RFC 8980 : Report from the IAB Workshop on Design Expectations vs. Deployment Reality in Protocol Development

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 février 2021

Date de publication du RFC : Février 2021

https://www.bortzmeyer.org/8980.html

L'atelier de l'IAB DEDR <https://www.iab.org/activities/workshops/dedr-workshop/> ("*Design Expectations vs. Deployment Reality*") s'est tenu à Kirkkonummi en juin 2019 (oui, il faut du temps pour publier un RFC de compte-rendu). Son but était, par delà la constatation que le déploiement effectif des protocoles conçus par l'IETF ne suit pas toujours les attentes initiales, d'explorer pourquoi cela se passait comme cela et ce qu'on pouvait y changer.

Souvent, lors de la mise au point d'un nouveau protocole, les personnes qui y travaillent ont en tête un modèle de déploiement. Par exemple, pour le courrier électronique, l'idée dominante était qu'il y aurait souvent un serveur de messagerie par personne. On sait que ce n'est pas la situation actuelle. En raison de soucis de sécurité, de pressions économiques et/ou politiques, et d'autres facteurs, on a aujourd'hui un courrier nettement plus centralisé, avec un caractère oligopolistique marqué, dominé par une poignée d'acteurs qui dictent les règles. Cette centralisation n'est pas souhaitable (sauf pour les GAFA). Mais où est-ce que le dérapage a commencé ? Parfois, cela a été rapide, et parfois cela a pris beaucoup de temps.

Quelques exemples :

— Le courrier électronique, on l'a dit, était conçu autour de l'idée qu'il y aurait beaucoup de serveurs, gérés par des acteurs différents. (À une époque, dans le monde universitaire, il était courant que chaque station de travail ait un serveur de courrier, et ses propres adresses.) Aujourd'hui, il est assez centralisé, chez des monstres comme Gmail et Outlook.com. Un des facteurs de cette centralisation est le spam, contre lequel il est plus facile de se défendre si on est gros.

— Le DNS avait été prévu pour une arborescence de noms assez profonde (l'exemple traditionnel était l'ancien domaine de premier niveau `.us` qui était découpé en entités géographiques de plus en plus spécifiques). Mais l'espace des noms est aujourd'hui plus plat que prévu. On voit même des organisations qui ont, mettons, `example.com` et qui, lançant un nouveau produit, mettons `foobar`, réservent `foobar.com`, voire `foobar-example.com` au lieu de tout simplement créer `foobar.example.com` (ce qui serait en outre moins cher). Un autre exemple de centralisation est la tendance à abandonner les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> locaux (qui, il est vrai, sont souvent mal gérés ou menteurs <https://www.bortzmeyer.org/google-detourne-par-orange.html>) pour des gros résolveurs publics comme Google Public DNS <https://www.bortzmeyer.org/google-dns.html> ou Quad9 <https://www.bortzmeyer.org/quad9.html> (et cette centralisation, contrairement à ce qui est souvent prétendu, n'a rien à voir avec DoH <https://www.bortzmeyer.org/doh-et-ses-adversaires.html>).
— Le Web est également un exemple de déviation des principes originels, vers davantage de centralisation. Le concept de base est très décentralisé. N'importe qui peut installer un serveur HTTP sur son Raspberry Pi et faire partie du "*World Wide Web*". Mais cela laisse à la merci, par exemple, des dDoS ou, moins dramatiquement, de l'effet Slashdot (même si un site Web statique peut encaisser une charge importante). On constate que de plus en plus de sites Web dépendent donc de services centralisés, CDN ou gros relais comme Cloudflare.
— Et ça ne va pas forcément s'arranger avec de nouvelles technologies, par exemple l'apprentissage automatique, qui sont difficiles à décentraliser.

L'IAB avait produit un RFC sur la question « qu'est-ce qui fait qu'un protocole a du succès », le RFC 5218[1]. Dans un autre document, le RFC 8170, l'IAB étudiait la question des transitions (passage d'un protocole à un autre, ou d'une version d'un protocole à une autre). L'atelier de Kirkkonummi avait pour but de poursuivre la réflexion, en se focalisant sur les cas où les suppositions de base n'ont pas tenu face à la réalité.

L'agenda de l'atelier était structuré en cinq sujets, le passé (qu'avons-nous appris), les principes (quelles sont les forces à l'œuvre et comment les contrer ou les utiliser), la centralisation (coûts et bénéfices), la sécurité et le futur (fera-t-on mieux à l'avenir et savons-nous comment). 21 articles ont été reçus (ils sont en ligne <https://www.iab.org/activities/workshops/dedr-workshop/position-papers/>), et 30 personnes ont participé.

Sur le passé, l'atelier a étudié des exemples de déploiement de protocoles, comme PKIX, DNSSEC, le NAT, l'IoT, etc. Souvent, ce qui a été effectivement déployé ne correspondait pas à ce qui était prévu. Par exemple, un protocole très demandé n'a pas eu le succès attendu (c'est le cas de DNSSEC : tout le monde réclame de la sécurité, mais quand il faut travailler pour la déployer, c'est autre chose) ou bien il n'a pas été déployé comme prévu. C'est d'autant plus vrai que l'IETF n'a pas de pouvoir : elle produit des normes et, ensuite, d'autres acteurs décident ou pas de déployer, et de la manière qu'ils veulent (le « marché » sacré). Le RFC cite quelques leçons de l'expérience passée :

— Les retours du terrain arrivent toujours trop tard, bien après que la norme technique ait été bouclée. C'est particulièrement vrai pour les retours des utilisateurs individuels (ceux que, d'après le RFC 8890, nous devons prioriser).
— Les acteurs de l'Internet font des choses surprenantes.
— On constate la centralisation mais on ne peut pas forcément l'expliquer par les caractéristiques des protocoles. Rien dans HTTP ou dans SMTP n'impose la centralisation qu'on voit actuellement.
— En revanche, certaines forces qui poussent à la centralisation sont connues : cela rend certains déploiements plus faciles (c'est un argument donné pour refuser la décentralisation <https://signal.org/blog/the-ecosystem-is-moving/>). Et les solutions centralisées ont nettement la faveur des gens au pouvoir, car ils préfèrent travailler avec un petit nombre d'acteurs bien identifiés. (C'est pour cela qu'en France, tous les hommes politiques disent du mal des GAFA tout en combattant les solutions décentralisées, qui seraient plus difficiles à contrôler.)

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5218.txt`

— On ne sait pas toujours si un nouveau protocole sera vraiment utile ou pas (cf. la 5G et le porno dans l'ascenseur <https://www.bortzmeyer.org/usages-5g.html>).
— Il est facile de dire que l'IETF devrait davantage interagir avec tel ou tel groupe, mais certains groupes sont difficiles à toucher (le RFC 8890 détaille ce problème).

Sur les principes, on a quand même quelques conclusions solides. Par exemple, il est clair qu'un nouveau protocole qui dépend de plusieurs autres services qui ne sont pas encore déployés aura davantage de mal à s'imposer qu'un protocole qui peut s'installer unilatéralement sans dépendre de personne. Et puis bien sûr, il y a l'inertie. Quand quelque chose marche suffisamment bien, il est difficile de la remplacer. (Le RFC donne l'exemple de BGP, notamment de sa sécurité <https://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html>.) Et cette inertie génère le phénomène bien reconnu de la prime au premier arrivant. Si un protocole fournit un nouveau service, un remplaçant aura le plus grand mal à s'imposer, même s'il est meilleur, face au tenant du titre. Le monde du virtuel est lourd et ne bouge pas facilement. Quand un protocole a eu un succès fou (terme défini et discuté dans le RFC 5218), le remplacer devient presque impossible. Autre principe analysé : l'IETF ne devrait de toute façon pas avoir d'autorité sur la façon dont ses protocoles sont déployés. Ce n'est pas son rôle et elle n'a pas de légitimité pour cela. Et, on l'a dit, les usages sont durs à prévoir. L'atelier a aussi constaté que certains modèles de déploiement, qui s'appliquent à beaucoup de cas, n'avaient pas été prévus et planifiés. C'est le cas de l'extrême centralisation, bien sûr, mais également le cas de « tout via le Web » qui fait que tout nouveau service sur l'Internet tend à être accessible uniquement à distance, avec les protocoles et les formats du Web. Cela tend à créer des silos fermés, même s'ils utilisent des protocoles ouverts. (C'est en réponse à ce problème qu'a été créée la licence Affero.)

Concernant le troisième sujet, la centralisation, l'atelier a constaté que la tendance à la centralisation n'est pas toujours claire dès le début. Le RFC cite l'exemple (très mauvais, à mon avis <https://www.bortzmeyer.org/doh-et-ses-adversaires.html>) de DoH. Autre constatation, la sécurité, et notamment le risque d'attaques par déni de services réparties est un puissant facteur de centralisation. Si vous voulez gérer un site Web sur un sujet controversé, avec des opposants puissants et prêts à tout, vous êtes quasiment obligé de faire appel à un hébergement de grande taille (face aux dDoS, la taille compte). Ceci dit, l'atelier a aussi identifié des forces qui peuvent aller en sens contraire à la centralisation. Une fédération peut mieux résister aux attaques (qui ne sont pas forcément techniques, cela peut être aussi la censure) qu'un gros silo centralisé, le chiffrement peut permettre même aux petits de limiter la surveillance exercée par les gros, les navigateurs Web peuvent adopter de meilleures pratiques pour limiter les données envoyées à la grosse plate-forme à laquelle on accède (toute cette liste du RFC est d'un optimisme souvent injustifié…), l'interopérabilité <https://framablog.org/2019/06/12/cest-quoi-linteroperabilite-et-pourquoi-est-ce-beau-et-bien/> peut permettre davantage de concurrence (cf. le bon rapport du Conseil National du Numérique <https://cnnumerique.fr/Interoperabilite_Concurrence_Etude>), et certaines tendance lourdes peuvent être combattues également par des moyens non-techniques (le RFC cite la régulation, ce qui n'est pas facilement accepté par les libertariens, même si ceux-ci ne sont pas plus nombreux à l'IETF qu'ailleurs).

Quatrième sujet, la sécurité. Traditionnellement, le modèle de menace de l'Internet (RFC 3552 mais aussi RFC 7258) est que tout ce qui est entre les deux machines qui communiquent peut être un ennemi. Cela implique notamment le choix du chiffrement de bout en bout. Toutefois, ce modèle de menace ne marche pas si c'est l'autre pair qui vous trahit. Ainsi, utiliser TLS quand vous parlez à Facebook vous protège contre des tiers mais pas contre Facebook lui-même. À l'heure où tant de communications en ligne sont médiées par des GAFA, c'est un point à prendre en considération. (Attention à ne pas jeter le bébé avec l'eau du bain ; le chiffrement de bout en bout reste nécessaire, mais n'est pas suffisant. Certains FAI remettent en cause le modèle de menace traditionnel pour combattre ou restreindre le chiffrement, en faisant comme si les GAFA étaient les seuls à faire de la surveillance.) Les participants à l'atelier sont plutôt tombés d'accord sur la nécessité de faire évoluer le modèle de menace mais il faudra veiller à ce que ne soit pas un prétexte pour relativiser l'importance du chiffrement, qui reste indispensable. À noter une autre limite d'un modèle de menace qui ne mentionnerait que les tiers situés sur le trajet : non seulement la partie distante (par exemple Facebook) peut être une menace, mais votre propre machine peut vous trahir, par exemple si vous n'utilisez pas du logiciel libre.

Enfin, cinquième et dernier sujet, le futur. L'IETF n'a pas de pouvoir contraignant sur les auteurs de logiciels, sur les opérateurs ou sur les utilisateurs (et heureusement). Elle ne peut agir que via ses normes. Par exemple, pour l'Internet des Objets, le RFC 8520 permet davantage d'ouverture dans la description des utilisations qu'un objet fera du réseau. Outre la production de bonnes normes, l'IETF peut être disponible quand on a besoin d'elle, par exemple comme réserve de connaissance et d'expertise.

La conclusion du RFC (section 5) indique que le problème est complexe, notamment en raison de la variété des parties prenantes : tout le monde n'est pas d'accord sur les problèmes, et encore moins sur les solutions. (Il n'existe pas de « communauté Internet », à part dans des discours politiciens.) D'autre part, certains des problèmes n'ont pas de solution évidente. Le RFC cite ainsi les dDoS, ou le spam. Cette absence de solution satisfaisante peut mener à déployer des « solutions » qui ont un rôle négatif. Le RFC note ainsi à juste titre que l'absence d'une solution de paiement en ligne correcte (anonyme, simple, bon marché, reposant sur des normes ouvertes, etc) pousse à faire dépendre la rémunération des créateurs de la publicité, avec toutes ses conséquences néfastes. Et l'Internet fait face à de nombreux autres défis stratégiques, comme la non-participation des utilisateurs aux questions qui les concernent, ou comme la délégation de décisions à des logiciels, par exemple le navigateur Web.

On l'a dit, la conclusion est que l'IETF doit se focaliser sur ce qu'elle sait faire et bien faire, la production de normes. Cela implique :

— Travailler sur une mise à jour du modèle de menace cité plus haut,
— Réfléchir aux mesures qui peuvent être prises pour limiter la centralisation,
— Mieux documenter les principes architecturaux de l'Internet, notamment le principe de bout en bout,
— Travailler sur les systèmes de réputation (cf. RFC 7070),
— Etc.

Un autre compte-rendu de cet atelier, mais très personnel, avait été fait par Geoff Huston <https://www.potaroo.net/ispcol/2019-06/dedr.html>.