Proposal for the implementation of IPv6 in an operational IPv4 infrastructure

Jhordy Esteban Salinas Santiago, Ing. Sistemas[1], Carlos Andrés Sánchez Venegas, Ing. Sistemas, Juan Camilo Herrera Velásquez, Ing. Sistemas y Claudia P Santiago C, Msc. Gestión de Información [1]
[1] Escuela Colombiana de Ingeniería Julio Garavito, Colombia, jhordy.salina@mail.escuelaing.edu.co, claudia.santiago@escuelaing.edu.co
[2] Escuela Colombiana de Ingeniería Julio Garavito, Colombia, carlos.sanchez-v@mail.escuelaing.edu.co, juan.herrera@escuelaing.edu.

Abstract -- Internet protocol Ipv6 is a technology created in the late 1990s, but it has not been implemented in network infrastructures as expected. This paper presents the IPv6 protocol, its advantages and the challenges for its adoption and proposes a mechanism to implement it in an IPv4 environment without losing connectivity with IPv4 and IPv6 networks. Finally, the paper presents a case of implementation in a real IPv4 infrastructure and the tools and configuration applied for its operation.

Keywords– IPv6, IPv4 vs IPv6, IPv6 implementation.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.300
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

17th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Industry, Innovation, And Infrastructure for Sustainable Cities and Communities", 24-26 July 2019, Jamaica.

Propuesta de implementación de IPv6 en una infraestructura IPv4 en operación

Jhordy Esteban Salinas Santiago, Ing. Sistemas[1], Carlos Andrés Sánchez Venegas, Ing. Sistemas, Juan Camilo Herrera Velásquez, Ing. Sistemas y Claudia P Santiago C, Msc. Gestión de Información [1]
[1] Escuela Colombiana de Ingeniería Julio Garavito, Colombia, jhordy.salina@mail.escuelaing.edu.co, claudia.santiago@escuelaing.edu.co
[2] Escuela Colombiana de Ingeniería Julio Garavito, Colombia, carlos.sanchez-v@mail.escuelaing.edu.co, juan.herrera@escuelaing.edu.co

Abstract*– Internet protocol Ipv6 is a technology created in the late 1990s, but it has not been implemented in network infrastructures as expected. This paper presents the IPv6 protocol, its advantages and the challenges for its adoption and proposes a mechanism to implement it in an IPv4 environment without losing connectivity with IPv4 and IPv6 networks. Finally, the paper presents a case of implementation in a real IPv4 infrastructure and the tools and configuration applied for its operation.

***Keywords*-- IPv6, IPv4 vs IPv6, IPv6 implementation.**

***Resumen*- El protocolo de internet IPv6 es una de las tecnologías, creadas a finales de los 90. que se encuentran en el mercado hace un tiempo y no ha sido explotada y/o aprovechada de la mejor manera. Este artículo presenta una revisión del protocolo, sus ventajas, mejoras y tecnologías asociadas y sus retos para implantación. Además, propone una implementación de la misma en un ambiente productivo y las herramientas y configuraciones necesarias para su convivencia con su antecesor IPv4, pero aprovechando todas las ventajas que éste ofrece. Manteniendo conectividad con redes IPv6 e IPv4**

***Palabras claves*- IPv6, IPv4 vs IPv6, implementación IPv6**

I. Introducción

El protocolo IPv6, sucesor de IPv4 (protocolo tradicional de Internet) es una tecnología que a pesar que no es tan nueva, realmente no ha sido implementada de forma masiva, pero es importante comenzar a hacerlo, ya que cada vez es más sentida la necesidad de hacer una migración hacia IPv6, es por esto que se realizó una implementación de esta tecnología en la red LAN del Laboratorio de Informática de la Escuela Colombiana de Ingeniería Julio Garavito.

Como se muestra en la figura 1 se observa que, en países como Nicaragua, Colombia y República Dominicana la adopción del protocolo de internet IPv6 es muy bajo (0.34%, 0.92% y 1.23% respectivamente), en países como Paraguay, Canadá, México, Brasil, Uruguay y Estados Unidos la adopción del mismo está entre el 23 y el 36% lo cual muestra la baja adopción de este estándar en toda la región. Esta fue una de las motivaciones para realizar este proyecto, ya que si los países de la región, y en particular en el caso de Colombia, desde donde se origina este trabajo, comienzan a adaptar este estándar y apoyarse en el trabajo que se presenta en este artículo, puede tener grandes oportunidades en cuanto a conectividad con mejor calidad de servicio (QoS) con otros países que ya están adoptando esta tecnología.

Para llevar a las organizaciones a la adopción de IPv6 dentro de su infraestructura de IT, es necesario conocer el protocolo IPv6, sus ventajas, su funcionamiento y las recomendaciones que diferentes entidades, organizaciones y grupos de profesionales han dado, para luego pasar a la revisión de la infraestructura con la que usualmente se cuentan en las redes IPv4 de las empresas actuales y finalmente, hacer una propuesta de implementación y adopción del protocolo IPv6, aprovechando sus beneficios como por ejemplo la implementación nativa de nuevas alternativas de seguridad.

Y se debe partir del hecho de que las empresas y personas en los países de la región usan en sus rede en mayor medida IPv4, tal es el caso de Colombia, en donde el 99.69% de la población se encuentra utilizando la versión de internet IPv4 [1].

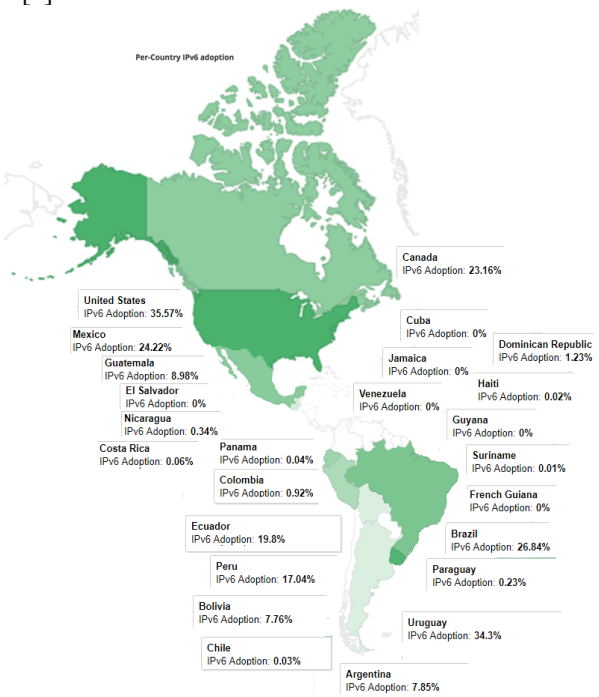

Figura 1. Mapa de adopción del protocolo IPv6 por países en sur América.[1]

Con esto en mente, para la realización del presente artículo, en el capítulo dos se presentan las justificaciones por las cuales se realizó el proyecto, en el capítulo tres se mostrará el estudio realizado con el fin del entendimiento del protocolo IPv6, sus ventajas, diferencias con el protocolo IPv4 y las implicaciones de su implementación, en el

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.300
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

capítulo cuatro se presenta la propuesta planteada para la implementación de IPv6 y su convivencia real con IPv4 y los resultados que se consiguieron en una red en operación y por último en el quinto capítulo se muestran las conclusiones a las que se llegaron con el desarrollo mencionado.

II. JUSTIFICACIÓN

A finales del siglo XX e inicios del siglo XXI las organizaciones y las personas sintieron la necesidad de interconectarse con el fin de compartir información en la búsqueda de la generación de un reconocimiento globalizado, a tal punto de requerir nuevas tecnologías y recursos para abastecer sus requerimientos [2]. A lo largo de la historia se ha venido trabajando sobre las bases que se pactaron inicialmente (protocolos, maquinaria, arquitecturas, etc.) en un intento por mejorar sus propiedades tales como los controles que se tiene sobre la información y la velocidad a la que ésta se transmite, pero ignorando otros enfoques que podrían ser el inicio de una nueva generación de redes.

Los usuarios cada vez más requieren mayor velocidad, rendimiento y confiabilidad, para hacer posible el uso de diferentes servicios proporcionados por Internet. En un principio no se esperaba la masificación de dispositivos conectados entre sí, es decir, que se tenían en cuenta las principales primitivas para su escalabilidad, pero no se anticipó la magnitud del requerimiento de flujo de datos sobre la red ("Desde 1984 a 2012: 1.2 zettabytes generados, Pronóstico al 2017: 1.4 zettabytes"). Proporcionando una base, pero también dejando un gran campo de acción para su mejora y evolución [3].

El protocolo de internet IPv6 se comenzó a desarrollar en 1990 cuando la IETF (Internet Engineering Task Force) se dio cuenta de la futura necesidad de ampliar el rango de direcciones disponibles para interconectar dispositivos, en 1994, se generó el RFC 1752, en donde se expone las recomendaciones para la siguiente generación del protocolo IP (IPng), el cual especifica que éste va a suplir la necesidad de direcciones de por vida [4].

La migración hacia el protocolo IPv6 es imprescindible, por este motivo es importante realizar dicha migración desde ya y revisar las implicaciones reales de dicha migración, este artículo mostrará dichas implicaciones, la importancia de la misma, de igual manera se mostrará una migración a IPv6 en un ambiente productivo.

III. IPv6

A. Origen

A inicios de los años 90's se hizo evidente el problema que se generaría a raíz de la falta de direcciones IPv4. Desde 1990 hasta el 2000 se pensaron en varias estrategias en donde se proponían soluciones a dicho problema, algunas de estas soluciones se implementaron como por ejemplo el servicio NAT, el cual nació para ahorrar direcciones en IPv4[5].

Sin embargo, los esfuerzos que se realizan para evitar la escasez de estas direcciones no fue suficiente, así que en el año 1995 el grupo encargado por la IETF para revisar esta situación, recomendó la formalización de un nuevo protocolo denominado IPng (IP next generation), y su especificación se completó en el año 1998 [6].

Actualmente hay diversas instituciones públicas y privadas financiando e impulsando el despliegue de IPv6. El pionero en la investigación e implementación de casos de pruebas con el protocolo IPv6 fue México, seguido de países como España y Estados Unidos [7]. Estos países han trabajado en la adopción del protocolo y han logrado la definición de procedimientos de implementación e implementaciones de prueba que usan de manera nativa el protocolo IPv6 y permiten conectividad a internet con este protocolo, así como comunicación con otras entidades que también cuentan con implementaciones de sus portales en IPv6 nativo.

B. Generalidades

Como se mencionó anteriormente, la intención con la inclusión de IPv6 en las redes actuales es buscar cubrir muchas de las necesidades de los usuarios. Principalmente, se busca responder a la necesidad de más direcciones IP para seguir conectando mayor cantidad de dispositivos y de diferentes naturalezas, como por ejemplo los tradicionales computadores y servidores y una serie de nuevos dispositivos relacionados con las tendencias de Internet de las Cosas (IoT) como son: teléfonos móviles, impresoras, cámaras, televisores y asistentes personales, entre otros.

Así mismo, se simplificó el formato de encabezado, ya que el encabezado de los paquetes IPv4 tiene muchos campos que en un principio estaban destinados para casos particulares de envío de más información, pero en la actualidad no están siendo usados y complican la gestión de los equipos encargados de la transmisión a través de Internet. También se mejoraron las opciones de extensión en los paquetes, es decir a futuro será sencillo agregar opciones de direccionamiento a los encabezados de los paquetes, lo cual añade flexibilidad a la solución.

Adicionalmente se hizo una mejora en el aspecto de seguridad trabajando en la triada de seguridad de la información (confidencialidad, integridad y disponibilidad) y se incrementó la velocidad de transmisión gracias a la mayor eficiencia del protocolo, debido principalmente a las modificaciones de direccionamiento y encabezado mencionadas en el párrafo anterior [8].

Por otro lado, a pesar que el protocolo IPv6 fue creado para solucionar problemas que se han identificado con el pasar de los años en el protocolo IPv4, éste no fue creado para ser compatible con su antecesor, es decir, la convivencia del protocolo IPv4 e IPv6 no es nativa ni natural, por ende, es necesario implementar diferentes tecnologías para lograr la convivencia de estos.

C. Ventajas

Dentro de las ventajas más representativas del protocolo IPv6, se encuentra el espacio de direcciones. Este espacio se amplió gracias al cambio de direcciones de 32 bits en IPv4 a 128 bits en IPv6, brindando la oportunidad de contar con un rango mayor de direcciones que permiten conectar un número mayor dispositivos. Otra de las ventajas para resalta en éste protocolo es que el encabezado se logró reducir en complejidad, a pesar del aumento de su tamaño debido al tamaño de las direcciones de este protocolo, esto hace que el procesamiento de los paquetes sea más rápido y por ende la velocidad de transmisión aumentó.

Así mismo en los routers alineados para 64 bits se quitó la fragmentación de paquetes, esto hace que el tiempo que se tarda un paquete en el router disminuya. Se amplió la capacidad para el envío de datos, esto quiere decir que con IPv6 se puede enviar mayor cantidad de datos en un mismo paquete.

Se mejoró la calidad del servicio (QoS) que, como se mencionó anteriormente, hace referencia al rendimiento de la red. Por último, IPv6 incluye en su configuración la opción de "plug and play" esto significa que fácilmente cualquier equipo que soporte IPv6 se puede conectar a una red con este protocolo y se le asignara rápidamente una o varias direcciones IP [9].

D. Direccionamiento

Como ya se ha mencionado anteriormente las direcciones que se manejan en este protocolo son de 128 bits. Existen tres tipos de direcciones [10], que son:

- Unicast: Es la dirección que se asigna a una interfaz de red, esto quiere decir que cuando algún paquete se envíe a esta dirección va a llegar únicamente a ésta.
- Anycast: Un identificador para un conjunto de interfaces. Un paquete enviado a una dirección anycast se entrega a una de las interfaces identificadas por esa dirección, la más cercana, de acuerdo con la medida de distancia de los protocolos de enrutamiento.
- Multicast: Un identificador para un conjunto de interfaces. Un paquete enviado a una dirección multicast se entrega a todas las interfaces identificadas por esa dirección.

La representación de las direcciones IPv6 se hace de la forma "dirección/prefijo" las direcciones se encuentran en grupos de 16 bits usando la notación hexadecimal y separando dichos grupos por ":", un ejemplo de una dirección IPv6 es `12AB:0000:0000:CD30:0000:0000:0000:0000/60`.

Adicionalmente, se han previstos mecanismos para abreviar estas direcciones, suprimiendo o resumiendo las posiciones compuestas por varios 0´s. Es así como para la dirección presentada en el ejemplo anterior se puede llegar a la forma `12AB::CD3:0:0:0:0/60` o a la forma `12AB:0:0:CD3::/60` en donde un solo 0 indica que ese grupo de 16 bits son 0's y los "::" representan que todos los bits que faltan para completar la dirección contiene únicamente 0's.

E. Seguridad

IPv6 cuenta con varios mecanismos de seguridad implementados a través de IPSec. IPSec hace referencia a el conjunto de protocolos de seguridad implementados por IETF que proporciona el cifrado en la capa de red[11], sus especificaciones se encuentran en los RFC 2401[12], RFC 2402[13], 2406[14] y 2408[15].

Estos protocolos de seguridad están especificados para que sean usados tanto en IPv4 como en IPv6 pero este último cuenta con la ventaja que IPSec viene implementado de manera nativa. A continuación, se mostrarán algunas de las opciones de seguridad que se incluyeron específicamente para IPv6.

- Encabezados de autenticación: Con este encabezado en IPv6 se puede verificar la autenticación e integridad de la carga útil de datos. Este encabezado usa una asociación de seguridad establecida por el remitente y el destinatario de los paquetes, puede estar basada en el intercambio de claves secretas entre ambas partes.
- La autenticación en IPv6 crea un código de integridad del mensaje (MIC), este código es creado fusionando varios componentes del mensaje, tales como la llave que se mencionó en el punto anterior y la carga útil del mensaje, esto para eliminar por completo los posibles ataques de replicación, cuando el receptor del mensaje re-calcula el MIC, verifica la integridad de los datos con el fin de rectificar que le mensaje no fue alterado o reenviado durante su transmisión.
- Encabezado de fragmentación: En IPv4 se tenía la opción de fragmentar los paquetes a cualquier altura de la transmisión, esta opción fue eliminada en IPv6,

dejando sólo la opción de fragmentar en los nodos de inicio y fin, esto con el fin de asegurar la integridad de la información y su confidencialidad.

- Encapsulación de la carga útil de seguridad (ESP): Los encabezados de autenticación ayudan a verificar la integridad de los datos de una manera bastante efectiva pero no asegura que nadie pudo ver el contenido de información de los paquetes durante su transmisión. Esta opción de IPv6 permite el cifrado de los paquetes con unos altos índices de privacidad e integridad. Esta seguridad, ESP, es implementada en la capa de red. [16]

F. IPv4 vs IPv6

A continuación se presenta la tabla 1, en la cual se observa un resumen de las principales diferencias entre los protocolos IPv4 e IPv6. Es de mencionar nuevamente que estos protocolos no son compatibles, la subsistencia y comunicación entre los dos en un mismo ambiente de red dependerá de elementos de traducción que permitan convertir los paquetes, direcciones y forma de operación de cada uno de ellos en los equivalentes del otro, de los cuales se hablará más adelante.

TABLA 1.
COMPARACIÓN IPV4 E IPV6

	IPv4	**IPv6**
Año de desarrollo	1981	1999
Tamaño de direcciones	32 bits	128 bits
Formato de direcciones	Decimales separados por puntos (192.34.65.2), 4 grupos de 8 bits cada uno	Hexadecimal separados por dos puntos (4AB8:F834:AB7F:0000 :0000:0000:342A:F553), 8 grupos de 16 bits cada uno.
Notación (con máscara)	192.34.0.0/24	4AB8:F834:AB7F::/48
Número de direcciones	2^{32}	2^{128}
Fragmentación	Host + routers	Host
Velocidad	Menor	Mayor
Checksum	Si	No
Configuración	Manual	Automática

El uso de IPv6 soluciona varios de los problemas que se pueden encontrar en el protocolo IPv4, como por ejemplo la disponibilidad de direcciones y la facilidad de configuración, entre otras. Esto se debió, en una gran medida, a que la manera IPv4 llevaba en operación más de 20 años y esto facilitó la identificación de oportunidades de mejora, tales como las direcciones y campos innecesarios en los encabezados (ej. verificaciones redundantes y fallas de seguridad). Esto permitió que la IETF y el grupo de personas que desarrollaron las especificaciones del protocolo IPv6 incluyeran las soluciones a estos fallos de manera nativa.

G. Interacción IPv4 e IPv6

La integración del protocolo IPv4 y el protocolo IPv6 en este momento es una necesidad si se plantea la implementación de un ambiente local que funcione completamente en IPv6. Actualmente pensar en hacer una migración completa a IPv6 no es viable ya que más del 78% de internet se encuentra operando en un ambiente exclusivamente IPv4. Por ende, es necesario encontrar herramientas para lograr la convivencia entre el ambiente local que estaría usando el protocolo de siguiente generación con el protocolo IPv4.

Un ejemplo de sitio web configurado con el protocolo IPv6 es el portal de Google y según las estadísticas que publica con relación a la cantidad de personas que acceden su portal por medio del protocolo IPv6 (sólo IPv6), se ha encontrado que para 2018 fue entre un 20% y 25% aproximadamente [1].

Para realizar la integración antes mencionada es necesario implementar servicios de conversión IPv6 - IPv4, un ejemplo de estas implementaciones es NAT64. El cual, hace la traducción de las direcciones versión 4 a direcciones versión 6. Adicionalmente se requiere un servicio de traducciones de dominios, DNS64, que hace la traducción de dominios a las direcciones IPv6 (certificado de "AAAA") e IPv4 (certificado de "A") y viceversa.

H. NAT64

Como se indicó en la sección anterior, NAT64 es un protocolo que surgió a raíz de la necesidad de lograr la convivencia de los protocolos IPv4 e IPv6. Esta tecnología brinda la posibilidad de hacer una "traducción" de los encabezados, incluyendo direcciones, IPv4 a IPv6 y viceversa. Esta implementación es útil en ambientes locales (redes LAN) configuradas con IPv6 y que necesitan acceso a internet versión 4, por lo cual se necesita que los paquetes construidos inicialmente en IPv6 sean traducidos a IPv4.

Al realizar la búsqueda de diferentes tecnologías que permiten implementar este servicio, se encontraron las siguientes:

1) *Wrapsix:* Proyecto desarrollado por "xHire", el proyecto es de código abierto. Es una forma rápida de implementar NAT64 ya que el software brinda facilidades como la obtención de la dirección MAC de la inferfaz de red por la que entrará y saldrá el tráfico, además de hacer la traducción de IPv6 a IPv4 y viceversa. El proyecto está escrito en el lenguaje de bajo nivel "C"[17][18].
2) *Tayga:* Es una implementación de NAT64, utiliza el controlador TUN para intercambiar paquetes y así

lograr hacer la traducción de IPv6 a IPv4 y vicieversa. Es un proyecto que, así como Wrapsix, es de código abierto[19].

3) *Ecdysis:* Al igual que los anteriores proyectos mencionados, éste es de código abierto, fue desarrollado para funcionar sobre Linux y BSD. El traductor de las direcciones en Linux saca provecho del módulo de Kernel usando las facilidades de Netfilter y en BSD como una modificación de PF[20].

I. DNS64

Con NAT64 ya se tiene una traducción a nivel de capa IP, esta traducción permite el envío de paquetes de un host IPv6 a un host que cuente con una configuración IPv4, pero al momento de hacer una búsqueda por nombre, como por ejemplo "www.google.com", es necesario realizar la traducción de nombres a una dirección IP. Esta traducción también se entrega en diferente formato dependiendo de la versión del protocolo IP que se esté manejando; para que esta respuesta por parte del DNS sea compatible es necesario incluir en el sistema el servicio de DNS64, el cual se encarga del mismo procedimiento que un servidor DNS para IPv4 pero adicionalmente al momento de entregar la respuesta al host IPv6 incluye los registros AAAA que mapean las direcciones IPv4 junto con el prefijo NAT64.

Al igual que para el servicio NAT64, para DNS64 se hizo una revisión de soluciones que responden a estas necesidades y se encontraron las siguiente:

1) *TOTD:* Es el DNS64 que soporta la integración con el NAT64 Tayga, este software al igual que Tayga es un proyecto de código abierto [21].
2) *ECDYSYS DNS64:* Así como cualquier DNS64, éste permite que un host con IPv6 nativo logre ver contenido IPv4, ECDYSYS DNS64 se realizó para ser compatible con NAT64 fabricado por Ecdysis [22].
3) *BIND9:* según [17], es un DNS64 fácil de configurar y más rápido que las soluciones que proveen Tayga y Ecdysis. Es un estándar de facto para el servicio de DNS. Fue escrito desde ceros para superar dificultades arquitectónicas y soportar correctamente el protocolo IPv6.

J. DHCPv6

Ahora que ya se expuso, la solución para la convivencia de un ambiente local IPv6 con internet IPv4, se tiene otra necesidad y es la asignación de direcciones IPv6 para cada uno de los clientes. A pesar que el protocolo IPv6 permite que los clientes se auto configuren, en algunas ocasiones es necesario llevar un registro de las direcciones asignadas, para esto se requiere realizar la implementación del protocolo DHCPv6. Este protocolo se encarga de la asignación dinámica de direcciones IPv6 y se puede hacer de dos maneras stateless y stateful

1) *Stateless:* Stateless Address Autoconfiguration (SLAAC). Esta configuración tiene la ventaja de que no necesita interversión humana en ningún punto de la configuración. [23]
   En esta configuración se envía un Router Advertisement (RA) por parte del servidor DHCP o también puede ser el cliente quien haga esta solicitud por medio de un mensaje de solicitud RA. Este mensaje de Router Advertisement se envía por medio del protocolo ICMPv6. Luego del envío del mensaje el servidor le da al cliente un prefijo para que él configure una dirección IPv6 con base en su dirección MAC y su DUID (DHCPv6 Unique Identificator) y una ruta de salida (default gateway) que se la entrega el servidor [24].
   Ahora para que el servicio de DHCPv6 envíe también la información del DNS al cliente es necesario hacer configuraciones adicionales, dado que las banderas que permiten el envío de dicha información están deshabilitadas por defecto.
2) *Stateful:* En esta configuración en lugar de enviar el prefijo para que el cliente genere su propia dirección IPv6, el servidor le asigna una dirección junto con la ruta de salida y el DNS, esta configuración es exactamente igual a la que funciona hoy en día para IPv4 [25].

A pesar del funcionamiento y las ventajas que tiene el protocolo DHCPv6, en una infraestructura LAN en donde se realice la implementación del protocolo IPv6, es necesario el envío del gateway por parte del DHCPv6. Para que este envío se realice de manera correcta es necesario integrar DHCPv6 con la aplicación RADVD.

K. RADVD

Es un software de código abierto, la primera versión estable que salió al mercado fue el 1 de Febrero de 2017. Este software implementa enlaces de anuncios locales para IPv6 usando el protocolo Neighbor Discovery Protocol (NDP). Se encuentra especificado en el RFC 2461. [26][27]

Este software es usado por administradores de red para la configuración sin estado (stateless) en redes con clientes IPv6. Este software sirve como un complemento al DHCPv6 ya que está implementación hace más sencillo el envío del servidor DNS al momento de la asignación de las direcciones a los clientes.

IV. CASO DE IMPLEMENTACIÓN DE IPV6 EN UNA RED IPV4

A. Descripción del ambiente

Para la implementación de IPv6 en un ambiente real se contó con el apoyo del Laboratorio de Informática de la Escuela Colombiana de Ingeniería Julio Garavito en Bogotá, Colombia. Dicho laboratorio cuenta con servidores que soportan diferentes servicios, tales como:

1. Servidores Web
2. Bases de datos MySQL
3. Bases de datos Oracle
4. Directorio Activo (AD)
5. VPN
6. Proxy

Adicional a esto, el Laboratorio de Informática cuenta con más de 200 estaciones de trabajo con sistemas operativos Windows, Linux y Mac OS, en donde los estudiantes desempeñan sus labores diarias, como se puede ver en la Figura 2.

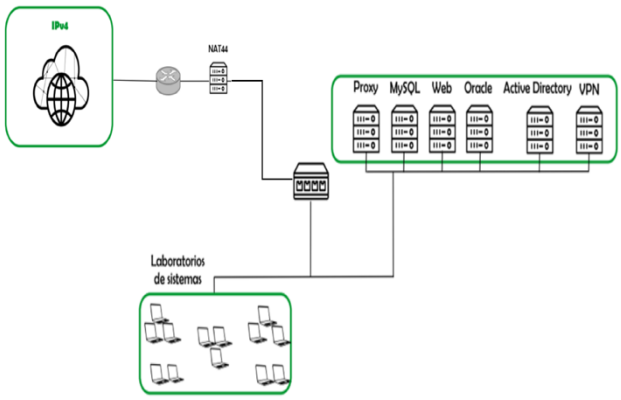

Figura 2. Infraestructura IPv4 del Laboratorio de Informática

B. Implementación

Se crearon los primeros servicios que fueron NAT64 y DNS64 y las pruebas de conectividad se hicieron con máquinas virtuales Windows server 2016.

Para este proceso se decidió que se utilizaría Wrapsix como herramienta NAT64, ya que su configuración es más amigable y su funcionamiento es más conveniente en la arquitectura de red que está implementada en el ambiente del Laboratorio de Informática. Adicionalmente se quizo aprovechar que el servicio de NAT64 opera a nivel de Kernel, esto ayuda a tener un mejor desempeño.

Como se mencionó anteriormente el laboratorio cuenta con varios servicios como Web, AD y bases de datos. Por este motivo se le solicitaron las especificaciones de estos servidores y algunas plantillas de los mismos al Laboratorio de Informática para crear el ambiente de pruebas.

En primera instancia se realizaron pruebas de conexión entre el protocolo IPv4 e IPv6, estas pruebas fueron realizadas en un ambiente controlado, con una conexión real a internet, como se observa en la figura 3.

Las pruebas se realizaron con los siguientes equipos y herramientas:

- Computador-servidor
- Una tarjeta de red dual stack
- SO Ubuntu client
- NAT64 y DNS64 Wrapsix
- Computadores cliente
- SO Windows 10
- Una tarjeta de red con configuración IPv6 e IPv4 inhabilitado
- Switch Capa 2
- Router
- Salida a internet

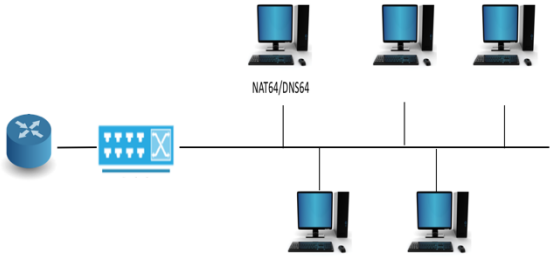

Figura 3. Ambiente de prueba

El servidor tenía instalado el sistema operativo Linux Slackware. Dicha instalación se hizo con los requerimientos mínimos para el funcionamiento de las herramientas NAT64 y DNS64, esto con el fin de no dejar brechas de seguridad a nivel de SO. Los requerimientos mínimos son:

a. Paquete A – Base Linux
b. Paquete D – C & C++
c. Paquete L – System libraries
d. Paquete N – Networking

NAT64, configuración básica de DNS64 y adicionalmente los necesarios para el funcionamiento del protocolo DHCPv6 y el software RADVD son las tecnologías que requiere esta solución para el ambiente de producción que se trabajó.

1) Instalación y configuración de nat64

En el computador que actúa como servidor se instaló el servicio de NAT64 para que haga la traducción de los paquetes IPv4 a IPv6 y viceversa.

En el computador-servidor se configuró la dirección IPv6 “2001:db8:1::1” a la interfaz de red “eth0” y la dirección IPv4 192.168.0.2 como se ve en la figura 4

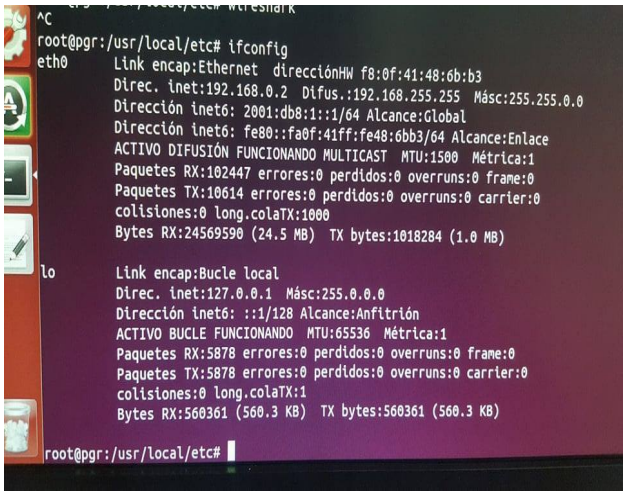

Figura 4. Configuración de las interfaces de red del computador-servidor

Posteriormente se configuró la ruta para el funcionamiento de Wrapsix con el comando “ip route add ::/0 dev eth0”, por útlimo se sigue la configuración que dice el archivo README dentro de la carpeta principal de Wrapsix, básicamente es la configuración de un archivo ubicado en /usr/local/etc/wrapsix.conf. Configurar el MTU (se deja por defecto en 1280 Bytes), el prefijo (éste quiere decir que cualquier paquete que le llegue a él con una dirección IPv6 que comience por 64:ff9b:: corresponderá a una dirección IPv4), la interfaz por donde se va a recibir y enviar el tráfico (nótese que esta interfaz tiene que ser dual stack, es decir, permitir enviar y recibir paquetes IPv4 e iPv6) y la dirección IPv4 dentro de la red (esta IP tiene que estar disponible).

Por último, se corre el programa Wrapsix para habilitar el servicio de NAT64 como se observa en la figura 5.

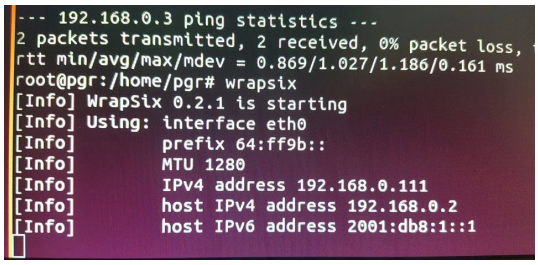

Figura 5. Servicio de NAT64 funcionando en el computador-servidor.

Ahora en los computadores cliente (Windows) se les configura una dirección IPv6 que esté en el mismo rango que la dirección asignada al servidor y se le asigna como gateway y DNS la dirección IPv6 del computador-servidor para que éste traduzca los paquetes y se obtenga la comunicación con el ambiente IPv4.

2) Configuración de DNS64

Para el caso de DNS64 se utilizó el software BIND9 que viene integrado en los sistemas operativos que se utilizaron en el proyecto, por lo cual no fue necesario realizar la instalación adicional del mismo.

Para complementar el servicio de DNS se realizó la configuración del servicio de DNS64 entrando al archivo /etc/named.conf y se realizó la configuración que se muestra en la figura 6, que básicamente permite configurar el puerto que se usará por el servicio de DNS, las direcciones IPv4 e IPv6 a las que le dará respuesta, el prefijo que se usó y el rango de direcciones que se excluyen, esto quiere decir el rango de direcciones que se le asignaron a los servidores y clientes de la red LAN.

Figura 6. Configuración archivo /etc/named.conf

Posteriormente se creó una zona de prueba llamada cpsc.com. Para esto, en el mismo archivo /etc/named.conf se realizó la configuración que se muestra en la figura 7, que consistió en definir la nueva zona dentro del servidor DNS.

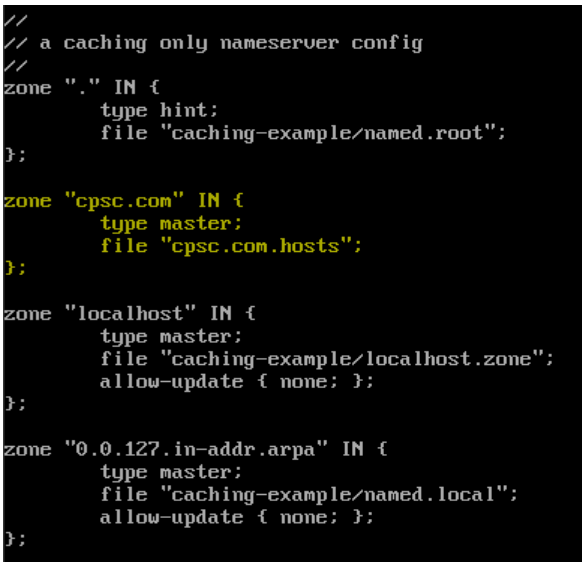

Figura 7. Configuración 2 del archivo /etc/named.conf

Después, se crea el archivo de configuración de la zona, que en el ejemplo es cpsc, en este caso será "etc/DNS/cpsc.com.hosts" como se ve en la figura 8, en donde se definen 3 servicios dentro de cpsc.com que son pgr, www y arena, y sus equivalencias en direcciones IPv6.

```
; /etc/DNS/cpsc.com.hosts file
$INCLUDE named-is.soa

cpsc.com.       IN      NS      pgr.cpsc.com.

pgr.cpsc.com.   IN      AAAA    2001:db8:1::1
www.cpsc.com.   IN      AAAA    2001:db8:1::4
arena.cpsc.com. IN      AAAA    2001:db8:1::10
```

Figura 8. Archivo cpsc.com.hosts,.

Se define el SOA (State Of Authotity), en el archivo named-is.soa y se define la versión. Cada vez que se haga una modificación en el archivo de los hosts (cpsc.com.hosts) se tiene que actualizar la versión del named-is.soa que como se ve en la figura 9.

```
;
$TTL    604800
$ORIGIN cpsc.com.
@       IN      SOA     pgr.cpsc.com. root.pgr.cpsc.com. (
        201802189
        43200
        3600
        432000
        86400
)
```

Figura 9. Archivo named-is.soa

Por último, se prende el servicio de DNS ejecutando los comandos que se ven en la Figura 10.

```
root@jhordy:/etc/rc.d# chmod +x rc.bind
root@jhordy:/etc/rc.d# ./rc.bind restart
Stopping BIND:  /usr/sbin/rndc  stop
rndc: neither /etc/rndc.conf nor /etc/rndc.key was found
Starting BIND:  /usr/sbin/named
root@jhordy:/etc/rc.d# _
```

Figura 10. Comandos para prender el servicio de DNS

Después de hacer la configuración de los archivos mencionados anteriormente, se prosigue a escalar el servicio para que soporte la arquitectura de DNS secundario o esclavos, de manera similar como se hace la configuración con el servicio de BIND para IPv4. Luego de realizar esta configuración se debe verificar que la solución está operando correctamente realizando pruebas de conectividad a internet usando IPv6.

3) Instalación y configuración de DHCPv6

Después de realizar la configuración mencionada en el apartado anterior, se prosigue a realizar la configuración del servicio de DHCP en donde el archivo de configuración se encuentra en /etc/dhcp/dhcpd6.conf. Para hacer la configuración de las direcciones IP con DHCP es necesario tener el "DUID de cliente DHCPv6" (en caso que se quiera hacer la asignación de una IP específica para cada cliente Windows). Este DUID se puede encontrar en los clientes corriendo el comando ipconfig /all ver figura 11.

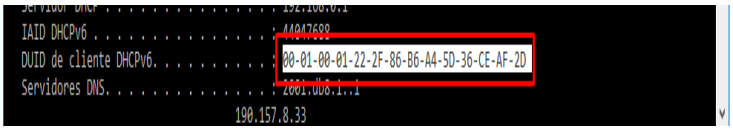

Figura 11. DUID en clientes IPv6

Posteriormente se descarga RADVD de la página oficial, se configuran las bandearas como se puede apreciar en la figura 12 y por último se corre RADVD con el fin que los clientes que están conectados a la red sepan que hay un servidor que les va a asignar una dirección IPv6 de tipo stateful, con una configuración completa que incluirá dirección IPv6, Gateway, DNS y máscara.

```
interface eth0

{
        MaxRtrAdvInterval 10;
        AdvSendAdvert on;
        AdvManagedFlag on;
        AdvOtherConfigFlag on;
        prefix 2001:db8:1::/64
        {
                AdvAutonomous off;


        };

};_
```

Figura 12. Archivo de configuración de RADVD

Luego de realizar las pruebas en un ambiente controlado y se prosigue a hacer la implementación en el ambiente de producción respectivo.

4) Configuración de otros servicios

Para la configuración real completo de la red IPv6 es necesario revisar otros servicios propios del escenario utilizado para la implantación, por ejemplo, el servidor de autenticación, (Directorio Activo de Windows - AD), servidores web y bases de datos.

En relación con el AD, para la autenticación de los clientes, se debe dejar la dirección IPv6 del servidor de AD como DNS de los hosts y el servidor de AD se debe configurar para que el servidor de DNS64 sea el que cumpla la labor de DNS. Esto se hace configurando el mismo servidor como un forwarder del DNS del servidor de AD.

Para los servicios web y servicios de bases de datos, la configuración que se realiza se reduce a habilitar la interfaz IPv6 en los servidores dejándolos configurados para recibir dirección IPv6 a través del protocolo DHCPv6 y RADVD.

5) Producto final

El producto final es una arquitectura similar a la mostrada en la Figura 13.

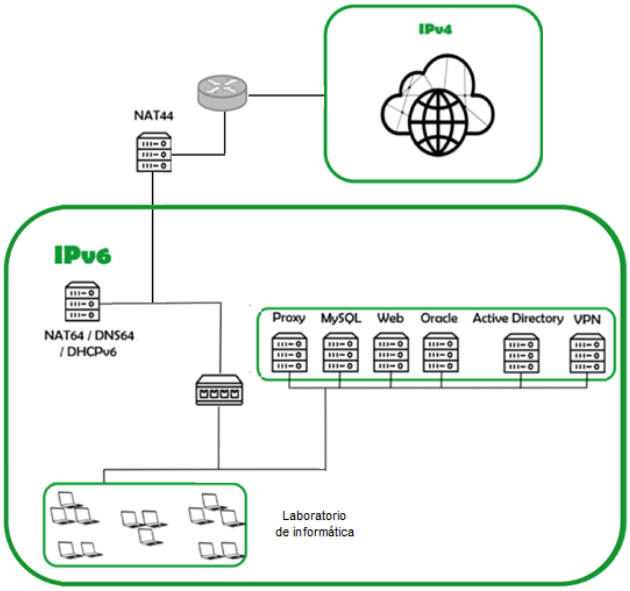

Figura 15. Arquitectura final del laboratorio de Informática de la Escuela Colombiana de Ingeniería Julio Garavito.

Se logró realizar la implementación de los servicios de NAT64, DNS64 y DHCPv6 en un ambiente productivo, permitiendo que las estaciones de trabajo navegaran y accedieran a los servicios que usualmente se usan en Internet. Además, se logró la migración exitosa de la mayoría de servicios ofrecidos en la infraestructura de prueba, esto incluye controladores de dominio, bases de datos, servicios web y ambientes de desarrollo, entre otros. Algunos servicios no fue posible migrarlos, tal es el caso de la VPN, la cual no se logró migrar por temas de conectividad con agentes externos y generación de certificados de VPN para IPv6. Adicionalmente, no se realizó la implementación de ip6tables para este ambiente, ya que las características de IPv6 anycast permiten que a pesar que el gateway bloquee la salida a internet, el paquete encuentre un dispositivo en su red que le brinde la posibilidad de usarlo como puente en la red hacia otras redes.

IV. Conclusiones

Las ventajas de IPv6 son pensadas con un alcance de gran magnitud, que en algún momento dejarán de ser ventajas para convertirse en necesidades comunes, implementando una migración temprana a esta tecnología se logra reducir costos en un cambio inminente.

Para realizar la migración del protocolo IPv4 al protocolo IPv6 se debe conocer detalladamente la infraestructura IPv4 instalada y los servicios que se prestan desde la misma para determinar las implicaciones la migración a IPv6 y planear así las pruebas que se deben ejecutar para lograr una implantación exitosa. Adicionalmente, es importante contar con un ambiente de pruebas lo más parecido posible al ambiente de producción para poder aplicar los cambios sobre este ambiente y realizar las pruebas planeadas antes de hacer la implementación sobre el ambiente productivo como tal.

Se encuentran gran cantidad de herramientas para la implementación de IPv6 pero no todas cumplen con las necesidades de la infraestructura que se desea migrar, es por eso que la identificación de herramienta es una fase crítica del proceso y se debe conocer a fondo dichas herramientas y cómo funcionan a bajo nivel ya que allí se puede encontrar la respuesta a la mayoría de los problemas que se presentan en el proceso de instalación, configuración y puesta en operación del sistema.

Referencias

[1] Google, "IPv6 – Google," 2018-04-24, 2018. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html. [Accessed: 24-Apr-2018].

[2] M. Luque, "La influencia de internet en la sociedad actual," SoloCiencia, 2015. [Online]. Available: http://www.solociencia.com/informatica/influencia-internet-sociedad-actual-origen-evolucion-historica.htm. [Accessed: 23-Aug-2017].

[3] C. Holloway, "Las redes al 2017: el desenfrenado crecimiento de la información que generamos," TecnoAmerica, 2013. [Online]. Available: https://tecno.americaeconomia.com/articulos/las-redes-al-2017-el-desenfrenado-crecimiento-de-la-informacion-que-generamos. [Accessed: 23-Aug-2017].

[4] S. Hagen, IPv6 essentials - Integrating IPv6 into Your IPv4 Network. 3rd Edition. Silvia Hagen. P. 414. O'Reilly, ASIN: B011DBDPH4. June 2014.

[5] J. L. Alcoba, "NAT (Network Address Translation): Qué es y cómo funciona," Xatakamovil, 2014. [Online]. Available: https://www.xatakamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona. [Accessed: 24-Aug-2017].

[6] L. Y. Becerra-sánchez, B. Valencia-suárez, and S. Santacruz-pareja, "Uso de Mininet y Openflow 1 . 3 para la enseñanza e investigación en redes IPv6 definidas por software," vol. 12, no. 24, pp. 89–96, 2017.

[7] Scientia, "IPv6 en la universidad de Pamplona: Estado de arte," vol. 37, 2007.

[8] S. E. Deering, "Internet Protocol, Version 6 (IPv6) Specification," 2008. [Online]. Available: https://tools.ietf.org/html/rfc2460. [Accessed: 27-Aug-2017].

[9] A. Martinez, "IPv6 (Características, ventajas y desventajas)," Alejandro Martinez, 2016. [Online]. Available: https://alejandromartinezclase.wordpress.com/ipv6-caracteristicas-ventajas-y-desventajas/. [Accessed: 29-Aug-2018].

[10] R. M. Hinden and S. E. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture," 2003.

[11] J. Domingo, A. Pascual et al., "Ipv6 - More than a protocol.". Novática [Online]. Available: http://www.cepis.org/upgrade/files/full-2005-II.pdf. [Accessed: 27-Aug-2018].

[12] R. Atkinson and S. Kent, "Security Architecture for the Internet Protocol.". RFC Editor, United States. DOI 10.17487/RFC2401.

[13] R. Atkinson and S. Kent, "IP Authentication Header.". RFC 4302. IETF – Network working group. 2005

[14] P. Wouters, D. Migault, J. Mattsson, Y. Nir, T. Kivinen, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)).". RFC 8221. IETF. ISSN: 2070-1721. October 2017.

[15]T. Kivinen and J. Snyder, “Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)”. RFC 7427. IETF. ISSN: 2070-1721. January 2015.
[16]M. A. Badamchizadeh, M. Ali, and A. Chianeh, “Security in IPv6,” wseas, 2006.
[17]xHire, “WrapSix – the fastest software NAT64.” [Online]. Available: https://www.wrapsix.org/. [Accessed: 26-Nov-2017].
[18]J. Miguel, M. Bier, C. Miguel, and T. Calafate, “Instalación de una infraestructura de red IPv6,” 2009.
[19]Litech, “Tayga README,” 2010. [Online]. Available: http://www.litech.org/tayga/README-0.9.2. [Accessed: 30-Nov-2017].
[20]Viagenie, “Ecdysis: open-source implementation of a NAT64 gateway,” 2017. [Online]. Available: https://ecdysis.viagenie.ca/.
[21]W. Project, “TOTD DNS64,” Dillema, 2012.
[22]J. C. Alonso and C. Marenez, “NAT64 / DNS64 Comunicando los mundos v4 – v6,” 2011.
[23]Cisco, “DHCPv6 Based IPv6 Access Services,” 2011. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html. [Accessed: 25-Apr-2018].
[24]S. Thomson, “IPv6 Stateless Address Autoconfiguration.”
[25]Nir Yechiel’s blog, “IPv6 address assignment – stateless, stateful, DHCP… oh my!,” 2014. [Online]. Available: https://thenetworkway.wordpress.com/2014/07/02/ipv6-address-assignment-stateless-stateful-dhcp-oh-my/. [Accessed: 25-Apr-2018].
[26]Wikipedia, “Radvd,” 2018. [Online]. Available: https://en.wikipedia.org/wiki/Radvd. [Accessed: 25-Apr-2018].
[27]W. A. Simpson and E. Nordmark, “Neighbor Discovery for IP Version 6 (IPv6),” IETF, 1998.