

RFC 4924 : Reflections on Internet Transparency

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 Août 2007

Date de publication du RFC : Juillet 2007

<http://www.bortzmeyer.org/4924.html>

Ce RFC nommé « Réflexions sur la neutralité de l'Internet » est essentiellement consacré à un rappel de l'importance qu'il y a à ne pas préjuger des usages et des applications. L'Internet doit rester transparent c'est-à-dire traiter de la même façon tous les paquets IP, sans privilégier certaines applications. C'est cette transparence qui a permis le développement spectaculaire de nouvelles applications et qui est aujourd'hui menacée.

Aujourd'hui, cette transparence est sérieusement menacée. Par exemples, certains opérateurs voudraient traiter de manière privilégiée certaines applications, ou au contraire contrarier certaines, comme la téléphonie sur IP, qui s'attaque à leur marché le plus rentable. C'est contre cette tendance que s'est développé le courant qui défend la neutralité du réseau.

Mais il y a d'autres menaces, par exemple, le déploiement de plus en plus fréquent de mécanismes qui empêchent la connexion de bout en bout, que ce soit :

- le NAT pour pallier le manque d'adresses IPv4,
- les coupe-feux mis au nom de la sécurité,
- ou, pire, certains FAI qui redirigent discrètement les paquets, bloquent certains ports comme le 25 (SMTP) ou modifient les réponses DNS dans les récuseurs qu'ils offrent à leurs clients.

Notre RFC est donc consacré à l'analyse de ces problèmes et à un rappel de leur caractère négatif. En effet, le fait que l'Internet soit un réseau **neutre**, un "*oblivious transport*" (terme utilisé dans le rapport "*New Arch*" <<http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf>>, que cite notre RFC), un simple transporteur de paquets, qui ne se permet pas de les examiner ou de les modifier, est l'un des points les plus importants de l'architecture de ce réseau. C'est ce point qui permet le développement d'applications nouvelles et non planifiées dès l'origine. L'exemple archétypal est bien sûr le Web, non prévu à l'origine de l'Internet et qui a pu être déployé progressivement ; sur un réseau transparent, il suffit que deux machines soit d'accord et elles peuvent tout de suite commencer à utiliser le nouveau protocole.

À l'opposé des réseaux transparents se trouvent des réseaux ossifiés comme les réseaux des opérateurs téléphoniques, liés à une seule application et ne permettant donc pas l'innovation, puisque tout changement doit être approuvé et mis en œuvre par l'opérateur.

L'Internet, traditionnellement transparent, devient de plus en plus ossifié. C'est ainsi que les routeurs NAT et les coupe-feux qui examinent le contenu des paquets ne laissent guère de chance à des nouveaux protocoles de transport comme SCTP (RFC 3286¹) d'être déployés. De même, les nouvelles applications sont souvent obligées de « tricher » en passant au dessus de HTTP, de façon à franchir les coupe-feux.

Il est temps de réagir. Ce RFC n'est pas le premier document sur la question, le pionnier avait été le RFC 2775 et notre nouveau RFC se consacre surtout aux nouveautés. Il décrit les facteurs qui s'opposent à la transparence comme le filtrage (section 2.1), d'autant plus problématique que très rares sont les FAI qui publient leur règle de filtrage, malgré le RFC 4084, certaines utilisations de la QoS (section 2.2), les passerelles applicatives (ALG, section 2.3), puisqu'elles doivent être mises à jour pour tout changement du protocole applicatif, mais aussi la manipulation des réponses DNS (section 2.5.2).

Certains FAI (apparemment, aujourd'hui, en France, Noos, Club-Internet et Tiscali) modifient les réponses DNS reçues par les serveurs faisant autorité. Typiquement, ils remplacent les réponses NXDOMAIN ("No Such Domain", ce nom de domaine n'existe pas) par une adresse IP prédéterminée où un serveur Web leur propose moteur de recherche et publicités. Le RFC note que, outre leur incompatibilité avec DNSSEC, ces manipulations cassent le modèle de référence du DNS (qui est que le gérant d'une zone est l'autorité suprême sur le contenu de la zone).

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc3286.txt>