RFC 7305 : Report from the IAB Workshop on Internet Technology Adoption and Transition (ITAT)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 août 2014

Date de publication du RFC : Juillet 2014

https://www.bortzmeyer.org/7305.html

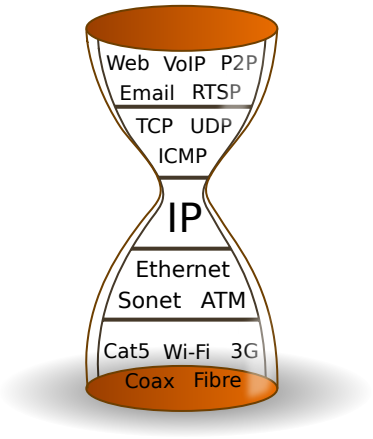
En décembre 2013, à Cambridge, l'IAB a tenu un atelier sur l'adoption des nouvelles technologies dans l'Internet. Qu'est-ce qui fait que telle technologie réussit dans le monde réel et que telle autre reste éternellement sur le papier ? Sérieuse question pour l'IETF, qui a a normalisé aussi bien des succès fous que des échecs plus ou moins complets. (Par exemple, le déploiement de la grande œuvre de l'IETF, IPv6, est extrêmement lent.)

Ce RFC résume les contributions à l'atelier. Comme on s'en doute, il n'y a eu aucun consensus, à part sur l'importance d'étudier l'angle de l'économie, et sur la référence à Bitcoin, grande vedette de l'atelier et source de nombreux exemples. Attention, donc, ce RFC n'est pas une prise de position de l'IAB, mais le compte-rendu d'un colloque pluraliste, aussi bien dans ses participants que dans les opinions exprimées. (Le rôle de l'IAB n'est pas de faire des protocoles - c'est la tâche de l'IETF, sous la direction de l'IESG - mais de réfléchir sur le long terme et sur les questions les plus fondamentales.)

On représente souvent l'écosystème de l'Internet sous forme d'un sablier : le protocole standard d'interconnexion est forcément unique et occupe donc la « taille », le tuyau fin du sablier. Au contraire, les protocoles d'application, beaucoup plus nombreux, occupent le bulbe du haut, et les protocoles « physiques », pour lesquels il y a également un grand choix, sont le bulbe du bas. Dans la vision traditionnelle de l'Internet, la taille était IP.

Dans la biologie, c'est l'ATP qui joue ce rôle central, la brique de base sur laquelle tout le reste est bâti (papier de Meyer <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_9.pdf>).

Aujourd'hui, en raison de l'ossification de l'Internet et de la prévalence de stupides "*middleboxes*" qui bloquent tout, la taille (ou faut-il l'appeler le cou ?) du sablier est plutôt HTTP... Il devient de plus en



plus difficile pour un protocole de s'imposer, surtout s'il ne tourne pas sur HTTP. En prime, le poids de l'existant est bien plus important qu'aux débuts de l'Internet. Aujourd'hui, un nouveau protocole doit lutter contre des concurrents bien installés.

La section 2 de notre RFC résume les motivations de ce travail, et les travaux équivalents déjà réalisés. On constate souvent que des protocoles, développés soigneusement par l'IETF, ont peu ou pas de succès dans le monde réel et, quand ils se répandent, c'est à un rythme bien trop lent. Trois exemples sont cités par le RFC, IPv6 (RFC 2460 [1]), SCTP (RFC 4960) et DNSSEC (RFC 4034). Ce retard peut à son tour retarder d'autres déploiements. Ainsi, DNSSEC est indispensable à DANE (RFC 6698) et le déploiement trop lent de DNSSEC, goulet d'étranglement, affecte donc DANE. Par contre, si les protocoles nouveaux ont du mal, les protocoles existants continuent à évoluer (le RFC cite SMTP et IMAP, qui peuvent être vus comme des réfutations de la théorie comme quoi « HTTP est le nouvel IP, la taille du sablier »).

Un excellent RFC avait déjà étudié les causes du succès ou de l'échec des protocoles, le RFC 5218. Une conséquence de ce RFC 5218 est l'importance plus grande désormais donnée aux facteurs de réussite. Faire un bon protocole ne suffit plus. Les groupes de travail de l'IETF doivent désormais aussi réfléchir à la valeur ajoutée de leurs propositions : le nouveau protocole apporte-t-il suffisamment pour surmonter les barrières situées devant l'adoption ?

Ces barrières étant largement financières, il n'est pas étonnant que plusieurs des papiers présentés à l'atelier portaient sur l'économie (section 3). Le RFC en résume quelques uns. D'abord, la théorie de Weber, S., Guerin, R., et J. Oliveira <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_2.pdf>, sur le couplage. Peut-on augmenter les chances de succès d'un protocole en le livrant avec d'autres ? Ou, au contraire, le couplage va-t-il ralentir le succès ? Comme cité précédemment, DANE dépend de DNSSEC. Cela simplifie son développement, permettant de s'appuyer sur les propriétés de sécurité de DNSSEC. Mais, du point de vue économique, cela fait dépendre DANE du succès de DNSSEC. Le couplage peut aider quand une technologie à succès en tire une autre, et ralentir si une technologie dépend d'une autre.

Autre exemple, très discuté à l'atelier (et c'est une nouveauté à l'IETF, puisque ce système a été développé en dehors de celle-ci), le succès de Bitcoin. Dans son papier <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_17.pdf>, R. Boehme suggère que les protocoles Internet s'inspirent de Bitcoin, exemple de grand succès (section 3.2 de notre RFC). Bitcoin n'a pas eu la

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2460.txt

partie facile : des médias hostiles (parfois au point de la propagande, comme dans le mensonge souvent répété comme quoi Bitcoin était une pyramide de Ponzi), des incertitudes juridiques (est-ce bien légal ?), des failles techniques (immédiatement exploitées par des voleurs), plusieurs tentatives de « monnaies Internet » avaient déjà été des échecs, des attaques par des spéculateurs visant le gain à court terme, même au prix de l'existence même du système. Mais Bitcoin a survécu à ces campagnes de presse et à ces problèmes techniques et de sécurité. Selon l'auteur, les raisons principales sont :

— Un mécanisme de récompense des premiers qui adoptent le système. Au début de Bitcoin, miner (créer de nouveaux bitcoins) est relativement facile et cela se durcit par la suite. Les plus difficiles à convaincre, les premiers adoptants, sont donc récompensés davantage, ce qui est logique et efficace. (J'ajoute personnellement que c'est juste : il est normal que ceux qui ont pris des risques au début reçoivent plus que ceux qui attendaient passivement.)
— Bitcoin ne vit pas dans son coin, isolé. Dès le début, des mécanismes de conversion ont été mis en place de et vers les monnaies d'État. Ainsi, adopter Bitcoin ne signifiait pas s'enfermer dans un monde à part. Un autre exemple, cité par le RFC, est le succès du courrier électronique : dès le début, le courrier Internet a eu des passerelles de et vers les autres systèmes de courrier. Autrement, il n'aurait pas été choisi.
— Les bitcoins ont une valeur pour leurs possesseurs, ce n'est pas juste pour le bien de l'humanité qu'on demande aux utilisateurs d'adopter la nouvelle technologie : ils y trouvent un intérêt. (Une remarque personnelle : les discussions à l'atelier supposaient acquis un point de vue égoïste, où les gens n'agissent qu'en fonction d'un intérêt personnel à court terme. Le problème serait très différent si on se plaçait dans une perspective plus volontariste, où on considère que les humains peuvent changer leur mentalité.)

Bref, Bitcoin fournit des motivations à ses adopteurs. (Un problème bien connu des militants pro-IPv6 : lorsqu'on suggère aux gens de migrer vers IPv6, la question est souvent « qu'est-ce que ça m'apporte, à moi ? », et elle n'a guère de réponse.)

Troisième étude de cas, le déploiement de DNSSEC (section 3.3) via le récit <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_5.docx> de A. Eklund Lowinder et P. Wallstrom sur le déploiement de cette technique en Suède, à commencer par le TLD .se. Le travail d'IIS <https://www.iis.se/> pour encourager DNSSEC a pris la forme d'une contribution au financement d'OpenDNSSEC (pour abaisser les barrières techniques), et d'incitations financières (auprès des bureaux d'enregistrement).

Une des conclusions de cette partie de l'atelier était qu'il faut éviter d'accrocher une technologie exclusivement à une autre. Le logiciel privateur Skype a été cité comme exemple : il teste plusieurs transports disponibles et choisit celui qui marche. De même, lier une application à SCTP serait probablement une erreur : si SCTP ne réussit pas à se répandre, cette application serait fichue). Il faudrait plutôt essayer plusieurs transports et garder le premier qui marche, un peu comme le fait l'algorithme des globes oculaires heureux dans le RFC 6555.

Et puisqu'on parlait d'économie, il y a eu évidemment des discussions sur le modèles de prix, comme suite au papier de S. Sen <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_101.pdf>. Par exemple, certains protocoles pourraient bénéficier d'un prix dépendant de l'heure (pour encourager le trafic à se déplacer vers les heures creuses).

Ah, une question qui est dans la section 5 mais qui aurait eu sa place dans celle sur l'économie : celle des brevets. Leurs effets néfastes sont bien connus. Le papier de E. Lear et D. Mohlenhoff décrit leurs relations <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_11.docx> avec la normalisation. Le plus gros problème identifié est celui des « brevets sous-marins », brevets que l'IETF ne connait pas... jusqu'au moment où il est trop tard.

Mais l'économie ne peut pas tout résoudre. Les choix se font aussi, mais si ce n'est pas la seule motivation, sur la qualité technique. De ce point de vue-là, pour qu'un protocole réussisse, il faut aussi

faire en sorte qu'il soit le « meilleur » possible. Par exemple, est-ce que le processus de normalisation de l'Internet est suffisamment bien connecté au monde de la recherche, où s'élaborent les idées du futur ? Normalement, l'IETF ne normalise que des technologies bien maîtrisées. L'interaction avec la recherche se fait via l'IRTF.

Les chercheurs suggèrent parfois que l'architecture actuelle de l'Internet n'est plus adaptée aux défis futurs, et qu'il faudrait la changer, par exemple dans la direction du "*Lowest Common Denominator Networking*" <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_3.pdf>, idée qui a apparemment été mal reçue à l'atelier.

Un atelier n'est pas complet sans une rubrique « Divers » (section 6) et deux autres points ont donc été abordés. D'abord, la résilience de l'Internet, et notamment la sécurité du routage. Le papier d'A. Robachevsky <http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_12.pdf> l'abordait en partant de l'éculée référence à la tragédie des terres communales. L'Internet est composé d'un grand nombre de réseaux distincts, sans administration centrale (ce qui est une bonne chose). La tentation peut donc être forte de se servir des communs (comme la table de routage globale) sans souci de leur pérennité, sans gestion collective.

Et un deuxième point « Divers » concernait TLS. TLS est très largement adopté et ne souffre pas, a priori, du syndrome du protocole qu'on n'arrive pas à déployer. Mais la très grande majorité des clients et serveurs existants utilisent des vieilles versions du protocole TLS, ayant des vulnérabilités connues (comme Beast <https://www.bortzmeyer.org/beast-tls.html>). La version la plus récente de TLS, la 1.2, est normalisée dans le RFC 5246. Comment faire en sorte qu'elle soit déployée partout ? Et le problème ne concerne pas que le protocole lui-même mais aussi les algorithmes de cryptographie utilisés. (Au cours de l'atelier, il a été noté qu'une grande partie du trafic est toujours chiffrée avec Triple DES, algorithme aux faiblesses connues.)

Maintenant, les actions (section 7). La conclusion de ce RFC reconnait l'importance de regarder le succès des systèmes comme Bitcoin, mentionné pour la première fois dans un RFC, et un exemple pour tout nouveau système. Autrement, l'idée la plus intéressante me semble être celle de pousser la collaboration avec le monde académique, par exemple en enrôlant des étudiants pour relire et critiquer les documents IETF. Cela fournirait à ces étudiants une excellente occasion d'apprendre, et à l'IETF plein de regards neufs.