IPv6, passeport pour l'Internet du Futur

Résumé

Après un rappel historique remettant dans son contexte le phénomène d'épuisement de l'espace d'adressage IPv4, ce dossier souligne les vrais enjeux liés à ce phénomène et à la transition inéluctable IPv4 - IPv6. Ensuite, ce document met en évidence les apports d'IPv6 de manière concise, rappelle les rôles des différents acteurs du réseau et décrit les modèles de communication nécessitant la prise en compte en priorité de l'intégration d'IPv6. Quelques mécanismes de transition sont donnés à titre indicatif et non limitatif en vue d'illustrer de manière pratique l'intégration d'IPv6 dans des contextes techniques variés. Enfin, ce document émet des recommandations pratiques pour accompagner le déploiement sur le terrain et lance un appel pour saisir – sans délai - les opportunités présentées par IPv6, afin de faire de l'« Internet du Futur » un champ ouvert pour l'innovation.

1 Rappel historique

Le réseau Internet est né au début des années 1970 aux États-Unis et a connu une croissance plutôt douce jusqu'à la fin des années 1980. L'avènement du web au début des années 1990, notamment comme outil de présence commerciale sur Internet, a entraîné un déploiement massif de millions de nouveaux nœuds du réseau et par conséquent un succès fulgurant. La croissance exponentielle de la demande d'adresses IP (numéros uniques assurant l'identification et la localisation des équipements réseau) a fait de l'Internet une victime de son propre succès. Et voilà une première prévision pour la « fin de l'Internet » en 1994 !

Aussitôt, des mesures d'urgence ont été décrétées et appliquées individuellement ou combinées afin d'« arrêter l'hémorragie ». Parmi ces mesures, on peut citer l'allocation exceptionnelle de blocs d'adresses de « classe B »[1], la réutilisation des blocs de classes C[2], puis l'abolition des classes dans les mécanismes d'allocation et de routage des préfixes IP (CIDR, *Classless Internet Domain Routing*[3]). S'y sont ajoutés par la suite l'« aménagement » d'un espace d'adressage privé ([RFC 1918][4]), l'utilisation de mandataires (*proxy*) ou de boîtiers de traduction d'adresse (NAT[5]) pour communiquer avec l'extérieur.

Mais parallèlement à l'application de ces mesures d'urgence, l'IETF a lancé dès 1993 les travaux de recherche pour préparer la succession d'IPv4 dont les limites venaient d'être démontrées.

2 Cahier des charges de la nouvelle version d'IP (v6)

Les principaux objectifs suivants ont été assignés à la nouvelle version d'IP à élaborer : étendre l'espace d'adressage IP, corriger les défauts d'IPv4 et améliorer les performances autant que faire se peut, anticiper les besoins futurs et favoriser l'innovation en simplifiant la mise en œuvre d'extensions fonctionnelles au protocole.

Ces objectifs ont été toutefois soumis à des contraintes, celles de conserver les principes qui ont fait le succès d'IPv4 : communication de bout en bout, robustesse et « faire de son mieux » (*Best effort*).

3 Qu'y a-t-il de nouveau avec IPv6 ?

Ceux qui souhaitent connaître dans les détails les apports d'IPv6 et la manière dont cette nouvelle version du protocole IP fonctionne peuvent se référer au livre en ligne, « IPv6, Théorie et pratique »[6].

Tout d'abord, IPv6 offre un plus grand espace d'adressage qu'en IPv4 : on passe d'un codage des adresses en IPv4 sur 32 bits (4.3 milliards d'adresses) à un codage en IPv6 sur 128 bits ($3.4\ 10^{38}$, soit 340 milliards de milliards de milliards de milliards d'adresses). De ce fait, IPv6 apparaît comme « activateur » d'usage (*enabler*), quelque chose qui repousse l'imagination. C'est aussi l'occasion de rétablir le modèle de communication « de bout en bout », l'un des fondements d'IPv4 qui a été ébranlé par l'arrivée massive de boîtiers de traduction d'adresses (« NAT »).

Par ailleurs, IPv6 apporte une nouvelle forme d'auto-configuration, dite « sans état » pour les machines hôtes. Ce mécanisme consiste pour un hôte à construire automatiquement une adresse locale lui permettant de communiquer avec ses voisins, puis à construire une adresse IPv6 globale sur la base d'informations annoncées par un routeur local au lien réseau. Le mode d'auto-confiuration sans état s'ajoute à celui de l'auto-configuration « avec état » existant, rendu par le service DHCP.

Enfin, IPv6 offre une meilleure intégration du multicast ainsi qu'une meilleure prise en charge des extensions fonctionnelles, en les encapsulant dans des en-têtes optionnels dédiés, tels que ceux pour la sécurité ou la mobilité.

[1] La notion de classe a disparu avec CIDR. Un bloc de classe B comprend 2^{16} adresses, l'équivalent aujourd'hui en nombre avec un /16.
[2] Un bloc de classe C comprend 2^{8} adresses, équivalent en nombre à un /24.
[3] http://fr.wikipedia.org/wiki/Adresse_IP#Agr.C3.A9gation_des_adresses
[4] http://www.ietf.org/rfc/rfc1918.txt
[5] http://fr.wikipedia.org/wiki/Network_address_translation
[6] http://livre.g6.asso.fr/

4 Vous avez dit « épuisement de l'espace IPv4 » ? C'est quoi ? Que se cache-t-il derrière ?

En 2003, Geoff Huston (Chief Scientist, APNIC) avait fait des prévisions sur la durée de vie de l'espace d'adressage IPv4 (*IPv4 Address Lifetime*) : http://www.ripe.net/ripe/meetings/ripe-46/presentations/ripe46-IPv4-lifetime.pdf
Le message que son public (les RIR essentiellement) a compris était le suivant : s'il n'y a pas de grosse surprise (changement du modèle, réveil numérique de la chine…), on aura encore des adresses IPv4 jusqu'à 2030-2037 (cf. transparents 49-51 de la présentation ci-dessus). Quoi de plus rassurant pour les RIR qui étaient déjà dans la gestion de la pénurie mais qui n'étaient pas très enthousiastes à l'idée de pousser pour l'adoption d'IPv6. Ouf, pas la peine donc de se précipiter sur IPv6 et tâchons d'y avancer tranquillement au rythme de la consommation du stock restant.

Cependant, quelle n'a pas été la surprise des RIR lorsque le même G. Huston leur apprend en 2007 que finalement l'épuisement aurait lieu bien avant ! Les nouvelles prévisions donnaient ainsi 2010 et 2012 comme années où le stock IPv4 de l'IANA et celui des RIR seront respectivement épuisés : http://www.ripe.net/ripe/meetings/ripe-55/presentations/huston-ipv4.pdf (cf. transparents 12-15, 37, 38).

Debout, vous n'avez plus le temps ! Panique à bord côté RIR. Vite, il faut faire quelque chose et Randy Bush de remuer le couteau dans la plaie avec sa présentation dans un style « on va tous souffrir » : http://rip.psg.com/~randy/071022.v6-op-reality.pdf

Depuis cette date, le rapport quotidien et automatique dont G. Huston est l'auteur est devenu une référence mondiale en matière de prévisions : http://www.potaroo.net/tools/ipv4/index.html

Au 3 février 2011 le stock IPv4 de l'IANA[7] a été épuisé, annonce faite à l'occasion d'une conférence de presse ICANN-NRO-IAB-ISOC[8].

La prochaine échéance sera l'épuisement du stock des adresses IPv4 chez chaque RIR. Cela dépendra du rythme de consommation chez chaque RIR, mais il est prévisible que cela commence dès fin 2011 – début 2012 au plus tard.

Alors, quels sont les vrais enjeux que recèle ce problème d'épuisement d'adresses IPv4, qui semble encore surprendre dans certains milieux au point d'y créer un climat de psychose ? Que se passera-t-il après cet épuisement ? Qui sera impacté et que faudra-t-il faire alors pour que l'Internet continue de fonctionner de manière acceptable ?

Autant de questions qui méritent chacune de longues réponses, mais voici des éléments de réponse synthétiques.

Pour la plupart des acteurs de l'Internet, il sera encore possible de (sur)vivre avec IPv4 pour une durée variable, pouvant atteindre plusieurs années, même après l'épuisement des stocks IANA + RIR. En effet, ceux qui ont déjà fait le plein d'IPv4 peuvent en rationner la gestion (gestion de la pénurie), les « marchés gris »[9] d'IPv4 sont une option, certes déconseillée, mais prévisible et enfin certains s'accommodent de plusieurs « étages » de NATs qui conviennent à leurs besoins depuis plusieurs années.

Cependant, cela ne ferait que repousser le problème, car le coût/complexité de déploiement de nouveaux services en IPv4 et la maintenance de l'existant croît de manière significative (recrudescence des boîtiers de traduction v4privé-v4public, recrudescence des tunnels/encapsulation v4-in-v6 et v6-in-v4 aussi bien au niveau des dorsales qu'à l'accès au réseaux). En outre, ceux qui n'auront pas pris le temps de pratiquer ces techniques et de les maîtriser risquent de rencontrer de gros problèmes de stabilité de leurs infrastructures et services réseau.

Enfin, il est à souligner qu'à mesure que les acteurs réseau déploient IPv6, celui qui y résistera encore, assumera le risque d'être exclu (perte de marché / compétitivité économique). En somme, se contenter d'IPv4 devient un véritable frein à l'innovation si bien que la fracture numérique ne fera que se creuser (mais la facture aussi, à terme).

[7] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
[8] http://www.nro.net/news/ipv4-free-pool-depleted
[9] On parle de « marché gris » et non de « marché noir » dans la mesure où il est possible de connaître les acteurs des transactions de vente de préfixes IPv4, mais pas du montant de la transaction.

5 Intégration d'IPv6 : Quoi faire ? Par qui et où ?

L'intégration d'IPv6 est une démarche progressive et collective, qui incombe à tout acteur du réseau, chacun selon ses missions et responsabilités. Il n'y aura pas de jour J pour un « basculement » brutal vers IPv6. Avant de savoir comment faire, se posent tout d'abord les questions suivantes : que faut-il faire ? Par qui et où exactement ?

Commençons tout d'abord par ce que tout acteur doit faire sur son propre ordinateur : mettre à niveau/jour son système d'exploitation et les applications réseau qu'il utilise, en vue de les rendre compatibles avec IPv6. Pour la plupart des systèmes d'exploitation et des applications réseau classique, il n'y a presque plus rien à faire, les versions récentes gèrent IPv6 correctement.

Les utilisateurs gérant eux-mêmes leur réseau local (particuliers, entreprises, campus) doivent intégrer IPv6 dans leurs routeurs et souscrire un service de connectivité vers un fournisseur d'accès interne (FAI) IPv6 (de préférence leur FAI habituel en IPv4 s'il dispose d'une offre IPv6, ou même quelqu'un d'autre).

Les FAI/Opérateurs doivent quant à eux, intégrer IPv6 dans leurs routeurs d'accès, de cœur de réseau et de bordure, ainsi que dans leurs autres équipements réseau tels que les pare-feu et les équilibreurs de charge.

Par ailleurs, les hébergeurs de services (web, dns…) doivent intégrer IPv6 dans leurs équipements et services réseau dédiés ou mutualisés.

Mais à moins d'être un administrateur d'un grand réseau, on n'a en général pas à gérer tous ces aspects à la fois. Autrement dit, on prend généralement en charge sa partie et on demande par la suite aux autres acteurs de prendre en charge la leur, surtout lorsqu'on ne dépend pas d'eux ! Et quand bien même on serait administrateur d'un grand réseau assumant plusieurs responsabilités, on ne ferait pas tout en même temps, mais plutôt progressivement après un exercice de priorisation et de planification.

Afin d'avoir plus de renseignement au sujet du rôle de chaque acteur, le site web suivant peut être d'une grande utilité :
http://www.ripe.net/v4exhaustion/

6 Intégration IPv6 : modèles de communication, classification

Modèle de communication

Une communication IP nécessite la coopération verticale et horizontale de tous les composants sous-jacents ou intermédiaires du réseau. Le modèle de communication suivant[10] nous permet d'identifier les types de communication qui méritent une attention particulière et qui nécessitent des mécanismes pratiques de transition. Qui parle avec qui et comment ?

1. Un système IPv4 se connecte à un système IPv4 à travers un réseau IPv4 ;
2. Un système IPv6 se connecte à un système IPv6 à travers un réseau IPv6 ;
3. Un système IPv4 se connecte à un système IPv4 à travers un réseau IPv6 ;
4. Un système IPv6 se connecte à un système IPv6 à travers un réseau IPv4 ;
5. Un système IPv4 se connecte à un système IPv6 ;
6. Un système IPv6 se connecte à un système IPv4 ;

Une analyse de la complexité et des besoins montre que 1 & 2 sont triviaux, que 3 & 4 sont moins faciles mais ne présentent pas d'obstacles majeurs, et que 5 & 6 sont plus complexes et que nous ne disposons à ce jour pas de solutions globales et satisfaisantes.

[10] Ce modèle s'inspire des scénarios décrits dans le document produit par le groupe de travail behave de l'IETF : http://tools.ietf.org/html/draft-ietf-behave-v6v4-framework

Classification des techniques de transition

Pour 4/4 & 6/6, la technique de double pile IPv4-IPv6 (*Dual-Stack*) est aujourd'hui la plus pratique, tant que des adresses IPv4 sont disponibles. Communication v6-v6 ou v4-v4

Pour les cas 4/6 & 6/4 qui nécessitent la traversée d'un réseau de famille différente, il existe plusieurs techniques à base de tunnels **automatiques** ou **manuels** (configurés). Par exemple, un tunnel IPv6 dans IPv4 consiste à encapsuler un paquet IPv6 dans un paquet IPv4 et de faire router le paquet IPv4 obtenu par l'ensemble des routeurs IPv4 du chemin vers la destination, jusqu'au bout du tunnel (routeur *dual stack*) qui décapsulera le paquet IPv6 et le fera suivre à la destination IPv6 finale.

Les cas 4/6 & 6/4 représentent des scénarios de cohabitation entre des réseaux existants compatibles IPv4 uniquement (*IPv4-only*) et de nouveaux réseaux *IPv6-only*. Les techniques souvent appliquées dans ces cas-là sont des formes différentes de traduction au niveau IP ou des mandataires (ou relais) applicatifs[11] (*Application Level Gateway*). Notons que le type 4/6 ci-dessus a été jugé peu prioritaire pour l'instant, la priorité ayant été fixée pour l'accès au monde IPv4 (toujours dominant) à partir de systèmes IPv6 (encore minoritaires).

7 Quelques exemples de mécanismes de transition

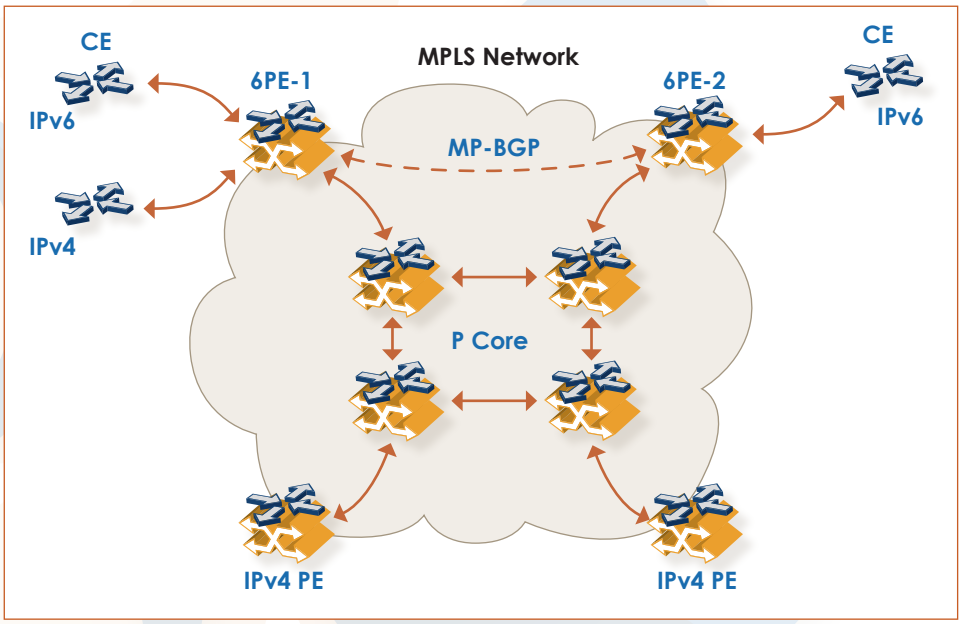
Il est très difficile de décrire de manière exhaustive ou dans le détail l'ensemble des mécanismes de transition qui ont été proposés jusqu'ici. Nous nous contenterons de quelques exemples qui illustrent les classes de techniques mentionnées ci-dessus.

Ces techniques ne doivent pas être vues comme des recettes à appliquer systématiquement, mais plutôt comme des outils à disposition des acteurs du réseau à sélectionner en fonction des besoins, contraintes et souhaits de chacun.

Tunnels 6PE / MPLS dans le cœur de réseau d'un opérateur

Les opérateurs disposant déjà d'un cœur de réseau en MPLS (*Multi-Protocol Label Switchnig*) peuvent utiliser des tunnels appelés 6PE, comme spécifié dans le [RFC 4798][12]. Il s'agit plus précisément d'établir des *peerings BGP* entre routeurs de bordure rendu IPv6 compatible, sans modification pour les routeurs du cœur de réseau, répondant ainsi à la problématique 6/4 du modèle ci-dessus. Cette technique a l'avantage d'être flexible, extensible progressivement et peu coûteuse.

Le schéma suivant illustre le mécanisme 6PE :



[11] http://fr.wikipedia.org/wiki/Serveur_mandataire

[12] *Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE)*, http://www.ietf.org/rfc/rfc4798.txt

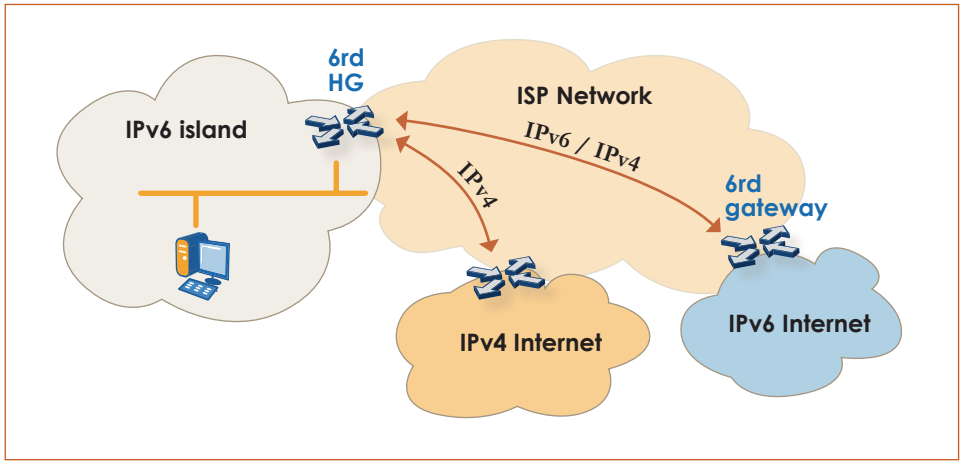
Tunnels 6rd (« Rapid Deployment »), du 6to4 mais en mieux pour connecter un site client !

Il s'agit d'une solution dérivée de 6to4 ([RFC 3056][13]), spécifiée dans le [RFC 5569][14] informatif, puis dans le [RFC 5969][15] qui vise la standardisation de ce mécanisme . Cette solution répond à la problématique 6/4 du modèle de communication ci-dessus.

Le principe est relativement simple : le FAI fournit de la connectivité IPv6 à ses abonnés avec un impact minimum sur son réseau d'accès, en réutilisant les bonnes propriétés de 6to4. En effet, le préfixe IPv6 de l'abonné est en partie dérivé de l'adresse IPv4 qui lui a été attribuée (pas de plan d'adressage spécifique à déployer) et le FAI peut dimensionner de manière incrémentale son réseau d'accès en y déployant progressivement des relais Anycast[16]. Ces derniers se chargent de décapsuler, puis de router les paquets IPv6 des abonnés, et les problèmes de sécurité/performance de 6to4 pointés par [RFC 3964][17] se trouvent en grande partie évités.

Cette solution a été déployée pour la première fois en 2007 chez le FAI français Free et depuis, elle a suscité un intérêt grandissant chez d'autres FAI, à titre expérimental ou pour un déploiement en production[18].

Le schéma suivant illustre le mécanisme 6rd :



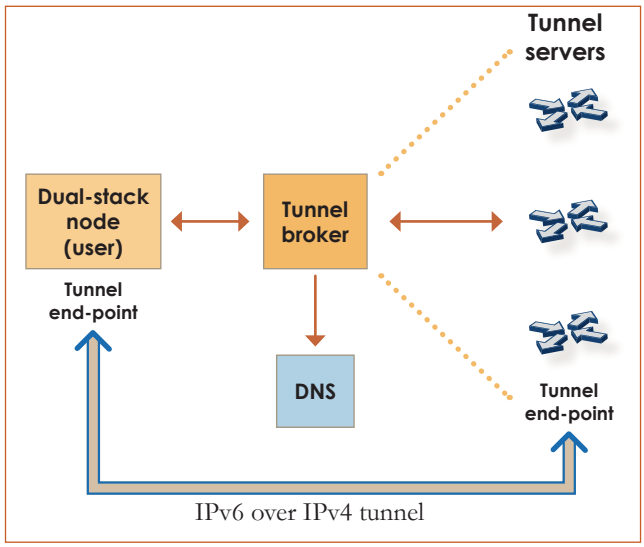
Connectivité de site/terminal client : Le *Tunnel Broker*

Il s'agit de techniques légèrement différentes les unes des autres, mais toutes s'appuyant sur le concept de *Tunnel Broker* décrit dans [RFC 3053][19]. Cette solution répond à la problématique 6/4 du modèle de communication.

Comme son nom l'indique, le *Broker* (ou courtier), assure une interface d'échange entre un client souhaitant connecter sa machine ou son site à l'Internet IPv6 et un fournisseur de connectivité IPv6 via des tunnels négociés et dédiés (IPv6 dans IPv4). Via cette interface intermédiaire (typiquement, une interface web), le client spécifie ses *desiderata* en matière d'allocation d'adresse(s) IPv6 (soit adresse unique, soit « préfixe / longueur » selon la politique du fournisseur de tunnels) et fournit des renseignements complémentaires, notamment son adresse IPv4 (pour le tunnel), son système d'exploitation, etc. Le *Broker* transmet d'une part au fournisseur de tunnels ces informations récoltées, et d'autre part, il met à disposition du client les paramètres proposés pour se connecter (adresse ou préfixe IPv6 choisi(e), script de lancement selon le système d'exploitation, etc.). Client et serveur de tunnel activeront alors chacun de son côté son bout de tunnel et le tour est joué.

[13] http://www.ietf.org/rfc/rfc3056.txt
[14] *IPv6 Rapid Deployment on IPv4 infrastructures (6rd) »*, Rémi Després
http://www.ietf.org/rfc/rfc5569.txt
[15] http://www.ietf.org/rfc/rfc5969.txt
[16] http://fr.wikipedia.org/wiki/Anycast
[17] http://www.ietf.org/rfc/rfc3964.txt
[18] http://en.wikipedia.org/wiki/IPv6_rapid_deployment
[19] http://www.ietf.org/rfc/rfc3053.txt
Plus récemment, le protocole TSP (*Tunnel Setup Protocol*), conçu de longue date, a été publié en [RFC 5572]
http://www.ietf.org/rfc/rfc5572.txt (« EXPERIMENTAL »).

Le schéma suivant illustre le mécanisme générique de « Tunnel Broker » :



IPv6 over IPv4 tunnel

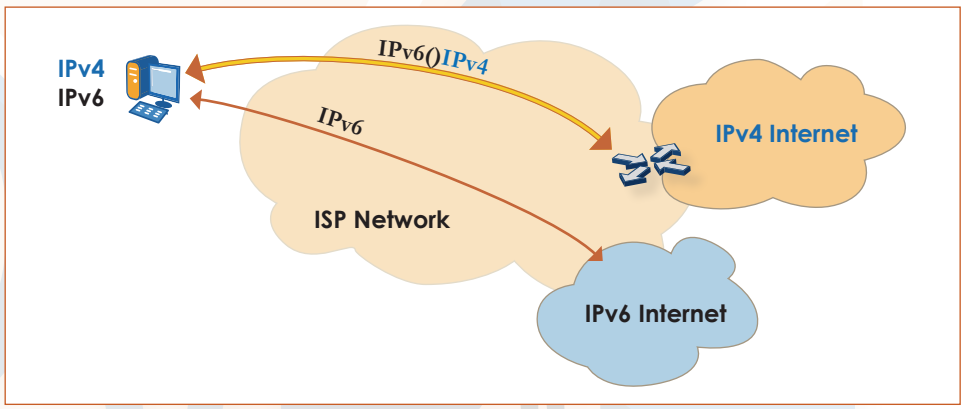
Il existe plusieurs fournisseurs de tunnels répartis sur des régions différentes. Parmi ceux qui sont mondialement connus, on peut citer les trois suivants : gogo6/Freenet6[20], Hurricane Electric[21] et SixXS[22]. La page suivante donne plus d'informations et de détails sur les fonctionnalités offertes par les différentes solutions : http://en.wikipedia.org/wiki/List_of_IPv6_tunnel_brokers

DS-Lite : L'accès abonné à IPv6 et à IPv4, sans adresse IPv4 publique

Cette technique a été élaborée au sein du groupe de travail *softwires*[23] de l'IETF par anticipation à l'épuisement de l'espace d'adressage IPv4. Elle est spécifiée dans le document (en cours) *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*[24].

DS-Lite prévoit un boîtier NAT associé à plusieurs abonnés, hébergé par le FAI, le *Carrier Grade NAT* (CGN)[25]. Les clients obtiennent de leur FAI un préfixe IPv6 et une adresse IPv4 privée. Le CGN assure la traduction entre l'IPv4 privé côté abonné et IPv4 public côté FAI (cœur de réseau). En outre, le trafic IPv4 de l'abonné est transporté au-dessus d'IPv6. Ainsi, au lieu d'un scénario double-NAT, les paquets IPv4 (adresse source privée) sont « tunnelés » dans des paquets IPv6 jusqu'au CGN. Ce dernier conserve le contexte sur la base de l'adresse IPv6 publique de l'abonné.

Le schéma suivant illustre le mécanisme DS-Lite :



Cette technique est implémentée par l'ISC, sous le nom AFTR[26], adopté par Comcast (www.networkworld.com/news/2010/031810-comcast-isc-ipv6-tool.html)
Un déploiement industriel est également prévu chez FT-Orange (France).

[20] http://gogonet.gogo6.com/
[21] http://tunnelbroker.net/
[22] http://www.sixxs.net/
[23] http://datatracker.ietf.org/wg/softwire/
[24] http://tools.ietf.org/html/draft-ietf-softwire-dual-stack-lite
[25] http://en.wikipedia.org/wiki/Carrier_Grade_NAT
[26] http://www.isc.org/software/aftr

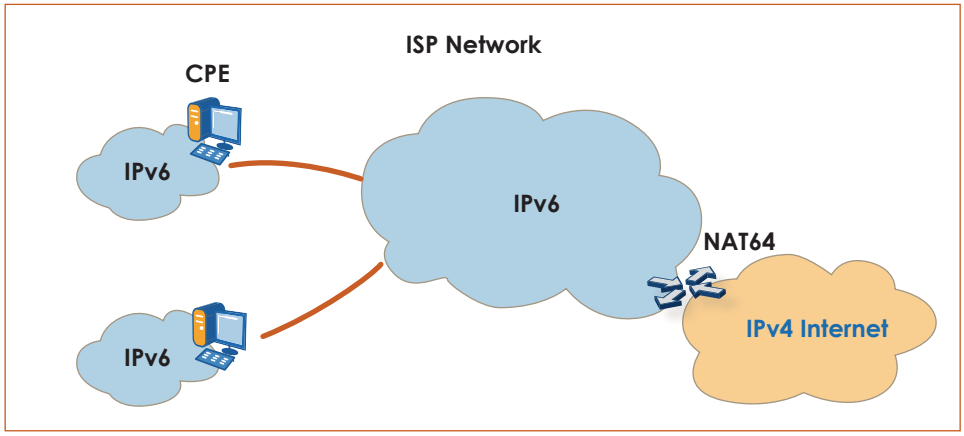
« NAT64 + DNS64 » pour la cohabitation : permettre à un équipement IPv6 de solliciter un équipement IPv4

Cette technique est l'œuvre du groupe de travail *behave*[27] de l'IETF. Elle répond à la problématique 6/4 identifiée dans le modèle ci-dessus.

Alors que le *Dual-Stack* était supposé devenir massivement déployé pour une transition fluide v4-v6 avant l'épuisement de l'espace d'adressage IPv4, cela n'a pas marché comme prévu. Très peu de déploiement a été enregistré jusqu'ici et les jours de l'espace IPv4 sont comptés. Il est donc difficile de contourner la traduction v4-v6 si l'on souhaite continuer à accéder aux services *IPv4-only* existants.

Les principes, le cadre et les principales contraintes d'application de cette technique sont décrits dans le document IETF suivant : [RFC 6144] *Framework for IPv4/IPv6 Translation*[28].

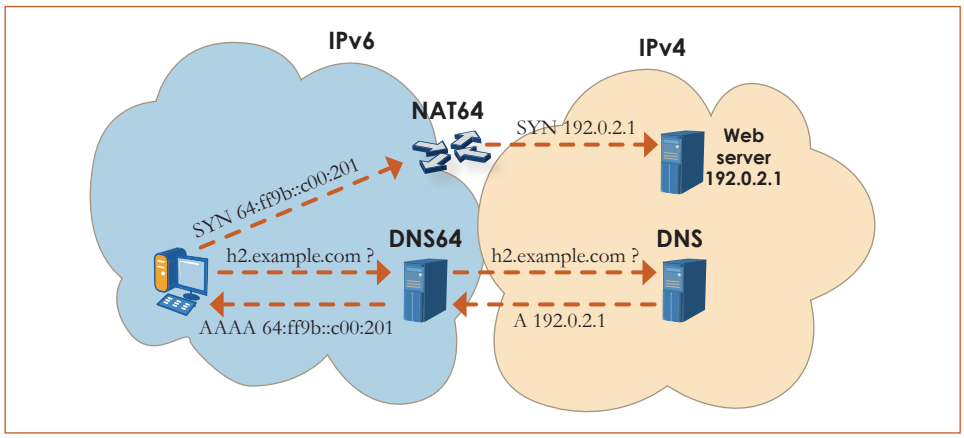
Le schéma suivant illustre la problématique :



Les mécanismes de traduction eux-mêmes sont spécifiés dans trois documents IETF séparés :

- [RFC 6145] *IP/ICMP Translation Algorithm*[29] : un mécanisme de traduction sans état ;
- [RFC 6146] *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*[30] : un remplacement efficace de NAT-PT (déprécié par [RFC 4966][31], en raison des problèmes et risques associés) ;
- [RFC 6147] *DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*[32] : un mécanisme pour synthétiser des enregistrements DNS IPv6 (AAAA) à partir d'enregistrements DNS IPv4 (A) et permettre ainsi à un équipement *IPv6-only* d'engager une communication vers un équipement *IPv4-only*, en passant par le boîtier de traduction NAT64.

Le schéma suivant illustre les mécanismes NAT64/DNS64 :



La société canadienne Viagénie offre une implémentation de NAT64/DNS64[33], qu'elle a expérimentée à l'occasion de meetings IETF récents. Pour en savoir plus, le lecteur peut consulter la présentation suivante : http://www.slideshare.net/IOSHints/nat64-and-dns64-in-30-minutes

27 http://datatracker.ietf.org/wg/behave/
28 http://www.ietf.org/rfc/rfc6144.txt voir aussi le résumé de ce RFC en français : http://www.bortzmeyer.org/6144.html
29 http://www.ietf.org/rfc/rfc6145.txt voir aussi le résumé de ce RFC en français : http://www.bortzmeyer.org/6145.html
30 http://www.ietf.org/rfc/rfc6146.txt voir aussi le résumé de ce RFC en français : http://www.bortzmeyer.org/6146.html
31 http://www.ietf.org/rfc/rfc4966.txt
32 http://www.ietf.org/rfc/rfc6147.txt voir aussi le résumé de ce RFC en français : http://www.bortzmeyer.org/6147.html
33 http://ecdysis.viagenie.ca/

8 Quelques recommandations pratiques pour l'intégration d'IPv6

Au risque d'enfoncer des portes ouvertes, il est utile de le rappeler : l'IPv6 **natif partout** est la **seule solution viable**. Mais comme cet objectif à terme ne peut être atteint en un jour, les recommandations pratiques suivantes sont données pour accompagner la transition progressive :

- consolider IPv6 dans l'infrastructure là où c'est possible, sans délai ;
- assurer le *dual-stack* là où c'est possible (pour une intégration fluide d'IPv6 en production) ;
- sécuriser/fiabiliser les réseaux et services IPv6 au fur et à mesure de leur déploiement. Ce document du NIST peut être alors d'une grande aide : *Guidelines for the Secure Deployment of IPv6*[34];
- penser à la parité fonctionnelle IPv6-IPv4 dans les déploiements, mais aussi à la parité en termes de performances : charge/débit, résilience, temps de réponse…

Une autre évidence qu'il est utile de rappeler, ne serait-ce que pour rassurer ceux qui tardent à adopter IPv6, la complexité de déploiement d'IPv6 décroît, et par conséquent, son coût.

En effet, les cycles de rafraîchissement naturel des équipements et logiciels réseau permettent d'avoir IPv6 sans même le demander dans la plupart des cas, et très souvent sans surcoût financier[35]. Il convient donc de faire attention à ne pas acheter des solutions déjà obsolètes ou qui le deviendront dans peu de temps, encouragé par un prix intéressant, même si on est sûr que le déploiement d'IPv6 n'interviendra que plusieurs mois plus tard, l'amortissement de tels investissement se faisant généralement sur plusieurs années (3-5 ans) ! À ce sujet, pour un acteur souhaitant acquérir des solutions matérielles/logicielles réseau, des exigences en matière de compatibilité IPv6 peuvent être formulées en s'appuyant sur le document suivant : http://ripe.net/docs/ripe-501.html[36]

Comme toute technologie nouvelle, IPv6 nécessite un gros investissement en formation. Étudiants, ingénieurs et formateurs, y compris les enseignants en réseau, doivent s'y mettre en temps utile. La formation est considérée aujourd'hui comme le poste de coût le plus important dans une démarche d'intégration progressive d'IPv6.

Enfin, ceux qui sont convaincus de la nécessité de déployer IPv6, qui se sont déjà attelés à la tâche mais qui appréhendent encore l'impact opérationnel du passage à IPv6 sur leurs services en production, même partiellement, peuvent saisir, s'il est encore temps, l'*IPv6 Day*[37], événement programmé pour la journée du 8 juin 2011. Il s'agit d'une expérimentation mondiale qui consiste à fournir pendant 24 heures le contenu de son site web en double pile (IPv4 et IPv6)[38]. Le fait d'avoir une participation massive à cet événement permet de diagnostiquer le plus grand nombre de problèmes opérationnels éventuels et de les résoudre collectivement dans les meilleurs délais, favorisant ainsi un déploiement plus soutenu d'IPv6. Les organismes qui ont déjà IPv6 en production dans leurs services réseau, comme l'AFNIC qui est prête depuis 2003[39], peuvent eux aussi y participer. En effet, même si ce n'est pas pour les mêmes objectifs (test), ceux qui ont de l'expérience dans IPv6 sont invités à manifester leur soutien à ceux qui s'y mettent maintenant et à les accompagner dans leur opération de transition IPv4-IPv6.

9 Avec IPv6, des opportunités à saisir. Maintenant !

Les ressources IP sont à nouveau abondantes avec l'arrivée d'IPv6. L'équité dans l'accès à ces ressources au niveau mondial se trouve de fait rétablie[40].

De ce point de vue, grâce à IPv6, l'innovation se trouve favorisée et l'économie numérique stimulée. C'est sans doute le plus l'avantage le plus important et le plus concret d'IPv6, l'exercice de recherche d'une « application qui tue » (*killer application*) s'étant révélé vain.

Alors que pour certaines technologies, il y a une bataille sur les ressources essentielles, pour IPv6, il en est autrement. Les adresses IPv6 étant abondantes, la bataille se situe plutôt au niveau de la maîtrise de la technologie IPv6 elle-même et de la disponibilité à temps des produits et services innovants qui s'y appuient.

[34] http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[35] Il y a quelques années, certains constructeurs et éditeurs logiciels proposaient IPv6 contre un prix à payer pour acheter la licence ou cartes spécifiques qui vont avec. D'autres proposaient IPv6 « sans surcoût », mais en réalité, il fallait dépenser quand même pour obtenir de la mémoire supplémentaire afin d'accommoder IPv6.

[36] Une version traduite en français est en cours de révision sur le wiki du G6 : http://www.g6.asso.fr/index.php/Public:ExigencesAppelsOffresIPv6

[37] http://isoc.org/wp/worldipv6day/how-to-join/

[38] http://test-ipv6.com/ipv6day.html

[39] http://www.afnic.fr/actu/nouvelles/118/communique-de-presse-nbsp-ipv6-entierement-integre-dans-le-systeme-de-production-de-l-afnic-des-le-1er-octobre-2003

[40] C'est loin d'être le cas pour IPv4 compte tenu de l'historique de son adoption et déploiement.

10 Références utiles

Portails :

- http://www.g6.asso.fr/
- http://www.ipv6actnow.org/ (RIPE)
- http://www.getipv6.info/ (documentation Wiki ARIN)
- http://www.ipv6forum.com/
- http://www.sixxs.net/

Livres, blogs, rapports, articles :

- Le blog du G6 : http://g6.asso.fr/blog
- Livre *IPv6, Théorie et pratique* du G6 (Gisèle Cizault :-)) : http://livre.g6.asso.fr/
- Autre blog technique : http://blog.ioshints.info/search/label/IPv6
- Rapport OCDE avec mesures du déploiement : http://www.oecd.org/sti/ict/ipv6
- http://www.circleid.com/posts/ip_address_exhaustion_in_12_easy_questions/
- http://www.circleid.com/posts/ipv6_and_transitional_myths/
- http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-303870A1.pdf
- Dossier ZDnet sur IPv6 : http://www.zdnet.fr/dossier/ipv6.htm

Dossier réalisé par Mohsen Souissi, responsable R&D de l'AFNIC

Retrouvez tous les dossiers thématiques de l'AFNIC :
www.afnic.fr/actu/presse/liens-utiles

www.afnic.fr - afnic@afnic.fr