RFC 5772 : A set of possible requirments for a future routing architecture

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 février 2010

Date de publication du RFC : Février 2010

https://www.bortzmeyer.org/5772.html

Ce RFC qui expose un cahier des charges pour le routage global de l'Internet est essentiellement un document historique. Écrit il y a pas mal d'années, il est publié aujourd'hui (avec quelques mises à jour et annotations) dans le cadre des efforts de définition d'une future architecture de routage. Il accompagne le RFC 5773 [1] qui décrivait l'existant et se focalise sur les deux cahiers des charges qui avaient été redigés par deux groupes de travail en 2001. (Attention, donc, en le lisant, une bonne partie a été écrite au tout début du siècle.)

La section 1 résume la genèse compliquée de ce document. Il est issu d'un travail d'un groupe de l'IRTF qui devait travailler sur le routage « en partant d'une page blanche », c'est-à-dire sans être gêné par la nécessité de rester proche des mécanismes actuels. Un autre groupe, nommé Babylon, travaillait au même moment sur le même sujet, mais avec une perspective différente puisque Babylon se limitait aux solution incrémentales, ne nécessitant pas de tout jeter. Les contributions des deux groupes ont été réunis dans ce RFC 5772 (le « groupe A » est celui de l'IRTF et le « groupe B » est Babylon). Les deux groupes n'ont pas été fusionnés car ils partaient de principes trop différents pour qu'une fusion puisse marcher. La liste des membres des deux groupes figure dans la section 6.

Leurs contributions ont été un peu éditées pour la publication dans ce RFC mais, à part cela, elles reflètent en gros le point de vue du début des années 2000. Dans les deux cas (groupe A et groupe B), il s'agit d'une liste au Père Noël, de tout ce qu'il serait bien d'avoir dans le routage et la section 1 note qu'il n'est pas forcément possible de rééaliser toutes ces exigences (surtout simultanément).

La section 2 est rédigée par le groupe A, celui qui partait d'une feuille blanche. On y trouve tous les bons principes de conception, par exemple qu'une **architecture** doit être définie et bien documentée,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5773.txt

avant de se plonger dans les détails des protocoles (section 2.1.1). Idéalement, les changements des composants de cette architecture devraient pouvoir se faire séparement pour chaque composant. Et, encore plus vœu pieux, l'**adressage** devrait être séparé de la **topologie** du réseau (actuellement, sans être complètement liés, les deux sont fortement connectés ; cela explique les bonnes performances de l'Internet, malgré sa taille, mais c'est aussi dans cette forte connexion que se trouvent souvent les conflits, par exemple autour des adresses PI, ces adresses qui ne suivent pas la topologie).

L'architecture vue par le groupe A doit passer à l'échelle, c'est-à-dire accepter des réseaux bien plus grands qu'aujourdhui (« idéalement, pour les vingt prochaines années »), par exemple pour plusieurs dizaines de milliers d'AS, chiffre qu'une note d'un éditeur en 2005 prévient qu'il a déjà été atteint. Une autre prévision est déjà dépassée dans la même section 2.1.3. Le texte de 2001 prenait le risque de pronostiquer que, en raison de certaines limites physiques, les 40 Gb/s d'OC768 seraient difficiles à dépasser alors qu'ils le sont déjà.

La section 2.1.6 demande que l'architecture nouvelle gère proprement le "*multi-homing*". La 2.1.9, encore plus ambitieuse, demande que le nouveau système de routage soit sûr. Par exemple, une des exigences est la possibilité de dissimuler aux regards extérieurs la topologie de son réseau ce qui, pris au pied de la lettre, veut dire qu'il faut pouvoir empêcher traceroute de fonctionner.

Bien que le point de départ originel du projet du groupe A était de partir de zéro, une section, la 2.1.12 est quand même consacrée au déploiement incrémental de la nouvelle architecture, le considérant comme impératif. C'est compréhensible (l'expérience de beaucoup d'autres **objets techniques** complexes montre la vanité qu'il y a à vouloir faire table rase de l'investissement financier, technique et social) mais cela rend l'ensemble du cahier des charges encore plus... Comment dire ? Ambitieux ? Irréaliste ?

Le caier des charges du groupe A ne s'arrête pas là. Il demande encore une complète portabilité des adresses IP (section 2.1.14), que l'architecture soit simple à comprendre (« en moins d'une heure », dit la section 2.1.17 mais il est vrai que sa simplicité conceptuelle fut une des raisons de la victoire d'IP contre OSI). l'indépendance du système de routage par rapport aux autres composants de l'architecture (comme le DNS cf. section 2.1.20), et bien d'autres choses.

La liste est donc impressionnante. Et pourtant, tout n'a pas été inclus. La section 2.2 liste les non-buts, ce que le groupe A n'a pas considéré comme faisant partie des objectifs. On y trouve l'ingéniérie de trafic (section 2.2.2), terme très flou et trop vaste pour avoir été inclus dans les objectifs. la « sécurité absolue » (section 2.2.6), qui pourrait, en cas de problème, empêcher les opérateurs de faire leur travail, le routage dynamique en fonction de la charge du réseau (section 2.2.7), une vieille idée de l'Arpanet qui s'est toujours avérée très « casse-gueule », et, naturellement, la compatibilité avec l'existant (section 2.2.10) puisque l'idée de départ était une approche « table rase ».

La section 3 donne ensuite la parole au groupe (alias Babylon). Après un résumé du contexte, les exigences commencent en 3.2.3 qui note que tout cahier des charges laisse en général en blanc la question de l'évaluation des résultats : comment savoir qu'on a réussi ?

Parmi les demandes, l'exigence que le routage fournisse suffisamment d'informations pour pouvoir être utilisé par plusieurs services, autres que la délivrance de datagrammes au meilleur effort (section 3.2.3.2), le passage à l'échelle (section 3.2.3.3, où le RFC note que, dans ce secteur, l'échec est bien plus facile à détecter que le succès), etc. La sécurité fait l'objet de la demande 3.2.3.8,qui réclame une protection contre les DoS en notant que, dans l'Internet actuel, le fait de connaître une route sert également d'autorisation à y envoyer un paquet et qu'il faudrait changer cela (les notes récentes du RFC critiquent le groupe B en se demandant si ce ne serait pas une violation de la transparence du réseau).

Le groupe B souhaite également que les erreurs de configuration des routeurs (comme celle d'un routeur Microtik tchèque <http://www.renesys.com/blog/2009/02/longer-is-not-better.shtml>) ne puissent plus avoir des conséquences poiur l'Internet entier (section 3.2.3.10).

L'Internet n'est pas un objet purement technique. Il nécessite beaucoup de moyens humains et financiers, qui n'arrivent pas tout seuls. La section 3.4 se lance dans l'étude des contraintes extérieures, qui limitent les solutions possibles. Un des exemples le plus simple est celui de la très forte dépendance du soi-disant « cyberespace » vis-à-vis du monde physique (section 3.4.3). Combien d'entreprises ont acheté leur connectivité Internet à deux fournisseurs « pour la redondance » avant de découvrir que leurs câbles passaient dans la même tranchée et pouvaient tous être tranchés par la même pelleteuse ? (Comme ce fut le cas lors de la coupure égyptienne <http://www.renesys.com/blog/2008/12/deja-vu-all-over-again-cables.shtml>.)

Les exigences détaillées apparaissent ensuite en section 3.6. Groupées en sections, chacune reçoit un numéro, chaque section faisant l'objection d'une discussion groupée. Ainsi, l'exigence R(13) ("*Requirment 13*"), « Le routage doit pouvoir gérer différents chemins selon le service demandé » (nécessaire pour la QoS) fait partie de la section 3.6.2.2 sur les annonces de routes.

Il y a en tout 64 de ces exigences. Quelques exemples :

— R(26) ne tranche pas entre les différentes familles d'adresses et demande que le futur système de routage sache gérer IPv4 **et** IPv6 et également des familles non-IP.
— R(55) demande qu'il ne soit pas nécessaire de prévoir un "*flag day*" pour le déploiement du futur système de routage.
— R(62) voudrait que le futur système de routage permette d'authentifier les annonces de route (un problème brûlant aujourd'hui <https://www.bortzmeyer.org/securite-bgp-et-reaction-rapide.html>).

La section 3.10 couvre ensuite les questions « contestables », celles où le consensus du groupe B est moins fort. Cela va de questions très vagues (3.10.1 regrette qu'on modélise toujours les réseaux sous forme de graphes et demande qu'on accepte d'autres modèles - sans donner aucune idée de ce qu'ils pourraient être) à des considérations sur des problèmes transversaux comme le général byzantin (section 3.10.10).