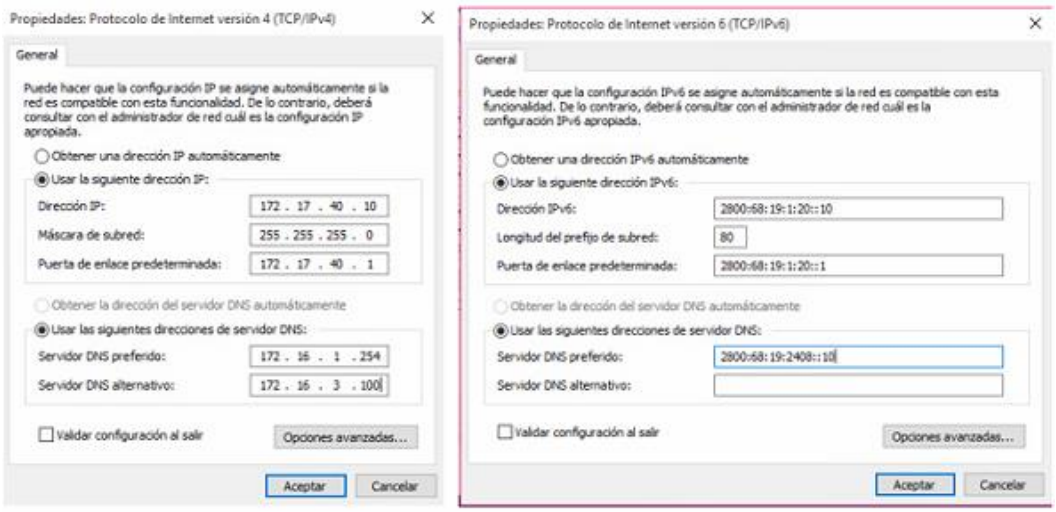


Figura 112. Configuración de equipos de laboratorios en doble pila

Fuente: Equipo de Laboratorio 4 – FICA

4.2 PRUEBAS DE FUNCIONAMIENTO

4.2.1 Pruebas de funcionamiento de mecanismo DS-Lite

Como referencia de funcionamiento del mecanismo de transición se toma en cuenta las solicitudes en ambos protocolos de internet, al servidor web de la Universidad Técnica del Norte, mediante el uso de wireshark filtramos sobre la eth0 del servidor y se observa si un usuario IPv6 o IPv4 está generando trafico al servidor web.

4.2.1.1 Pruebas en red local

El equipo del usuario tiene una dirección física (MAC) 00:0e:c6:f0:2b:6b y realiza una consulta hacia el servidor web como usuario nativo IPv6.

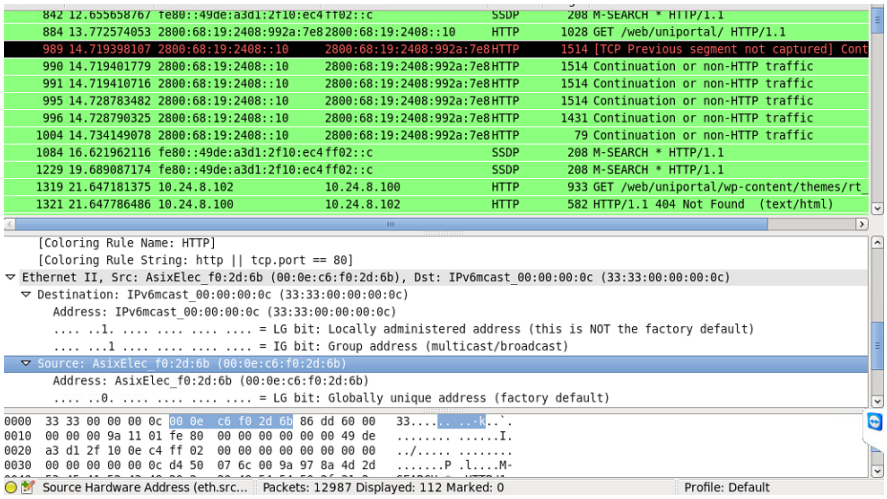


Figura 113. Visualización de MAC de usuario en wireshark

Fuente: Departamento de desarrollo tecnológico e informático

Para comprobar los datos anteriormente mencionados en la terminal del usuario se digita el comando ipconfig para revisar los parámetros de las tarjetas de red del equipo, donde se puede notar que el usuario no tiene asignado un direccionamiento estático sobre ipv6, sino que es asignado por el servidor DHCPv6 con la finalidad de que equipos en la

red local que no tengan una configuración en ipv6 puedan acceder a los servicios en este protocolo de internet.

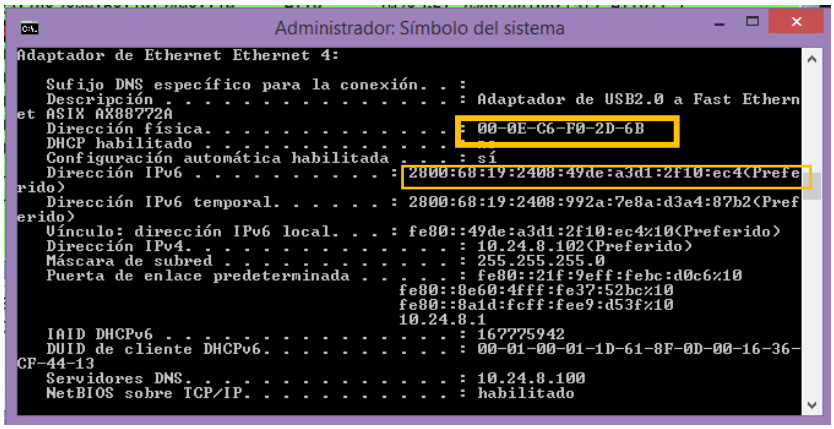


Figura 114. Información tarjeta de red usuario local

Fuente: Equipo de Laboratorio 4 – FICA

Con lo ya mencionado cuando el usuario ingresa al portal universitario a través de IPv6 la respuesta será desde este mismo protocolo, pero si la solicitud proviene de un usuario que utiliza IPv4 entonces quien responderá será el servidor que se encuentra operando sobre el protocolo de internet versión cuatro.

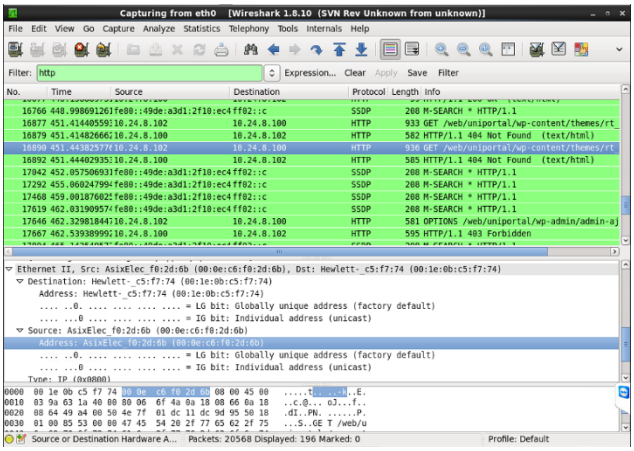


Figura 115. Visualización de trafico IPv4 hacia servidor WEB

Fuente: Departamento de desarrollo tecnológico e informático

4.2.1.2 Pruebas de funcionamiento red externa

En la ejecución de pruebas fuera de la red universitaria se accede al servidor web desde un host en la red de doble pila del proveedor de internet CNT EP. que actualmente hay en algunos hogares.

Deshabilitando el protocolo IPv4 en el equipo del usuario conectado a la red del proveedor de internet, se realiza consultas desde usuarios nativos IPv6 hacia el dominio de la UTN (www.utn.edu.ec) obteniendo como resultado el portal universitario.

Figura 116. Acceso desde red CNT EP a portal universitario

Fuente: Recuperado de http://www.utn.edu.ec

4.2.1.3 Pruebas de coexistencia de protocolos IPv6/IPv4 en internet

Se puede realizar un test de conectividad para la verificación de la coexistencia y funcionamiento de IPv6 e IPv4 en la red de la Universidad Técnica del Norte desde el enlace: http://www.mrp.net/ipv6_survey/

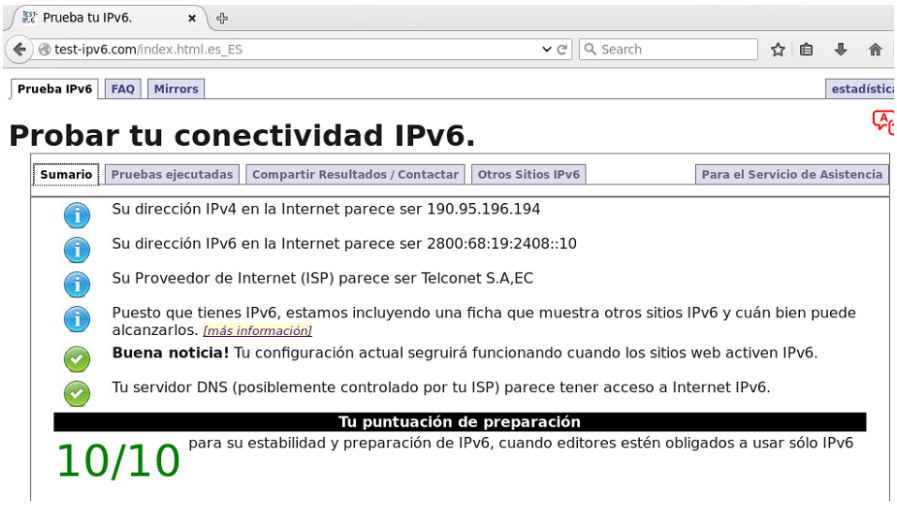


Figura 117. Pruebas de conexistencia IPv4 – IPv6 sobre internet

Fuente: Recuperado de http://test-ipv6.com/index.html.es_ES

Figura 118. Pruebas ejecutadas de conexistencia IPv4 – IPv6 sobre internet

Fuente: Recuperado de http://test-ipv6.com/index.html.es_ES

4.2.2 Pruebas de acceso a aplicación WEB desde usuarios IPv4 e IPv6

Como ya se mencionó anteriormente los usuarios que estén configurados con el mecanismo de doble pila pueden interactuar con los servicios tanto en ipv4 como en ipv6.

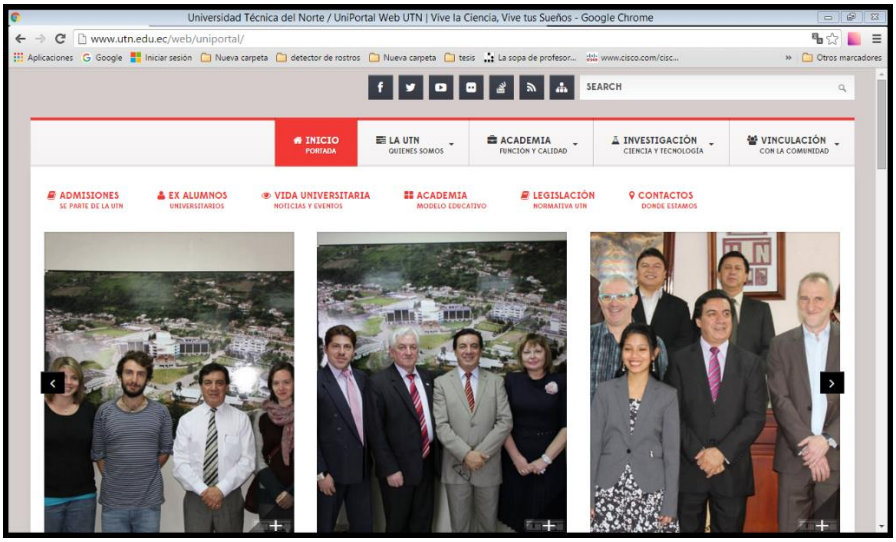


Figura 119. Portal Universitario UTN

Fuente: Departamento de desarrollo tecnológico e informático

En la actualidad se tiene conocimiento de que la mayoría de usuarios trabajan sobre el protocolo de internet versión cuatro, por tanto, es a quien toca dar prioridad de funcionamiento, no obstante, el servidor de nombres está preparado para brindar conexión ya sea nativa IPv6, así como IPv4 o ambos protocolos al mismo tiempo.

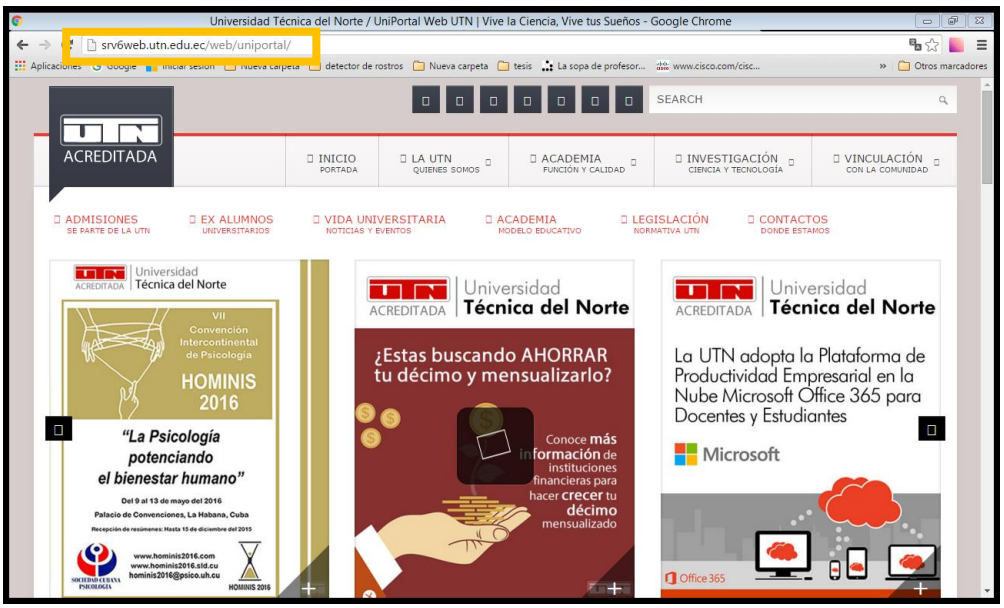


Figura 120. Acceso servidor Web UTN sobre IPv6

Fuente: Departamento de desarrollo tecnológico e informático

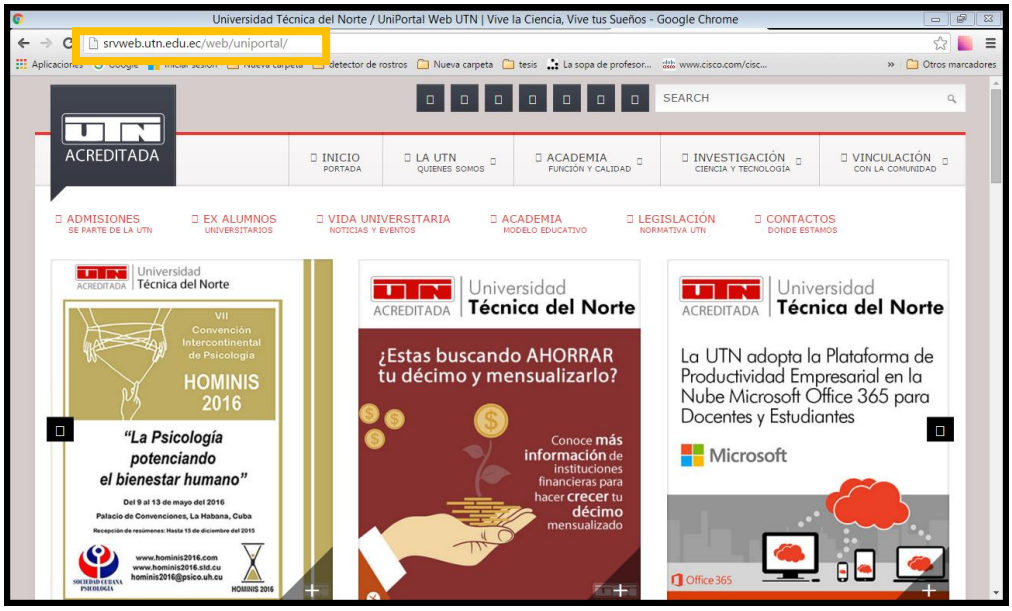


Figura 121. Acceso servidor Web UTN sobre IPv4

Fuente: Departamento de desarrollo tecnológico e informático

El sitio web mrp.net ha creado un algoritmo de encuesta IPv6 que se actualiza cada 24 horas, consiste en saber qué servicios están activos actualmente sobre este protocolo de quienes ya cuentan con un recurso asignado, con la finalidad informar sobre el crecimiento y desarrollo del protocolo de internet versión 6.

La Universidad Técnica del Norte al tener habilitado un portal web utilizando una dirección IPv6 de el rango designado por CEDIA, aporta al desarrollo e implementación de aplicaciones sobre IPv6, esto se puede comprobar en el sitio web mrp.net.

Ecuatorian Universities

Organisation (domain)	Web	Mail	DNS	NTP	XMPP	SIP	Access	Submit
Escuela Politécnica del Chimborazo (espoch.edu.ec)	PROBLEM	FAIL	1/1 4/4	PROBLEM				
Escuela Politécnica del Ejército (espe.edu.ec)	FAIL	SUCCESS	0/1 0/3					
Escuela Politécnica Nacional (epn.edu.ec)	FAIL	FAIL	0/1 0/3					
Escuela Superior Politécnica del Litoral (espol.edu.ec)	FAIL	FAIL	0/1 0/3					
Instituto Oceanográfico de la Armada (inocar.mil.ec)	FAIL	FAIL	0/0 0/2					
Pontificia Universidad Católica del Ecuador Sede Ibarra (pucesi.edu.ec)	PROBLEM	SUCCESS	0/0 0/2					
Pontificia Universidad Católica del Ecuador Sede Quito (puce.edu.ec)	FAIL	FAIL (MA)	0/1 0/3					
Secretaría Nacional de Ciencia y Tecnología (senescyt.gob.ec)	FAIL	FAIL	0/0 2/2					
Universidad Católica Santiago de Guayaquil (ucsg.edu.ec)	FAIL	FAIL	0/0 0/2					
Universidad Central del Ecuador (uce.edu.ec)	FAIL	FAIL	0/1 4/6					
Universidad de Cuenca (ucuenca.edu.ec)	FAIL	PARTIAL	1/1 3/3	PROBLEM	FAIL			
Universidad Estatal de Bolivar (ueb.edu.ec)	FAIL	FAIL	0/2 0/2					
Universidad Estatal de Milagro (unemi.edu.ec)	PROBLEM	FAIL	0/0 0/2					
Universidad Internacional del Ecuador (uide.edu.ec)	FAIL	FAIL	0/0 0/2					
Universidad Nacional de Chimborazo (unach.edu.ec)	PROBLEM	FAIL	0/1 2/3					
Universidad Nacional de Loja (unl.edu.ec)	FAIL	SUCCESS	0/0 0/2					
Universidad Politécnica Salesiana (ups.edu.ec)	FAIL	FAIL	0/0 0/2					
Universidad Regional Autónoma de los Andes - Ambato (uniandes.edu.ec)	FAIL	SUCCESS	0/0 0/2					
Universidad San Francisco de Quito (usfq.edu.ec)	PROBLEM	PROBLEM	0/2 0/2	PROBLEM	S:FAIL			
Universidad Tecnológica Equinoccial (ute.edu.ec)	PROBLEM	FAIL	0/0 0/2					
Universidad Tecnológica Indoamérica (uti.edu.ec)	FAIL	FAIL	0/0 0/2					
Universidad Técnica de Ambato (uta.edu.ec)	FAIL	FAIL	0/1 0/2					
Universidad Técnica del Norte (utn.edu.ec)	SUCCESS	FAIL	0/0 0/2					
Universidad Técnica Particular de Loja (utpl.edu.ec)	FAIL	FAIL	0/1 0/3			FAIL		

Figura 122. Prueba de servicio Web IPv6 de la UTN en Producción

Fuente: Recuperado de http://www.mrp.net/ipv6_survey/

4.2.3 Pruebas de acceso a servicio FTP desde usuarios IPv4 e IPv6

Todos los Usuarios también podrán entrar al servidor de transferencia de archivos, que está operando en el protocolo de internet versión 6, mediante la dirección de dominio *ftp://srv6web.utn.edu.ec*, luego se ingresa el usuario y contraseña que provee el administrador del servicio.

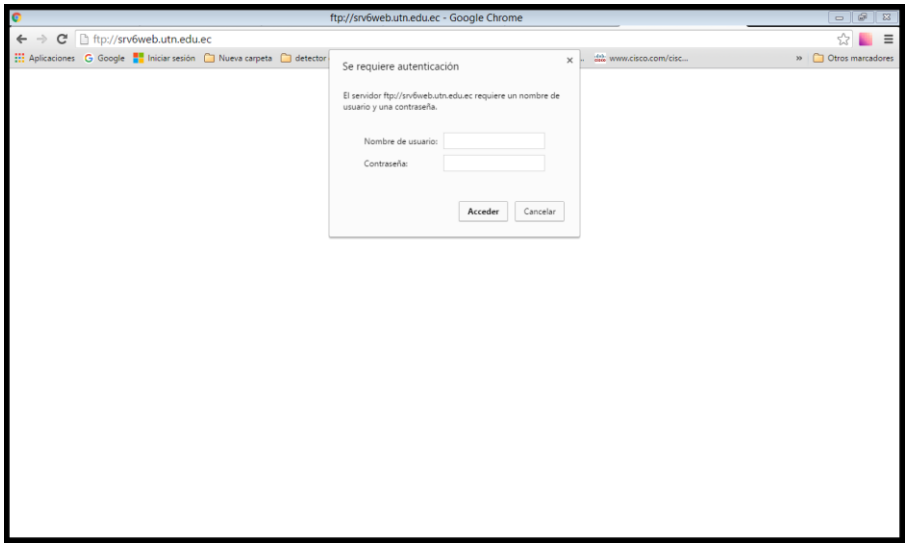


Figura 123. Ingreso a servidor FTP ipv6

Fuente: Departamento de desarrollo tecnológico e informático

CAPITULO 5

5 Análisis de costo

El análisis de costo de los elementos utilizados en la implementación de un mecanismo de transición de servicios WEB y FTP de IPv4 a IPv6 mediante el uso de DS-lite (dual-stack) con el uso de los equipos que se encuentran en la red universitaria.

Se utilizó la segmentación de red y el nuevo direccionamiento IPv6 se lo ejecuta en los equipos de red existentes, El servidor que se utiliza para la transición utiliza software libre, mismo que no tiene costo alguno para su implementación, el análisis se centra en el software y hardware necesario para lograr este proyecto.

5.1 Presupuesto

La implementación del mecanismo de transición se realiza mediante la configuración en los distintos equipos de la red universitaria, se utiliza los dispositivos detallados en la tabla 13.

Tabla 13. Presupuesto de Hardware

PRESUPUESTO DE HARDWARE Y SOFTWARE		
Unidad	Descripción	Valor(USD)
1	Cisco Switch 3750	$ 4,086.96
1	Cisco ASA 5520 Series	$ 2,227.53
1	Exinda 4761	$ 49 225.00
1	Nexus 5548	$ 13,864.81
1	Swicht The Core Catalys 4510R + E / 4500 +E Series	$ 5,150.00
1	Switch The Core Catalys FICA	$ 5,150,00
1	Blade Hp Proliant BL460c G1	$ 1 218.00
	TOTAL	$ 80,922.30

Fuente: Basado en cotizaciones de empresas de telecomunicaciones (Anexo 6)

Entre las posibilidades de software se puede presentar dos soluciones, software propietario y Open Sourse (software libre).

Tabla 14. Costos de Software

Software	**Valor (USD)**
Linux Centos 6.5	$ 0.00
Microsoft Windows Server 2012 R2 Essentials	$ 501.00
Total	$ 501.00

Fuente: Recuperado de https://www.microsoft.com/es-es/server-cloud/products/windows-server-2012-r2/purchasing.aspx, https://www.redhat.com/es/technologies/linux-platforms/enterprise-linux

Todos los equipos mencionados en la tabla 13, fueron adquiridos con anterioridad, actualmente son elementos funcionales y forman parte de los activos fijos de la universidad, por tal razón no es necesario realizar ninguna compra de hardware, en consideración de software se utiliza Open Sourse para la implementación del proyecto.

5.2 Costo - Beneficio

Este proyecto es con fines educativos, orientado a la optimización de los recursos existentes en la red universitaria, además de la actualización del protocolo de internet que se utilizara como estándar a nivel mundial en un futuro no muy lejano, de tal forma la universidad permanecería a la vanguardia en este tipo de tecnología y con acceso a la red avanzada disponible de CEDIA.

Tabla 15. Costo / Beneficio

Costos		**Beneficios**	
Descripción	Valor (USD)	Descripción	Valor (USD)
Hardware	$ 80,922.30	Optimización de hardware	$ 80,922.30
Software	$ 0.00	Ahorro / software	$ 501.00

Asesoramiento / Ejecución		$ 4000.00	Conectividad Avanzada (IPv6)	red	$ 4000.00
Total		$ 81,423.30	Total		$85,423.30
				B / C	1.05

Fuente: Recuperado de http://agesic.gub.uy/innovaportal/file/3284/1/modelo_para_el_analisis_de_costos_y_beneficios_v20130822.pdf (Anexo 6)

La relación costo - beneficio (B/C) se define del valor total de beneficio dividido por el valor total de los costos, obteniendo como resultado un número > 1, tabla 15. Esto quiere decir que el proyecto no generará gastos a la institución, pero si será beneficioso en el ámbito tecnológico y educativo.

CONCLUSIONES

Al terminar el presente proyecto de titulación se han obtenido las siguientes conclusiones:

- ✓ La red de la Universidad Técnica del Norte trabaja en doble pila, es decir trabaja con ambos protocolos de internet y tiene servicios tanto en IPv4 como en IPv6, la coexistencia entre estos protocolos de internet sobre la red de la UTN permite a la casona universitaria interactuar en la red avanzada que propone CEDIA, de esta forma se pueden realizar prácticas, estudios y tener acceso a bibliotecas virtuales y documentación para trabajos de investigación que solo se encuentran disponible para usuarios que tienen conectividad en dicha red.

- ✓ El despliegue en Ecuador de IPv6 no es muy alto, pero si tiene una gran importancia en las instituciones educativas de nivel superior, tanto públicas como privadas que pertenecen a CEDIA, quien a su vez proporciona el recurso en este protocolo para las distintas universidades en el país con la finalidad de que se desarrollen mecanismos de transición, pruebas de funcionamiento e interacción de diferentes servicios y aplicaciones utilizando IPv6.

- ✓ Con el tiempo se tendrá a ambos protocolos de internet en coexistencia, la mayor parte del trabajo es para los proveedores de servicios y los usuarios finales serán los últimos en percibir el cambio, debido a que no todas las aplicaciones con las que se cuenta en internet fueron desarrolladas para funcionar con IPv6.

- ✓ El uso de un traductor de direcciones a nombres de dominio facilita el acceso a las aplicaciones para los usuarios, por tal razón en este proyecto se implementó un servidor DNS64 el cual sintetiza los registros AAAA partiendo de la información de registros A, pero también el levantamiento del servicio DHCP en IPv6 ayuda a que la implantación del mecanismo de transición sea aún más rápida en los dispositivos que se asocien a la red de la UTN haciendo trasparente el proceso de transición para los usuarios.

- ✓ El protocolo IPv6 tiene mucha información que se puede estudiar e investigar con mayor profundidad, en este proyecto el objetivo era brindar un mecanismo de transición que garantice la coexistencia de ambos protocolos de internet, así como también aplicaciones que estén sobre IPv6, siendo el servidor web con el portal universitario la principal prueba de funcionamiento y el cual sea una pauta de inicio que permita a la UTN desarrollar otros servicios en el protocolo de internet versión seis.

- ✓ La utilización de Linux Centos y los diferentes paquetes que brinda la plataforma fueron esenciales en la preparación y configuración de los parámetros necesarios para el funcionamiento de DS-lite, DNS64 y DHCPv6 como parte en el proceso de transición de IPv4 a IPv6, del mismo modo se usó este sistema para levantar las aplicaciones Web y FTP sobre IPv6, Centos nos permite que cada uno de estos servicios se manejen de forma independiente, siendo una solución escalable en la implementación del mecanismo de transición.

- ✓ La Universidad Técnica del Norte al poseer equipos que soportan IPv6 y con la utilización de software libre no genera gastos a la institución, pero si un beneficio en la actualización y utilización de los equipos de red con el protocolo de internet versión 6, dando soporte para el aprendizaje y el desarrollo académico en el ámbito tecnológico.

- ✓ El periodo de propagación de un dominio oscila de 24 a 72 horas, debido a que deben de actualizarse los distintos servidores. En el proceso de actualización de la dirección de dominio en IPv6 de la UTN se realizó la petición al proveedor de servicio, dado el caso de realizar un cambio de dirección de servicios se debe de tener en cuenta el tiempo de cambio o propagación del dominio y dirección asociada al mismo.

RECOMENDACIONES

Al terminar el presente proyecto de titulación se han obtenido las siguientes recomendaciones:

- ✓ Si bien Linux Centos permite que el manejo de cada uno de los servicios sea independiente se recomienda que servicios como DNS y WEB se instalen y funciones en diferentes equipos, ya que son dos aplicaciones que reciben un gran número de peticiones en la red universitaria, el propósito es que los equipos solo se dediquen a una tarea específica permitiendo que la respuesta a los usuarios sea más rápida.

- ✓ No todos los equipos cisco se configuran de la misma manera para habilitar y utilizar IPv6, se recomienda revisar antes de deducir que el sistema operativo o el equipo no soportan este protocolo de internet versión seis.

- ✓ La manipulación de los equipos servidores no deben estar expuestos para el uso de personal no autorizando y menos aún sin los conocimientos necesarios de administración y gestión de las aplicaciones instaladas que componen el mecanismo de transición, con lo que se evita que la red quede inoperable.

- ✓ Se recomienda el desarrollo de más aplicaciones y servicios que se encuentren en IPv4 de la red universitaria para que puedan ser usados sobre IPv6, ya que este protocolo será el que se use como base de funcionamiento de los proveedores de internet.

- ✓ El mecanismo de transición debe de tener una metodología establecida, donde los usuarios no sufran el cambio tecnológico, es decir, el proceso debe ser transparente ya que no todos los dispositivos, aplicaciones y servicios están preparados para realizar una migración inmediata de IPv4 a IPv6.

- ✓ En el proceso de generar un mecanismo de transición para una institución como la Universidad Técnica del Norte, requiere de tiempo ya que existe una gran variedad de servicios que brinda a la comunidad universitaria, tanto para usuarios en el interior de la casona universitaria como afuera de la misma.

- ✓ Es importante contar con todas las herramientas, equipos, software y más aún el personal adecuado para realizar el proceso de transición en una red en producción, con la finalidad de no generar fallas de conexión o una pérdida total de la misma.

- ✓ Para un proceso de transición es importante que los equipos inmersos en dicha actividad tengan el soporte para operar sobre el protocolo de internet versión seis; en el caso de la adquisición de nuevos equipos para la red universitaria.

GLOSARIO DE TÉRMINOS

TERMINO	DESCRIPCIÓN
A	Host (registro de dominio IPv4)
AAAA	Host Ipv6 (registro de dominio IPv6)
AEPROVI	Asociación ecuatoriana de proveedores de valor agregado de internet
AFTR	Address Family Transition Router
BGP	Border Gateway Protocol
CEDIA	Consorcio ecuatoriano para el desarrollo de internet avanzado
CGNAT	Carrier Grade Network Address Translation
CNAME	Canonical Name
CPE	Customer Premises Equipment (Equipo Local del Cliente)
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)
DMZ	Demilitarized Zone (Zona desmilitarizada)
DNS64	Domine Name Systemr 64 (Sistema de nombres de dominio 64)
DS-lite	Dual stack lite (doble pila)
FTP	File Transfer Protocol (protocolo de transferencia de archivos)
Gbps	Gigabit por segundo
HTTP	Hypertext Transfer Protocol o HTTP (Protocolo de Transferencia de Hipertexto)
IANA	Internet Assigned Numbers Authority (Autoridad de Asignación de Números de Internet)
ID	Identificador
IETF	Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)
IPSec	Internet Protocol Security
IPv4	Protocolo de Internet versión 4 (Internet protocol versión 4)
IPv6	Protocolo de Internet versión 6 (Internet protocol versión 6)
ISP	Internet Service Provider (proveedor de servicios de Internet)
LACNIC	Latin America & Caribbean Network Information Centre (Registros de Direcciones de Internet para Latinoamérica y el Caribe)
LSN	Local System Network
Mbps	Megabits por segundo
MTU	Maximum Transmission Unit (Unidad Maxima de Transferencia)
NAT	Network Address Translation (traducción de direcciones de red)
NIC	Network Interface Card (Tarjeta de Interfaz de Red)

NRENs	National Research and Education Networks (Red Nacional de Investigación y Educación)
NS	Name Server
NTP	Network Time Protocol
RACE	Red Avanzada de CEDIA
redCLARA	Cooperación Latinoamericana de redes Avanzadas
RFC	Request for Comments
RISRs	Registros Regionales
SIP	Session Initiation Protocol (SIP o Protocolo de Inicio de Sesiones)
SSH	Secure Shell (Intérprete de órdenes seguro)
STM-1	Módulo de Transporte Síncrono correspondiente al primer nivel básico
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión)
UTN	Universidad Técnica de Norte
WAF	Web Application Firewall
WEB	Conjunto de información que se encuentra en una dirección determinada de internet.

BIBLIOGRAFÍA

LIBROS

A., P. (2011). *Tejiendo un Sueño. Apuntes para la historia de la Universidad Tecnica del Norte.* Quito: Mariscal.

ACOSTA, A., AGGIO, S., CICILE, G., LYNCH, T., MOREIRA, A., ROCHA, M., . . . SILVA, S. (2014). *IPv6 Para Operadores De Red.* Buenos Aires: Ebook.

ENAMORADO, L. &. (2011). *Servicios de red e Internet.* Madrid: Ibergarceta Publicaciones.

Barrios, J. (2015). *Configuración De Servidores Con GNU/Linux.* México D.F.: Alcance Libre.

Gerometta, O. (Diciembre de 2011). *Mis Libros de Networking.* Obtenido de http://librosnetworking.blogspot.com/2011/12/beneficios-de-ipv6.html

PALET, J. (2011). *IPv6 para España.* Madrid: Consulitel.

Palet, J. (2011). *Ipv6 para Operadores de Red.* Consulitel.

Guillermo Cicileo, R. O. (2009). *Ipv6 para todos, Guia de uso y apliacaciones para diversos entornos.* E-book.

SERVIN., S. S. (2014). *Introduccón a IPv6 y mecanismos de transición.* LACNIC.

Castillo, Y. (2014). Agotamiento de IPv4 en la. *Actualidad y Tecnología*.

TESIS

Adriana Morales, J. R. (2010). *Estudio Técnico- Economico para la transición IPv4 a IPv6 de un punto de intercambio de tráfico de internet (NAP.EC) que utiliza BGP como protocolo de enrutamiento.* Quito: Universidad Pilitécnica Salesiana.

Sánches, D. (2006). *Estudio del proceso de tansición del protocolo IPv4 hacia el IPv6.* Cuenca: Universidad Politécnica Salesiana.

Verdejo, G. (2000). *El protocolo IPv6 y sus extensiones de seguridad IPSec.* Balleterra.

REVISTAS

Alonso J, Martines C. . (2012). *LACNIC.* Obtenido de NAT64/DNS64 Comunicando los mundos v4 -v6: http://www.labs.lacnic.net/site/sites/default/files/051-nat64-dns64-lacnic-01_0.pdf

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

AEPROVI. (s.f.). *AEPROVI*. Obtenido de http://www.aeprovi.org.ec/quienes-somos/mision

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

CEDIA. (s.f.). *cedia.org.ec*. Obtenido de http://www.cedia.org.ec

Cerf, V. (2012). *Google*. Obtenido de http://www.google.com/intl/es/ipv6/index.html

CISCO. (s.f.). *IPv6 Routing: EIGRP Support.* Obtenido de cisco.com: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-3s/ire-xe-3s-book/ip6-route-eigrp-xe.html

Digani, K. (22 de Marzo de 2012). *Citrix.* Obtenido de DS-Lite – IPv4 over IPv6 and NAT: https://www.citrix.com/blogs/2012/03/22/ds-lite-%E2%80%93-ipv4-over-ipv6-and-nat/

DOYLE, J. (2009). *NetworkWord.* Obtenido de Understanding Dual-Stack Lite: http://www.networkworld.com/article/2232181/cisco-subnet/understanding-dual-stack-lite.html

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

Hopps, C. (Octubre de 2008). *tools.ietf.org.* Obtenido de https://tools.ietf.org/html/rfc5308

LACNIC. (2015). *fases de agotamiento ipv4.* Obtenido de http://www.lacnic.net/web/lacnic/agotamiento-ipv4

LACNIC. (s.f.). *Portal Ipv6*. Obtenido de http://portalipv6.lacnic.net/reporte-de-terminacion-de-direcciones-ipv4/

Malkin, G. G. (1997). RIPng para IPv6. *https://tools.ietf.org/html/rfc2080*.

Marcelo. (Abril de 2013). *Redes I.* Obtenido de http://redesiuv.blogspot.com/2013/04/historia-del-protocolo-tcpip-y-ipv4-ipv6.html

N. Sheth, L. Wang, J. Zhang. (Enero de 2013). *tools.ietf.org*. Obtenido de https://tools.ietf.org/html/rfc6845

Oracle. (2010). *http://docs.oracle.com/*. Obtenido de http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-planning-9/index.html

P. Marques, F. Dupont. (Marzo de 1999). *tools.ietf.org.* Obtenido de https://tools.ietf.org/html/rfc2545

R. Hiden, S. Deering. (Abril de 2003). *tools.ietf.org*. Obtenido de https://tools.ietf.org/html/rfc3513

Ralli, C. (2012). *http://long.ccaba.upc.es/.* Obtenido de http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf

ANEXOS

Anexo 1 – Instalación Linux

1. Instalación Linux Centos 6.5

Para empezar con la instalación se elige la primera opción del menú que ofrece Centos una vez se inicie el asistente.

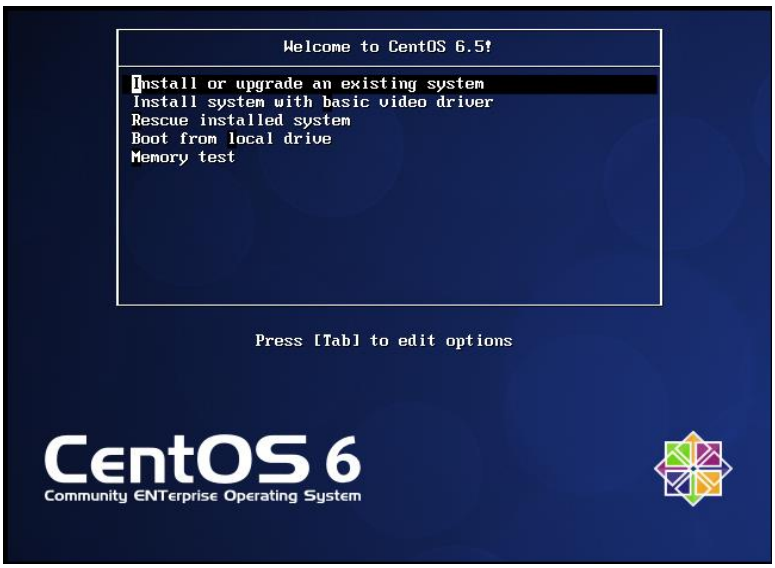


Figura 124. Menú de opciones Centos

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

En la siguiente pantalla se elige la opción de skip para continuar con la instalación personalizada, si se desea hacer una evaluación de los medios de comunicación.

Figura 125. Elección de evaluación de medios de comunicación

Fuete: Elaborado por Autor, Curso Linux Basico IECEIT

El inicio de la instalación personalizada empieza desde la siguiente pantalla clic en Next.

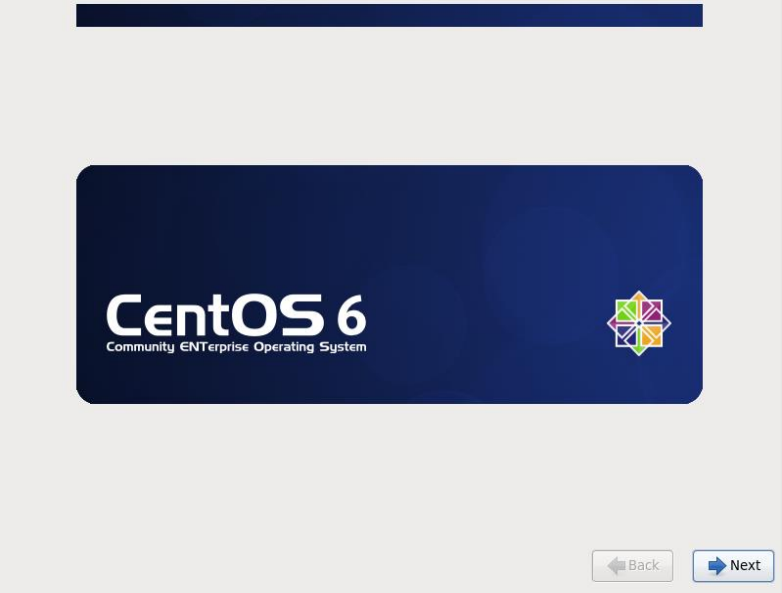


Figura 126. Portada de bienvenida a la Instalación

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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.

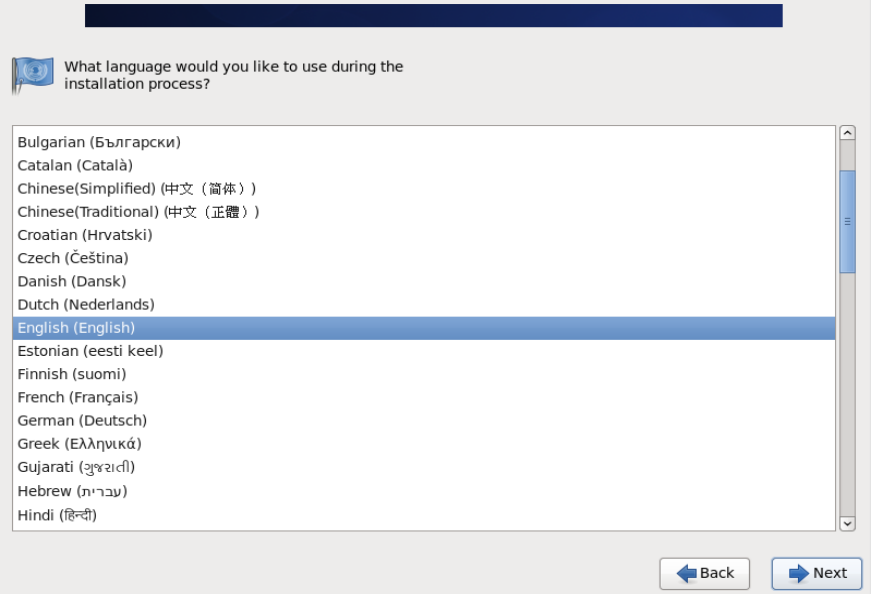


Figura 127. Selección de idioma de instalación

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Se elige la distribución del idioma del teclado que se tiene en el equipo servidor

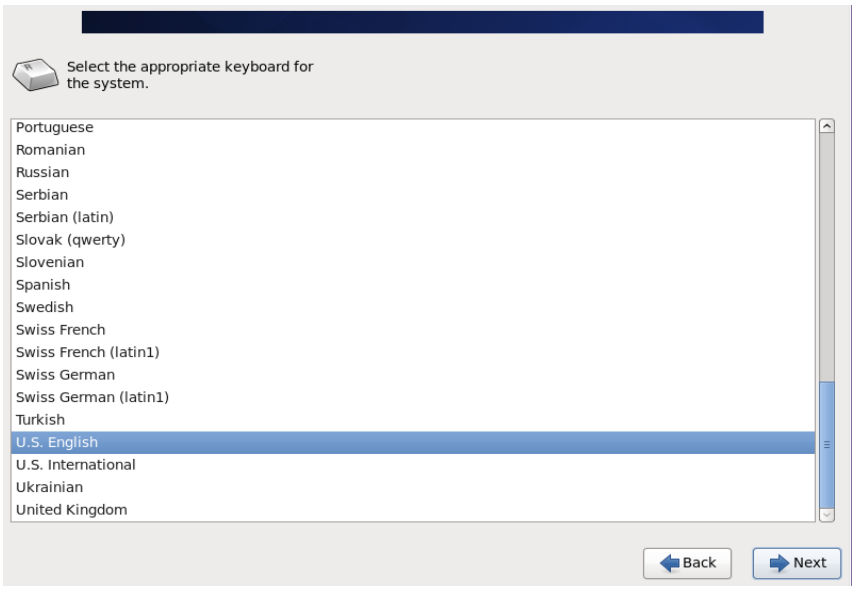


Figura 128. Selección de idioma de teclado

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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

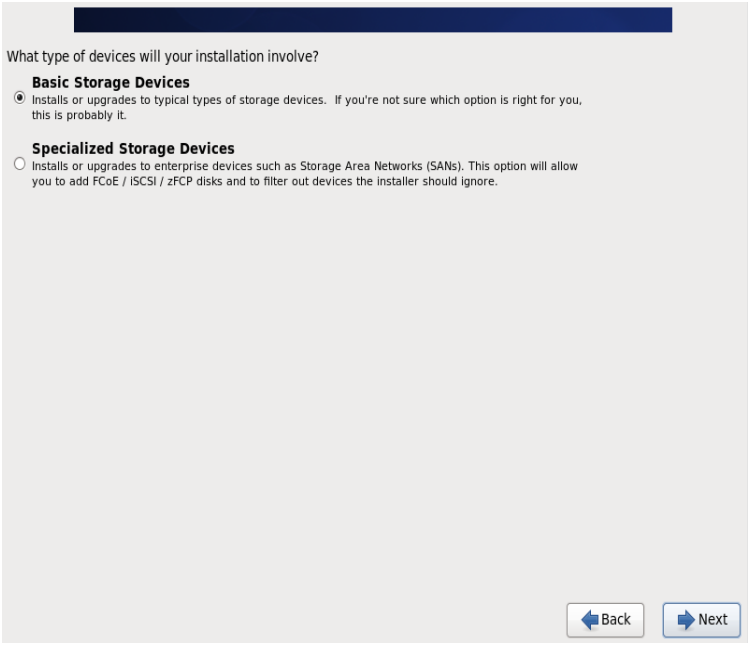


Figura 129. Tipo de dispositivo de instalación

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

En la siguiente ventana se coloca que si descarte todos los datos de la unidad para proceder con la instalación.

Figura 130. Descarte de datos en unidad de disco duro

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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

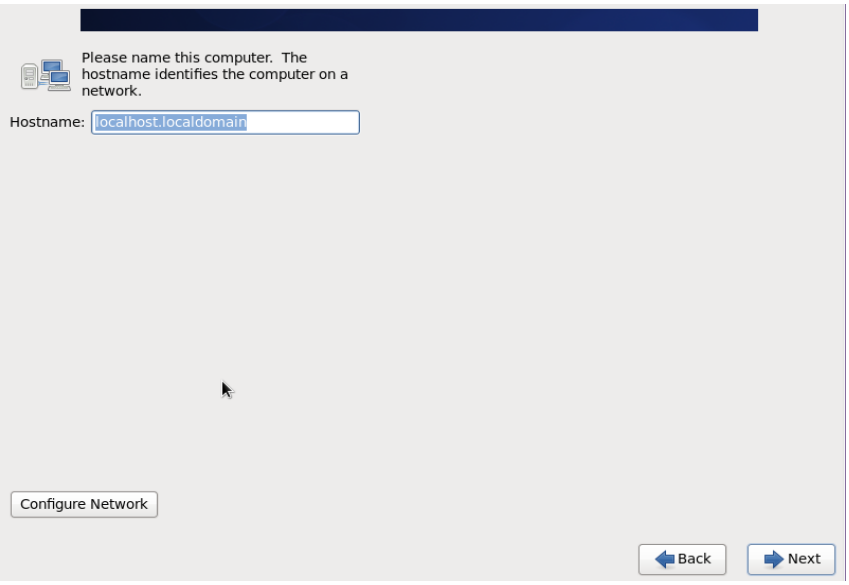


Figura 131. Introducción de nombre del servidor

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Selección de ubicación Geográfica, siguiente.

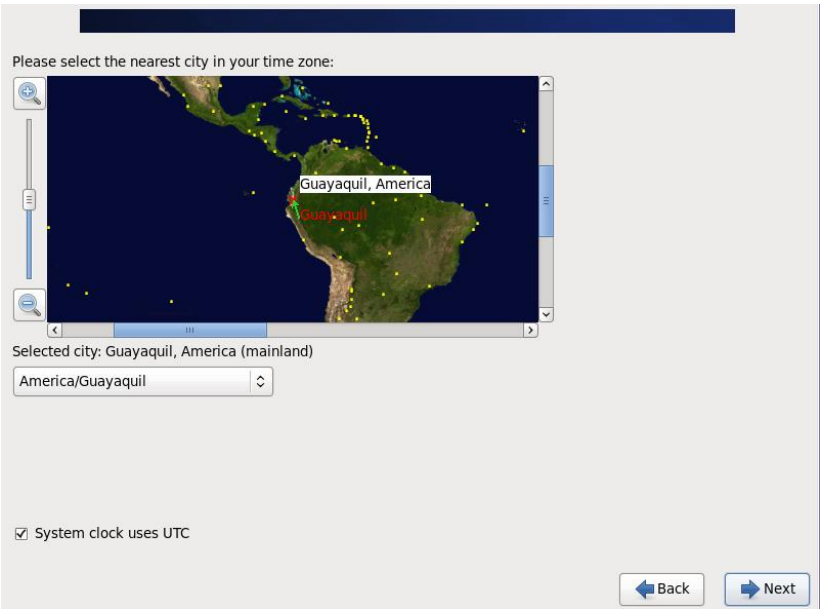


Figura 132. Ubicación Geográfica

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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.

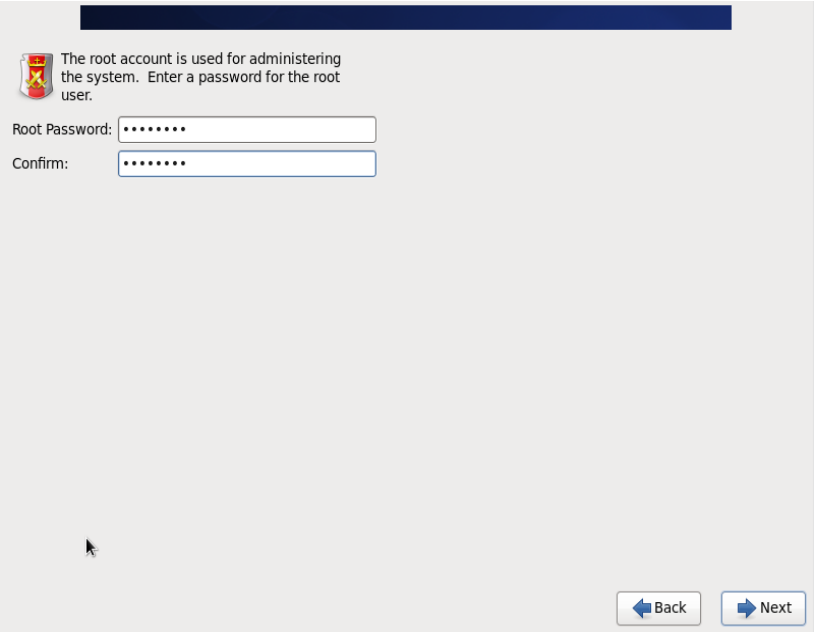


Figura 133. Contraseña de Administrador

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Seleccionamos la forma en que queremos configurar o crear las particiones de disco en las que va a estar ubicado Centos.

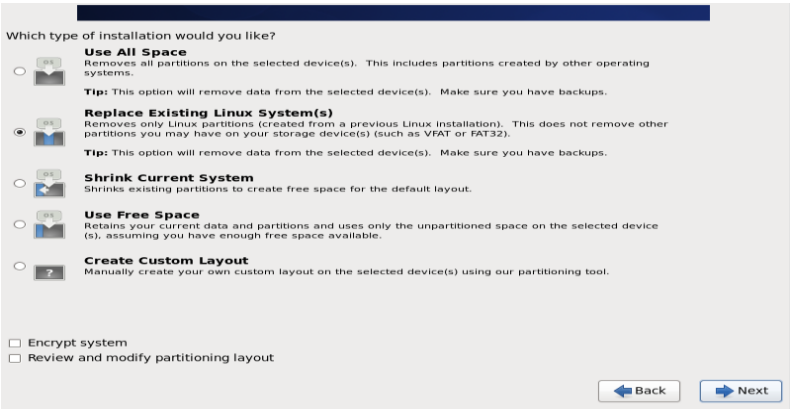


Figura 134. Selección del tipo de instalación

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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

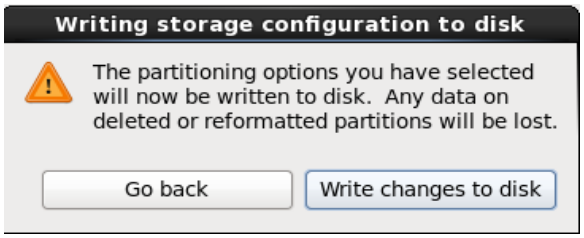


Figura 135. Escribir los cambios en el disco duro

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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.

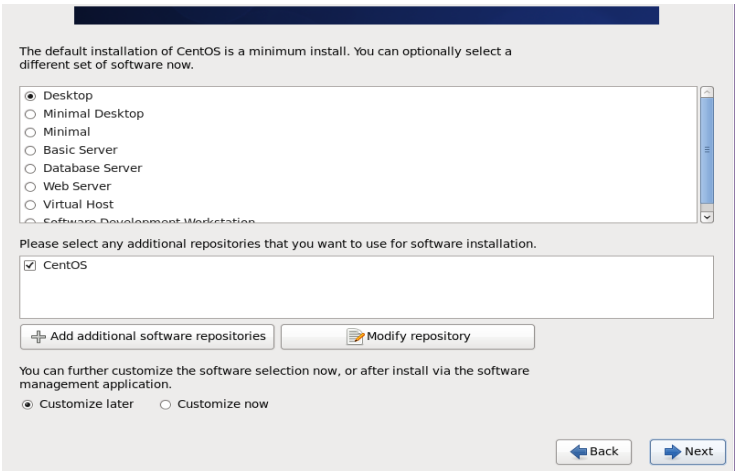


Figura 136. Tipos de instalación de servidor

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Instalación de Centos 6.5 en progreso.

Figura 137. Instalación en progreso

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Reiniciar el servidor para culminar la instalación.

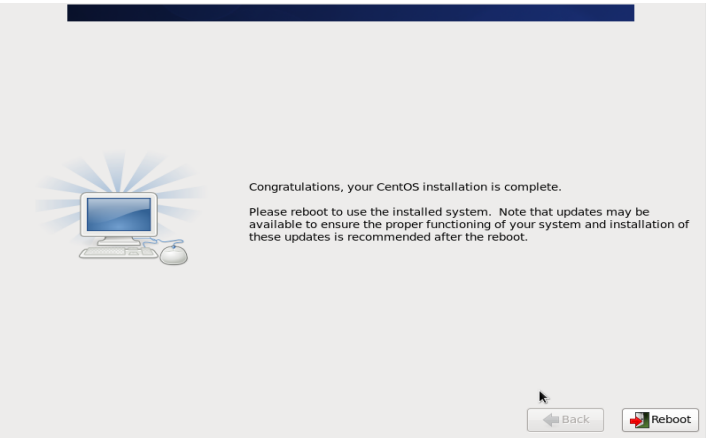


Figura 138. Reinicio de ordenador

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

2. Pantalla de bienvenida cuando se inicia por primera vez el Centos.

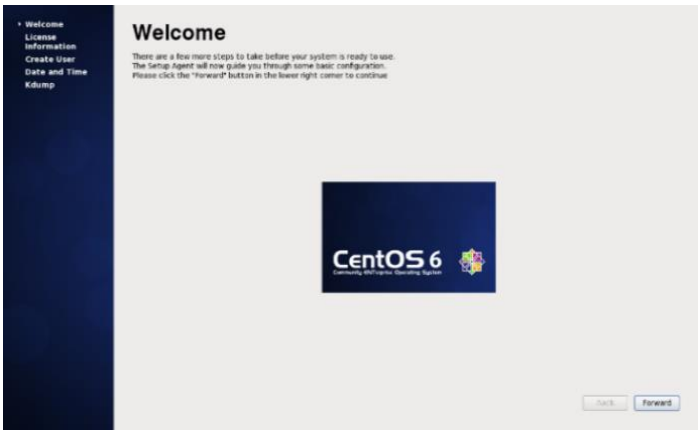


Figura 139. Bienvenida Centos Linux

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Aceptación del contrato de uso del Sistema Operativo.

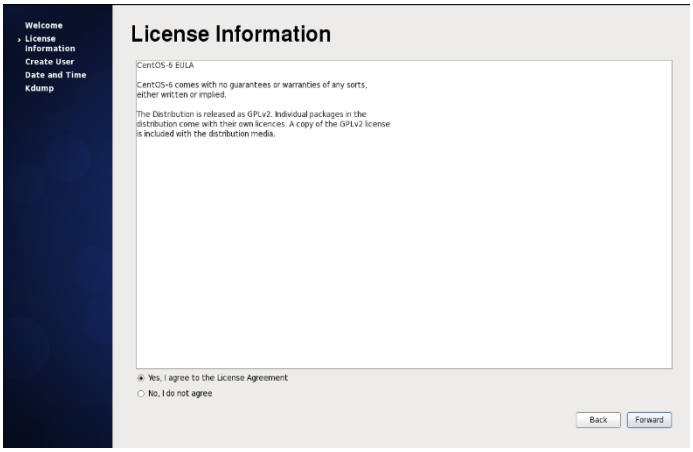


Figura 140. Información de Licencia

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Si se desea se puede crear un usuario o solo utilizar el usuario administrador dando clic en forward.

Figura 141. Creación de Usuario

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Seleccionar la configuración de Fecha y hora

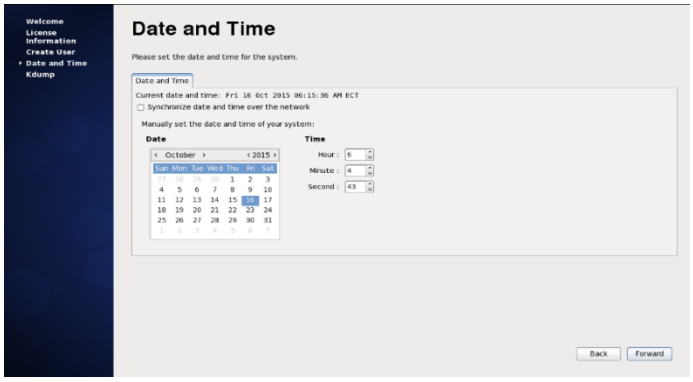


Figura 142. Hora y fecha del Sistema

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Finalización de parámetros de inicio de sesión.

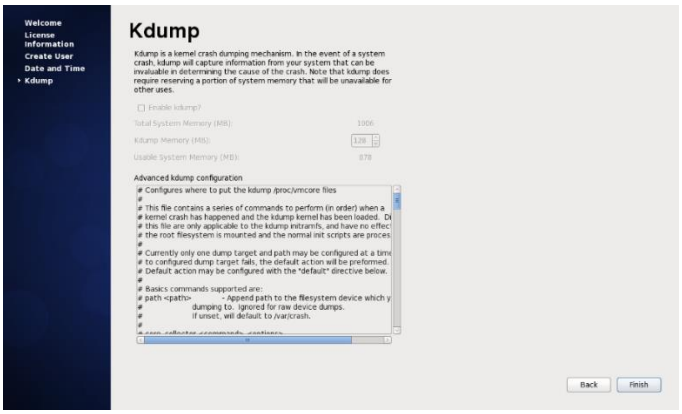


Figura 143. Finalización de configuración de inicio de sesión

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

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

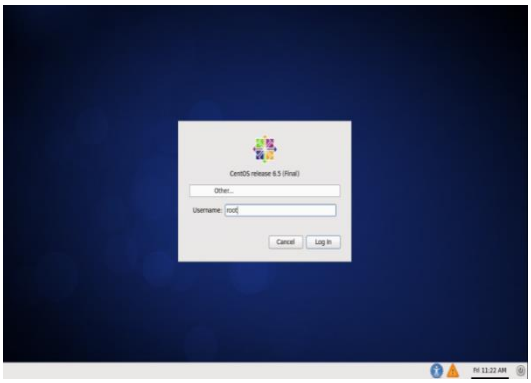


Figura 144. Inicio de sesión

Fuente: Elaborado por Autor, Curso Linux Basico IECEIT

Anexo 2 - Instalación y configuración MySQL

Para instalar MySQL se utiliza el siguiente comando:

yum -y install mysql mysql-server

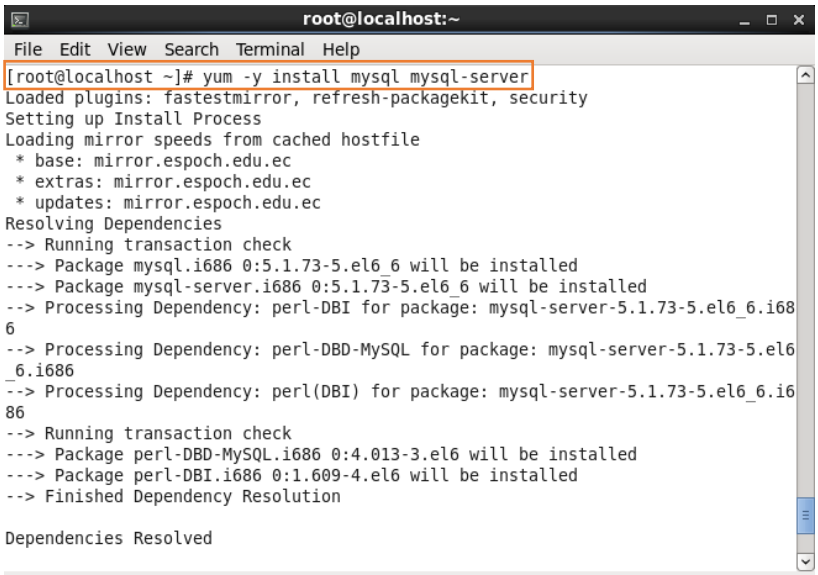


Figura 145. Instalación MySQL server

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Instalación de componentes PHP necesarios para este proyecto.

yum -y install php-mysql php-devel php-pecl-memcache php-pspell php-snmp php-xmlrpc php-xml

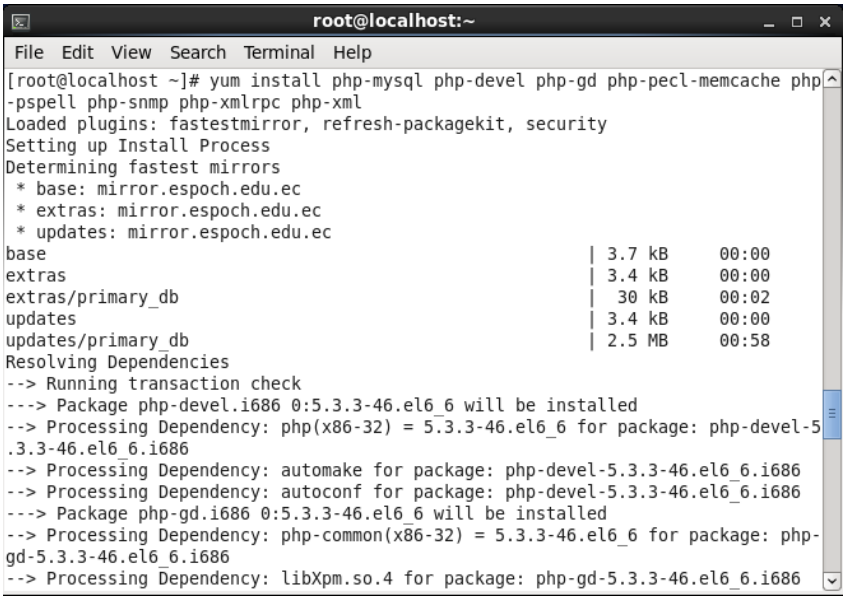


Figura 146. Instalación PHP

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Al terminar la instalación de estos componentes se inicia el servicio de MySQL ejecutando el comando service mysqld start.

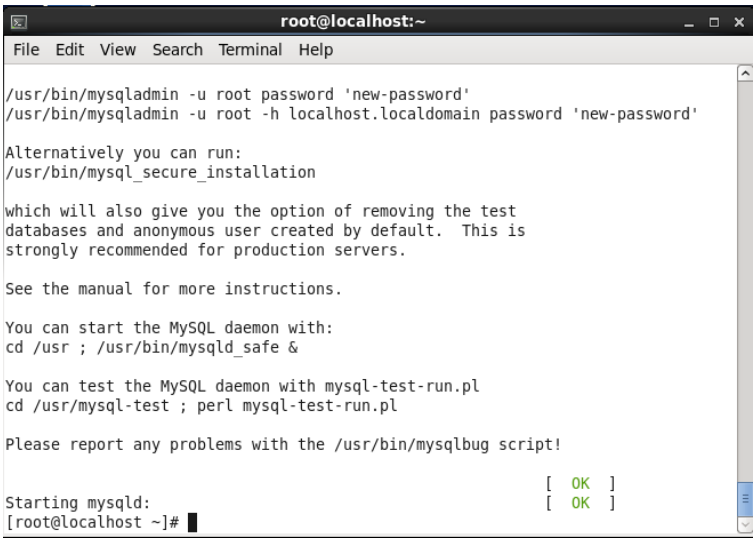


Figura 147. Reinicio de MySQL server

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Configuración de servidor de base de datos se inicia mediante el comando /usr/bin/mysql_secure_installation, Enter para empezar con la configuración, si se desea

agregar una contraseña para el servidor de la base de datos colocamos Y. y escribimos el password.

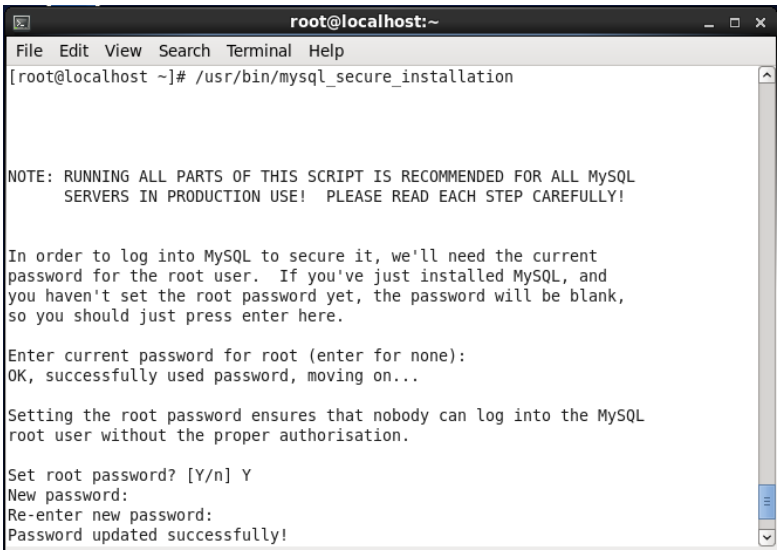


Figura 148. Confiuración de MySQL

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Después siguen las siguientes configuraciones.

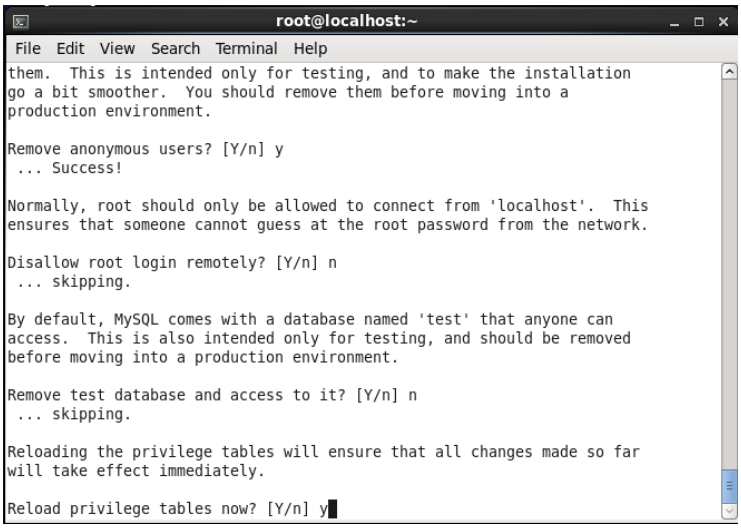


Figura 149. configuraciones de Inicio MySQL

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

El ingreso a MySQL mediante Comando se realiza por:

mysql -u root –p

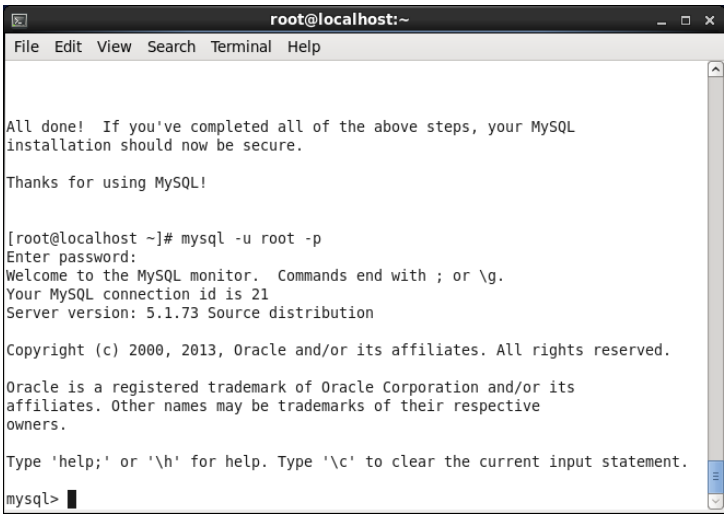


Figura 150. Ingreso a MySQL

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Adentro de MySQL se puede realizar la creación de bases de datos, se necesita al menos una, para iniciar el servidor el portal universitario. Para crear una base de datos se sigue la secuencia de los siguientes comandos

- create database utnwebdb;
- grant usage on *.* to utnwebuser@localhost identified by ‘utnwebpasswd’;
- grant all privileges on utnwebdb. * to utnwebuser@localhost ;

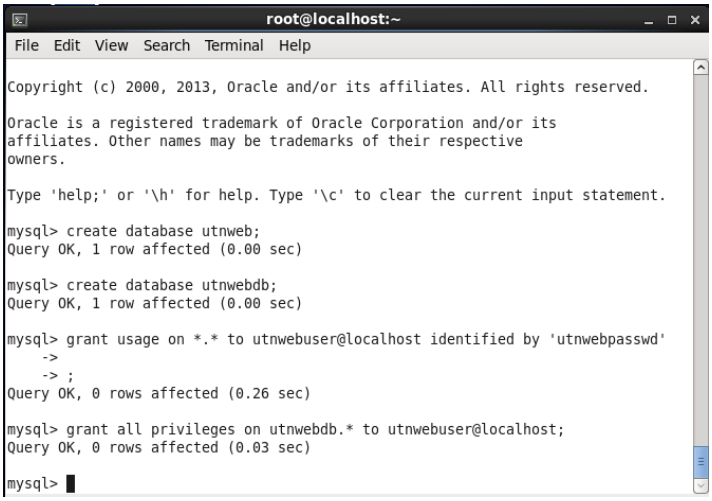


Figura 151. Creación de base de datos en MySQL

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Para realizar la prueba del correcto funcionamiento de la base de datos creada se escribe el siguiente comando:

mysql -u utnwebuser -p'utnwebpasswd' utnwebdb

```
mysql> exit
Bye
[root@localhost ~]# mysql -u utnwebuser -p'utnwebpasswd' utnwebdb
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Figura 152. Comprobación de funcionamiento Base de datos

Fuente: Elaborado por el Autor, Curso Linux Avanzado IECEIT

Para asignar todos los privilegios al usuario root se escribe el comando: *GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost';*

Para que MySQL se ejecute automáticamente con el inicio del sistema se escribe chkconfig --level 2345 mysqld on en el terminal de administrador (root).

Activación de ssl para MySQL

Para empezar la activación de ssl se entra al fichero /etc/my.cnf y se edita agregando las líneas:

Old_passwords=1

ssl

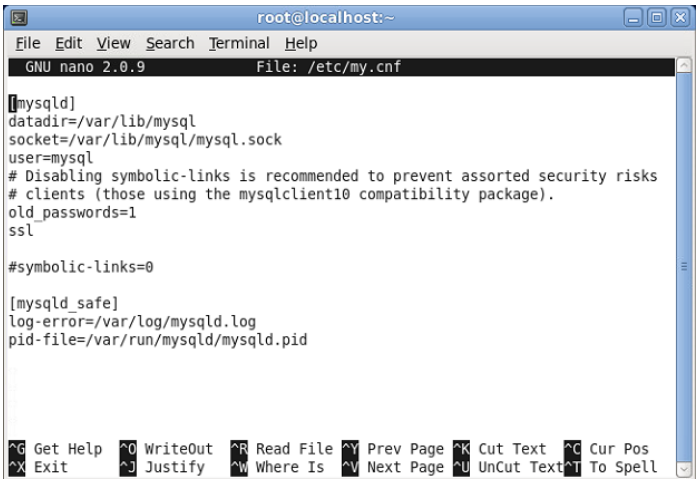


Figura 153. Edición de fichero my.cnf

Fuente: Recuperado de https://www.howtoforge.com/how-to-set-up-mysql-database-replication-with-ssl-encryption-on-centos-5.4

El siguiente paso es reiniciar el servicio de MySQL usando "*service mysqld restart*", al finalizar se realiza la comprobación del servicio entrando a MySQL y ejecutando el comando:

show variables like %ssl%';

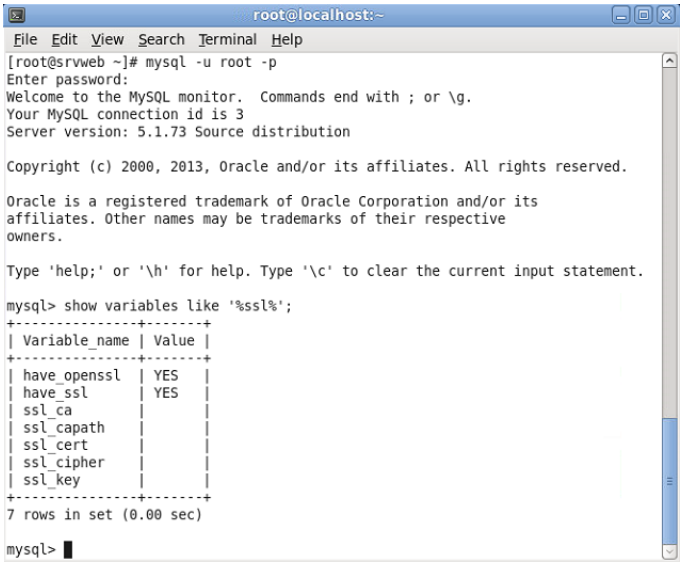


Figura 154. Comprobación de activacion ssl MySQL

Fuente: Recuperado de https://www.howtoforge.com/how-to-set-up-mysql-database-replication-with-ssl-encryption-on-centos-5.4

Anexo 3 – Calculo y Generación de zonas de DNS en IPv6

Para generar un archivo de zona Bind se puede utilizar una herramienta disponible en internet en el enlace *http://rdns6.com/zone*, entre los parámetros que se debe de tener disponibles son: un rango asignado o disponible en IPv6 y el nombre de dominio al cual se quiere realizar la traducción.

Paso 1. Entrar al navegador web preferido e ingresar http://rdns6.com/zone en la barra de navegación en la aplicación.

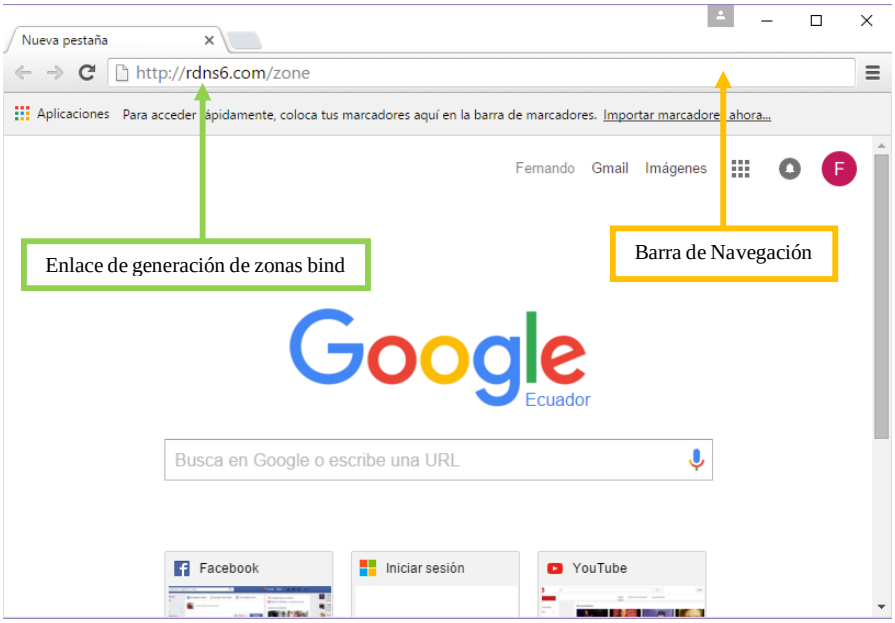


Figura 155. Ingreso a enlace de generación de zonas bind

Fuente: Navegador Google Chrome

Paso 2: Cuando ya se carga el enlace, lo siguiente es llenar los datos de los parámetros necesarios para la generación de la zona, entre los cuales está la dirección de red donde se encuentra el servicio de resolución de nombres (DNS), nombre del dominio, host o servicios que se desea resolver y tiempo de referencia para las acciones del servidor.

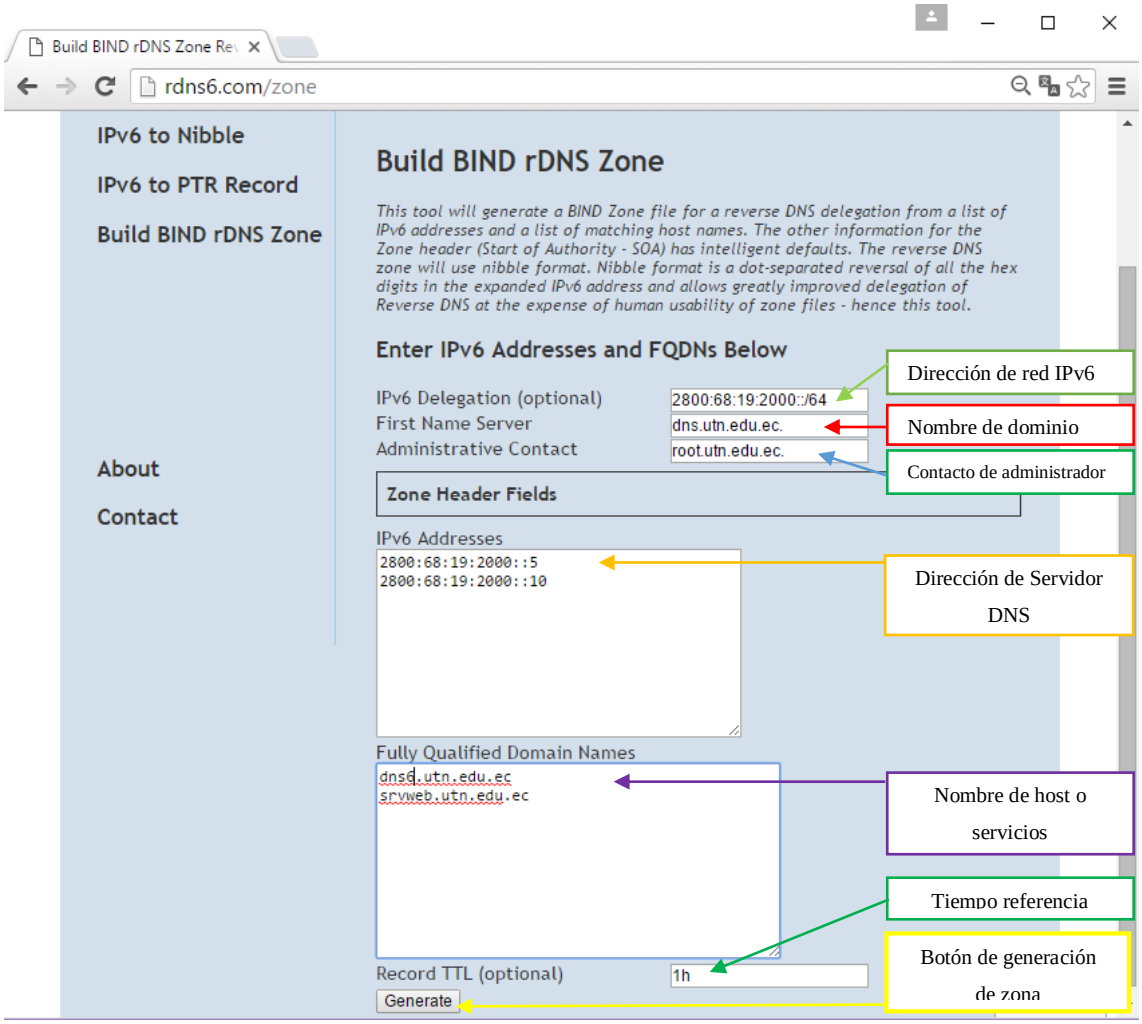


Figura 156. Parametros para generación de zonas bind

Fuente: Recuperado de http://rdns6.com/zone

Al finalizar el ingreso de todos los parámetros solicitados en el formulario de generación de zona se debe presionar el botón “Generate”

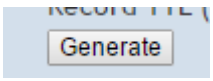


Figura 157. Botón generación de zonas bind

Fuente: Recuperado de http://rdns6.com/zone

La respuesta a la solicitud de generación de zona indica los parámetros de: número de identificación y tiempo de acciones del servidor, dirección IPv6, registro AAAA, Nombre de host o servicio.

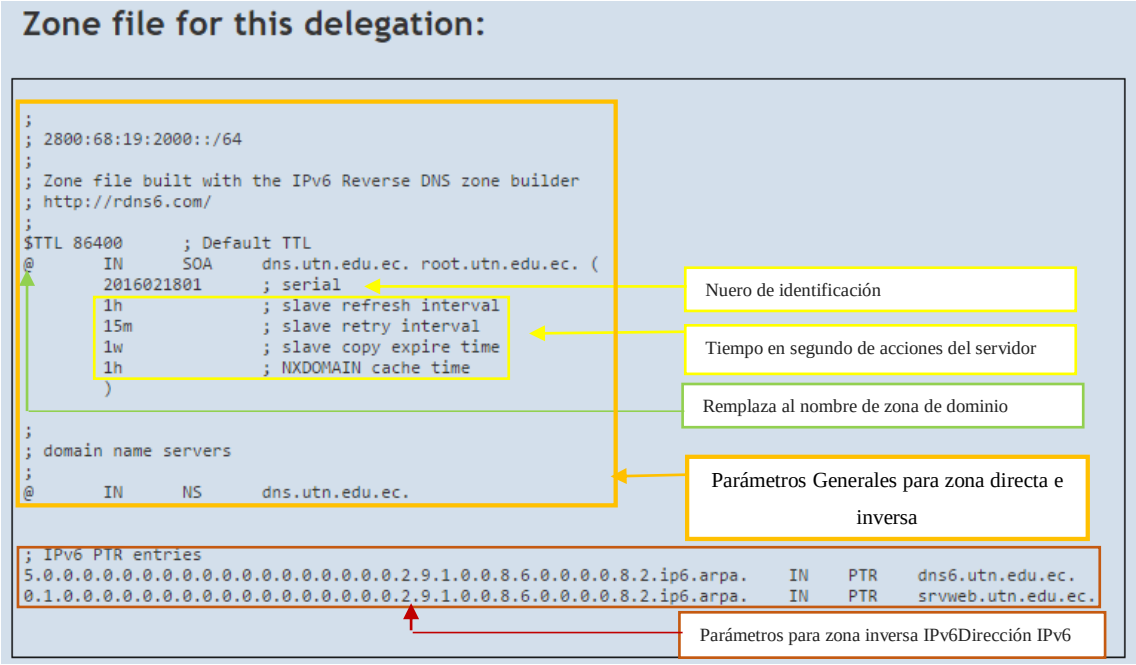


Figura 158. Parametros de Zonas Bind

Fuente: Recuperado de http://rdns6.com/zone

Anexo 4 – Instalación de Wireshark en Centos.

Para instalar wireshark desde la consola de Centos primero se ejecuta el comando *yum install wireshark.x86_64*, de esta manera se instalarán los componentes necesarios para que el software funcione correctamente.

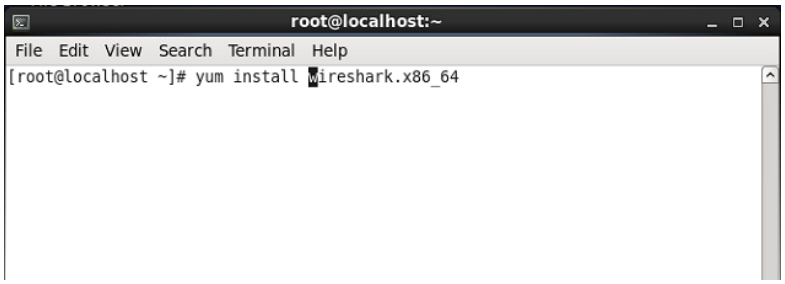


Figura 159. Instalación Wireshark

Fuente: Recuperado de http://centoshowtos.org/network-and-security/wireshark/

Luego se acepta la descarga y la instalación de las dependencias necesarias para wireshark escribiendo la letra Y.

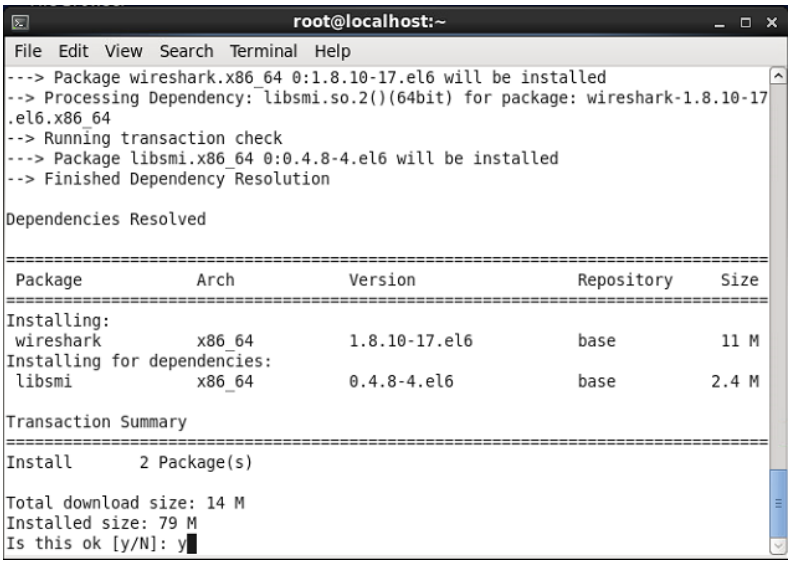


Figura 160. Aceptar instalación wireshark

Fuente: Recuperado de http://centoshowtos.org/network-and-security/wireshark/

Después de instalar los componentes necesarios para el funcionamiento de wireshark se instalará la parte grafica del sniffer introduciendo el comando:

#yum install ethereal-gnome

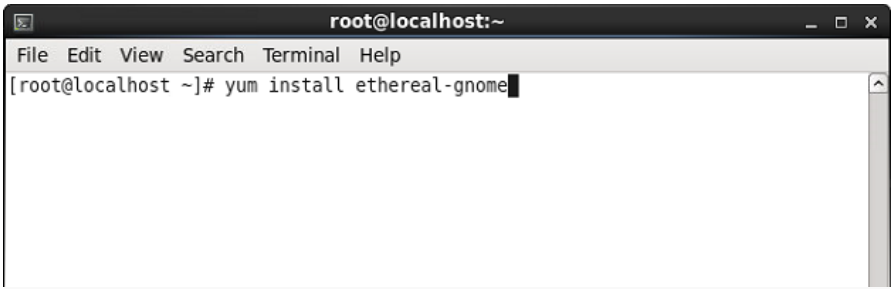


Figura 161. Instalación interface gráfica wireshark

Fuente: Recuperado de http://www.enlinux.org/instalar-wireshark-en-gnulinux-centos-6-de-64-bits/

Luego se acepta la descarga y la instalación de las dependencias necesarias para el entorno grafico de wireshark escribiendo la letra Y.

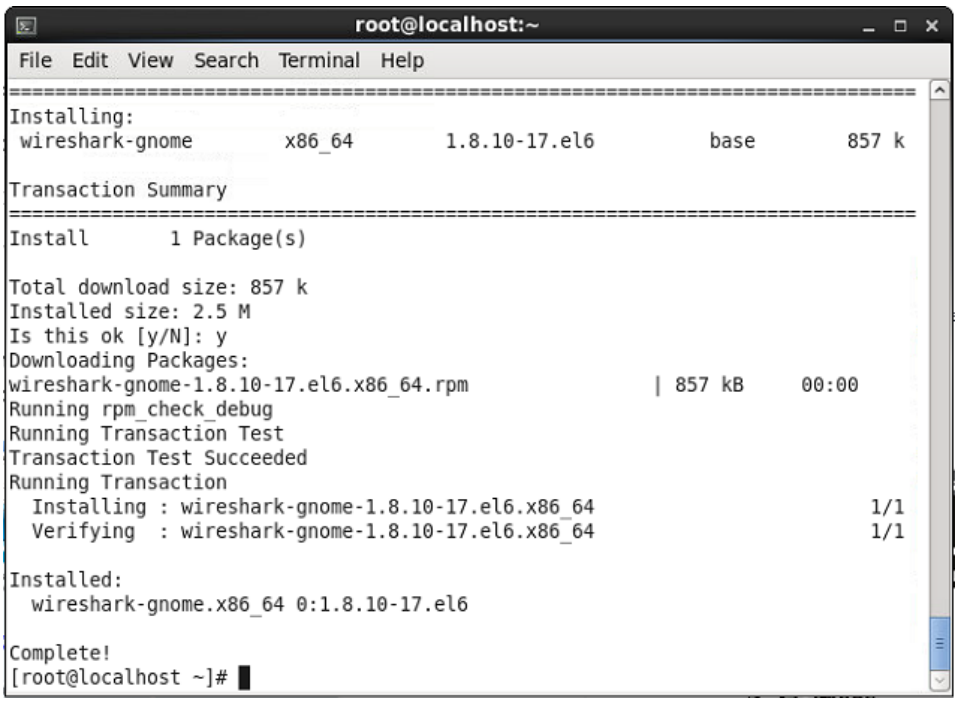


Figura 162. Aceptar instalacion de dependecias entorno grafico wireshark

Fuente: Recuperado de http://www.enlinux.org/instalar-wireshark-en-gnulinux-centos-6-de-64-bits/

El ingreso al analizado de redes wireshark es necesario dirigirse a Aplications ➔ internet ➔ wireshark Network Anayzer

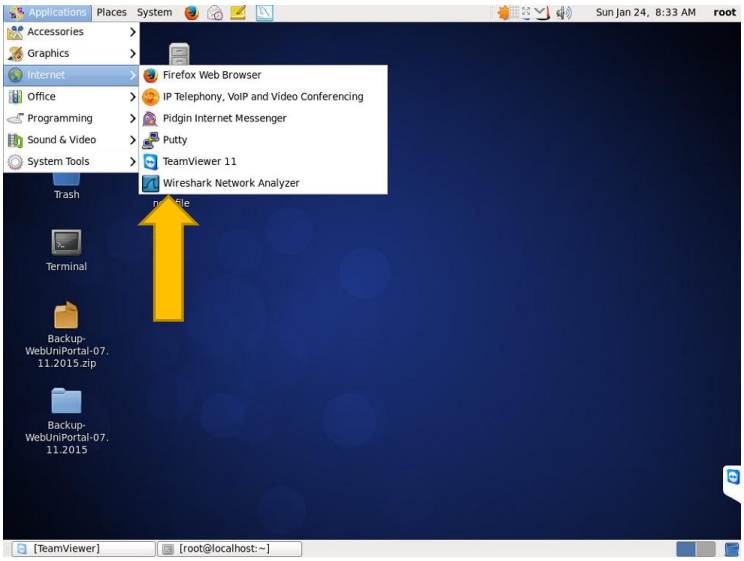


Figura 163. Ingreso a wireshark

Fuente: Recuperado de http://www.enlinux.org/instalar-wireshark-en-gnulinux-centos-6-de-64-bits/

Una vez en el entorno de wireshark se puede escoger la interfaz que se desea analizar, luego de elegir la interfaz se da clic en start (inicio).

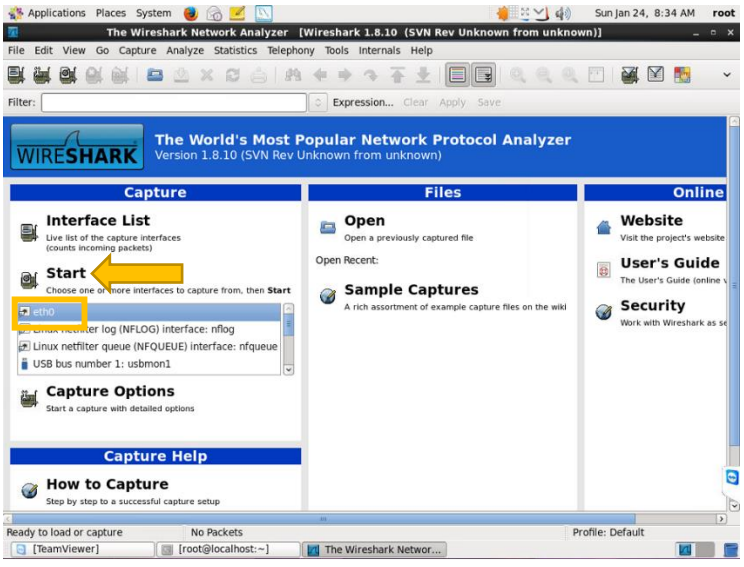


Figura 164. Inicio de analisis con wireshark

Fuente: Recuperado de http://www.enlinux.org/instalar-wireshark-en-gnulinux-centos-6-de-64-bits/

El análisis se puede realizar utilizando varios filtros o visualizar todo el tráfico que se da por la interfaz seleccionada, un ejemplo es utilizar el filtro http para poder analizar el tráfico del servidor web.

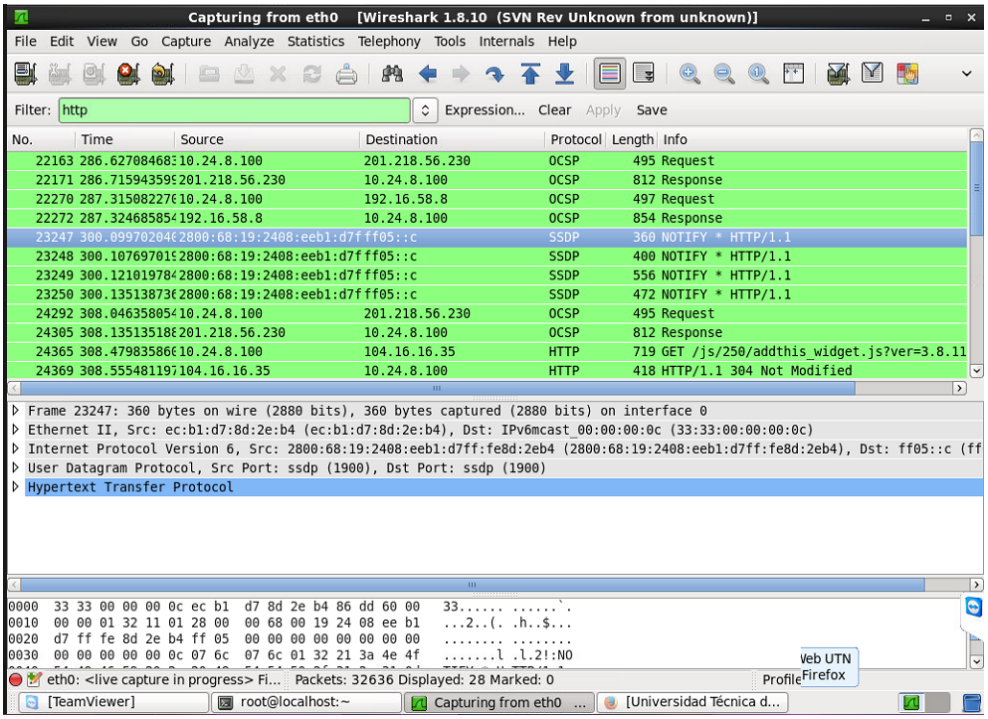


Figura 165. Tráfico http de interfaz seleccionada.

Fuente: Wireshark

Anexo 5 - Configuración de equipos de laboratorio (usuarios)

Los equipos de laboratorio tienen instalado el sistema operativo Windows 10, el cual, si tiene soporte para el funcionamiento del protocolo de internet versión 6, la configuración se realizará de la siguiente manera.

Usuarios IPv4/IPv6

En la parte inferior derecha de la pantalla situar el mause en la sección de configuraciones de red.

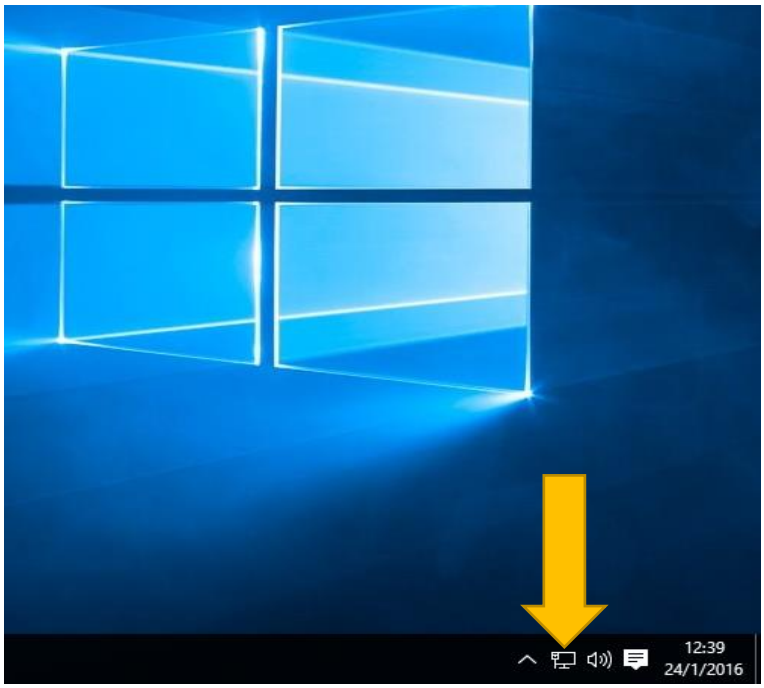


Figura 166. Sección de configuraciones de red

Fuente: Equipo de laboratorio 4 – FICA

Aparece un menú con las opciones de solucionar problemas y abrir el centro de redes y recursos compartidos, clic en la segunda opción.

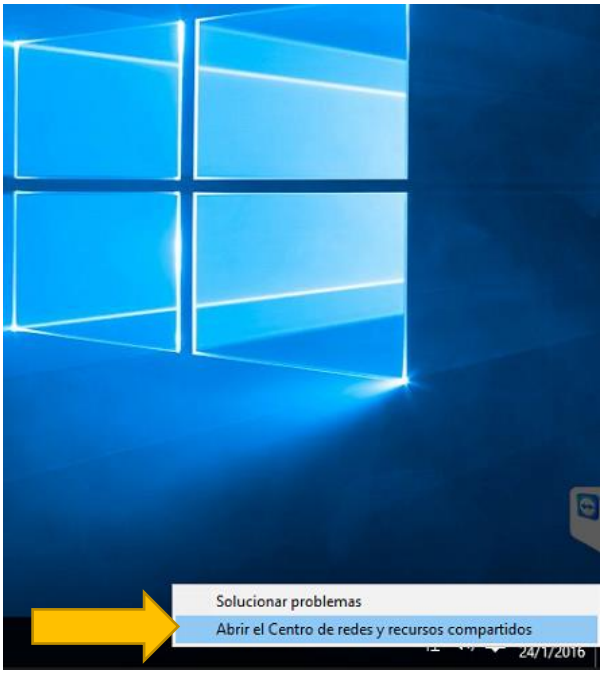


Figura 167. Abrir el Centro de redes y recursos compartidos

Fuente: Equipo de laboratorio 4 – FICA

En la siguiente ventana se elige el adaptador de red en cual se tiene la conexión a la red universitaria.

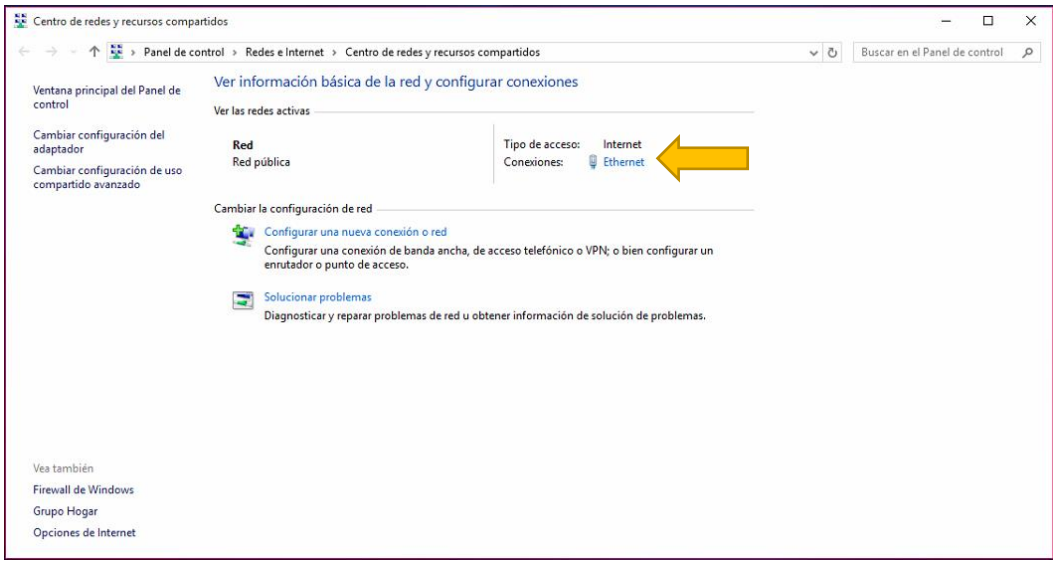


Figura 168. Selección de adaptador de red

Fuente: Equipo de laboratorio 4 – FICA

Para configurar cada uno de los protocolos de internet seleccionar propiedades

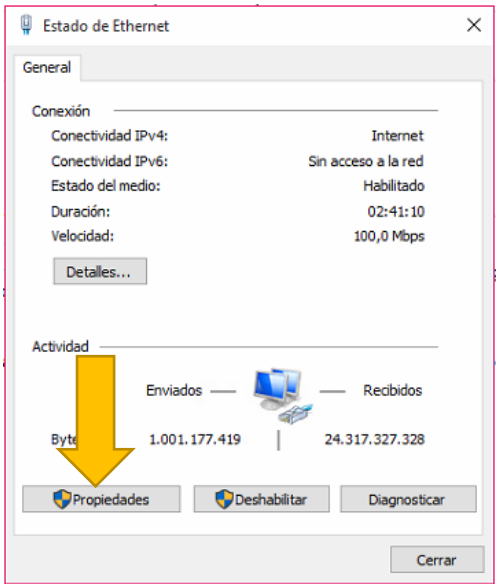


Figura 169. Estado de ethernet

Fuente: Equipo de laboratorio 4 – FICA

En las diferentes opciones que se presentan a continuacion se selecciona protocolo de internet vesión 4 (TCP/IPv4) y clic en propiedades.

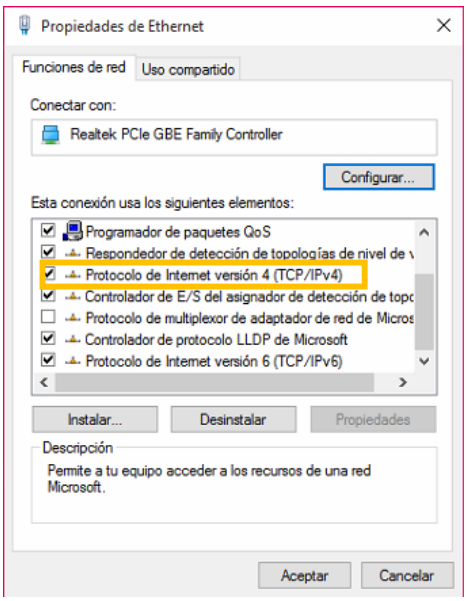


Figura 170. Propiedades Ethernet seleccion Ipv4

Fuente: Equipo de laboratorio 4 – FICA

Los campos de la siguiente ventana se ingresan los parámetros de red correspondientes a la red universitaria correspondiente de laboratorios FICA y clic en aceptar para que se realicen los cambios.

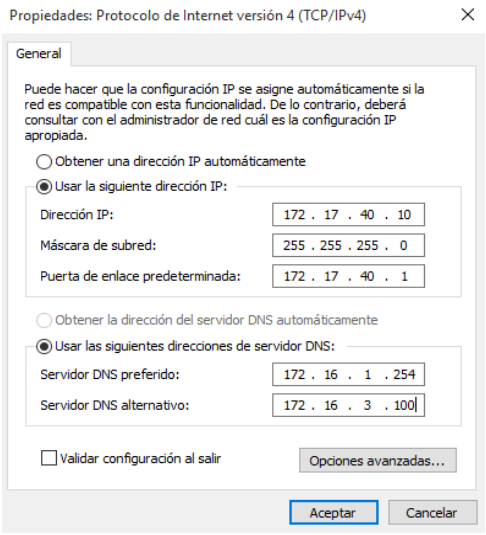


Figura 171. Parametros de red IPv4

Fuente: Departamento de desarrollo tecnológico e informático UTN

Ahora se selecciona protocolo de internet vesión 6 (TCP/IPv6) y clic en propiedades.

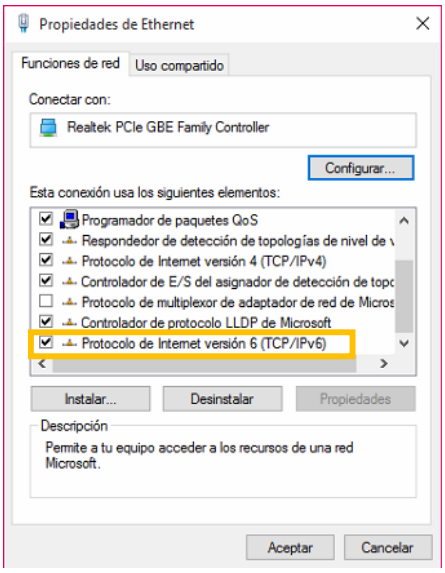


Figura 172. Propiedades Ethernet seleccion IPv6

Fuente: Equipo de laboratorio 4 – FICA

Los campos de la siguiente ventana se ingresan los parámetros de red correspondientes a la red universitaria en ipv6 correspondiente de laboratorios FICA y clic en aceptar para que se realicen los cambios.

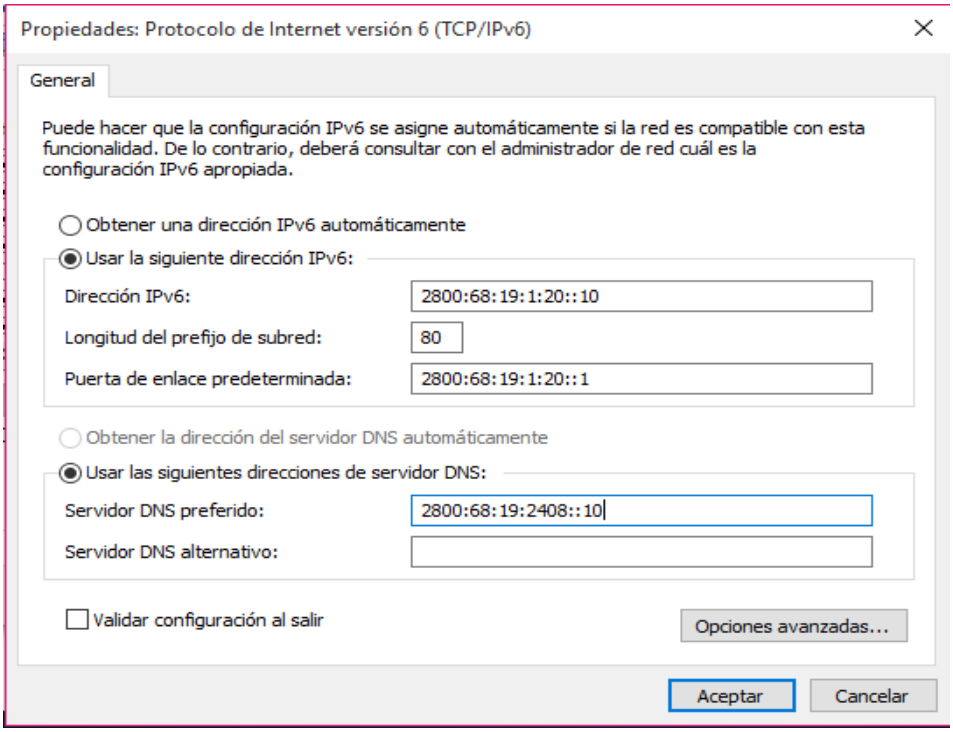


Figura 173. Parametros de red IPv6

Fuente: Departamento de desarrollo tecnológico e informático UTN

Anexo 6 – Cotizaciones de Servicios & equipos

Costo de implementación de mecanismo de transición IPv4 / IPv6

Inprise
SOLUCIONES TECNOLÓGICAS EMPRESARIALES
www.inprise.ec

Inprise

Soluciones Tecnológicas Empresariales
EXPERTOS EN SOFTWARE LIBRE

PROFORMA P-0454

Ibarra, 7 de Abril del 2016

Sr. Fernado Obando Villada

Reciban un cordial saludo por parte de la empresa Inprise Soluciones Tecnológicas Empresariales, líder en la región en sistemas de información y telecomunicaciónes, adjunto a ustedes la propuesta de implementación un mecanismo de transición IPV4 – IPV6. Tomando en cuenta los requerimientos del cliente y previa revision técnica de los equipos a ser configurados.

DETALLES DEL PROYECTO

- Implementacion y configuracion doble pila(IPv4/IPv6)
- Implementacion NAT64/DNS64
- Implementacio y Coniguracion servidor web, transferencia de archivos y DHCP

PRESUPUESTO

INVERSIÓN TOTAL DEL PROYECTO	$ 4000

Se deberá cancelar el 50% de anticipo para iniciar el proyecto.
Este valor no incluye IVA.

Validez de la propuesta

La presente propuesta tiene una validez de 10 días calendario.

Santiago Burbano R.
INPRISE

Dirección: José Miguel Leoro 7-18 y Sánchez y Cifuentes
Teléfonos: 062 610751
E-mail: info@inprise.ec

Costo de equipo Switch CISCO 3750

Figura 174. Switch 3750 12S-S

Fuente: Recuperado de http://articulo.mercadolibre.com.ec/MEC-408630235-switch-de-fibra-catalyst-3750x-12-puertos-ge-sfp-ip-base-_JM

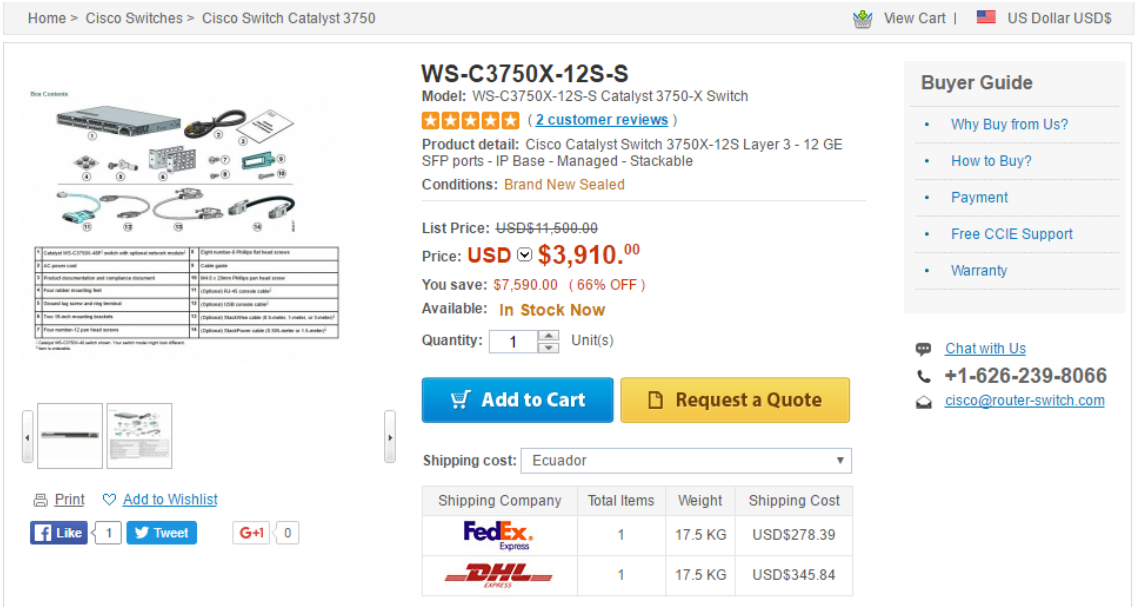


Figura 175. Switch 3750 12S-S

Fuente: Recuperado de http://www.router-switch.com/ws-c3750x-12s-s-p-4381.html

Costo de equipo CISCO ASA 5520 Series

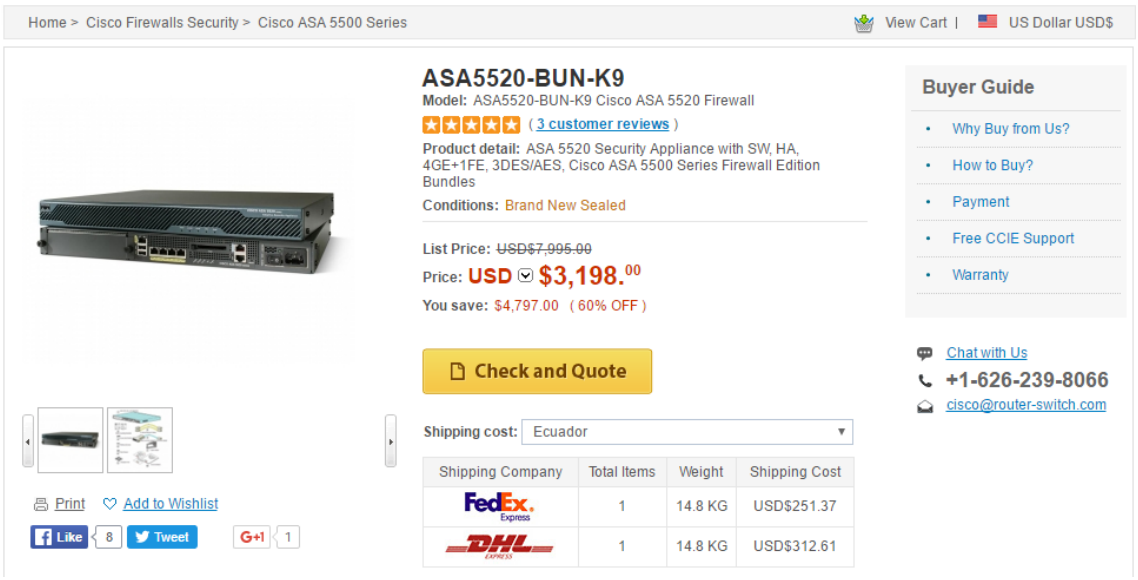


Figura 176. CISCO ASA 5520 Series

Fuente: Recuperado de http://www.router-switch.com/asa5520-bun-k9-p-626.html

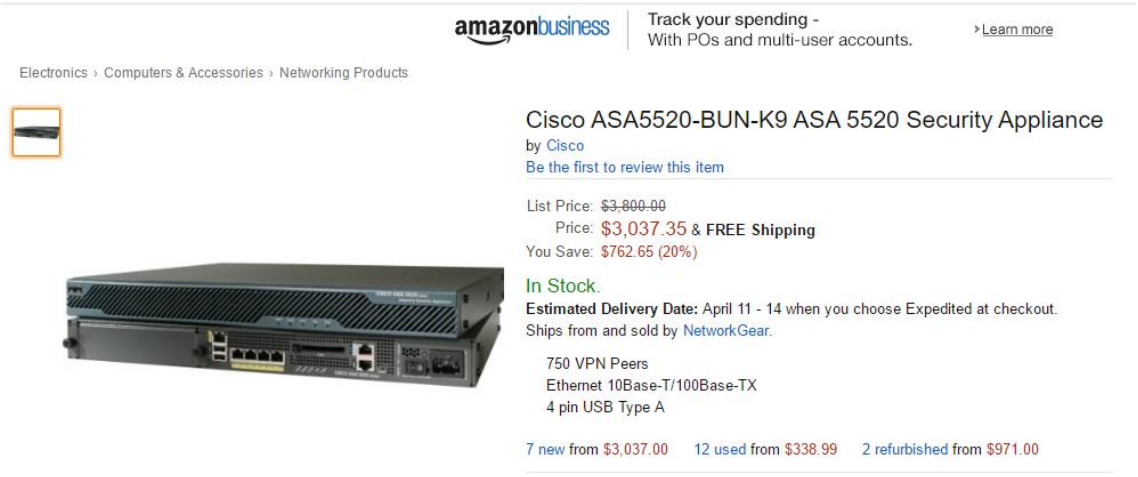


Figura 177. CISCO ASA 5520 Series

Fuente: Recuperado de http://www.amazon.com/Cisco-ASA5520-BUN-K9-5520-Security-Appliance/dp/B006VYY7HG/ref=pd_sim_sbs_147_1?ie=UTF8&dpID=41dLL0ZReRL&dpSrc=sims&preST=_AC_UL160_SR160%2C160_&refRID=1ZVP1NY5PCKZKQN07KPM

Costo de equipo CISCO NEXUS 5548

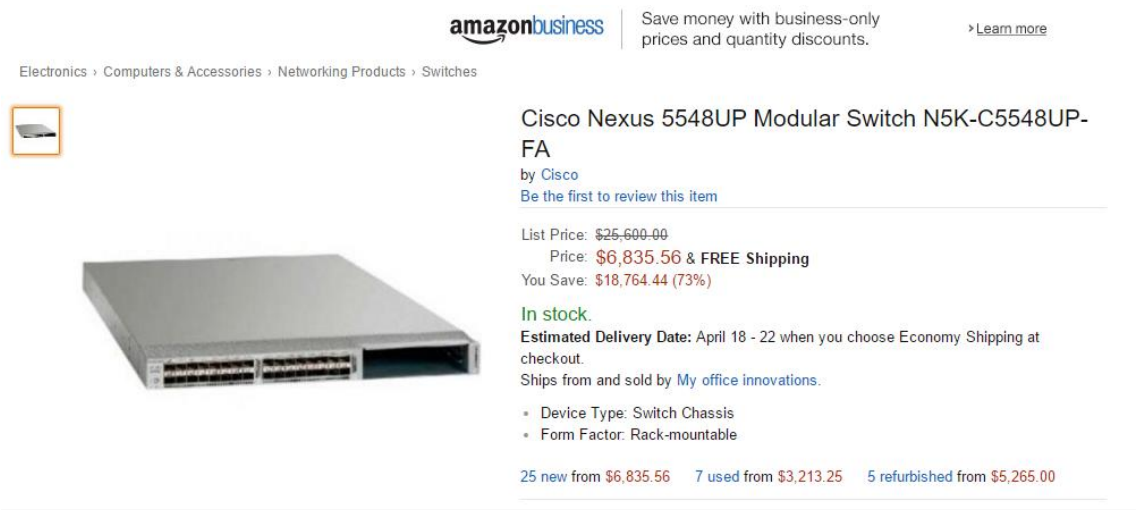


Figura 178. Costo de equipo CISCO NEXUS 5548

http://www.amazon.com/Cisco-5548UP-Modular-Switch-N5K-C5548UP-FA/dp/B004YWLDVU

Figura 179. Costo de equipo CISCO NEXUS 5548

http://www.ebay.com/itm/NEXUS-5548-UP-CHASSIS-Cisco-N5K-C5548UP-FA-/301905834982?hash=item464afd73e6

Costo de equipo Switch The Core Catalys 4510R+E/4500 + E Series

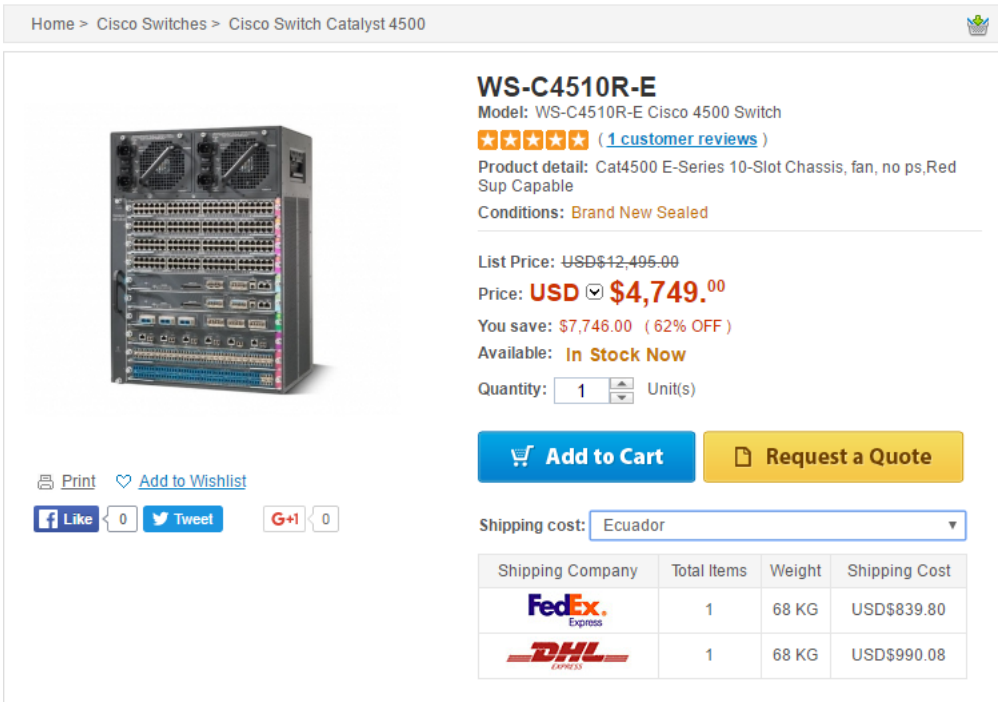


Figura 180. Costo de equipo Switch The Core Catalys 4510R+E/4500 + E Series

http://www.router-switch.com/ws-c4510r-e-p-517.html

Figura 181. Costo de equipo Switch The Core Catalys 4510R+E/4500 + E Series

http://www.amazon.com/Cisco-Catalyst-4510R-Rack-Mountable-Networking/dp/B00VQQKREQ/ref=sr_1_fkmr1_2?s=pc&ie=UTF8&qid=1460303703&sr=1-2-fkmr1&keywords=Switch+Catalys+4510R

Costo Equipo servidor Blade hp proliant BL460c GI

Figura 182. Costo Equipo servidor Blade hp proliant BL460c GI

http://www.ebay.com/itm/HP-Proliant-C7000-Chassis-16x-BL460C-G1-Blade-Server-Barebone-/350891719510?hash=item51b2c6bb56:g:gMEAAOSwB4NW0N~J

Figura 183. Costo Equipo servidor Blade hp proliant BL460c GI

http://www.ebay.com/itm/HP-Proliant-C7000-Chassis-8x-BL460C-G8-Blade-8-CORE-E5-2660-16GB-256GB-SSD-/131578140432?hash=item1ea2ab1710:g:5UQAAOSwzgRW11ru