

“12 Pasos para Activar IPv6 en la Red de un ISP”

Este documento no pretende ser un compendio técnico exhaustivo y detallado de cómo implementar IPv6 en una red de un ISP que actualmente tenga IPv4, sino un sumario ejecutivo de los 12 pasos fundamentales, sin incluir los servicios (DNS, web, correo electrónico, etc.), para el soporte nativo de IPv6 y el mantenimiento de IPv4 como un servicio transparente.

1. ¿Cuántos clientes (residenciales+ corporativos) tiene tu red y cuál es tu crecimiento previsto a corto/medio plazo? Si el total es inferior a 50.000 clientes, te recomendamos que solicites a LACNIC un /32, si tienes hasta 100.000 clientes pide un /31, hasta 200.000 clientes un /30, y así sucesivamente. Si ya tienes un /32 y superas los 50.000 clientes, pide aplicar el cambio de prefijo. Para solicitar tu prefijo IPv6, visita [Solicitar Recursos](#).
2. Audita toda tu red, necesitas saber que equipos no tienen buen soporte IPv6, cuales hay que actualizar y cuales hay que reemplazar. Es importante un inventario muy detallado, desde la conexión con tus upstreams hasta los CPEs de los clientes. Si los fabricantes no te dan buen soporte, es importante presionarles. Generalmente, el mercado es grande y libre ...
3. Realiza una capacitación profesional con empresas que tengan experiencia demostrada en despliegue de IPv6 en ISPs. IPv6 no es más difícil, pero IPv4 e IPv6 son diferentes y no es tan fácil “cambiar el chip”: Es necesario “desaprender” IPv4 para comprender bien IPv6. Posiblemente, sea conveniente que contrates un servicio de consultoría en conjunto con la capacitación. Puede parecer excesivo, pero te ahorrará una gran pérdida de tiempo, pues cada vez será más importante y urgente la transición a IPv6 y ese tiempo costará mucho más en pérdida de negocio y problemas con IPv4 que el coste de esa capacitación y consultoría.
4. Confirma que tus upstream providers tienen soporte IPv6 y actívalo en tu BGP con ellos. Igual con CDNs, cachés e IXs. Si los upstreams actuales no tienen soporte, realmente necesitas buscar mejores socios. Esta parte de la red tiene que ser dual-stack. En el peor de los casos, si no hubiera posibilidad de que uno o varios upstreams providers tuvieran soporte dual-stack, quizás tengas que utilizar algún túnel, típicamente 6in4 (protocolo 41, manualmente configurado) o GRE, pero debes pensar que esto ha de ser algo temporal.
5. Revisa tus políticas de seguridad. Deben ser equivalentes a las que apliques con IPv4, pero recuerda no filtrar ICMP en IPv6 y algunos otros detalles relacionados que impedirían el correcto flujo de tráfico en tu red. Revisa también el filtrado de prefijos para IPv6 en tus peers BGP, de nuevo son políticas conceptualmente equivalentes a lo que conoces con IPv4, pero con protocolos diferentes.
6. Configura soporte de IPv6 en todos tus sistemas de monitorización. IPv6 es tan importante como IPv4. Cualquier sistema que permita, tanto desde dentro, como desde fuera de tu red, ver la calidad del tráfico, cantidad de tráfico, estabilidad del mismo, visibilidad de tu prefijo, etc., etc., debe de soportar en igualdad de condiciones IPv4 e IPv6.
7. Ahora que ya sabes bien las diferencias entre IPv4 e IPv6, estás preparado para diseñar tu plan de numeración, aunque quizás gran parte de él lo pueda haber realizado la consultoría. Esto es una pieza clave para un buen despliegue de IPv6, es muy diferente que con IPv4 y sin duda

necesitas un dispositivo o herramienta de IPAM (IP Address Management). Es imposible gestionar millones de IPs con un Word o Excel como hacías con IPv4.

8. Despliega IPv6 en tu red de core y distribución. Posiblemente sea suficiente con dual-stack en una primera fase. Más adelante quizás puedas eliminar IPv4 de esa parte de la red y aprovechar esas direcciones IPv4 en lugares más importantes de la red.
9. Sería conveniente que hagas algún pequeño piloto, en tu propia red de empleados. Recuerda que el mínimo en cada LAN o VLAN es un /64, que la regla de oro es mantener dual-stack en las LANs/VLANs (aun cuando uses direcciones IPv4 privadas), y que lo más fácil y práctico es usar SLAAC y RDNNS. DHCPv6 es un extra, que muchas veces es innecesario, además Android no lo soporta. También en esta fase puede ser interesante involucrar a algún cliente corporativo en el piloto, e incluso a algunos residenciales. No importa que en este paso se haga con aprovisionamiento manual.
10. Prepara tu red de acceso, y tu sistema de aprovisionamiento. Quizás puede afectar también a tu sistema de billing. Es el momento de estudiar que mecanismo de transición vas a utilizar. Mi recomendación es 464XLAT¹, por lo menos a los clientes residenciales y redes celulares. Es fundamental que tengas buen soporte por parte de los fabricantes de los CPEs. Para el aprovisionamiento lo más fácil es utilizar DHCPv6-PD. Estudia el [BCOP de RIPE](#) al respecto de cómo numerar tus clientes.
11. Configura PLAT (NAT64+DNS64) en tu red. No uses CGN, te traerá muchos más problemas, mucho más coste (no sólo por los CGN sino también por los sistemas de logging). Si tienes una red celular, con el despliegue del PLAT, y la habilitación de un APN IPv6-only, ya tendrías todo funcionando para los smartphones y otros dispositivos 3G/LTE. En el caso de Android y Windows, incorporan el cliente CLAT, mientras que en el caso de iOS/Apple, usan sólo el PLAT pues se obliga al soporte de IPv6 en todas las apps.
12. Actualiza los CPEs. Vuelve a probar con algunos clientes, una vez actualizados; esto es lo más crítico y lo más complejo de todo el proceso. Hay muchas formas de afrontarlo. A partir de aquí, ya estás preparado para activar IPv6 masivamente (quizás por fases, regiones, etc.) y realizar un anuncio comercial.

¡Ya tienes tu red preparada para el futuro!

Ahora empieza a pensar en sacar provecho de IPv6 con nuevos servicios y aplicaciones, IoT es la pista clave, pero seguramente encontrarás otras ventajas.

Author: Jordi Palet, "The IPv6 Company"

¹ 464XLAT es uno de los más modernos mecanismos de transición (y el más utilizado, con millones de usuarios en las redes 3G/4G), que tiene la ventaja de utilizar sólo-IPv6 en la red de acceso, con lo cual el ISP no requiere direcciones IPv4 en la misma, y sin embargo proporciona direcciones IPv4 privadas a los usuarios (a través del CLAT), de tal forma que sus dispositivos y aplicaciones siguen funcionando de un modo transparente.