Durante los años del boom de las telecomunicaciones no se paraba de hablar de las excelencias de dos tecnologías que revolucionarían el mundo de la telefonía móvil y de Internet, UMTS e IPv6, respectivamente. Sabemos que la primera, tras muchos retrasos, por fin empezará a despegar, pero ¿qué ha pasado con IPv6? ¿Es realmente necesario?

¿Qué ha pasado con IPv6?

El funcionamiento de IPv4, la versión actual del protocolo IP, ha sido totalmente satisfactorio, pero las nuevas tendencias del mundo de las telecomunicaciones pusieron de manifiesto nuevas necesidades que no eran cubiertas por esta versión, como la conexión de un mayor número de dispositivos, la convergencia de todo tipo de tráfico en la misma red y la seguridad de las comunicaciones. Por el momento, la introducción de nuevos protocolos en torno a IP ha permitido ir superando estas limitaciones, pero sólo temporalmente o de forma parcial. El despliegue de la nueva versión de IP, IPv6, no puede continuar demorándose más, pues la aplicación actual del protocolo IPv4 podría limitar a medio plazo el despliegue completo de los servicios de la tercera generación de móviles, de las redes domóticas y de las redes de computación distribuida.

Mayor número de direcciones

La razón principal que originó la necesidad de IPv6 fue la evidencia de falta de direcciones, derivada del vertiginoso crecimiento de Internet, problema que se vio agravado por la falta de coordinación en la delegación de direcciones durante los años 80, lo que provocaba que incluso se dejaran grandes espacios discontinuos. No obstante, esta falta de direcciones no es igual en todos los puntos de la red: mientras que, de momento, es casi inapreciable en Norteamérica (donde se asignaron la mayor parte de las direcciones clase A y B), en zonas como Europa y Asia la situación es crítica. Además, el problema es creciente, debido principalmente al tremendo desarrollo de la telefónica móvil celular y la inminente aparición comercial de UMTS. Los móviles se convertirán en dispositivos siempre conectados a Internet y será necesario asignarlos una dirección IP fija y única. Del mismo modo, la domótica requiere que la pasarela residencial o punto de acceso al hogar, tenga una conexión permanente de banda ancha a Internet, con una dirección IP fija y bien conocida.

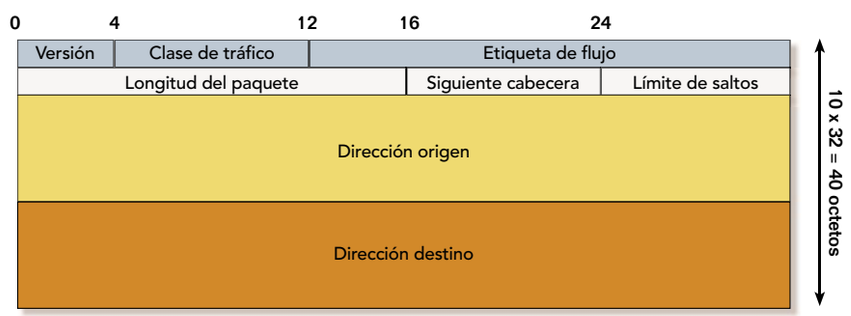
Para solventar los problemas de disponibilidad de direcciones IP, los proveedores de servicios Internet proporcionan a sus clientes direcciones IP privadas, es decir, no reconocidas en Internet, mediante mecanismos de conversión de direcciones (NAT – Network Address Translation). De este modo, se usa una sola dirección IP pública para toda una red privada. El inconveniente es que este mecanismo no puede utilizarse en los terminales móviles ni con tecnologías como IPSec y VoIP.

Por otro lado, el crecimiento de Internet ha puesto también de manifiesto la pobre flexibilidad de la jerarquía de direcciones de IPv4. Debido a la pocos niveles de esta jerarquía de las direcciones, que sólo consideran una parte de subred y otra de sistema, las tablas de encaminamiento de las redes troncales de Internet han crecido enormemente, reduciendo la eficiencia de los routers. Este problema ha sido resuelto, aunque únicamente en parte, mediante el *supernetting* o CIDR, que básicamente consiste en dividir las direcciones en bloques de tamaño variable. Del mismo modo, para poder reducir las redes en subredes surgió el proceso conocido como *subnetting*. El *subnetting* proporciona al administrador varios beneficios, como una flexibilidad adicional, un uso más eficiente de las direcciones de red y la capacidad de soportar tráfico de *broadcast* (el tráfico de *broadcast* nunca atraviesa los routers).

Para solucionar definitivamente estos problemas, en IPv6 el espacio de direcciones se incrementa de 32 a 128 bits, soportando jerarquías de direccionamiento más flexibles basadas en la agregación, un mayor número de nodos direccionables y la auto configuración de las direcciones. Los 128 bits de las direcciones IPv6 identifican interfaces individuales o grupos de interfaces, perteneciendo cada una de ellas a un único nodo.

Una única interfaz puede tener múltiples direcciones IPv6 de cualquier tipo; por ejemplo, podría tener una dirección unicast

Cabecera de IPv6



(destinada a una única interfaz), otra *anycast* (destinada a una interfaz entre varias posibles) y otra *multicast* (destinada a varias interfaces) simultáneamente. Es decir, desaparecen las direcciones *broadcast* (destinada a todas las interfaces) que tantos problemas de diseño y sobrecarga de la red originan en IPv4, pero sin perder funcionalidad, pues el *broadcast* es realmente un subconjunto del tráfico multicast. Por otro lado, aparecen las direcciones *anycast*, muy útiles, por ejemplo, para aplicaciones grid.

En IPv6 se han definido varios tipos distintos de direcciones, que vienen indicadas por los primeros bits de la dirección. Este campo de longitud variable se denomina prefijo y permite conocer dónde está conectado un determinado nodo, es decir, su ruta de encaminamiento. La dirección IPv6 se compone, por consiguiente, de un prefijo seguido de un identificador de nodo. Existen direcciones globales agregables basadas en el proveedor utilizadas para comunicaciones globales en todo Internet. También hay direcciones de uso local que tienen un ámbito de encaminamiento local, pero que de forma automática se puede renumerar cuando sea necesaria la conexión a Internet. En IPv6 la renumeración de las direcciones locales o privadas se hace automáticamente, facilitando, por ejemplo, el cambio de proveedor de servicios.

La auto configuración, finalmente, resulta de gran utilidad cuando hay que tratar con muchos dispositivos IPv6. El protocolo ND, sustituto de ARP, ofrece, entre otros, mecanismos para descubrir routers, auto configurar direcciones, resolver direcciones, determinar el siguiente salto, detectar direcciones duplicadas o cambios, redirección, etc. Por lo tanto, ya no es prioritaria la utilización de DHCPv6, basada en el modelo cliente-servidor y que requiere trabajos explícitos, por parte de los administradores de redes, para facilitar la realización de cambios en las redes y mejorar el aprovechamiento del espacio de direcciones asignado.

Breve glosario

- **ARP.** Address Resolution Protocol
- **ATM.** Asyncronous Transfer Mode
- **CIDR.** Classless Inter-Domain Routing
- **DHCP.** Dynamic Host Configuration Protocol
- **Diffserv.** Differentiated services
- **DNS.** Domain Name Service
- **IETF.** Internet Engineering Task Force
- **IP.** Internet Protocol
- **IPSec.**Internet Protocol Security
- **MPLS.** MultiProtocol Label Switching
- **NAT.** Network Address Translation
- **ND.** Neighbour Discovery
- **QoS.** Quality of Service
- **RFC.** Request For Comments
- **SSL.** Secure Sockets Layer
- **TCP.** Transmission Control Protocol
- **TE.** Traffic Engineering
- **UMTS (3G).** Universal Mobile Telecommunications System
- **VoIP.** Voice over IP
- **VPN.** Virtual Private Network

Aplicaciones en tiempo real

Una de las limitaciones inherentes a IPv4 es que no está preparado para soportar las nuevas aplicaciones de Internet como la transmisión de vídeo y audio en tiempo real, si bien se han ido incorporando gradualmente ciertas mejoras. Por ejemplo, MPLS (Multi-Protocol Label Switching) ha permitido que los *routers* de la red troncal, además de encaminar, puedan conmutar algunos de los paquetes que procesan. Por otro lado, ha supuesto otras ventajas como realizar TE, cursar tráfico con diferentes grados de calidad de servicio (QoS) y crear redes privadas virtuales (VPN) basadas en IP. Por otro lado, Diffserv es un protocolo que se ejecuta en el extremo de la red para indicar la calidad requerida para cada paquete. En IPv6, a diferencia de IPv4, tanto Diffserv como MPLS están integrados dentro del propio protocolo; por ejemplo, la etiqueta MPLS es un campo más de la cabecera. Por otro lado, el encaminamiento en la red troncal es más eficiente en IPv6.

Pero, además, para reducir el tiempo de procesamiento de los paquetes, se ha simplificado el formato de la cabecera de IPv4. La cabecera de IPv6 elimina o hace opcionales varios campos de la cabecera del IP actual, consiguiendo una cabecera de tamaño fijo y más simple. En concreto, de los 12 campos de la cabecera IPv4 se ha pasado a 8 en la nueva versión, eliminando campos redundantes o no necesarios para el encaminamiento, que son codificados ahora en cabeceras opcionales de extensión. La cabecera básica de IPv6 tiene una longitud fija de 40 octetos, lo cual facilita mucho su procesamiento, a pesar de que el tamaño sea mayor que la mínima de la versión 4, que era de 20 octetos. La cabecera básica y las de extensión en IPv6 están además alineadas a un múltiplo entero de 64 bits, pudiendo ser así más eficientemente

Recursos Web

- IETF: http://www.ietf.org.
- IPv6 Forum: http://www.ipv6forum.com.

procesada por la nueva generación de procesadores.

Seguridad de las comunicaciones

La seguridad en IPv4 se consigue mediante IPSec, que es una colección de estándares diseñados específicamente para crear conexiones punto a punto seguras utilizando encriptación fuerte y criptografía de clave pública. IPSec no es actualmente parte de la versión 4 de IP, pero sí de IPv6. Además, todas las debilidades del estándar han sido corregidas en la nueva versión de IP.

Los paquetes IPv6 disponen de una cabecera optativa de extensión destinada a la autenticación evitando, entre otras cosas, el camuflaje de direcciones y el envío masivo de correo. También se ha incluido un campo optativo de seguridad encapsulado en una cabecera de extensión que permite la encriptación del contenido de forma independiente del método de cifrado.

Aunque, según los expertos, en 2008 el uso de la llamada Internet 2, basada en IPv6, estará generalizado, en estos momentos, Japón y Corea son los únicos países en donde está más implantada, ya que allí existía una gran escasez de direcciones. En Estados Unidos, la introducción del nuevo IP va lenta, puesto que en este país el problema de direccionamiento es menor que en el resto del mundo, pues, de hecho, poseen la mayor parte de las direcciones IP. En Europa, se habrá generalizado probablemente antes de esa fecha. No en vano, y concretamente en España, son varias las empresas e instituciones que, como, por ejemplo, Telefónica I+D o la Universidad Politécnica de Madrid, ya están preparadas para soportarlo.

RAMÓN JESÚS MILLÁN TEJEDOR
Ingeniero de Telecomunicación y Master en Tecnologías de la Información

Transición a la nueva versión

En la actualidad, como la gran mayoría de las operadoras y empresas utiliza nodos IPv4, es muy baja la motivación para el cambio. Se pensaba que las nuevas mejoras que hacen que las redes IPv6 sean más fáciles de configurar y mantener serían lo suficientemente atractivas como para activar su despliegue por las nuevas operadoras surgidas a finales del siglo pasado, obligadas a realizar un despliegue de infraestructura muy rápido, pero, en la práctica, no ha sido así.

El nuevo IP puede ser implementado como una actualización software en la mayoría de los nodos IPv4 actuales, pero la adquisición y despliegue de este software conlleva una fuerte inversión para las operadoras de telecomunicaciones. La introducción

de IPv6 supondrá, además, que todo el personal de ingeniería y soporte de las operadoras y empresas adquiera competencias en la nueva tecnología, lo cual supone tiempo e inversiones. Respecto de los usuarios particulares, instalar el nuevo protocolo requiere añadir un software al sistema operativo Linux, Unix o Windows, aunque en los más modernos, como es el caso de Windows XP, lo único que hay que hacer es activarlo, puesto que ya está instalado.

Proceso gradual. Como la transición de IPv4 a IPv6, dada la magnitud de los sistemas implicados, el proceso se llevará a cabo de forma gradual, teniendo que coexistir ambas versiones durante varios años. El principal problema de la migración es que, mientras los sistemas IPv6 son compatibles hacia atrás (es decir, pueden enviar, encaminar y recibir paquetes IPv4), los sistemas IPv4 actuales no son capaces de manejar paquetes IPv6. Lo ideal sería declarar unos días de inactividad, durante los cuales todas las máquinas de Internet se desactivarían, y se migraría al nuevo estándar. No obstante, una tarea así, con millones de máquinas y de administradores de redes implicados, es prácticamente imposible. En cualquier caso, para facilitar la migración es importante que las aplicaciones existentes –como los navegadores, por ejemplo- sean capaces de operar también con las aplicaciones IPv6.

Existen dos alternativas (que pueden trabajar de forma aislada o conjunta) para llevar a cabo la migración de las redes. La primera opción consiste en introducir una doble pila completa de IPv4 e IPv6 en los nodos IPv6. De esta forma, estos nodos pueden enviar y recibir los dos tipos de paquetes. Para ello, deben tener direcciones de ambas clases y han de ser capaces, mediante DNS, de descubrir si otro nodo es capaz de utilizar el nuevo protocolo o sólo la versión 4.

La segunda opción es utilizar túneles, lo que permitiría que los nodos extremos IPv6 se comuniquen siempre en IPv6, aunque haya nodos intermedios IPv4. Se considera un túnel a todos los nodos IPv4 entre dos nodos IPv6. Utilizando esta técnica, el nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, y lo pone en el campo de datos de un paquete IPv4. Este paquete tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que conforma el túnel. Los nodos de este tipo del túnel encaminan el paquete, sin tener constancia de que el paquete que están manejando contiene un paquete IPv6. Cuando este paquete llega al extremo receptor IPv6 del túnel, que es precisamente el destino del paquete, determina que el paquete contiene un paquete IPv6, lo extrae y lo encamina exactamente del mismo modo que si lo hubiera recibido el paquete de un nodo IPv4 vecino.