Responsabilidad Corporativa y Sostenibilidad

Cuaderno Red de Cátedras Telefónica

Universidad Carlos III de Madrid

La farragosa transición a IPv6

Cátedra Telefónica de Internet del Futuro para la Productividad

La Internet se encuentra en tiempos difíciles ya que se está quedando sin direcciones y tendrá que ser solucionado para permitir el continuo crecimiento en la segunda mitad de la década 2010 y posterior. La idea era que la solución a este problema pasaría silenciosamente en segundo plano, pero en los últimos años, ha quedado claro que el cambio del actual IPv4 que se está quedando sin direcciones a la nueva versión IPv6 resultará un asunto bastante complicado.

Iljitsch van Beijnum, Lisardo Prieto, Marcelo Bagnulo

Diciembre 2010

www.catedras.telefonica.es
www.rcysostenibilidad.telefonica.com

Telefónica

Biografía

Iljitsch van Beijnum

Iljitsch es investigador en el Instituto IMDEA Networks y realiza sus estudios de doctorado en la Universidad Carlos III de Madrid. Iljitshc ha escrito dos libros, uno sobre BGP y otro sobre IPv6.

Lisardo Prieto

Lisardo es Profesor Ayudante del Departamento de Ingeniería Telematica de la Universidad Carlos III de Madrid donde realiza sus estudios de doctorado.

Marcelo Bagnulo

Marcelo es Profesor Titular del Departamento de Ingeniería Telematica de la Universidad Carlos III de Madrid. Es el Director de la Catedra Telefónica de Internet del Futuro para la productividad de la Universidad Carlos III de Madrid.

Índice

1. Resúmen

En 1993, 1.3 millones [1] de hosts (PCs, estaciones de trabajo, servidores, etc.) estaban conectados a Internet. Este verano, ese número alcanzó 769 millones [2] de hosts, únicamente teniendo en cuenta los equipos que tienen un nombre DNS. La noción de un ordenador que no está conectado a Internet es potencialmente absurda [3] en estos días. Por supuesto, hay problemas como el spam o los virus de tipo gusano, sin embargo no han conseguido ralentizar las cosas. Todo eso va a cambiar en los próximos años. La Internet se encuentra en tiempos difíciles ya que se está quedando sin direcciones y tendrá que ser solucionado para permitir el continuo crecimiento en la segunda mitad de la década 2010 y posterior. La idea era que la solución a este problema pasaría silenciosamente en segundo plano, pero en los últimos años, ha quedado claro que el cambio del actual IPv4 (Internet Protocol versión 4) que se está quedando sin direcciones a la nueva versión IPv6 resultará un asunto bastante complicado.

2. El problema en general

En las tecnologías de la información se emplean grandes cantidades de esfuerzo y dinero para mantener sistemas antiguos “heredados” en ejecución durante décadas. Hay aviones que vuelan en círculos quemando valioso combustible porque el control aéreo no puede estar al día y utiliza sistemas menos potentes que un teléfono inteligente. Las redes Wi-Fi no alcanzan sus velocidades máximas porque un original 802.11 (sin letra) sistema a 2 Mbps podría aparecer, nunca se sabe. Los ejemplos varían desde enormes y costosos hasta pequeños y simplemente molestos. Así que los ingenieros sueñan, soñamos en dejar toda la tecnología de ayer atrás y empezar de cero. Pero cuando llegamos a hacer eso, una de dos: o el nuevo sistema puntero no funciona tan bien como se esperaba, o lo hace pero los usuarios no quieren implementarlo. Joel Spolksy lo explica en su post “Cosas que nunca debería hacer, Parte I” [4].

Incluso si el nuevo sistema es en realidad superior al anterior, los usuarios podrían negarse a actualizar por una gran variedad de razones. La historia de la nueva Coca-Cola [5] es ilustrativa a este respecto: a las personas simplemente no les gusta el cambio (pregunte a cualquier persona si alguna vez ha rediseñado su sitio web). E incluso cuando ese problema se puede evitar, a veces simplemente no hay forma de hacerlo. Por ejemplo,

la especificación original de Ethernet a 10 Mbps permite paquetes de 1500 bytes. Llenar los 10 Mbps requiere unos 830 de esos paquetes de 1500 bytes por segundo. Entonces llegó Fast Ethernet, a 100 Mbps, pero el tamaño del paquete sigue siendo el mismo, de forma que se pueda interconectar a una Ethernet de 10 Mbps sin problemas de compatibilidad. Fast Ethernet necesita 8300 paquetes por segundo para llenar el canal. Gigabit Ethernet necesita 83000 y 10 Gigabit Ethernet casi un millón de paquetes por segundo. Por cada estándar más rápido de Ethernet los proveedores de conmutadores necesitan más paradas para procesar ese número cada vez más indignante de paquetes por segundo, ejecutando las CAMs que almacenan las tablas de reenvío a velocidades de locura y consumiendo enormes cantidades de energía. La necesidad de conectar las tarjetas antiguas NE2000 significa atarse a 1500 bytes para Fast Ethernet, y entonces la necesidad comunicarse con esas "rústicas" tarjetas Fast Eternet implican atarse también a 1500 bytes para Gigabit Ethernet, y así sucesivamente, ad nauseum ad infinitum. En cada punto el siguiente paso tiene sentido, pero todo el viaje decididamente menos.

3. La cintura del reloj de arena

Pero espere un minuto… ¿Las tecnologías de Internet no se encuentran en un cambio constante? Pasamos de una Ethernet a 10 Mbps hasta una de 10 Gbps, de alámbrico a inalámbrico, de una Web que apenas era capaz de mostrar texto parpadeante a una con capacidad de ejecutar todo tipo de aplicaciones. Incluso creamos el DNS y el control de congestión en TCP sólo a finales de los 80. La razón por la que fueron capaces de cambiar todas estas tecnologías, se debe a que se produzcan por encima o por debajo del Protocolo de Internet en la capa de red. Los protocolos de red se construyen como "pilas" donde un número de capas proporcionan una parte de la funcionalidad requerida. El famoso modelo de referencia OSI tiene siete capas, pero la pila TCP/IP sólo tiene cuatro. El nivel de enlace (de datos) sabe cómo enviar los paquetes a través de cables o del aire. La capa de red sabe cómo encaminar y direccionar, permitiendo a los paquetes encontrar su camino a través de la red. La capa de transporte consigue que las comunicaciones multi-paquete funcionen y finalmente la capa de aplicación hace que las aplicaciones funcionen en red. Esas capas se corresponden con los niveles OSI 2, 3, 4 y 7 respectivamente. Cada una de esas capas tiene muchos protocolos diferentes para elegir, con excepción de la capa de red, que sólo tiene IP. Esto es lo que asemeja el modelo a la cintura de un reloj de arena.

Ethernet opera en la capa de enlace de datos (y también en la capa 1 del modelo OSI, la capa física) y soporta redes complejas en sí misma, sin embargo las redes Ethernet están limitadas en tamaño y alcance, y pueden ser actualizadas con relativa facilidad. Cada red de enlace de datos es únicamente un salto en encaminamiento IP, por lo que sólo los dos

routers frontera tienen la necesidad de ser compatibles con la tecnología de enlace de datos en cuestión; toda la información del enlace de datos es eliminada en cada salto IP. La capa de transporte, con sus miembros principalmente conocidos TCP y UDP, tiene algunos problemas de capacidad de actualización en sí mismo, pero en principio los routers no miran más allá de la capa de red, por lo que no importa si un paquete es TCP, UDP o algún otro *P. Así pues, cambiar a un nuevo protocolo de transporte implica únicamente la actualización de los sistemas terminales que envían y reciben los paquetes, los routers intermedios no importan (los Firewalls lo hacen, por tanto hay más complicaciones en la práctica). Lo mismo ocurre para protocolos de aplicación como HTTP (web), FTP (transferencia de archivos) o SMTP (correo). Si su navegador decide iniciar la descarga de páginas web a través de FTP, esto es, entre el navegador y el servidor remoto, el resto de la red no importa. Pero IP está en todas partes. El origen del paquete necesita crear un paquete IP válido, paquete que será necesario procesar por todos los routers del camino a fin de enviarlo por la ruta correcta, y el destino debe ser capaz de decodificar dicho paquete IP. Así que cambiar el Protocolo de Internet significa cambiar todos los hosts y routers.

4. IPng: ¡necesitamos algo más grande, algo mejor!

Al principio de los años 90, se hizo evidente que las direcciones de 32-bit en el actual Protocolo de Internet (IPv4) eran demasiado pequeñas para permitir el crecimiento continuo de Internet más allá de los primeros años del siglo 21. 4,3 billones de direcciones posibles (con 3,7 billones realmente útiles), no dan para mucho en un mundo con 6, 7 o incluso 10 billones de personas. Así que la IETF decidió adoptar el protocolo OSI/ITU-T para reemplazar IP, es decir, CLNP (Connectionless Network Protocol) [6]. El protocolo de red no orientado a conexión es básicamente IP desde un universo paralelo donde todo tiene un nombre distinto, tal como NSAP (Network Service Access Point) o punto de acceso de servicio de red para el término “dirección”. Los NSAPs tienen una longitud variable con un máximo de 160 bits, lo cual sería una buena mejora sobre las existentes direcciones IP de 32-bits.

Pero la IETF, sufriendo un grave caso del síndrome “no-inventado-aquí” [7], no lo aceptó. Así que alrededor de 1995, el esfuerzo por un IP de próxima generación dio lugar a una nueva versión del protocolo IP para arreglar el problema de la limitación de longitud en las direcciones. El IETF aprovechó esta oportunidad para arreglar algunas limitaciones del

existente IPv4 pero con moderación: las quejas sobre el nuevo protocolo IPv6 están equilibradas entre "han cambiado demasiado" y "no han arreglado lo suficiente". Como resultado, la forma en la que IPv6 (no pregunten qué pasó con la versión 5 [8]) interactúa con Ethernet o con otras capas más bajas es bastante diferente a como lo hace IPv4, DHCP ha sido revisado de forma significativa, y existe una autoconfiguración sin estado para configurar las nuevas direcciones de 128-bits. Pero aparte de eso, IPv6 es todavía IP, lo que haría sencillo el proceso de transición de IPv4 a IPv6.

5. Todo esto ya había pasado antes

Curiosamente, la Internet ya vivió una transición de un protocolo a otro. En la década de 1970, ARPANET utilizaba NCP (Network Control Program). NCP estaba lleno de pintorescas nociones tales como la habilidad de contactar con un IMP remoto (router) y averiguar cuando un mensaje anterior había sido recibido en el otro extremo o no. Un poco como cuando se envía una carta a un amigo y se le pregunta al servicio de mensajería si una carta enviada anteriormente llegó o no. Estas y otras complejidades eran difíciles de manejar en redes lentas, y más aún en las redes rápidas, por lo que un nuevo y brillante protocolo fue desarrollado alrededor de 1980: IP/TCP (hoy en día decimos TCP/IP. O bien IPv4, o sólo IP, asumiendo la parte TCP implícita). La RFC 801 [9] explica cómo hacer la transición de NCP a TCP/IP. Básicamente, los dos protocolos podrían coexistir durante 1982, y el 1 de enero de 1983, NCP se extinguiría y sólo quedaría TCP/IP. Así pues, necesitaban un año para la transición de una red con cerca de un centenar de nodos y tres aplicaciones principales (telnet, FTP y correo electrónico). Por lo tanto difícilmente puede ser una sorpresa que haciendo lo mismo (la transición del "pronto-a-ser-obsoleto" IPv4 al nuevo IPv6) menos de dos décadas después para una red con cientos de millones de nodos y cientos si no miles de tipos de aplicaciones, podría llevar un largo tiempo. La única gracia salvadora es que el IETF comenzó con el esfuerzo de su IP de próxima generación (IPng), que finalmente produjo IPv6, muy temprano, dándonos cerca de 20 años entre el momento en el que IPv6 fue estandarizado (1995) y el momento en el que las direcciones IPv4 se agoten (probablemente en el 2012). Las malas noticias son que esos 20 años casi han concluido.

6. Barcos en la noche y la pista de carreras

Aunque para los usuarios y las aplicaciones, IPv4 e IPv6 sean muy parecidas, "en el cable", los protocolos son completamente distintos y no interactúan. En encaminamiento, llamamos esto un enfoque de "barcos en la noche". La ventaja de este diseño es que no hay necesidad de cambiar la infraestructura existente IPv4 (IPv6 es añadido simplemente como un nuevo protocolo). Todas las limitaciones y fallos que son parte de IPv4 quedan atrás. El problema con este enfoque es que la primera persona que quiere desconectar IPv4 tiene que esperar a la última persona que añada IPv6. Es como tener una red de telefonía móvil que no estuviera conectada a la telefonía fija. Todo el mundo tiene que tener ambos tipos de teléfono, con la expectativa de que en un futuro lejano, podamos desconectar las líneas fijas y usar únicamente teléfonos móviles. Y con los teléfonos móviles existe una ventaja real para el cambio: no hay cable (aunque las líneas fijas también presentan algunas ventajas). Con IPv6 no existen ventajas reales para hacer que muchos de los usuarios decidan cambiar ya que muchos usuarios no tienden a ser impresionados por la elegancia tecnológica y la argumentación futura.

Esto hace que la transición de IPv6 sea como la estrategia trackstand [10] en ciclismo en pista, donde los competidores tratan de hacer que sus oponentes tomen la iniciativa. Una vez que el oponente está en cabeza, el "ganador" del trackstand puede tomar ventaja del rebufo y mantenerse con un esfuerzo menor. Tras una década haciendo trackstand, la migración hacia IPv6 está finalmente poniéndose en marcha, pero por desgracia demasiado tarde para evitar los problemas que vengan cuando se agoten las direcciones IPv4. Pero vamos a volver a eso. En primer lugar, vamos a echar un vistazo a algunas de las diferencias entre IPv4 e IPv6 que se interponen en el proceso de una transición fácil.

7. ¿Quieres decir que IPv6 en realidad es diferente a IPv4?

Cuando IPv6 se desarrolló hacia la mitad de la década de 1990, las cosas que damos por sentado hoy en día no existían o no se utilizaban tan ampliamente. Por ejemplo, hoy en día casi todos los sistemas que no son routers o servidores dedicados obtienen su dirección IP y otro montón de información a través de DHCP (Dynamic Host Configuration Protocol).

DHCP es muy complejo y propenso a errores en comparación a cómo otros protocolos de la década de 1980, tales como IPX y AppleTalk, resolvían estos problemas. Con DHCP, el cliente envía una petición. Con suerte, uno o más servidores verán la petición de dirección y enviarán un ofrecimiento de dirección IP. El cliente entonces evalúa las ofertas y elije una. El servidor elegido debe ahora recordar no dar la misma dirección a otro sistema hasta que pase el tiempo de concesión, y el cliente debe recordar renovar la concesión de la dirección con el servidor antes de que se agote el tiempo. Con IPX esto resultaba mucho más sencillo, sin dependencia de información almacenada en el servidor o de temporizadores: los routers propagan una "dirección de red" y cada sistema crea su propia dirección individual combinando la dirección red anunciada y la dirección MAC grabada en su chip Ethernet. AppleTalk es bastante parecido, pero las direcciones son más cortas, así que AppleTalk utiliza un número aleatorio en vez de una dirección MAC. Igualmente envía unos pocos paquetes para determinar si algún otro sistema ya ha elegido la dirección. Muy sencillo.

Así que cuando se creó IPv6, el IETF miró protocolos como IPX y AppleTalk y desarrollo una configuración automática sin estado, la cual es básicamente un enfoque IPX. Posteriormente, motivos de privacidad hicieron que se descartara la opción de adjuntar la dirección MAC de una máquina en su dirección IPv6, así que se añadió una opción similar a la de AppleTalk: seguir utilizando la dirección MAC, sustituirla por un número aleatorio, aclarar y repetir cada 24 horas para mantener el gobierno y otros espías en estado de alerta. ¿Pero por qué limitarnos a dos mecanismos para configurar las direcciones IPv6 (tres si contamos la configuración manual)? Así se rediseñó DHCP como DHCPv6. A pesar de que ambos DHCPs comparten los mismos conceptos y arquitectura, sus formatos de mensaje y varios detalles operacionales son completamente diferentes: DHCP está tan íntimamente entrelazada con IPv4 que simplemente hacer los campos de dirección suficientemente largos como para soportar IPv6 fue casi imposible. Todos los sistemas IPv6 soportan autoconfiguración sin estado. Windows Vista y 7 soportan DHCPv6, pero Windows XP y Mac OS X no lo hacen. En los sistemas operativos de código libre, un cliente DHCPv6 puede ser instalado si no viene por defecto con la distribución. Vista y 7 también utilizan la dirección temporal generada por un número aleatorio por defecto. Otros sistemas operativos no lo hacen.

8. No es tan sencillo ser un administrador de sistemas

Llegado tan lejos en la historia, muchos administradores de sistemas comienzan a estar muy incómodos sobre la transición a IPv6: no pueden configurar un gran servidor DHCPv6 que monitorice todas las asignaciones de direcciones y terminar. En las redes que necesitan dar soporte a cosas distintas que un Windows Vista/7, es inviable cambiar a una autoconfiguración sin estado, porque entonces algunos sistemas simplemente no podrían obtener una dirección IPv6 con DHCPv6. Sin embargo, incluso si las correcciones que se han desarrollado se llevaran a cabo, algunos administradores de sistemas sostienen la necesidad de coordinar la información en DHCPv6 y esto resulta demasiado oneroso hacerlo en los anuncios de los routers, pues la gente de routing y la gente de servidores no deberían necesitar hablarse entre sí.

Hace diez años, esta diferencia entre IPv4 e IPv6 podría haberse recibido con una actitud de se-puede-hacer o quizá resignación, pero las peculiaridades de IPv4 están tan arraigadas y los recuerdos de un mundo multi-protocolo que existió durante las últimas décadas del siglo anterior se desvanecieron ante la falta de parecido entre IPv4 e IPv6, lo que podría ser hoy en día un verdadero obstáculo.

9. Configúralo y olvídate

Un problema mucho más fundamental en la migración a IPv6 es el problema de "configurar y olvidarse". Si una organización decide adoptar IPv6, es posible que tenga que actualizar hardware y software, el ISP debe proporcionar conectividad IPv6 y direcciones IPv6, y entonces el nuevo protocolo debe habilitarse en routers y en DNS [11]. Hasta aquí todo bien. A continuación, algunos pings y traceroutes IPv6 se llevan a cabo, y cuando todo funciona como debería todos vuelven a sus negocios como siempre. Debido a que hay demasiados participantes involucrados en el tema las redes, de vez en cuando se rompen cosas. Esto puede ser el resultado de un fallo hardware, cables rotos, actualizaciones de software, reconfiguraciones… lo que sea. A menudo, los ISPs y los departamentos de tecnologías de la información son muy proactivos a la hora de arreglar esos problemas, y si no lo son, los usuarios siempre son de ayuda para darse cuenta de lo costoso e inaceptable que resulta el corte. Por eso los problemas suelen ser solucionados con relativa rapidez. Para IPv4. Si algo falla en IPv6, nueve de cada diez veces nadie se da

cuenta: la mayor parte de la comunicación es sobre IPv4. Y si una sesión es iniciada sobre IPv6 pero falla, normalmente se pasa automáticamente a IPv4. Esto podría pasar tras un retardo significativo, o en una fracción de segundo. Si los usuarios se quejan, no es insólito que las cuestiones relacionadas con IPv6 tienen una prioridad muy baja. Por ejemplo, Mac OS X 10.6 Snow Leopard tiene un error grave en su código de DNS que hace ignorar IPv6 en el DNS cuando existe un recurso de tipo CNAME involucrado (lo cual no es infrecuente). Un año y cuatro actualizaciones más adelante, el error sigue ahí.

Una variante de este problema es cuando una nueva tecnología se implementa en software, pero no se ha desplegado todavía. Entonces, cuando se utiliza la nueva mejora, las cosas no funcionan tan bien, a menudo debido a que las primeras implementaciones son problemáticas. Un ejemplo distinto a IPv6 es el pipelining en HTTP. Cuando su navegador le dice "cargando 93 de 126" al ir a un sitio web, el protocolo original HTTP requiere una nueva sesión TCP por cada una de esas 126 transferencias. Esto introduce una gran sobrecarga. Así que en HTTP 1.1 es posible mantener una sesión TCP abierta, y volver a utilizarla para posteriores peticiones HTTP. Esto se conoce como pipelining. El pipelining se implementó de forma incorrecta en el servidor de Microsoft IIS 4, con el resultado de que cuando los navegadores empleaban esta característica, ocurrían cosas malas. Durante muchos años, los navegadores han tenido deshabilitado el pipelining por defecto.

Algo similar pasó con BitTorrent e IPv6. La operación básica de BitTorrent es conectarse a un "tracker" y decirle qué archivo se pretende descargar y qué puertos pueden emplear los demás para conectarse a ti. Entonces el tracker devuelve la dirección IP y los números de puerto de otros hosts que también están activos y descargando el mismo archivo. Los clientes de BitTorrent se conectan a las direcciones/puertos de sus "peers", los cuales les son asignados por el tracker. Llegados a este punto, los peers intercambian partes del archivo en cuestión directamente entre ellos. La especificación original del protocolo BitTorrent permitía el uso de direcciones IPv4 o IPv6 al igual que nombres de dominio como referencias desde el tracker a los clientes/peers. Pero la mayoría de la gente no tiene un nombre de dominio fijo en casa y no hubo suficientes trackers con capacidad IPv6 en los primeros días de BitTorrent, sólo direcciones IPv4 fueron utilizadas, y tras un buen tiempo, el protocolo BitTorrent fue modificado con capacidad de intercambiar las direcciones IPv4 en formato binario entre peers, quitando un montón de sobrecarga al proceso. Por supuesto rompiendo la compatibilidad con IPv6. Entonces, el tracker de BitTorrent más grande (bueno, sin duda el más visible), dirigido por The Pirate Bay, obtuvo una dirección IPv6. Para evitar problemas con los protocolos BitTorrent actualizados, The Pirate Bay decidió tener clientes BitTorrent conectados al tracker por duplicado: sobre IPv4 para recibir la dirección de los peers IPv4, y sobre IPv6 para recibir las direcciones de los peers IPv6. Eso funciona bien si el cliente lo soporta, pero no tanto

para los clientes existentes con capacidad silenciosa IPv6 (lo cual fue común, ya que muchos de ellos se escribieron en lenguajes de alto nivel en los que no importan las diferencias entre IPv4 e IPv6). Estos clientes sólo verían los peers IPv6, si acaso.

10. Listas blancas en DNS

Y como ejemplo del problema "no se puede llegar desde aquí" es el ocurrido con los hosts que creen tener IPv6, pero en realidad no funciona (hace algunos años Google determinó que esos hosts son más del 25 por ciento de los hosts que tienen IPv6). A pesar de que sabemos cómo ejecutar IPv4 y sabemos cómo ejecutar IPv6, nos encontramos en un mundo donde ambos protocolos coexisten lado a lado, e interactúan de formas inesperadas. Hosts que creen tener conectividad IPv6 intentarán conectarse a servidores con dirección IPv6 en los DNS sobre IPv6. Pero si la conectividad IPv6 no funciona, nada ocurre durante un tiempo hasta que la vence un temporizador en la aplicación y reintenta con otra dirección proporcionada por el DNS. Si esto es una dirección IPv4, la conexión irá adelante y todo funcionará, pero tras una molesta espera. Estos retardos o esperas le cuestan a entidades como Google un montón de dinero, así que Google optó por renunciar a poner las direcciones IPv6 de sus servidores en el DNS. Estas direcciones IPv6 sólo están expuestas a los servidores DNS de los ISPs que participan en el programa de Google sobre IPv6. Por lo tanto sabemos a dónde queremos llegar: una red totalmente habilitada con IPv6. Pero para lograrlo hay que sufrir tiempos de espera, los cuales generan llamadas al soporte técnico y la pérdida de ingresos, o el uso de capas adicionales de esfuerzo y complejidad.

11. Los últimos días de IPv4 con NAT

Mientras tanto, el 99 por ciento de Internet utiliza solamente IPv4. Simplemente no hay manera de que todo funcione con IPv6 antes de que nos quedemos sin direcciones IPv4 en dos o quizá tres años. Así pues, necesitamos dar a IPv4 algún tipo de soporte vital. En realidad, para aquellos de nosotros que tenemos direcciones IPv4 hoy en día, realmente no hay mucho problema a corto plazo. Sólo es que no habrá más direcciones para nuevos usuarios dentro de unos años. Pero, obviamente, sólo atender a los usuarios existentes, sin ninguna oportunidad de crecimiento no va a funcionar en Wall Street. La solución: hacer que los usuarios compartan una misma dirección IPv4. La gente ya hace esto en sus casas

utilizando NAT (Network Address Translation). Esto hace que sea posible que un edificio entero de viviendas salga a Internet con una única dirección IP. Pero ese nivel de frugalidad no será suficiente: pronto, los ISPs se ocuparán de hacer NAT de forma que muchos clientes compartan una única dirección IPv4.

Arquitectónicamente, NAT es una cosa mala. Rompe todo tipo de supuestos relacionados con los protocolos, pudiendo interponerse en la forma en la que las aplicaciones hacen su trabajo. Esto es especialmente cierto para las aplicaciones peer-to-peer como BitTorrent, pero también para VoIP (incluyendo Skype). Sin embargo, a lo largo de los años los creadores de aplicaciones han descubierto una forma de convivir con los NATs. Una forma de hacer esto es hablar con el router local que esté empleando NAT y pedirle que redirija las conexiones entrantes utilizando un protocolo de mapeo de puertos. Esto funciona bien cuando se utiliza NAT en casa, pero no demasiado bien cuando el ISP utiliza un gran NAT. No sólo diferentes tipos de usuario compiten por los mejores números de puerto, sino también los protocolos de mapeo de puertos utilizados frecuentemente (UPnP IGD y NAT-PMP), los cuales no pueden hablar con un NAT a varios saltos de distancia. Y hacer que las aplicaciones peer-to-peer funcionen o no es de alta prioridad para los ISPs –los cuales tienden a distribuir contenidos de vídeo y/o a dedicarse al negocio de las llamadas de voz. Peor aún, el NAT proporcionado por el ISP podría acabar con el mecanismo de tunneling de IPv6 que permite a la gente obtener conectividad IPv6 si su ISP no se lo proporciona. Y la implementación de esos complejos y costosos equipos NAT puede quitar los recursos que de otra forma serían utilizados para llevar a cabo un despliegue de IPv6 en la red.

12. NAT en IPv6

Mientras tanto, hay acaloradas discusiones en el interior del IETF sobre la posibilidad de especificar el temido NAT IPv6 después de todo. El argumento en contra es el disgusto arquitectónico –el IETF también aprobó en principio la creación de un NAT IPv4- pero el argumento a favor es que un NAT IPv6 con buen comportamiento no sería tan malo como un NAT IPv4 recompilado para direcciones de 128-bits. Lo que crea la mayor parte de los problemas con NAT es la compartición de direcciones. Con NAT IPv6, podría ser posible crear asignaciones de direcciones 1-a-1 en vez de las 1-a-muchos utilizadas con NAT IPv4, por lo que todavía sería posible ocultar la red interna que utiliza direcciones privadas, pero las aplicaciones peer-to-peer –si se permite a través de un cortafuegos- podrían trabajar con un poco de lógica adicional. La falta de NAT IPv6 también es citada como un obstáculo en el despliegue de IPv6, ya que es otro aspecto que diferencia IPv4 e IPv6. El NAT de IPv6, diferente al NAT IPv4 no sería de gran ayuda en este ámbito. Entonces de

nuevo, la única cosa que realmente parece, huele y sabe como auténtico IPv4 es… IPv4. En algún momento, IPv6 tiene que ser un protocolo por sí mismo.

13. Plan B

No hay plan B. A pesar de la larga lista de problemas con IPv6 y/o su implementación, no hay alternativas. Nos ha llevado la mejor parte de dos décadas llegar hasta aquí con IPv6 – no hay manera de que lleguemos a implementar y desplegar una alternativa antes de que la falta de direcciones IPv4 sea un problema serio. La compartición de direcciones utilizando NAT y alguna otra forma de redistribución de direcciones (remunerado o no) permitirá a IPv4 seguir operando sin muchos problemas durante un par de años después del agotamiento de direcciones. Sin embargo, actualmente estamos poniendo en uso cada año unas 200 millones de direcciones nuevas. Eso conlleva unas reglas muy pesadas sobre quién puede obtener las direcciones y el despliegue intensivo de NATs. Al contrario que los Estados Unidos, los países de Europa septentrional y occidental, que no recibieron grandes cantidades de espacio de direcciones IPv4 cuando había muchas en la década de 1980, todavía usan más de una dirección IPv4 por habitante y todavía están creciendo un poco. Incluso los Estados Unidos – con 1.5 billones de direcciones IPv4 – están utilizando cada vez más direcciones IPv4 nuevas cada año.

No importa cómo se reparta el espacio de direcciones IPv4, no va a sostener una red global en el futuro donde países como China y Brasil están avanzando rápidamente mientras que muchos países en el mundo desarrollado no tienen nada parecido a un reparto equitativo todavía. Así que, aunque todavía estamos tratando de entender la pregunta, la respuesta tendrá que ser “IPv6”. Algunas de las deficiencias reales y detectadas de IPv6 están siendo abordadas por el IETF y otros lugares. A pesar de que hay muy poco despliegue de IPv6 hoy en día, ya existe un problema heredado: algunas implementaciones iniciales de IPv6 no tienen soporte para DHCPv6, por ejemplo. Pero la mayor parte de sistemas habilitados para IPv6 todavía están recibiendo actualizaciones (semi)automáticas de software, así que los problemas heredados no deberían ser insuperables en esta ocasión. Vamos a tener que movernos a través de un periodo en el que IPv4 va de bueno a peor debido al aumento de capas de NAT, mientras que IPv6 todavía se encuentra en una fase torpe y carente de funcionalidades secundarias o de la sencilla compatibilidad a la que nos hemos acostumbra do con IPv4. Y quizá algunos sistemas acaben siendo sólo IPv4 mientras otros sean sólo IPv6. A pesar de que la transición no va a ser tan fácil como esperábamos, vamos a terminar con una Internet más fuerte y estable, con un potencial casi infinito para el crecimiento después de la transición. Justo mientras nos aseguramos de que hay una forma de llegar desde aquí.

14. Referencias

[1] http://ftp.isc.org/www/survey/reports/1995/01/report.html

[2] http://ftp.isc.org/www/survey/reports/2010/07/

[3] http://blogs.apress.com/?p=1328

[4] http://www.joelonsoftware.com/articles/fog0000000069.html

[5] http://www.ajc.com/business/25-years-since-coca-484445.html

[6] http://www.itu.int/rec/T-REC-X.233/en/

[7] http://www.joelonsoftware.com/articles/fog0000000007.html

[8] http://www.iana.org/assignments/version-numbers/version-numbers.xhtml

[9] http://tools.ietf.org/rfcmarkup?rfc=801

[10] http://www.youtube.com/watch?v=Q0O8ZzFuMkQ

[11] http://www.apress.com/book/downloadfile/2446

[12] http://ars-technica.com/hardware/news/2007/05/ipv6-firewall-mixed-blessing.ars/2