RFC 6264 : An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 juin 2011

Date de publication du RFC : Juin 2011

https://www.bortzmeyer.org/6264.html

Verra-t-on un jour la fin des RFC sur les plans de transition d'IPv4 vers IPv6 ? Sans doute pas tant que la transition traîne. En effet, la lenteur imprévue du déploiement d'IPv6 remet en cause les plans initiaux (qui reposaient sur l'idée qu'il resterait des adresses IPv4 pendant toute la phase de transition) et nécessite le développement de nouveaux plans, pour répondre à une situation différente.

Le plan présenté ici est une variante des plans reposant sur l'idée de CGN ("*Carrier-Grade NAT*"), ces routeurs NAT installés, non pas dans la "*box*" de M. Michu, pour son usage et celui de sa famille, mais installés chez le FAI, pour l'usage partagé de plusieurs clients du FAI. Le CGN a l'avantage de nécessiter zéro logiciel ou configuration chez l'utilisateur (qui n'a probablement pas le temps et l'envie de maîtriser ces mécanismes). Ces solutions reposant uniquement sur le travail du FAI sont donc tentantes pour répondre au problème de la trop lente migration chez les utilisateurs. (Toutefois, mon impression personnelle est que beaucoup de réseaux de M. Michu, plein de gadgets récents, sont plus avancés vers IPv6 que pas mal de réseaux de FAI, conçus il y a des années.)

La nouveauté par rapport aux autres plans reposant sur le CGN est l'introduction de mécanismes pour éviter que ce CGN ne se transforme en impasse, et pour le faire évoluer vers de l'IPv6 natif complet. En effet, dans la plupart des cas, le terme de CGN fait penser à un mécanisme pour **retarder** la transition, le NAT444 <https://www.bortzmeyer.org/nats.html>, qui permet au FAI paresseux de continuer à utiliser IPv4 même alors qu'il ne peut plus distribuer ne serait-ce qu'une seule adresse IPv4 publique <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> à ses clients. Ce CGN-là ne fait pas progresser vers IPv6 (section 1 du RFC).

D'où cette idée de proposer un plan de migration reposant sur le CGN mais prévoyant dès le début les moyens d'en sortir. Ce RFC ne contient pas de nouveaux protocoles, il ne fait que combiner les protocoles existants.

Dans un certain nombre de FAI, la situation est actuellement la suivante (section 2) :

— Plus d'adresses IPv4 publiques,
— Un réseau interne purement IPv4, par manque de proactivité du FAI (qui aurait dû déployer IPv6 depuis longtemps), et qu'on ne peut pas migrer en cinq minutes,
— La prise de conscience qu'IPv6 est nécessaire, et à relativement court terme.

Dans d'autre cas, FAI ayant fait son travail à l'avance et ayant déployé IPv6 depuis longtemps, ou bien FAI tout récent et préférant l'approche radicale de déployer un réseau purement IPv6, avec NAT64 (RFC 6144 [1], et section 2.6 de notre RFC) pour assurer la liaison avec le vieux protocole, ces hypothèses ne sont plus vraies et l'approche de ce RFC ne s'applique donc pas. Comme toujours avec la transition vers IPv6, il faut analyser son réseau et déterminer la ou les meilleures stratégies de transition : chacune s'applique à un cas bien particulier.

Le dessin n° 1 en section 2.1 résume bien l'approche « CGN progressif » ("*Incremental Carrier-Grade NAT*"). En partant de chez M. Michu (ou plutôt M. Li car le cas décrit est plus proche de ce que vivent les FAI asiatiques), on a :

— Les machines de M. Li, certaines en IPv6 mais pas toutes,
— Un nouveau composant, le HG ("*Home Gateway*"), une "*box*" capable d'assurer certaines fonctions comme de tunneler le trafic IPv6 vers le routeur NAT situé plus loin dans le réseau du FAI,
— Le tunnel IPv6-sur-IPv4 qui commence à la HG et se termine au routeur CGN,
— Le réseau purement IPv4 du FAI,
— Le CGN, une très grosse boîte,
— Des serveurs restés purement v4 sur le réseau du FAI (serveur Web du portail, par exemple),
— L'accès à l'Internet, en IPv4 et en IPv6.

Les deux composants nouveaux, que n'a pas forcément le FAI aujourd'hui, sont le HG et le CGN. Le HG doit obéir au RFC 7084. Autrement, tous les équipements (routeurs classiques et machines terminales) ne changent pas (cf. section 2.5).

Quelle technique de tunnel choisir entre le HG et le CGN ? La section 2.2 rappelle les possibilités. Les tunnels configurés manuellement du RFC 4213 paraissent peu pratiques. Ceux du RFC 3053 peuvent ne pas être très utilisables par l'utilisateur résidentiel. Cela laisse 6rd (RFC 5969) et peut-être GRE (RFC 2784). Si le FAI a déjà une infrastructure MPLS, il peut aussi considérer RFC 4798, mais cela suppose que MPLS aille jusqu'au HG, ce qui est peu probable. Bref, le RFC recommande 6rd.

La section 2.3 peut alors décrire en détail le fonctionnement de la HG ("*Home Gateway*", la "*box*"). Lorsqu'elle reçoit un paquet de l'intérieur :

— Si c'est un paquet IPv4, elle le fait suivre sur l'infrastructure v4 normale du FAI (peut-être après traduction), jusqu'au CGN qui fera alors une traduction v4-v4 (il aura donc pu y avoir deux traductions),
— Si c'est un paquet IPv6, elle l'encapsule pour l'envoyer, via le tunnel, jusqu'au CGN (le gros routeur/traducteur situé plus loin dans l'infrastructure du FAI).

Et le CGN ("*Carrier-Grade NAT*", un routeur NAT qui sert plusieurs clients) ? La section 2.4 lui est consacrée. Lorsqu'il reçoit un paquet IPv4 venu d'une HG (rappelons que tout ce RFC est consacré au cas où l'infrastructure du FAI est purement IPv4), deux cas :

— C'est un paquet v4 normal, et on le transmet après traduction (puisque le FAI n'a pas assez d'adresses IPv4 publiques, le paquet a certainement une adresse source privée) ; comme tout routeur NAT, le CGN mémorise la correspondance port¡-¿adresse,
— C'est un paquet IPv6 encapsulé dans du v4. Le CGN le décapsule, et le transmet.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6144.txt`

Voilà, sur le papier, c'est tout simple. Quelles sont les conséquences pratiques ? La section 2.7 discute divers points. D'abord, comme toute solution à base de NAT, notre schéma a tous les inconvénients du partage d'adresses. Pire, comme le CGN est situé loin de l'utilisateur, et que celui-ci ne peut pas le configurer, des techniques permettant d'avoir des connexions entrantes comme les correspondances statiques ou comme UPnP ne fonctionnent plus. D'autre part, le tunnel v6-sur-v4 entre le HG et le CGN posera les habituels problèmes de MTU (dont le RFC se débarasse avec une pirouette).

L'originalité de l'approche de ce RFC est la possibilité de migrer de cette solution NAT complexe et fragile vers une solution IPv6 propre. Comment ? C'est ce que décrit la section 3, qui prévoit plusieurs étapes, en supposant :

— On installe un CGN pour faire du NAT444. À court terme, cela réduit la demande en adresses IPv4 publiques. Mais cela n'aide pas en soi à migrer vers IPv6. Le HG doit être mis à jour pour utiliser le CGN.
— On déploie 6rd (nouvelle mise à jour du logiciel du CGN),
— On déploie alors tranquillement IPv6 sur le réseau du FAI. Dès que la zone desservie a un routage IPv6, on peut couper 6rd dans le HG, supprimant ainsi le tunnel v6-sur-v4 (IPv4 continuant à être envoyé au CGN). Cette coupure du tunnel peut se faire automatiquement, si le HG a été programmé pour détecter les RA ("*Router Advertisment*") ou réponses DHCP IPv6.
— Cette dernière possibilité suppose une forme de double-pile (v4 et v6) sur le réseau du FAI pendant un temps. Si celui-ci préfère n'avoir qu'un seul protocole à gérer, l'approche est au contraire de basculer du routage purement v4 du début à un routage purement v6. C'est alors IPv4 qui sera tunnelé, via DS-Lite. Le FAI sera alors arrivé jusqu'au bout, il sera purement IPv6.

Comme indiqué, le passage d'une étape à une autre peut être détecté automatiquement par le HG, la "*box*", qui peut par exemple interroger le CGN pour noter les nouvelles fonctions disponibles. Cela éviterait une action explicite sur la HG.

Il reste à étudier les conséquences de ce schéma en terme de sécurité (section 4). Le NAT en général pose de nombreux problèmes de sécurité (RFC 2663 et RFC 2993). Le partage massif d'adresses, par exemple dans un CGN, crée des failles expliquées dans le projet de RFC `draft-ietf-intarea-shared-addressing-i`
Les protocoles spécifiques utilisés ont également leurs propres questions de sécurité, documentées dans leur norme respective (par exemple, pour 6rd, dans la section 12 du RFC 5969).

Toutefois, le fait que ce schéma concerne uniquement des mécanismes utilisés **à l'intérieur** du réseau d'un FAI, la sécurité est simplifiée. On peut certes sécuriser les tunnels avec le RFC 4891 mais ce n'est peut-être pas nécessaire, à l'intérieur d'un réseau unique et géré.

Par construction, il n'y a pas d'implémentation complète de ce RFC, mais des implémentations de certaines des fonctions. Par exemple, DS-Lite est mis en œuvre dans AFTR <`http://www.isc.org/software/aftr`>.