IPv6 para Gobiernos y Empresas:
Impacto e Implementación en 12 Pasos (Parte 2)

Autor: Jordi Palet Martínez (@jordipalet)

En la primera parte de este artículo, analizamos el impacto del despliegue de IPv6 en redes corporativas, que incluyen gobiernos, empresas y organizaciones. En esta segunda parte se exponen, a modo de guía rápida, los pasos necesarios para afrontar el proyecto de despliegue de IPv6.

1. **Capacitación experimentada**

   El proyecto de despliegue de IPv6 en cualquier red, es un gran paso mirando hacia el futuro y no debemos correr riesgos. IPv6 no es lo mismo que IPv4. Es inconcebible planificar y ejecutar adecuadamente el proyecto sin haberse capacitado apropiadamente y no sólo de una forma teórica o virtual, sino con profesionales "on-site", con experiencia en este tipo de redes, y con profundos conocimientos técnicos, así como en estandarización, operación de redes, buenas prácticas y políticas.

   El coste de dicha capacitación es una pequeña inversión que sin duda redundará en ahorros y en la calidad del trabajo posterior, evitando caer en errores que pueden ser muy costosos y que pueden requerir repetir tareas. Por ejemplo, si se realizan inversiones en nuevo equipamiento que luego resultan ser inadecuadas, por haber "pensado en IPv6 como si fuera IPv4" y no haber tenido en cuenta muchos cambios muy relevantes.

2. **Desarrollo del proyecto de despliegue y pruebas de IPv6**

   Una vez realizada la capacitación, y cuando ya tenemos suficientes conocimientos de IPv6, se puede trabajar en el proyecto de despliegue. Este proyecto debe comenzar con una auditoría de la infraestructura actual y de los cambios previstos a futuro, en todos sus aspectos, desde los equipos de clientes, sistemas operativos, aplicaciones, servicios de red, servidores, equipamiento de seguridad y, por supuesto, todo el equipamiento que soporta la propia red (conmutadores, routers, WiFi, etc.).

   El proyecto de despliegue de IPv6 debe estudiar detenidamente todas las tareas, sus interrelaciones, cuellos de botella y soluciones de la organización. Además de confirmar que con cada paso que demos, realizamos las pruebas necesarias para confirmar que funciona como se espera y que no ha afectado adversamente al resto de la red, ni de sus usuarios internos ni externos, tanto si se conectan con sólo-IPv4, sólo-IPv6 o doble-pila. Es indispensable realizar pruebas desde diversos puntos de Internet, para confirmar que nuestra red no es sólo accesible desde nuestro entorno cercano, país o región, pues a menudo vemos casos de redes que no han hecho estas comprobaciones y no tienen una visibilidad global correcta.

Generalmente, este proyecto obligará a replantear muchos de los aspectos del diseño actual de la red. No en todos los casos será necesario hacer cambios, eso dependerá de cada red, pero debemos aprovechar el despliegue de IPv6 como una oportunidad, para asegurarnos que la red y las aplicaciones y servicios de la misma cumplen con los requisitos que IPv6 puede requerir y las ventajas que puede ofrecer en desarrollos futuros, como IoT (Internet de las Cosas).

Los siguientes pasos de esta guía han de formar parte integral del proyecto de despliegue de IPv6. Los enumeramos como pasos adicionales, para resaltar la importancia que cada uno de ellos tiene en dicho proyecto.

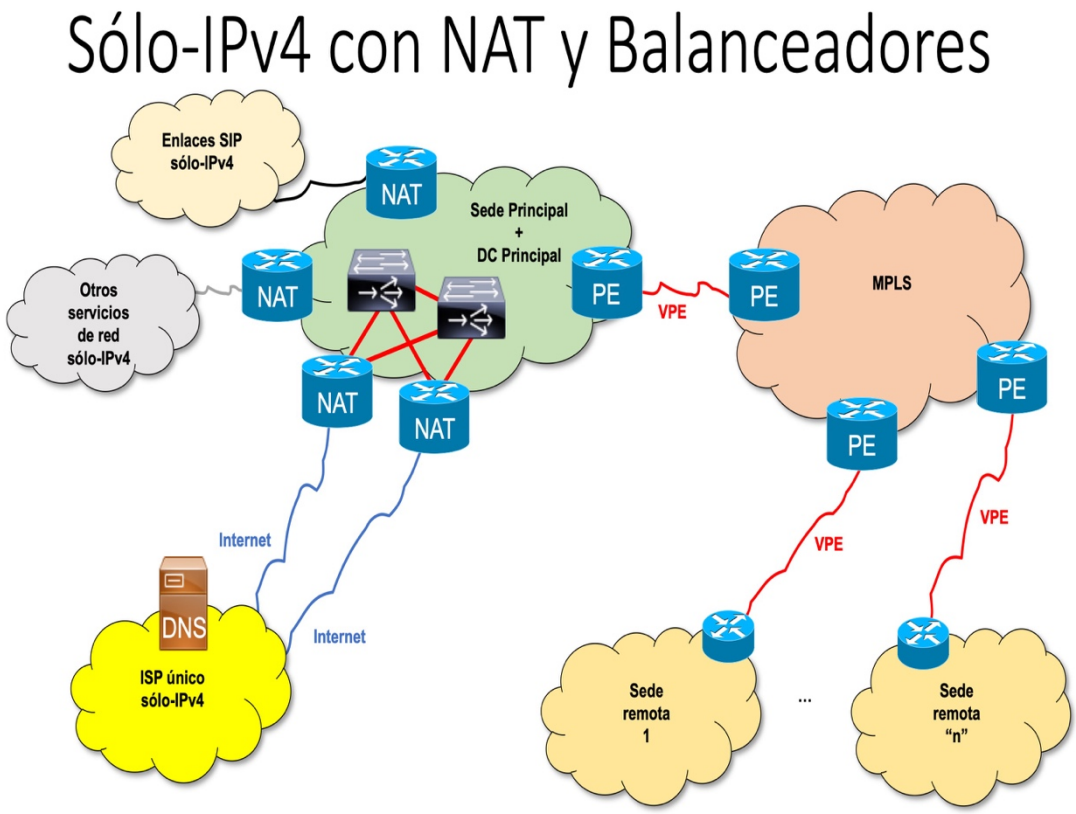

Diagrama de la red antes del despliegue de IPv6

3. DNS

Uno de los aspectos mas importantes para un adecuado despliegue de IPv6, es el control de las zonas autoritativas de DNS. La transición a IPv6 se basa muy especialmente en que el sistema operativo y/o las aplicaciones sean capaces de elegir adecuadamente si deben utilizar IPv4 o IPv6. Ello implica un uso intensivo de DNS para toda la red, a lo que no siempre estamos acostumbrados con IPv4.

Si no tenemos el control del DNS, o dependemos de terceras partes para hacer cambios, es muy complejo el despliegue y las pruebas, lo que puede generar grandes e innecesarios retrasos y dificultades en todo el proyecto.

4. BGP

Muchas redes corporativas actuales con IPv4 no disponen de BGP con sus proveedores de Internet, sino que dependen estrechamente de NAT, e incluso de otros mecanismos o soluciones, que son poco recomendables, pues tienen implicaciones negativas, y que en el caso de IPv4 pueden quedar ocultas.

Sin embargo, en el caso de IPv6 no existe NAT ni direcciones privadas. Por lo tanto, el uso de BGP no sólo es una buena práctica, sino que es imprescindible si queremos tener un direccionamiento independiente del proveedor y evitar así renumerar toda nuestra red cuando cambiemos de proveedor (como es habitual, cada "n" años,) en casos de contratos de entidades de gobierno, o por razones de competencia.

Imaginemos un ministerio con 5.000 funcionarios, cada uno con su propio computador, además de toda la infraestructura de la red, y otros 5.000 teléfonos de VoIP. ¿Es deseable o incluso aceptable, tener que renumerar toda esa infraestructura cada cuatro años? ¿Podemos imaginar el coste económico, el impacto en recursos humanos y el tiempo de desconexión con los ciudadanos para realizar dicho cambio? No menospreciemos el impacto aún cuando hablemos de sólo 500 o 1.000 dispositivos de usuario.

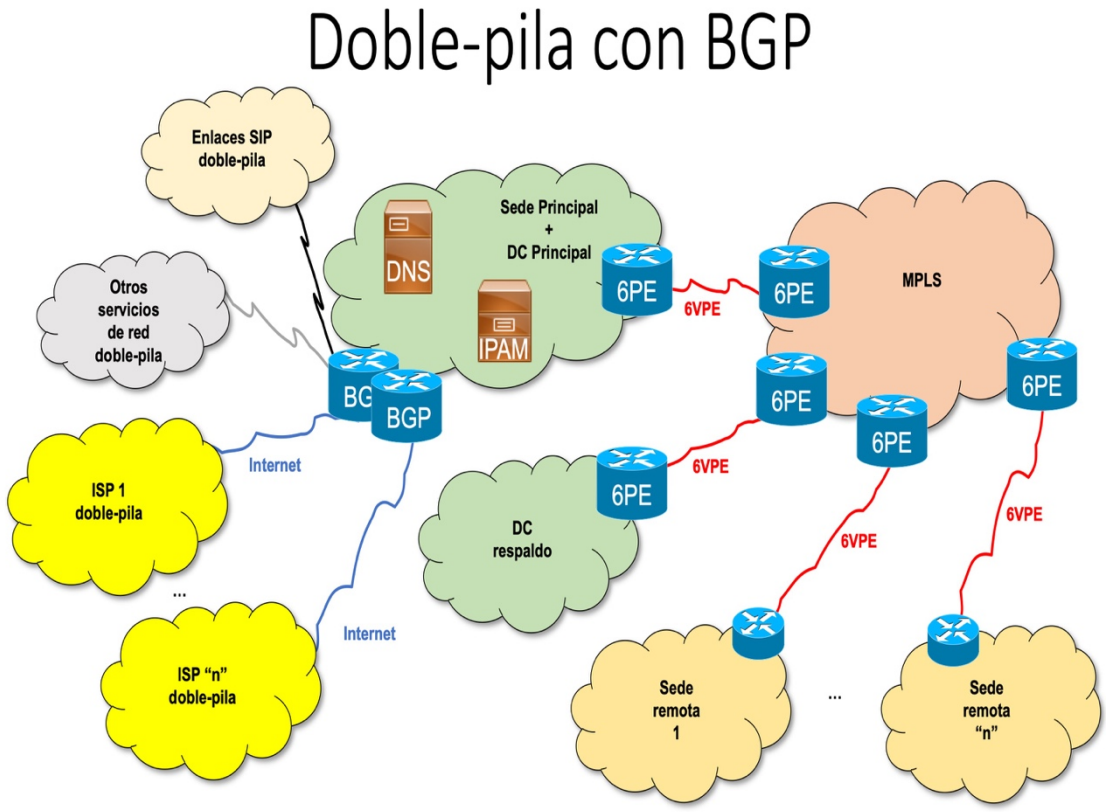

Diagrama de la red después del despliegue de IPv6

5. Desarrollo del plan de direccionamiento

En muchas ocasiones, el plan de direccionamiento existente con IPv4 puede ser una referencia para IPv6. Sin embargo, la recomendación es que partamos de cero, pues sin duda, en el transcurrir de los años, se habrán realizado "parches" en IPv4, y además muy probablemente estará basado en direcciones privadas que pueden incluso estar duplicadas en diferentes partes de la red. IPv6 es una oportunidad para hacerlo bien, incluso para darnos ideas para mejorar esos parches que hayamos aplicado en el plan de direccionamiento de IPv4.

Podemos decir que IPv6 tiene un espacio casi ilimitado de direcciones, pero hay que ser meticuloso y no desperdiciar direcciones donde no sea conveniente. En muchas guías se recomienda utilizar "bits", para facilitar identificar redes/VLANs, servicios, geografía o varios de estos aspectos.

Es importante estudiar cada caso detalladamente, de lo contrario, seguir al pie de la letra dichas recomendaciones, puede derivar en un desperdicio masivo de direcciones debido al uso innecesario e indebido de bits.

6. Obtención de recursos de Internet (ASN, direcciones IPv4 e IPv6)

Si deseamos evitar la renumeración que antes mencionábamos, y poder disponer de nuestras propias direcciones con BGP, tenemos que solicitar a nuestro RIR un número de Sistema Autónomo (ASN), espacio de direccionamiento IPv4 e IPv6.

En el caso de IPv4, si se justifica adecuadamente la necesidad, se puede obtener hasta un /22, es decir 1.024 direcciones. Esto sólo será posible mientras queden direcciones IPv4 en el RIR correspondiente y siempre que sea la primera vez que se solicitan, pues las entidades que ya habían recibido IPv4 de un RIR, según las políticas actuales, no podrán recibir mas recursos IPv4. Alternativamente, un IP bróker podría proporcionarlas.

En el caso de IPv6, si se trata de una entidad que sólo utiliza el direccionamiento para su propia red y no para terceros, se califica para un mínimo de un /48 por cada "sede" o "sitio" de la red, como "usuario final" (direccionamiento Independiente del Proveedor (PI, "Provider Independent"). Esto permite direccionar hasta 65.536 sub-redes (/64) dentro de dicho "sitio".

Si se trata de una red más grande, que puede necesitar subasignar direcciones a terceros (incluso a otras instituciones en el caso de una red de gobierno), entonces calificará para un mínimo de un /32 (lo que permite 65.536 "sitios" cada uno con su propio /48). Grandes redes de gobiernos a menudo requerirán prefijos mas cortos, por ejemplo, /25 o /26, lo cual es posible, desde hace varios años, porque las políticas de todos los RIRs han sido adaptadas para permitir este tipo de redes.

7. Gestión de direccionamiento IP (IPAM)

Es frecuente que para el plan de direccionamiento en IPv4 utilicemos un documento de texto u hoja de cálculo, cuando no un cuaderno de notas. El espacio de direccionamiento de IPv6, y las posibilidades de crecimiento de la red, hacen prohibitivo utilizar estos mecanismos y nos obligan a adoptar herramientas de gestión de direccionamiento IP, denominadas IPAM (IP Address Management), que pueden ser de código abierto, soluciones comerciales, o incluso dispositivos ("appliances").

A menudo estas soluciones permiten coordinar con DNS e incluso con DHCPv4 y DHCPv6.

8. Asignación y auditoría de direcciones

Uno de los aspectos más importantes al desplegar IPv6, es entender las diferencias entre los diferentes mecanismos de asignación de direcciones, como la autoconfiguración con SLAAC, DHCPv6, o la combinación de ambos e incluso el uso de múltiples direcciones en cada interfaz. Igualmente hay que entender qué dispositivos o sistemas operativos pueden utilizar unos u otros y en qué circunstancias.

En aquellas redes en las que se requiere "auditar" qué dispositivo, o qué usuario está accediendo a determinadas aplicaciones o servicios de la red (lo cual es habitual en redes de gobierno o de entidades financieras), estos aspectos tienen una especial relevancia y suponen cambios muy significativos respecto de IPv4 que pueden impactar en aplicaciones, bases de datos y mecanismos de seguridad de red.

9. Dispositivos de la infraestructura de la red y clientes

Cuando se realiza la auditoría de los equipos que constituyen la propia red, como servidores, equipos de clientes, sus sistemas operativos, etc., a menudo se tiende a pensar erróneamente que basta con que el fabricante indique "soporta IPv6".

No existe una definición clara de qué significa "soporte de IPv6" porque depende exclusivamente del contexto donde se utilizará dicho dispositivo o sistema operativo. Es decir, qué RFCs debe cumplir en función de su ubicación y funciones en cada punto concreto de la red.

Este punto trata de evitar que nos encontremos con situaciones en donde los fabricantes indican que soporta IPv6 pero al realizar el despliegue, no soportan uno o varios RFCs que son fundamentales para que cumpla con los requisitos que se esperaban, en una determinada ubicación o función en la red.

10. Impacto en aplicaciones y servicios

Esta es sin duda la faceta más complicada del despliegue de IPv6. Nos podemos encontrar con aplicaciones que utilizan direcciones literales, aplicaciones que utilizan librerías antiguas sin soporte de IPv6, aplicaciones

que guardan en bases de datos campos de sólo 32 bits, y un sinfín de problemas adicionales.

Todas estas aplicaciones podrían seguir funcionando cuando despleguemos IPv6 coexistiendo con IPv4 (doble-pila), pero no funcionarán cuando se retire IPv4 de la red y, esto va a ocurrir, mas bien pronto que tarde. Aún manteniendo doble-pila en la red, aquellas aplicaciones que dependan de IPv4, por cuestiones de seguridad o auditoría, no funcionarán correctamente cuando los usuarios accedan a ellas con IPv6. Igualmente, muchas aplicaciones se verían impactadas cuando usuarios externos sólo tengan acceso a IPv6.

En definitiva, ello nos obliga a hacer un estudio de las aplicaciones para clasificarlas y adoptar soluciones apropiadas a cada "grupo" de dicha clasificación.

11. Una red a largo plazo: mecanismos de transición

El despliegue de IPv6 no debe considerarse exclusivamente dependiendo de la coexistencia con IPv4. Si bien en la actualidad el pasó lógico es que ambos protocolos inicialmente coexistan, el futuro muy próximo es que las redes sean sólo-IPv6.

Ello implica que todo el proyecto de despliegue debe contemplar ambas situaciones, y resolver los problemas que se plantean en ambos casos, con la especial afección antes mencionada de las aplicaciones, ya que algunas de ellas no podrán ser modificadas (el fabricante no existe, no se tiene el código fuente, el cambio es muy costoso, etc.), y adoptar en algunos casos mecanismos de transición que permitan la coexistencia al inicio, y finalmente una red sólo-IPv6.

12. Contratos con operadores y conexiones con otras organizaciones

A menudo, y especialmente en redes grandes, tenemos varios proveedores de Internet que no colaboran entre ellos. También ocurre que hay otros proveedores diferentes para voz, u otros servicios. Como hemos indicado antes, en el caso de IPv4 se resolvía con NAT.

Con el despliegue de IPv6 deberemos renegociar esos contratos, tanto de datos como de voz u otros servicios, para que no sólo tengan soporte de IPv6 (inicialmente en modalidad doble-pila, en el futuro podrían ser sólo-IPv6), con BGP. Sólo en los casos de un único proveedor común para todos los servicios podremos evitar el uso de BGP, aunque sigue siendo conveniente y una buena práctica disponer de múltiples caminos con diversos proveedores, y anunciar nuestro propio espacio de direccionamiento en nuestro sistema autónomo.

Una vez tenidos en cuenta todos estos pasos, y solo entonces, podremos terminar de elaborar el proyecto detallado de despliegue de IPv6 y posteriormente iniciar su ejecución. Dependiendo del tamaño de la red, podrá suponer varios meses,

incluso años para los aspectos mas complicados, como es el análisis y adaptación de todas las aplicaciones.

Es importante tener en cuenta otros aspectos además de los indicados en esta guía. Por ejemplo, será necesario preparar una guía de compras para que futuras adquisiciones y contrataciones cumplan con los requisitos. Asimismo, pensar en capacitaciones para los desarrolladores de software, tanto internos como externos, estén preparados para el nuevo desafío. Otro aspecto puede ser preparar una hoja de ruta para maximizar el aprovechamiento del despliegue de IPv6, etc. También hay que presuponer que la red contará en el futuro con servicios IoT (Internet de las Cosas) y, por ejemplo, en el caso de redes de gobierno, pensar en SmartCities.

Todos estos aspectos, y muchos otros, sin duda nos darán una visión y dimensionamiento muy diferentes al de nuestra red actual con IPv4, de ahí la importancia de la capacitación y consultoría con garantía de experiencia previa en redes de gobierno y en general corporativas con IPv6.