

RFC 5902 : IAB thoughts on IPv6 Network Address Translation

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 Juillet 2010

Date de publication du RFC : Juillet 2010

<http://www.bortzmeyer.org/5902.html>

Les mécanismes de traduction d'adresse (NAT) ont toujours suscité des polémiques, en raison de leur remise en cause des principes d'architecture de l'Internet. Avec IPv4, ces mécanismes sont nécessaires en raison de la pénurie d'adresses <<http://www.bortzmeyer.org/epuisement-adresses-ipv4.html>> qui fait que, par exemple, un particulier n'a aucune chance d'obtenir plus qu'une adresse IPv4, même s'il a chez lui plusieurs équipements IP. Mais en IPv6? La pénurie disparaît. Est-ce que le NAT doit donc disparaître avec elle? Dans ce RFC, l'IAB étudie la question et donne une réponse, certes hostile au NAT, mais très étayée et pointant du doigt quelques problèmes qui peuvent pousser certains à déployer du NAT IPv6 malgré tout.

La question initiale est pratique (section 1 du RFC) : l'IETF doit-elle normaliser des mécanismes de NAT pour IPv6? Elle ne l'avait pas fait pour IPv4, considérant, à juste titre, que c'était un bricolage ayant trop d'effets néfastes et, résultat, le NAT a quand même été largement déployé, de manière non standardisée. Le groupe de travail behave <<http://www.bortzmeyer.org/behave-wg.html>> de l'IETF a été créé bien plus tard pour essayer de documenter ce bricolage et ses conséquences, et pour trouver des solutions partielles à certains de ses inconvénients.

Évidemment, pas mal de participants à l'IETF craignent que la même chose se produise avec IPv6. Selon un scénario possible, l'IETF, attachée aux principes de l'adresse IP unique, de la neutralité du réseau, et de la transparence de bout en bout (RFC 4924¹), refuserait fermement de normaliser des solutions de NAT IPv6 et celles-ci seraient déployées quand même, menant à une prolifération de routeurs NAT différents et gardant l'actuel cauchemar que vivent les applications, notamment pair-à-pair. Mais la situation est-elle la même qu'avec IPv4?

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc4924.txt>

Les opposants à cette vision font remarquer que la motivation initiale du déploiement du NAT pour IPv4 était uniquement la pénurie d'adresses. (Je me souviens bien de mon émerveillement quand le premier routeur NAT utilisable, un PC Linux avec ce qui s'appelait à l'époque "*IP masquerading*", est apparu vers 1995. Soudainement, le particulier pouvait avoir plusieurs machines IP chez lui.) Cette pénurie disparaissant avec IPv6, la motivation du NAT disparaît aussi. Compte-tenu des défauts du NAT, où un équipement intermédiaire interfère avec la relation entre deux machines, il ne faudrait surtout pas déployer des NAT IPv6 et donc pas les normaliser.

Ce n'est pas et de loin la première fois que la question se pose. Ainsi, le RFC 4864 avait déjà discuté des avantages et inconvénients des NAT. Où en est-on aujourd'hui ?

Pour évaluer la possibilité que des systèmes de NAT soient déployés pour IPv6, même en l'absence de pénurie d'adresses, la section 2 du RFC étudie successivement les motivations possibles pour le NAT ou, en d'autres termes, les bénéfices perçus par certains utilisateurs.

Premier avantage perçu (section 2.1), dispenser de renumérotation. Avec un routeur NAT devant son réseau, celui-ci peut avoir des adresses IP stables, indépendantes des adresses vues de l'extérieur. Si celles-ci changent (par exemple parce qu'on a changé de fournisseur d'accès), il suffit de reconfigurer le routeur et tous les autres problèmes de renumérotation (RFC 5887) sont évités. Notre RFC 5902 note que cet argument saute si on dispose d'adresses PI mais que celles-ci posent d'autres problèmes, les mécanismes de routage actuels de l'Internet ne pouvant peut-être pas gérer un trop grand nombre de préfixes PI.

Autre motivation parfois citée pour déployer du NAT, le désir d'être "*multi-homé*" (section 2.2). Aujourd'hui, la seule solution qui isole le routage mondial du "*multi-homing*" est le NAT. Autrement, il faut utiliser des adresses PI qui sont routées globalement. Les techniques basées sur la séparation de l'identificateur et du localisateur <<http://www.bortzmeyer.org/separation-identificateur-localisateur.html>> ne sont pas encore prêtes. Donc, bien que la solution à base de NAT ne fournisse pas tous les services qu'on attend du "*multi-homing*" (par exemple, elle ne protège pas les sessions déjà établies d'une défaillance d'un des fournisseurs), elle reste tentante.

Pour un FAI, le NAT a un autre avantage : il permet d'homogénéiser la configuration des réseaux locaux des clients. Avec le NAT, tous les clients ont 192.168.0.0/24, tous les routeurs CPE ont l'adresse 192.168.0.1, etc. Cela peut simplifier le support utilisateur (section 2.3). En IPv6, un mécanisme équivalent serait d'utiliser les adresses locales au lien (section 2.5.6 du RFC 4291) mais il y a trop peu d'expérience pratique aujourd'hui pour juger de la validité de cette approche.

Lorsqu'on demande à un administrateur réseaux pourquoi il utilise du NAT alors qu'il dispose de suffisamment d'adresses, il répond souvent « la sécurité ». Cet argument est souvent vague et peu étayé. En creusant un peu, on peut trouver deux propriétés du NAT qui ont un rapport avec la sécurité. La première est le fait de dissimuler partiellement le réseau, sa structure et les machines qui s'y connectent (section 2.4). L'idée est que, sans faire reposer toute la sécurité du réseau sur cette dissimulation, on peut toutefois se dire qu'il n'y a aucune raison que le monde entier puisse analyser facilement le réseau, ce qui faciliterait la préparation d'une éventuelle attaque. Ainsi, le NAT permet de rendre plus difficile le recensement des machines (section 2.4.1). Cachées derrière le routeur NAT, les machines ne sont plus accessibles à un comptage, par exemple. Dans ce domaine, la plupart des administrateurs réseau surestiment beaucoup les protections fournies par le NAT. Un article comme « "*A technique for counting NATted hosts*" » <<http://www.cs.columbia.edu/~smb/papers/fnat.pdf>> montre bien que le NAT n'empêche nullement le recensement des machines. Des mécanismes de NAT plus complexes pourraient permettre de limiter certaines des attaques que décrit Bellovin (pas celles par "*fingerprinting*", par exemple) mais ils seront aussi plus difficiles à traverser pour des services comme SIP ou SCTP. La règle traditionnelle s'applique ici : les progrès de la sécurité se font presque toujours au détriment de la facilité

d'usage. Notre RFC détaille les contre-mesures possibles mais il n'en existe aucune de miraculeuse. La machine derrière le NAT ne doit donc pas se sentir en complète sécurité.

À défaut de cacher les machines, peut-on cacher la topologie du réseau (section 2.4.2)? Là encore, l'étude indique un résultat mitigé. On peut dans une certaine mesure rendre l'analyse du réseau interne plus difficile mais on ne peut pas la rendre impossible et ces améliorations de la dissimulation seront presque toujours au détriment des usages du réseau. Bref, comme le résume la section 2.4.3, le NAT fournit davantage une sécurité perçue qu'une sécurité réelle. Et les vrais gains de sécurité seront obtenus en empêchant les techniques de traversée de NAT comme STUN, ce qui diminuera l'utilité du réseau.

La deuxième propriété du NAT qui peut sembler augmenter la sécurité est l'impossibilité de faire une connexion depuis l'extérieur vers une machine NATtée (section 2.5). En fait, cette propriété n'a rien de spécifique au NAT : tout pare-feu à états en fait autant et il n'y a pas besoin du NAT pour avoir ce résultat.

Une fois examinées les bonnes (et moins bonnes) raisons de faire du NAT, même en IPv6, la section 3 de notre RFC prend de la hauteur et essaie de voir quelles sont les conséquences architecturales du NAT. Il n'y a pas de doute que le NAT a des avantages : si les gens le déploient, c'est bien qu'ils y trouvent des bénéfices. La vraie question est donc plutôt « Quel est le coût à payer, notamment pour les autres ? ». Le RFC ne mentionne pas cet exemple mais, aujourd'hui, le déploiement massif des NAT est payé essentiellement par les développeurs d'application (qui doivent consacrer beaucoup d'efforts et une grande partie de leur code réseau à contourner les NAT, à l'aide de solutions comme TURN - RFC 5766) et par les utilisateurs (dont certaines applications marchent ou ne marchent pas selon les spécificités du système NAT rencontré). L'administrateur réseaux qui déploie le NAT pour se faciliter la vie transmet donc les coûts à d'autres. Les RFC 2993 et RFC 4924 discutent plus en détail ce point.

Donc, avant de décider de normaliser un service de NAT, il ne faut pas seulement considérer les avantages perçus par ceux qui les déploient (la section 2 couvrirait ces avantages) mais aussi les conséquences globales. Le principe (qui est au cœur de l'architecture de l'Internet) est que deux machines qui **veulent** se parler (le pare-feu peut donc légitimement filtrer le trafic qu'on ne veut pas) doivent pouvoir le faire sans se soucier du NAT, c'est-à-dire sans avoir à déployer des solutions complexes comme ICE - RFC 5245. Le programmeur, au lieu de consacrer l'essentiel de son code à contourner les NAT, devrait pouvoir tenir pour acquise une connectivité de bout en bout. Des techniques comme la référence (j'indique l'adresse IP à laquelle la suite du trafic doit être envoyé) sont triviales avec l'architecture normale de l'Internet et cauchemardesques avec les NAT.

Bref, l'objectif est que le système NAT, s'il existe, n'aie un effet que purement local et pas, comme actuellement, des conséquences pour tous les utilisateurs. Est-ce possible ?

La section 4 regroupe les solutions qui permettent d'atteindre les avantages cités plus haut (notamment le "*multihoming*" et la non-nécessité de renuméroter) en **trois classes** :

- Adresses PI systématiques : très simple et marchant très bien, cette approche a pour principal inconvénient de faire porter un gros effort sur le système de routage mondial, qui doit gérer les adresses de tout le monde, sans possibilité d'agrégation. Le sujet a fait l'objet de nombreux travaux comme, par exemple, « "*Extending the Life of Layer 3 Switches in a 256k+ Route World*" <http://www.nanog.org/meetings/nanog44/presentations/Monday/Roisman_lightning.pdf> ».
- Adresses uniques et stables en local, mais utilisation d'un tunnel pour communiquer avec le reste du monde. C'est l'approche de la plupart des techniques comme LISP et elle est rare aujourd'hui.
- Adresses stables en local, avec traduction d'adresses avant d'atteindre l'Internet. C'est ce que fait le NAT et cette classe de solutions est la plus difficile à combiner avec la connectivité de bout en bout. C'est toutefois possible, si la traduction est réversible. (C'était le cas du NAT original, où toute adresse interne était mise en correspondance avec une et une seule adresse externe, mais c'est moins vrai avec les déploiements actuels, où les adresses IP globales sont partagées et où des numéros de port sont alloués dynamiquement pour désambiguer.)

Maintenant, place à la conclusion. La section 4.1 résume les pensées de l'IAB : le NAT est une mauvaise idée, car il est très difficilement compatible avec la transparence du réseau (RFC 4924), celle-ci étant la clé du succès de l'Internet. Mais certains problèmes (comme le "*Multihoming*") ne sont pas encore traités par l'IETF. Il ne suffit donc pas de dire que le NAT est négatif, il faut encore travailler à fournir des solutions pour les problèmes qu'il semble traiter. Dans tous les cas, toute évaluation d'une nouvelle norme (que ce soit du NAT ou pas) devrait se faire en priorité sur le critère de la transparence du réseau aux applications.