RFC 6589 : Considerations for Transitioning Content to IPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 23 avril 2012

Date de publication du RFC : Avril 2012

https://www.bortzmeyer.org/6589.html

Ce document rassemble un certain nombre d'analyses et de conseils sur la transition vers IPv6 pour les gens qui hébergent du contenu, typiquement les sites Web. Les gérants de ces sites souhaiteraient pouvoir rendre ce contenu accessible en IPv6, sans que cela entraîne de conséquences fâcheuses pour les lecteurs. Ce RFC décrit notamment la technique du "*whitelisting*", qui consiste à ne renvoyer d'adresses IPv6 (les enregistrements AAAA du DNS) qu'à certains réseaux, identifiés comme mettant en œuvre correctement IPv6. Cette technique a été popularisée par Google mais elle est contestée. Le RFC estime qu'elle est acceptable et qu'il est utile d'informer, non pas les sites qui la pratiquent (ils connaissent déjà) mais la communauté Internet en général.

Bien sûr, ce RFC peut être utile à d'autres qu'aux gérants de sites Web. Mais il se focalise particulièrement sur leurs besoins. Un site Web se caractérise par un gros déséquilibre : au lieu de deux pairs qui veulent communiquer, on a un fournisseur de contenu, et des clients passifs, à qui on ne peut pas demander d'effectuer des réglages particuliers. Ça doit marcher, point. En outre, les sites Web à plus fort trafic sont souvent des entreprises commerciales, qui ne veulent pas prendre de risques et n'acceptent pas même un très faible pourcentage de clients pénalisés par IPv6.

Le but est donc de migrer de gros sites Web uniquement accessible en IPv4 (la grande majorité des gros sites Web à l'heure actuelle, la principale exception étant Google) vers un accès possible en IPv4 (protocole qui ne va pas disparaître de si tôt) **et** IPv6.

Mais quels sont les problèmes qu'IPv6 pourrait causer ? Le site Web typique publie son adresse dans le DNS. Pour l'adresse IPv4, il utilise un enregistrement de type A. Pour IPv6, de type AAAA. Ainsi, aujourd'hui, `www.bortzmeyer.org` annonce deux AAAA et un A :

```
% dig A www.bortzmeyer.org
...
;; ANSWER SECTION:
www.bortzmeyer.org.     42641   IN      A       204.62.14.153
...

% dig AAAA www.bortzmeyer.org
...
;; ANSWER SECTION:
www.bortzmeyer.org.     10222   IN      AAAA    2605:4500:2:245b::bad:dcaf
www.bortzmeyer.org.     10222   IN      AAAA    2001:4b98:dc0:41:216:3eff:fece:1902
...
```

Par contre, la très grande majorité des sites Web ne publient que des A, par exemple `www.gouvernement.fr` :

```
% dig A www.gouvernement.fr
...
;; ANSWER SECTION:
www.gouvernement.fr.    86383   IN      CNAME   www.premier-ministre.gouv.fr.
www.premier-ministre.gouv.fr. 86383 IN  CNAME   cdn2.cdn-tech.com.c.footprint.net.
cdn2.cdn-tech.com.c.footprint.net. 213 IN A     209.84.9.126
...

% dig AAAA www.gouvernement.fr
...
;; ANSWER SECTION:
www.gouvernement.fr.    86358   IN      CNAME   www.premier-ministre.gouv.fr.
www.premier-ministre.gouv.fr. 86358 IN  CNAME   cdn2.cdn-tech.com.c.footprint.net.
...
```

Certains de ces sites sont simplement gérés par des incompétents ou des paresseux, qui ne peuvent pas ou n'envisagent pas de publier des enregistrements AAAA, qui permettraient à leur lecteurs d'accéder au contenu en IPv6. Mais, dans d'autres cas, l'administrateur du site Web connaît IPv6, a refléchi, et a décidé de ne pas publier le AAAA. Pourquoi ? Parce qu'il craint le problème du **malheur des globes oculaires** ("*eyeball misery*" ?). J'ai décrit ce problème dans un autre article <`https://www.bortzmeyer.org/globes-oculaires-heureux.html`> et il fait en outre l'objet de deux autres RFC, les RFC 6555[1] et RFC 6556. En deux mots, le malheur des globes oculaires peut venir d'une connexion IPv6 cassée, ou simplement de qualité très inférieure. Si le site Web ne publie pas d'enregistrement AAAA, le client ne tentera pas de se connecter en IPv6 et sa connexion pourrie n'aura donc pas de conséquences négatives. Mais dès que le site Web publie son AAAA, patatras, l'expérience utilisateur se dégrade sérieusement et le pauvre client doit supporter des délais, voire des pannes.

Le problème n'arriverait pas si les administrateurs réseaux prenaient autant soin de la connexion IPv6 que de l'IPv4 mais ce n'est pas toujours le cas en pratique : quand un des deux protocoles marche nettement moins bien que l'autre, aujourd'hui, c'est presque toujours IPv6. Logiciels moins testés, surveillance moins sérieuse, moindre réactivité lors des pannes, sont la triste réalité d'IPv6 chez beaucoup d'opérateurs réseaux. Un autre problème est quantitatif : certaines bogues ne se déclenchent qu'à partir d'une certaine quantité de trafic et les tests en laboratoire ne les détectent donc pas. Si un gros site Web très populaire publie tout à coup des enregistrements AAAA, on peut imaginer que l'augmentation de

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6555.txt`

trafic résultante plante des équipements réseaux qui marchaient l'instant d'avant. Ou, tout simplement, dépasse leur capacité (section 2.3 de notre RFC). Prenons l'exemple d'un FAI qui déploie 6rd (RFC 5969) et le fait tourner sur trois vieux PC avec Linux (le noyau Linux a désormais 6rd en standard), cela peut marcher très bien tant que les utilisateurs font un peu de ping6 et traceroute6, et ne pas suffire si tout à coup YouTube devient accessible en IPv6.

Bien sûr, tous les sites Web ne sont pas logés à la même enseigne, car ils n'ont pas tous le même public. <http://www.ietf.org/> a un AAAA depuis très longtemps, sans problèmes. Mais son public, les gens qui suivent le travail de l'IETF, ne ressemble pas à celui de TF1 : il est nettement plus soucieux de la qualité de sa connexion et s'assure qu'elle marche en v4 et en v6. D'autres sites Web qui ont un public moins "*geek*" ne veulent pas prendre le moindre risque.

Quelle est l'ampleur de ce risque ? Quelques organisations ont fait des études sur le malheur des globes oculaires et trouvent jusqu'à 0,078 % de malheureux. C'est évidemment très peu mais cela fait encore trop de monde pour un gros site Web qui a des millions de visiteurs. (Voir les études « "*IPv6 & recursive resolvers : How do we make the transition less painful ?*" <http://www.ietf.org/proceedings/77/slides/dnsop-7.pdf> », « "*Yahoo proposes 'really ugly hack' to DNS*" <http://www.networkworld.com/news/2010/032610-yahoo-dns.html> », « "*Evaluating IPv6 adoption in the Internet*" <http://www.google.com/research/pubs/archive/36240.pdf> » et « "*Measuring and Combating IPv6 Brokenness*" <http://ripe61.ripe.net/presentations/162-ripe61.pdf> ».) Le risque est donc jugé inacceptable par beaucoup de gérants de gros sites Web.

Bref, il faut trouver une solution. Sinon, le risque est que les gérants de sites Web les plus timides retardent éternellement la migration vers IPv6.

Alors, quelles sont les solutions possibles (section 4) ? Comme avec toutes les techniques de migration vers IPv6, il ne faut pas les appliquer toutes bêtement. Chacune a ses avantages et ses inconvénients et le choix de la meilleure technique dépend des caractéristiques du site Web qui veut se rendre accessible en v6. Première méthode, la plus satisfaisante techniquement, est de résoudre le problème à la source en s'assurant que tous les clients du site aient un IPv6 qui marche bien. C'est ainsi que cela fonctionne pour les sites Web qui visent un public technique, comme <http://www.ietf.org/> : les problèmes sont discutés et résolus collecivement. C'est en effet la meilleure solution sauf qu'elle est souvent impossible : au contraire de ce qui se passe pour le site Web interne à une organisation, le site Web public typique n'a pas de contrôle sur la connectivité de ses clients, ni sur le logiciel utilisé (navigateur Web, par exemple). Toutefois, s'il s'agit d'un gros site très populaire, il peut influencer les utilisateurs en recommandant ou en déconseillant des logiciels, des FAI, ou des configurations, par exemple via une page Web d'aide sur le site.

Comme le problème, par exemple d'un FAI donné, a des chances de toucher tous les gros sites qui servent du contenu, ceux-ci peuvent aussi se coordonner pour faire pression sur le maillon faible. Ce genre de coordinations entre acteurs différents n'est jamais facile mais elle a eu lieu pour le "*World IPv6 Day* " <http://isoc.org/wp/worldipv6day/>. En deux mots, celle approche du problème est possible mais sans doute insuffisante.

Deuxième tactique possible, avoir des noms de domaine spécifiques à IPv6 (section 4.2). Par exemple, à la date d'écriture de cet article, Facebook n'a pas d'enregistrement AAAA pour www.facebook.com (attention, cela dépend du résolveur qui demande, pour les raisons expliquées plus loin) mais il en a un pour www.v6.facebook.com. Ainsi, l'utilisateur naïf ne risque pas d'avoir des problèmes IPv6 mais l'utilisateur plus tenté par la technique pourra essayer l'accès en IPv6 et aider au déboguage initial. Cela permet une transition progressive, au lieu d'ouvrir les vannes en grand d'un coup. Et cela permet de tester la connectivité v6 du site, celle de certains de ses clients, d'introduire IPv6 en production (si le

nom en question bénéficie de la même surveillance et des mêmes exigences de qualité de service que les noms classiques).

Mais cette méthode ne permet pas d'aller très loin : comme il faut une action consciente de l'utilisateur pour se connecter en IPv6, le trafic restera très limité. Comme la population de testeurs n'est pas représentative, les logiciels ou FAI qui sont peu utilisés par les utilisateurs "*geeks*" ne seront pas réellement testés. Cette technique ne peut donc convenir qu'au tout début de la migration.

Une autre méthode, qui a été mise au point et popularisée par Google, et qui est la plus détaillée dans ce RFC, est le "*whitelisting*" (section 4.3). Il s'agit de configurer les serveurs DNS faisant autorité pour le domaine, afin de ne renvoyer d'enregistrements AAAA qu'aux clients dont on sait qu'ils ont de l'IPv6 correct, et qui ont été placés sur une **liste blanche**, indiquant les réseaux jugés corrects. Notez bien que la liste indique des réseaux, pas des machines individuelles. Non seulement il serait humainement impossible de gérer une liste de machines, mais en outre le serveur DNS faisant autorité ne voit pas la machine individuelle, il est interrogé par les résolveurs, typiquement des machines du FAI.

Cette technique ressemble donc à celle de certains systèmes de "*load-balancing*" ou de CDN (cf. sections 4.3.2 et 4.3.3, ainsi que le RFC 1794), qui eux-aussi renvoient une réponse DNS différente selon le client. Cela évoque donc aussi le "*split DNS*" (section 4.3.4) décrit dans la section 3.8 du RFC 2775. Le "*split DNS*" (conçu à l'origine pour renvoyer des réponses différentes au client du réseau local, par exemple des adresses RFC 1918) a toujours été très contesté. Les objections des sections 2.1 et 2.7 du RFC 2956 concernent surtout le fait que le FQDN n'est plus un identificateur stable, si la résolution DNS dépend du client. Cette fragmentation de l'espace de nommage est la principale raison pour laquelle beaucoup de gens n'aiment pas le "*whitelisting*".

Déployé par Google <http://www.google.com/intl/en/ipv6/>, le "*whitelisting*" est documenté dans l'article de C. Marsan « "*Google, Microsoft, Netflix in talks to create shared list of IPv6 users*" <http://www.networkworld.com/news/2010/032610-dns-ipv6-whitelist.html> » et dans celui de E. Kline « "*IPv6 Whitelist Operations*" <http://sites.google.com/site/ipv6implementors/2010/agenda/IPv6_Whitelist_Operations.pdf> ». Son principe est donc « plutôt que de résoudre le problème, masquons-le ».

Voici le "*whitelisting*" en action : je demande l'adresse IPv6 de `google.com` depuis Free, qui est "*whitelisté*".

```
% dig AAAA google.com
...
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
google.com.             300     IN      AAAA    2a00:1450:4007:802::1005
```

Par contre, depuis Orange, on n'a pas de réponse.

```
% dig AAAA google.com
...
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
...
```

Notez bien que le "*whitelisting*" est **complètement** indépendant du protocole utilisé pour le transport de la requête DNS. Le fait que le résolveur utilise IPv4 ou IPv6 pour interroger le serveur faisant autorité n'implique **rien** quant aux capacités v4 ou v6 de la machine cliente (celle sur laquelle tourne le navigateur Web). La liste blanche contient donc aussi bien des adresses IPv4 qu'IPv6.

Par définition, le fait d'être dans la liste blanche nécessite une évaluation du réseau client. Sa maintenance est donc non triviale et consomme des ressources humaines, nécessite des mesures, etc. Google peut se le permettre, mais ce n'est pas accessible à tout le monde.

Notez que cette technique nécessite d'avoir le contrôle de tous les serveurs faisant autorité sur le domaine, y compris les secondaires. Et qu'elle n'est pas toujours mise en œuvre dans les logiciels serveurs typiques, il faut donc se préparer à programmer un peu. Je n'ai pas testé mais je suppose qu'on peut mettre en œuvre le "*whitelisting*" sur BIND en utilisant les vues, avec deux fichiers de zone (un avec AAAA et un sans) et en définissant une ACL pour la liste blanche, dirigeant ses membres vers la vue ayant les AAAA :

```
acl v6-whitelist {
               192.0.2.0/24;
               2001:db8:3003::/48;
};
...
view "with-aaa" {
   match-clients { v6-whitelist; };
   zone "example.com" {
        ...
        file "/etc/bind/example.com-with-aaaa";
   };
};
view "external" {
   match-clients { any; };
   zone "example.com" {
        ...
        file "/etc/bind/example.com-without-aaaa";
   };
};
```

La solution n'est pas parfaite : un réseau peut avoir correctement déployé IPv6 mais un utilisateur peut avoir un navigateur Web qui a des problèmes avec IPv6. La liste blanche stockant des réseaux, les globes oculaires de cet utilisateur seront malheureux quand même. Mais cela reste une des meilleures solutions existantes.

Aujourd'hui, on l'a vu, cette solution est manuelle : les réseaux qui veulent être "*whitelistés*" soumettent leur candidature, sont évalués (ce qui peut nécessiter une interaction qui consomme donc également des ressources humaines du côté du FAI), et mis (ou pas) dans la liste. Dans le futur, on verra peut-être une automatisation de la procédure, avec des tests faits de temps en temps. Autre évolution possible, le passage en mode « liste noire » où tous les clients DNS recevraient l'enregistrement AAAA, sauf ceux explicitement listés dans la liste noire (section 4.4). Cela sera intéressant le jour où la majorité des FAI auront un IPv6 qui marche, et où seuls quelques maillons faibles subsisteront.

Un résumé des inquiétudes sur le "*whitelisting*" figure dans l'article de Brzozowski, J., Griffiths, C., Klieber, T., Lee, Y., Livingood, J., et R. Woundy, « "*IPv6 DNS Resolver Whitelisting - Could It Hinder IPv6 Adoption ?*" <http://www.comcast6.net/IPv6_DNS_Whitelisting_Concerns_20100416.pdf> ». Outre la fragmentation de l'espace de nommage, la principale inquiétude concerne l'introduction d'une nouvelle composante dans le réseau, qui rend le déboguage plus compliqué (un principe cardinal de l'Internet est que les décisions « politiques » doivent être faites aux extrémités, pas dans des équipements

intermédiaires, cf. RFC 3724 et l'article de Blumenthal, M. et D. Clark, « "*Rethinking the design of the Internet : The end to end arguments vs. the brave new world*" <http://dspace.mit.edu/bitstream/handle/1721.1/1519/TPRC_Clark_Blumenthal.pdf> » et, sur le cas spécifique du DNS, la section 2.16 du RFC 3234.) Un bon exemple est donné par les résultats de dig cités plus haut : déboguer l'accès à Google va dépendre du réseau où on fait le dig. De beaux malentendus peuvent alors survenir. Mais le débat est complexe : s'il y a un large consensus sur l'importance de ne **pas** mettre trop d'état et de décisions dans les équipements intermédiaires (le principe « de bout en bout »), la discussion a toujours fait rage sur qu'est-ce qu'un équipement intermédiaire. Est-ce qu'un serveur DNS fait partie des "*middleboxes*" qui perturbent si souvent la connexion de bout en bout ?

Enfin, la dernière tactique de migration possible est le saut direct (section 4.5) : activer IPv6 sur le serveur, le tester, puis publier un AAAA normal. Cela n'est pas forcément si radical que ça car on peut le faire nom par nom (par exemple, pour `static-content.example.com` avant `www.example.com`) mais c'est quand même la méthode la plus audacieuse. À ne faire qu'une fois qu'on maîtrise bien IPv6. Relativisons tout de même les choses : des tas de sites Web vus par un public non technique (comme <http://www.afnic.fr/>) ont un AAAA depuis de nombreuses années et sans que cela crée de problèmes.

Si on est toutefois inquiets, on peut utiliser cette tactique, mais pendant une période limitée : on teste, on publie le AAAA pendant quelques heures, on arrête, on analyse les résultats, on corrige les éventuels problèmes et on recommence.

Pour les lecteurs pressés, la section 5 résume les étapes possibles d'un plan de transition. Là encore, pas question de l'appliquer aveuglément. Chacun doit l'adapter aux caractéristiques spécifiques de son réseau. Rappelez-vous en outre que le RFC cible les gros sites : la plupart des petits n'auront pas envie d'autant d'étapes. Voici ces étapes potentielles successives :

- Uniquement IPv4 (malheureusement la situation de la grande majorité du Web aujourd'hui),
- Activation d'IPv6 et publication par des noms spécifiques, genre `www.ipv6.example.org`,
- Peut-être une étape de "*whitelisting*" avec gestion manuelle,
- Peut-être suivi par une étape de "*whitelisting*" automatique,
- Le "*whitelisting*" étant prévu pour être une étape temporaire, on va le couper, une fois les problèmes résolus. (Cela peut se faire lors d'une occasion un peu solennelle comme le "*World IPv6 Launch*" <http://www.worldipv6launch.org/> le 6 juin 2012.)
- À partir de là, le site est complètement accessible en IPv6 (et en IPv4), avec le nom de domaine normal.
- La section 6.3 discute du cas, très futuriste à l'heure actuelle, où certains auront une meilleur connectivité en IPv6 qu'en IPv4. Il faudra alors mettre au point des techniques de transition pour retirer l'accès IPv4 petit à petit.

Voici, vous connaissez maintenant l'essentiel. La section 6 du RFC liste quelques points de détail. Par exemple, contrairement à ce que certains pourraient croire au premier abord, le "*whitelisting*" est tout à fait compatible avec DNSSEC (section 6.1), puisqu'il se fait sur les serveurs faisant autorité. Ceux-ci peuvent donc parfaitement signer les deux versions de la réponse, avec ou sans AAAA, et ces deux réponses pourront être vérifiés comme authentiques.

Par contre, si un résolveur DNS s'avisait de faire des manipulations analogues au "*whitelisting*", par exemple en retirant les réponses AAAA vers des clients qu'il sait ne pas gérer IPv6 correctement, alors, là, DNSSEC détecterait la manipulation comme une tentative d'attaque, et la réponse ne pourrait pas être validée.

On a vu que la gestion d'une liste blanche représentait un certain travail. Il est donc tentant de partager les résultats de ce travail entre plusieurs acteurs. Mais attention à le faire en respectant la vie privée (section 6.2). Il n'y a pas de problèmes avec les listes actuelles, dont la granularité ne descend pas jusqu'à l'individu, mais, si des listes plus précises devaient apparaître, ce problème est à garder en tête.