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

B. Caranqui Autor, C. Vásquez Director
Facultad de Ingeniería en Ciencias Aplicadas, Universidad Técnica del Norte
Ibarra, Ecuador
bdacaranquiv@utn.edu.ec cavasquez@utn.edu.ec

Resumen— El trabajo de titulación que se presenta a continuación consiste en la implementación de un mecanismo de transición de IPv4 a IPv6 de dos aplicaciones del Sistema Integrado de la Universidad Técnica del Norte, se realiza una fundamentación teórica, una situación actual para conocer el equipamiento con el que cuenta la universidad, el diseño del desarrollo del proyecto, la implementación con cada uno de las metodologías de transición y las respectivas pruebas de funcionamiento. Dentro del desarrollo se determina un DNS64/NAT64 para la traducción de dominios AAAA y A, además de la traducción del pool de direcciones de la UTN. Finalmente se da a conocer los resultados obtenidos a través de las diferentes pruebas realizadas en los laboratorios de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte.

Abstract— The degree paper work that is presented consists of the implementation of an IPv4 to IPv6 transition mechanism of two applications of the Integrated System of the University "Técnica del Norte, a theoretical basis is made, also a current situation to know the equipment that currently has the University, furthermore, the design of the development of the project, the implementation with each one of the methodologies of transition and the respective tests of operation. Within the development a DNS64 / NAT64 is determined for the translation of AAAA and A domains, in addition, the translation of the address pool of the UTN. Finally, the results obtained through the different tests carried out in the laboratories of the Faculty of Engineering in Applied Sciences of the University "Técnica del Norte".

Índice de Términos — IPv4, IPv6, Transición, DNS64, NAT64, A, AAAA.

I. INTRODUCCIÓN

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

Uno de los problemas que se da, es el agotamiento de direcciones IPv4 para que los hosts puedan conectarse a la red, este caso se manifiesta en la Universidad Técnica del Norte. Anteriormente ya se empezaron a realizar estudios sobre el proceso de migración al protocolo conocido como IPv6, para de esta manera poder reemplazar al antiguo protocolo y así obtener la cantidad de direcciones IP suficientes para abastecer a todos los dispositivos que cuenten con una dirección IP en todo el mundo, una de las razones para realizar este cambio es que los usuarios de la Internet cada vez requieren nuevos servicios y aplicaciones ya que la tecnología avanza increíblemente.

La institución quiere formar parte del Consorcio Ecuatoriano de Internet Avanzando, por lo cual ha optado por realizar una transición paulatina de los servicios y las aplicaciones con las que cuenta la universidad, para este proceso se ha optado por realizar la configuración de los equipos de red para que trabajen mediante un mecanismo conocido como Doble Pila, es decir, cuentan con una dirección tanto en IPv4 como en IPv6.

Con la utilización del nuevo protocolo IP se puede tener muchas ventajas tales como son calidad de servicio, Multicast y Anycast, además de la movilidad IP y también por el hecho de que muchas veces en su cabecera no se va a necesitar de examinar cada una de ellas sino más bien solo hop by hop lo que permitirá que se tenga una mejor velocidad de transmisión.

II. CONCEPTOS BÁSICOS

La arquitectura TCP/IP fue desarrollado por ARPANET, ésta fue creada por el Departamento de Defensa de los Estados Unidos, con la finalidad de brindar conectividad a universidades e instalaciones gubernamentales de ese país. Recibe este nombre ya que sus dos principales protocolos son tanto el Protocolo de Control de Transmisión (TCP) como el Protocolo de Internet (IP). (Nuria Oliva, 2013)

A. Protocolo de internet versión 4 (IPv4)

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

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

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

La cabecera que utiliza IPv4 contiene la información de control del protocolo dividiéndose en dos partes, una parte que es fija de 20 bytes existente en todos los datagramas y otra variable, múltiplo de 32 bits. La información que es transportada por el protocolo IP está contenida por los datos, teniendo por lo general la información que pasa por el nivel de transporte (figura 1). (Miranda, 2014)

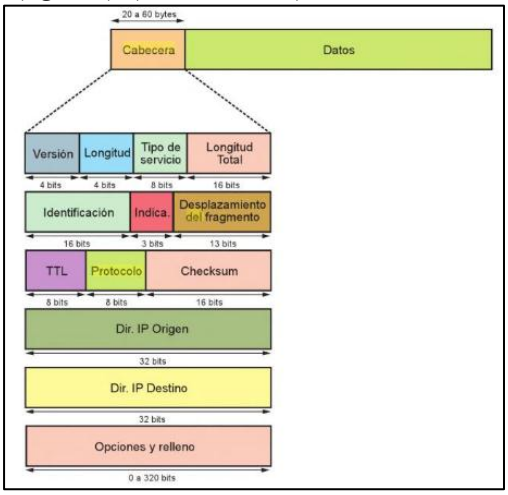

Figura 1. Cabecera IPv4

- **Versión:** Indica la versión del protocolo, como en este caso se está explicando sobre el protocolo IPv4, contendrá el valor 4.
- **Longitud de la cabecera:** Indica la longitud de la cabecera en byte, se puede tener un máximo de 2 16 con un total de 16 bytes.
- **Tipo de servicio:** Indica el tipo de servicio que se ha solicitado siendo este un campo que no es muy utilizado, la IETF redefinió su uso como ECN (Explicit Congestion Notification) para enviar información sobre la congestión de la red.
- **Longitud total:** En este campo se especifica el tamaño en bytes de todo el datagrama, de tal maneraque se incluye a los datos. El tamaño máximo del datagrama es de 2 16 con un total de 65.535 octetos.
- **Identificación:** En caso de que exista fragmentación se lo utiliza para identificar el datagrama. La fragmentación se produce cuando la MTU de una red es menor que la de la red que originó el datagrama.
- **Indicadores:** Los indicadores se utilizan únicamente para labores de fragmentación siendo un valor único asignado al datagrama por el emisor permitiendo identificar a que datagrama pertenece el fragmento.
- **Desplazamiento del fragmento:** Se utiliza para identificar la posición de un fragmento respecto al datagrama original, si el valor es 0 indica que es el primer o único fragmento además es medido en unidades de 8 bytes.
- **TTL (Tiempo de Vida):** Indica el número de saltos de un datagrama. El origen especifica un valor inicial y cada vez que el datagrama atraviesa un router, este valor decrementa. El paquete es descartado el momento que el campo llega a 0 de tal manera que elimina el datagrama.
- **Protocolo:** Indica el tipo de protocolo de nivel superior utilizado para de esta manera poder entregar un paquete, existen algunos tipos de protocolos como lo son TCP, UDP, ICMP, EGP, etc.
- **Checksum:** Es un código de redundancia que se utiliza para determinar si se han producido errores en la cabecera, en caso de que el checksum de la cabecera no concuerde, se descarta el datagrama, de tal manera que se realiza un control de la información.
- **Dirección de Origen:** Es aquella que identifica el origen de la comunicación, es la dirección IP origen del datagrama, siento la dirección que quiere realizar la comunicación.
- **Dirección de Destino:** Es aquella que identifica el destino de la comunicación, es decir es la dirección destino del datagrama, cuando se requiere hacer una comunicación, la dirección destino es importante para conocer hacia dónde va dirigido el datagrama.
- **Opciones:** El campo de Opciones IP se utiliza en caso de enviar información adicional.

1) Direccionamiento IPv4

El esquema de direccionamiento IP se puede decir que es de tipo jerárquico de tal manera que se tiene una porción destinada a la identificación de la red y una porción destinada a la identificación de un host de dicha red.

Las direcciones IP constan de 4 campos separados por un punto entre cada uno de ellos, es decir tiene un total de 4 bytes de longitud, de tal manera que se puede representar tanto de manera decimal y como alternativa se tiene la binaria.

Anteriormente se ha mencionado que existen diferentes

clases de direcciones IP, para lo cual se explicará de manera rápida la cantidad de direcciones que se puede tener en cada caso, se debe tener en cuenta que la que más utilizada es clase C.

2) Ventajas del Protocolo IPv4

El protocolo IPv4 ha sido el más utilizado en los últimos años, tanto es así que su manejo y adaptamiento para los usuarios se ha hecho más sencillo, empezando por una gran ventaja que la notación de sus direcciones es en decimal, siendo cuatro octetos que pueden ser representados como cuatro secuencias de números.

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

3) Problemas del Protocolo IPv4

La versión actual IPv4 presenta algunos problemas, sin embargo los problemas que presenta este protocolo se han ido identificando conforme los requerimientos de los usuarios han ido incrementando, es decir, la cantidad de direcciones IPv4 han ido agotándose debido a la cantidad de dispositivos electrónicos que se tienen conectados a la red, por lo que el número de direcciones disponibles en IPv4 ya no va a satisfacer las necesidades de los usuarios.

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

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

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

B. Protocolo de internet versión 6 (IP64)

IPv6 surge con el crecimiento de cantidad de usuarios con IPv4, ya que con el agotamiento de las direcciones IPv4, el IETF ha comenzado un desarrollo de este nuevo protocolo en el año de 1993, de tal manera que ya se tenía prevista una limitación del protocolo IPv4. A mediados del año 1995 se tuvo el diseño final de IPv6, que ha sido definido en el RFC 2460.

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

1) Definición de Protocolo IPv6

IPv6 (Internet Protocol Version 6) se ha diseñado para poder manejar la tasa de internet y realizar los requisitos de calidad de servicio, movilidad y seguridad de extremo a extremo.

Es una evolución del protocolo IPv4, pero no posee ningún cambio del mismo, ya que las funciones se mantienen simplemente fueron mejoradas y las funciones que ya no tienen validez fueron eliminadas, cabe mencionar que como una característica importante esla reducción de tablas de ruteo.

En la actualidad forma parte del soporte IP o IPng (IP siguiente generación) que incluye en los principales sistemas operativos del ordenador.

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

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

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

IPv6 es aquel que permite extensiones para un paquete que especifique un mecanismo para autenticar su origen, de tal manera que, se pueda garantizar la integridad e intimidad de

datos. Además, optimiza el encabezado lo que causa que sea más eficiente en la comunicación de sistemas de comunicaciones. Incluso provee nuevas funcionalidades como autentificación y seguridad. Este organiza cada datagrama como secuencia de encabezados proseguida de datos.

2) Características del Protocolo IPv6

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

3) Notación IPv6

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

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

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

Para la dirección IPv6:
2001:1001:0000:0000:0000:0000:0000:DACA

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

2001:1001::DACA

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

2001::1001::DACA

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

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

4) Formato de Encabezado

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

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

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

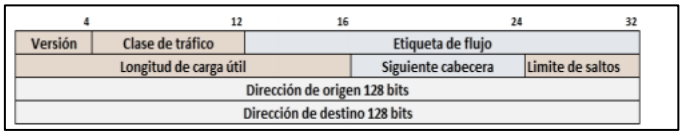

Figura 2. Formato de cabecera IPv6

- **Versión:** Como en el caso de IPv4 simplemente identifica el protocolo para este caso será 6.
- **Traffic Class o Clase de Tráfico: 8 bits:** El campo clase de tráfico se utiliza para identificar y distinguir las diferentes clases o prioridades de los paquetes IPv6.
- **Flow Label o Etiqueta de flujo: 20 bits:** La información que contiene este campo por el momento es experimental y se usa para aprovechar las ventajas de una subred de datagramas y una subred de circuitos virtuales, ya que se creará una pseudoconexión entre el origen con el destino para que exista un flujo continuo de datos, a su vez aprovechando las tablas de ruteo permitiendo una flexibilidad para establecer un camino.
- **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.
- **Payload Length o Longitud de carga útil: 16 bits:** Indica la longitud del paquete en bytes, es decir que indica la longitud de los datos o información que siguen a la cabecera, incluyendo las cabeceras de extensión (extension header), la máxima longitud puede ser de 65.536 bytes o 2^16 posibilidades.
- **Next Header o Encabezado siguiente: 8 bits:** Este campo indica qué cabecera de extensión sigue a la

cabecera principal.

- **Hop Limit o Límite de saltos: 8 bits:** Se encarga de evitar que los paquetes se queden permanentemente en la red, delimitando un tiempo de vida por "saltos" que debe realizar el paquete para llegar a su destino, en cada salto que realiza el paquete se decrementa una unidad, en caso de que el valor llegue a 0, se dice que éste se ha descartado.
- **Source Address o Dirección de origen: 128 bits:** Contiene la dirección desde donde es enviada la información, es decir indica el origen del paquete dentro del formato de IPv6 de 128 bits.
- **Destination Address o Dirección de destino: 128 bits:** Contiene la dirección hacia donde es enviada la información, es decir indica el destino del paquete dentro del formato de IPv6 de 128 bits.
- **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.

5) Cabeceras de Extensión de IPv6

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

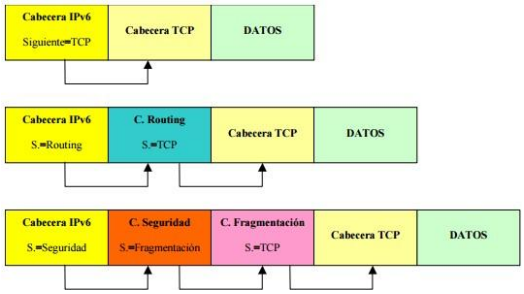

Figura 3. Cabeceras de Extensión

a) Cabecera de Encaminamiento (Routing Header)

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

b) Cabecera de Fragmentación (Fragment Header)

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

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

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

d) Cabecera de Autenticación (Authentication Header)

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

e) Cabecera de Opciones de Destino

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

6) Direccionamiento IPv6

a) Direcciones Unicast o Unidifusión

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

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

- **Local de Enlace:** En estos tipos de enlace se puede identificar las interfaces dentro de un enlace de la misma red local, es utilizada para el descubrimiento de vecinos configurándose de manera automática.
- **Local de sitio:** Para este tipo de direcciones, se dice que son aquellas que permiten encontrar interfaces dentro de un mismo sitio.
- **Global:** En el caso de las direcciones global, son aquellas que permiten identificar una interfaz en el internet, siendo su equivalente las direcciones públicas dadas en IPv4.

7) Direcciones Anycast

Este tipo de direcciones permiten identificar un grupo o conjunto de interfaces, en donde los paquetes enviados a una dirección anycast, éste será entregado a cualquiera de las direcciones asociadas, existe un protocolo de media distancia en donde especifica que el paquete será entregado al más cercano, además cabe recalcar que este tipo de agrupación no existe en IPv4.

8) Direcciones Multicast

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

Dentro de la clasificación de direcciones IPv6 también se puede encontrar en función del alcance:

- **Link-Local:** Estas tienen sentido solamente en el ámbito del enlace.
- **Site-Local:** Tienen sentido en el ámbito de una organización.
- **Global:** Estas en cambio son de manera global, abarcando las dos anteriores. (Verdejo, 2000)

9) Enrutamiento IPV6

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

Las rutas estáticas son utilizadas para hacer el enrutamiento forzado de algunos prefijos a través de enrutadores específicos. Cuando la configuración del enrutamiento es de manera estática, estas tienen la mayor preferencia en una tabla de enrutamiento sobre las rutas aprendidas por los protocolos dinámicos.

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

Enrutamiento Dinámico

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

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

10) Mecanismo de transición

Las redes en la actualidad necesitan trabajar tanto en IPv4 como en IPv6, para esto ambos protocolos deben existir dentro de una red, de tal manera que, exista una coexistencia de protocolos o incluso se pueda trabajar como un IPv6 nativo, por esta razón se han implementado tres tipos de mecanismos que poseen diferentes características, más adelante se detallará cada uno de dichos mecanismos.

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

Coexistencia de Aplicaciones y Servidores

La estructura de red en La Internet está basada en el protocolo IPv4, un cambio inmediato de protocolo es inviable debido al tamaño y la proporción que posee la red, se ha realizado una adopción de IPv6 pero que se debe implementar de una forma gradual, existiendo un periodo de transición y coexistencia entre los dos protocolos.

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

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

11) Metodologías de transición

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

a) Método de transición Doble-Pila

Se ha conseguido introducir IPv6 de una manera más fácil en una red, este proceso se lo conoce como "mecanismo de Doble Pila", el cual está descrito en el RFC 2893. Por este método se logró que un host o un router alcancen ambas pilas de protocolos (IPv4 e IPv6) provistas como un componente del sistema operativo. Por lo tanto, las dos pilas envían y reciben datagramas que pertenecen a ambos protocolos y así podrán comunicarse con cada nodo IPv4 e IPv6 en la red.

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

b) Método de transición Tunelling

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

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

c) Mecanismo DNS64 y NAT 64

El mecanismo NAT64 está definido en la RFC 6146, es una técnica para traducción de paquetes y puertos IPv6 a IPv4, permite simultáneamente el uso compartido de direcciones IPv4. El DNS64 está definido en la RFC 6147, éste en cambio es una técnica auxiliar de mapeo para nombres de dominio, conocido como resolución de nombres de dominio, que se utiliza en conjunto con NAT64.

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

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

Una de las desventajas del uso de DNS64 y NAT64 es que actualmente existen aplicaciones o equipos que no soportan IPv6, es por eso que si el equipo o la aplicación no puede trabajar en el nuevo protocolo IPv6 de nada serviría las técnicas de traducción, por esa razón, actualmente es un poco inviable la implementación inmediata de dicha técnica, a pesar de que a un plazo no muy lejano se convierta ya en un us común el nuevo protocolo. (Juárez, 2015)

12) Servicios y aplicaciones

La capa de Aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el tratamiento de los datos. Un único programa ejecutable debe utilizar los tres componentes e inclusive el mismo nombre.

Por ejemplo: cuando se analiza "Telnet" se puede referir a la aplicación, el servicio o el protocolo.

Definición de Servicios y Aplicaciones

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

Servicios y Aplicaciones que se pueden transicionar

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

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

Se ha determinado que tanto el Servidor de Aplicaciones como el servidor de la Basede Datos serán transicionados al nuevo protocolo, este análisis se lo ha podido

verificar una vez que se estudió las características de los equipos, llegando a la conclusión de que el soporte para IPv6 es aceptable.

Sistema Informático Integrado de la Universidad Técnica del Norte

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

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

Figura 4. Sistema Informático Integrado UTN

Aplicaciones en la Universidad Técnica del Norte

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

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

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

El Servidor de Aplicaciones Reports también se encuentra implementado con un Sistema Operativo Oracle Linux 5, este se encuentra categorizado dentro de las áreas de inteligencia de negocios, una de las carácterísticas es que cuenta con estabilidad en el servidor, es decir, que se crea una característica con la base de datos en caso de que existan algunos errores, tiene una alta disponibilidad ya que como cuenta con la base de datos, permite que las tareas programadas no se pierdan, y además tiene una facil administración ya que dispone de una ventana de administración pudiendo visualizar gráficamente la cola de impresión, número de reportes programados, en ejecución, terminados, etc. (Cañar & Cordero, 2013)

III. Análisis de Requerimientos, Implementación y Pruebas del Método de Transición

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

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

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

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

A. Topología lógica de red de datos UTN

La Universidad Técnica del Norte cuenta con un cuarto de equipos ubicado en el Edificio Central de la institución que se interconectan cada una de las subredes de las dependencias de la Universidad. (Figura 14)

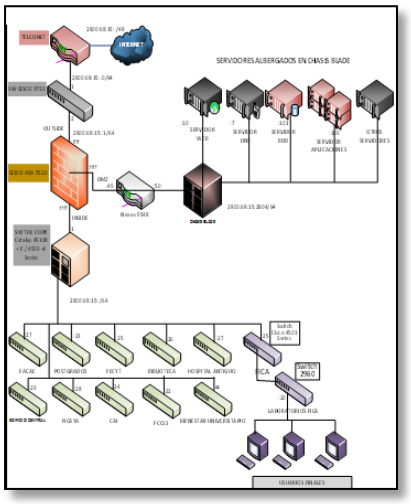

Figura 5. Topología de Red UTN

B. Requerimientos para implementación

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

C. Configuración de red IPv4/IPv6 en Centos 6.5

Se debe asignar una dirección IPv6 en la tarjeta de red para esto se debe acceder al fichero mediante el comando *#nano /etc/sysconfig/network-scripts/ifcfg-eth0*

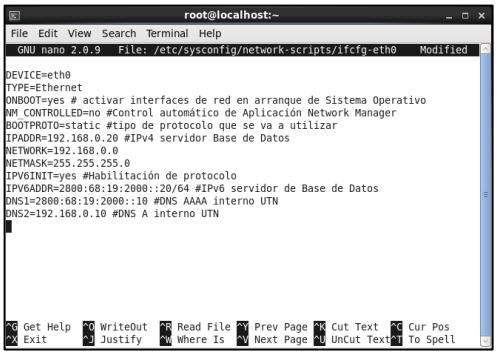

Figura 6. Configuración interfaz de red

Se debe realizar la habilitación de los protocolos de internet en los cuales se va a trabajar, se ingresa al archivo de configuración de red, mediante el comando #nano /etc/systemconfig/network

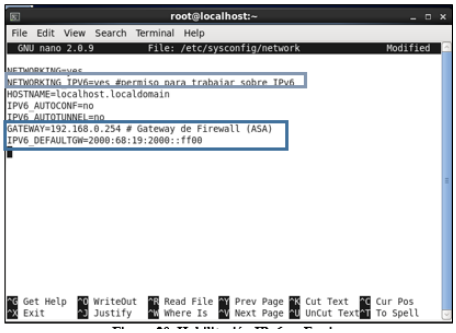

Figura 7. Habilitación de IPv6

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

D. Configuración De Mecanismos de Transición

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

1) Configuración de Mecanismo de Transición DNS64

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

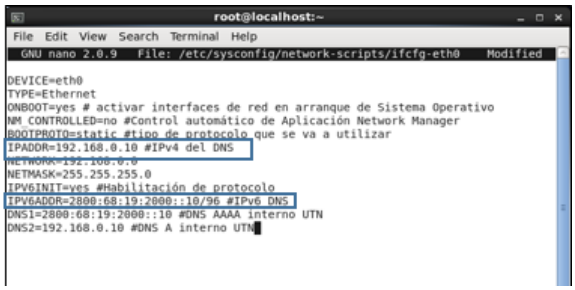

Figura 8. Configuración Interfaz de Red del DNS

Habilitar y dar permiso para trabajar sobre IPv4 e IPv6 en el DNS visto en la figura 26, para lo cual se setea NETWORKING y NETWORKING_IPV6 en YES.

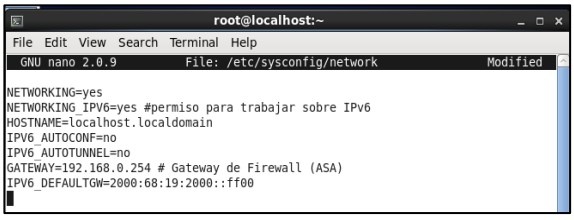

Figura 9. Habilitación para trabajar sobre IPv6 en DNS

Se reinicia el servicio y se ejecuta los cambios que se realizaron en las tarjetas de red para que la configuración no se modifique en el reinicio del sistema.

Es importante tener en cuenta que para el DNS se debe instalar la aplicación BIND (Berkeley Internet Name Domain) para lo cual se lo realiza con el comando *# yum install bind*

Se procede aceptar la instalación de la aplicación poniendo Y en la pantalla que se despliega

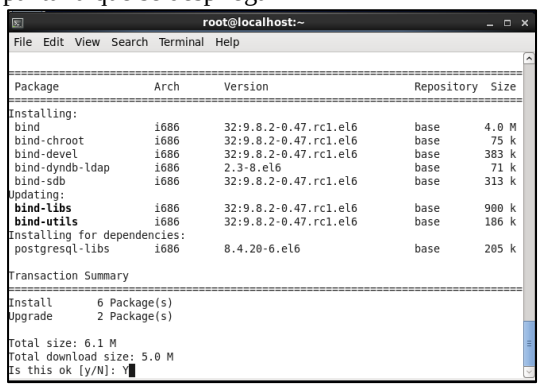

Figura 10. Aceptación de Instalación BIND

Se ingresa al archivo de configuración general BIND del DNS con el comando *nano /etc/named.conf*. Hay que editar las direcciones de las cuales se escuchará las peticiones mediante el puerto 53, estás direcciones tendrán un encaminamiento y una traducción hacia su destino.

El puerto será direccionado, se agregará las direcciones del servidor, siendo IPv4 e IPv6 y además se asignarán los Forwards del proveedor de Internet, estos permiten que se envíen las consultas ya generadas hacia los servidores DNS externos

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

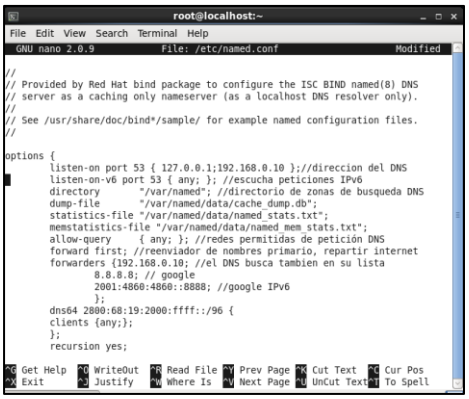

Figura 11. Direccionamiento servidor DNS64

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

a) Zonas Directas

Se realiza la configuración y establecimiento de las Zonas Directas de tal manera que se define el tipo de zona y el nombre del archivo con el que se va a buscar la zona directa

Figura 12. Zonas Directas

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

Figura 13. Configuración de Registros y Aplicaciones del DNS64

b) Zonas Inversas

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

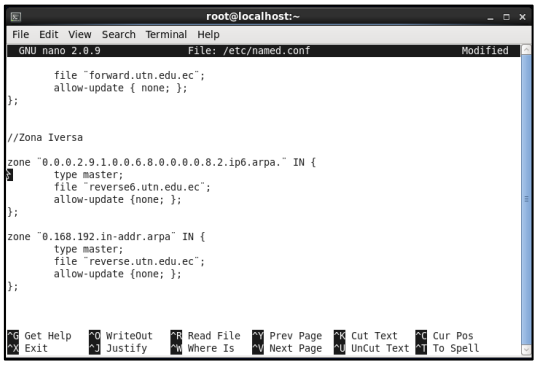

Figura 14. Zonas Inversas

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

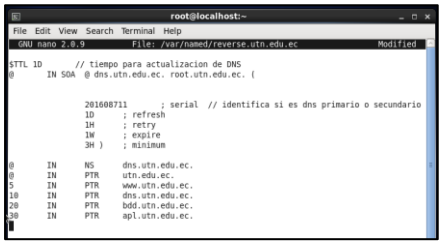

Figura 15. Zona inversa DNS64 IPv4

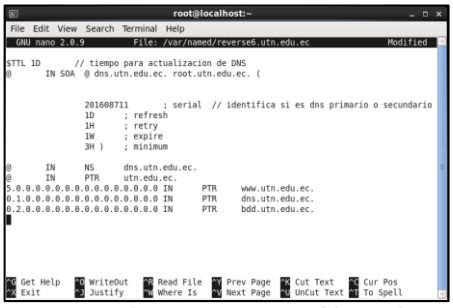

Figura 16. Zona Inversa DNS64 IPv6

2) Configuración de Mecanismo de Transición NAT64

Para la configuración del NAT64 lo primero que se va a realizar es la instalación de TAYGA, se realiza la descarga de este paquete para luego continuar con el proceso.

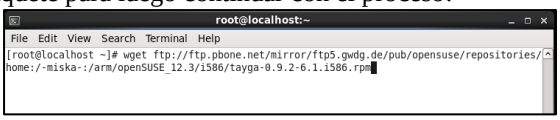

Figura 17. Descarga de TAYGA

De manera gráfica se procede a realizar la instalación, para esto simplemente se busca en el root, la instalación de este paquete y se da doble clic para continuar con la instalación, aparece un mensaje en el cual se debe poner en la opción *continue anyway*

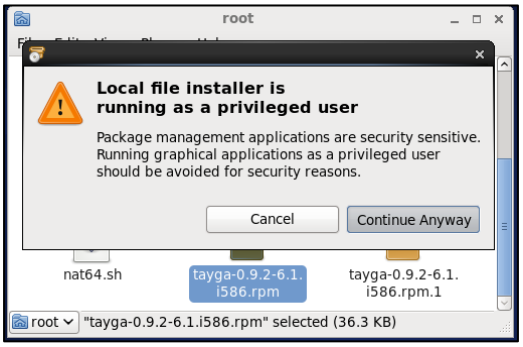

Figura 18. Instalación de TAYGA

Se procede a la creación de las rutas estáticas e interfaz virtual NAT64 para la asignación y traducción de direcciones IPv4, de tal manera que puedan acceder todos los hosts nativos IPv6.

Figura 19. Rutas estáticas e Interfaz virtual

Se ingresa al archivo de configuración de las Iptables para crear cada una de las reglas, las siguientes reglas aceptan el tráfico de los puertos de DNS, ICMP. Además, realiza el encaminamiento entre las interfaces tanto virtual como real en el proceso de la traducción.

Figura 20. Configuración Iptables

Se procede a dar el rango de direcciones con las que se va a realizar la traducción de direcciones además se muestra el prefijo asignado para realizar la traducción de direcciones, el cual debe ser el mismo que se ha configurado en las rutas estáticas y en el fichero de configuración global del DNS64.

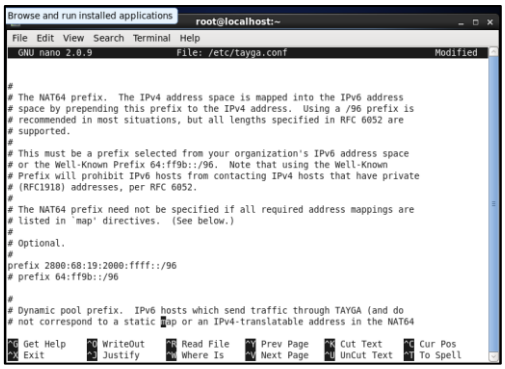

Figura 21. Configuración de TAYGA

Para culminar con la configuración del NAT64 se procede a inicializar la interfaz virtual del mismo y también las configuraciones previamente realizadas.

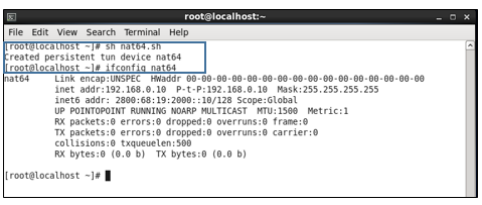

Figura 22. Inicialización de la Interfaz Virtual

3) IMPLEMENTACIÓN DE MECANISMO

E. Mecanismo de Transición Doble Pila

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

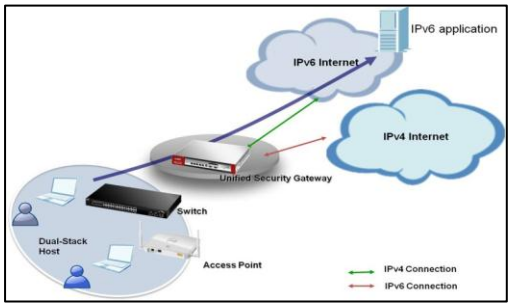

Figura 23. Metodología Doble Pila

Para que el dispositivo final pueda acceder y enviar paquetes en IPv4 e IPv6 se digita los siguientes comandos en el fichero "*/etc/named.conf*"

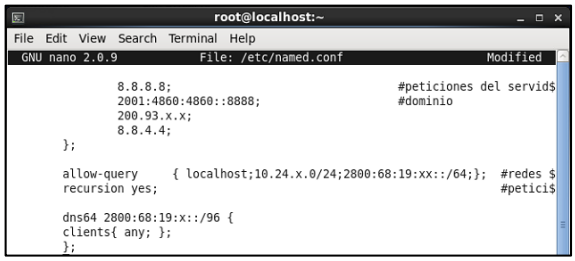

Figura 24. Configuración para consultas IPv4 e IPv6

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

A continuación, se detalla la configuración de los equipos que interactúan dentro del proyecto de transición.

1) Switch cisco 3750

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

Lo primero que se va a realizar es la habilitación del protocolo IPv6:
Switch# configure terminal
Switch(confg)# sdm prefer dual-ipv4-and-ipv6 default
Switch(confg)# end
Switch# reload
Switch# configure terminal
Switch(confg)#ipv6 unicast-routing
Switch(confg)#interface vlan 400
Switch(confg-if)#ipv6 address 2800:68:19::x/y
Switch(confg-if)#enable ipv6
Switch(confg-if)#no shutdown
Switch(confg-if)#exit
Switch(confg)#ipv6 route ::/0 2800:68:19::x
Switch(confg)#ipv6 route 2800:68:19::/48 2800:68:19::x

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

2) Configuración CISCO ASA 5520

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

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

Se procede a realizar la autenticación mediante un nombre de usuario y una contraseña para el acceso al equipo tal y como se lo observa en la figura 57 que se presenta a continuación.

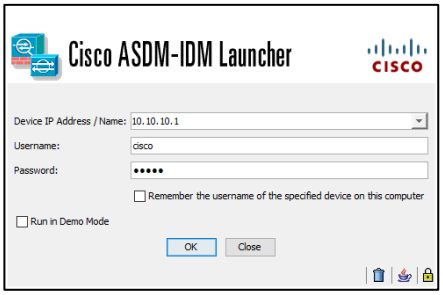

Figura 25. Cisco ASDM-IDM launcher

El primer paso es la asignación de direcciones IPv4 e IPv6 de cada una de las interfaces.

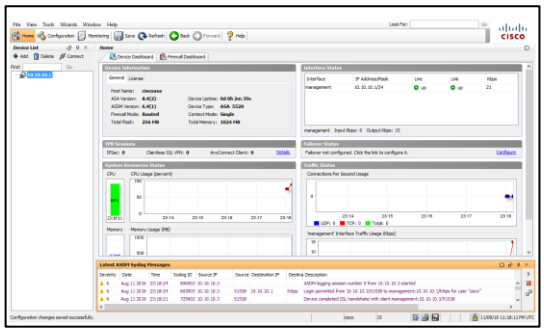

Figura 26. Interfaz de Gestión

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

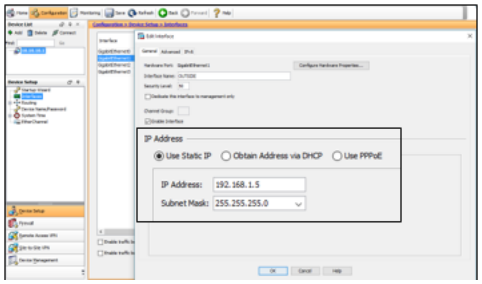

Figura 27. Dirección IPv4 interface OUTSIDE

La configuración que se presenta anteriormente se la debe realizar tanto para IPv4 como para IPv6, de igual manera se realiza la configuración para cada una de las interfaces.

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

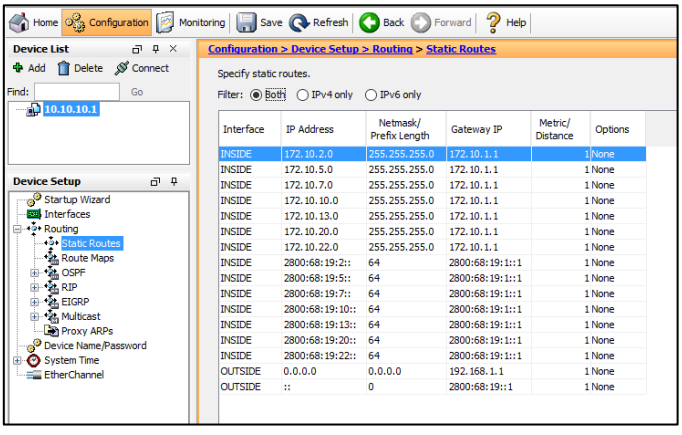

Figura 28. Direccionamiento IPv4 e IPv6 CISCO ASA

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

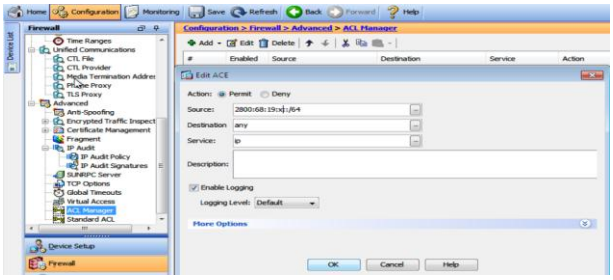

Figura 29. Reglas de trafico para resolución de nombres

3) Switch de Core FICA

Es el equipo de distribución para la red de acceso local (LAN), están definidas las VLANs y está directamente conectada a cada una de las dependencias universitarias. (FICA, BIENESTAR, FACAE, ETC.) Se debe configurar en Doble Pila.

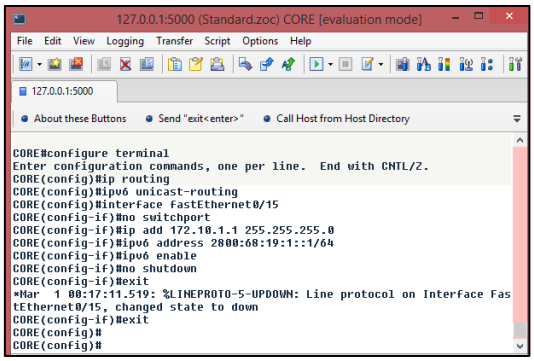

Figura 30. Configuración Switch the Core

Las interfaces que se encuentran conectadas directamente a los switchs de acceso de cada dependencia universitaria establecen enlaces en modo troncal.

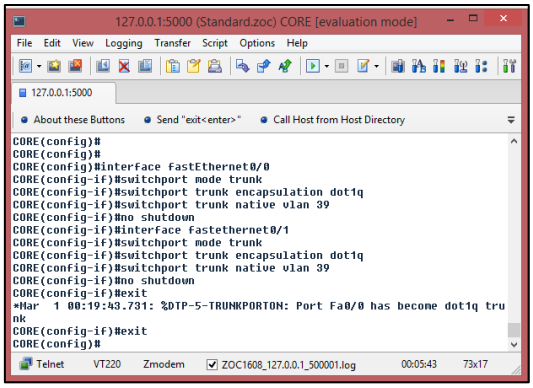

Figura 31. Configuración modo Troncal Switch de Core FICA

4) Configuración de Switch Cisco 2960

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

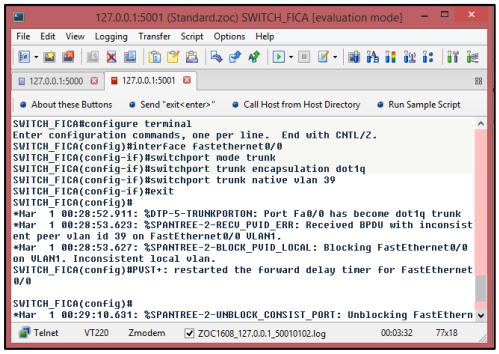

Figura 32. Habilitación Interfaz conectada al Switch de Core

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

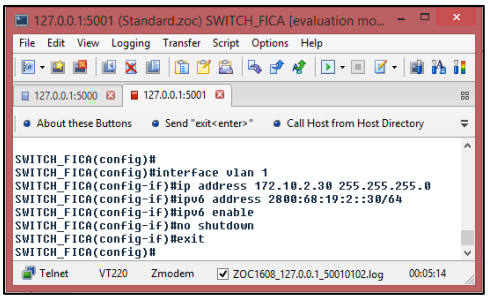

Figura 33. Asignación IPv4 e IPv6 en Vlan 1Nexus

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.

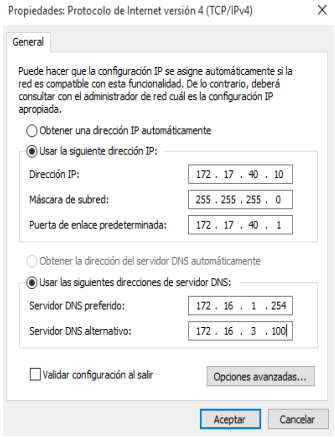

Figura 34. Configuración equipo nativo IPv4 de laboratorio

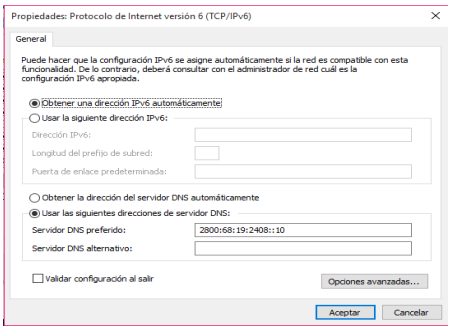

Figura 35. Configuración DNS equipo doble pila

F. Pruebas De Funcionamiento

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

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

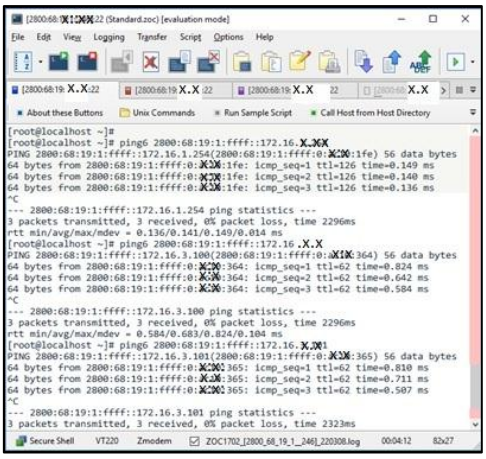

Figura 36. Prueba de funcionamiento de traducción de direcciones

Acceso desde la red local, de tal manera que se puede acceder al portafolio de los estudiantes y docentes de la Universidad Técnica del Norte.

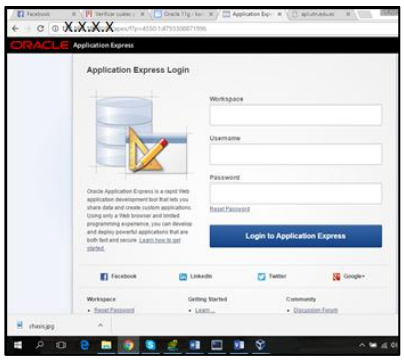

Figura 37. Acceso a Portafolio Estudiantil

IV. CONCLUSIONES Y RECOMENDACIONES

A. Conclusiones

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

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

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

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

• El desarrollo del proyecto, conlleva a realizar una investigación más profunda de lo que se ha venido aprendiendo en las aulas de la casona universitaria, de esta manera, se logra concluir con el trabajo de tesis planteado, para desarrollarlo dentro de la universidad.

B. Recomendaciones

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

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

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

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

V. BIBLIOGRAFÍA

Libros

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

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

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

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

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

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

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

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

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

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

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

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

Tesis

Alex, A. (2008). *Análisis y diseño para la instalación del protocolo IPv6 en la red.* Obtenido de http://repositorio.utc.edu.ec/bitstream/27000/1841/1/T-UTC-1332.pdfBaus, G. A. (Julio de 2016). *Google Académico.* Obtenido de bibdigital.epn.edu.ec: http://bibdigital.epn.edu.ec/bitstream/15000/16491/1/CD-7173.pdf

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

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

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

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

Revistas

- Awduche, D. (Noviembre de 2010). Beneficios de IPv6 para las empresas. Obtenido de http://www.verizonenterprise.com/resources/whitepapers/wp_beneficios-de-ipv6-para-las-empresas_es_xg.pdf
- Cabellos, A. (2004). S6S, ipv6 servicio de información y soporte. Obtenido de Protocolo IPv6: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

URL

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

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

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

Brayan Caranqui Autor Nació en Ecuador el 29 de octubre de 1991, reside en Mira provincia del Carchi. Realizó sus estudios secundarios en el colegio Experimental ¨León Ruales¨, obteniendo el título de bachiller en la especialidad de Físico-Matemáticas. 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.