Le zoo des systèmes de traduction d'adresse IP

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 novembre 2010

http://www.bortzmeyer.org/nats.html

La réunion IETF 79 <http://www.ietf.org/meeting/79/> à Pékin a été l'occasion de mettre à jour mes connaissances sur les derniers progrès du jargon IETF et notamment d'apprendre la nouvelle liste des variantes du NAT, où des numéros indiquent la version d'IP utilisée.

On trouve ainsi :

— **NAT44** : un niveau de traduction, de IPv4 vers IPv4. C'est le NAT traditionnel, que Linux avait été le premier système à introduire, sous le nom de "*IP masquerading*". En raison du manque d'adresses IPv4 <http://www.bortzmeyer.org/epuisement-adresses-ipv4.html>, il n'y a en général qu'une seule adresse IP externe et le routeur ne fait donc pas de la réelle traduction d'adresses (NAT) mais de la traduction « adresse et port » (NAPT pour "*Network And Port Translation*"), il traduit les adresses internes en tuples adresse_externe+port. C'est ce NAT44 dont les inconvénients sont décrits dans les RFC 2663[1], RFC 3424 et RFC 5128 et pour lequel le groupe de travail Behave v1 <http://www.bortzmeyer.org/behave-wg.html> a proposé plusieurs bonnes pratiques qui limitent les dégâts (cf. RFC 4787, RFC 5382, RFC 5508, etc). C'est lui qui impose aux serveurs publics de désormais journaliser le port en même temps que l'adresse <http://www.bortzmeyer.org/loguer-adresse-et-port.html> (autre gros sujet de discussion à Pékin)

— **NAT46** et **NAT64** sont les cas où on traduit de IPv4 en IPv6 (cas d'un réseau ancien qui accède à un Internet IPv6) ou réciproquement (cas d'un réseau récent qui veut accéder à l'Internet traditionnel). C'est cette technique qui était normalisée à l'origine dans le RFC 2766 (abandonné par la suite car trop complexe) et qui fait désormais l'attention du groupe de travail Behave v2 <http://tools.ietf.org/wg/behave/>, qui a produit des RFC normalisant l'utilisation de la traduction d'adresses pour faire coexister IPv4 et IPv6 (RFC 6052, RFC 6144, etc). Notons que le mécanisme de transition envisagé à l'origine, la double-pile (toutes les machines ont une adresse IPv4 **et** une adresse IPv6, tant que la transition dure), a été annulé par l'insuffisant déploiement d'IPv6 <http://www.bortzmeyer.org/ipv6-et-l-echec-du-marche.html> (cf. RFC 5211).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2663.txt

— Mais, désormais, on applique la logique Shadok à son maximum : « pourquoi faire simple quand on peut faire compliqué ? » C'est ainsi qu'est né le **NAT444**, technique déjà largement déployée par des FAI, notamment en Asie et Afrique. Il s'agit ici d'avoir deux niveaux de traduction successifs, entre le réseau local de l'utilisateur et celui du FAI, puis entre celui du FAI et l'Internet. Le RFC 5684 expose en détail les conséquences néfastes que cela peut avoir, si les adresses privées des deux côtés sont dans le même préfixe. Une bonne partie des discussions à la réunion IETF de Pékin tournait autour de la demande de réservation d'un préfixe /10 pour l'adressage des réseaux internes des FAI, limitant ainsi certains des risques évoqués par ce RFC. Autre problème avec NAT444, s'il existe des mécanismes standard permettant à une machine de détecter son adresse IP publique (RFC 5389), l'adresse intermédiaire, elle, est complètement invisible.
— Quant à **NAT66**, il s'agit de traduction entre IPv6 et IPv6 (RFC 6296). Cette fois, vue l'abondance des adresses IPv6, on peut faire de la vraie traduction d'adresses, sans numéro de port, chaque adresse interne correspondant à une et une seule adresse externe. Mais, justement, puisque les adresses IPv6 sont abondantes, pourquoi diable faire du NAT ? Eh bien certaines personnes croient voir des avantages au NAT, même sans qu'il y ait de pénurie d'adresses (par exemple, une légende fréquente est que le NAT améliore la sécurité). Un RFC de l'IAB, le RFC 5902 détaille ainsi la question du NAT sur IPv6 et explique que, bien que ce soit une mauvaise idée, il faut sans doute s'attendre à le voir arriver. En tout cas, c'est bien plus facile à programmer (pas besoin de conserver un état, il suffit juste de remplacer une adresse par une autre) comme le montre le programme C (en ligne sur `http://www.bortzmeyer.org/files/ropitault-nat66.tar.gz`) dû à Tanguy Ropitault (merci !).
— Encore plus amusant à déboguer, **NAT464** et **NAT646**, pas encore déployés, et qui permettraient, pour le premier, de connecter le réseau local IPv4 du client (IPv4, car rempli de vieilles machines n'ayant que v4) au réseau IPv6 du FAI (pour le cas d'un FAI récent qui n'a pas eu d'allocation v4 du tout) puis à l'Internet traditionnel resté v4 et, pour le second mécanisme, NAT646, à un réseau local composé d'objets récents purement v6, de se connecter au réseau d'un FAI traditionnaliste resté en v4 et de là à un Internet passé en v6.
— Et pourquoi s'arrêter en si bon chemin ? Comme personne n'ose dire aux bricoleurs qu'ils travaillent salement, cela peut continuer, et on verra peut-être apparaître du **NAT4444** (trois niveaux de traduction)...

Bref, c'était plus simple avant. Le modèle IP tel qu'il était enseigné aux débutants (adresse IP unique au niveau mondial, connectivité de bout en bout (toute machine IP peut envoyer un paquet à toute autre qui le désire), et transparence du réseau (le paquet ne sera pas modifié en cours du route), ce modèle dont la simplicité est largement responsable du succès de l'Internet, est désormais très menacé, pour le plus grand plaisir de ceux qui n'ont jamais vraiment accepté que les machines et, derrière elles, leurs utilisateurs, puissent communiquer facilement.