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

F. Obando Autor, C. Vásquez Director
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte
Ibarra, Ecuador
cmobandov@utn.edu.ec cavasquez@utn.edu.ec

Resumen—El presente proyecto 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 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 have been realized in the devices from FICA's network.

Índice de Términos — IPv4, IPv6, Transición, Doble pila lite, DNS64, NAT64, CEDIA.

I. INTRODUCCIÓN

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.

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.

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.

II. CONCEPTOS BÁSICOS

Un protocolo de internet es un método de transmisión de datos por una red. Los datos enviados se dividen en datagramas (paquetes) individuales e independientes, cada usuario o dispositivo final (host) tienen como mínimo una dirección que lo distingue de otros usuarios, de tal manera cada paquete tiene una dirección origen y destino (emisor y receptor). Actualmente existen dos protocolos de internet operables, IPv4 e IPv6.

A. 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.

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 1)

Figura 1. Cabecera de un datagrama Internet

• 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.

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 2) 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)

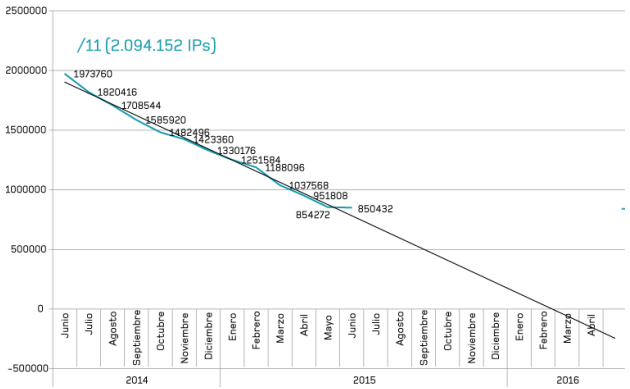


Figura 2. Proyección de agotamiento lineal -Fase 2

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).

B. Protocolo de internet versión 6 (IPv6)

El protocolo de internet versión 6 con una longitud de 128 bits, tiene una disponibilidad de 340 sixtillones de direcciones aproximadamente, además este protocolo maneja términos de 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, además, 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 se diseñó 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)

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 3)

Figura 3. Estructura paquete IPv6

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 4)

Figura 4. Cabecera IPv6

- 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 5). (Cabellos, 2004)

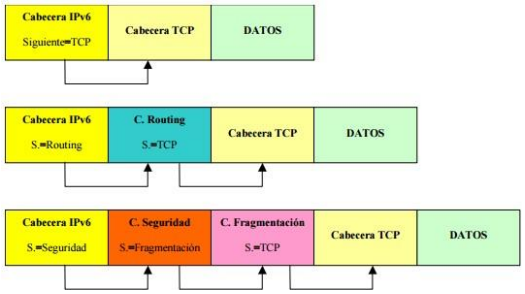


Figura 5. Extensión de cabeceras

1) 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.

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. (Figura 6)

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

Figura 6. Sintaxis de direcciones IPv6

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 (Figura 7). (R. Hiden, S. Deering, 2003)

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

Figura 7. Forma alternativa en entornos mixtos de nodos IPv4 e IPv6

2) 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 8)

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.

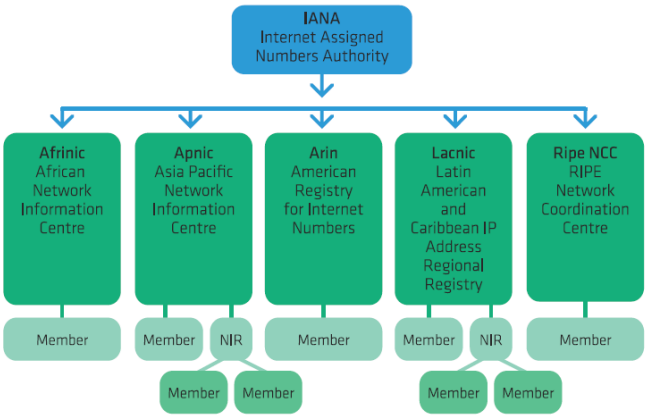


Figura 8. Modelo IANA – RIR

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)

3) 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)

4) 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

5) 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.

6) 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 1)

Tabla 1. Empresas con implementación IPv6

EMPRESA / INFRAESTRUCTURA	SOPORTE DE IPv6 NATIVO	COMENTARIOS

NAP.EC	SI	Punto de intercambio de tráfico local de Internet (IXP) del Ecuador. Administrado por AEPROVI.
Transnexa	SI	Proveedor de servicios portadores incluyendo tránsito internacional de Internet.
Telconet	SI	Proveedor de servicios portadores incluyendo tránsito internacional de Internet.

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 2). (AEPROVI, s.f.)

Tabla 2. 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

C. 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.

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 9). (ACOSTA, y otros, 2014)

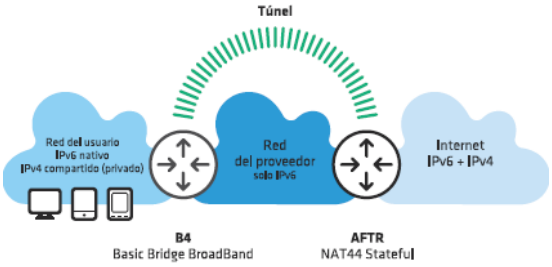


Figura 9. DS-LITE

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

2) 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 10)

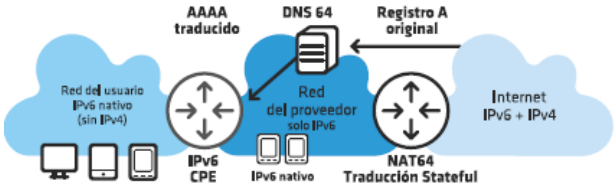


Figura 10. DNS64 y NAT64

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)

D. 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)

1) 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 11)

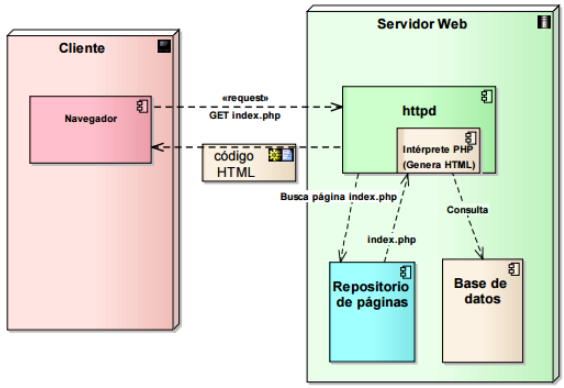


Figura 11. Esquema de Funcionamiento de servidor web

2) 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 12)

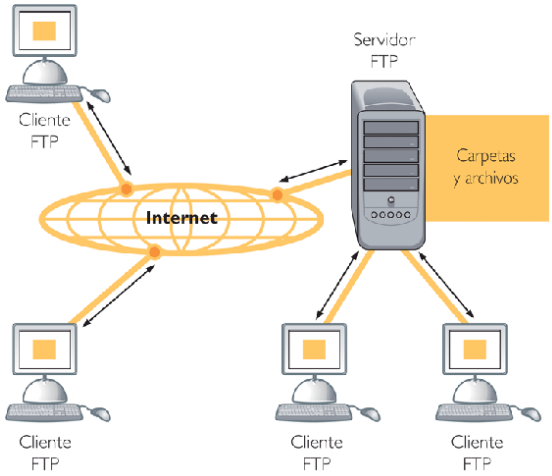


Figura 12. Funcionamiento de FTP

E. 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.

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 13. Centos 6.5

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)

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.

III. DESARROLLO DE LA TECNOLOGÍA DE TRANSICIÓN

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.

A. 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 14)

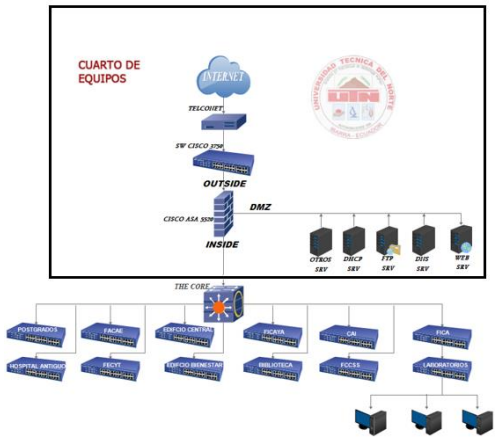


Figura 14. Topología de Red UTN

B. *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.

C. *Configuración de red IPv4/IPv6 en Centos 6.5*

Para configurar la interface de red ingresamos al fichero siguiente:

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

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.

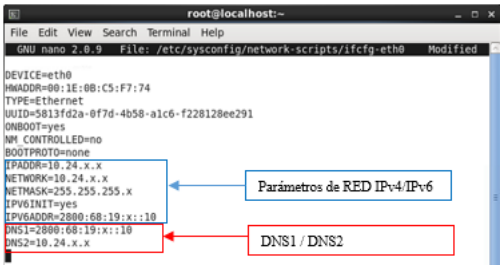


Figura 15. Configuración interfaz de red

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,

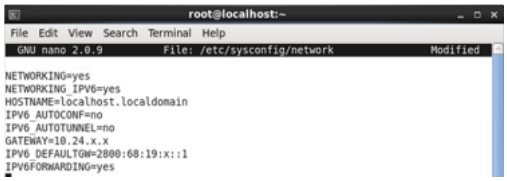


Figura 16. Habilitación de IPv6

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

#service network restart

D. *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

1) *Levantamiento de servicio DHCP en IPv6*

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

#yum install dhcp

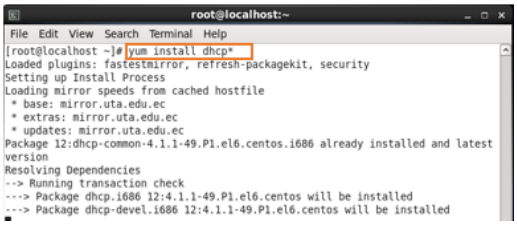


Figura 17. Instalación Paquete dhcp

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

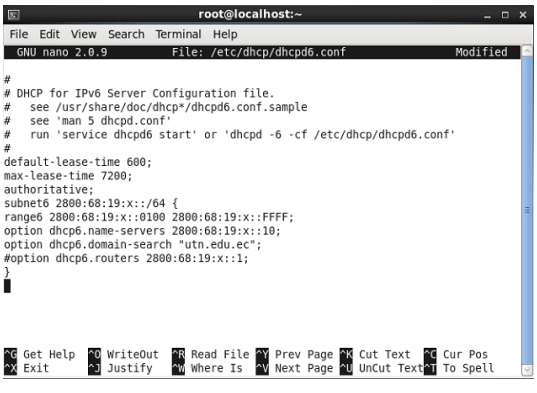


Figura 18. Fichero dhcpd6.conf

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

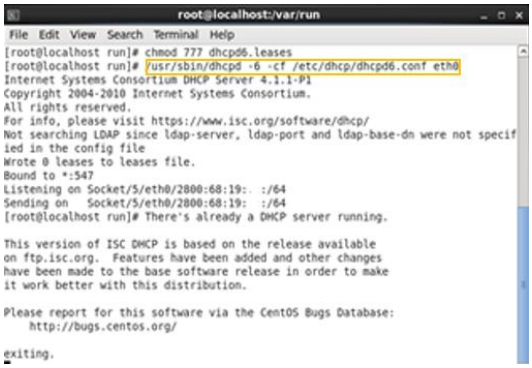


Figura 19. Iniciar el servicio dhcp en IPv6

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

2) 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.

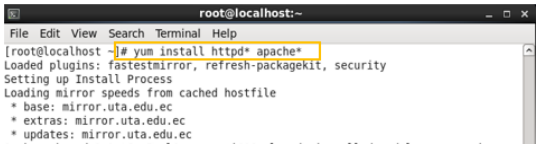


Figura 20. Instalación de httpd y Apache

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

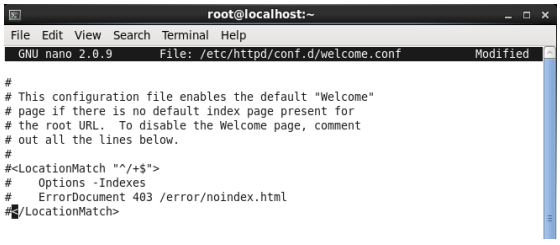


Figura 21. Archivo welcome.conf

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

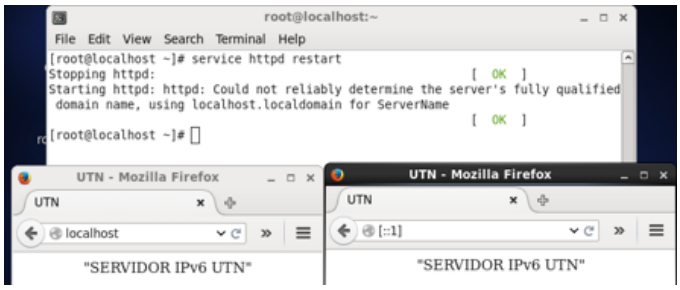


Figura 22. Prueba de funcionamiento servidor Web

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

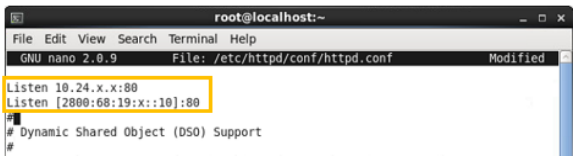


Figura 23. Direccionamiento IPv6 de servidor Web

Se debe salir del editor y se procede a reiniciar el servicio
#service httpd restart

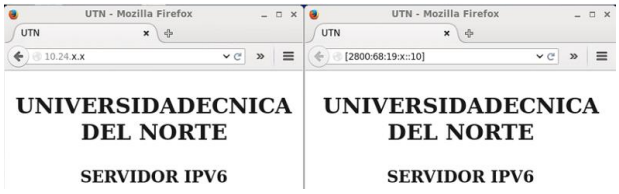


Figura 24. Prueba de funcionamiento por IP de servidor Web

3) 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

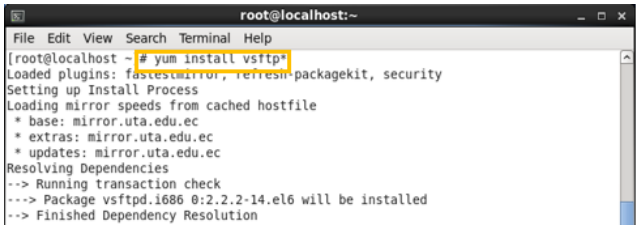


Figura 25. Instalación servidor FTP

Inicialización del servicio ftp se hace mediante el comando "service vsftpd start"

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

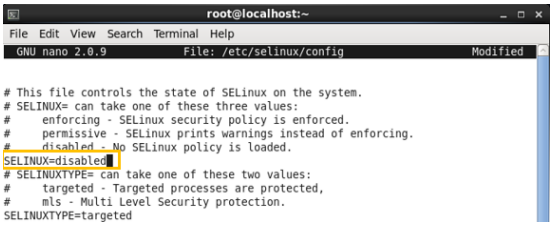


Figura 26. Archivo de configuracion Selinux

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

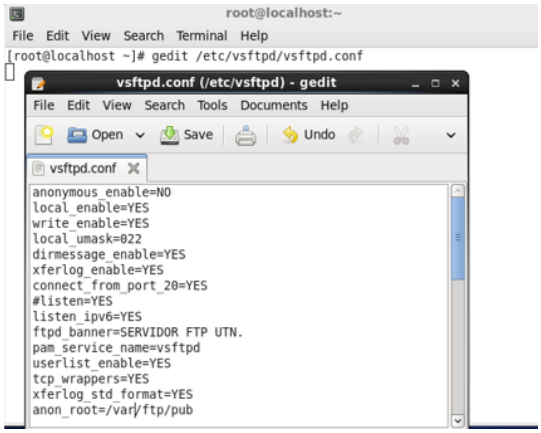


Figura 27. Configuración de archivo vsftpd.conf

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.

#service vsftpd restart

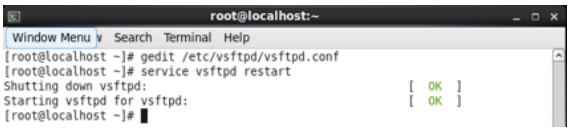


Figura 28. Reinicio de servidor vsftpd.conf

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.

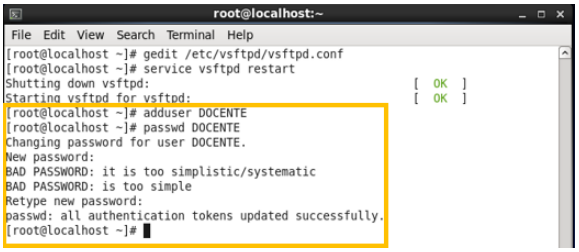


Figura 29. Creación de usuarios y asignación de contraseña

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.

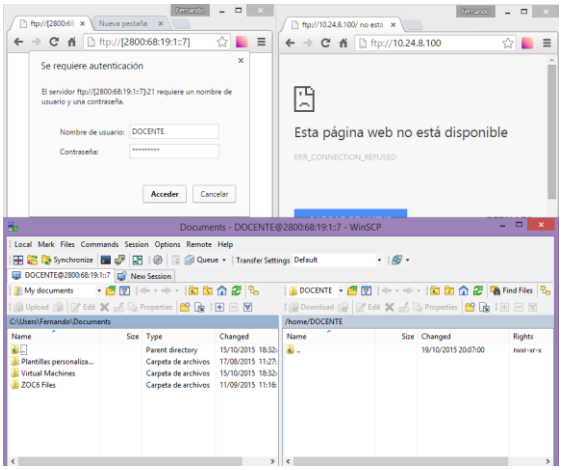


Figura 30. Acceso a servidor FTP

4) 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

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.

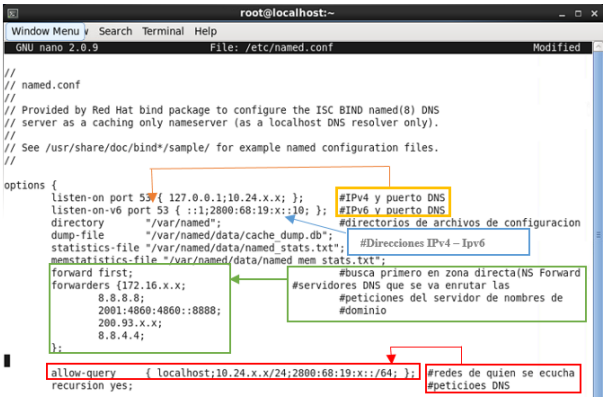


Figura 31. Direccionamiento servidor DNS64

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.

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.

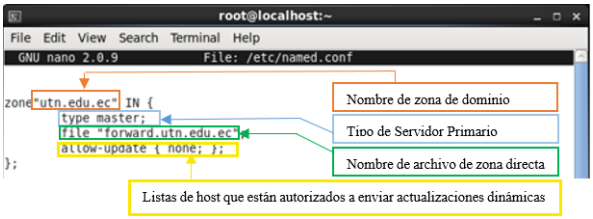


Figura 32. Zona directa en named.conf

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.

La zona directa tiene el siguiente contenido y se crea utilizando el siguiente comando:

nano /var/named/forwad.utn.edu.ec

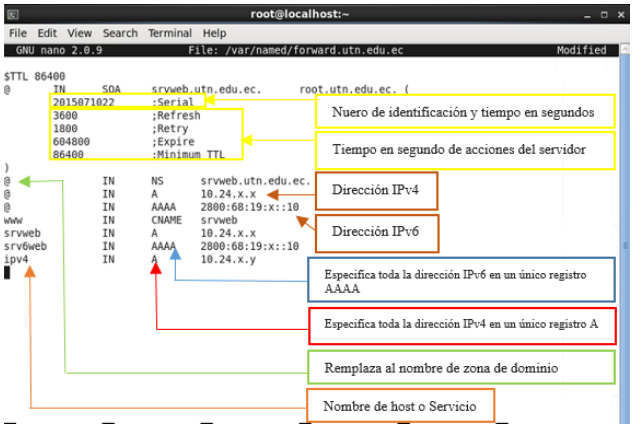


Figura 33. Zona directa DNS64

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

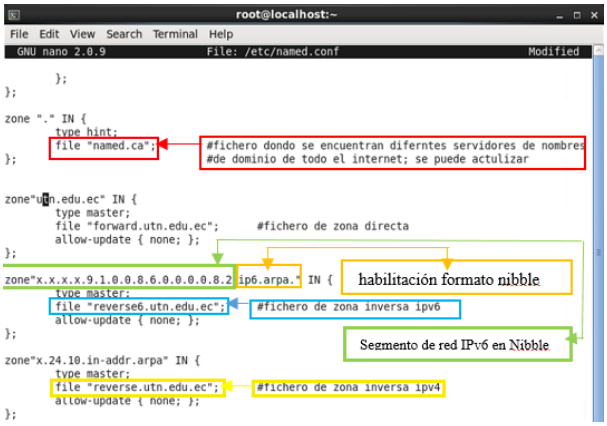


Figura 34. Zonas Inversas en named.conf

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.

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

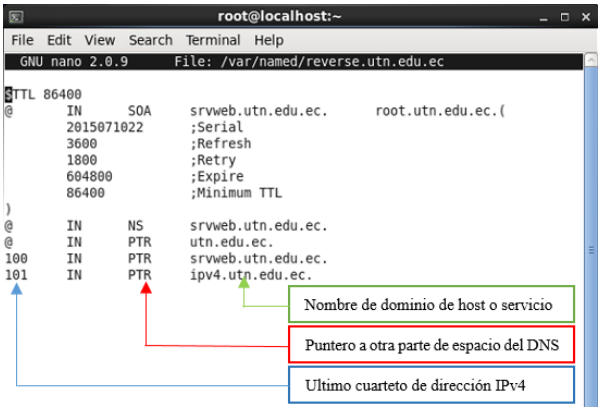


Figura 35. Zona inversa DNS64

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

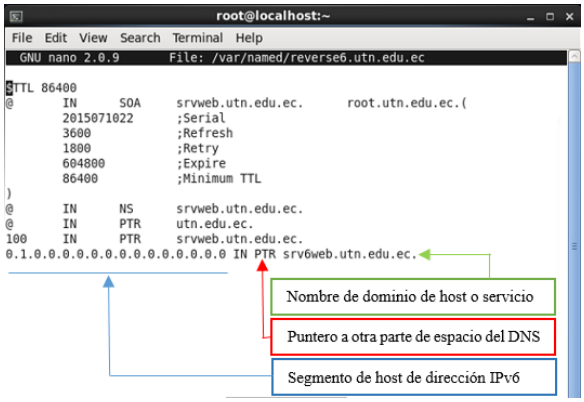


Figura 36. Zona inversa6 DNS64

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

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

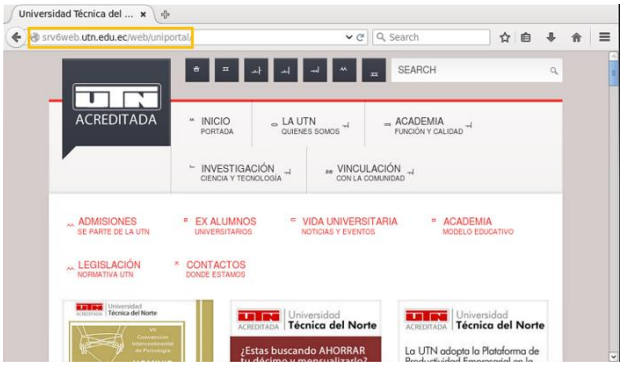


Figura 37. Acceso web por dominio IPv6

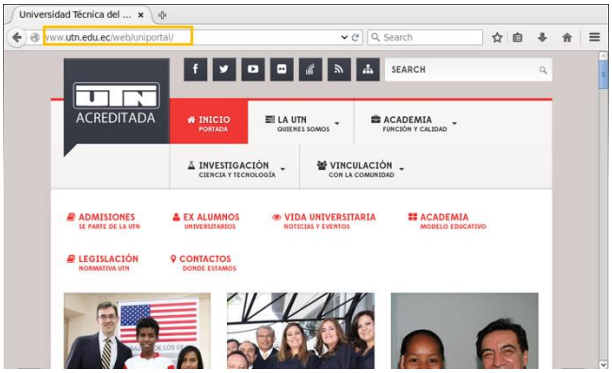


Figura 38. Acceso web por dominio universitario

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

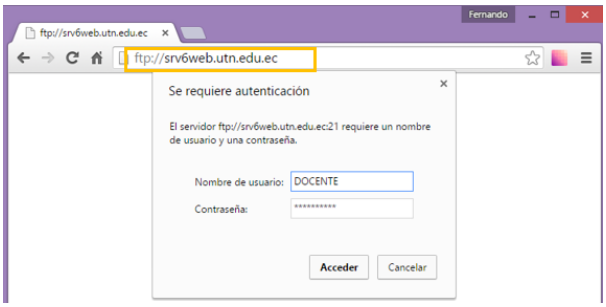


Figura 39. Acceso a FTP por dominio

IV. IMPLANTACIÓN DE MECANISMO

A. 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.

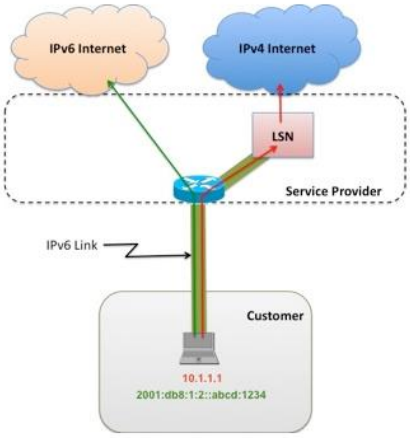


Figura 40. Modelo DS-Lite

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

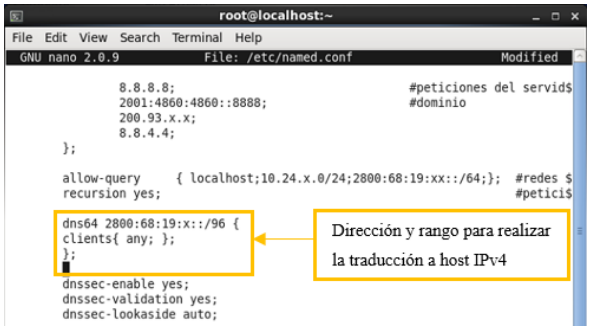


Figura 41. Configuración consultas ipv4 - ipv6

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

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.

B. Configuración de Equipos

Teniendo en cuenta la topología de la red universitaria, se configura en doble pila cada uno de los equipos en la infraestructura de red en involucrados el proceso de transición.

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.

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.

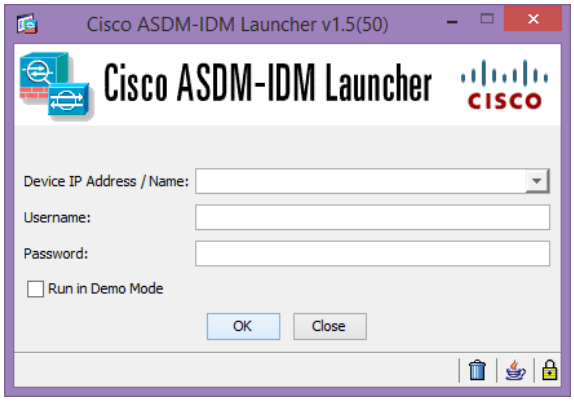
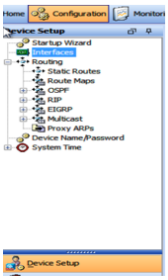
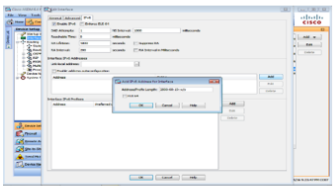


Figura 42. Cisco ASDM-IDM launcher

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

Tabla 3. 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.	

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).

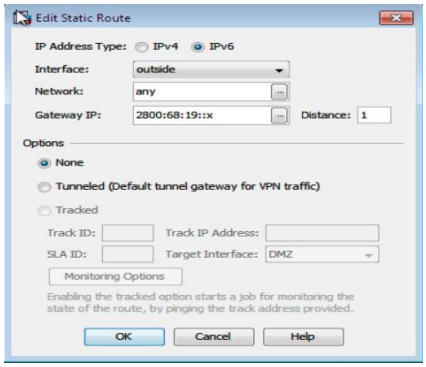


Figura 43. Direccions IPv6 OUTSIDE – INSIDE - DMZ

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.

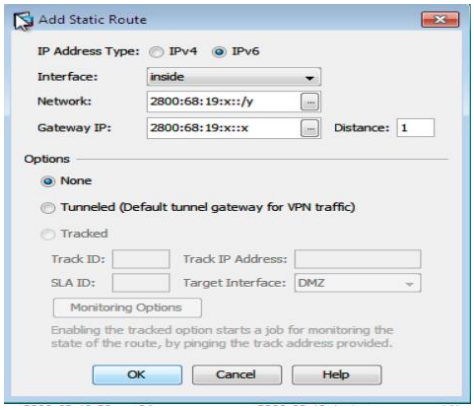


Figura 44. Enrutamiento VLANs UTN

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

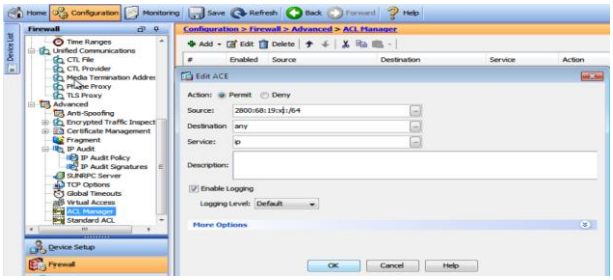


Figura 45. Reglas de trafico de resolucion de nombres

3) Configuración de Switchs

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.

a) 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
```

b) 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
```

c) 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
```

d) 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
```

e) 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
```

f) Configuración de equipos de laboratorio

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 4. 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.

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.

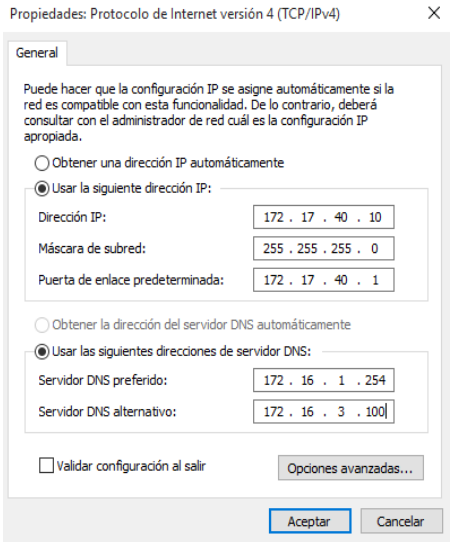


Figura 46. Configuración equipo nativo IPv4 de laboratorio

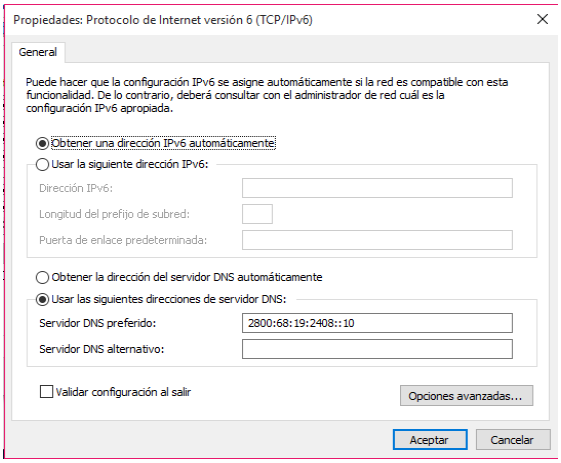


Figura 47. Configuración DNS equipo doble pila

C. *Pruebas De Funcionamiento*

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 48. Acceso desde red CNT EP a portal universitario

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.

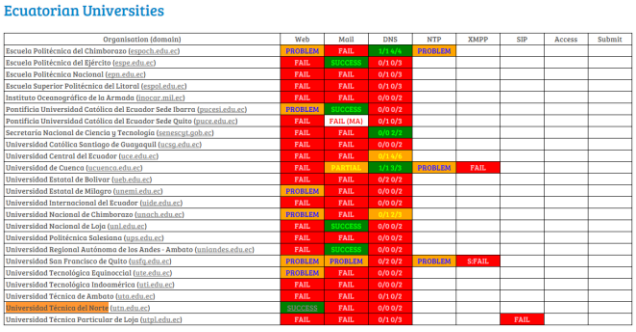


Figura 49. Prueba de servicio Web IPv6 de la UTN en Producción

1) *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.

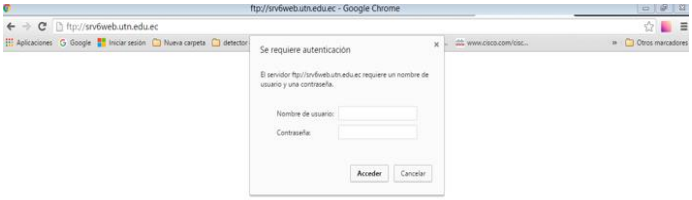


Figura 50. Ingreso a servidor FTP ipv6

V. CONCLUSIONES Y RECOMENDACIONES

A. 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.

B. 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.

VI. Referencias

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.

URL

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

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

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

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

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

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

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

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

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

Fernando Obando Autor Nació en Colombia el 22 de abril de 1987, reside en Ibarra provincia de Imbabura. Realizo sus estudios secundarios en el colegio Nacional “Atahualpa”, obteniendo el título de bachiller en la especialidad de Físico Matemático. Actualmente, es egresado de la Universidad Técnica del Norte en la Carrera de Ingeniería en Electrónica y Redes de Comunicación.

Ing. C. Vásquez Director Es un profesional en Ingeniería Electrónica y Telecomunicaciones. Actualmente es docente de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte en áreas como: Networking, WLAN, Fibra Optica entre otras áreas relacionadas.