Modelo para la integración de redes IPv4 –IPv6 basado en túneles

Model for integration of IPv4-IPv6 network based in tunnels

Danilo López
Ingeniero Electrónico, Magíster en Teleinformática. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. dalopezs@udistrital.edu.co

Nancy Yaneth Gelvez García
Ingeniera de Sistemas, candidata a Magíster en Ciencias de la Información y las Comunicaciones. Docente de la Escuela Colombiana de Carreras Industriales (ECCI). Bogotá, Colombia. Nayag24@hotmail.com

Luis F. Pedraza
Ingeniero Electrónico, Magíster en Ciencias de la Información y las Comunicaciones. Docente de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. lfpedrazam@udistrital.edu.co

Clasificación del artículo: investigación (Conciencias)

Fecha de recepción: febrero 20 de 2010 Fecha de aceptación: agosto 3 de 2010

Palabras clave: Encapsulamiento Host, IPv4, IPv6, Nodos.

Key words: Tunneling Host, IPv4, IPv6, Node.

Resumen

El presente artículo tiene como finalidad plantear un modelo general para interconectar redes heterogéneas IPv4-IPv6 garantizando la integridad de los datos, haciendo uso de técnicas de transición.

Abstract

The intention of this paper is to set up a general model in order to interconnect heterogeneous nets IPv4-IPv6, guarantying the integrity of the data, making use of transition techniques.

* * *

1. Introducción

Desde hace más de una década el crecimiento de la red Internet ha venido generando un comportamiento creciente de tipo exponencial, causado por la oferta y demanda de nuevos y más sofisticados servicios que incluyen la posibilidad de conectarse

y ser controlados mediante este. Esto se traduce en la necesidad de disponer de un gran número de direcciones IP. Sin embargo, el protocolo IPv4 que contaba con 4.294.967.296 direcciones, hoy solamente dispone de menos del 5% de su totalidad según LACNIC [1]. Por otro lado, el tráfico circundante hoy en día exige garantías de autenticidad, seguridad, confiabilidad y movilidad, elementos que IPv4 no posee en el núcleo de su estructura sino que podría implementar mediante la inclusión de "parches". A nivel de aplicaciones en tiempo real multimediales es fundamental la garantía de calidad de servicio (QoS), aunque IPv4 cuenta con el campo "servicios diferenciados"; dentro de la estructura del protocolo este no garantiza dicha variable tan importante de las redes de siguiente generación. Todas estas falencias han conducido al desarrollo del protocolo IPv6, que es capaz de soportar un innumerable espacio de direcciones, además de mejorar las prestaciones para el transporte de aplicaciones multimediales en tiempo real, incluyendo elementos importantes de QoS y seguridad a los usuarios en Internet. Desde este punto de vista es claro que IPv6 será el protocolo que sustituya a IPv4. No obstante, este proceso será gradual ya que muchos ISP (proveedores de servicios de Internet) han invertido grandes cantidades de dinero en los *backbone* IPv4 y hasta que no se recupere la inversión no pensarán en la migración al IP de siguiente generación. Esto se traduce en la coexistencia de IPv4 e IPv6 durante los próximos años. No obstante, estas dos versiones del protocolo IP son heterogéneos entre sí, lo que conlleva a la aparición de una serie de problemas a solucionar debido a la incompatibilidad entre los protocolos. Existen mecanismos de transición de Ipv4 a Ipv6 como la traducción de direcciones, *tunneling* que permite su interacción en un mismo entorno y facilita la migración hacia un ambiente IPv6 nativo. El presente artículo pretende generar un modelo de red que permita la interacción entre estos dos protocolos a través de la utilización de túneles.

2. Características del protocolo IP de siguiente generación

Dentro de las características fundamentales de IPv6 está el rango de direcciones, el cual se eleva a 128 bits organizados en 16 octetos y es capaz de funcionar holgadamente por tiempo indefinido [2]. Este nuevo protocolo define tres tipos principales de direcciones: unicast, anycast y multicast [3] (ver Figura 1).

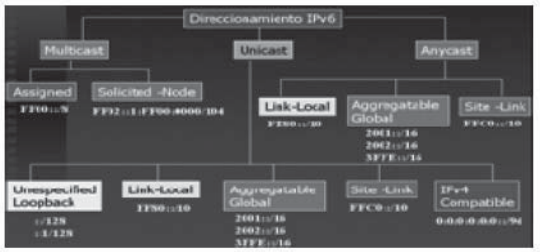

Figura 1. Tipos de direcciones en la arquitectura IPv6 [4].

Otro elemento sobresaliente es el formato del datagrama, el cual se diseñó enfocándose en la simplicidad y manteniendo un tamaño de cabecera fijo de 40 bytes. La razón principal de esta decisión fue maximizar el desempeño en el procesamiento, ya que una cabecera fija puede ser procesada más rápidamente, y a su vez proveer extensiones de la misma para poder ser flexible y extensible en futuras características de las redes [5].

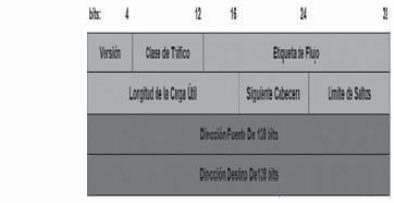

Figura 2. Encabezado del protocolo [6].

IPv6 mejora el descubrimiento de rutas y la detección de enrutadores defectuosos o inalcanzables y presenta un campo de flujo, el cual es usado para identificar el tipo de servicio y ofrecer un robusto sistema de QoS [4] entre muchas otras prestaciones.

3. Metodología

Se han planteado tres estrategias, con el fin de garantizar la existencia de ambas versiones del protocolo IP en la misma red de Internet:

3.1. Doble pila de protocolos (dual stack)

En esta configuración, la máquina fuente hace consultas al servidor DNS para obtener la dirección IP de destino; si dicha dirección de destino es IPv4, la máquina fuente envía datagramas IPv4. Si la dirección entregada por un servidor DNS corresponde a una dirección IPv6, entonces la máquina fuente enviará datagramas IPv6 [6]. Si la máquina de destino tiene una dirección IPv6 con una dirección IPv4 embebida, los paquetes IPv6 son encapsulados dentro de paquetes IPv4 (ver Figura 3).

Figura 3. Modelo doble pila de protocolos.

No obstante, decir que se implementará *dual stack* en una red completa es complicado, debido a la carencia de soporte a IPv6 por parte de los fabricantes de algunos equipos viejos que nunca fueron concebidos para trabajar con este nuevo protocolo, pero que hacen parte necesaria de la red; además, la operación de una red con doble pila significa dos redes independientes que deben ser administradas al mismo tiempo.

3.2. Traducción de direcciones

En este mecanismo de transición los datagramas IP de un tipo son transformados en datagramas IP del otro tipo y enviados sobre la red (ver Figura 4). Esto no es muy recomendado como mecanismo de transición, ya que tiene varias limitaciones, como que muchos de los protocolos de seguridad como IPsec no pueden ser usados a través de un dispositivo de translación [7].

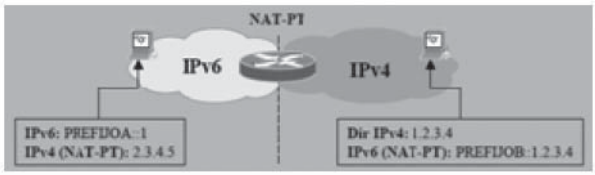

Figura 4. Modelo NAT-PT [7].

3.3. Túneles

Todo el tráfico IPv6 es transportado completamente por medio de encapsulamiento en IPv4 a través de un dispositivo con doble pila de protocolos. Estos datos viajan encapsulados y en el dispositivo de doble pila de destino son desencapsulados y entregados en forma de IPv6 nuevamente, como se muestra en la Figura 5 [8].

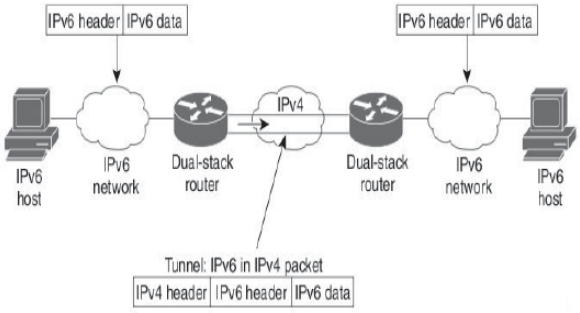

Figura 5. Modelo general del esquema túnel [8].

Existen tres tipos de túneles como mecanismos de transición en IPv6:

3.4. Túneles automáticos

Entre los que se encuentran 6to4, Isatap y toredo, la característica más importante es que proveen una

dirección IPv6 o prefijos basados en direcciones IPv4. La desventaja de este tipo de servicio es que las direcciones y prefijos no son fijos, por lo que se hace difícil enrutar redes [6], ya que una desconexión significa volver a solicitar direccionamiento.

3.5. Túneles manuales

Basado en dos pares de direcciones, un par de direcciones IPv4 y un par de direcciones IPv6 [7]. El par de direcciones IPv4 es comprendido entre la dirección de la maquina cliente o enrutador fuente y la dirección del servidor del túnel en el lado destino. El par de direcciones IPv6 son las direcciones que van dentro del túnel y se asignan a la fuente y al destino.

3.6. Túneles negociados

Los nodos clientes se conectan a servidores que proveen el servicio de túneles. Este mecanismo se basa en el protocolo TSP (*Tunnel Setup Protocol*) y es provisto por un software entregado por el servidor. El protocolo TSP es liviano y ha sido diseñado para que trabaje en cualquier tipo de maquina cliente, incluyendo pequeños equipos embebidos [7]. Estos protocolos adicionan capacidades de autenticación, haciendo las conexiones más seguras. Esto es posible ya que el cliente debe registrarse y obtener una cuenta, la cual tendrá la capacidad de ser monitoreada.

4. Resultados

Una de las formas más sencillas, prometedoras y menos traumáticas deobtener conectividad IPv6 en Internet es utilizando los mecanismos de túneles. Por tal motivo en este estudio en particular se hará uso de túneles automáticos y túneles automáticos negociados en la realización del diseño, con el fin de garantizar la interconexión en la *networking* y poder evaluar su rendimiento cuando coexiste IPv4 e IPv6 dentro del mismo *backbone*. Para el diseño de la red se utilizará un esquema basado en el RFC3056 (sección 5.5), en el cual hay múltiples sitios IPv6, conectados a un *backbone* IP de un proveedor cualquiera. En este diseño, particularmente se contemplan tres equipos de borde conectados al *backbone* IPv6 mediante la técnica de 6to4.

La *networking* está integrada por tres subredes. Puntualmente las subredes (sedes) 1 y 2 poseen características similares y están interconectadas a través de 6to4, usando un equipo de borde (ver Figura 6).

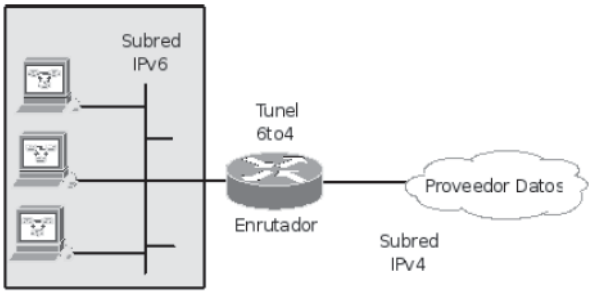

Figura 6. Esquema de interconexión de las subredes 1 y 2 al backbone de IPv6 mediante 6to4.

La sede 3 presenta un equipo de borde el cual se conecta al *backbone* de IPv6 mediante el mecanismo 6to4.Posee dos subredes, una para direccionar los *host* y otra para direccionar la DMZ, como se muestra en la Figura 7.

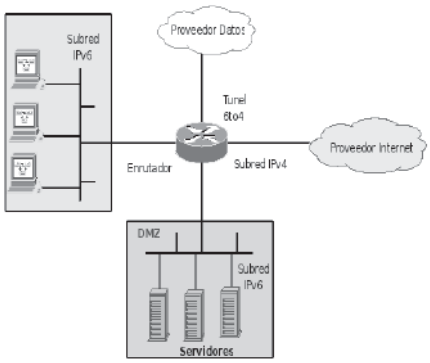

Figura 7. Interconexión de la sede 3 al backbone de IPv6 mediante el mecanismo 6to4.

La estructura de la *networking* integrada por las distintas subredes se muestra en la Figura 8.

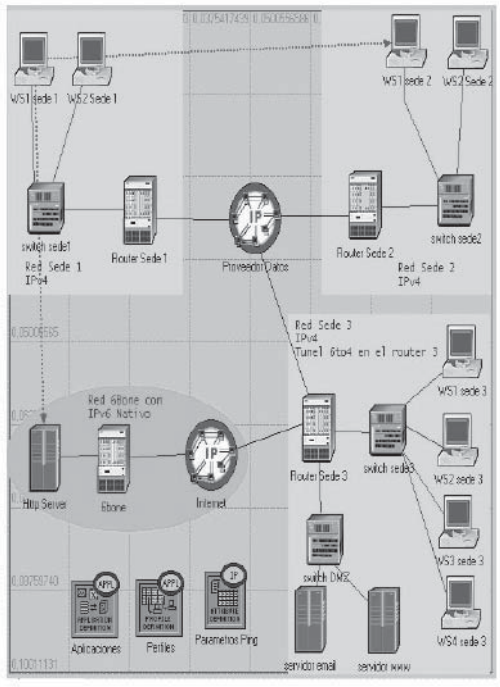

Figura 8. Integración del prototipo de red IPv6.

El prototipo diseñado en la Figura 8 fue creado con la herramienta de simulación OPNET (específicamente con la versión de prueba existente en la web del fabricante, la cual es bastante limitada [9]) y representa a un gran número de redes empresariales típicas, las cuales interconectan sus sedes a través de proveedores de datos. Lo anterior, mediante lo que se conoce como red WAN, donde dichos ISP les proveen comunicación desde o hacia sus servicios compartidos y les brinda conectividad a Internet. Como sucede en la gran mayoría de empresas, para toda la red solo se contrata un canal de Internet; en este caso el canal de Internet se ubica en la sede 3 y se comparte su servicio mediante NAT sobre el enrutador *Router* sede 3.

La idea principal del diseño es lograr la comunicación desde cualquier máquina de la red interna con un servidor ubicado en uno de los *backbones* de Internet, en este caso 6bone, ya que es el que se dispone en la versión de prueba del simulador OPNET. Como se estableció anteriormente, uno de los mecanismos para lograr una comunicación IPv6 es el de túneles; se escogió esta opción de implementación para establecer si mediante esta técnica es posible lograr menor traumatismo y bajas del servicio en la red diseñada. Como se observa en la Figura 8, existen cuatro subredes a nivel de *host*, las cuales poseen direccionamiento IPv6, interconectados a través de tres túneles desde los enrutadores de borde de cada una de las sedes.

4.1. Direccionamiento del modelo

Además de las cuatro subredes nombradas anteriormente (las cuales tienen el nombre sede1, sede2, sede3 y DMZ), también existen cuatro redes de conexión para cada una de las sedes con el proveedor, las cuales son sede1-proveedor, sede2-proveedor, sede3-proveedor, sede3-DMZ. El direccionamiento de las sedes se estableció de acuerdo a la Tabla 1.

Tabla 1. Asignación de prefijos IPv4/IPv6 para el modelo.

Nombre de la red	Direccionamiento IPv4	Direccionamiento IPv6
Sede 1	173.16.1.0/24	2002:be9f:ca26:1::/64
Sede 2	173.16.2.0/24	2002:be9f:ca26:2::/64
Sede 3	173.16.3.0/24	2002:be9f:ca26:3::/64
DMZ	173.16.4.0/24	2002:be9f:ca26:4::/64
Sede1-proveedor	173.16.13.0/30	2002:be9f:ca26:5::/64
Sede2 -proveedor	173.16.13.4/30	2002:be9f:ca26:6::/64
Sede3 -proveedor	173.16.13.8/30	2002:be9f:ca26:7::/64

4.2. Simulación del modelo

De forma general, el enrutamiento utilizado fue OSPFv3 asociado con *routing* estático; el direccionamiento fue incluido de forma estática debido a la falta de un mecanismo de autoconfiguración en el software. La evaluación del modelo incluyó los dos casos que se muestran a continuación:

4.3. Caso A. Solicitud de flujo http

Este primer escenario corresponde a la solicitud de tráfico http desde el *host* llamado WS1 sede 1, al servidor llamado http Server ubicado en la red de 6bone. Particularmente el gráfico 9 visualiza la solicitud del servicio web desde el *host*WS1 sede 1al servidor http ubicado en la red 6bone y la correspondiente respuesta generada. Allí se aprecia que el tráfico enviado y recibido es IPv6.

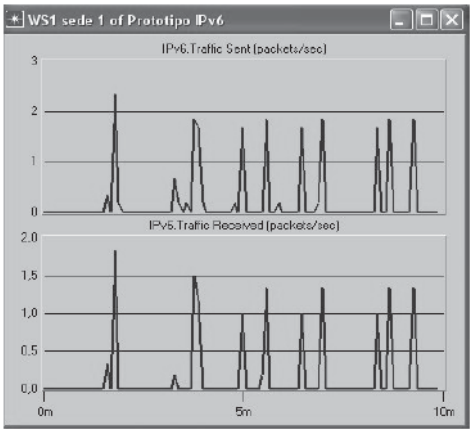

Figura 9. Tráfico IPv6 del la maquina WS1 sede1 ubicada en la red sede 1.

En la Figura 10 aparece el flujo de tráfico enviado y recibido por el servidor http Server. Particularmente se observa en la gráfica la interacción entre las solicitudes http de la máquina WS1 sede 1y el servidor http Server. De esta misma se concluye que el modelo planteado funciona perfectamente ya que el flujo mostrado es netamente IPv6, a pesar de que las redes a través de las cuales se conecta la máquina cliente son IPv4.Esto se traduce en que el túnel 6to4 ofrece todas las ventajas de transporte limpio del protocolo IPv6 sobre IPv4 hacia redes nativas IPv6.

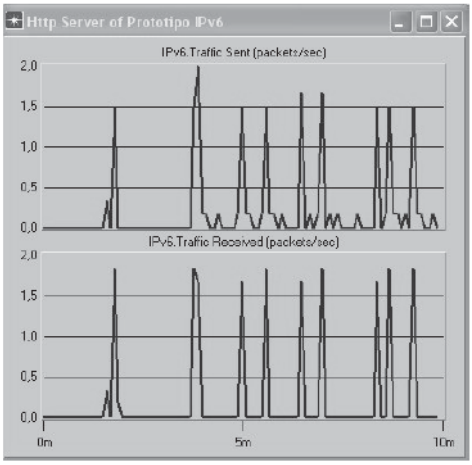

Figura 10. Tráfico IPv6 del servidor http.

Si se compara el tráfico enviado en la Figura 9 con el recibido en la Figura 10 y se hace lo mismo con el flujo enviado desde la Figura 10 y el recibido en la gráfica 9 se puede afirmar que estos son semejantes, dejando claro que el mecanismo de túneles automáticos no solo garantiza la interconexión de las redes sino que además garantiza el transporte y confiabilidad de la información.

4.4. Caso B. Solicitud de ping

Este escenario corresponde al resultado obtenido de solicitar respuesta a un ping6 generado desde WS1 sede 1hacia el http Server ubicado en 6bone y desde WS1 sede 1 al *host*WS1 sede 2. El resultado de esta solicitud aparece en la Tabla 2.

Tabla 2. Resultado del ping solicitado por el host WS1 sede 1.

	Traza completa de la solicitud y respuesta al Ping entre las maquinas WS1 Sede1 y http Server		
	IP Address	**Hop Delay**	**Node Name**
1	2002:be9f:ca26:1:0:0:0:2	0.000	WS1 sede 1
2	2002:be9f:ca26:5:0:0:0:2	0.000	Router Sede 1
3	2002:be9f:ca26:7:0:0:0:1	0.000	Router Sede 3
4	2003:2:1:0:0:0:0:2	0.000	Internet
5	2003:2:3:0:0:0:0:1	0.000	6bone
6	2003:2:3:0:0:0:0:2	0.000	Http Server
7	2003:2:3:0:0:0:0:2	0.000	Http Server
8	2003:2:1:0:0:0:0:1	0.000	6bone
9	2003:1:3:0:0:0:0:2	0.000	Internet
10	2002:be9f:ca26:7:0:0:0:2	0.000	Router Sede 3
11	2002:be9f:ca26:1:0:0:0:1	0.000	Router Sede 1
12	2002:be9f:ca26:1:0:0:0:2	0.000	WS1 sede 1
14	Total Response Time:	0.001 seconds	
	Traza completa de la solicitud y respuesta al Ping entre las maquinas WS1 Sede1 y WS1 Sede2		
	IP Address	**Hop Delay**	**Node Name**
1	2002:be9f:ca26:1:0:0:0:2	0.000	WS1 sede 1
2	2002:be9f:ca26:5:0:0:0:2	0.000	Router Sede 1
3	2002:be9f:ca26:2:0:0:0:1	0.000	Router Sede 2
4	2002:be9f:ca26:2:0:0:0:2	0.000	WS1 sede 2
5	2002:be9f:ca26:2:0:0:0:2	0.000	WS1 sede 2
6	2002:be9f:ca26:6:0:0:0:1	0.000	Router Sede 2
7	2002:be9f:ca26:1:0:0:0:1	0.000	Router Sede 1
8	2002:be9f:ca26:1:0:0:0:2	0.000	WS1 sede 1
10	Total Response Time:	0.002 seconds	

Se observan claramente los diferentes nodos por los que pasa la solicitud de ping hasta llegar al destino. Nótese particularmente que los saltos para ir de la sede 1 a la sede 2 no pasan por el *backbone* de IPv6, lo que indica que el tráfico IPv6 entre estas sedes es directo.

5. Conclusiones

La técnica de *tunelling* es una opción que debe ser tenida en cuenta por los ISP para brindar interconectividad en redes heterogéneas, ya que garantiza la integridad de la información. Sin embargo, es posible que se genere una sobrecarga introducida por el mismo túnel ya que, a pesar de que se tenga una comunicación extremo a extremo IPv6, este está formado entre direcciones IPv4. Lo anterior afectará el rendimiento del mismo, gracias a las limitaciones existentes entra las que se encuentran las innumerables tablas de enrutamiento o el número de campos obsoletos en la cabecera de IPv4 que impiden la agilización del servicio.

Finalmente se debe indicar que IPv6 no es del todo desconocido, ya que muchos fabricantes de equipos, teléfonos móviles, entre otros, se han preocupado por incluir IPv6 en sus artículos; otros fabricantes también proporcionan actualizaciones de *firmware* para lograr adicionar IPv6 a sus productos.

Referencias bibliográficas

[1] Informe LACNIC. (2010). "Distribuciones/ Asignaciones IPv4, espacio disponible y pronósticos". [En línea]. Disponible: http://www.lacnic.net/sp/registro/espacio-disponible-ipv4.html

[2] I. Beijnum, (2007). "Everything you need to know about IPv6". [En línea]. Disponible: http://arstechnica.com/articles/paedia/IPv6.ars

[3] RFC3513 Internet Protocol Version 6 (IPv6) Addressing Architecture. [En línea]. Disponible: http//www.ietf.org/rfc/rfc3513.txt

[4] H. Silvia, *Ipv6 Essentials*, ed. 2, United States of America: O`Reilly, 2006.

[5] J. Tatuya, S. Keiichi, *IPv6 Core Protocols Implementation*, San Francisco: MK, 2007.

[6] M. Blanchet, *Migrating to IPV6England:*, Wiley, 2010.

[7] P. Loshin, *IPV6: Theory, protocol and practice*, San Francisco: MK, 2004.

[8] S. McFarland, S. Muninder, S. Nikhil, *Ipv6 for Enterprise Network*, New York: Cisco System, 2007.

[9] Application and Network Performance. [En línea]. Disponible: www.opnet.com

[10] IPv6 Servicio de Información y Soporte. [En línea]. Disponible: http://www.6sos.org

[11] Fasg.org, "IPv6 RFC2373 Arquitectura de direccionamiento en Ipv6". [En línea]. Disponible: http://www.faqs.org/rfcs/rfc2373.html

[12] R. Coltun, D. Ferguson, J. Moy, "RFC2740 OSPF para Ipv6". [En línea]. Disponible: http://www.ietf.org/rfc/rfc2740.txt

[13] A. Conta, S. Deering, "RFC2473 Especificaciones genéricas de tunelización de paquetes en IPv6". [En línea]. Disponible: http://www.ietf.org/rfc/rfc2473.txt