

IPv6, un enjeu d'aujourd'hui pour préparer l'avenir

1. Introduction

Dès les débuts "en production" d'IPv4 (comprenez au début des années 90), l'évolution des réseaux sur ce protocole est apparue comme limitée. La conception même d'IPv4 limitait la quantité d'équipements susceptibles de s'inter-connecter. L'arrivée en 1992 d'activités commerciales sur Internet a décuplé le nombre de machines connectées. Des technologies comme le NAT (Network Address Translation, la possibilité d'avoir plusieurs machines connectées derrière un *frontal*) sont alors apparues pour palier à court terme à ce problème. C'est alors que des groupes de chercheurs se sont mis à étudier la possibilité d'un nouveau protocole de transport. Il allait s'appeler IP version 6.

Peut-être vous êtes vous posé vous même les questions qui sont dans toutes les bouches : "Pourquoi passer à IPv6 puisque IPv4 fonctionne parfaitement à l'usage ?", "Pourquoi tout remettre en cause alors qu'IPv4 est universellement reconnu comme un standard ?", etc. Et vous avez raison de vous les poser. C'est donc ce à quoi je vais essayer de répondre dans un premier temps. Dans un second temps, j'aborderai plus les aspects techniques d'IPv6, ce que cela permet, ce qu'il faut faire ou éviter... Enfin, pour finir, j'essaierai d'aborder la question de la migration d'un point de vue prévisionnel.

2. Enjeux

2.1. La quantité d'adresses

IPv4 ne permet plus, aujourd'hui, d'adresser simplement et universellement tous les équipements du monde. Ce manque peut se constater tous les jours. Pour s'en rendre compte, il suffit de regarder du côté des technologies développées sur IPv4 (comme le NAT).

De plus, les États-Unis ayant été les premiers à déployer les bases du réseau mondial, ils se sont arrogés énormément d'adresses IPv4. Aujourd'hui, ce sont les plus gros détenteurs d'adresses de classe A ¹. Ainsi, si on prend la répartition géographique des adresses IPv4, on retrouve (je ne garantis pas l'exactitude des chiffres que j'avance) 73% des adresses aux USA, et le reste que se partagent l'Asie (le Japon, la Chine avec 1,2 milliard d'habitants, les Indes, la Russie, etc...), l'Europe, l'Afrique, l'Amérique du Sud... Comme on peut le voir, en sachant que le réseau des réseaux prendra une part stratégique dans le développement économique de demain, IPv4 met d'ores et déjà beaucoup de nations à l'écart de cet avenir (aujourd'hui la Chine aurait 22 millions d'adresses IPv4 pour 17 million d'internautes et 1.2 milliard d'habitants).

Ce premier point est déjà un point extrêmement décisif pour la migration vers IPv6. D'autant que le nombre d'équipements potentiellement connectables au réseau mondial ne va pas cesser de croître, et ce dans des proportions que l'on n'est pas encore aptes à considérer. (Le mot "équipement" n'a pas été choisi au hasard... Il se peut tout à fait que la future suspension "intelligente" de votre voiture ait un intérêt à être reliée au Réseau.)

2.2. Le routage au coeur du réseau mondial

Depuis quelques années, le nombre de "routes" stockées dans les mémoires des grands routeurs du coeur du réseau ne cesse d'augmenter. Il y a quelques années, nous étions autour des 80.000 routes; aujourd'hui, nous sommes à 120.000 routes. Cela signifie clairement que les besoins en mémoire et en temps de traitement augmentent sans cesse. Et les prévisions donnent des résultats encore plus impressionnants pour les années à venir.

Cette montée en puissance peut avoir deux solutions :

- Ajout "continu" de mémoire dans les routeurs
- Passage à un nouveau protocole de transport (IPv6) intégrant des solutions à ce souci

La première est celle qui est à l'ordre du jour actuellement, et elle ne suffit plus. C'est pour cette raison que la seconde solution est plus que d'actualité, car c'est aujourd'hui que les grandes décisions de demain se prennent.

Les adresses IPv6 ont été conçues de manière à hiérarchiser le réseau. Avec IPv4, l'adressage était anarchique. Du coup, les routeurs centraux se devaient de connaître tous les réseaux joignables. Avec IPv6, les routeurs centraux n'auront à connaître que les préfixes de ces réseaux. Les routeurs suivants n'auront qu'à re-subdiviser, et ainsi de suite. De cette manière, on évite une mémorisation exhaustive de toutes les routes et de tous les réseaux.

Cette explication est un peu *raccourcie*, mais j'espère qu'elle vous aura permis de comprendre grossièrement l'impact d'IPv6 sur le 6Bone, le coeur du réseau.

3. Aspects techniques

3.1. L'adressage

L'adressage est l'évolution majeure (devrais-je dire la plus visible ?) qu'apporte IPv6 par rapport à IPv4... et ce sur de nombreux aspects. Une grande partie d'entre eux ont déjà été vu dans la partie précédente. En résumé :

- Adressage sur 128 bits, entre 1.564 et 3.911.873.538.269.506.102 adresses par m² de surface terrestre (océans inclus).
- Adressage hiérarchique, découpage "géographique" clair via les préfixes, allègement de la charge des routeurs centraux.

Pour approfondir un peu cette notion d'adressage hiérarchique, prenons un exemple concret avec les adresses unicast (reprise du concept classique des adresses IPv4) :

- Lors de la définition des types d'adresses IPv6, il a été défini que les adresses unicast mondiales allaient toutes commencer avec un préfixe de 3 bits, 001, autrement dit de 2000::/3 (équivalent au niveau notation de 2000:0000:0000:0000:0000:0000/3).

- Sur ce premier préfixe vient s'ajouter une unité d'agrégation haute (TLA, Top Level Aggregator) sur 13 bits. Ces préfixes, sur 16 bits au total, sont donnés aux opérateurs internationaux gérant l'adressage sur le réseau mondial. Ainsi on trouve couramment des adresses dont les 16 premiers bits commencent par 2001, ce qui signifie que l'opérateur international s'est vu acquérir le préfixe 2001::/16.
- Ensuite viennent 8 bits réservés pour la possible évolution future des besoin en TLA ou en NLA (on y vient).
- Sur ces 24 bits viennent se rajouter encore 24 bits dis NLA (Next Level Aggregator) ou unités d'agregation basse. Ce sont les plages de NLA qui sont distribués aux opérateurs nationaux. Le plus souvent les plages NLA données aux opérateurs ont leurs 32 premiers bits fixes, leur laissant ainsi la possibilité de redistribuer des "/48", avec donc les 48 premiers bits fixes, à leurs clients. Par exemple, Nerim possède la plage suivante : 2001:7a8::/32.
- Ces mêmes opérateurs sont ainsi habilités à redistribuer des adresses sur 48 bits dont 16 auront été définies par leurs soins. Nous avons par exemple ici la plage d'adresses 2001:7a8:4b09::/48.
- Après les 48 premiers bits, nous arrivons sur la topologie de site, dite SLA (Site Level Aggregator). Elle se décrit sur 16 bits.
- C'est l'identifiant d'interface qui définit ensuite les 64 derniers bits.

Avec les possibilités d'adressage que nous avons vu, on peut déjà imaginer demain toutes les ouvertures que cela implique, surtout avec les objets communicants. C'est aussi dans cette optique que IPv6 veut essayer de prévoir les évolutions à venir. Qui sait où en seront les besoins dans 15 ans ?

Au delà de l'élargissement considérable du nombre d'adresses IPv6, cette évolution forcée du protocole a amené les chercheurs à se questionner sur les manques d'IPv4. C'est à partir de cette réflexion que sont apparues les autres fonctionnalités majeures d'IPv6 :

3.2. L'intégration de fonctionnalités

L'auto-configuration

La facilité de configuration... "tout ce fait tout seul". Voilà un argument de vente majeur pour les industriels ayant des intérêts dans IPv6. Il y a deux raisons à l'émergence d'une telle idée. L'évolution de l'auto-configuration d'IPv4, et la mobilité.

Avec IPv4, les problèmes de mise en place ont toujours été une difficulté. Ils avait été contournés partiellement par le protocole DHCP mais cela n'était pas très "propre" (émissions de paquets en broadcast). De plus DHCP ne pouvait pas répondre à tous les besoins de mobilité et exigeait qu'un client soit installé et configuré sur toutes les machine du réseau. Ainsi, IPv6 introduit directement dans son fonctionnement interne ce genre de mécanisme. Cela comporte plusieurs intérêts, allant de la possibilité de mobilité à la simplicité de mise en place (il suffit de dire à son système "je veux que tu t'auto-configures").

L'auto-configuration fonctionne de manière très simple. Au moment de la reconnaissance par la couche *liaison de donnée*², la couche réseau (IP) se voit assigner une adresse dite de "lien local" permettant de dialoguer avec tous ses proches voisins. C'est à partir de ce moment là qu'elle peut (la couche réseau) définir ses différentes routes, ses adresses de portée ("scope") globale, etc...

La mobilité

En effet, IPv6 intègre des fonctionnalités dites de *roaming* (passage d'un réseau physique à un autre, à la manière des téléphones portables passant d'une antenne à une autre au fil de ses déplacements). Grâce à ces fonctionnalités, il sera possible de changer de réseau, et donc d'adresse IP, de manière totalement transparente à l'utilisation.

Ce concept de mobilité est quelque chose de véritablement nouveau par rapport à IPv4. En effet, la "mobilité" existait déjà, entre autre via le protocole DHCP, mais de manière véritablement moins poussée. Il s'agissait là de pouvoir essentiellement connecter un ordinateur portable sur différents réseaux avec le minimum de configuration possible. Aujourd'hui, DHCP existe aussi sur IPv6 (plus communément connu sous le nom de DHCPv6) mais revient avec les mêmes défauts (déjà vu) et les mêmes qualités (possibilité de mise à jour automatisée des DNS, etc...) que sur IPv4.

Cette possibilité de mobilité va permettre le développement et le déploiement d'un grand nombre de technologies comme l'informatique embarquée, l'UMTS (téléphonie portable), etc... Ça fait déjà partie des grandes avancées de demain en matière de technologie.

La sécurité

Les notions de sécurité sont apparues assez tardivement avec IPv4, ce qui explique la manière avec laquelle cela était implémenté (IPsec) : rien d'intégré directement au protocole... A notre époque où la "sécurité" est autant un argument économique et politique qu'une réelle nécessité, IPv6 se devait de mettre en oeuvre de manière native des solutions permettant de palier ce défaut majeur d'IPv4.

Avec IPv6, grâce aussi au principe d'auto-configuration, nous devrions voir naître l'universalisation de l'aspect cryptographique des échanges sur les réseaux. Voilà encore l'une des qualités non négligeables de ce nouveau protocole : l'intégration directe de la sécurité dans IPv6. Ainsi toute machine implémentant IPv6 sera capable de communiquer de manière sécurisée, et ce de bout en bout (quantité d'adresses IP, et capacités de cryptographie intégrées).

3.3. Le DNS

Depuis longtemps, l'utilisation directe d'adresses IP est déconseillée. On préfère donc utiliser le nom de domaine désiré, en laissant sa résolution au système. IPv6 va encore amplifier cette tendance : adresses conséquemment plus longues, auto-configuration, mobilités, etc... C'est pourquoi l'importance des DNS dans l'Internet de demain va encore croître par rapport à ce qu'il n'est aujourd'hui. Pourtant, dès maintenant, le DNS est un service clé, voire critique. Il suffit de se rappeler les tentatives de déni de service sur les DNS root.

Ainsi, comme toute ressource critique, il y a des précautions à prendre pour la migration vers IPv6. Deux principes sont à garder en mémoire :

- Un domaine DNS doit pouvoir être joint aussi bien en IPv4 qu'en IPv6, au risque de limiter la diffusion de son information;
- Un serveur DNS doit fournir un même contenu, quelque soit le protocole par lequel on y accède (IPv4 ou IPv6).
- Tous les serveurs d'une même zone doivent être capables de comprendre les enregistrements AAAA (IPv6), sinon quoi vous irez au devant de sérieux problèmes. Pour cela, si vous utilisez bind, il faut utiliser des versions supérieures ou égales à bind-8.1.x.

Une fois toutes ces contraintes respectées, il ne reste plus qu'à implémenter vos adresses IPv6 telles des adresses IPv4. Le changement, une fois cette barrière franchie, n'est somme toute pas si compliqué que ça...

3.4. Et au delà...

Les interfaces réseaux et IPv6

Une interface réseau supportant IPv6 est dans l'"obligation" d'avoir la possibilité de posséder plusieurs adresses IPv6. Par exemple, nous le verrons plus loin, toute interface supportant IPv6 possède une adresse par défaut, dite de lien local. En plus de cette adresse, il doit être possible de rajouter des adresses autres, par exemple visibles depuis l'Internet. Ainsi, grâce à cette fonctionnalité, un serveur peut posséder un grand nombre d'adresses. Par exemple, une par site web hébergé (dans le cas d'un serveur web), ou une par service (HTTP, DNS, etc...).

Les adresses locales

IPv6 implémente une notion de portée (scope) sur certaines adresses.

Ainsi, dès la connexion physique au réseau, votre interface IPv6 prend une adresse dite de *lien local* (*Link-Local*). Ces adresses sont forcément dans la plage fe80::/10. De manière plus large, il existe un autre type d'adresse à la portée limitée. Il s'agit d'adresses de *lien de site* (*Site-Local*). Leur préfixe est FEC0::/10. Ce sont des adresses qui sont quand même routables, mais que en local.

Pour ces deux types d'adresses, les routeurs "publics" ne routeront pas de tels datagrammes. Pour la première (*lien local*), il s'agit des machines connectées physiquement sur le même réseau (pas de routeur à passer par exemple). Avec ce type d'adresse, les datagrammes envoyés ne pourront passer aucun routeur. Pour la seconde (*lien de site*), cela permet d'interconnecter des machines présentes sur un même site géographique. Des datagrammes envoyés sur ces adresses pourront passer les routeurs du site, mais seront bloqués à leur arrivée sur le premier routeur de l'Internet.

Multicast

Le multicast est une technique qui existait déjà avec IPv4 mais qui aura peut-être la chance de se voir démocratiser avec IPv6. En effet, le multicast IPv4 est très peu répandu du fait du manque de support de ce protocole par certains matériels réseaux (entre autre les routeurs se situant en bout de chaîne, comprenez juste après votre point d'entrée sur l'Internet). Une documentation NetBSD³ dit que « les spécifications d'IPv6 elles-mêmes utilisent intensivement le multidestinataire ». Ainsi, nous pouvons raisonnablement espérer que l'arrivée d'IPv6 amènera le multicast à la porte de chaque connecté.

Les applications concrètes du multicast utilisées massivement sont nombreuses et de taille. Il peut s'agir entre autre de vidéo-conférences, de télé-applications, de traitements répartis, de jeux, de télévision sur Internet, etc...

En IPv6, les adresses multicast sont toutes préfixées de fe00::/8. Pour plus de détails sur le fonctionnement du multicast, vous pouvez vous référer à la documentation de Jérôme DURAND (<http://www.renater.fr/Video/IPv6/IPv6Multicast/Index.htm>) (INSA Lyon, Association Aristote et GIP Renater) traitant du multicast IPv6 dans Renater. C'est une présentation en SMIL (recommandation du W3C) avec un support PDF téléchargeable zippé (désolé, je n'ai pas trouvé mieux pour le moment). Sinon, je ne peux que vous conseiller de lire le livre du G6 (<http://www.oreilly.fr/catalogue/ipv6-3ed.html>) (comité d'experts d'IPv6) aux éditions O'Reilly qui détaille cela très bien.

Anycast

Anycast est quelque chose de complètement nouveau, conçu avec IPv6. Le principe de fonctionnement est l'allocation d'une même adresse IPv6 à un ensemble de machines fournissant le même service. Ainsi il serait possible très simplement d'accéder à un service en empruntant la route réseau la plus directe possible.

Cette technique étant encore majoritairement expérimentale, je vous invite à lire l' *'Internet Draft'* _ écrit par l'IETF à propos d'anycast (en anglais) ou bien encore une fois, le livre du G6 (<http://www.oreilly.fr/catalogue/ipv6-3ed.html>) (comité d'experts d'IPv6).

4. Aspects prévisionnels

4.1. Imaginer demain ...

D'ici 5 ans, les routeurs du coeur de l'Internet vont arriver à saturation au niveau de leurs tables de routage. Tous les constructeurs auront du matériel totalement prêt depuis 4 à 5 ans. Les infrastructures seront prêtes à la migration.

Du côté usage, la Chine, le Japon, peut-être même l'Europe et l'Afrique seront arrivés à un point de saturation d'adresses IPv4 ne leur permettant plus d'avancer correctement. Leurs réseaux respectifs seront passés en grande partie à IPv6 en pile IP simple (plus de IPv4). Maintenir un réseau en IPv4 commencera à coûter plus cher tant au niveau matériel qu'humain.

4.2. ... pour l'anticiper aujourd'hui

La migration lente vers IPv6 doit se prévoir dès aujourd'hui. La véritable échéance de IPv6 arrivera dans 5 ou 6 ans. Mais ce n'est pas une fois face au mur qu'on doit prendre la décision de sauter.

En effet, il est estimé que le matériel réseau se remplace tous les 4 ou 5 ans. Cela signifie que c'est aujourd'hui que la problématique IPv6 doit être envisagée. Il faut penser dès maintenant à prendre en compte IPv6 dans le rachat de matériel réseau, même si sa mise en place effective en production ne doit pas se faire d'ici quelques années. Au moins, la migration peut se faire graduellement, en prenant en compte progressivement l'arrivée de cette technologie, évitant le passage brutal de IPv4 à IPv6 et prenant en compte le besoin d'adaptation des utilisateurs (au sens très large).

Ainsi, il est dit qu'une entreprise ne prenant pas cette technologie en compte lors de son prochain renouvellement de matériel sera obligée de faire une migration très brutale, presque forcée d'ici quelques années. Bien entendu les coûts d'une telle opération ne sont pas les mêmes, d'autant qu'une migration douce permet aussi une auto-formation du personnel compétent.

IPv6 est un enjeu de demain qui se joue aujourd'hui. Ceux qui auront réussi à anticiper suffisamment seront ceux pour qui le choc de la transition se sentira le moins.

5. Conclusion

Au delà de son aspect technologique très plaisant, IPv6 va permettre de redistribuer un peu les cartes du réseau des réseaux de demain. Il reste cependant de nombreuses questions. Quelle sera la place des États-Unis

d'Amérique à l'heure d'IPv6 ? Comment les pays en voie de développement auront-ils réussi à tirer leur épingle de cette nouvelle donne mondiale ? Industriellement, le Japon va-t-il réussir à faire la percée qu'il recherche depuis tant d'années face aux USA ? Quelle sera la place de l'Europe sur cet échiquier ?

Bref, l'important reste l'actualité : commencer à introduire IPv6 dans un environnement majoritairement v4 de manière à bien prévoir l'avenir. Cette stratégie sera peut-être le jeu de quelques changements clés.

6. L'auteur

Baptiste SIMON (<http://doc.gentoofr.org/Members/BeTa>) <baptiste.simon@e-glop.net
(mailto:baptiste.simon@e-glop.net)>

Administrateur système GNU/Linux, UNIX & IPv6

7. Annexes

7.1. Bibliographie

Pour pouvoir écrire ce document, je me suis beaucoup aidé de :

- "IPv6 : Théorie et pratique" de Gislène Cizault (comprenez les membres du G6), aux éditions O'Reilly, Paris, 2002, ISBN 2-84177-139-3
- La conférence IPv6 de Caen (<http://www.renater.fr/IPv6-2003Caen/>), juin 2003.
- Documentation NetBSD sur IPv6 (<http://www.netbsd.org/fr/Documentation/network/ipv6/>)

7.2. Aperçu des divers formats de ce document

Ce document a été rédigé au format RST (<http://docutils.sourceforge.net/>) avec KWrite puis converti aux formats DN-XML et Docbook avec dn2dbk.xsl (<http://membres.lycos.fr/ebellot/dn2dbk/>).

Les versions XHTML, HTML et XSL-FO a été réalisée avec les feuilles XSLT officielles de docbook⁴. Les versions PDF, postscript, RTF et texte ont été créées grâce à Jade (<http://openjade.sourceforge.net>).

Retrouvez toutes ces versions ici :

- XHTML ([ipv6-general.xhtml](#))
- HTML ([ipv6-general.html](#))
- PDF ([ipv6-general.pdf](#))
- postscript ([ipv6-general.ps](#))
- Texte brut ([ipv6-general.txt](#))

- RTF (ipv6-general.rtf)
- reStructuredText (ipv6-general.rst)
- DocBook - XML (ipv6-general.db-xml)
- DN-XML (ipv6-general.dn-xml)
- XSL-FO (ipv6-general.fo)

7.3. Licence de publication

Ce document issu de www.e-glop.net (<http://www.e-glop.net/>) ou de www.ipv6.e-glop.net (<http://www.ipv6.e-glop.net/>) est soumis à la licence GNU FDL (<http://www.gnu.org/copyleft/fdl.html>).
Permission vous est donnée de distribuer, modifier des copies de ce document (traduction, modifications, adaptation, etc...) tant que vous respectez la licence sus-citée.

Notes

1. Une plage d'adresses dites "de classe A" est une plage pouvant contenir 16.777.216 adresses. Ce sont ces plages qui peuvent contenir le plus d'adresses IPv4. IPv4 en a défini moins de 255 pour l'ensemble du réseau. La presque totalité de ces adresses se trouvent donc aux USA.
2. La couche *liaison de donnée* est la couche de niveau 2, située juste en-dessous des protocoles de *réseau* et au-dessus de la couche *physique* (les bits se promenant sur un support de type câble en cuivre)
3. Documentation NetBSD sur IPv6 : <http://www.netbsd.org/fr/Documentation/network/ipv6/>
4. paquet app-text/docbook-xsl-stylesheets (<http://www.oasis-open.org/docbook>) sur Gentoo Linux