# RFC 8170 : Planning for Protocol Adoption and Subsequent Transitions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 mai 2017

Date de publication du RFC : Mai 2017

https://www.bortzmeyer.org/8170.html

---

L'Internet existe depuis de nombreuses années (le nombre exact dépend de la façon dont on compte...) et, pendant tout ce temps, les protocoles utilisés ne sont pas restés identiques à eux-mêmes. Ils ont évolué, voire ont été remplacés. Cela soulève un problème : la **transition** entre l'ancien et le nouveau (le cas le plus fameux étant évidemment le passage d'IPv4 à IPv6...) Beaucoup de ces transitions se sont mal passées, parfois en partie car l'ancien protocole ou l'ancienne version n'avait pas prévu son futur remplacement. Contrairement à ce qu'espèrent souvent les techniciens, il ne suffit pas d'incrémenter le numéro de version pour que tous les acteurs adoptent la nouvelle version. Ce nouveau RFC de l'IAB raconte les leçons tirées, et regarde comment on pourrait améliorer les futures transitions.

Ce RFC se focalise sur les transitions techniques. Ce ne sont évidemment pas les seules (il y a par exemple des transitions organisationnelles) mais ce sont celles qui comptent pour l'IAB et l'IETF. Une transition peut être aussi bien le déploiement d'un tout nouveau protocole, que le passage d'un protocole d'une version à une autre. Le thème de la transition d'un protocole à l'autre est fréquent, et de nombreux RFC ont déjà été consacrés à une transition. C'est le cas de :

— Le RFC 3424 [1], qui parlait des techniques de contournement des NAT, en insistant sur le fait qu'elles devaient avoir un caractère provisoire, et ne pas ossifier encore plus l'Internet,
— Le RFC 4690 qui parlait de la transition d'une version d'Unicode à l'autre, dans le contexte des IDN,
— La déclaration de l'IAB sur NAT-PT <https://www.iab.org/documents/correspondence-reports-docu
docs2007/follow-up-work-on-nat-pt/>, qui critiquait une méthode de transition vers IPv6.

Outre les transitions à proprement parler, l'IAB s'est déjà penché sur les principes qui faisaient qu'un protocole pouvait marcher ou pas. C'est notamment le cas de l'excellent RFC 5218 qui étudie les facteurs qui font d'un protocole un échec, un succès, ou un succès fou. Parmi les leçons tirées par ce RFC 5218, les concepteurs d'un protocole devraient s'assurer que :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3424.txt

— Les bénéfices sont pour celui qui assume les coûts. Dans un réseau, coûts et bénéfices ne sont pas forcément alignés. Par exemple, le déploiement de BCP 38 <https://www.bortzmeyer.org/bcp38.html> bénéficie aux concurrents de celui qui paie, ce qui explique le manque d'enthousiasme des opérateurs. Notez que coûts et bénéfices ne sont pas déterminés par les lois physiques, ils peuvent être changés par la loi (amendes pour ceux qui ne déploient pas BCP 38 <https://www.bortzmeyer.org/bcp38.html>, ou à l'inverse code source gratuitement disponible et payé par l'argent public, comme cela avait été le cas pour encourager le déploiement de TCP/IP).
— Le protocole est déployable de manière incrémentale (dans un réseau comme l'Internet, qui représente des investissements énormes, toute solution qui nécessite de jeter tout l'existant d'un coup est condamnée d'avance).
— Le coût total est raisonnable. Il ne faut pas seulement regarder le prix des machines et d'éventuelles licences logicielles. Il faut aussi tenir compte de la formation, des changements de pratiques, des conséquences juridiques…

Le RFC 7305 discutait également des aspects économiques de la transition et notait l'importance de donner une carotte aux premiers à adopter le nouveau protocole, ceux qui font un pari risqué. C'est pour cela qu'il est parfaitement légitime que les premiers à avoir cru dans Bitcoin aient reçu une quantité importante de bitcoins à un prix très faible. Cette décision était une des meilleures prises par Satoshi Nakamoto. Ce RFC note aussi l'importance d'un partenariat avec des organisations qui peuvent aider ou contrarier la transition (comme les RIR ou l'ICANN).

La section 2 de notre RFC rappelle que, de toute façon, le terme « transition » risque d'être mal interprété. Il n'est plus possible depuis longtemps de faire un "*flag day*" dans l'Internet, un jour J où on change toutes les machines d'un coup de manière coordonnée. Les transitions sont donc forcément longues, avec une période de co-existence entre l'ancien et le nouveau.

Si l'ancien et le nouveau protocole ne peuvent pas interopérer directement (cas d'IPv4 et d'IPv6), il faudra parfois envisager un mécanisme de traduction (qui ne se situera pas forcément dans la même couche). Un tel traducteur, s'il est situé sur le chemin entre les deux machines, pose souvent d'ennuyeux problèmes de sécurité car il risque fort de casser le modèle de bout en bout.

La section 5 de notre RFC est consacrée aux plans de transition. Ah, les plans…Ils sont évidemment indispensables (on ne va pas se lancer dans une grande transition sans avoir planifié un minimum) mais ils sont aussi très fragiles (comme disent les militaires, « aucun plan ne survit à la première rencontre avec l'ennemi »), et ils terminent souvent au musée des mauvaises idées. Disons qu'il faut avoir un plan, mais ne pas en être esclave.

Quelles sont les qualités d'un bon plan de transition, en s'appuyant sur les expériences ratées et réussies ? D'abord, il faut bien connaitre l'existant. Par exemple, si l'ancien protocole a une fonction optionnelle qui n'a pas d'équivalent, ou un équivalent très différent dans le nouveau protocole, il est bon de savoir si cette fonction est utilisée en pratique (elle peut même ne pas être implémentée du tout, ce qui facilite les choses). De même, il est important de savoir si les logiciels existants mettent réellement en œuvre l'ancien protocole tel qu'il est spécifié, ou bien si, en pratique, ils en dévient, et ont des comportements qui vont poser des problèmes pendant la transition. (Un cas typique est celui de SSL où la plupart des programmes n'avaient pas mis en œuvre correctement le mécanisme de négociation, et plantaient donc lorsqu'une nouvelle version arrivait.)

Un autre élément important d'un plan de transition est d'avoir les idées claires sur les incitations à migrer. Les acteurs de l'Internet utilisent l'ancien protocole. Ça marche pour eux. Pourquoi feraient-ils l'effort de migrer vers un nouveau protocole, ce qui leur coûtera du temps et de l'argent ? Il faut donc des incitations (ou du marketing, qui arrive souvent à faire acheter un gadget inutile). Il n'y a pas que les coûts financiers directs, il faut aussi regarder d'autres problèmes à surmonter (par exemple l'hostilité

de certains acteurs, ainsi le chiffrement a du mal à se répandre car les acteurs de l'Internet qui font de la surveillance ont intérêt à continuer à violer la vie privée).

Il y a ensuite le plan proprement dit : une liste des étapes, avec un vague calendrier. Le calendrier est certainement la partie la plus fragile du plan ; l'Internet n'ayant pas de chef, une transition va dépendre des efforts d'un grand nombre d'acteurs non coordonnés, et prédire leurs délais de réaction est à peu près impossible. (Voir le RFC 5211 pour un exemple.)

Un bon plan doit aussi comprendre un moyen de déterminer le succès (ou l'échec). Là aussi, ce n'est pas évident du tout. Certains protocoles sont surtout utilisés dans des réseaux locaux, donc difficiles à mesurer de l'extérieur (comment savoir combien de FAI proposent un résolveur DNS sécurisé par le RFC 7858 ?) Parfois, les critères quantitatifs ne sont pas évidents à établir. Prenons l'exemple d'IPv6 (lisez à ce sujet le rapport <http://www.arcep.fr/index.php?id=8571&no_cache=0&tx_gsactualite_pi1[uid]=1905&tx_gsactualite_pi1[annee]=&tx_gsactualite_pi1[theme]=&tx_gsactualite_pi1[motscle]=&tx_gsactualite_pi1[backID]=26&cHash=e46b8063c1ba85ae60e274e de l'ARCEP sur la transition IPv6, qui traite la question en détail). Comment mesure-t-on le succès d'IPv6 ? Le pourcentage de sites Web du Top N d'Alexa qui a une adresse IPv6 ? Le pourcentage d'utilisateurs finaux qui a IPv6 ? Le pourcentage d'octets IPv6 vs. IPv4 ? (Et où ? Chez Google ? Sur un point d'échange comme le France-IX ? Sur le réseau d'un transitaire ? Les valeurs seront très différentes.)

On l'a dit, les plans, même les meilleurs, survivent rarement à la rencontre avec le monde réel. Il faut donc un (ou plusieurs) « plan B », une solution de secours. Souvent, de facto, la solution de secours est la coexistence permanente de l'ancien et du nouveau protocole…

Et puis bien des acteurs de l'Internet ne suivent pas attentivement ce que fait l'IETF, voire ignorent complètement son existence, ce qui ajoute un problème supplémentaire : il faut communiquer le plan, et s'assurer qu'il atteint bien tous les acteurs pertinents (tâche souvent impossible). C'est le but d'opérations de communication comme le "*World IPv6 Launch Day*".

Notre RFC rassemble ensuite (annexe A) quatre études de cas, illustrant des problèmes de transition différents. D'abord, le cas d'ECN. Ce mécanisme, normalisé dans le RFC 3168, permettait aux routeurs de signaler aux machines situées en aval de lui que la congestion menaçait. L'idée est que la machine aval, recevant ces notifications ECN, allait dire à la machine émettrice, située en amont du routeur, de ralentir, avant qu'une vraie congestion n'oblige à jeter des paquets. Les débuts d'ECN, vers 2000-2005, ont été catastrophiques <http://www.ietf.org/proceedings/68/slides/tsvarea-3/sld1.htm>. Les routeurs, voyant apparaitre des options qu'ils ne connaissaient pas, ont souvent planté. C'est un cas typique où une possibilité existait (les options d'IPv4 étaient normalisées depuis le début) mais n'était pas correctement implémentée en pratique. Toute transition qui se mettait à utiliser cette possibilité allait donc se passer mal. Pour protéger les routeurs, des pare-feux se sont mis à retirer les options ECN, ou bien à jeter les paquets ayant ces options, rendant ainsi très difficile tout déploiement ultérieur, même après correction de ces sérieuses failles dans les routeurs.

À la fin des années 2000, Linux et Windows ont commencé à accepter l'ECN par défaut (sans toutefois le réclamer), et la présence d'ECN, mesurée sur le Top Million d'Alexa, a commencé à grimper. De quasiment zéro en 2008, à 30 % en 2012 puis 65 % en 2014. Bref, ECN semble, après un très long purgatoire, sur la bonne voie (article « "*Enabling Internet-Wide Deployment of Explicit Congestion Notification*" <http://ecn.ethz.ch/ecn-pam15.pdf> »).

(Un autre cas, non cité dans le RFC, où le déploiement d'une possibilité ancienne mais jamais testé, a entrainé des conséquences fâcheuses, a été celui de BGP, avec la crise de l'attribut 99 <https://www.bortzmeyer.org/bgp-attribut-99.html>.)

L'exemple suivant du RFC est celui d'IDN. L'internationalisation est forcément un sujet chaud, vu les sensibilités existantes. Les IDN résolvent enfin un problème très ancien, l'impossibilité d'avoir des noms de domaine dans toutes les écritures du monde. (Voir la section 3 du RFC 6055, pour la longue et compliquée histoire des IDN.) Une fois que la norme IDN était disponible, il restait à effectuer la transition. Elle n'est pas encore terminée aujourd'hui. En effet, de nombreuses applications manipulent les noms de domaine et doivent potentiellement être mises à jour. Bien sûr, elles peuvent toujours utiliser la forme Punycode, celle-ci est justement conçue pour ne pas perturber les applications traditionnelles, mais ce n'est qu'un pis-aller (`[Caractère Unicode non montré` [2] `][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractèr Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractèr Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractèr Unicode non montré ][Caractère Unicode non montré ].[Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ][Caractère Unicode non montré ]` est quand même supérieur à `xn--8kcga3ba7d1akxnes3jhcc3bziwddhe.xn--clchc0ea0b2g2a9gcd`).

Pire, IDN a connu une transition dans la transition, lors du passage de la norme IDN 2003 (RFC 3490) vers IDN 2008 (RFC 5890). IDN 2008 était conçu pour découpler IDN d'une version particulière d'Unicode mais l'un des prix à payer était le cassage de la compatibilité : certains caractères comme le [Caractère Unicode non montré ] étaient traités différemment entre IDN 2003 et IDN 2008.

Le cas d'IDN est aussi l'occasion, pour le RFC, de rappeler que tout le monde n'a pas forcément les mêmes intérêts dans la transition. IDN implique, outre l'IETF, les auteurs de logiciels (par exemple ceux des navigateurs), les registres de noms de domaine, les domaineurs, et bien sûr les utilisateurs. Tous ne sont pas forcément d'accord et le blocage d'une seule catégorie peut sérieusement retarder une transition (diplomatiquement, le RFC ne rappele pas que l'ICANN a longtemps retardé l'introduction d'IDN dans la racine du DNS <`https://www.bortzmeyer.org/idn-racine.html`>, pour des pseudo-raisons de sécurité, et que leur introduction n'a pu se faire qu'en la contournant.)

Lorsqu'on parle transition douloureuse, on pense évidemment tout de suite à IPv6. Ce successeur d'IPv4 a été normalisé en 1995 (par le RFC 1833), il y a vingt-deux ans ! Et pourtant, il n'est toujours pas massivement déployé. (Il existe de nombreuses métriques mais toutes donnent le même résultat : IPv6 reste minoritaire, bien que ces dernières années aient vu des progrès certains. Notez que les réseaux visibles publiquement ne sont qu'une partie de l'Internet : plusieurs réseaux internes, par exemple de gestion d'un opérateur, sont déjà purement IPv6.) Il y avait pourtant un plan de transition détaillé (RFC 1933), fondé sur une coexistence temporaire où toutes les machines auraient IPv4 **et** IPv6, avant qu'on ne démantèle progressivement IPv4. Mais il a clairement échoué, et ce problème est maintenant un sujet de plaisanterie (« l'année prochaine sera celle du déploiement massif d'IPv6 », répété chaque année).

Là encore, un des problèmes était que tout le monde n'a pas les mêmes intérêts. Si les fabricants de routeurs et les développeurs d'applications bénéficient d'IPv6, c'est beaucoup moins évident pour les gérants de sites Web, ce qui explique que plusieurs sites à forte visibilité, comme Twitter, ou bien gérés par des gens pourtant assez branchés sur la technique, comme GitHub, n'aient toujours pas IPv6

2. Car trop difficile à faire afficher par LaTeX

(c'est également le cas de la totalité des sites Web du gouvernement français, qui pourtant promeut officiellement l'usage d'IPv6).

L'effet réseau a également joué à fond contre IPv6 : les pionniers n'ont aucune récompense, puisqu'ils seront tout seuls alors que, par définition, le réseau se fait à plusieurs. Bien sûr, IPv6 marche mieux que l'incroyable et branlante pile de techniques nécessaire pour continuer à utiliser IPv4 malgré la pénurie <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> (STUN, TURN, "*port forwarding*", ICE, etc). Mais tout le monde ne ressent pas ce problème de la même façon : le FAI, par exemple, ne supporte pas les coûts liés à la non-transition, alors qu'il paierait ceux de la transition. Ce problème de (non-)correspondance entre les coûts et les bénéfices est celui qui ralentit le plus les nécessaires transitions. Et puis, pour les usages les plus simples, les plus Minitel 2.0, IPv4 et ses prothèses marchent « suffisamment ».

La lenteur de la transition vers IPv6 illustre aussi la difficulté de nombreux acteurs à planifier à l'avance. C'est seulement lorsque l'IANA, puis les RIR sont l'un après l'autre tombés à court d'adresses IPv4 que certains acteurs ont commencé à agir, alors que le problème était prévu depuis longtemps <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>.

Il n'y a évidemment pas une cause unique à la lenteur anormale de la transition vers IPv6. Le RFC cite également le problème de la formation : aujourd'hui encore, dans un pays comme la France, une formation de technicien ou d'ingénieur réseaux peut encore faire l'impasse sur IPv6.

Le bilan du déploiement d'IPv6 est donc peu satisfaisant. Si certains réseaux (réseaux internes d'entreprises, réseaux de gestion) sont aujourd'hui entièrement IPv6, le déploiement reste loin derrière les espérances. Ce mauvais résultat nécessite de penser, pour les futurs déploiements, à aligner les coûts et les bénéfices, et à essayer de fournir des bénéfices incrémentaux (récompenses pour les premiers adoptants, comme l'a fait avec succès Bitcoin).

Dernier cas de transition étudié par notre RFC, HTTP/2 (RFC 7540). Nouvelle version du superpopulaire protocole HTTP, elle vise à améliorer les performances, en multiplexant davantage, et en comprimant les en-têtes (RFC 7541). HTTP/2 a vécu la discussion classique lors de la conception d'une nouvelle version, est-ce qu'on résout uniquement les problèmes les plus sérieux de l'ancienne version ou bien est-ce qu'on en profite pour régler tous les problèmes qu'on avait laissés ? HTTP/2 est très différent de HTTP/1. Ses règles plus strictes sur l'utilisation de TLS (algorithmes abandonnés, refus de la renégociation, par exemple) ont d'ailleurs entrainé quelques problèmes de déploiement.

Il y a même eu la tentation de supprimer certaines fonctions de HTTP/1 considérées comme inutiles ou néfastes (les réponses de la série 1xx, et les communications en clair, entre autres). Après un débat très chaud et très houleux, HTTP/2 n'impose finalement pas HTTPS : les communications peuvent se faire en clair même si, en pratique, on voit très peu de HTTP/2 sans TLS.

Et comment négocier l'ancien protocole HTTP/1 ou le nouveau HTTP/2 ? Ce problème du client (le même qu'avec les versions d'IP : est-ce que je dois tenter IPv6 ou bien est-ce que j'essaie IPv4 d'abord ?) peut être résolu par le mécanisme "*Upgrade*" de HTTP (celui utilisé par le RFC 6455), mais il nécessite un aller-retour supplémentaire avec le serveur. Pour éviter cela, comme presque toutes les connexions HTTP/2 utilisent TLS, le mécanisme privilégié est l'ALPN du RFC 7301.

Ce mécanisme marche tellement bien que, malgré le conseil du RFC 5218, HTTP/2 prévoit peu de capacités d'extensions du protocole, considérant qu'il vaudra mieux, si on veut l'étendre un jour, passer à un nouvelle version, négociée grâce à ALPN (cf. RFC 6709.)

En conclusion, on peut dire que la conception d'un nouveau protocole (ou d'une nouvelle version d'un protocole existant) pour que la transition se passe vite et bien, reste un art plutôt qu'une science. Mais on a désormais davantage d'expérience, espérons qu'elle sera utilisée dans le futur.

---