

Options IP interdites en pratique

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 juin 2008

<http://www.bortzmeyer.org/options-interdites.html>

Il devient de plus en plus difficile de déployer de nouvelles techniques sur l'Internet, en raison de coupe-feux excessivement zélés qui bloquent tout ce qu'ils ne connaissent pas. L'Internet s'ossifie, peut-être jusqu'au point où il faudra un nouveau réseau pour retrouver cette possibilité de déploiement de nouvelles techniques. Une étude de chercheurs de Berkeley montre ainsi que les options IP sont bloquées dans environ la moitié des cas.

Le protocole IPv4, normalisé dans le RFC 791¹, prévoit dans la section 3.1 du RFC l'ajout éventuel d'options dans l'en-tête du paquet IP. Ces options étaient prévues pour permettre certaines fonctions supplémentaires (le RFC 791 en normalisait quatre). En théorie, toute implémentation d'IP doit les reconnaître.

Et en pratique? Bien des fonctions parfaitement standards, normalisées depuis des années, comme ECN (RFC 3168) sont, en pratique, inutilisables car filtrées par beaucoup de routeurs. Un groupe de chercheurs a donc cherché ce qu'il en était des options IP et leur conclusion, publiée dans l'article "*IP Options are not an option*" <<http://www.eecs.berkeley.edu/Pubs/TechRpts/2005/EECS-2005-24.pdf>> est inquiétante : environ la moitié des chemins entre deux machines jettent les paquets IP ayant une option.

Comment ont-ils mesuré? Ils sont partis du réseau PlanetLab, qui comprend de nombreuses machines un peu partout dans le monde. Entre chaque couple de machines, ils ont tenté d'envoyer des paquets IP avec et sans option (et avec diverses options) et ont compté les cas où le paquet sans option arrivait, mais pas le paquet avec option.

Leur étude approfondit ce résultat en montrant également que le paquet est en général jeté près du point de départ ou bien d'arrivée, c'est-à-dire aux franges de l'Internet, pas dans les réseaux des grands opérateurs.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc791.txt>

À noter que, bien que IPv6 soit mentionné dans leur étude, les tests ont été effectués uniquement en IPv4. Il serait intéressant de voir ce que cela donne en v6 puisque le mécanisme d'options est complètement différent. En IPv4, tout paquet avait un champ Options, et de longueur variable, ce qui est très pénible à analyser rapidement pour les routeurs. En IPv6, les options (RFC 2460, section 4.2) sont en dehors de l'en-tête, dans une « extension d'en-tête ».

Une analyse équivalente pour TCP, pas plus optimiste, se trouve dans l'excellente étude de Google "*Probing the viability of TCP extensions*" <<https://www.imperialviolet.org/binary/ecntest.pdf>>.