INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

Diseño e implementación de una red IPv6 para transición eficiente desde IPv4

ELECTRICAL AND ELECTRONICS ENGINEERING

Design and implementation of IPv6 network for efficient transition from IPv4

Luis E. Bolivar*, Fabio G. Guerrero, Oscar Polanco** §**

**Infomedia, EMCALI;*
***Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Cali, Colombia;*

eduardo87060@gmail.com,fabio.guerrero@correounivalle.edu.co,
§ oscar.polanco@correounivalle.edu.co

(Recibido: Abril 24 de 2012 - Aceptado: Noviembre 19 de 2012)

Resumen

En este trabajo se presentan el diseño e implementación de una red IPv6 para la transición fácil y eficiente de IPv4. Se implementa un modelo que tiene una red IPv6 nativa en la oficina central de una red corporativa y que utiliza mecanismos de transición para la conexión a Internet IPv4, Internet IPv6 y oficinas remotas. Lo anterior tiene el propósito de ofrecer una alternativa viable para implementar IPv6 de forma nativa, sin perder acceso a los servicios IPv4 y sin incurrir en las desventajas que implican otras aproximaciones en términos de requerimientos de administración y seguridad, inherentes al funcionamiento de IPv4 e IPv6 simultáneamente. La integración del software GNS3 con VirtualBox representa una herramienta que permite hacer pruebas dentro de un solo computador para validar cada uno de los pasos en el proceso de migración hacia IPv6, sin perturbar una red IPv4 en operación.

Palabras clave: *Doble pila, Mecanismos de transición desde IPv4 a IPV6, MPLS, Mecanismos tipo túnel.*

Abstract

This paper reports both the design and implementation of an IPv6 network for easy and efficient transition from IPv4. A model that has a native IPv6 network in the central office of a corporate network using transitional mechanisms for the connection into an IPv4 Internet, IPv6 Internet, and remote offices is implemented. This is intended to offer a viable alternative for implementing IPv6 natively, without losing access to IPv4 services and incurring the disadvantages of other approaches in terms of both management and security requirements, inherently present in the simultaneously operation of IPv4 and IPv6. The GNS3 software integration with VirtualBox represents a tool that allows testing within a single computer to validate each of the steps in the process of migration to IPv6, without disrupting an operating IPv4 network.

Keywords: *Dual stack, IPv4 to IPv6 transition mechanisms, MPLS, Tunnel type mechanisms.*

1. Introducción

El enorme crecimiento del número de usuarios y dispositivos que hacen uso de la Internet ha ocasionado un rápido agotamiento de las direcciones IPv4, razón por la cual la implementación de IPv6 (Deering & Hinden, 1998) ha generado un gran interés y expectativa a nivel mundial.

En Colombia, la necesidad de implementar IPv6 se evidencia en la circular 000002 del 6 de Julio del 2011 con asunto "Promoción de la Adopción de IPv6 en Colombia" del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2010), donde uno de sus propósitos es garantizar que la tecnología proyectada (IPv6) sea la adecuada para cumplir sus metas, ya que dentro de su plan "Vive Digital Colombia" se tiene como objetivo principal ampliar el número de usuarios de Internet banda ancha de 2.2 a 8.8 millones de suscriptores en el periodo comprendido entre el 2010 y 2014.

Con respecto a la implementación de IPv6 varios de los trabajos y directrices que se han reportado, se han hecho extendiendo la funcionalidad de doble pila sobre la red, con el fin de que IPv6 pueda funcionar sin afectar la operación normal de la red IPv4, 6NET, (2005); Frankel et al., (2010). Otra estrategia consiste en separar la infraestructura IPv6 de la infraestructura IPv4 (Bolívar, 2012), donde se implementan sitios IPv6 nativos independientes de los sitios IPv4 y mediante el mecanismo de transición ISATAP (Intra Site Automatic Tunnel Addressing Protocol) se ofrece conectividad IPv6 a las estaciones con soporte IPv6 que se encuentran ubicadas en los sitios IPv4, (Templin et al., 2008; Blanchet, 2006). Además, como complemento de ISATAP se utilizan sitios doble pila para brindar los servicios de la red comunes a IPv4 e IPv6.

Cualquiera de las dos alternativas mencionadas antes para implementar IPv6, funciona bien y permite la coexistencia de IPv4 e IPv6 dentro de una misma red, pero éstas presentan ciertas desventajas inherentes al funcionamiento de IPv4 e IPv6 de forma simultánea, entre las cuales se encuentran:

a) Un mayor consumo de recursos debido a que se debe brindar soporte para ambos protocolos; esto tiene implicaciones, entre otros, en los servidores DHCP, tablas de encaminamiento y aplicaciones.

b) Necesidad de mayor administración de la red, ya que se deben establecer políticas de seguridad tanto para IPv4 como para IPv6.

c) Se sigue dependiendo fuertemente de las direcciones IPv4.

Con respecto a la transición de las redes IPv4 hacia IPv6, varios gobiernos han creado políticas y directrices para que este cambio sea de obligatorio cumplimiento en las entidades del Estado dentro de un plazo razonable. En muchas entidades públicas (por ejemplo, la Universidad del Valle) y privadas la infraestructura de red ya soporta IPv6. Uno de los mayores obstáculos que ha frenado el uso de dicho protocolo es el temor a que se afecte de manera crítica la operación de la red IPv4 y, a su vez, la operación y producción de la entidad. La mayoría de implementaciones de IPv6 se hacen conservando en paralelo el funcionamiento de IPv4, ya sea en un escenario de doble pila o implementando ambos protocolos por separado. En este trabajo se propone un modelo con una aproximación distinta, la cual consiste en la implementación de una red IPv6 nativa que utiliza algunos mecanismos de transición desde IPv4 para suplir las necesidades de interconexión. Esta aproximación cuenta con las siguientes ventajas:

a) La red trabaja sólo con IPv6 y por tanto no tienen lugar las desventajas asociadas al consumo de recursos que se presentan en una implementación de doble pila.

b) Se disminuye considerablemente la dependencia de direcciones IPv4; sólo se necesitan direcciones IPv4 para los equipos donde se aplican los mecanismos de transición.

c) Cuando el tamaño y uso de la red IPv6 que se implemente predomine sobre el tamaño y uso de la red IPv4 heredada y llegue el momento de desactivar IPv4, hacerlo resultará mucho más sencillo que en una implementación de

doble pila, ya que, en el esquema propuesto, los mecanismos de transición son implementados en unos pocos equipos y en un proceso que se ejecuta de forma transparente al resto de la red; por lo tanto, bastará con realizar el cambio en estos equipos e IPv4 será totalmente desactivado.

En este orden de ideas, en este trabajo se hacen las siguientes contribuciones: se diseña, implementa y valida el modelo de una red IPv6 nativa con conexión a Internet IPv6, Internet IPv4 y oficinas remotas IPv6. Este esquema puede ser considerado por las entidades públicas y privadas como una opción para realizar la transición de su infraestructura de red a IPv6. También se presenta una introducción al funcionamiento de los mecanismos de transición que permiten la interconexión de la red, se explica cómo se deben emplear estos mecanismos y se presentan los resultados que demuestran que los mecanismos abordados funcionan correctamente y posibilitan el logro de los resultados esperados.

2. Metodología

Los elementos constitutivos del modelo son: el establecimiento de una conexión IPv6 entre las oficinas remotas y la red de la oficina central mediante 6PE (camino 1 en la parte inferior de la figura 1), para obtener una Intranet IPv6 nativa; proveer el servicio de Internet IPv6 a la Intranet mediante 6to4 (camino 2 en la parte superior de la figura 1); conservar el acceso al servicio Internet IPv4 para la Intranet mediante el uso de NAT64 y DNS64 (figura 2).

2.1 Implementación de IPv6 de forma nativa

El principal inconveniente para utilizar IPv6 de forma nativa en la oficina central de una red corporativa (red interna o red de campus), es que IPv6 no está ampliamente implementado en las redes de los ISP, entonces si se implementa IPv6 de forma nativa en la oficina central de una red corporativa y el ISP no provee conexión directa para este protocolo, la red de la oficina central perdería toda conectividad externa, esto incluye Internet y la conexión a oficinas remotas, incluso si estas son compatibles con IPv6. Para solucionar este problema se pueden utilizar los siguientes dos mecanismos de transición: 1. 6PE sobre MPLS (Cisco, 2002), el cual permite que los sitios IPv6 se comuniquen usando caminos conmutados de etiquetas sobre un núcleo MPLS IPv4. 2. Túnel 6to4 (Carpenter & Moore, 2001), el cual es un mecanismo de túnel automático que usa infraestructura IPv4 para permitir la comunicación de dominios IPv6. Como consecuencia de esta solución se pierde conectividad a Internet IPv4, lo cual hace necesario utilizar como tercer mecanismo de transición a NAT64 (Bagnulo et al., 2011a), el cual se encarga de trasladar los datagramas IPv6 a IPv4, en conjunto con el mecanismo DNS64 (Bagnulo et al., 2011b) que permite la resolución de nombres. Estos mecanismos permitirán la implementación de IPv6 de forma nativa en la oficina central sin que se pierdan sus conexiones externas. En la figura 1 se presenta la red diseñada, en la cual se tiene una red IPv6 nativa con tres encaminadores de borde, uno para la conexión con oficinas remotas "R2. IPv6", otro para la conexión a Internet IPv6 "R. 6TO4" y finalmente uno para conexión con Internet IPv4 "R. NAT64", en la tabla 1 se presentan las direcciones de los dispositivos de la red que intervienen en el proceso de transición.

El funcionamiento de la red presentada en la figura 1 se comprobó a través del uso de una plataforma de pruebas utilizando la integración del software de emulación de redes empaquetado en GNS3 (Grossmann at al., 2008) y de estaciones virtuales emuladas con VirtualBox (Oracle, 2009), dichos programas se ejecutaron sobre un computador físico con sistema operativo Ubuntu 11.04. Se usó GNS3 v0.7.3 y el emulador Dynamips v0.2.8.3 for Linux 32 bits. Es de anotar que para la plataforma de pruebas utilizada, las funciones que realizan las máquinas virtuales mediante VirtualBox también se pueden obtener con cualquier otro paquete de software equivalente (por ejemplo, VMware). No obstante, para obtener las funciones requeridas en las pruebas mediante el uso de GNS3, es necesario asegurarse de que la plataforma de enrutamiento seleccionada para ser emulada por GNS3 soporte los protocolos IPv6, BGP y MPLS. Lo anterior

también aplica cuando se desee remplazar GNS3 por Juniper JunOS o Quagga/Zebra (el sitio web de este último no reporta soporte de MPLS). En las siguientes secciones se describe el funcionamiento de la red y la forma en que los mecanismos de transición solucionan las necesidades de la conexión externa.

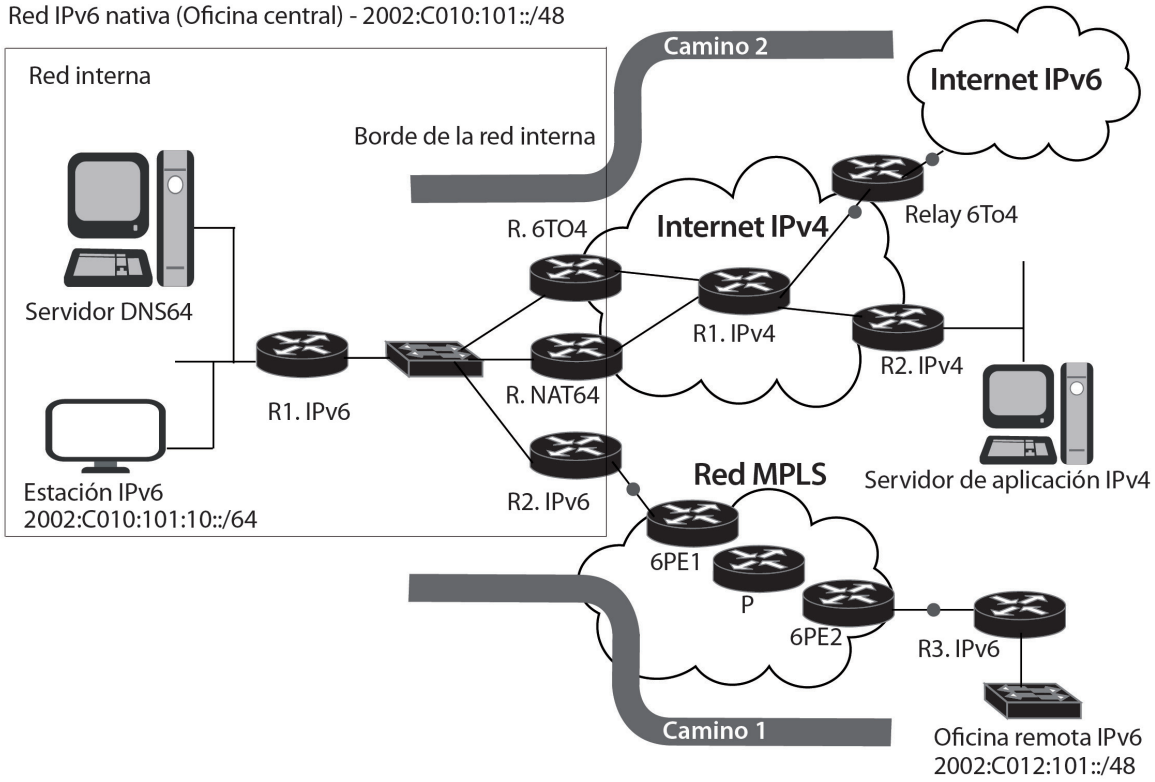

Figura 1. *Red IPv6 diseñada con los mecanismos 6to4, NAT64 + DNS64 y 6PE sobre MPLS.*

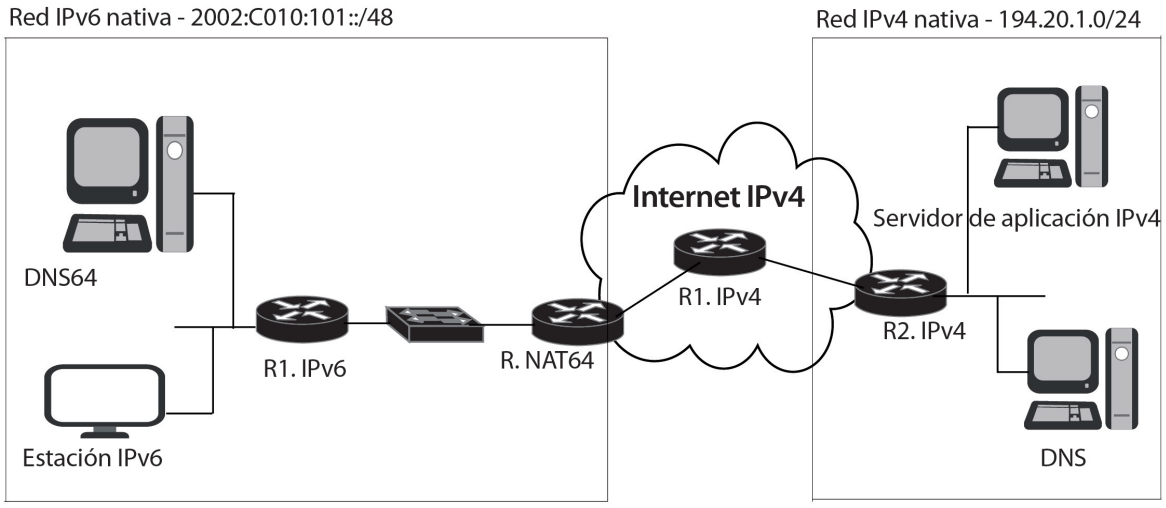

Figura 2. *Funcionamiento del mecanismo NAT64 + DNS64.*

Tabla 1. *Direcciones y parámetros importantes en los dispositivos de la red diseñada.*

Equipo	Direcciones y parámetros	Destino
R1. IPv6	2002:C010:101:64::1/64 2002:C010:101::10/64	Red interna Routers de borde
R2.IPv6	2002:C010:101::8/64 2002:C010:101:8::1/64	Red interna Oficinas remotas
6PE1	2002:C010:101:8::2/64 192.30.1.1/24	Red del usuario Red MPLS
P	192.30.1.2/24 192.40.1.2/24	6PE1 6PE2
6PE2	2002:C010:101:9::2/64 192.40.1.1/24	Red del usuario Red MPLS
R3.IPv6	2002:C012:101::9/64 2002:C010:101:9::1/64	Oficina remota Conexión a la Red diseñada
R.6to4	2002:C010:101::1/64 192.16.1.1/24	Red interna Internet IPv4
R1.IPv4	192.16.1.2/24 192.16.4.2/24 192.18.1.2/24 192.19.1.2/24	R.6to4 R.NAT64 Relay.6to4 R2.IPv4
Relay.6to4	2000:1000:100::1/64 192.18.1.1/24	Internet IPv6 Internet IPv4
R.NAT64	2002:C010:101::64/64 192.16.4.64/24	Red interna Internet IPv4
R2.IPv4	192.19.1.1/24 194.20.1.1/24	Internet IPv4 Red IPv4

2.2 Conexión con las oficinas remotas

Las alternativas estáticas existentes para transportar IPv6 sobre un túnel IPv4 y dar servicio IPv6 a las oficinas remotas son túnel configurado manualmente e IPv6 sobre túnel GRE IPv4. Estas opciones son difíciles de gestionar cuando el número de oficinas aumenta, especialmente en topologías completamente enmalladas. Las alternativas dinámicas son: 1. Tunnel Broker, requiere que el servicio soporte cambios remotamente y tiene implicaciones de seguridad. 2. Túnel 6to4, debido a que la dirección IPv4 pública subyacente determina el valor de los 32 bits siguientes al prefijo 2002::/16, una futura migración en la que se requiera que IPv6 sea el único protocolo de red (a lo cual se le denomina IPv6 nativa o IPv6-only) requiere un cambio en la numeración de las direcciones IPv6. 3. IPv6 sobre MPLS, usa la infraestructura MPLS existente y puede ser dispendioso de configurar dependiendo del método subyacente utilizado (IPv6 en circuitos de transporte sobre MPLS, IPv6 usando túneles IPv4 en los encaminadores de borde de usuario o IPv6 con núcleo MPLS basado en IPv4 "6PE/6VPE"). Para el camino 1 de red entre los equipos "R2. IPv6" y "R3 IPv6" de la figura 1 se presenta la alternativa seleccionada para solucionar la conexión con las oficinas remotas IPv6, la cual consiste en la implementación por parte del ISP del mecanismo 6PE sobre MPLS; este mecanismo consiste en activar el intercambio de rutas IPv6 entre los encaminadores de borde del proveedor (equipos 6PE1 y 6PE2 en la figura 1).

La ventaja de este mecanismo es que no requiere la realización de cambios en el núcleo MPLS ya que una vez el datagrama IPv6 llega a los equipos 6PE, es encapsulado dentro de MPLS y el encaminamiento se hace a nivel de etiquetas

y no de IP, lo cual permite transportar paquetes IPv6 sobre una red MPLS IPv4 (Dooley & Brown, 2007).

Para que los encaminadores 6PE (PE) intercambien información sobre las rutas IPv6, aparte de la configuración normal que se utiliza para el intercambio de rutas sobre redes MPLS, se les debe adicionar los comandos que se presentan en la figura 3 para equipos con la plataforma IOS del fabricante Cisco. La línea 6 de la figura 3 presenta el comando clave que activa el envío de las rutas IPv6 a la dirección IPv4 que se especifica y que en este caso pertenece al PE con el cual se quiere realizar el intercambio de las rutas.

```
1  mpls ipv6 source interface loopback0
2  !
3  router bgp (número que identifica al sistema autónomo [AS] BGP)
4  address-family ipv6
5  neighbor (dir. IPv4 del 6Pe) activate
6  neighbor (dir. IPv4 del 6PE) send-label
7  exit-address-family
8  !
```

Figura 3. *Configuración adicional para activar el intercambio de rutas IPv6 entre equipos 6PE.*

2.3 Conexión a Internet IPv6

La conexión a Internet IPv6 se aborda suponiendo un escenario donde el ISP sólo ofrece conexión a Internet IPv4. Una solución es emplear un túnel entre la red IPv6 nativa y un encaminador que pueda ser utilizado como puente de conexión entre Internet IPv4 e Internet IPv6. Para el escenario propuesto se implementó el mecanismo tipo túnel 6to4 sobre el camino 2 existente entre los equipos "R. 6TO4" y "Relay 6TO4" de la figura 1, esto debido a que dicho mecanismo es automático, sencillo de configurar y proporciona un bloque de direcciones IPv6 válidas que sirven para conectar la red a Internet IPv6 (el mecanismo Tunnel Brokers o el mecanismo 6rd también proporciona la misma funcionalidad), lo cual es realmente útil cuando el ISP no ofrece bloques de direcciones IPv6. Es importante anotar que si una red que utiliza 6to4, logra tener una conexión directa a Internet IPv6 y recibir un bloque de direcciones IPv6 globales, ésta puede mantener el esquema de numeración que venía utilizando con 6to4 ya que basta con cambiar los primeros 48 bits del bloque de direcciones 6to4, por los obtenidos del ISP al cual se conecte.

El mecanismo 6to4 funciona creando un bloque de direcciones IPv6 a partir de una dirección IPv4 perteneciente al encaminador encargado del túnel (en este caso "R. 6TO4"). Esto se hace para que cuando otro encaminador 6to4 desee enviar un paquete a la red IPv6 nativa, éste pueda extraer de la dirección IPv6 destino la dirección IPv4 a donde se debe enviar el paquete encapsulado. 6to4 es un mecanismo que se realiza de forma transparente a la red, por lo tanto, no se necesita realizar configuraciones especiales sobre ésta, lo único que se necesita es que el encaminador 6to4 sea utilizado como puerta de enlace para alcanzar a Internet IPv6. Además de habilitar el funcionamiento de 6to4 (Cisco, 2008) sobre el encaminador de borde "R. 6TO4", éste debe estar configurado para utilizar un relay 6to4 (un relay 6to4 es un encaminador 6to4 que se encuentra conectado a Internet IPv4 y a Internet IPv6) que servirá como puente para conectarse con Internet IPv6.

La configuración del encaminador "R. 6to4" para plataformas del fabricante Cisco se presenta en la figura 4. En las líneas 1 a 4 de la figura 4 se encuentran los comandos necesarios para implementar 6to4. En las líneas 6 y 7 se establecen las rutas necesarias para que el mecanismo pueda funcionar; en la línea 6 se configura la dirección del relay 6to4 que se encargará de conectar la red a IPv6 y la línea 7 sirve para que cuando el encaminador tenga que enviar un paquete a un destino 6to4, lo haga encapsulando el paquete en IPv4 utilizando como destino la dirección IPv4 embebida en la dirección 6to4.

```
1  interface tunnel 0
2  ipv6 address (asignar dir. IPv6 a la interfaz tunnel 0)
3  tunnel source (nombre de la interfaz física conectada a IPv4)
4  tunnel mode ipv6ip 6to4
5  !
6  ipv6 route ::/0 (dirección del relay 6to4)
7  ipv6 route 2002::/16 tunnel (número asignado al túnel )
8  !
```

Figura 4. *Configuración del encaminador 6to4.*

2.4 Conexión a Internet IPv4

La razón principal por la que se implementa IPv6 en escenarios de doble pila es para poder seguir utilizando los servicios que actualmente se prestan con IPv4; hay que reconocer que aunque IPv6 es superior en muchos sentidos a IPv4, la mayoría de servicios que actualmente se prestan en la Internet lo hacen bajo IPv4, y no resulta aceptable implementar una red que no pueda acceder a estos servicios. Para resolver esta necesidad se implementó el mecanismo NAT64 en combinación con DNS64 representados en la figura 2. Este mecanismo de traducción le permite a la red IPv6 nativa diseñada, acceder a servicios de la Internet IPv4, evitando así los inconvenientes que se presentan en una red doble pila.

El mecanismo NAT64 funciona por medio de un servidor DNS64 que recibe las consultas de clientes IPv6, el servidor DNS64 a su vez se comunica con otros servidores DNS (Albitz & Liu, 2006) ubicados en Internet. Cuando la consulta corresponde a un nombre de host que tiene dirección IPv4, el DNS64 transforma esta dirección en una dirección IPv6 anteponiéndole el prefijo que identifica el servicio NAT64. La red debe estar configurada de tal forma que los paquetes enviados a un destino que contenga el prefijo del NAT64, utilicen el encaminador NAT64 como puerta de enlace, la función de este encaminador es convertir paquetes IPv6 en paquetes IPv4 y viceversa.

El servidor DNS64 debe comunicarse con otros servidores DNS IPv4 para resolver nombres de dominios. Puesto que el servidor DNS64 se encuentra en la red IPv6 nativa, se le realizó a éste una modificación que consistió en configurar las direcciones de los servidores DNS IPv4 externos como direcciones IPv6 utilizando el prefijo del NAT64, de esta manera cuando el servidor DNS64 necesite realizar una consulta a un DNS IPv4, lo hará mediante IPv6 utilizando al encaminador NAT64 como puerta de enlace y éste se encargará de realizar las traducciones correspondientes.

En la implementación de este escenario se utilizó el servidor de nombres de dominio de Internet de Berkeley BIND para proveer los servidores DNS64 y DNS (Internet Systems Consortium, 2012) de la figura 2. Para implementar el encaminador NAT64, se utilizó un desarrollo de la firma Viagénie denominado "Ecdysis: open-source implementation of a NAT64 gateway", el cual permite habilitar una estación para que realice las funciones de este encaminador. El encaminador NAT64 que se implementó dentro de una estación, es un mecanismo relativamente nuevo que se encuentra implementado solamente en encaminadores modernos.

Para activar el funcionamiento de DNS64 se debe adicionar al archivo de opciones del servidor BIND la configuración presentada en la figura 5. Para activar el funcionamiento del encaminador NAT64, basta con descargar el disco compacto "cd-live" que se encuentra disponible en Viagénie (2010), configurar las direcciones IPv4 e IPv6 sobre las interfaces de la estación y ejecutar el script de configuración "nat64-config.sh" que se encuentra dentro del "cd-live".

```
1  dns64 64:ff9b::/96{
2  clients{Any;};
3  };
```

Figura 5. *Activando la función de DNS64.*

3. Resultados y discusión

3.1 Mecanismo 6PE sobre MPLS

La figura 6 presenta una captura tomada desde el terminal del encaminador "R3. IPv6" de la oficina remota, donde se puede comprobar el funcionamiento de este mecanismo con la realización de una interrogación hacia una estación perteneciente a la red interna de la oficina central IPv6 nativa. En la figura 6 se puede observar que mediante un intercambio BGP con el equipo 6PE2, el encaminador del usuario "R3. IPv6" obtuvo información sobre las rutas de la red de la oficina central IPv6 nativa (2002:C010:101::/48). A su vez, el equipo 6PE2 obtuvo dichas rutas del equipo 6PE1 mediante el protocolo BGP. El hecho de que la prueba de interrogación (mensaje ICMP) se pudo realizar de manera satisfactoria, demuestra que la red de la oficina remota (IPv6 nativa) se puede conectar a la oficina central (IPv6 nativa) mediante una red MPLS basada en IPv4. Hay que resaltar que el mecanismo implementado aquí requiere de la intervención del ISP. Si no es posible la intervención del ISP, se pueden utilizar mecanismos de tipo túnel como 6to4 o túneles manuales, dichos túneles se deben configurar entre las redes de la oficina central y las oficinas remotas para que estas se puedan conectar de forma transparente al ISP.

```
oficina_remota#:sh ipv6 route bgp
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS Ll, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OEl - OSPF ext 1, OE2 - OSPF ext 2
       ONl - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
B      2002:C010:101::/64 [20/0]
        via FESO::C003:FFF:FEF8:l, FastEthernetO/O
B      2002:C010:l01:8::/64 [20/0]
        via FE80::C003:FFF:FEF8:1, FastEthernetO/O
B      2002:C010:10l:64::/64 [20/0]
        via FE80::C003:FFF:FEF8:1, FastEthernetO/O

oficina_remota#ping 2002:c0l0:10l:64::20
Type escape sequence to abort.
Sending 5, l00-byte ICMP Echos to 2002:C010:101:64::20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/88/120 ms
```

Figura 6. *Prueba de conexión entre las redes de la oficina central y la oficina remota.*

3.2 Mecanismo 6to4

La figura 7 presenta una captura realizada desde el terminal de una estación Ubuntu 10.04, ubicada dentro de la red IPv6 nativa, probando que existe conexión entre la red IPv6 nativa y la Internet IPv6 representada por la dirección IPv6 global 2000:1000:100::1/64. Como se puede observar en la figura 7, el mensaje ICMP de solicitud de eco obtiene sus respectivas respuestas, lo que demuestra que la red nativa IPv6 se encuentra habilitada para conectarse con cualquier red alcanzable por el relay 6to4, es decir, con cualquier red que forme parte de Internet IPv6.

3.3 Mecanismo NAT64 y DNS64

Las líneas 1 a 4 de la figura 8 presentan una captura para verificar el funcionamiento de este mecanismo. En la figura 8 se puede observar la interrogación desde la estación IPv6 de la red IPv6 nativa de la oficina central hacia el servidor de aplicación IPv4 (pc1.bolivar.com) ubicado

en una red IPv4 y al que le corresponde la dirección 194.20.1.20. Como se puede observar, la estación realiza la interrogación a una dirección IPv6 generada por el DNS64, el cual le antepone el prefijo NAT64 64:ff9b::/96 al sufijo C214:114, este último corresponde a la notación hexadecimal de la dirección 194.20.1.20. Para lograr que la estación pueda tener conexión a la dirección IPv6 obtenida por medio del DNS64 (es decir, que la estación pueda comunicarse con la red IPv4), es necesario que su encaminador más cercano "R1.IPv6" se configure para que los paquetes con destino a la dirección 64:ff9b::/16, utilicen el encaminador NAT64 "R. NAT64" como puerta de enlace. Las líneas 5 a 8 y 9 a 12 de la figura 8 presentan una captura realizada con el analizador de protocolos Wireshark (Combs, 1998) sobre las dos interfaces de "R. NAT64". Al correlacionar las dos figuras, se puede deducir que el encaminador recibe los paquetes IPv6 en su interfaz conectada a la red IPv6 nativa, convierte los paquetes IPv6 en paquetes IPv4, y envía dichos paquetes IPv4 hacia su respectivo destino, usando su interfaz conectada a la red Internet IPv4. En el sentido contrario se presenta el proceso opuesto en la traducción de los paquetes IP.

```
eduardo@eduardo-laptop:~$ ping6 2000:1000:100::1
PING 2000:1000:100::1(2000:1000:100::1) 56 data bytes
64 bytes from 2000:1000:100::1: icmp_seq=l ttl=62 time=121 ms
64 bytes from 2000:1000:100::1: icmp_seq=4 ttl=62 time=99.4 ms
```

Figura 7. *Prueba de la conexión de la red IPv6 nativa con Internet IPv6.*

```
1. eduardo@eduardo-laptop:~$ ping6 pc1.bolivar.com
2. PING pc1.bolivar.com(64:ff9b::c214:114) 56 data bytes
3. 64 bytes from 64:ff9b::c214:114: icmp_seq=1 ttl=125 time=57.9 ms
4. 64 bytes from 64:ff9b::c214:114: icmp_seq=3 ttl=125 time=33.5 ms
5. Frame 3: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
6. Ethernet II, Src: CadmusCo_94:c2:1e (08:00:27:94:c2:1e), Dst: c2:00:0d:d4:00:00 (c2:00:0d:d4:00:00)
7. Internet protocol version 6, Src: 2002:c010:101:64::20 (2002:c010:101:64::20), Dst: 64:ff9b::c214:114 (64:ff9b::c214:114)
8. Internet Control Message Protocol v6
9. Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
10. Ethernet II, Src: CadmusCo_14:67:f0 (08:00:27:14:67:f0), Dst: c2:01:0d:d4:00:00 (c2:01:0d:d4:00:00)
11. Internet protocol, Src: 192.16.4.64 (192.16.4.64), Dst: 194.20.1.20 (194.20.1.20)
12. Internet Control Message Protocol
```

Figura 8. *Estación IPv6 realizando un Ping a una estación Ipv4 (1 a 4). Captura sobre la interfaz de R. NAT64 conectada a la red IPv6 nativa (5 a 8) y a Internet IPv4 (9 a 12).*

3.4 Validación de una conexión cliente servidor

Para validar el funcionamiento correcto del mecanismo NAT64 se estableció una conexión entre una estación IPv6 nativa (ejecutando un programa cliente de navegación) y un servidor Web IPv4 (en nuestro caso la Registraduría Nacional del Estado Civil de Colombia). Se logró evidenciar que la estación IPv6 se pudo conectar al servidor de la Registradora Nacional de Colombia con dirección IPv4 (201.232.123.9), a través del NAT64, este último equipo es el encargado de traducir la dirección IPv6 (64:ff9b::C9E8:7B09) a su correspondiente dirección IPv4 (201.232.123.9) y, finalmente enviar la respectiva respuesta a la estación cliente. En la prueba realizada se pudo probar que la capa de aplicación no se afectó por la traducción NAT64.

4. Conclusiones

La transición hacia IPv6 es un paso que las entidades se ven obligadas a realizar en el corto plazo debido al rápido agotamiento de

las direcciones IPv4, esto se debe llevar a cabo de una manera planeada y sistemática, minimizando el impacto en la operación de la red.

Una aproximación que demanda menor administración de recursos de procesamiento, se basa en un modelo en el que se implementa una red IPv6 nativa en la oficina central, teniendo conectividad IPv6 con las oficinas remotas mediante 6PE, y acceso a la Internet IPv6 mediante 6to4. El uso de DNS64, combinado con el reciente mecanismo de traducción NAT64, hace posible implementar IPv6 de forma nativa sin perder el acceso a los servicios que se presten en la Internet IPv4.

Dos opciones que se pueden usar cuando el ISP no soporte 6to4, son el mecanismo Tunnel Broker o el mecanismo 6rd; estas realizan la misma función de 6to4 y facilitan la depuración de la conexión.

La integración de GNS3 con estaciones virtuales es una herramienta que les permite a las empresas crear laboratorios de pruebas completos dentro de una sola máquina y validar cada uno de los pasos en el proceso de migración hacia IPv6.

5. Referencias Bibliográficas

6NET (Large-Scale International IPv6 Pilot Network). (2005). *An IPv6 Deployment Guide*. The 6NET Consortium. http://www.6net.org/book/deployment-guide.pdf

Albitz, P., & Liu, C. (2006). *DNS and BIND*. Sebastopol, California: O'Reilly Media, Inc. 25-28

Bagnulo, M., Matthews, P., & van Beijnum, I. (2011a). *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*. In IETF (The Internet Engineering Task Force) Request for Comments 6146. http://tools.ietf.org/html/rfc6146

Bagnulo, M., Sullivan, A., Matthews, P., & van Beijnum, I. (2011b). *DNS64: DNS Extentions for Network Address Translation from IPv6 Clients to IPv4 Servers*. In IETF (The Internet Engineering Task Force) Request for Comments 6147. http://tools.ietf.org/html/rfc6147

Blanchet, M. (2006). *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*. Chichester, West Sussex: Jhon Wiley & Sons. 90-293

Bolívar, L. (2012). *Diseño e implementación de una red IPv6 con enfoque en la transición IPv4 a IPv6*. Trabajo de Grado, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Cali, Colombia.

Carpenter, B. & Moore, K. (2001). *Connection of IPv6 Domains via IPv4 Clouds*.In IETF (The Internet Engineering Task Force) Request for Comments 3056. http://www.ietf.org/rfc/rfc3056.txt

Cisco Systems Inc. (2002). *IPv6 over MPLS (Cisco 6PE)*. http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/iosip_an.pdf

Cisco Systems Inc. (2008).*Cisco IOS IPv6 Configuration Guide*. http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.pdf

Combs, G. (1998). *Wireshark*. http://www.wireshark.org

Deering, S., & Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification*.I In IETF (The Internet Engineering Task Force) Request for Comments 2460. http://www.ietf.org/rfc/rfc2460.txt

Dooley, K., & Brown, I. (2006). *Cisco IOS CookBook*. Sebastopol, California: O'Reilly Media, Inc.

Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). *Guidelines for the Secure Deployment of IPv6*. National Institute of Standards and Technology. http://www.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

Grossmann, J., Marsili, B., Goudjil, C., Thamini, X., & Eromenko, A. (2008). *GNS3: Graphical Network Simulator Software*. http//www.gns3.net.

Internet Systems Consortium [ISC] (2012). *BIND DNS Software*. http://www.isc.org/software/bind

Ministerio de Tecnologías de la Información y las Comunicaciones [MINTIC] (2010). *Circular 000002 del 6 de Julio de 2011 Promoción IPv6*. http://184.106.30.252/E-DocumentManager/gallery/Normatividad/Circular000002del6deJuliode2011Promoci%C3%B3nIPv6.TIF

Oracle (2009). *VirtualBox*. https//www.virtualbox.org

Templin, F., Gleeson, T., & Thaler, D. (2008). *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*. In IETF (The Internet Engineering Task Force) Request for Comments 5214.http://www.ietf.org/rfc/rfc5214.txt

Viagénie (2010). *Ecdysis: open-source implementation of a NAT64 gateway*. http://ecdysis.viagenie.ca