RFC 5625 : DNS Proxy Implementation Guidelines

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 août 2009

Date de publication du RFC : Août 2009

https://www.bortzmeyer.org/5625.html

La connexion à l'Internet typique du particulier ou de la petite entreprise passe aujourd'hui par une boîte aux fonctions mal définies. Parfois, celle-ci assure, parmi ses autres tâches, le rôle d'un relais DNS. Et ces relais, programmés en général avec les pieds par un stagiaire en Chine, violent souvent les règles du protocole DNS, et causent d'innombrables problèmes. Ce RFC dresse la liste des problèmes potentiels et formule les règles que doivent suivre les relais pour ne pas trop casser le DNS. Cela servira, pour le cas improbable où les bricoleurs qui écrivent le logiciel de ces boîtes lisent les RFC...

Ces « boîtes » sont parfois nommées "*box*" (en anglais, ça fait plus sérieux) parfois « décodeurs » (en souvenir de Canal+, première entreprise qui a réussi à mettre des boîtes chez ses clients), parfois « modem », parfois « routeur », ce qui est techniquement souvent correct, mais insuffisant, vue la variété des fonctions qu'elles assurent. Au minimum, la « boîte » devrait faire passer les paquets IP d'un côté à l'autre (du réseau local vers celui du FAI et réciproquement). Mais, pour des raisons comme celles expliquées par le RFC dans sa section 5.3, beaucoup de boîtes s'arrogent des rôles comme celui de relais DNS, rôle qu'elles remplissent mal.

La section 1 du RFC rappelle l'excellente étude <https://www.icann.org/committees/security/sac035.pdf> qu'avait fait le même auteur, Ray Bellis, employé du registre de .uk, pour le compte du SSAC de l'ICANN : cette étude, et celle du registre DNS suédois <http://www.iis.se/docs/Routertester_en.pdf>, montraient que la grande majorité des boîtes existantes, dans leur configuration par défaut) violaient largement le protocole DNS et qu'elles contribuaient ainsi à l'**ossification** de l'Internet (le fait qu'on ne puisse plus déployer de nouveaux services car les boîtes intermédiaires abusent de leur rôle et bloquent ce qu'elles ne comprennent pas). Des nouveaux services comme DNSSEC risquent donc d'être très difficiles à installer.

La boîte qui fait relais DNS (et pas simplement routeur IP, comme elle le devrait) n'a en général pas un vrai serveur DNS, avec capacités de cache et gestion complète du protocole. Elle est un être intermédiaire, ni chair, ni poisson, violant le modèle en couches, et dépend des résolveurs du FAI auquel

elle transmet les requêtes. Le RFC commence donc par recommander de ne **pas** utiliser de tels relais. Néanmoins, s'ils existent, il faudrait au minimum qu'ils suivent les recommandations du document.

La section 3 remet ces recommandations dans le contexte du **principe de transparence**. Un relais DNS ne peut espérer mettre en œuvre **toutes** les fonctions du DNS, surtout celles qui n'existent pas encore. En effet, la boîte a en général des ressources matérielles assez limitées, elle n'a souvent pas de mécanisme de mise à jour simple, ce qui veut dire qu'elle tournera toute sa vie avec le même code, et son interface de configuration doit idéalement être simple.

Alors, le relais, puisqu'il ne peut pas gérer complètement le DNS, devrait le laisser en paix. L'étude du SSAC montrait que, plus la boîte joue un rôle actif dans le protocole DNS, plus elle fait de bêtises. Le relais devrait donc juste prendre les paquets d'un côté et les envoyer de l"autre, sans jouer à les interpréter, ce qu'il fait toujours mal. Et, dans tous les cas, le RFC recommande que les machines du réseau local puissent écrire directement au résolveur DNS de leur choix, si celui de la boîte est vraiment trop mauvais (ce n'est pas toujours possible, par exemple dans les hôtels où le port 53, celui du DNS, est souvent filtré).

Dans le cadre de ce principe de transparence, la section 4 du RFC détaille ensuite point par point toutes les règles à respecter particulièrement. Ainsi, la section 4.1 rappelle que les relais ne doivent pas jeter un paquet DNS simplement parce que des options inconnues apparaissent dans celui-ci. Beaucoup de boîtes jettent les paquets où les bits AD ("*Authentic Data*") ou CD ("*Checking Disabled*") sont à un, simplement parce qu'ils n'existaient pas à l'époque du RFC 1035 [1] (section 4.1), le seul que le stagiaire qui a programmé la boîte a lu (quand il en a lu un). (Ces bits sont dans la plage "*Reserved for future use*", notée Z.)

De même, certaines boîtes ne laissent pas passer les types d'enregistrement inconnus, la section 4.3 rappelle donc, suivant le RFC 3597 qu'une mise en œuvre correcte du DNS doit laisser passer les types inconnus, sinon il sera impossible de déployer un nouveau type.

Un autre point sur lequel les logiciels des boîtes (mais aussi beaucoup de pare-feux) sont en général défaillants est celui de la taille des paquets DNS <https://www.bortzmeyer.org/dns-size.html>. Là encore, si le programmeur a lu un RFC (ce qui est rare), il s'est arrêté au RFC 1035, sans penser que, depuis vingt-deux ans qu'il existe, des mises à jour ont peut-être été faites et que la taille maximum de 512 octets n'est donc plus qu'un souvenir. La section 4.4 doit donc rappeler que les paquets DNS ne sont **pas** limités à 512 octets et que des réponses de plus grande taille sont fréquentes en pratique. Le relais doit donc gérer TCP correctement (section 4.4.1), et accepter EDNS0 (section 4.4.2, voir aussi le RFC 6891..

Les boîtes maladroites peuvent aussi interférer avec la sécurité. La section 4.5 rappelle que TSIG (RFC 2845) peut être invalidé si la boîte modifie certains bits des paquets (ce qui existe) ou bien retourne des réponses non signées à des requêtes signées (ce qui est courant sur les points chauds Wifi).

Une autre section, la 5, couvre les questions de l'interaction avec DHCP. La plupart du temps, la machine de M. Toutlemonde obtient l'adresse IP du résolveur DNS via DHCP (option 6, "*Domain Name Server*", RFC 2132, section 3.8). La plupart des boîtes indiquent leur propre adresse IP ici. Et, en général, il n'est pas possible de modifier ce paramètre (par exemple, la Freebox ne permet pas d'indiquer un autre serveur DNS, choisi par le client ; même chose chez SFR <http://www.justneuf.com/

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1035.txt

Configurer-Dhcp-Neufbox-Pour-viter-Dns-Menteurs-Sfr-t103181.html>). La seule solution pour court-circuiter le service DNS par défaut est donc d'indiquer en dur les résolveurs souhaités, dans la configuration de chaque machine. La section 5.1 appelle donc à une option de la boîte permettant de changer les serveurs DNS annoncés.

DHCP permet également une option indiquant le nom de domaine du réseau (option 15, section 3.17 du RFC 2132) et la section 5.2 du RFC 5625 demande qu'elle soit vide par défaut, en l'absence d'un domaine local normalisé <https://www.bortzmeyer.org/pourquoi-le-tld-local-n-est-pas-une-bonne-ide
html>.

La section 5.3 est consacrée à une discussion sur la durée du **bail** DHCP. Une des raisons pour lesquelles beaucoup de boîtes indiquent leur propre adresse IP comme résolveur DNS est que, au démarrage, la boîte ne connait pas forcément les adresses des résolveurs DNS du FAI. Mais cette technique oblige ensuite la boîte à agir comme relais DNS, ce qui est précisément la source de beaucoup de problèmes. Une solution possible, suggérée par notre RFC, est d'annoncer l'adresse IP de la boîte avec une durée de bail ultra-courte, tant que la boîte n'est pas connectée à l'Internet, puis d'annoncer les résolveurs du FAI ensuite, avec une durée de bail normale.

Les interférences provoquées par les boîtes mal conçues peuvent aussi avoir un impact sur la sécurité. C'est l'objet de la section 6. Il y a des boîtes qui, ignorant le RFC 5452, réécrivent le "*Query ID*", rendant ainsi les utilisateurs davantage vulnérables à la faille Kaminsky <https://www.bortzmeyer.org/comment-fonctionne-la-faille-kaminsky.html> (section 6.1). Il y en a qui répondent aussi aux requêtes DNS venues du WAN, permettant ainsi les attaques décrites dans le RFC 5358 (section 6.2).

Bref, les relais DNS des boîtes sont souvent plus dangereux qu'utiles. Le principe d'ingéniérie simple « si vous voyez un système inconnu, **bas les pattes** » est malheureusement très largement ignoré dans l'Internet. Pourquoi ? Pour les boîtes, il y a plusieurs raisons, typiquement liées à l'isolement complet dans lequel vivent les programmeurs anonymes de ces machines. Au contraire des logiciels libres comme Unbound ou BIND, dont les auteurs participent régulièrement à la communauté DNS, les programmeurs des boîtes sont inconnus, ne fournissent pas d'adresse pour leur envoyer des rapports de bogue ou de remarques. Pas étonnant, dans ces conditions, que le logiciel soit de mauvaise qualité.

Les abonnés à Free noteront que la Freebox n'a pas les problèmes mentionnés dans le RFC puisqu'elle est purement routeur, elle ne sert pas de relais DNS. Les serveurs DNS qu'elle indique en DHCP sont situés derrière elle, dans les salles de Free.