

RFC 6164 : Using 127-Bit IPv6 Prefixes on Inter-Router Links

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 avril 2011

Date de publication du RFC : Avril 2011

<https://www.bortzmeyer.org/6164.html>

Quelles adresses IP utiliser sur un lien point-à-point, lorsque les deux machines qui se parlent sont seules sur le lien ? Ce nouveau RFC recommande l'utilisation d'un préfixe de longueur /127 pour IPv6, ne permettant que deux adresses IP.

Cette recommandation existait déjà pour IPv4, dans le RFC 3021¹, qui recommande un /31. Pour IPv6, la norme, en l'occurrence le RFC 4291 préconisait au contraire un préfixe /64 pour tous les liens. Les adresses sous ce préfixe pouvaient alors être construites selon le format dérivé du EUI-64. Certains opérateurs avaient déjà ignoré cette norme et utilisaient des préfixes de longueur /127 (ne laissant qu'un seul bit pour identifier la machine), malgré l'avis du RFC 3627, qui mettait en avant le risque de confusion avec l'adresse "anycast" des routeurs. Notre RFC 6164 leur donne raison et officialise les préfixes /127.

Lorsqu'il n'y a que deux machines sur un lien (par exemple une liaison point-à-point, que ce soit parce qu'elle utilise un technologie purement point-à-point ou bien simplement parce qu'elle a été configurée ainsi), on peut aussi utiliser les adresses locales au lien (fe80::/10). Mais, comme le rappelle la section 2 de notre RFC, celles-ci ne sont pas toujours suffisantes : surveillance du réseau à distance, traceroute et BGP sont des exemples de bonnes raisons pour utiliser des adresses globales.

Quelles étaient les raisons pour se méfier des préfixes de longueur 127 ? La section 4 résume la principale : confusion possible avec l'adresse des routeurs du lien, définie en section 2.6.1 du RFC 4291. Or, non seulement l'expérience des opérateurs qui ont violé le RFC 3627 a été positive (pas de problèmes notés) mais on peut trouver des très bonnes raisons pour utiliser des préfixes plus spécifiques qu'un /64. La section 5 cite :

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc3021.txt>

- Risque de boucle de routage sur un préfixe plus général qu'un /127, si le lien n'utilise pas le NDP (c'est le cas de SONET).
- Risque d'attaque par déni de service en épuisant le cache des voisins. Imaginons nos deux routeurs sur un Ethernet et étant configurés dans un préfixe /64. Tout paquet IP à destination d'une adresse de ce préfixe va faire l'objet d'une tentative de résolution par NDP (RFC 4861), et, pendant ce temps, le routeur devra garder une entrée dans sa table des voisins, avant de renoncer. Évidemment, aucune machine n'a une table des voisins de $2^{\wedge}64$ entrées. Un méchant qui générerait des paquets à destination de toutes les adresses du préfixe /64 pourrait remplir cette table plus vite que l'expiration du délai de garde ne la vide. Notez que cette attaque n'est pas spécifique aux liens point-à-point mais ceux-ci sont souvent des liens vitaux, entre routeurs « importants ». Cette attaque peut être traitée en limitant le nombre de résolutions NDP en cours mais cela ne la résout pas complètement, alors que l'usage d'un /127 la supprime.
- Sensation de gaspillage des adresses si on bloque un /64 pour seulement deux machines. Vue la taille de l'espace d'adressage d'IPv6, c'est le moins convaincant des arguments.

Synthétisant tout cela, la section 6 de notre RFC conclut qu'il faut utiliser les /127. Le logiciel des routeurs doit accepter de tels préfixes. Les opérateurs doivent faire attention à ne pas utiliser certaines adresses, celles-ci ayant une signification particulière : adresses où les 64 bits les plus à droite sont nuls, ou bien adresses dont ces mêmes bits ont une des 128 plus grandes valeurs (réservées par le RFC 2526).

Pour un exemple des discussions récurrentes /64 vs. /127, voir « *Point-to-point Links and /64s* » <<https://blogs.infoblox.com/ipv6-coe/point-to-point-links-and-64s/>> ». Le RFC 3627 a été officiellement déclaré « d'intérêt historique seulement » par le RFC 6547. À noter que ce RFC 6164 ne met pas à jour formellement <<http://www.ietf.org/mail-archive/web/ipv6/current/msg16355.html>> le RFC 5375, qui continuait avec les anciennes recommandations.