

Fiche "IPv6"

- **Auteur** : Stéphane Bortzmeyer (AFNIC)
- **Dernière mise à jour** : 03/03/2009
- **Diffusion** : "Portail / Tout-Public"

L'Internet vit depuis plus de dix ans une difficile transition du protocole IPv4 vers IPv6. Les progrès réalisés, quoique réels, sont si lents, et la réalité actuelle si stable (le seul Internet qui compte est en IPv4) que certains se demandent même si la transition sera un jour finie.

Il est donc utile de revenir sur la situation d'IPv6, notamment dans le contexte de THD, où on envisage des nombreux utilisateurs connectés en permanence, disposant de grandes capacités réseau, et pouvant donc utiliser des applications qui seraient irréalistes aujourd'hui (comme la diffusion vidéo en pair-à-pair).

Oublions les différentes proclamations journalistiques qui avaient été faites sur le futur d'IPv6 et sur ses merveilleuses possibilités. Ne gardons que deux faits solides :

- le fait que le protocole réseau soit IPv4 ou IPv6 ne devrait normalement avoir aucune importance pour les utilisateurs, ni même pour la plupart des programmeurs. Ce détail de couche 3 devrait rester caché à la plupart, et ne pas faire l'objet de grands discours.
- le nombre d'adresses libres en IPv4 ne peut que décroître (les restitutions sont exceptionnelles, alors que les usages de l'Internet se développent) et donc la famine est certaine, contrairement à ce que certains affirment.

Si la famine n'est pas encore là (elle est prévue entre 2010 et 2012, (<http://www.bortzmeyer.org/epuisement-adresses-ipv4.html>)), la pénurie a commencé depuis longtemps : avoir des adresses IPv4 est depuis des années un parcours du combattant. Dans les régions les plus mal servies, une université de plusieurs dizaines de milliers d'étudiants ne peut décrocher que 16 adresses IP (cas de l'université de Cocody en Côte d'Ivoire). Même en France, on voit des "hôtels d'entreprises" qui fournissent une "connexion Internet" ... sans adresse IPv4 publique. Enfin, pour le particulier, avoir plus

Plate-forme THD : plate-forme ouverte d'expérimentations de contenus et de services très haut débit opérée par le pôle de compétitivité Cap Digital Paris Région – <http://www.portailthd.fr/>

qu'une seule adresse IPv4 publique est quasiment impossible.

Qu'est-ce qu'une adresse publique, au fait ? Ce sont les adresses IP normales, celles qui sont uniques dans le monde et permettent donc de communiquer directement avec n'importe quelle autre machine. Il existe également des adresses IP privées, normalisées dans le RFC 1918, qui ne sont pas uniques et qui ne peuvent donc pas être utilisées normalement (pour accéder à l'Internet, elles demandent des techniques spécifiques, souvent assez fragiles).

À l'époque où la possession d'un seul PC à la maison était déjà rare, n'avoir qu'une adresse IP n'était pas trop gênant. Mais aujourd'hui, le veinard connecté en très haut débit a probablement chez lui plusieurs appareils susceptibles de parler IP et d'utiliser le réseau : plusieurs ordinateurs, des "smart phones", un lapin Nabaztag, etc. La limite à une adresse IP publique par abonné est donc déjà gênante.

Est-ce grave d'avoir des adresses IP privées pour les machines ? Pas trop si elles n'ont besoin que de connectivité locale.

Mais d'autres machines ont un besoin légitime de communication de bout en bout. Un téléphone, par exemple, a clairement besoin de parler au monde extérieur. Comment font-ils avec des adresses privées ? Ils se débrouillent. Un grand nombre de bricolages ont été mis au point, comme la traduction d'adresses (NAT). Cela marche mais les coûts de développement sont élevés, et cela rend les applications très fragiles (comme tout utilisateur de la téléphonie sur IP peut en témoigner). En effet, ces bricolages cassent la communication de bout en bout, principe cardinal de l'architecture Internet. On arrive à ce paradoxe que les applications réseau doivent consacrer l'essentiel de leur code à contourner le NAT ! Seules les applications strictement client-serveur comme le Web se débrouillent à peu près correctement avec le NAT (encore que Google Maps, gros consommateur de connexions, réussisse à "planter" certains routeurs NAT, en utilisant davantage de ports qu'ils ne peuvent en allouer à leurs divers clients).

Donc, lorsque toutes les adresses IPv4 seront épuisées, pourra-t-on se contenter de ces bricolages ? Seulement si on accepte un Internet sérieusement amputé (il faut noter qu'il n'existe pas de définition commerciale de "connexion Internet" et on voit donc des hôtels annoncer une connexion Internet... sans préciser que l'adresse IP sera privée et que des limites du traducteur d'adresses empêcheront la téléphonie sur IP ou le VPN de fonctionner. Le RFC 4084 propose un vocabulaire standard pour décrire ces connexions "pas vraiment Internet", cf. <http://www.bortzmeyer.org/4084.html>).

Après l'épuisement de la dernière adresse IPv4, on verra donc les utilisateurs se partager en deux : ceux qui doivent se résigner à vivre derrière un NAT et à accepter que beaucoup d'applications, notamment pair-à-pair ne fonctionnent pas. Et ceux qui ont de l'argent et qui pourront acheter des adresses IPv4 sur le marché, marché qui sera

alimenté par les spéculateurs qui stockent des adresses qu'ils n'utilisent pas, pour les revendre après le déclenchement de la famine.

Le déploiement d'IPv6 est donc nécessaire si on veut éviter de se résigner à un Internet limité ou si on n'a pas suffisamment d'argent pour payer les prix du marché. Mais où en est-on et pourquoi est-ce aussi difficile ?

Aujourd'hui, le déploiement d'IPv6 est soit très avancé, soit presque inexistant, selon les critères qu'on choisit. Du plus avancé au moins avancé, les points à considérer sont :

- quasiment toutes les normes Internet sont désormais compatibles avec IPv6.
- quasiment tous les systèmes d'exploitation gèrent l'IPv6 (il y a encore des manques dans les routeurs de bas de gamme et certains équipements de filtrage ou de répartition de charge).
- les RIR (registres d'adresses IP) délivrent tous des adresses IPv6.
- les serveurs DNS de la racine et de tous les TLD importants ont des adresses IPv6.
- les grands logiciels (serveur HTTP Apache, serveur de courrier Postfix, navigateur Firefox, etc) ont tous IPv6 en série (il y a en revanche un très gros manque d'IPv6 chez le logiciel de bas de gamme).
- certains opérateurs, hébergeurs ou fournisseurs d'accès proposent IPv6 à leurs abonnés (mais presque toujours sous forme d'un service inférieur, avec notamment une réparation des pannes bien plus lente). En France, Nerim a montré la voie. Ce service est réparti très inégalement sur la planète (courant en Europe, variable en Asie, rare aux États-Unis, inexistant en Afrique).
- pour les clients des autres fournisseurs, il existe de très nombreux fournisseurs de solutions de connexions alternatives, à base de tunnel. La fiabilité n'est pas toujours au rendez-vous et les tunnels soulèvent leurs propres problèmes.

Résultat, selon une étude très détaillée de Google :

http://www.ripe.net/ripe/meetings/ripe-57/presentations/Colitti-Global_IPv6_statistics_-_Measuring_the_current_state_of_IPv6_for_ordinary_users_.7gzD.pdf

Google est le seul moteur de recherche à offrir un accès en IPv6, mais qui n'est pas activé par défaut), seuls 0,238% des utilisateurs accèdent à Google en IPv6 lorsque cet accès est activé. Pire, pour 0,09% des utilisateurs, l'accès IPv6 ne marche pas ou pas suffisamment et l'accessibilité en IPv6 est donc un recul.

Le problème de l'oeuf et de la poule n'a jamais été aussi évident : les opérateurs affirment qu'ils n'ont pas de demande des clients, les clients ne demandent pas car il y a peu de services accessibles en IPv6 et les gérants des services disent qu'il n'y a pas de demande...

L'intérêt collectif serait qu'IPv6 soit déployé mais la somme des intérêts individuels fait que le déploiement effectif reste très faible.

Quelques références sur IPv6 :

- <http://fr.wikipedia.org/wiki/IPv6>
- <http://www.g6.asso.fr/> : Groupe et association francophone pour le déploiement et la promotion d'IPv6 ; voir également le livre IPv6 co-écrit par des membres du groupe : <http://livre.g6.asso.fr/>
- <http://www.afnic.fr/actu/nouvelles/207/1-afnic-lance-dnswitness-logiciel-multi-usage-de-mesures-dns.html> : Mesures faites par l'AFNIC