Le groupe de travail BEHAVE de l'IETF

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 janvier 2008

https://www.bortzmeyer.org/behave-wg.html

L'IETF, comme les autres acteurs de l'Internet, se pose depuis longtemps la question de l'attitude à adopter face au déploiement massif du NAT. Cette technique, qui permet de ne pas donner aux machines situées derrière le routeur NAT une « vraie » connectivité Internet, est très répandue. Au fur et à mesure de l'épuisement des adresses IPv4 <http://www.ripe.net/ripe/meetings/ripe-55/presentations/huston-ipv4.pdf>, on voit de plus en plus de FAI qui connectent leurs clients ainsi. À la maison, l'abonné moyen n'a, depuis longtemps, qu'une seule adresse IPv4 et donc pas beaucoup d'autres choix que le NAT (ou les relais applicatifs, qui posent des problèmes analogues). Or, le NAT brise le modèle de « connectivité de bout en bout » qui est à la base de l'Internet. Pour cette raison, et d'autres, il est très mal vu chez les concepteurs et implémenteurs de protocoles. Que doivent faire ceux-ci dans un monde où le NAT est si répandu ? C'est tout l'objet du groupe de travail BEHAVE <http://tools.ietf.org/wg/behave>.

En présence du NAT, les application strictement client/serveur comme le Web fonctionnent encore assez bien, lorsque le serveur n'est pas lui-même derrière un routeur NAT. Par contre, les applications pair-à-pair, où chacun doit pouvoir contacter chacun, ou bien les protocoles pour le multi-média comme SIP (RFC 3261 [1]), où l'appelé doit pouvoir envoyer son flot de données à l'appelant, sont très handicapés. Les programmes mettant en œuvre ces protocoles consacrent une grande partie de leur code à contourner les NAT. Divers bricolages sont parfois nécessaires pour que le monde extérieur puisse parler aux machines bloquées derrière le routeur NAT (par exemple le "*port fowarding*" comme documenté ici pour un routeur Linux <https://www.bortzmeyer.org/emule-ports-linux.html>). Bref, le NAT fait faire des économies aux opérateurs <https://www.bortzmeyer.org/ipv6-et-l-echec-du-marche.html> Internet (à qui il évite de déployer IPv6) mais coûte cher aux autres acteurs.

Aujourd'hui, le NAT est tellement largement déployé que, même si plus aucune installation n'était faite, l'Internet devrait vivre avec pendant des années. Alors, que doit faire un organisation de normalisation comme l'IETF ? Comme le NAT met en cause la connectivité de bout en bout, il est largement

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3261.txt

considéré à l'IETF comme un mal à éradiquer. Comme on ne pactise pas avec le mal, l'opinion dominante à l'IETF était qu'il ne fallait pas chercher à limiter les dégâts, à améliorer le NAT, puisqu'il ne méritait que d'être supprimé. Même la normalisation des moyens de contournement du NAT (rapidement apparus, vue la créativité des développeurs réseaux face aux obstacles) a été pendant longtemps tenue en suspicion. En novembre 2002, l'IAB, dans le RFC 3424 appelait ces moyens de contournement « UNSAF » ("*UNilateral Self-Address Fixing*"), laissant entendre que le danger venait d'eux et pas du NAT, et imposant dans sa section 4 une série de questions auxquelles devaient répondre tous les protocoles de contournement. Le but était d'éviter que le remède soit pire que le mal, que le NAT, mais cela revenait à jeter une suspicion contre ceux qui cherchaient à trouver des solutions partielles, comme STUN.

Finalement, c'est en septembre 2004 qu'a été créé le groupe de travail BEHAVE <`http://www.ietf.org/html.charters/behave-charter.html`>, avec une charte très prudente qui lui intimait de « ne pas encourager le déploiement de NAT » comme si le développement de la médecine encourageait les maladies. On touche là à un problème presque philosophique : tenter de soulager la misère du monde détourne t-il de la réalisation de changements de fond ?

BEHAVE a travaillé sur les points suivants :

— Un travail de documentation et de classification des NAT (une partie du RFC 4787 et l'"*Internet-Draft*" `draft-ietf-behave-p2p-state`, qui est notament axé sur le pair-à-pair).
— Un protocole de base, STUN (RFC 5389) servant aussi bien à la découverte du comportement d'un routeur NAT ("*Internet-Draft*" `draft-ietf-behave-nat-behavior-discovery`) qu'à la traversée des NAT par les applications, par la technique du "*hole punching*" (la description de cette technique n'est pas faite par BEHAVE mais dans d'autres groupes de travail, plus orientés applications). Une extension de STUN, TURN (RFC 5766) normalise le relais de toute la session via un serveur extérieur, ce qui sera normalement le « dernier recours » pour communiquer, si les deux pairs sont coincés derrière des routeurs NAT peu coopératifs.
— Une série de règles auxquelles devraient idéalement obéir les routeurs NAT, pour que les techniques ci-dessus arrivent encore à fonctionner (RFC 4787, RFC 5382, RFC 5508).

BEHAVE a terminé plusieurs RFC dont les RFC 4787 (UDP), RFC 5135 et RFC 5382 (TCP).

Le groupe de travail a été depuis réorienté pour travailler sur les NAT dans le contexte de la coexistence d'IPv4 et IPv6. Son expertise sur les NAT44 lui a permis de normaliser rapidement NAT64 (cf. RFC 6144).