

# RFC 4787 : Network Address Translation (NAT) Behavioral Requirements for Unicast UDP

Stéphane Bortzmeyer  
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 Février 2007

Date de publication du RFC : Janvier 2007

<http://www.bortzmeyer.org/4787.html>

---

En raison, notamment, de la pénurie d'adresses IPv4, de nombreux réseaux utilisent le NAT. Cette technique est très pénalisante et notre RFC essaie de limiter les dégâts en notant le comportement minimal d'une mise en œuvre de NAT qui ne perturbe pas trop les applications.

Si les applications TCP traditionnelles, comme le Web ou SSH passent en général bien à travers le NAT, en sortie, ce n'est pas le cas des applications multimédia comme SIP (RFC 3261<sup>1</sup>) ou bien liées aux jeux en ligne. Celles-ci dépendent souvent d'UDP et ne passent pas à travers beaucoup de systèmes NAT. Plusieurs techniques ont été mises au point pour traverser ces systèmes proprement mais elles ne marchent pas toujours car il n'y a pas un seul type de NAT mais plusieurs. (Sur ces différents types, voir le RFC 2663, la terminologie du RFC 3489 n'ayant pas été retenue.)

Notre RFC, issu du travail du groupe de travail BEHAVE <<http://www.bortzmeyer.org/behave-wg.html>>, définit donc les comportements suivants, que doit respecter le système NAT :

- Indépendance par rapport à la destination: la table de correspondance entre un port et un couple (adresse IP, port) ne doit dépendre que de la source,
- Si le système NAT a plusieurs adresses IP de sortie à sa disposition, il doit utiliser la même pour toute requête provenant d'une adresse IP interne donnée,
  - Le système NAT ne doit pas réutiliser un port pour une communication différente,
  - Plus surprenant, un système NAT doit préserver la parité du port (si une requête d'une machine interne vient d'un port pair, elle doit sortir avec un port source pair, certaines applications en dépendent),
  - Le système NAT doit être déterministe, c'est-à-dire que ses choix doivent être répétables (il ne doit donc pas choisir un port au hasard, par exemple),
  - Le système NAT doit permettre le fonctionnement en épingle à cheveux ("*hairpinning*") où deux machines situées du même côté du routeur tentent de communiquer. Beaucoup de routeurs NAT ne permettent pas cette communication (section 6).
  - Et plusieurs autres obligations ou recommandations, toutes étant résumées dans la section 12, celle que tout implémenteur d'un système NAT devrait lire, s'il ne lit rien d'autre du RFC.
- Un très bon article pour faire le point sur les techniques permettant de contourner le NAT est "*Peer-to-Peer Communication Across Network Address Translators*" <<http://pdos.csail.mit.edu/papers/p2pnat.pdf>>.

---

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