

IPv6

El **Internet Protocol version 6 (IPv6)** (en español: *Protocolo de Internet versión 6*) es una versión del protocolo **Internet Protocol (IP)**, definida en el **RFC 2460** y diseñada para reemplazar a **Internet Protocol version 4 (IPv4)** **RFC 791**, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

Diseñado por **Steve Deering** de **Xerox PARC** y **Craig Mudge**, IPv6 sujeto a todas las normativas que fuera configurado —está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en **China**, **India**, y otros países asiáticos densamente poblados—. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

A principios de 2010, quedaban menos del 10 % de IP sin asignar.^[1] En la semana del 3 de febrero de 2011, la **IANA** (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPv4 posibilita 4 294 967 296 (2^{32}) direcciones de host diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada dispositivo, teléfono, PDA, tablet, etcétera. En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2^{128} o 340 sextillones de direcciones) —cerca de $6,7 \times 10^{17}$ (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de la Tierra.

Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008.^[2]

1 Motivación y orígenes de las IP

Durante la primera década de operación de Internet basado en TCP/IP, a fines de los 80, se hizo evidente que se necesitaba desarrollar métodos para conservar el espacio de direcciones. A principios de los 90, incluso después de la introducción del rediseño de redes sin clase, se hizo claro que no sería suficiente para prevenir el agotamiento de las direcciones IPv4 y que se necesitaban cambios adicionales. A comienzos de 1992, circulaban varias propuestas

de sistemas y a finales de 1992, la IETF anunció una convocatoria para *white papers* (**RFC 1550**) y la creación de los grupos de trabajo de “IP de próxima generación” (“*IP Next Generation*”) o (IPng).

IPng fue propuesto por el **Internet Engineering Task Force (IETF)** el 25 de julio de 1994, con la formación de varios grupos de trabajo IPng. Hasta 1996, se publicaron varios RFC definiendo IPv6, empezando con el **RFC 2460**.

La discusión técnica, el desarrollo e introducción de IPv6 no estuvo exenta de controversia. El diseño fue duramente criticado por la falta de interoperabilidad con IPv4 y otros aspectos por ingeniero D. J. Bernstein, entre otros.^[3]

Incidentalmente, IPng (IP Next Generation) no pudo usar la versión número 5 (**IPv5**) como sucesor de IPv4, ya que ésta había sido asignada a un protocolo experimental orientado al flujo de *streaming* que intentaba soportar voz, video y audio.

Se espera ampliamente que IPv6 sea soportado en conjunto con IPv4 en el futuro cercano. Los nodos solo-IPv4 no son capaces de comunicarse directamente con los nodos IPv6, y necesitarán ayuda de un intermediario.

2 Cambios y nuevas características

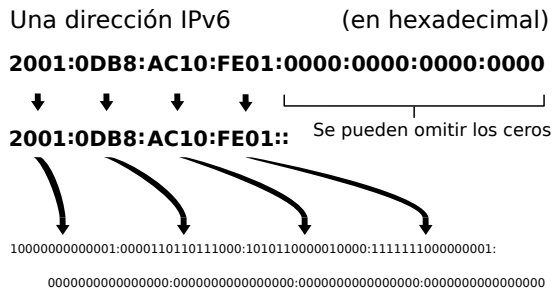
En muchos aspectos, IPv6 es una extensión conservadora de IPv4. La mayoría de los protocolos de transporte -y aplicación- necesitan pocos o ningún cambio para operar sobre IPv6; las excepciones son los protocolos de aplicación que integran direcciones de capa de red, como FTP o NTP.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

Algunos de los cambios de IPv4 a IPv6 más relevantes son:

2.1 Capacidad extendida de direccionamiento

El interés de los diseñadores era que direcciones más largas permitiesen una mejor entrega jerárquica, sistemática y definitiva de las direcciones, y una eficiente agrega-



Una ilustración de una dirección IP (versión 6), en hexadecimal y binario.

ción de rutas. Con IPv4, se desplegaron complejas técnicas de Classless Interdomain Routing (CIDR) para utilizar de mejor manera el pequeño espacio de direcciones. El esfuerzo requerido para reasignar la numeración de una red existente con prefijos de rutas distintos es muy grande, como se discute en [RFC 2071](#) y [RFC 2072](#). Sin embargo, con IPv6, cambiando el prefijo anunciado por unos pocos routers es posible en principio reasignar la numeración de toda la red, ya que los identificadores de nodos (los 64 bits menos significativos de la dirección) pueden ser auto-configurados independientemente por un nodo.

El tamaño de una subred en IPv6 es de 2^{64} (máscara de subred de 64-bit), el cuadrado del tamaño de la Internet IPv4 entera. Así, las tasas de utilización del espacio de direcciones será probablemente menor en IPv6, pero la administración de las redes y el ruteo serán más eficientes debido a las decisiones de diseño inherentes al mayor tamaño de las subredes y la agregación jerárquica de rutas.

2.2 Autoconfiguración de direcciones libres de estado (SLAAC)

Los nodos IPv6 pueden configurarse a sí mismos automáticamente cuando son conectados a una red ruteada en IPv6 usando los mensajes de descubrimiento de routers de [ICMPv6](#). La primera vez que son conectados a una red, el nodo envía una solicitud de router (*RS: Router Solicitation*) de [link-local](#) usando [multicast](#) pidiendo los parámetros de configuración; y si los routers están configurados para esto, responderán este requerimiento con un “anuncio de router” (*RA: router advertisement*) que contiene los parámetros de configuración de capa de red.

Si la autoconfiguración de direcciones libres de estado no es adecuada para una aplicación, es posible utilizar [Dynamic Host Configuration Protocol](#) para IPv6 ([DHCPv6](#)) o bien los nodos pueden ser configurados en forma estática.

Los routers presentan un caso especial de requerimientos para la configuración de direcciones, ya que muchas ve-

ces son la fuente para información de autoconfiguración, como anuncios de prefijos de red y anuncios de router. La configuración sin estado para routers se logra con un protocolo especial de reenumeración de routers.

2.3 Multicast

Multicast, la habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional (aunque usualmente implementado).

IPv6 no implementa *broadcast*, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado. El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (*all hosts*). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red (la dirección de broadcast en una red IPv4) es considerada una dirección normal en IPv6.

Muchos ambientes no tienen, sin embargo, configuradas sus redes para rutear paquetes multicast, por lo que en éstas será posible hacer “multicasting” en la red local, pero no necesariamente en forma global.

El multicast IPv6 comparte protocolos y características comunes con IPv4, pero también incorpora cambios y mejoras. Incluso cuando se le asigne a una organización el más pequeño de los prefijos de ruteo global IPv6, ésta también recibe la posibilidad de usar uno de los 4.2 billones de grupos multicast IPv6 ruteables de fuente específica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios ([RFC 3306](#)). En IPv4 era muy difícil para una organización conseguir incluso un único grupo multicast ruteable entre-dominios y la implementación de las soluciones entre-dominios eran anticuadas ([RFC 2908](#)). IPv6 también soporta nuevas soluciones multicast, incluyendo *Embedded Rendezvous Point* ([RFC 3956](#)), el que simplifica el despliegue de soluciones entre dominios.

2.4 Seguridad de Nivel de Red obligatoria

Internet Protocol Security ([IPsec](#)), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6. El soporte IPsec es obligatorio en IPv6; a diferencia de IPv4, donde es opcional o fue un agregado posterior (pero usualmente implementado). Sin embargo, actualmente no se está usando normalmente IPsec excepto para asegurar el tráfico entre routers de BGP IPv6, aunque también se puede utilizar en OSPFv3 y en movilidad IPv6 (ver Movilidad IPv6)

2.5 Procesamiento simplificado en los routers

Se hicieron varias simplificaciones en la cabecera de los paquetes, así como en el proceso de reenvío de paquetes para hacer el procesamiento de los paquetes más simple y por ello más eficiente. En concreto,

- El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, así los campos que son raramente utilizados han sido movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).
- Los routers IPv6 no hacen fragmentación. Los nodos IPv6 requieren ya sea hacer descubrimiento de MTU, realizar fragmentación extremo a extremo o enviar paquetes menores al MTU mínimo de IPv6 de 1280 bytes.
- El encabezado IPv6 no está protegido por una suma de comprobación (*checksum*); la protección de integridad se asume asegurada tanto por el checksum de capa de enlace y por un checksum de nivel superior (TCP, UDP, etc.). En efecto, los routers IPv6 no necesitan recalcular la suma de comprobación cada vez que algún campo del encabezado (como el contador de saltos o Tiempo de Vida) cambian. Esta mejora puede ser menos necesaria en routers que utilizan hardware dedicado para computar este cálculo y así pueden hacerlo a velocidad de línea (*wirespeed*), pero es relevante para routers por software.
- El campo Tiempo de Vida de IPv4, conocido como TTL (*Time To Live*), pasa a llamarse Límite de saltos, reflejando el hecho de que ya no se espera que los routers computen el tiempo en segundos que tarda en atravesarlo (que en cualquier caso siempre resulta menor de 1 segundo). Se simplifica como el número de saltos entre routers que se permita realizar al paquete IPv6.

2.6 Movilidad

A diferencia de IPv4 móvil (MIPv4), IPv6 móvil (MIPv6) evita el ruteo triangular y por lo tanto es tan eficiente como el IPv6 normal. Los routers IPv6 pueden soportar también Movilidad de Red (NEMO, por *Network Mobility*) (RFC 3963), que permite que redes enteras se muevan a nuevos puntos de conexión de routers sin reasignación de numeración. Sin embargo, ni MIPv4 ni MIPv6 o NEMO son ampliamente difundidos o utilizados hoy, por lo que esta ventaja es más bien teórica.

2.7 Soporte mejorado para las extensiones y opciones

Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

2.8 Jumbogramas

IPv4 limita los paquetes a 64 KiB de carga útil. IPv6 tiene soporte opcional para que los paquetes puedan superar este límite, los llamados jumbogramas, que pueden ser de hasta 4 GiB. El uso de jumbogramas puede mejorar mucho la eficiencia en redes de altos MTU. El uso de jumbogramas está indicado en el encabezado opcional *Jumbo Payload Option*.

3 Direccionamiento IPv6

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374 pero fue redefinida en abril de 2003 en la RFC 3513, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de $2^{128} \approx 3.4 \times 10^{38}$. Este número puede también representarse como 16^{32} , con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores (véase combinatoria).

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

3.0.1 Notación para las direcciones IPv6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales. Por ejemplo,

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

es una dirección IPv6 válida.

Se puede comprimir un grupo de cuatro dígitos si éste es nulo (es decir, toma el valor "0000"). Por ejemplo,

2001:0db8:85a3:0000:1319:8a2e:0370:7344

2001:0db8:85a3::1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos

tivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección:

```
2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab 2001:0DB8::1428:57ab
```

son todas válidas y significan lo mismo, pero

```
2001::25de::cade -- --
```

no es válida porque no queda claro cuántos grupos nulos hay en cada lado.

Los ceros iniciales en un grupo también se pueden omitir:

```
2001:0DB8:02de::0e13 2001:DB8:2de::e13
```

Si la dirección es una dirección IPv4 empotrada, los últimos 32 bits pueden escribirse en base decimal, así:

```
::ffff:192.168.89.9 ::ffff:c0a8:5909
```

No se debe confundir con:

```
::192.168.89.9 ::c0a8:5909
```

El formato ::ffff:1.2.3.4 se denomina *dirección IPv4 mapeada*, y el formato ::1.2.3.4 *dirección IPv4 compatible*.

Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal, 0x874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 o ::874B:2B34. Entonces, uno puede usar la notación mixta *dirección IPv4 compatible*, en cuyo caso la dirección debería ser ::135.75.43.52. Este tipo de dirección IPv4 compatible casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

Cuando lo que se desea es identificar un rango de direcciones diferenciable por medio de los primeros bits, se añade este número de bits tras el carácter de barra "/". Por ejemplo:

```
2001:0DB8::1428:57AB/96 sería equivalente a
2001:0DB8:: 2001:0DB8::874B:2B34/96 sería equi-
valente a 2001:0DB8:: y por supuesto también a
2001:0DB8::1428:57AB/96
```

3.0.2 Identificación de los tipos de direcciones

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los rangos definidos por los primeros bits de cada dirección.

::/128 La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1/128 La dirección de *loopback* es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4/96 La *dirección IPv4 compatible* se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0/96 La *dirección IPv4 mapeada* se usa como mecanismo de transición en terminales duales.

fe80::/10 El prefijo de *enlace local* (en inglés *link local*) especifica que la dirección sólo es válida en el enlace físico local.

fec0:: El prefijo de *emplazamiento local* (en inglés *site-local prefix*) especifica que la dirección sólo es válida dentro de una organización local. La RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Unicast.

fc00::/7 El prefijo de *dirección local única* (en inglés *unique local address*). Esta definido por la RFC 4193. Se usa en substitución de las direcciones 'site-local'.

ff00::/8 El prefijo de multicast. Se usa para las direcciones multicast.

Hay que resaltar que no existen las direcciones de difusión (en inglés *broadcast*) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección *multicast* FF01::1/128, denominada *todos los nodos* (en inglés *all nodes*)

4 Paquete IPv6

Un *paquete* en IPv6 está compuesto principalmente de dos partes: la cabecera (que tiene una parte fija y otra con las opciones) y la carga útil (los datos).

4.1 Cabecera fija

Los primeros 40 bytes (320 bits) son la cabecera del paquete y contiene los siguientes campos:

- direcciones de origen (128 bits)
- direcciones de destino (128 bits)
- versión del protocolo IP (4 bits)
- clase de tráfico (8 bits, Prioridad del Paquete)
- Etiqueta de flujo (20 bits, manejo de la Calidad de Servicio),
- Longitud del campo de datos (16 bits)
- Cabecera siguiente (8 bits)
- Límite de saltos (8 bits, Tiempo de Vida).

Hay dos versiones de IPv6 levemente diferentes. La ahora obsoleta versión inicial, descrita en el [RFC 1883](#), difiere de la actual versión propuesta de estándar, descrita en el [RFC 2460](#), en dos campos: hay 4 bits que han sido reasignados desde “etiqueta de flujo” (*flow label*) a “clase de tráfico” (*traffic class*). El resto de diferencias son menores.

En IPv6 la fragmentación se realiza sólo en el nodo origen del paquete, al contrario que en IPv4 en donde los routers pueden fragmentar un paquete. En IPv6, las opciones también desaparecen de la cabecera estándar y son especificadas por el campo “Cabecera Siguiente” (*Next Header*), similar en funcionalidad en IPv4 al campo Protocolo. Un ejemplo: en IPv4 uno añadiría la opción “ruta fijada desde origen” (*Strict Source and Record Routing*) a la cabecera IPv4 si quiere forzar una cierta ruta para el paquete, pero en IPv6 uno modificaría el campo “Cabecera Siguiente” indicando que viene una cabecera de encaminamiento. La cabecera de encaminamiento podrá entonces especificar la información adicional de encaminamiento para el paquete, e indicar que, por ejemplo, la cabecera TCP será la siguiente. Este procedimiento es análogo al de AH y ESP en [IPsec](#) para IPv4 (que aplica a IPv6 de igual modo, por supuesto).

4.2 Cabeceras de extensión

El uso de un formato flexible de cabeceras de extensión opcionales es una idea innovadora que permite ir añadiendo funcionalidades de forma paulatina. Este diseño aporta gran eficacia y flexibilidad ya que se pueden definir en cualquier momento a medida que se vayan necesitando entre la cabecera fija y la carga útil.

Hasta el momento, existen 8 tipos de cabeceras de extensión, donde la cabecera fija y las de extensión opcionales incluyen el campo de cabecera siguiente que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior. Luego las cabeceras de extensión se van encadenando utilizando el campo de cabecera siguiente que aparece tanto en la cabecera fija como en cada una de las citadas cabeceras de extensión. Como resultado de la secuencia anterior, dichas cabeceras de extensión se tienen que procesar en el mismo orden en el que aparecen en el datagrama. La Cabecera principal, tiene a diferencia de la cabecera de la versión IPv4 un tamaño fijo de 40 octetos. Especifica para asignarlos para aplicaciones multicast intra-dominio o entre-dominios ([RFC 3306](#)). En IPv4 era muy difícil para una organización como ésta.

Todas o parte de estas cabeceras de extensión tienen que ubicarse en el datagrama en el orden especificado:

Cada cabecera de extensión debe aparecer como mucho una sola vez, salvo la cabecera de opción destino, que puede aparecer como mucho dos veces, una antes de la cabecera ruteo y otra antes de la cabecera de la capa superior.

4.3 Carga útil

La carga útil del paquete puede tener un tamaño de hasta 64 KB en modo estándar, o mayor con una opción de carga jumbo (*jumbo payload*) en el encabezado opcional Hop-By-Hop.

La fragmentación es manejada solamente en el host que envía la información en IPv6: los routers nunca fragmentan un paquete y los hosts se espera que utilicen el *Path MTU discovery*.

5 IPv6 y el sistema de nombres de dominio

Las direcciones IPv6 se representan en el [sistema de nombres de dominio](#) (DNS) mediante registros AAAA (también llamados registros de *quad-A*, por tener una longitud cuatro veces la de los registros A para IPv4)

El concepto de AAAA fue una de las dos propuestas al tiempo que se estaba diseñando la arquitectura IPv6. La otra propuesta utilizaba registros A6 y otras innovaciones como las etiquetas de cadena de bits (*bit-string labels*) y los registros DNAME.

Mientras que la idea de AAAA es una simple generalización del DNS IPv4, la idea de A6 fue una revisión y puesta a punto del DNS para ser más genérico, y de ahí su complejidad.

La [RFC 3363](#) recomienda utilizar registros AAAA hasta tanto se pruebe y estudie exhaustivamente el uso de registros A6. La [RFC 3364](#) realiza una comparación de las ventajas y desventajas de cada tipo de registro.

5.1 Mecanismos de transición a IPv6

Ante el [agotamiento de las direcciones IPv4](#), y los problemas que este está ocasionando ya, sobre todo en los países emergentes de Asia como India o China, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos [protocolos](#) durante un año, aunque se piensa que la implantación mundial y total en internet de IPv6 se hará realidad hacia finales de 2012, dada la celeridad con la que se están agotando las direcciones IPv4. La red no podrá aguantar mucho más sin el cambio, y de no realizarse pronto este las consecuencias podrían ser muy graves. ^{[[cita requerida](#)]} Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición pueden clasificarse en tres grupos:

- Doble pila
- Túneles
- Traducción

La **doble pila** hace referencia a una *solución de nivel IP con doble pila* (RFC 4213), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo con doble pila en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

- **A favor:** Fácil de desplegar y extensamente soportado.
- **En contra:** La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

Los **túneles** permiten conectarse a redes IPv6 “saltando” sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como siguiente capa IP el protocolo número 41, y de ahí el nombre *proto-41*. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

La **traducción** es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con un nodo que sólo soporta IPv6. Los mecanismos de traducción se pueden dividir en dos grupos basados en si la información de estado está guardada o no:

- **Con estado:** NAT-PT (RFC 2766), TCP-UDP Relay (RFC 3142), Socks-based Gateway (RFC 3089)
- **Sin estado:** Bump-in-the-Stack, Bump-in-the-API (RFC 276)

6 Despliegue de IPv6

Varios de los mecanismos mencionados más arriba se han implementado para acelerar el despliegue de IPv6. Los distintos servicios de control de Internet han ido incorporando soporte para IPv6, así como los controladores de los dominios de nivel superior (o TLD, en inglés). Además surge como nueva idea para mejorar la ampliación que cubre el direccionamiento de los dispositivos móviles.

7 Anuncios importantes sobre IPv6

- En 2003, Nihon Keizai Shimbun informa que Japón, China y Corea del Sur han tomado la determinación de convertirse en las naciones líderes en la tecnología de Internet, que conjuntamente han dado forma parcialmente al desarrollo de IPv6, y que lo adoptarán completamente a partir de 2005.

- ICANN anunció el 20 de julio de 2004 que los registros AAAA de IPv6 de código de país para Japón (.jp) y Corea (.kr) ya son visibles en los servidores raíz de DNS.^[4] El registro IPv6 para Francia (.fr) fue añadido poco después.^[5]

- El 4 de febrero de 2008 se añade a los servidores raíz de la red (Master Address books) direcciones en IP versión 6 (IPv6). Esto significa que por primera vez las máquinas que utilicen IPv6 pueden encontrarse una a la otra sin la participación de toda la tecnología IPv4.^[6]

- Desde el 2006 muchos sistemas operativos han estado trabajando en IPv6 paralelamente con IPv4, sistemas como GNU/Linux, Mac,^[7] Unix y Windows.^[8]

- El 8 de junio de 2011 se lleva a cabo el Día Mundial de IPv6, que consistió en ofrecer el contenido de algunos de los portales de Internet también con IPv6, sin dejar de hacerlo con IPv4, durante 24 horas. Así mismo algunos de los principales proveedores de servicios de Internet (Telefónica, Claro y Nextel) realizan una prueba para comprobar el funcionamiento de esta tecnología.

- El 6 de junio de 2012 a las 00:00 GMT, se lleva a cabo el Lanzamiento Mundial de IPv6, cuando los principales proveedores de servicios de Internet y Compañías web (Akamai, AT&T, Cisco, Comcast, D-Link, Facebook, Free Telecom, Google, Internode, Kddi, Limelight, Microsoft Bing, Time Warner, XS4ALL, Yahoo!, etc.) habilitaron permanentemente IPv6 en sus productos y servicios <http://www.worldipv6launch.org/>. Falta el título= (ayuda)

8 Referencias

- [1] *Number Resource Organization document*, La NRO es la encargada de asignar IP a los cinco registros internacionales.
- [2] *The source for IPV6 information, trainig, consulting and hardware* Página del gobierno de USA para la implementación de IPV6.
- [3] The IPv6 mess.
- [4] ICANN (20 de julio de 2004). «Next-generation IPv6 Address Added to the Internet's Root DNS Zone» (en inglés). Consultado el 3 de enero de 2010.
- [5] AFNIC (16 de septiembre de 2003). «IPv6 fully integrated in the Production System of AFNIC from October, the 1st 2003» (pdf) (en inglés). Consultado el 3 de enero de 2010.

- [6] ICANN (29 de enero de 2008). «IPv6 Addresses for the Root Servers» (en inglés). Consultado el 3 de enero de 2010.
 - [7] Apple Inc. (2009). «Mac OS X Server Snow Leopard - Networking» (en inglés). Consultado el 3 de enero de 2010.
 - [8] Microsoft Inc. (10 de julio de 2007). «Preguntas más frecuentes sobre el protocolo IPv6 para la familia Windows Server 2003». Consultado el 3 de enero de 2010.
- [Comprueba tu conectividad IPv6](#)
 - [Escanea online puertos en servidores IPv6](#)
 - [Serie de artículos sobre IPv6](#)
 - (en alemán) [Status der IPv6-Einführung in .es](#) (Estado de lanzamiento IPv6 en .es)

9 Véase también

- Internet de las cosas
- Agotamiento de las direcciones IPv4
- Despliegue de IPv6
- Dirección IPv6
- Comparación de soporte IPv6 de aplicaciones
- Mecanismos de transición IPv6
- Anexo:Proveedores de túneles IPv6
- ICMPv6
- Miredo
- SATSIX
- Teredo

10 Enlaces externos

- [RFC 2460](#)
- [RFC 2460 \(en español\)](#)
- [Página del Proyecto y Grupo de Trabajo de IPv6 de la UNAM](#)
- [Breve descripción del protocolo IPv6 y otros protocolos](#)
- [Implicaciones de seguridad en IPv6](#)
- [Tutoriales y formación gratuitas de IPv6 - Castellano e Ingles](#)
- [Libro Gratuito “IPv6 para Todos”](#)
- [Ayuda y Soporte de IPv6](#)
- [Ayuda y Soporte de IPv6 para México](#)

11 Origen del texto y las imágenes, colaboradores y licencias

11.1 Texto

- **IPv6** Fuente: <https://es.wikipedia.org/wiki/IPv6?oldid=85945562> Colaboradores: Manuel González Olaechea y Franco, JorgeGG, Tony Rotondas, Sam Hocevar, Dodo, Triku, Sms, Netgrino, Ihavenomouth, Adal, Barcex, Jarfil, Jazzka, Enric Naval, Jag2k4, Kalcetin, Barasoaindarra, Almorca, Ecemaml, Chewie, Niqueco, Renabot, Caos, Javier Valero, Airunp, Rembiapo pohiyete (bot), Ttwaring, Johnbojaen, Aadrover, Orgullobot~eswiki, RobotQuistnix, Yrbot, FlaBot, Vitamine, YurikBot, Mortadelo2005, Icvav, Equi, Zam, KnightRider, Mercy, Fravia, Er Komandante, Lasneyx, Davis15, Carlosdavid~eswiki, Qwertyytrewqqwerty, CEM-bot, Damifb, Laura Fiorucci, Pablo.roschiani, FrancoGG, Resped, PabloCastellano, Renatux~eswiki, Mahadeva, Jquince, Cratón, Isha, Xoneca, JAnDbot, Jugones55, Death Master, Muro de Aguas, Gaius iulius caesar, TXiKiBoT, Sifter, Kiocone, Humberto, Rei-bot, Pólux, Chandro, AlnoktaBOT, Cinevoro, Aibot, VolkovBot, Luinav, Technopat, Matdrones, Alejandroscf, Barri, Ingteleco, Muro Bot, Edmenb, BotMultichill, SieBot, Bigsus-bot, RICAR-DOSA, Ugly, Chico512, Yonseca, Mutari, Egjose, [?][?][?] robot, Reyesoft, Finnwind, Aleix87, Facundov60i, Botellín, MenoBot, LordT, Furti, Alexbot, Valentin estevez navarro, PhoneixS, Macuro, UA31, AVBOT, DayL6, Dermot, FerLezcano, Diegusjaimes, Linfocito B, Arjuno3, EdBever, Saloca, Luckas-bot, Valor 108, Valor10, Davidbqzt, Nallimbot, Gacpro, Yonidebot, Arcenal, Olmosv6, Xor085, DSisyphBot, ArthurBot, SuperBrailio13, Juamax, Manuel15, Xqbot, Jkbw, Rubinbot, Edvac, Josemariasaldana, Cejota edu, Bodigami, Botarel, AstaBOTH15, TiriBOT, Hprmedina, RedBot, Kizar, Enrique Cordero, Dbritos, Leugim1972, PatruBOT, KamikazeBot, TjBot, Jefri002, GrouchoBot, Wikiléptico, Cesarolvera, EmausBot, Savh, ZéroBot, Remux, Barbanegra, Grillitus, KLBOT, Victoria84, Nicepawn, Jordipalet, NETLab, Mtorrecilla, MerliwBot, KLBOT2, MetroBot, Invadibot, Nickmman, Cristovan, Mega-buses, LlamaAl, Elvisor, Asqueladd, Tsunderebot, Chmarkine, Balles2601, Jyanez747, MangelC13, Jarould, El chidjkjfl y Anónimos: 287

11.2 Imágenes

- **Archivo:Ipv6_address-es.svg** Fuente: https://upload.wikimedia.org/wikipedia/commons/1/1a/Ipv6_address-es.svg Licencia: Public domain Colaboradores:
- **Ipv6_address.svg** Artista original: Ipv6_address.svg: Indeterminate

11.3 Licencia del contenido

- Creative Commons Attribution-Share Alike 3.0