Visión General del Protocolo IPv6*

Albert Cabellos-Aparicio, Jordi Domingo-Pascual

Departament d'Arquitectura de Computadors,

Universitat Politècnica de Catalunya, Spain

{acabello,jordid}@ac.upc.edu

Resumen: IP significa "Internet Protocol" y fue diseñado en los setenta con el propósito de interconectar redes con tecnologías heterogéneas. IP fue un gran éxito e hizo posible la Internet actual. Hoy en día, Internet funciona básicamente con la versión 4 del protocolo IP (IPv4); sin embargo, el propio éxito de Internet esta llevando IPv4 a sus límites. La IETF diseñó IPv6 como substituto a IPv4. Este nuevo protocolo, al margen de tener nuevas funcionalidades, soluciona la mayoría de problemas de IPv4. Este artículo presenta una visión general del protocolo IPv6, el formato de su cabecera, el protocolo "Neighbour Discovery" y uno de los aspectos más críticos de IPv6: su transición. Se presentan una serie de mecanismos de transición que proporcionan comunicación entre IPv4 e IPv6.

Palabras Clave: IPv6, Formato cabecera IPv6, Cabeceras de Extensión, Nieghbour Discovery, Direccionamiento IPv6, Mecanismos de Transición

1.- Introducción

IP significa "Internet Protocol" y fue desarrollado en la década de los 70 con el propósito de interconectar tecnologías de red heterogéneas. IP fue un gran éxito, e hizo posible la Internet de hoy en día. Actualmente Internet funciona con la versión 4 (IPv4) [1] del protocolo IP, sin embargo el gran crecimiento experimentado por Internet lo esta llevando a sus límites.

Durante la década de los 90, en la Internet Engineering Task Force (IETF) [2] se empezaron a identificar varios problemas relacionados con el protocolo IPv4. Éste utiliza 32 bits para identificar interfaces de red (comúnmente conocidos como Dirección de Internet). 32 bits eran suficientes en la época en que IPv4 fue diseñado, y, de hecho, jamás se pensó en soportar una red tan grande como Internet. Sin embargo, para la

* Este trabajo ha sido parcialmente financiado por el MCyT (Ministerio Español de Ciencia y Tecnología) bajo el contrato FEDER-TIC2002-04531-C04-02 y el CIRIT (Consell Interdepartamental de Recerca i Innovació Tecnològica) bajo el contrato 2001-SGR00226.

Internet de hoy en día, la capacidad de direccionamiento de 32 bits resulta escasa y esto ha conllevado la aparición del Network Address Translation (NAT) y otros mecanismos que, a pesar de permitir conectarse a Internet usando una sola dirección IPv4 rompen con los principios de Internet. La arquitectura de Internet se basa en el principio extremo a extremo [3] que dice que dos nodos cualesquiera de Internet deben poder comunicarse sin impedimento alguno. Esta restricción frena el crecimiento de Internet así como la creación de nuevos servicios y aplicaciones. Por estos y otros motivos, a IETF diseñó un substituto para IPv4: IPv6.

IPv6 [4] es la nueva versión del "Internet Protocol" y tiene substanciales mejoras. Tiene un espacio de direccionamiento mucho más amplio que el de IPv4, concretamente 128 bits. Con IPv6 tenemos muchísimas direcciones (3.4×10^{28}), podemos conectar innumerables dispositivos a Internet sin romper el principio de comunicación extremo a extremo, podemos crear una compleja jerarquía de direcciones y conseguir una auto configuración mucho más simple. IPv6 también proporciona un formato de cabecera más eficiente y los enrutadores son capaces de procesarla más rápidamente. Las opciones en IPv4 son simplemente parches (como la movilidad y la seguridad) pero en IPv6, las opciones se integran más eficientemente (utilizando las nuevas cabeceras de extensión). En resumen, Internet será aún más escalable con IPv6 de lo que ya lo es con IPv4.

Internet aún esta usando IPv4, sin embargo IPv6 se esta empezando a desplegar en redes experimentales. En el futuro, es previsible que Internet sea sólo IPv6, pero hasta ese momento, IPv4 e IPv6 deben coexistir. El despliegue de IPv6 no puede interrumpir la actual Internet, ya que muchos servicios y aplicaciones dependen hoy en día de ella. Esto se consigue usando mecanismos de transición, que permiten la comunicación entre el mundo IPv4 y el IPv6. Se han especificado diseñado e implementado multitud de mecanismos de transición pero o bien proporcionan un enrutamiento menos eficiente que la comunicación nativa (IPv4 con IPv4 o IPv4 con IPv6) y en general son difíciles de desplegar.

2.- El protocolo IPv6

2.1.- El formato de la cabecera de IPv6

El nuevo formato de cabecera de IPv6 tiene una longitud fija de 40 octetos, mientras que en IPv4 el tamaño de cabecera era de 20 octetos más opciones (si es que son necesarias). La figura 1 muestra el formato de la cabecera IPv6.

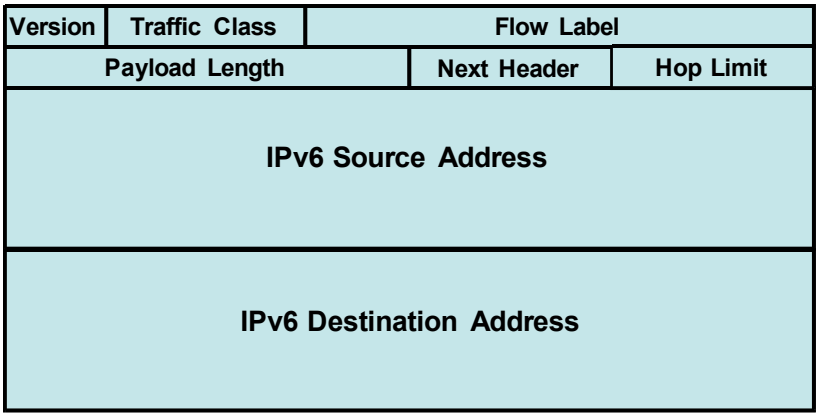

Figura 1 –*Formato de cabecera de IPv6*

Version (4 bits) → La versión del protocolo, un "6" para IPv6 y un "4" para IPv4. Este campo es idéntico en IPv4.

Traffic Class (8 bits) → Una etiqueta usada para Calidad de Servicio, similar al campo "Type of Service" de IPv4.

Flow Label (20 bits) → Este campo es nuevo, y se usa para etiquetar flujos que los enrutadores podrán tratar de forma homogénea..

Payload Length (16 bits) → La longitud del campo de datos (los bits siguientes a la cabecera IPv6) en octetos. Un paquete IPv6 puede transportar hasta 65536 octetos.

Next Header (8 bits) → El tipo de cabecera siguiente a la de IPv6. Este campo es similar al campo "Protocol" de IPv4, aunque incorpora la identificación de las cabeceras de extensión.

Hop Limit (8 bits) → El valor de este campo se decrementa al pasar por cada enrutador, y cuando llega a cero el paquete se descarta. Este campo es similar al campo "Time to Live" del protocolo IPv4.

Source Address (128 bits) → La dirección del nodo originador del paquete.

Destination Address (128 bits) → La dirección destino del paquete.

La cabecera IPv6 tiene menos campos que la cabecera IPv4. El "checksum" se considera que no es relevante ya que la probabilidad de que un fallo en la transmisión provoque el descarte del paquete es muy baja. La campos usados para la fragmentación en IPv4 ("Identification" y "Fragment Offset") también han sido eliminados, ya se decidió que para conseguir mayor eficiencia en IPv6 un paquete no puede ser fragmentado en ruta, y por tanto sólo el nodo originador del paquete puede implementar la fragmentación usando una cabecera especial. Esto obliga a que cuando un nodo decide comunicarse con otro debe conocer cuál es la MTU (Maximum Transfer Unit) del camino [5] y enviar los paquetes con el tamaño correcto, o utilizar la MTU mínima garantizada de 1280 bytes.

Tal y cómo se ha comentado, la cabecera IPv6 tiene una longitud fija y los octetos van alineados a 64 bits para conseguir una mayor eficiencia en los nuevos procesadores de red de 64 bits

2.2.- Cabeceras de Extensión de IPv6

En IPv6, la información opcional de la capa de red se codifica en unas cabeceras al margen de la propia de IPv6. Estas cabeceras se colocan entre la de IPv6 y la del protocolo de transporte.

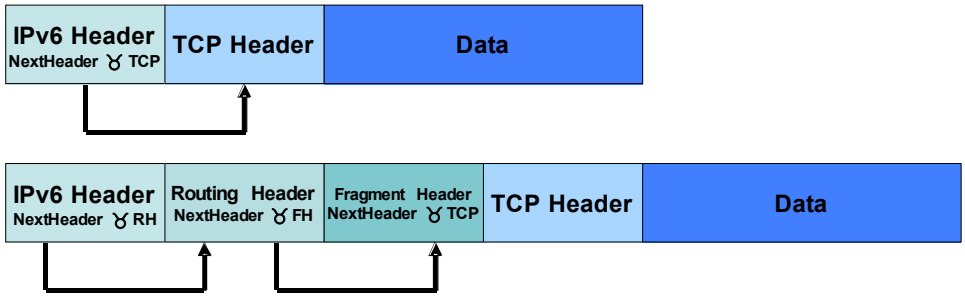

Figura 2 – *Cabeceras de Extensión de IPv6.*

La figura 2 muestra cómo se codifican estas cabeceras de extensión dentro del paquete IPv6. Estas cabeceras proporcionan una gran flexibilidad en el protocolo. Usándolas, el protocolo puede extender sus funcionalidades de una manera sencilla y eficiente. La cabecera IPv6 mide 40 octetos, y en el campo "Next Header" apunta a la siguiente cabecera, que puede ser la del protocolo de transporte (TCP, UDP…) o bien una cabecera de extensión.

El estándar de IPv6 define seis tipos de cabeceras de extensión que salvo una excepción (Hop-by-Hop) no son examinadas ni procesadas por ningún enrutador en el camino hasta el destino. En IPv4 las opciones vienen limitadas por el tamaño de la cabecera IPv4, mientras que en IPv6 no existe una limitación virtual. En general, en IPv6 se ha tratado de optimizar el rendimiento de forma que no se procesan salvo que sea el momento de ser usadas. Las opciones del protocolo IPv4 se usan escasamente, y muchas de las nuevas funcionalidades (como movilidad o seguridad) de IPv6 basan su funcionamiento en las cabeceras de extensión.

3.- Funcionamiento del protocolo IPv6

3.1.- Direccionamiento IPv6

Las direcciones IPv6 son campos de 128 bits de extensión que identifican únicamente una o más interfaces de red. Es más, podemos asignar una o más direcciones IPv6 a una interfaz de red. IPv6 tiene tres tipos de direcciones:

- Unicast → Este tipo de direcciones identifican únicamente una sola interfaz de red, son el tipo de direcciones más comunes.
- Multicast → Identifican un conjunto de interfaces de red, usualmente pertenecientes a diferentes nodos. Si un paquete se envía a una dirección multicast, éste se entregará a todas las interfaces de red identificadas por esa dirección en concreto.
- Anycast → Este tipo de direcciones se asigna a más de una interfaz de red y, si un paquete se envía a una dirección "Anycast" el paquete se enrutará a la interfaz más "cercana" (en términos de distancia de enrutado).

Las direcciones IPv6 se representan como una cadena de caracteres en el formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx donde 'xxxx' es un número de 16 bits en hexadecimal. La figura 3 muestra algunos ejemplos:

Dirección IPv6 Multicast:

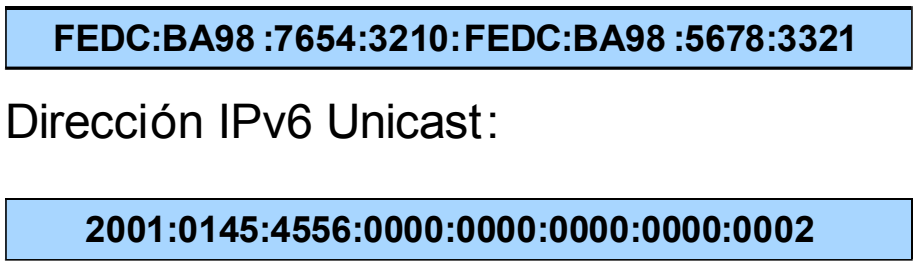

Figura 3 – *Representación en formato texto de las direcciones IPv6.*

Algunas direcciones IPv6 pueden contener largas cadenas de ceros, en este caso se puede usar "::" que indica uno o más grupos de 16 bits de ceros. Por ejemplo, la dirección "2001:0145:4556:0000:0000:0000:0000:0002" se puede representar como "2001:145:4556::2" (también se eliminan los ceros que están antes de los dígitos hexadecimales significativos) de una manera más simple.

La figura 4 muestra la estructura básica de las direcciones unicast actualmente utilizadas en IPv6:

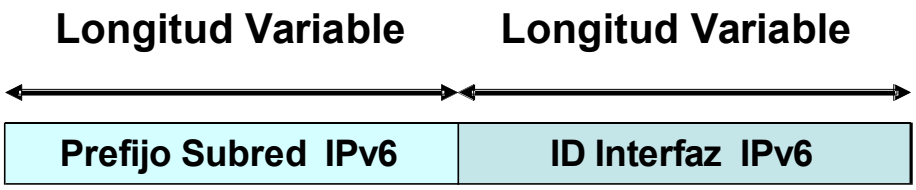

Figura 4 – *Estructura de las direcciones Unicast*

La representación textual de los prefijos de red IPv6 es similar a CIDR (Classless Interdomain Routing) para IPv4, y la notación utilizada para expresar un prefijo es la de "Dirección IPv6/Longitud del prefijo". La Longitud del prefijo es un valor decimal que especifica cuántos bits contiguos de la parte izquierda de la dirección forman parte del prefijo de red a un nivel de encaminamiento dado. Por ejemplo "2001:0145:4556::2/48" representa el prefijo de 48 bits "2001:0145:4556".

Dependiendo del ámbito de una dirección "Unicast", ésta puede pertenecer a un subtipo diferente, si el ámbito es Internet, se denominan "Global Unicast Addresses" y si el ámbito es simplemente un enlace se conocen como "Link-Local IPv6 Unicast Addresses". El primer tipo de direcciones unicast tienen un "prefijo de subred" subdividido en "Global Routing Prefix" donde su valor es asignado a un dominio y el "subnet IP" que identifica un enlace en ese dominio. Las direcciones tipo "Link-Local" se han diseñado para ser usadas en el enlace y su propósito es, entre otros, la auto configuración de IPv6.

El estándar IPv6 define algunas direcciones especiales, siendo mostradas las más importantes en la tabla I:

Direcciones en notación CIDR	Significado
::/128	Dirección no especificada. Se usa cuando la

	interfaz aún no tiene ninguna dirección asignada.
::1/128	La dirección de "loopback", se corresponde con la dirección IPv4 127.0.0.1.
::/96	Las direcciones compatibles IPv4 usadas por SIIT (ver abajo).
::FFFF:0:0/96	Las direcciones compatibles IPv4, también usadas por SIIT (ver abajo).
FE80::/10	El prefijo para las direcciones "Link-Local".
FF00::/8	Direcciones multicast.

Tabla I – *Direcciones IPv6 especiales*.

3.2.- Neighbour Discovery en IPv6

Este protocolo [7] soluciona el conjunto de problemas relacionados con la interacción entre nodos conectados al mismo enlace, definiendo mecanismos para descubrir enrutadores, autoconfigurarse y resolver direcciones de nivel de enlace entre otros. El protocolo IPv6 Neighbour Discovery (ND) es similar al protocolo ARP de IPv6, sin embargo tiene más funcionalidades. Además, ND se basa en el protocolo ICMPv6 [8] que usa multicast a nivel de red, mientras que ARP depende de las diferentes implementaciones del nivel de enlace. Cuando dos nodos pertenecientes al mismo enlace desean enviarse paquetes, deben conocer sus respectivas direcciones de nivel de enlace, típicamente una dirección MAC Ethernet. En este caso, el nodo que inicia la comunicación envía un mensaje especial ICMPv6 "Neighbour Solicitation" a una dirección multicast, preguntando por la dirección MAC del nodo. El otro nodo al recibir este mensaje, responde con un mensaje "Neighbour Advertisement" anunciando su dirección MAC.

En IPv6 los nodos se suelen configurar automáticamente. Los enrutadores IPv6 tienen un prefijo de red configurado manualmente en sus interfícies y envían mensajes de "Router Advertisement" periódicamente. En estos mensajes incluyen dicho prefijo y algunos otros parámetros importantes para la auto configuración. Los nodos, al arrancar, configuran una dirección "Link-local" IPv6 basándose en su propia dirección de nivel dos en todas sus interfícies de red. Esta dirección la pueden usar para comunicarse en ese mismo enlace. Una vez asignada esta dirección deben configurar una dirección "Global Unicast Address" para poder comunicarse con otros nodos que no estén conectados a su mismo enlace. El nodo crea un identificador de interfaz (64 bits), basándose de nuevo en la dirección de nivel 2 [9] y, añadiendo el prefijo

obtenido gracias a los mensajes “Router Advertisement” genera una “Global Unicast Address”. Este tipo de configuración se denomina “Stateless Autoconfiguration”. IPv6 también soporta “Stateful Autocnfiguration” donde los nodos se configuran usando DHCPv6 [10], y configuración manual.

3.3.- Arquitectura de Direccionamiento de IPv6

IPv6 se esta desplegando ampliamente en redes experimentales, y la IANA (Internet Assigned Numbers Authority) a través de los RIRs (Regional Internet Registries) está asignando direcciones IPv6. RIPE (Réssaux IP Européens) es el RIR encargado de Europa, y está asignando direcciones IPv6 a ISPs y otras entidades. La actual política de asignación de direcciones IPv6 [11,12,13] define que el bloque de direcciones 2000::/3 será el primero en ser asignado. Los RIRs asignarán prefijos /32 a los ISPs, a su vez, los ISPs asignarán /48 a redes finales (como universidades) y a los usuarios finales (como subscriptores DSL) se les asignarán bloques /64. Finalmente, si un usuario sólo requiere una dirección (como usuarios móviles) y no necesitarán más direcciones en el futuro, se les asignará un prefijo /128. IANA y los RIRs asignarán bloques de direcciones adyacentes siempre que sea posible. En Febrero de 2005 se han asignado cerca de 1500 millones de prefijos de /48 bits (a centros de educación, ISPs comerciales…), siendo más de la mitad asignados por RIPE [14].

4.- Mecanismos de Transición

No es previsible que IPv6 se despliegue de manera rápida. Actualmente existe una gran infraestructura IPv4 desplegada y funcionando, y por lo tanto, el despliegue de IPv6 debe ser tan poco disruptivo como sea posible. Esto significa que, aunque IPv4 e IPv6 no son compatibles, deberán coexistir por un periodo de tiempo indeterminado. Los mecanismos de transición proporcionan comunicación entre nodos IPv4 e IPv6, y aunque se han definido varios, la IETF se está centrando en unos pocos.

Los mecanismos de transición se pueden dividir en tres clases:

- Doble Pila → Se instalan ambos protocolos (IPv4 e IPv6) en nodos y enrutadores. Si se desea comunicación IPv4 se usa la infraestructura IPv4, y lo mismo sucede si se desea una comunicación IPv6.
- Entunelamiento → Los paquetes IP se encapsulan en otros paquetes IP creando un enlace virtual. Se pueden encapsular paquetes IPv6 en paquetes IPv4 y atravesar redes IPv4 o viceversa.

- Mecanismos de Traducción → Las cabeceras IPv4 se traducen a cabeceras IPv6 y viceversa siguiendo unas reglas predefinidas.

4.1.- Doble Pila

La doble pila es el mecanismo de traducción más simple, proporciona comunicación entre todos los nodos, sin necesitar encapsulación ni traducción (que en general son procesos costosos). Sin embargo existen inconvenientes, los administradores de sistemas deben mantener dos infraestructuras y no se reduce la demanda de direcciones IPv4.

4.2.- Entunelamiento

Existen diferentes tipos de mecanismos de transición basados en el entunelamiento: Configured Tunnels [15], Automatic Tunnels y 6to4 [16]. En general, el principal objetivo es permitir comunicación entre nodos o redes IPv6 asiladas atravesando redes IPv4. La figura 5 muestra un ejemplo:

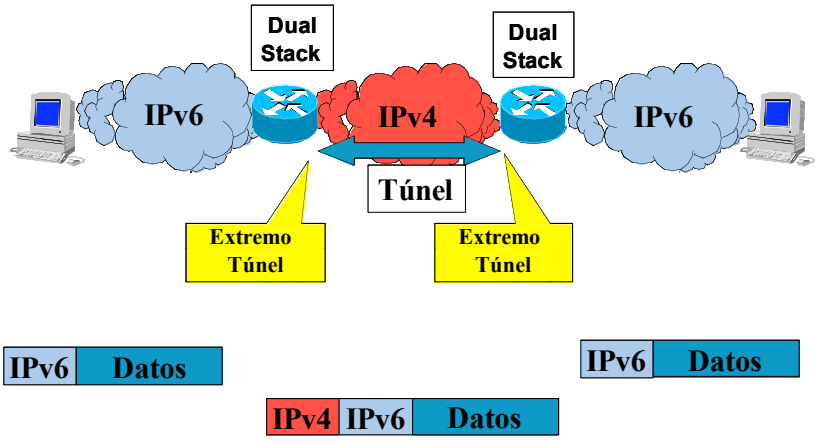

Figura 5 – *Dos redes IPv6 se comunican usando una red IPv4***.**

Dependiendo en qué tipo de túneles se usen, la configuración se hace automáticamente (a través de direcciones IPv6 especiales, bajo demanda por el usuario o bien usando vínculos predefinidos entre direcciones IPv4 e IPv6) o manualmente (por los administradores). En general los mecanismos de transición basados en entunelamiento son fáciles de desplegar, son transparentes para los nodos IPv6. Sin embargo deben enviarse dos cabeceras IP, en algunos casos configurar los túneles manualmente o usar direcciones IPv4 (lo que sigue sin reducir la demanda).

Esta aproximación al problema de la transición ha sido probada con éxito en la red del 6BONE [17] o la del proyecto LONG [18] entre otras. Este mecanismo ha sido definido para las etapas iniciales del despliegue de IPv6, donde la infraestructura IPv6 existente es escasa, y la IPv4 abundante.

4.3.- Mecanismos de Traducción

Los mecanismos de traducción proporcionan comunicación entre nodos IPv4 e IPv6 traduciendo las cabeceras de los paquetes IP/ICMP. El algoritmo que se sigue es "Stateless IP/ICMP Translation Algorithm" (SIIT) [19] que especifica cómo debe hacerse esa traducción, las reglas pueden verse en la tabla II:

Campo de la cabecera IPv6	**IPv4 →**	**IPv6**
Version	4	6
Traffic Class (Class of Service)	Xxxxxxxx	Xxxxxxxx (el TOS y el bit de preferencia se copian)
Flow Label	N/A	0
Payload Length	X	X-tamaño(cabecera IPv4)-tamaño(opciones IPv4)
Next Header	X	X
Hop Limit	X	X-1
Source Address	A.B.C.D	::FFFF:A.B.C.D
Destination Address	E.F.G.H	::FFFF:0:E.F.G.H

Campo de la cabecera IPv4	**IPv6 →**	**IPv4**
Version	6	4
IP Header Length	N/A	5 (sin opciones)
TOS y precedence	Xxxxxxxx	Xxxxxxxx
Total Length	X	X + tamaño(cabecera IPv4)
Identification	N/A	0
Flags	N/A	MF=0 DF=1
Fragment Offset	N/A	0
TTL	X	X-1
Protocol	Next Header=X	X
Header Checksum	-	(generado)
Source Address	::FFFF::A.B.C.D	A.B.C.D
Destination Address	::FFFF:0:E.F.G.H	E.F.G.H

Tabla II – *Reglas de SIIT para traducir cabeceras IPv4 a IPv6 y viceversa.*

NAT-PT (Network Address Translation- Protocol Translation) [20] se basa en NAT y utiliza las reglas de SIIT para traducir el paquete, aunque presenta algunas diferencias respecto a cómo se traducen las direcciones. En efecto, mientras SIIT requiere de algún mecanismo complejo de asignación y encaminamiento temporal de direcciones IPv4 a nodos IPv6, en NAT-PT se puede hacer una asignación de direcciones disponibles (de un conjunto dado) más sencilla.. Puede proporcionar comunicación bidireccional entre nodos IPv4 y nodos IPv6 siendo transparente para éstos, además, ya existe una gran experiencia configurando dispositivos basados en NAT. Sin embargo, la traducción es un proceso costoso, hereda algunos de los problemas de NAT (no puede proporcionar comunicación extremo a extremo y si el protocolo de transporte envía la dirección IP se requiere algún sistema específico para ese determinado protocolo) y, finalmente, no soporta cabeceras de extensiones. Por lo tanto, muchas de las nuevas funcionalidades de IPv6 (como la movilidad) no son soportadas por NAT-PT. A pesar que NAT-PT ha sido usado intensamente en redes experimentales, la IETF se esta planteando prescindir de la especificación debido a su baja aplicabilidad.

5.- Sumario

IPv6 es la versión 6 del "Internet Protocol", IETF lo ha diseñado como el substituto natural de IPv4, éste jamás fue diseñado para soportar una red tan grande como Internet y a pesar que ha demostrado su escalabilidad, el actual crecimiento de Internet lo esta llevando a sus limites.

Este artículo presenta una visión general del protocolo IPv4, mostrando el formato de su cabecera y su modo de funcionamiento. También se presenta el protocolo "Neighbour Discovery" y su arquitectura de direccionamiento. Uno de los mayores problemas de IPv6 es su transición desde IPv4. El artículo explica el funcionamiento de diferentes mecanismos de transición existentes definidos por la IETF.

IPv6 esta preparado para un despliegue global, cerca de 1500 millones de prefijos de /48 bits han sido asignados por IANA, y la IETF ha finalizado la estandarización del protocolo (tan solo quedan por definir aspectos puntuales). Los fabricantes ya disponen de implementaciones experimentales de IPv6, y los principales sistemas operativos ya disponen de soporte para IPv6.

Referencias

[1] Postel J. “Internet Protocol”, RFC 791, Septiembre 1981

[2] The Internet Engineering Task Force (IETF) http://www.ietf.org

[3] David D. Clark, “Rethinking the design of the Internet: The end to end arguments vs. the brave new world”, ACM Transactions on Internet Technology, Vol 1, No 1, Agosto 2001

[4] S. Deering, R. Hinden “Internet Protocol Version 6 (IPv6) Specification” RFC 2460

[5] J. McCann, S. Deering, J. Mogul “Path MTU Discovery for IP version 6” RFC 1981

[6] Fransson P, Jonsson A “End-to-End measurements on performance penalties of IPv4 options”, Global Telecommunications Conference, Diciembre 2004

[7] T. Narten, E. Nordmark, W. Simpson “Neighbor Discovery for IP Version 6 (IPv6)” RFC 2461

[8] A. Conta, S. Deering “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification” RFC 2463

[9] S. Thomson, T. Narten “IPv6 Stateless Address Autoconfiguration” RFC 2462

[10] D. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)” RFC 3315, Julio 2003

[11] D. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)” RFC 3315, July 2003

[12] APNIC, ARIN, RIPE NCC, “IPv6 Address Allocation and Assignment Policy”, ripe-267, Enero 2003

[13] R. Hinden, S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture”, RFC 3513, Abril 2003

[14] RIPE IPv6 Allocation, Statistics http://www.ripe.net/rs/ipv6/stats/

[15] R. Gilligan, E. Nordmark, “Transition Mechanisms for IPv6 Hosts and Routers”, RFC 1933, April 1996

[16] B. Carpenter, K. Moore “Connection of IPv6 Domains via IPv4 clouds”, RFC 3056, February 2001

[17] 6BONE, testbed for deployment of IPv6, http://www.6bone.net

[18] LONG, “Laboratories over Next Generation Networks” IST-1999-20393. http://long.ccaba.upc.edu

[19] E. Nordmark, “Stateless IP/ICMP Translation Algorithm (SIIT)” RFC 2765, Febrero 2000

[20] G. Tsirtsis, P. Srisuresh, “Network Address Translation – Protocol Translation (NAT-PT)”, RFC 2766, Febrero 2000

Albert Cabellos-Aparicio es estudiante de doctorado en el departamento de Arquitectura de Computadores de la Universidad Politécnica de Cataluña (UPC). Allí recibió el título de Ingeniero en Informática (2001). Sus principales temas de investigación son Movilidad, gestión y provisión de Calidad de Servicio y transición a IPv6. Actualmente está trabajando con diversos protocolos de movilidad. Simultáneamente al inicio de la tesis Doctoral también está desempeñando tareas de soporte a la investigación al Centro de Comunicaciones Avanzadas de Banda Ancha (CCABA). Aparte también ha formado parte en proyectos IST, como por ejemplo LONG (http://long.ccaba.upc.edu) y en proyectos del Ministerio de Ciencia y Tecnología como SABA y SAM. Actualmente participa en E-NEXT y EuQoS. Para información más detallada se puede consultar http://www.ccaba.upc.edu. <acabello@ac.upc.edu>

Jordi Domingo Pascual. Ingeniero de Telecomunicación (ETSETB UPC), Doctor en Informática (FIB UPC), Catedrático de Universidad del Departament d'Arquitectura de Computadors (UPC). Promotor y fundador del Centro Específico de Investigación de Comunicaciones Avanzadas de Banda Ancha (CCABA) de la UPC. Participación en proyectos de investigación: Technology for ATD, EXPLOIT, InfoWin, MICC, IMMP, LONG, ENET, E-NEXT y EuQoS. Participación como responsable en proyectos financiados por la CICYT: PLANBA, AFTER, TR-1, SABA, SABA2, SAM. Participación en proyectos financiados por la CICYT: TIC99-0572-C02-02, CASTBA, MEHARI, MIRA. Otros proyectos de I+D: Internet2 Catalunya (i2CAT), responsable de la infraestructura de comunicaciones de banda ancha (proyecto GigaCAT). Participación en proyectos de cooperación: Programa Erasmus/Socrates, Leonardo, COST237 (Multimedia Telecommunication Services), COST264 (Enabling Networked Multimedia Group Communication), COST263 (Quality of Future Internet Services). Temas de investigación en los que ha publicado: conmutación ATM, redes ATM, encaminamiento ATM, control de admisiones ATM, caracterización de tráfico en redes ATM, comunicaciones de Banda Ancha, multicast, provisión de calidad de servicio en redes IP, servicios avanzados de red (multicast, IS, DS, MPLS, movilidad, IPv6), análisis de tráfico IP, coexistencia IPv4-IPv6 y mecanismos de transición. Más información en: http://personals.ac.upc.edu/jordid/ y http://www.ccaba.upc.edu. <jordi.domingo@ac.upc.edu>