RFC 6782 : Wireline Incremental IPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 novembre 2012

Date de publication du RFC : Novembre 2012

https://www.bortzmeyer.org/6782.html

Parfois, je me dis que si on consacrait tous les efforts qui ont été voués à écrire des RFC à propos d'IPv6 à **déployer** IPv6 au lieu d'expliquer comment le faire, ce protocole aurait remplacé IPv4 depuis longtemps... Toujours est-il que voici un nouveau RFC, consacré à la synthèse de l'état de l'art en matière de déploiement **incrémental** d'IPv6 pour un opérateur filaire (FAI ADSL ou câble par exemple).

« Incrémental » car peu d'opérateurs ont la possibilité de déployer un réseau purement IPv6. Par contre, je ne sais pas pourquoi le RFC se limite au filaire, la plus grande partie de son texte peut tout à fait s'appliquer aussi bien à un opérateur mobile (genre 3G).

Plein de textes ont déjà été écrits sur ce même sujet mais les choses changent et il est peut-être bon de temps en temps de refaire une synthèse. Donc, l'idée est de prendre par la main un opérateur qui, en 2012, serait toujours en IPv4 pur (c'est donc un opérateur assez retardé techniquement), pour l'amener (à long terme !) en IPv6 pur (cf. section 3.6). Le point important à garder en mémoire est que chaque opérateur est différent et que, s'il existe plusieurs mécanismes de migration d'IPv4 vers IPv6, ce n'est pas uniquement parce que l'IETF aime écrire beaucoup de RFC, c'est surtout parce qu'il n'y a pas **un** mécanisme qui conviendrait miraculeusement à tous les cas (cf. le RFC 6180[1] qui décrivait tous ces mécanismes).

Donc, point de départ, un opérateur Internet qui a des clients en IPv4 (et qu'il n'est pas question de migrer immédiatement), qui veut déployer IPv6 mais en ne cassant pas ce qui existe, en minimisant la quantité de travail nécessaire (donc sans déployer de technologies inutiles). En outre, on veut une qualité de service optimum, donc éviter les tunnels, si possible.

Avec un tel cahier des charges, une migration soudaine de tout le réseau d'un protocole vers un autre est hors de question. Il faut une démarche progressive, où IPv6 arrive petit à petit pendant qu'IPv4 continue de fonctionner correctement. Le problème, c'est que, sur le papier, une telle approche progressive ("*phased approach*") est très sympa mais, en pratique :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6180.txt

— Par suite de la procrastination <https://www.bortzmeyer.org/ipv6-et-l-echec-du-marche.html> d'un grand nombre d'acteurs, les adresses IPv4 sont déjà épuisées <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>,
— Si IPv6 est mis en œuvre dans tous les logiciels et équipements sérieux, depuis de nombreuses années, il n'a pas toujours été utilisé en production avec la même intensité qu'IPv4 et des bogues traînent donc toujours,
— Le FAI ne contrôle en général pas les équipements des clients (c'est une des différences entre le FAI filaire et le mobile) et ceux-ci peuvent avoir des vieux systèmes, avec peu ou pas de gestion d'IPv6,
— Le retour à un réseau multi-protocoles (qui n'est pas une nouvelle chose : dans les années 1980, tous les réseaux locaux étaient multi-protocoles) va poser quelques problèmes opérationnels.

Le RFC rappelle que le client final, le mythique « M. Michu », ne demande pas IPv6. Il ne demande pas IPv4 non plus. Il veut un accès à l'Internet, point. C'est aux professionnels de faire en sorte que son accès fonctionne, aussi bien en IPv4 qu'en IPv6. Les deux protocoles coexisteront sur le réseau local pendant encore longtemps (section 3.1 du RFC).

La section 3 du RFC examine plus en détail ces défis pratiques. La pénurie de plus en plus aiguë <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> d'adresses IPv4 va nécessiter du partage d'adresses IP, avec tous ses inconvénients (RFC 6269, et la section 4.2 de notre RFC). Les autres solutions (gratter les fonds de tiroir à la recherche de préfixes oubliés, acheter au marché gris ou noir des adresses vendues sans garantie <https://www.bortzmeyer.org/le-reseau-1.html>) ne suffiront sans doute pas.

Mais IPv6 ne peut pas se déployer en cinq minutes. Sans même prendre en compte l'existence de vieux systèmes ne parlant qu'IPv4, l'opérateur qui va déployer IPv6 va devoir prévoir une période d'assimilation des nouvelles pratiques (IPv6 est très proche d'IPv4 mais pas identique). Souvent, les humains ne sont pas au même niveau en IPv6 qu'en IPv4, et c'est pareil pour les logiciels (pas toujours testés au feu). Si la connectivité IPv4 de l'opérateur va dépendre de sa connectivité IPv6 (comme c'est le cas avec certaines techniques comme DS-Lite - RFC 6333 - ou NAT64 - RFC 6146), un problème IPv6 va également toucher IPv4.

Il faut donc faire attention à ne pas déployer IPv6 sans supervision et de réaction adaptés. Trop souvent, des organisations ont mis un peu d'IPv6, se disant que c'était facile et sans conséquences, puis se sont aperçu après qu'un réseau non géré était moins utile : pannes IPv6 non détectées par le système de surveillance, par exemple.

Certaines des techniques de transition n'ont pas aidé, en proposant des mécanismes qui avaient l'avantage de permettre de faire de l'IPv6 rapidement, et l'inconvénient de fournir aux utilisateurs un vécu de moins bonne qualité. C'est le cas notamment avec les tunnels (tous les tunnels ne sont pas forcément mauvais mais, dans l'histoire d'IPv6, il y a eu beaucoup de problèmes à cause de certains tunnels) : ajoutant une complication supplémentaire, forçant le passage par un chemin qui n'est pas toujours optimum, les tunnels ne devraient être utilisés que lorsqu'il n'y a pas d'autre choix, et en toute connaissance de cause. L'objectif est bien de fournir de la connectivité native.

Avec ces défis en tête, la section 4 du RFC rappelle les techniques de transition et de coexistence possibles. La première citée est la catégorie des tunnels automatiques, 6to4 et Teredo, à mon avis la pire (le RFC 6343 documente certains des problèmes avec 6to4 et le RFC 7526 demande qu'il ne soit plus utilisé). Le problème de fond de ces techniques est qu'elles ne fournissent aucun moyen de contrôler le chemin de retour, ou même de savoir s'il existe. Elles ne devraient à mon avis être utilisées que si on veut décourager les gens de faire de l'IPv6

6rd (RFC 5969) bouche certains des trous de 6to4 et c'est la technique qu'a utilisé Free pour distribuer IPv6 sur son réseau, en attendant un hypothétique accès natif. Son principal avantage est qu'il limite l'investissement initial pour l'opérateur, lui permettant de croître progressivement.

DS-Lite (RFC 6333) tunnele l'IPv4 sur un réseau IPv6. Il est surtout intéressant pour un opérateur qui part de zéro (par exemple parce qu'il vient de se créer) et qui peut donc construire un réseau entièrement IPv6 (ce qui peut être difficile avec certains équipements, encore aujourd'hui), tout en ayant des clients IPv4 à satisfaire. Le CPE doit être capable de faire du DS-Lite donc cette solution marche mieux si le FAI contrôle les CPE.

NAT64 (RFC 6146) est pour le cas où les clients sont bien en IPv6 mais où certains services à l'extérieur ne sont accessibles qu'en IPv4. Elle ne semble donc pas d'une grande actualité aujourd'hui, puisque le réseau local purement IPv6 est encore dans le futur (voir RFC 6586). Elle sera plus utile lorsque les réseaux purement IPv6 devront accéder aux derniers dinosaures IPv4.

La technique de coexistence IPv4/IPv6 qui donne les meilleurs résultats, est la double pile ("*dual stack*") où les machines ont les deux protocoles et deux adresses. Pour permettre l'étape suivante (IPv6 pur), elle nécessite un réseau entièrement IPv6 (y compris les services, par exemple le DNS). Elle ne résout pas le problème de l'épuisement des adresses IPv4 donc, pour un opérateur actuel, le vécu IPv4 restera marqué par le partage d'adresses, le CGN et autres horreurs.

À noter que j'ai fait un exposé comparant toutes ces techniques de transition en 2011 à Grenoble <https://www.bortzmeyer.org/transition-ipv6-guilde.html>.

Après les défis, et les techniques disponibles, la section 5 présente les différentes phases du déploiement. Une organisation qui va passer à IPv6 peut utiliser cette section comme point de départ pour établir son propre plan de migration. Il est important de noter que ce RFC ne fournit pas un plan tout prêt adapté à tout le monde. Il fournit des lignes directrices, mais chacun doit créer son propre plan, en tenant compte de son réseau, de ses clients, de ses moyens humains et financiers. (Une vision plus technique est dans le RFC 6180.)

La section 5 liste successivement plusieurs phases. J'espère qu'en 2012, plus personne n'en est encore à la phase 0 mais on ne sait jamais... La **phase 0** commence par la formation : si personne dans l'organisation (ou bien seulement un ou deux "*geeks*") ne connait IPv6, il faut apprendre. Cela peut se faire par des formations formelles, ou en lisant des livres ou des textes sur le Web. Pour le personnel d'exécution, le RFC rappelle qu'il vaut mieux que la formation soit faite juste avant le déploiement, pour qu'elle ne soit pas oubliée lorsque le moment de s'en servir viendra. Cette phase 0 ne doit pas être purement théorique, et il faut aussi pratiquer, dans un laboratoire dédié à cet effet, à la fois pour que les gens apprennent par la pratique, et pour tester si les matériels et logiciels utilisés dans l'organisation n'ont pas de problème avec IPv6.

Armé de cette formation et de cette expérience en laboratoire, les techniciens peuvent alors commencer à planifier le futur routage IPv6 de leur réseau. Est-ce la même tâche qu'en IPv4 ? On peut argumenter dans un sens ou dans l'autre. Le RFC met plutôt l'accent sur les différences mais on peut aussi considérer que le modèle de routage est tellement proche dans les deux protocoles qu'il ne faut pas dramatiser les différences.

Outre la politique de routage, trois autres points doivent retenir l'attention de l'équipe qui conçoit le plan de migration vers IPv6 :

— La sécurité, pour laquelle IPv6 peut poser quelques différences (comme pour le routage, je les trouve mineures) : les RFC 4942, RFC 6092 et RFC 6169 contiennent des analyses utiles sur la sécurité d'IPv6 (dommage, à mon avis, que le RFC 6104 ne soit pas cité).
— L'administration des adresses IP (IPAM adaptés à IPv6) et la gestion du réseau,
— Et bien sûr les techniques de transition adaptés à cette organisation particulière.

On peut espérer qu'en 2012, la plupart des grosses organisations sérieuses ont au moins franchi la phase 0. Mais pas mal de petites organisations ne l'ont même pas encore commencé.

Étape suivante, la **phase 1**. Il s'agit cette fois de donner un accès IPv6 à ses clients ou utilisateurs, via des tunnels pour l'instant, car le réseau n'est pas forcément prêt pour de l'IPv6 natif partout. Par exemple, il est courant que le réseau interne d'un opérateur, équipé de routeurs récents, permette IPv6 mais que l'accès aux clients passe par des équipements qu'on ne contrôle pas complètement (par exemple des DSLAM) et qui ne sont pas prêts pour IPv6. (Notez qu'il n'est pas obligatoire de passer par **toutes** les phases. Si on a un réseau où on peut utiliser du natif tout de suite, nul besoin d'un détour par des tunnels.) La phase 1 peut se faire avec une technologie comme 6rd (RFC 5569), si on contrôle le CPE.

Naturellement, à cette phase 1, il n'y aura pas de miracle : on utilisera des tunnels, donc on aura les problèmes associés aux tunnels comme la MTU diminuée.

Ensuite, place à la **phase 2**. Cette fois, on fournit de l'IPv6 natif. Tout fonctionne en IPv6 et, surtout, avec le même niveau de qualité qu'en IPv4. C'est un point très important car un certain nombre de fournisseurs qui se vantent de permettre IPv6 ne surveillent pas automatiquement la connectivité IPv6 (laissant les clients faire cette surveillance) et, même lorsqu'on leur signale un problème, le traitent uniquement dès qu'ils ont du temps libre (alors qu'un problème IPv4 est traité immédiatement). Un niveau de service équivalent à celui d'IPv4 est crucial si on veut convaincre les clients de migrer. Si vous faites l'audit du niveau de préparation IPv6 d'un fournisseur d'accès ou d'hébergement, ce sont les meilleurs tests : 1) le "*monitoring*" est-il également fait pour IPv6 ? 2) en cas de panne IPv6, y a-t-il le même niveau de mobilisation que pour IPv4 ? (Ou bien, est-ce que le NOC réagira en se disant « ah, IPv6, c'est Richard, on va attendre qu'il revienne de vacances », ce qui est le cas de la majorité des sociétés prétendant faire de l'IPv6 aujourd'hui.)

À ce stade, il faut encore fournir le service IPv4. Compte-tenu de l'épuisement des adresses, il faudra probablement déployer du CGN/NAT444 <https://www.bortzmeyer.org/nats.html>, peut-être avec l'aide de technologies comme DS-Lite (RFC 6333). Au début du déploiement, le CGN peut encore être une grosse machine centrale puis, si son usage croît, être réparti petit à petit sur d'autres machines.

Normalement, l'usage d'IPv4 devrait ensuite suffisamment baisser pour qu'on puisse passer à la **phase 3**, un réseau purement IPv6. En novembre 2012, au moment où j'écris ces lignes, cela semble une perspective très lointaine, sauf peut-être sur des réseaux très spécifiques. Mais cela arrivera bien un jour.

Même dans ce cas, il est possible qu'il faille fournir une connectivité IPv4 à certains clients. DS-Lite, qui tunnele le trafic IPv4 sur le réseau IPv6, est là encore utile. Si, ce qui est plus vraisemblable, on a juste besoin de permettre l'accès des clients IPv6 à des sites Web qui sont restés en IPv4, NAT64 (RFC 6144 et RFC 6146) sera sans doute la bonne solution. Mais, bon, c'est un problème pour le futur... Le RFC a un ton plutôt pessimiste et, à mon avis, voit le verre IPv6 plutôt à moitié vide.