L'Avenir D'Internet
Le protocole IPv6

Cassier Anne
Burie Antoine
Tchomgue Ivan

10 février 2012

Résumé

Internet peut être défini comme le point de convergence de trois choses : d'une architecture industrielle distribuée (serveurs, fibres, satellites, etc.), de multiples langages informatiques interopérables (TCP, IP, Protocoles, etc.), avec un très grand nombre de pratiques intellectuelles (chercher dans une banque de données, jouer, dialoguer, etc.).
Deux traits marquants de l'évolution d'Internet sont d'une part le web 2.0. D'autre part, son évolution n'a été guidée par personne, elle est la résultante d'une multitude d'inventions qui partent de la base, qui partent des utilisateurs ayant créé et fait évoluer de nouveaux outils.
La futurologie reste un exercice périlleux. C'est encore plus difficile quand il s'agit d'Internet, car son avenir est encore plus obscure que celui de tout autre chose. En 1993, année d'arrivée de l'Internet en France, il y avait neuf cent mille utilisateurs et deux cents sites web dans le monde. Aujourd'hui, 19 ans plus tard, on dénombre plus de deux milliards d'utilisateurs et plus de trente milliards de sites web. On n'a donc pas idée de ce que deviendra Internet dans les vingt prochaines années. Il est donc légitime de s'interroger sur son avenir. On s'interessera ici au mode d'adressage utilisé par internet et de son amélioration éventuel.

Table des matières

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 remmettre 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 on va essayer de répondre dans un premier temps. Dans un second temps, on abordera plus les aspects techniques d'IPv6, Enfin, on essaiera d'aborder la question de la migration d'un point de vue prévisionnel.

Première partie

Développement d'un nouveau protocole

1 Raisons de développement d'un nouveau protocole IP

Lors de la conception d'IP (Internet Protocole) en 1978, les ingénieurs pensaient que seuls quelques milliers d'ordinateurs seraient concernés répartis sur une douzaine de réseaux. Or tout le monde sait, aujourd'hui que ce n'est pas le cas. Avec IPv4 (Internet Protocole version 4), l'adressage se fait sur 32 bits, ce qui serait suffisant comme espace, mais, IPv4 est un protocole qui est trop restreint de par son utilisation et qui est donc coûteux en terme d'adresses gaspillées. Bientôt, étant donné l'expansion de l'Internet, il n'existera plus d'adresse disponible sous Ipv4. Certains spécialistes pronostiquent la pénurie d'adressage sous Ipv4 d'ici 2008-2010.

Par exemple :

Les adresses de classe A : elles représentent douze réseaux de 16.7 millions de noeuds. Toutes les adresses de classe A sont déjà toutes épuisées.

Les adresses de classe B : elles représentent 16368 réseaux de 65534 noeuds. Ce sont les adresses les plus répandues parmi les industriels et certains fournisseurs d'accès. Elles sont déjà presque toutes utilisées.

Les adresses de classe C : elles représentent 2 millions de réseaux de 254 noeuds. Elles sont principalement pour les petites organisations, et, actuellement, elles sont distribuées aux fournisseurs d'accès. Ces adresses sont déjà épuisées. De plus, aujourd'hui, le nombre de réseaux connectés est devenu très important, les tables de routage ont pris des proportions considérables, donnant ainsi une charge de travail énorme aux administrateurs.

De par la taille des tables de routage, le traitement des paquets est fortement ralenti. Actuellement, les routeurs principaux des infrastructures de

l'Internet comptent environ 7000 routes. Le nouveau protocole, IPv6, doit permettre un adressage plus grand et un routage plus simple et plus rapide.

2 Objectifs et caractéristiques de L'IPv6

2.1 Principaux objectifs de l'IPv6

Dès le milieu des années 1990, le réseau Internet était utilisé largement par les universités, les industries de pointes, et le gouvernement. Les principaux objectifs du protocole IPv6 sont de :

- Supporter des milliards d'ordinateurs, en se libérant de l'inefficacité de l'espace des adresses IP actuelles.
- Réduire les tables de routage.
- Simplifier le protocole, pour permettre aux routeurs de router plus rapidement,
- Fournir une meilleure sécurité que l'actuel protocole IP,
- Accorder plus d'attention au type de service, et notamment aux services associés au trafic temps réel,
- Faciliter la diffusion multi-destinataire en permettant de spécifier l'envergure,
- Donner la possibilité à un ordinareur de se déplacer sans changer son adresse,
- Permettre au protocole une évolution future, c'est-à-dire anticiper sur des utilisations futures demandant des fonctions evoluées, telles que la mobilité, le multimédia etc.
- Accorder à l'ancien et au nouveau protocole une coexistance pacifique

2.2 Caractéristiques de l'IPv6

Les caractéristiques de IPv6 :

Adressage étendu : passage de 4 à 16 octets.

Nouveau type d'adressage « Anycast »

Abandon des « broadcast » en faveur des « multicast » .

Simplification du header (l'entête de trame).Élimination des champs qui ne servaient pas vraiment, simplification et généralisation des options.

Identification : Une extension à l'entête permet d'inscrire de l'information permettant l'identification sécure de la provenance d'un paquet. Ceci est essentiel pour l'utilisation fiable des nouvelles capacités de routage.

Discrétion :Une extension permet l'encryption de confidentialité.

Qualité de service .

Tunelling : Encapsule différent types d'adresses.

Nouvelle capacité de routage : On peut forcer le chemin de retour. Ce qui est particulièrement utile pour renforcer la qualité de service.

Autoconfiguration : Possibilité d'autoconfigurer une machine simplement en combinant son adresse Ethernet et en obtenant d'un serveur les 80 bits manquant.

Deuxième partie

Fonctionnement de l'IPv6

3 Les adresses

Les adresses sont maintenant représentées sur 128 bits. Elles comprennent 8 groupes de 4 chiffres hexadécimaux séparés par le symbole « : » .
Exemple 8000 :0000 :0000 :0000 :0123 :4567 :89AB :CDEF .
On peut dans chaque groupe enlever les zéros de tête et les groupes de 4 zéros (0000) peuvent être supprimés sous condition que l'on garde le « : » avant et après (exemple de réécriture de l'adresse précédente 8000 : :123 :4567 :89AB :CDEF). Les masques de sous réseaux sont sous la forme CIDR (à savoir la représentation avec le slash « / »). Ainsi , en prenant par exemple le masque par défaut pour une adresse de type lien-local, l'adresse précédente devient avec un masque 8000 : :123 :4567 :89AB :CDEF/64.

IPv6 reconnaît 3 types d'adressages :

Le type unicast : L'adresse désigne une et une seule machine. Elle se divise en 2 fois 64 bits, la partie réseau (ou préfixe) et la partie hôte (ou suffixe). La partie réseau (à gauche) contient tout d'abord 48 bits publics « Global Routing Prefix » puis 16 bits de site définissant le sous-réseaux. La partie hôte identifie la machine dans le réseau (elle est codée à partir de l'adresse MAC).

Le type multicast (préfixe FF00 : :/8) : elles remplacent les adresses de type « broadcast » (diffusion) . Une adresse multicast correspond à un groupe d'interfaces donné. Une interface est libre de s'abonner ou de quitter un groupe à tout moment. Suite au préfixe, on a un champ Drapeau sur 4 bits puis un champ d'envergure sur 4 bits encore et enfin l'identificateur de groupe sur 112 bits.

Le type anycast : cette technique est similaire à la diffusion multidestinataire car l'adresse de destination est un groupe d'adresses.Cependant au lieu de livrer le datagramme à tous les membres du groupe, on livre au plus proche ou au plus apte à le recevoir.

Enfin une nouvelle notion va avec les adresses IPv6, c'est le scope (la portée). En faite une interface ne possède pas qu'une seule adresse IPv6 mais peut en avoir plusieurs. Les 4 portées d'adresses sont :

- Noeud-local : il s'agit de l'adresse de loopback. Elle est notéé : :1/128.
- Lien-local : adressage commun aux mahines d'un même lien physique reliées entre elles sans routeur intermediaire. Ces adresses ont le préfixe FE80 : :/64.
- Site-local : adressage commun des machines d'un même site. Par exemple, un site qui n'est pas encore relié à Internet peut utiliser ce type d'adresse. C'est un peu le principe des adresses privées en IPv4 (192.168.x.x ou 10.x.x.x). Une adresse site local a comme préfixe FEC0 : :/48 suivi d'un champ de 16 bits permettant de définir des sous réseaux.
- Globale : ce sont les adresse dont le routage est effectué sans restriction. Leur préfixe est 2000 : :/3.

4 Les en-têtes IPv6

La taille des en-têtes est fixée à 40 octets Les en-têtes sont représentées comme suit :

Version 6	DiffServ	Flow Label
Payload Length	Next header	Hop Limit
Source Adress		
Destination Adress		

TABLE 1 – En-têtes IPv6

Le DiffServ est utilisé pour distinguer les sources qui doivent bénéficier du contrôle de flux des autres. Des priorités de 0 à 7 sont affectées aux sources capables de ralentir leur débit en cas de congestion. Les valeurs 8 à 15 sont assignées au trafic temps réel dont le débit est constant. (8 bits)

Le flow Label contient un numéro unique choisi par la source qui a pour but de faciliter le trvail des routeurs et de permettre la mise en oeuvre des fonctions de qualité de services comme RSVP. (8 bits)

Le playload length contient la taille des données utiles, sans prendre en compte la longueur de l'en-tête. (16 bits)

Le next header identifie le type de header qui suit immmédiatement selon la même convention qu'IPv4 (8 bits)

Le Hop Limit remplace le champ « TTL » en IPv4. Sa valeur est décrémentée à chaque noeud traversé. Si cette valeur atteint 0 alors que le paquet traverse un routeur, il sera rejeté avec l'emission d'un message ICMPv6 d'erreur. (8 bits)

Et enfin les champs d'adresse source et d'adresse de destination.

A la suite de cet en-tête peut suivre des en-têtes d'extension : Le paquet IPv6 inclut un champs d'extension pour les fonctionnalités optionnelles (sécurité, source routing, ...). Les options de IPv6 sont placées dans des en-têtes séparés, intercalés entre l'en-tête IPv6 et l'en-tête de la couche transport.

Les différents en-têtes optionnels sont :

- Option hop-by-hop : Contient les options qui doivent être honorés par tous les routeurs de transit.
- Routage : Permet de modifier le routage à partir de la source.
- Fragment : Contient les informations relatives à la fragmentation (si le paquet était trop gros au depart)
- Authentification Header : Contient les informations nécessaires à l'authentification de l'en-tête.
- Encapsulating Security Payload (ESP) : Contient les informations relatives au chiffrement du contenu.
- Options de destination : Options qui doivent être traitées par la destination finale.
- No Next Header : Indique qu'il n'y a aucune charge utile qui suit.

Fragmentation Alors que dans le cas du protocole IPv4 tous les routeurs pouvaient fragmenter les datagrammes, pour IPv6, ce n'est plus le cas ; Seule la source a le droit de fragmenter et seule la destination celui de défragmenter (fragmentation de bout en bout). S'il est nécessaire de fragmenter, la source insère un petit en-tête d'extension après l'en-tête de base de chaque fragment. Le but de la fragmentation de bout en bout est de réduire les frais de gestion de la fragmentation dans les routeurs et permettre ainsi à chaque routeur de traiter plus de datagrammes par unité de temps. Une des conséquences

est que si un routeur tombe en panne, il est difficile de changer le chemin car cela peut changer la MTU du chemin. Lorsqu'un protocole utilise la fragmentation de bout en bout, la source doit faire une recherche de MTU minimum tout au long du chemin et fragmenter tout datagrammes sortant inférieur au MTU. La fragmentation de bout en bout s'accommode mal des modifications de chemin.

5 Attribution des adresses

Il existe deux méthodes différentes, la configuration manuelle et l'automatique.Lors de la manuelle, l'administrateur fixe l'adresse.Et dans l'automatique, il y a plusieurs façons :

L'autoconfiguration sans état : Elle ne demande aucune configuration manuelle des machines, une configuration minimum pour les routeurs et aucun serveur supplementaire. Elle se sert du protocole ICMPv6 et peut fonctionner sans la présence de routeurs. Elle nécessite cependant un sous réseau à diffusion. Cette méthode ne s'applique que pour des machines et ne peut être retenue pour la configuration des routeurs. Le principe de base de l'autoconfiguration sans état est qu'une machine génère son adresse IPv6 à partir d'informations locales et d'informations fournies par un router. Le routeur fournit à la machine les informations sur le sous-réseau associé au lien, il donne le préfixe

L'autoconfiguration avec tirage pseudo aléatoire : adresse temporaire modifiées régulièrement

Génération cryptographiquement.

Attribution par un serveur DHCPv6 (autoconfiguration avec état) : Elle permet à une machine IPv6 d'obtenir les adresses et/ou d'autres informations de configuration par l'intermédiaire d'un serveur. Tout mécanisme d'autoconfiguration avec état est bâti sur le modèle client-serveur et repose sur l'utilisation d'un protocole DHCPv6. Le serveur maintient une table lui permettant de connaitre les adresses déjà alouées. L'ensemble des adresses générées par le serveur est créé par l'administrateur du site. Le serveur DHCP ne se trouve pas forcement sur le même lien client et, dans ce cas, les échanges DHCPv6 passent par des relais.

Troisième partie

Adaptabilité et mise en place de l'IPv6

A cause du manque d'adresse IP, il est nécessaire de passer au protocole IPv6 rapidement. A cause de l'étendue d'Internet et d'absence d'autorité de décision ou de contrôle sur la globalité du réseau Internet, il est impossible d'effectuer ce changement en une seule fois sur la totalité de réseau. C'est pourquoi le changement d'IPv4 à IPv6 doit obligatoirement se faire de manière graduelle et sans échéance sur la disparition d'IPv4.
Une solution pour « forcer » ce changement serait de trouver une utilisation d'Internet (appelée « killer application ») qui n'est utilisable qu'avec IPv6. Or comme IPv6 n'est qu'une évolution d'IPv4, elles possèdent les mêmes caractéristiques (telles que les fonctionnalité ou encore la qualité de service). Ainsi il n'a été trouvé aucune application de ce type à ce jour.
Le seul moyen de passer à IPv6 est donc d'adapter les réseaux et les stations à l'utilisation d'IPv6 en attendant qu'IPv4 disparaisse de lui-même. Pour cela, il faut rendre les machines compatibles avec IPv6 et pouvoir transporter des adresses IPv6 sur le réseau Internet.

6 Intégrer le protocole IPv6 sur les stations

- Les routeurs sont capables de gérer des adresses IPv4. Or il coûterait trop cher et il serait trop long de remplacer tous les routeurs afin de leur permettre de gérer uniquement IPv6. Ainsi les routeurs sont aujourd'hui équipés d'une double pile : chaque pile est dédiée à une version d'adresse IP (IPv4 ou IPv6) et permet d'allouer les adresses et d'effectuer le routage sur chaque réseau Internet. Ainsi un tel routeur peut communiquer indifféremment avec des stations utilisant IPv4 ou IPv6. De plus, dès la mise en oeuvre d'IPv6, les stations terminales ont été munies de cette double pile.
- Il faut toutefois faire attention car les applications qui utilisent Internet doivent être reprogrammées avant de pouvoir utiliser des adresses IPv6. De plus, les stations devraient comporter un serveur pour les

deux types d'Internet existant (Internet Ipv4 ou Internet IPv6), et un utilisateur d'IPv6 ne pourrait en théorie pas avoir accès aux applications programmées pour utiliser IPv4 (et la réciproque est également vraie). Afin d'éviter que les stations ne possèdent deux serveurs, on utilise un algorithme qui permet de voir une adresse IPv4 comme une partie d'adresse IPv6 : les 32 premiers bits de l'adresse IPv6 sont en fait vu comme l'adresse IPv4. Ainsi un utilisateur peut avoir accès à toutes les applications, quelles que soit le type d'adresse IP qu'il utilise.

7 Transporter des adresses IPv6

Il est évident que deux machines adjacentes utilisant un protocole IPv6 peuvent communiquer sans problème. Les complications apparaissent lorsque deux stations IPv6 veulent communiquer sans être adjacentes. En effet, il n'est pas sur que tous les routeurs se trouvant entre les deux stations possèdent une double pile permettant de gérer IPv6. Si jamais il existe effectivement un routeur ne gérant pas IPv6 entre les stations, il faut alors utiliser des tunnels. Cela consiste à transporter les adresses IPv6 via le réseau Internet IPv4.
Pour cela, on découpe l'adresse IPv6 et on l'intègre dans des paquets IPv4. Cette opération est appelée encapsulation d'IPv6 dans IPv4. Ensuite, il suffit de transporter les paquets IPv4 jusqu'à un routeur muni d'une double pile qui recréera l'adresse IPv6. Différents mécanismes d'encapsulation d'IPV6 dans IPv4 peuvent être mis en place, selon qu'il s'agit d'un réseau global ou d'un réseau local.

7.1 6to4 : le déploiement d'IPv6 sur un réseau global

- 6to4 est un logiciel que peut télécharger un utilisateur d'IPv6 ne disposant pas d'un accès à Internet IPv6. Il suffit pour cela que son fournisseur d'accès internet ait crée au moins un relai 6t04 (i.e un ensemble de routeurs munis de doubles piles et ayant tous le même préfixe IPv6, ceci afin d'éviter l'engorgement des tables de routage IPv6) qui va encapsuler les adresses IPv6 dans IPv4. Ce relai est connecté aux réseaux IPv4 et IPv6 et va permettre de créer un tunnel entre deux réseaux IPv6. Une station munie de 6t04 peut alors communiquer avec

un réseau ou une machine IPv6 lointaine.

- Les fournisseurs d'accès internet peuvent donc se contenter de fournir quelques routeurs gérant à la fois IPv4 et IPv6. Ainsi, même si une station n'a pas directement accès à l'Internet IPv6, grâce au logiciel 6t04 elle peut quand même utiliser Internet IPv6. Il faut toutefois être conscient que cette technique risque d'augmenter les temps de transmission de l'information (à cause du temps d'encapsulation) et qu'il ne s'agit donc que d'une technique temporaire avant qu'IPv4 disparaisse.

7.2 ISATAP : le déploiement d'IPV6 sur un réseau local

- ISATAP est un processus similaire à 6t04. Tout comme 6t04, il permet de se connecter à Internet IPv6, mais à partir d'un réseau local et non d'un réseau global. Tout comme 6t04, ISATAP possède un processus qui permet de faire le tunelling automatique, i.e il gère l'encapsulation de manière automatique et permet de connecter des terminaux IPv6 dans un réseau IPV4. Comme ISATAP est utilisé dans un réseau local, toutes les stations de ce réseau possède le même préfixe IPv6 et appartiennent au même lien (afin de réduire la taille des tables de routage).
- Le fonctionnement d'ISATAP :
  Nous allons voir comment le processus ISATAP fonctionne (ceci donne également une idée du fonctionnement de 6t04). Dans un premier temps, l'entité terminale doit connaître l'adresse IPv4 du routeur utilisé (il est évident que ce routeur doit être capable de gérer un processus ISATAP). Une fois cette adresse connue, le terminal envoie un message de sollicitation au routeur. Ce message contient une adresse source (qui est en fait l'adresse du réseau privé) et une adresse destination (qui est l'adresse du routeur). Ce message de sollicitation est encapsulé dans des paquets IPv4 (qui ont évidemment l'adresse du routeur pour adresse destination). Le routeut répond alors au message de sollicitation, sa réponse est contenue dans des paquets IPv4 transporté avec une connexion en point-à-point. Dans sa réponse, il envoie également les préfixes IPv6 que les stations du réseau local seront autorisées à utiliser.

Conclusion

Le changement des adresses IPv4 vers des adresses IPv6 ne peut se faire que progressivement. Pour que ce changement ne soit pas trop complexe à la vue des utilisateurs, il est nécessaire de modifier les routeurs et les stations terminales afin de leur permettre d'utiliser à la fois des adresses IPv4 et des adresses IPv6. Toutefois cette technique ne peut pas forcer l'utilisation d'adresses IPv6 et ne garantit donc pas la disparition d'IPv4. Dans ce cas, il peut sembler improbable qu'IPv6 remplace totalement les adresses IPv4 dans le futur.
Toutefois, le manque d'adresses IPv4 (qui risque d'arriver plus vite que ce qui était prévu à cause du développement de l'Asie) peut être un moyen de forcer ce changement à avoir lieu. On peut donc espérer que dans le futur, les routeurs et les stations ne géreront plus que des adresses IPv6 et que le protocole IPv4 disparaîtra conplètement.

Le problème du manque d'adresses IP et l'évolution nécessaire vers un nouveau protocole montre les difficultés liées à Internet : en effet, à cause de son étendue et de l'abscence d'autorité au niveau global, il n'est pas possible d'effectuer de changements radicaux et l'on doit se contenter d'adapter les équipements pour supporter deux protocoles différents en attendant que le changement soit forcé à cause d'une situation critique.