

RFC 5382 : NAT Behavioral Requirements for TCP

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 Octobre 2008

Date de publication du RFC : Octobre 2008

<http://www.bortzmeyer.org/5382.html>

Comme son compagnon, le RFC 4787¹, qui concerne UDP, ce RFC décrit les règles que doit suivre un routeur NAT pour être utilisable sans trop de problèmes par les applications TCP.

La lecture préalable du RFC 4787 est recommandée, car il fixe le vocabulaire et les principes généraux. Notre RFC les complète ensuite pour le cas de TCP.

TCP a beaucoup évolué depuis le début (cf. le RFC 4614 pour une bonne description de cette évolution) mais le mécanisme de connexion initial, le fameux « *Three-Way handshake* », n'a pas changé, des tentatives comme T/TCP (cf. RFC 1644) ayant échoué. C'est cette connexion initiale qui est le plus gênée par le NAT.

Les exigences de notre RFC pour un routeur NAT sont principalement :

- 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,
- Le routeur doit accepter la totalité de la machine à états de TCP (décrite dans le RFC 793) et notamment, ce que beaucoup de routeurs NAT ne font pas, l'ouverture simultanée (où deux machines tentent une connexion TCP à peu près en même temps),
- Les éventuels délais avant qu'une session TCP « inactive » soit coupée doivent être d'au moins deux heures (aujourd'hui, il est courant que des routeurs NAT suppriment une connexion de leur table au bout de quelques minutes, car leurs concepteurs n'ont pensé qu'aux sessions HTTP, jamais à SSH, où il est courant qu'une session dure des jours et n'envoie pas de paquets tout le temps).

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc4787.txt>