IPv6 para Gobiernos y Empresas:
Impacto e Implementación en 12 Pasos (Parte 1)

Autor: Jordi Palet Martínez (@jordipalet)

En un artículo anterior (http://www.lacnic.net/innovaportal/file/2943/1/12-pasos-para-activar-ipv6-en-la-red-de-un-isp-es.pdf) estudiamos los 12 pasos de desplegar IPv6 en una red de un proveedor de Internet. En esta ocasión, nos centraremos en redes corporativas, que incluyen casos de gobiernos, empresas y organizaciones en general.

Recientemente, trabajando con un nuevo cliente -un Gobierno de la región de LACNIC-, me encontré con una solución de despliegue de IPv4 que era peculiar y que planteaba ciertas dificultades para el despliegue de IPv6.

Se trata de la red de un Ministerio y, según he averiguado posteriormente, es un mecanismo ampliamente utilizado en prácticamente todas las organizaciones gubernamentales, no sólo de ese país, sino de gran parte de la región e incluso en otros países del mundo.

Se trata de una dependencia exagerada de NAT y balanceo de carga (Load Balancing), que sustituye el uso de BGP, que sería lo correcto. Para el funcionamiento de este mecanismo, los DNS autoritativos se alojan en el proveedor con TTLs (tiempos de vida) extremadamente bajos, lo que permite que al detectar la caída de un enlace los balanceadores alteren registros tipo CNAME (y otros).

La consecuencia técnica inmediata y negativa, es que el sistema de cache global es "invisible" para esa red y como resultado, se incrementan las consultas DNS, se genera tráfico innecesario y costoso para todos los agentes de Internet (no sólo para esa organización), y por supuesto, se ralentiza el acceso a esa organización.

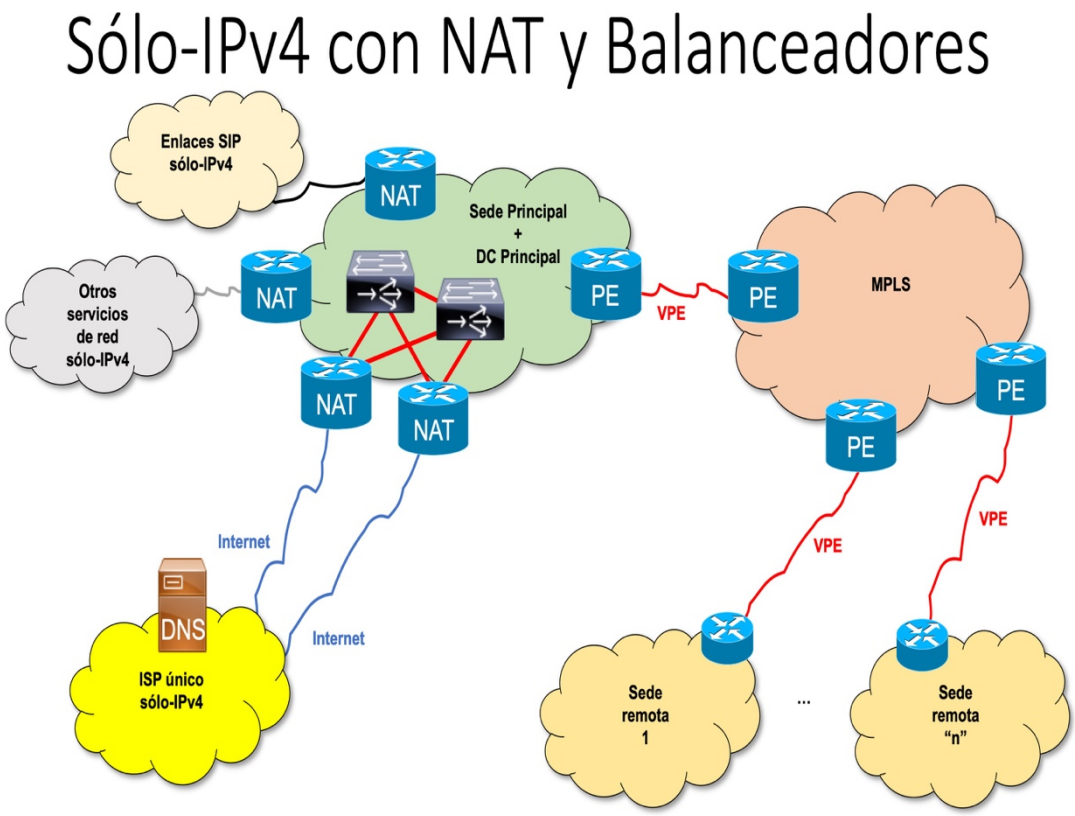

Diagrama de la red antes del despliegue de IPv6

Este mecanismo considerado como una mala práctica, es tan sólo un ejemplo de como resolver un problema que no existe: evitar disponer de BGP.

Asumo que es muy probable que haya muchos fabricantes y operadores de redes, en todo el mundo, que estén vendiendo estas soluciones para organizaciones y empresas de todos los tamaños como algo positivo y como buena práctica. Ello trae otra consecuencia negativa, en este caso no técnica, que es la dependencia de un único operador (aunque pueda ofrecer a esa red múltiples conexiones por caminos que pueden ser divergentes, posiblemente sólo de forma parcial). Todo esto impacta de forma negativa en el coste para los clientes, e incluso respecto de la calidad del servicio y los tiempos de respuesta ante cualquier cambio requerido en la red (por ejemplo, modificaciones en los DNS autoritativos).

Con el uso de NAT y las direcciones privadas en IPv4, y por ende en este tipo de soluciones, se podría considerar como ventaja que cuando se cambia de proveedor, no sea necesario renumerar toda la red de usuarios de la misma. Si es preciso, en cualquier caso, cambiar todas las reglas de firewalls, proxy-reverso y similares, que son necesarias para permitir el acceso desde el exterior de la red a recursos internos que se desea publicar en Internet (aplicaciones, webs, etc.).

Sin embargo, estas soluciones basadas en NAT no son válidas para IPv6 y su uso sería un grave error, y en ese caso ¿que sentido tiene la transición a IPv6 si reproducimos algunos de los problemas que genera NAT?

NAT resuelve exclusivamente el problema de la falta de direcciones IPv4, pero no es una solución para proporcionar seguridad, como a menudo se cree. IPv6 no tiene el problema de la falta de direcciones y, por lo tanto, no requiere NAT. De hecho, el IETF no ha estandarizado NAT para IPv6, ni el mismo concepto de direcciones privadas que en IPv4.

Se podría considerar que las ULAs (Unique Local Address) y NPT (Network Prefix Translation), son lo equivalente. Pero no es así, hasta el punto que NPT es un protocolo experimental y, por lo tanto, sólo debe ser usado en entornos de prueba, ya que no se puede garantizar la interoperabilidad del mismo y por tanto los efectos adversos que puede generar en la red. Es importante recalcar que, a menudo, se confunde NAT y el hecho de no tener direcciones públicas para todos los dispositivos, con un mecanismo de seguridad. Sin embargo, el hecho de que en IPv6 haya suficientes direcciones globales (equivalentes a las públicas en IPv4), para todos los dispositivos, no es una debilidad, sino más bien al contrario, pues nos obliga a recordar que en cualquier red, siempre debe haber un firewall en cada nodo (el 80% de los ataques de seguridad provienen del interior de las propias redes), y un firewall perimetral, y que ambos deben estar configurado para proteger a la red y a cada dispositivo, tanto del tráfico IPv4 como del tráfico IPv6 que no sea admisible.

Existen varios intentos para buscar soluciones alternativas al BGP para multihoming corporativo, como el descrito en el RFC8475 (“Using Conditional Router Advertisements for Enterprise Multihoming”). Por ahora, esta solución no ha sido implementada por ningún fabricante, y para que funcione correctamente debería de estar soportado por todos y cada uno de los equipos de la infraestructura de la red y tendría un impacto en los TTLs de DNS. Es más, el propio documento indica que sólo es útil para redes sencillas (posiblemente redes pequeñas que sólo tengan clientes, no servidores) y sin preservar las conexiones existentes.

Por lo tanto, sería poco acertado que, como profesionales, recomendemos soluciones como NPT, NAT66 (que no existe como estándar, pero se puede implementar en Linux, no en otras plataformas) o incluso soluciones de multihoming que no están implementadas por todos los fabricantes, sólo aplican a pequeñas redes y que tienen grandes contraindicaciones.

¿Cómo resolvemos esta situación? ¿Cómo evitamos que si una red cambia de proveedor tenga que renumerarse? Sencillo: con buenas prácticas basadas en el uso de BGP, y direccionamiento propio, lo que comúnmente se denomina “direccionamiento de usuario final” o “Independiente del Proveedor” (PI o Provider Independent).

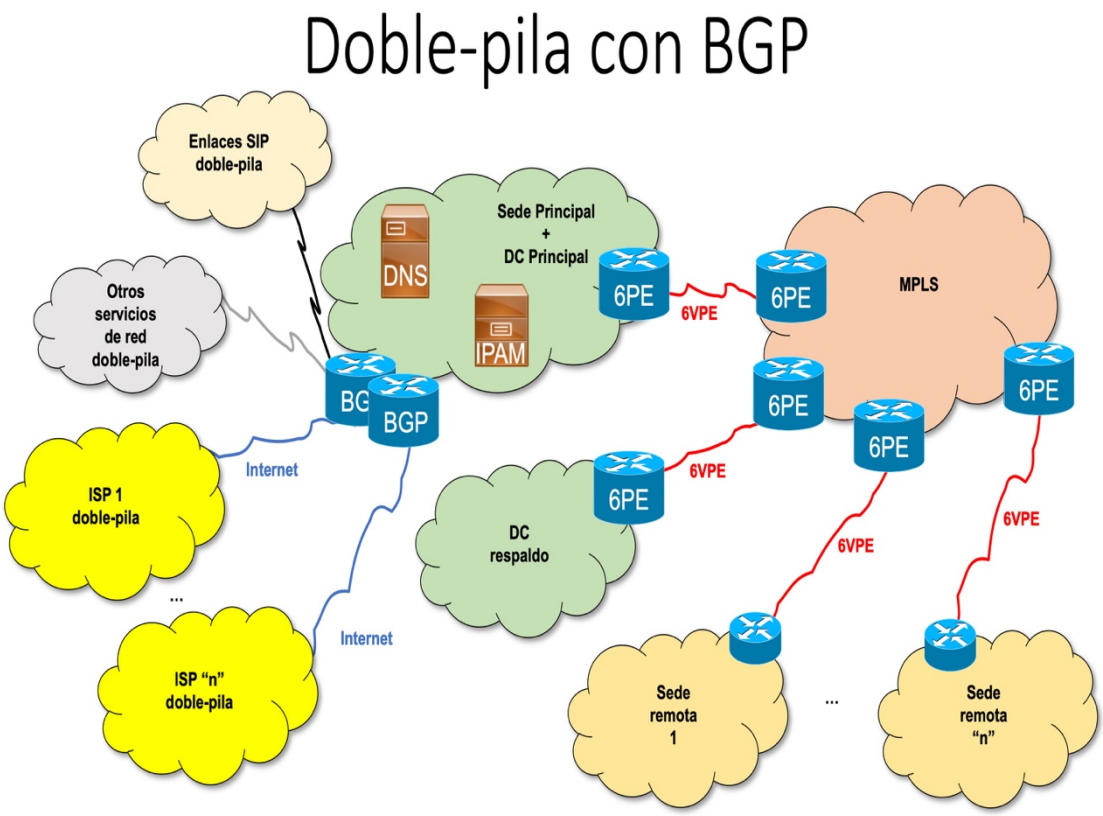

Diagrama de la red después del despliegue de IPv6

Todos los RIRs tienen políticas que permiten que una organización pueda recibir tanto su propio número de Sistema Autónomo (ASN), como las direcciones IPv4 e IPv6 que requiera.

Es cierto que para el caso de IPv4 seguiremos dependiendo de NAT, por la única razón que no hay direcciones suficientes. Sin embargo, si una organización requiere un determinado número de direcciones IPv4 públicas, y hasta ahora no las tenía del RIR correspondiente, mientras sigan quedando algunas en dicho RIR, podrá solicitar hasta un máximo de 1.024 (/22).

En el caso de IPv6, lo lógico es solicitar tantos /48 como "sedes" (sitios) tenga dicha organización. Así, si una organización tiene una única sede, bastará con un /48; pero si tiene 13 sedes, en ubicaciones con conexiones distintas, deberá solicitar a su RIR un /44, que es el prefijo inmediatamente superior a la necesidad de esta red (contiene 16 x /48).

Si la organización es más grande, o en su infraestructura incluye redes o dispositivos de otras organizaciones (por ejemplo, un ministerio gestiona una red que conecta diferentes ministerios, municipalidades, sedes de policía, escuelas, centros de salud, etc.), en lugar de utilizar la política de usuario final, deberá solicitar al RIR correspondiente direccionamiento de LIR/ISP, dado que en este caso se comporta como un "ISP" para otras organizaciones. Aunque en el caso de IPv4, no podrá recibir más espacio, sino como máximo un único /22, en el caso de IPv6 puede recibir un /32

(que contiene 65.536 x /48) o justificar la necesidad de un espacio mucho mayor. A modo de ejemplo, en Europa se han realizado asignaciones para gobiernos en torno al /24-/26.

Inicialmente las políticas de los RIRs no contemplaban los casos de redes de gobiernos (pues no eran comunes en el caso de IPv4), pero hace años, por el consenso de la comunidad, se han adaptado para cubrir esta necesidad.

En el caso del gobierno mencionado al inicio, el uso apropiado de estás políticas permitiría, por ejemplo, crear una red de gobierno en la que se interconectan entidades (generalmente las pequeñas y medianas), con direccionamiento proporcionado por la organización del gobierno que gestiona dicha red, y entidades más grandes (o las más avanzadas en el despliegue de IPv6), con direccionamiento de "usuario final". Esa red de gobierno permite, a primera vista, el ahorro de unos 300 millones de dólares (USD), solamente conectando 1.800 municipalidades. Este proyecto ofrece, además, entre otras muchas ventajas, dos centros de datos (principal y respaldo), configurados en alta disponibilidad para servicios centralizados, como seguridad de la red, transición, servidores virtualizados, y mesa de ayuda para atender todas las incidencias de dichos municipios.

Es evidente que cuando se piensa en conectar a través de esa red también a centros de salud y hospitales, escuelas, cuarteles del ejército, oficinas de policía, juzgados, sólo por citar algunos de los ejemplos más relevantes, el ahorro se multiplica y da como resultado cantidades muy relevantes para cualquier país.

Obviamente, lo dicho hasta ahora es sólo una pequeña parte, dado que el proyecto de despliegue de IPv6 en una red debe ir acompañado de un estudio detallado, para lo cual es necesario analizar las capacidades respecto de IPv6 tanto de los dispositivos de la propia infraestructura de la red, como de los clientes que a ella se conectan y especialmente de las aplicaciones, que suele ser el mayor de los problemas. No hay que olvidar los servicios que existan en la red, como pueden ser bases de datos, servidores web, servicios de correo electrónico/mensajería, servicios de voz/multimedia, etc.

IPv6 es mucho más sencillo que IPv4. Sin embargo, antes es imprescindible "desaprender IPv4" para poder realizar esa auditoría de la red, o caeremos en muchos errores, ya que el despliegue de IPv6 puede requerir cambios importantes en nuestra infraestructura, básicamente un importante replanteo de la misma en muchos aspectos. Por eso es fundamental una capacitación por parte de profesionales que tengan experiencia en este tipo de redes, y que nos garantice todos los conocimientos y recursos necesarios.

Asimismo, una vez comprendida la red, es necesario realizar un plan de direccionamiento detallado, que es además imprescindible para poder solicitar los recursos de Internet adecuados a nuestro caso, al RIR correspondiente. Estos recursos, en IPv6 son cantidades astronómicas de direcciones, y ya no podrán ser gestionadas

con una hoja de cálculo o documento de texto, sino que requeriremos un gestor de direcciones (IPAM, IP Address Management).

Finalmente, el estudio de la red y de las aplicaciones, así como el plan de direccionamiento, definirá las posibles alternativas para iniciar la transición de nuestra red a IPv6, y si necesitamos el apoyo de mecanismos de transición y en que partes de la red y para que servicios y aplicaciones.

En conclusión, para que la implementación de IPv6 sea un éxito en cualquier red corporativa es importante tener en cuenta los siguientes aspectos:

1. Capacitación
2. Proyecto de despliegue y pruebas de IPv6
3. DNS
4. BGP
5. Plan de direccionamiento
6. Recursos de Internet (ASN, direcciones IPv4 e IPv6)
7. Gestión de direcciones (IPAM)
8. Asignación y auditoria de direcciones
9. Dispositivos de la infraestructura de la red y clientes
10. Impacto en aplicaciones y servicios
11. Mecanismos de transición
12. Contratos con operadores y conexiones con otras organizaciones

A menudo se cae en el error de pensar que IPv6 sólo afecta a la conexión de la red con Internet. En otros casos se piensa que es lo contrario, que solo afecta a los usuarios internos. La globalidad de las redes, servicios y aplicaciones, implica que el despliegue de IPv6 afecta a ambos aspectos de la red, salvo en casos muy específicos (y que a menudo adolecen de pensar en el futuro próximo: “hoy esto no esta conectado, pasado mañana sí”), y es preciso estudiar el despliegue de IPv6 como un todo.

En la segunda parte de este artículo, visto ya el impacto del despliegue de IPv6, en redes de gobiernos, empresas y organizaciones, expondremos a grandes rasgos, los pasos necesarios para afrontar el proyecto de despliegue de IPv6.