

Comparación, ventajas, problemas y una metodología para la transición de IPv4 a Ipv6 en las redes de comunicaciones

Yezid Donoso Meisel*

Resumen

Las redes de computadores que hoy en día utilizan TCP/IP con IP versión 4 tendrán en pocos años el problema de ocupar en su totalidad el espacio de direcciones posibles. Este ha sido el motivo para que investigadores y empresas que tengan que ver con redes y comunicaciones estén analizando el diseño y desarrollo de una nueva versión de IP, la cual ha sido denominada IPv6, IPng o Fast IP. El IPv6, como lo denominaremos de ahora en adelante, nace como una posible solución a los problemas presentados y en la versión IPv4.

Palabras claves: Ipv6, Ipng, Fast IP.

Abstract

Within a few years, computer networks using TCP/IP, IP version 4, will have the problem of occupying completely the possible address space. For this reason, researchers and organisations dealing with networks and communications are analysing the design and development a new IP version named IPv6, IPng, or Fast IP. Thus, IPv6, as we call it henceforth, rises as a possible solution to the presented and yet not resolved problems in IPv4.

Key words: IPv6, IPng, Fast IP

Fecha de recepción: Septiembre 15 de 1998

1. Introducción

Debido a los problemas presentados por la versión 4 de IP, se ha realizado una investigación con el propósito de diseñar un nuevo modelo de IP, al cual se ha denominado Ipv6 o Ipng o Fast IP.

En la primera parte de este trabajo se establece una comparación entre IPv4 e

* MSc. Ingeniero de Sistemas de la Universidad del Norte. Minor en Gestión de Proyectos de Ingeniería de la misma universidad. Magister en Ingeniería de Sistemas de la Universidad de los Andes, con área de investigación en redes de comunicaciones. Profesor e investigador del Departamento de Ingeniería de Sistemas de la Universidad del Norte. (E-mail: ydonoso@guayacan.uninorte.edu.co)

IPv6, luego se mencionan las ventajas de este nuevo protocolo, se revisan algunas desventajas o complicaciones que puede presentar esta nueva versión, y finalmente se propone una metodología de transición de IPv4 a Ipv6.

2. Comparación entre IPv4 - IPv6

La versión actual de Ipv4 presenta, entre otros, los siguientes problemas:

- Cantidad de direcciones disponibles en IPv4.
- Debido a las diferentes clases de direccionamiento de redes (clase A, B, C, D y E) cuando la cantidad de *hosts* crece a un número mayor del soportado por el tipo de red, entonces se presenta el problema de pasar a otro tipo de red o segmentar la red.
- Requerimientos de transmisión de

las aplicaciones que viajan por la red.

A continuación se presentan unas comparaciones técnicas entre la versión actual de TCP/IP (IPv4) y la nueva versión (IPv6).

Los conceptos referentes a IPv4 se pueden encontrar en [COMER 96], y los relacionados con IPv6, en [COMER 96], [TANENBAUM96], [DEERING95].

• Encabezados del IP

La versión IPv4, que es la utilizada actualmente en las redes a nivel mundial, presenta el formato que se muestra en la figura 1.

El encabezado consta de 20 bytes de

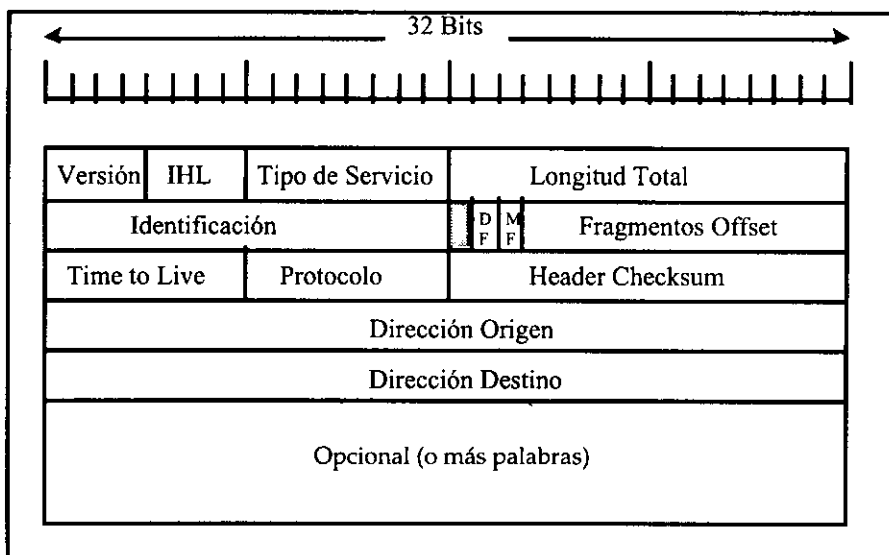


Figura 1. Encabezado del Ipv4

parte fija y una longitud variable en la parte opcional.

En la versión IPv6, el encabezado fijo se reemplaza por un encabezado base y por unas extensiones de encabezados, de ser necesario, en el enrutamiento del paquete. El formato del encabezado base del IPv6 se presenta en la figura 2, y en la figura 3, el formato de un encabezado base con extensiones del IPv6.

Este nuevo formato trae como consecuencia una mejora en lo referente a que se envía por la red sólo los encabezados que sean necesarios para una comunicación en particular. Es decir

que cuando se organiza un paquete en IPv6, éste es más flexible que en IPv4, donde el encabezado es fijo, ya sea que se necesite o no toda la información de control.

Claro está de que no todo es ventaja, ya que por el hecho de ser flexible, cuando un *router* va a revisar el paquete, éste tiene que revisar todos los encabezados y sus extensiones.

• **Fragmentación en IPv4 y en IPv6**

El funcionamiento de la versión IPv4 es diferente al de la IPv6, debido a que la importancia del MTU se fundamenta en

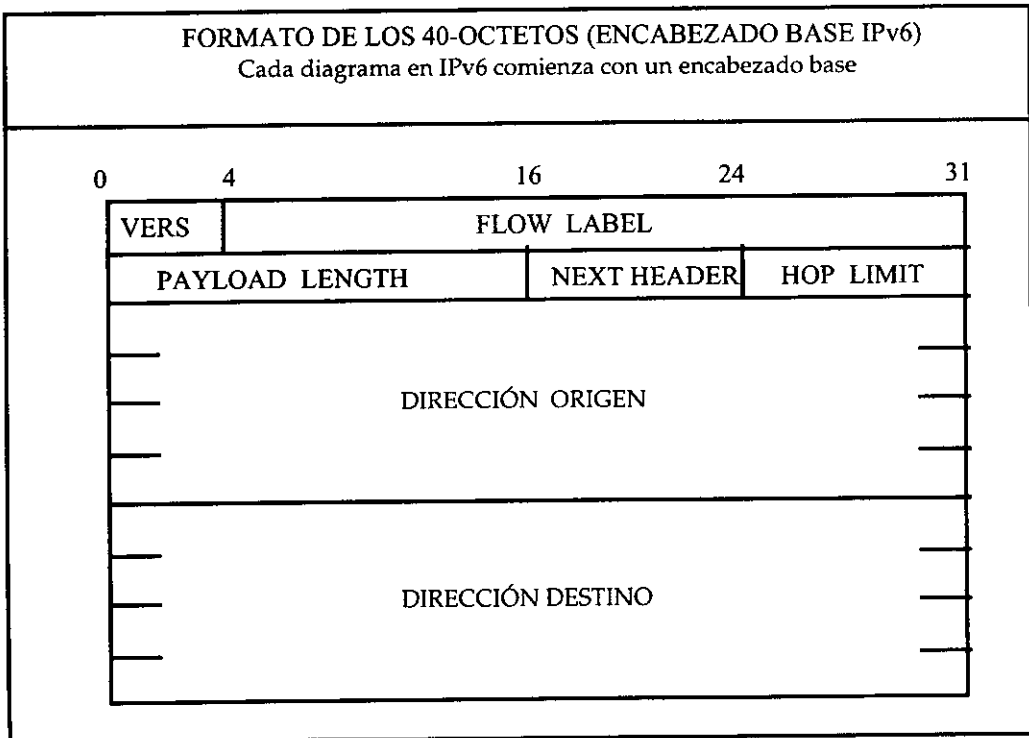


Figura 2. Encabezado base del IPv6

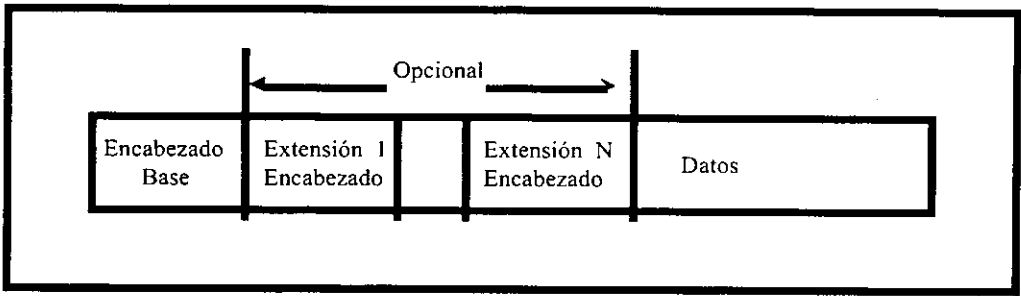


Figura 3. Encabezado base con extensiones en IPv6

dos enrutadores adyacentes, ya que los enrutadores están en capacidad de fragmentar los paquetes de acuerdo con el MTU encontrado.

En cambio, en la versión IPv6 se le quita ese recargo de trabajo a los enrutadores y se establece lo que se conoce como **fragmentación end-to-end**, la cual consiste en que sólo el origen es el que fragmenta los paquetes de acuerdo al mínimo MTU encontrado en todo el trayecto desde el nodo de origen hasta el nodo de destino. En efecto, este enfoque genera una serie de inconvenientes en caso de que se pierda la comunicación entre un par de enrutadores. Para esto hay pocas soluciones, pero desde mi perspectiva de investigador planteo la siguiente:

Si en un punto del trayecto se pierde la comunicación, el enrutador debería estar en capacidad—obviamente se estaría sobrecargando la funcionalidad de éste— de encontrar otro camino con un MTU mayor o igual al tamaño de los fragmentos. Si este camino es encontrado, deben enviarse los paquetes por la nueva ruta. Pero aquí se origina otro

problema, y consiste en que si este camino con ese requerimiento de MTU no se encuentra, deberá comunicársele al nodo de origen que la comunicación se perdió y que resulta imposible reestablecerla, para que el nodo de origen tome las medidas necesarias, tales como volver a encontrar otra ruta hasta el nodo de destino y retransmitir la información.

Bajo este esquema, y como se observa en la figura 4, si el protocolo es la versión IPv4, cada enrutador (A,B,C,D,E,F,G) irá fragmentando cada paquete de acuerdo al MTU (x,y,z,w,r,s,t) entre cada par de enrutadores.

En cambio, si la versión es el IPv6, primero se establecerá la ruta que deberá seguir cada paquete entre el *host* de origen y el *host* de destino, luego se determina el mínimo MTU en toda la ruta escogida, a continuación el *host* origen y sólo éste fragmentará los paquetes de acuerdo al mínimo MTU hallado, para finalmente ser enviados y que viajen por la red hasta el nodo de destino.

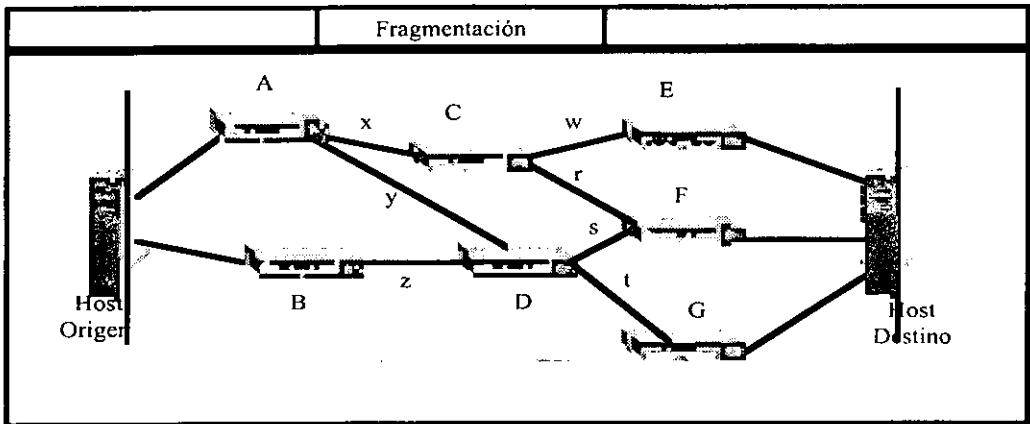


Figura 1.4. Fragmentación de paquetes

- *Seguridad en el ancho de banda y en el retardo*

Este es otro aspecto que marca diferencia entre el IPv4 y el IPv6, puesto que a la hora de escoger el camino que debe seguirse entre un nodo de origen y uno de destino, no sólo se hallará el mínimo MTU, sino que se buscará el camino que proporcione un ancho de banda requerido y con un retardo razonable para la aplicación que vaya a viajar por la red. Con esto se podría asegurar la transferencia de video en tiempo real; pero aquí se presentaría el mismo problema que en el de la fragmentación: Si se cae un enlace entre un par de enrutadores, ¿qué pasaría?, porque tocaría volver a buscar otro camino con las mismas especificaciones de ancho de banda y de retardo.

- *Se cambia el tiempo de vida por el número de saltos*

En la versión IPv6 se ha cambiado el

campo *Time to Live* de IPv4 por el campo *Hop Limit*. Entonces ya no se tiene en cuenta el tiempo que el paquete esté viajando por la red, sino por el número de nodos o enrutadores por los que esté pasando hasta su llegada al destino final.

- *El formato de las direcciones*

En IPv4 las direcciones constan de 32 bits de longitud, los cuales son expresados por 4 números decimales separados por un punto entre ellos. Una dirección típica en IPv4 es la siguiente:

128.10.2.1

En la versión IPv6, las direcciones consisten de 128 bits de longitud, los cuales son expresados por números hexadecimales, y cada grupo de 16 bits es representado por su correspondiente en base 16. Además, los números son separados con dos puntos. Una dirección típica en IPv6 es la siguiente:

FF05:0:0:0:0:0:0:B3

Ahora, la notación en IPv4 se puede representar en IPv6 de la siguiente manera:

0:0:0:0:0:0:128.10.2.1

Pero en IPv6 los ceros se pueden abreviar por dos puntos consecutivos, y entonces quedaría de la siguiente forma:

::128.10.2.1

3. Ventajas del IPv6 sobre el IPv4

En cuanto a las ventajas que presenta la versión IPv6 con respecto a la IPv4, podemos mencionar las siguientes:

- **Direcciones más largas.** El nuevo tamaño de la dirección es el cambio más notable. IPv6 cuadruplica el tamaño de la dirección del IPv4 de 32 a 128 bits. El espacio disponible para una dirección IPv6 es tan grande que no puede llegar a agotarse en un futuro previsible.
- **Formatos de cabecera flexible.** IPv6 utiliza un nuevo formato de datagrama. A diferencia del IPv4, que utiliza una cabecera de datagrama de formato fijo, donde todos los campos, excepto la parte opcional (ver figura 1), ocupan un número fijo de octetos, el IPv6 utiliza un conjunto opcional de cabeceras.
- **Fragmentación end-to-end.** Esta ventaja radica en el hecho de que a los enrutadores se les elimina la función de fragmentar los paquetes que les lleguen debido al MTU. En cambio, esta función queda determinada para el nodo de origen que quiere enviar la información por medio de la red.
- **Soporte para reserva de recursos.** IPv6 reemplaza la especificación del tipo de recursos del IPv4 con un mecanismo que permite la reserva con anterioridad de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones como video en tiempo real, el cual requiere que se garantice el ancho de banda y el retardo.
- **Provisión de extensiones al protocolo.** Quizás el cambio más significativo en el IPv6 es el desplazamiento de un protocolo en el que estaban especificados totalmente todos los recursos a otro que permite características adicionales. La capacidad de extensión tiene el potencial para permitir que el protocolo se adapte a cambios en el hardware de la red o a nuevas aplicaciones.
- **Número de saltos.** Al cambiarse el tiempo de vida en un paquete IPv4 por el número de saltos en IPv6 se está mejorando el hecho de que si existe congestión en la red, este paquete no sea eliminado sin que tenga la opción de llegar hasta el nodo de destino. Como es bien sabido, en TCP el camino es establecido desde un principio, y por lo tanto se sabe de antemano cuáles es el número de nodos

por los que debe pasar.

4. Desventajas o complicaciones en IPv6

A pesar de que este nuevo protocolo de IP ha sido pensado para solucionar los problemas presentados por la versión anterior—IPv4—, no deja de tener complicaciones, como las que se mencionan a continuación:

- **Asegurar especificaciones de recursos.** Como es bien sabido, este nuevo protocolo asegura un ancho de banda y un retardo específico de acuerdo con la calidad necesitada en la transmisión. Pero, ¿qué pasaría si uno de los enlaces entre un par de enrutadores se cae y no se puede reestablecer la comunicación? Aquí es cuando se presentan los problemas, los cuales afectan los siguientes factores:
 - Tamaño de los fragmentos de acuerdo al mínimo MTU.
 - Ancho de banda específico para esa comunicación.
 - Retardo aceptable en la transmisión.

Este caso fue analizado en el ítem de comparaciones, y la posible solución sería sobrecargar a los enrutadores en la tarea de tratar de encontrar otro camino hasta el nodo de destino con las mismas especificaciones requeridas para la transmisión o, de lo contrario, volver a generar la comunicación desde el nodo de origen.

- **Transición de IPv4 a IPv6.** Este as-

pecto no es considerado como un problema, pero sí hay que tomarlo con mucha seriedad y con mucho profesionalismo, debido a la tecnología disponible y a la gran cantidad de nodos (*hosts* y *routers*) con soporte de IPv4 que hay en el mundo.

5. Esquema de una metodología de transición de IPv4 a IPv6

Después de revisar las ventajas y complicaciones del nuevo protocolo IPv6 y de establecer las comparaciones entre ambas versiones, surge el problema de cómo se podría llegar a implementar en su totalidad esta nueva versión, o más bien, cuáles serían las etapas para poder llegar hasta ese punto.

La situación actual, en cuanto a la tecnología de enrutamientos, exige que se utilicen buenas estrategias, puesto que no se podría desechar de la noche a la mañana tanta cantidad de enrutadores que funcionan única y exclusivamente en IPv4.

Los conceptos referentes a la transición de IPv4 a IPv6 se encuentran referenciados en [LEHTPVIRTA96], [GILLIGAN96].

Para este problema se plantea una metodología de transición de IPv4 a IPv6, la cual consiste en lo siguiente:

Como en la actualidad sólo existen nodos IPv4, entonces se deben crear nodos que soporten tanto el IPv4 como el IPv6 hasta cuando todos los nodos

puedan llegar a hablar la misma versión de IP, es decir, el IPv6. Esta solución se podría llevar a cabo por medio de dos formas:

- **Con nodos IPv4/IPv6.** Los enrutadores y máquinas de esta categoría tienen tanto IPv4 como la pila de protocolos IPv6. Además, tienen mecanismos como tunelado IPv6 sobre IPv4. Estos nodos pueden interoperar directamente tanto con nodos IPv4 como con nodos IPv6, pero para una comunicación con nodos solamente IPv4 tienen que ser configurados con unas direcciones IPv6 compatibles con IPv4.
- **Con enrutadores traductores de cabeceras IPv6/IPv4.** Estos son enrutadores que traducen paquetes de IPv6 a paquetes de IPv4 y viceversa. Al respecto, el enrutador podría saber cuál es la versión por medio del campo *versión* del encabezado del paquete.

Ahora, este tunelado se puede rea-

lizar por medio de un encapsulamiento, es decir que el paquete en el cual vienen encabezados y datos en Ipv6 se convierte sólo en datos para Ipv4 y luego se le adiciona el encabezado de Ipv4. Pero si el nodo es únicamente Ipv4, entonces la dirección Ipv6 se tendrá que mandar en formato de Ipv4 de la siguiente forma:

0:0:0:0:0:128.10.2.1
o en su defecto ::128.10.2.1

Aquí surge un gran interrogante con respecto a si el tamaño del paquete que se arma en Ipv4 es mayor al MTU en todo el trayecto. ¿Qué pasaría si el nodo origen es Ipv4 y él no sabe ni está diseñado para buscar el mínimo MTU entre el nodo de origen y el nodo de destino?

La solución propuesta a este caso es que los nodos (*Host* y *Routers*) que sean Ipv4 fragmentarán de acuerdo al MTU que conocen; y lo seguirán realizando mientras que los nodos por donde transite el paquete sean Ipv4. Cuando lleguen a un nodo IPv4/IPv6 que sepa que tiene que buscar el mínimo MTU en la

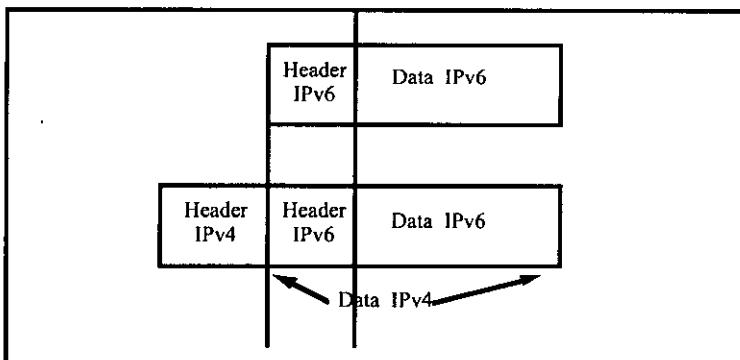


Figura 5. Encapsulamiento de Ipv6 dentro de Ipv4

ruta escogida, éste procederá a encontrarlo, y una vez hallado tomará la decisión de fragmentar o no y a qué tamaño, en caso de requerir de la fragmentación. Estos nodos sí están en capacidad de fragmentar, puesto que tienen en su pila de protocolos tanto Ipv4 como Ipv6, es decir que pueden fragmentar y reensamblar, y además pueden encontrar el mínimo Mru en la ruta escogida.

Ahora, ¿de qué forma se enviarían los paquetes por medio de la red ? Al respecto se pueden plantear varias soluciones:

- **Mapeo de direcciones.** Esta técnica consiste en enviar la dirección IPv4 de 32 bits en el extremo derecho del formato de IPv6, es decir, ocupando 4 bytes de los 16 que lo componen. Los 12 bytes ubicados a la izquierda son rellenados con ceros (0).

96 bits (12 bytes)	32 bits (4 bytes)
0:0:0:0:0:0:0:0:0	Dirección IPv4

- **Capa IP dual.** Esta técnica consiste en incluir completamente el IPv4 en un sistema nuevo con IPv6. Estos son los llamados nodos IPv6/IPv4. Estos nodos están en capacidad de transmitir información tanto en formato IPv4 como en IPv6.
- **Por medio de un protocolo de encapsulación.** Esta técnica también es llamada IPv6 en IPv4 o tunelado de IPv6 sobre IPv4. El tunelado se utiliza para llevar paquetes de IPv6 a través de áreas de red de envío tipo IPv4.

Uno de los requisitos para el tunelado es que el comienzo y los extremos (*endpoints*) del túnel sean nodos IPv6/IPv4 con direcciones IPv6 compatibles con IPv4. Tunelado significa que todos los paquetes IPv6 son mapeados en el cuerpo de un paquete IPv4 y enviados a través de áreas de red de IPv4. La forma más sencilla de realizar el tunelado consiste en adicionar al paquete IPv6 los encabezados de IPv4 y transmitirlo; cuando se necesite recibir, se le remueve el encabezado IPv4 y se procesa el resto del paquete como IPv6.

De esta forma se podría ir pasando de la versión IPv4 a la IPv6, tanto en los nodos de procesamiento de información como en los nodos de enrutamiento de paquetes.

6. Conclusiones

Después de haber analizado la nueva configuración de este protocolo de enrutamiento de paquetes, hemos llegado a las siguientes conclusiones:

- Ipv6 presenta ventaja en cuanto al tamaño de bytes que ocupan los encabezados, los cuales son variables; en cambio, en Ipv4 se tiene que incluir un tamaño fijo, sea que se utilice o no en su totalidad.
- En este modelo, debido al nuevo tamaño de 128 bits de direcciones, se supera el problema de la cantidad de direcciones disponibles que presenta el modelo en Ipv4.

- La ventaja que representa el quitarles a los enrutadores el trabajo de la fragmentación, lo cual permite agilizar las transmisiones de paquetes y descongestiona el tráfico en la red, debido a que a los enrutadores se les deja nada más la función de direccionar paquetes y no la de fragmentación de paquetes de acuerdo al MTU.
- La ventaja que significa el cambio del campo *Time-to-Live* de Ipv4 por el campo *Hop Limit* de Ipv6. Esto se puede observar cuando la red se encuentra congestionada, entonces muchos paquetes pueden llegar a ser eliminados por el tiempo sin que realmente debieran serlo.

Referencias

[COMER96] COMER Douglas, STEVENS David. *Internetworking with TCP/IP*. Vol. Y. 3ª ed. Prentice Hall, 1996.

[TANENBAUM96] TANENBAUM, Andrew. *Computer Networks*. 3ª ed. Prentice-Hall, 1996.

[LEHTOVIRTA96] LEHTOVIRTA, Juha. Transition from IPv4 to Ipv6, 1996, <http://www.tascomm.fi/~jlv/ngtrans/>

[GILLIGAN96] GILLIGAN, R., NORDMARK, E. Transition Mechanisms for IPv6. Host and Routers, 1996, http://206.21.31.20/notes/rfcs1/3472_le2.html

[DEERING95] DEERING, S., HINDEN, R. Internet Protocol Version 6 (IPv6) Specification, 1995, <http://seusa.sumitomo.com/docs/rfc/rfc1883.txt>

Terminología

- **Nodo:** Un dispositivo o equipo que pertenece a una red de comunicaciones, ya sea para

procesar información y transmitirla o bien para enrutar esta información.

- **Paquete:** Cantidad de información que viaja por la red como una unidad en particular y entendible por la capa de red del modelo OSI o el modelo TCP/IP. La forma de entender este flujo de información es por medio de campos de encabezados constantes y bien definidos por los equipos que intervienen en el proceso de transmisión.

- **Enrutador (Router):** Es un nodo que redirige un paquete de información ya sea a otro enrutador o al equipo que le debe llegar la información en caso de que este equipo pertenezca a dicho enrutador. Los métodos de enrutar estos paquetes de información son por unos algoritmos establecidos, como por ejemplo: El camino más corto entre dos nodos; enrutamiento por el Vector de Distancias, etc.

- **Host:** Es cualquier nodo que primeramente no es un enrutador, sino que transmite información producida localmente a otro equipo de red o estación de trabajo, o que, a su vez, puede recibir información de otro equipo de la red para procesarla. Para que esta información llegue de un *host* a otro se necesita de los enrutadores, los cuales van encaminando esta información para que llegue a su lugar de destino.

- **Puentes (Bridges):** Son dispositivos que pueden interconectar redes de diferentes protocolos a nivel de la capa de *mac*. Por ejemplo, pueden conectar redes que trabajen con los protocolos 802.3 (*Ethernet*), 802.4 (*Token Bus*), 802.5 (*Token Ring*) entre sí.

- **MTU (Unidad de Transferencia Máxima):** La MTU es el tamaño máximo de un paquete o datagrama soportado por la red en la cual es transportado.

- **Tunneling:** El tunelado o *Tunneling* se utiliza para llevar paquetes de IPv6 a través de áreas de red de envío tipo IPv4. Tunelado significa que todos los paquetes IPv6 son mapeados o convertidos en el cuerpo de un paquete IPv4 y enviados a través de áreas de red de Ipv4.

- **MAC:** Subcapa de acceso medio.