RFC 7157 : IPv6 Multihoming without Network Address Translation

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 avril 2014

Date de publication du RFC : Mars 2014

https://www.bortzmeyer.org/7157.html

Pour la petite entreprise ou association, il est très intéressant d'être "*multi-homé*", c'est-à-dire d'avoir plusieurs connexions à l'Internet, afin d'être sûr que l'accès fonctionne toujours. Financièrement, acheter deux connexions Internet grand public, de fiabilité moyenne, est nettement moins cher qu'une seule connexion supposée de grande fiabilité. Il reste à permettre aux machines du réseau local à utiliser les deux connexions. En IPv4, cela se fait traditionnellement en utilisant le NAT, qui est de toute façon nécessaire en raison de la pénurie d'adresses <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html>. Et en IPv6 ?

On pourrait utiliser le NAT, comme le mettent en œuvre un certain nombre de boîtiers existants actuellement. Les machines du réseau local utiliseraient un seul préfixe, un ULA et le routeur traduirait vers les préfixes de l'un ou l'autre FAI (peut-être en tenant compte de la charge, du prix, etc). Mais le NAT a de nombreux inconvénients et l'un des buts d'IPv6 était justement de s'en débarrasser (ceci dit, si vous voulez tenter l'aventure, il existe un RFC sur ce sujet, le RFC 6296 [1], cf. section 7.1). Autre solution, faire du beau "*multi-homing*" propre avec des adresses PI et BGP. Mais c'est complètement hors de portée de la petite organisation, notamment par les ressources humaines que cela nécessite. (Voir le RFC 3582 pour un cahier des charges d'une solution idéale pour le "*multi-homing*".)

Je vous le dis tout de suite, il n'existe pas encore de solution propre et déployable pour ce problème. À court terme, le RFC 6296 reste la seule solution. Notre RFC explore ce qui pourrait être utilisé pour après, en supposant un réseau "*multi-homé*" avec plusieurs préfixes IP (MHMP pour "*multihomed with multi-prefix*"). C'est donc plutôt un cahier des charges qu'un catalogue de solutions.

A priori, IPv6 permet parfaitement d'avoir deux préfixes d'adresses (un par FAI, si on est "*multi-homé*" à seulement deux FAI) sur le même réseau. Mais cela laisserait les machines face à bien des problèmes :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6296.txt

— S'il y a deux routeurs (un pour chaque FAI), lequel choisir pour sortir ?
— Quelle adresse IP source choisir pour les connexions sortantes ? Notez que c'est lié au problème précédent : si le FAI met en œuvre le filtrage du RFC 2827, il faut choisir le préfixe correspondant au FAI de sortie.
— Et c'est encore pire si le FAI impose l'usage de ses résolveurs DNS car il y met des informations spécifiques à ses clients (comme Orange où `smtp.wanadoo.fr` et `smtp.orange.fr` donnent des résultats différents selon le réseau, interne ou externe).

Bref, simplement connecter le réseau local à deux FAI et distribuer leurs adresses sur ledit réseau ne suffit pas.

La section 3 décrit plusieurs scénarios typiques, pour rendre plus concret le problème. Le premier est celui où le réseau a deux routeurs, chacun connecté à un FAI et ignorant de l'autre routeur. C'est le cas par exemple de l'abonnement à deux FAI ADSL avec chaque FAI fournissant sa "*box*". Le deuxième scénario imagine un seul routeur sur le réseau local, connecté à deux FAI. L'unique routeur du réseau local peut publier sur le réseau local tout ou partie des informations (préfixe IP, résolveurs DNS) reçues. Ce scénario peut se trouver, entre autres, si on a un abonnement Internet plus un tunnel vers un fournisseur de VPN. Enfin, dans le troisième scénario, c'est la machine terminale qui a deux connexions et qui doit les gérer. C'est le cas du téléphone drôlement intelligent qui est connecté en WiFi et en 3G.

Quels vont être les principaux problèmes à résoudre avec ces trois scénarios (section 3.3) ?

— Dans le premier cas, celui à deux routeurs, la sélection, par une machine du réseau local, de son adresse IP source, en cohérence avec le routeur choisi pour la sortie (si elle se trompe, le paquet sera refusé par le FAI s'il met en œuvre le RFC 2827), et la répartition de charge (chaque machine n'enverra du trafic qu'à un seul routeur),
— Dans le deuxième scénario, avec un seul routeur sur le réseau local, le même problème de sélection d'adresse IP source, si le routeur publie les deux préfixes sur le réseau local, et la sélection du FAI de sortie par le routeur,
— Pour le troisième exemple, celui de la machine terminale à plusieurs connexions, le manque d'informations (sur la facturation, par exemple) pour décider quel trafic envoyer à quelle interface (curieusement, notre RFC ne cite pas l'excellent RFC 6419, entièrement consacré à cette question des machines terminales "*multi-homées*").

Et, dans les trois scénarios, le problème du résolveur DNS, si les deux résolveurs ne donnent pas les mêmes résultats.

Maintenant, il faut résoudre ces problèmes, en respectant deux principes (section 4) : maintien du principe de bout en bout (donc pas de NAT), puisque c'est l'un des principaux buts d'IPv6, et passage à l'échelle, la solution devant fonctionner même pour des gros déploiements.

Les sections 5 et 6 explore les angles d'attaque possibles. Pour la sélection de l'adresse IP source (sections 5.1 et 6.1), la référence actuelle est le RFC 3484, qui est loin de donner un résultat optimum, puisqu'il utilise uniquement l'adresse IP de destination (dans la scénario 1 ci-dessus, il ne garantit pas qu'on sélectionne une adresse qui correspondra au routeur de sortie). Une approche actuellement étudiée à l'IETF serait de distribuer (par exemple en DHCP), depuis le routeur, des politiques de sélection d'adresse (actuellement, elles sont configurées dans chaque machine, `/etc/gai.conf` sur la plupart des Linux, par exemple). Pour que ces politiques soient complètes, cela nécessitera la coopération du FAI..

Pour la sélection du routeur (sections 5.2 et 6.2), c'est à peu près la même chose : les machines terminales n'ayant actuellement pas assez d'informations pour prendre une décision intelligente, il faudra leur envoyer (via DHCP), les informations permettant de choisir le routeur. Une telle information ne peut pas facilement être transmise avec les RA ("*Router Advertisement*"), qui ne permettent pas d'envoyer des informations différentes selon la machine. (On pourrait envisager d'utiliser les protocoles

de routage eux-mêmes mais il y a bien longtemps qu'on a cessé de les faire tourner sur les machines terminales, et pour de bonnes raisons.)

Enfin, pour le dernier gros problème, la sélection du résolveur DNS (sections 5.3 et 6.3), notre RFC rappelle que les machines ont pu connaître le résolveur via DHCP (RFC 3646) ou RA (RFC 8106). Dans le cas du "*multi-homing*", la machine aura typiquement plusieurs résolveurs DNS. Parfois, il faudra utiliser un résolveur spécifique pour un domaine donné (dans l'exemple d'Orange, cité plus haut, il faut utiliser les résolveurs d'Orange pour les noms en `wanadoo.fr`, car on obtient des résultats différents avec les serveurs publics). Cette pratique, connue sous le nom de "*split DNS*" est typiquement très mal vue (entre autres, elle rend le débogage très compliqué) mais elle existe. Notre RFC décide donc, sans l'entériner, de « faire avec ».

Là encore, un travail est en cours à l'IETF pour normaliser une politique de sélection du résolveur, en fonction du domaine à résoudre, et distribuée par DHCP (RFC 6731).

Bien sûr, il existe des tas d'autres techniques qui peuvent aider dans ce cas du "*multi-homing*". Le RFC cite SHIM6 (RFC 5533), SCTP (RFC 4960), HIP <`https://www.bortzmeyer.org/hip-resume.html`> (RFC 5206), etc. Mais elles sont aujourd'hui trop peu déployées pour qu'on puisse compter dessus.

Enfin, la section 8 nous rappelle que tout ceci va certainement poser des problèmes de sécurité amusants. Par exemple, si on distribue une politique de sélection (d'adresse IP source, de résolveur DNS, etc) sur le réseau, il y aura toujours des machines qui n'obéiront pas. Contrôle et filtrage resteront donc nécessaires. D'autre part, il existe déjà aujourd'hui des serveurs DHCP pirates, qui répondent à la place du vrai, et le problème sera pire encore lorsque des politiques de sélection (de routeur, de réolveur DNS, etc) seront distribuées via DHCP.