IPv6-Only vs IPv6-Mostly: Casos de Uso Apropiados

"Cada oveja con su pareja"

Cuestión de terminología

A menudo la terminología del IETF no se define de forma clara y explícita y ello conlleva confusiones e incluso usos no apropiados de los originalmente contemplados por los estándares, que pueden tener consecuencias en la calidad de servicio ofrecida al usuario.

Términos como IPv6-Only e IPv6-Mostly, son un claro ejemplo de ello, y por eso, a pesar de la complejidad alcanzar consenso en definiciones, finalmente en v6ops se está avanzando en el documento draft-palet-v6ops-ipv6-only.

Lo más importante a tener en cuenta es que, para utilizar correctamente estos términos, es preciso indicar un ámbito de aplicación.

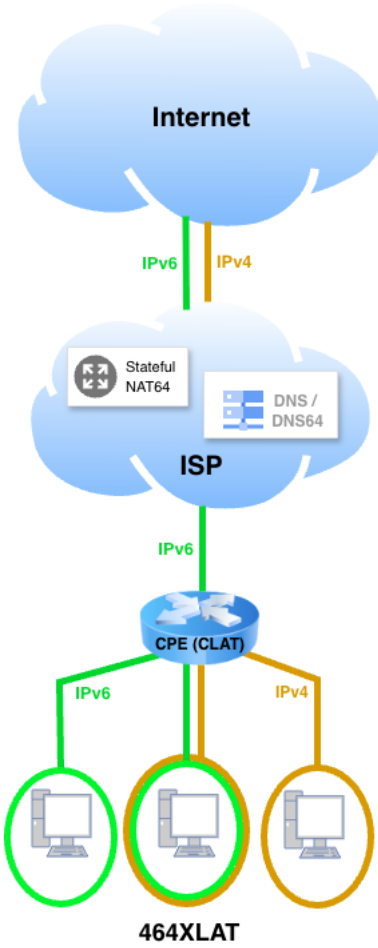
Por ejemplo, si decimos que una red es IPv6-Only, posiblemente no es correcto, porque implicaría, que en ninguna parte de la red se configura ni se usa IPv4, lo cual hoy en día no es un caso nada común (servicios, aplicaciones o contenidos internos o externos, no serían alcanzables con IPv4-Only). Si en cambio decimos "IPv6-Only Access network", estamos dejando claro que la parte de la red en la cual sólo existe IPv6 configurado de forma nativa (capa 2), es la red de acceso, y por lo tanto en las LANs del CPE, sí que puede haber doble-pila, igual que en el resto de la red del operador.

IPv6-Only+IPv4aaS

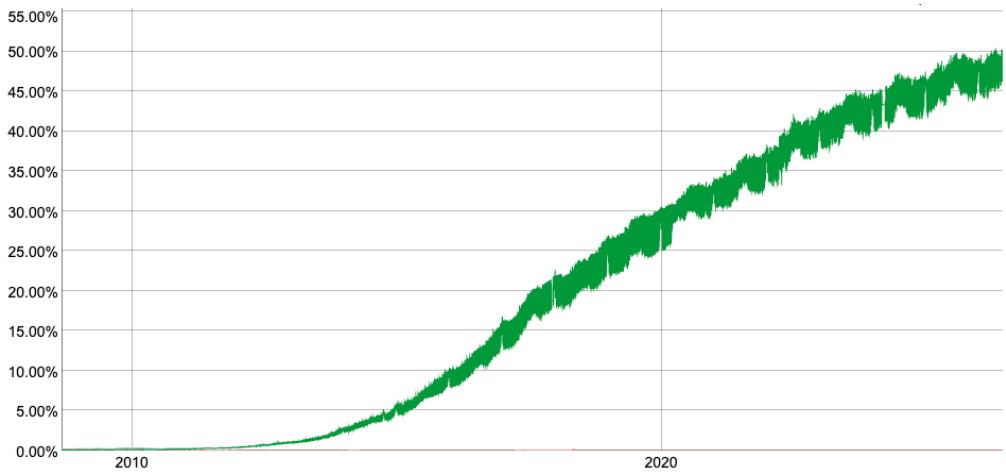
Este es el caso más común hoy en día en las redes de acceso móviles, por medio de 464XLAT, y es tendencia creciente en redes de acceso residenciales. Es uno de los 5 mecanismos de transición IPv6-Only+IPv4aaS ("IPv4 as a Service", IPv4 como servicio) para las **redes de acceso**. Permite que la parte WAN sea IPv6-Only, y al mismo tiempo mantiene dual-stack en la red del usuario, evitando que ningún dispositivo o aplicación deje de funcionar. Los documentos relevantes son: RFC6877, RFC8585, RFC8683, RFC9313, draft-ietf-v6ops-rfc6146-bis y draft-ietf-v6ops-rfc7084bis.

Estos 5 mecanismos, y especialmente **464XLAT** (que es el único soportado en redes móviles) tienen un claro caso de uso: **Redes no gestionadas** (unmanaged networks). Los usuarios de estas redes no necesitan realizar configuraciones especiales, independientemente de si los dispositivos que tiene en sus redes

residenciales o redes de “tethering” (cuando el teléfono móvil se convierte en router para dar acceso a otros dispositivos), usan IPv4, IPv6 o ambos, ya que el CPE incorpora un mecanismo de “stateless NAT46” (CLAT o equivalente), para facilitar la comunicación entre IPv4 e IPv6, **sin que el tráfico de las comunicaciones locales tenga que salir de la red local ni ser traducido**.



En los últimos años, el despliegue de IPv6 ha ido progresando de forma global, especialmente en redes móviles y residenciales. Esto se puede observar en las estadísticas de Akamai, APNIC, Facebook, Google, etc., las cuales indican una adopción de IPv6 superior al 50%, y ello sin tener en cuenta el tráfico de China (con obligaciones legales para los ISPs de transicionar hacia IPv6-Only), lo que posiblemente situaría ese porcentaje más cerca del 70-75% y creciendo rápidamente en este país. Sin embargo, aunque grandes proveedores de contenido han desplegado Data Centers con IPv6-Only, en general las organizaciones (públicas y privadas), tienen bajos niveles de adopción de IPv6.



IPv6-Mostly

Por ello, en el IETF se han dado pasos para facilitar el despliegue en **redes gestionadas** (managed networks), es decir redes corporativas, con mecanismos para llegar al modelo "IPv6-Mostly" (draft-ietf-v6ops-6mops).

IPv6-Mostly frente al modelo de dual-stack, en redes corporativas, tiene varios objetivos:

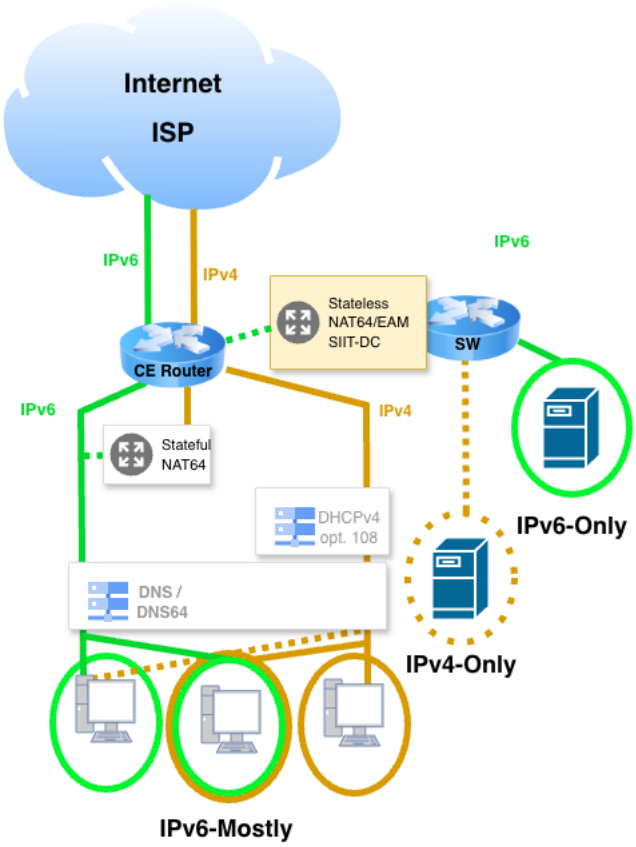
- Reducir el consumo de direcciones IPv4 privadas y uso de recursos DHCPv4.
- Evitar enmascarar problemas de IPv6 (por el fall-back a IPv4 que realiza HappyEyeballs), facilitando la depuración de errores con IPv6.
- Permitir una transición a IPv6-Only gradual, host a host, evitando la necesidad de segmentos específicos IPv6-Only y simplificando la operación, incrementando la escalabilidad.
- Descubrir y evitar incompatibilidades en un futuro IPv6-Only.
- Reducción del uso de NAT44.

IPv6-Mostly parte de la premisa del RFC8925: un host doble-pila, puede señalizar mediante una nueva opción (108) de DHCPv4, que no necesita utilizar IPv4 en su interfaz. El objetivo es evitar desplegar segmentos de red específicos IPv6-Only, sino que el host pueda comportarse como tal en un segmento dual-stack, siempre y cuando el administrador de la red así lo considere oportuno en dicho segmento. Para ello, la configuración del servidor DHCPv4 en dicho segmento, debe habilitarse con soporte de la opción 108, lo que permite controlar de forma granular que hosts pueden deshabilitar IPv4.

Ahora bien, deshabilitar IPv4 en un host, implica que no podrá acceder a destinos IPv4-Only, y por eso el administrador de la red sólo debe habilitar la opción 108 si ha implementado soporte de "stateful NAT64" (el PLAT en terminología de 464XLAT).

Si además se requiere soporte de direcciones IPv4 literales, aplicaciones sin soporte de IPv6, y similares situaciones, es necesario que los hosts que soporten la opción 108, incorporen también CLAT. De hecho, el soporte de CLAT (draft-ietf-v6ops-claton) en sistemas operativos de sobremesa, se ha venido incorporando progresivamente desde que se publicó el RFC8925, primero en MacOS y Linux, y recientemente (Public Preview) en Windows 11.

Los sistemas operativos móviles (iOS, Android, Harmony) incorporaron CLAT o equivalente, en sus interfaces celulares desde el nacimiento de 464XLAT, y recientemente también lo han incorporado a otras interfaces (como WiFi). Sin embargo, IPv6-Mostly no está soportado en la interfaz celular, porque generalmente, no hay implementación de DHCPv4 en dicha interfaz, tanto en el propio dispositivo, como en los dispositivos de la infraestructura de la red móvil.



Hay que tener en cuenta que el uso de IPv6-Mostly en un host, también impide la comunicación con dispositivos IPv4-Only en el mismo u otros segmentos de dicha red (incluso su acceso desde el exterior con IPv4 en caso de servidores). Es decir, una impresora, cámaras u otros dispositivos IPv4-only, no podrán ser utilizados por los dispositivos IPv6-Mostly. Obviamente, en una red corporativa, el administrador configurará explícitamente soluciones para permitir dicha comunicación, como por ejemplo a través del PLAT interno, o bien mecanismos

"stateless NAT64" con EAM (Explicit Address Mappings, RFC7757/STD103), SIIT-DC (RFC7755), etc.

En común

Tanto en el caso de 464XLAT como de IPv6-Mostly, para el descubrimiento del prefijo NAT64, se han venido utilizando diversos mecanismos, desde una configuración manual, hasta mecanismos propios de 3GPP en el caso de las redes móviles, pasando por sistemas heurísticos como RFC7050 (actualizado por RFC8880, pero que generalmente no es correctamente implementado en la mayoría de las redes). Recientemente se ha optado por una alternativa mejor, basada en mensajes RA (Router Advertisment), según el RFC8781.

Igualmente, por lo general es recomendable el uso de DNS64 (RFC6147), dado que ello implica evitar traducciones en el NAT46, reduce la carga en el DNS y mejora los tiempos de respuesta en el establecimiento de la conexión. Siempre que sea posible, aunque no es un problema habitual si el DNS64 está correctamente configurado, para evitar fallos de validación de DNSSEC, los Sistemas Operativos deben realizar "self-synthesis".

"Cada oveja con su pareja"

IPv6-Only+IPv4aaS (por ejemplo, 464XLAT) es un mecanismo de transición apropiado **para las redes de acceso**. Las redes conectadas mediante estos mecanismos, internamente suelen ser no-gestionadas, generalmente móviles y residenciales, incluso redes corporativas pequeñas y medianas cuando no requieren publicar servicios internos en Internet (o pocos y merece la pena una configuración manual).

IPv6-Mostly ha sido concebido **exclusivamente** para su uso en el **interior de redes corporativas gestionadas**, cuya red de acceso debería ser doble-pila. Aplicarlo a redes residenciales (no gestionadas) o móviles, implicaría:

- La red de acceso deberá mantenerse en doble-pila o bien incorporar CLAT en el CPE.
- La comunicación entre dispositivos IPv6-Mostly e IPv6-Only no es posible, salvo que se configuren manualmente mecanismos como PLAT, EAM o SIIT-DC, posiblemente en el CPE, en cuyo caso la red pasa a ser gestionada. Alternativamente esos mecanismos podrían ser configurados por el ISP de forma virtual en la nube o infraestructura del operador, teniendo en cuenta las implicaciones creadas porque muchos usuarios residenciales pueden

estar usando las mismas direcciones IPv4 privadas que otros. Ello obligaría a que ese tráfico en lugar de quedarse localmente "suba y baje" a la nube o infraestructura del operador, con los consiguientes retardos y ancho de banda adicional.

A menudo los fabricantes de CPEs residenciales no incorporan CLAT en los mismos, y la excusa habitual es su complejidad, lo cual no es cierto. Incorporar la opción 108 en DHCPv4, es incluso más complejo y supone más código, además de la necesidad de implementar PLAT, EAM o SIIT-DC y una interfaz amigable para facilitar su gestión a usuarios no expertos. Además, en todos los casos, hay múltiples implementaciones de código abierto, y el mayor coste en realidad es el profundo conocimiento de estos protocolos, incluso de IPv6 y de los mecanismos de transición.

464XLAT vs IPv6-Mostly		
	464XLAT	**IPv6-Mostly**
Red de Acceso	IPv6-Only	Dual-Stack
Ámbito del Mecanismo	Red de acceso	Segmentos de la red
Gestionado	NO	SI
Requisitos CPE	CLAT	Dual-Stack
Requisitos Red del ISP	PLAT DNS64 (recomendado)	
Requisitos Red Local		PLAT DHCPv6 Opción 108
Comunicación Local IPv4-IPv6	SI	Manualmente configurada: PLAT, EAM, SIIT-DC, otros
Soporte en Redes Móviles	SI	NO
Ventajas	Ahorra IPv4 públicas	Ahorra IPv4 privadas Facilita depuración de errores IPv6 IPv6-Only gradual Descubre Incompatibilidades Reduce uso de NAT44
RFCs Obligatorios	RFC6146/draft-ietf-v6ops-rfc6146-bis RFC6147 RFC6877 RFC7084/draft-ietf-v6ops-rfc7084bis	RFC6146/draft-ietf-v6ops-rfc6146-bis RFC6147 RFC8925 draft-ietf-v6ops-6mops RFC7757/STD103 RFC7755
RFCs Recomendados	RFC8585 RFC8683 RFC8781 draft-ietf-v6ops-claton	RFC8683 RFC8781 draft-ietf-v6ops-claton

Nota: Los RFCs indicados en la tabla son referencias en diversas partes de la red, su utilización concreta puede variar según detalles del modelo de despliegue.

Concluyendo

Lo más importante es la satisfacción del usuario, y ello nos obliga, por un lado, a utilizar los protocolos apropiados para cada caso y por otro lado, a hacer un llamamiento a los fabricantes de CPEs para que incorporen CLAT en sus dispositivos (y para uso corporativo los protocolos relevantes de IPv6-Mostly). Mismo llamamiento a los ISPs para que exijan dicho soporte. Hay alternativas en el mercado y debemos escoger no solo precio (a menudo se cumple “lo más barato sale caro”), sino lo mejor para los usuarios y nuestras redes. Sólo el propio mercado (o regulación explícita) obliga a que los fabricantes implementen lo que necesitamos. No descartemos opciones OEM muy competitivas con OpenWrt, el cual es válido incluso para evitar reemplazar los CPEs existentes con firmware a medida para nuestra red.