Une étude des « boxes » qui connectent notre maison à l'Internet

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 septembre 2010

http://www.bortzmeyer.org/home-gateway.html

Nos réseaux à la maison sont connectés via des « "*boxes*" », fournis par le FAI ou bien choisies et installées par nous, et dont il n'est pas facile de donner une définition précise. Routeur ? Commutateur ? Pare-feu ? Modem ? C'est en fait un peu de tout ça. Non seulement la "*box*" typique ne respecte pas le modèle en couches mais elle ne documente en général pas exactement ce qu'elle fait, et, étant en général munie d'un logiciel programmé avec les pieds par des anonymes, elle le fait souvent mal. La "*box*" typique ne respecte pas les RFC, même ceux qui visent spécifiquement ce genre d'équipements (comme les RFC 5625 [1] ou ceux du groupe Behave <http://www.bortzmeyer.org/behave-wg.html> comme le RFC 5383). D'où cette étude de chercheurs, notamment finlandais, qui essaie de déterminer expérimentalement les caractéristiques d'un certaine nombre de "*boxes*" qu'on trouve sur le marché en Europe (des D-Link, des Netgear, des Linksys, etc).

L'article se nomme « "*An Experimental Study of Home Gateway Characteristics*" <https://fit.nokia.com/lars/papers/2010-imc-hgw-study.pdf> » par Seppo H[Caractère Unicode non montré [2]]t[Caractère Unicode non montré]nen, Aki Nyrhinen, Lars Eggert, Stephen Strowes, Pasi Sarolahti et Markku Kojo. Un exposé résumant ses conclusions avait été fait à la réunion IETF 78 à Maastricht et les transparents sont en ligne <http://www.ietf.org/proceedings/78/slides/behave-8.pdf> (les graphiques y sont plus clairs que dans l'article, notamment avec l'ajout des recommandations IETF)..

Il y a déjà eu plusieurs études du même genre, par exemple dans le contexte de DNSSEC, comme celle pour le SSAC de l'ICANN <https://www.icann.org/committees/security/sac035.pdf> (la section 2 de l'article donne une bonne liste des études analogues.) Dans l'étude « finlandaise », 34 "*boxes*" ont été achetées et installées dans un réseau, entre une machine « cliente » et une machine « serveur », toutes les deux utilisant Linux. Le client a une adresse privée, et se connecte en IPv4 au serveur via la fonction NAT de la "*box*" (section 3).

Que montre cette étude ? Je ne citerai pas tous les résultats mais, parmi les plus intéressants :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5625.txt
2. Car trop difficile à faire afficher par LaTeX

— Lors de « connexions » en UDP, la durée pendant laquelle une correspondance est gardée (en l'absence de toute communication) dans la table du NAT (ce qui permet donc aux réponses de revenir au client) varie de 30 à 700 secondes (le RFC 4787, section 4.3, demande un minimum de 120 secondes).
— Pour TCP, c'est un peu mieux, avec des "*timeouts*" variant de 240 secondes à une durée inconnue (les auteurs de l'article ont attendu 24 heures sans que la connexion soit coupée). La moitié des "*boxes*" ne respectent pas le minimum du RFC 5382, section 5 (deux heures, quatre minutes).
— La réécriture des messages ICMP (qui peuvent inclure des adresses IP qui n'ont pas de sens en dehors du domaine de routage local, à cause du NAT) varie beaucoup d'une "*box*" à l'autre, là encore en ignorant les recommandations du RFC 5508, section 4.2.
— Une des plaies des "*boxes*" est qu'elles contribuent à l'ossification de l'Internet. Peu d'entre elles opèrent comme de purs routeurs, qui font passer des paquets IP en toute transparence, sans se soucier de ce qu'ils portent. Il est donc très difficile de déployer dans l'Internet un nouveau protocole de transport. Ainsi, un service qui serait accessible uniquement en SCTP (protocole probablement meilleur que le traditionnel TCP dans beaucoup de cas, cf. RFC 4960) ne serait pas joignable depuis beaucoup de réseaux. En effet, la moitié des "*boxes*" du test ne laissent pas du tout passer SCTP. (Les auteurs de l'article se réjouissent néanmoins de ce résultat, car ils s'attendaient à bien pire.) En revanche, DCCP (concurrent d'UDP normalisé dans le RFC 4340) ne passe à travers aucune des "*boxes*".
— Enfin, les auteurs ont fait des tests DNS (la plupart des "*boxes*" relaient le DNS, au lieu de le laisser passer intact) et trouvent à peu près les mêmes résultats que dans les études qui avaient précédé le déploiement de DNSSEC (par exemple, moins de la moitié des "*boxes*" accepte de faire du DNS sur TCP).

Y aurait-il d'autres résultats avec les "*boxes*" distribuées directement par les FAI comme la Livebox ou la Freebox ? D'abord, rien ne dit que ces "*boxes*" sont différentes de celles qu'on trouve en supermarché. Bien souvent, le FAI a juste mis son logo sur une "*box*" standard. Pour le cas où le FAI construit réellement sa "*box*" (cas de la Freebox), il faudrait tester pour être sûr. Cela serait certainement un test intéressant mais pas forcément facile ; par exemple, la Freebox utilise un protocole non-standard pour se connecter au réseau et ne rentrerait donc pas bien dans le banc de test fait par les chercheurs finlandais. (J'ai juste regardé que, sur ma Freebox v5, les paquets SCTP sortent bien, avec une adresse IP source NATée.)

Bref, des résultats peu satisfaisants, voire catastrophiques. Une des conséquences pratiques de cette mauvaise gestion, par la plupart des "*boxes*", de tout ce qui est considéré comme inhabituel (comme DCCP) est que le succès de nouveaux protocoles ou services dans l'Internet (SCTP, DNSSEC, IPv6) est rendu presque inatteignable.

Merci à Alexandre Archambault pour ses pertinentes remarques. Un expert anonyme ayant fait des remarques sur un blog, il y a une bonne réponse d'un des auteurs de l'article <http://serendipity.ruwenzori.net/index.php/2010/09/25/a-critical-opinion-of-nokias-experimental-study-of-

---

http://www.bortzmeyer.org/home-gateway.html