IP v6

Le but de ce dossier est avant tout de centraliser les données et synthétiser un maximum les informations sur l'IPv6, il ne s'agit donc pas d'une recopie de RFC.

Historique

Il faut bien commencer l'article, ainsi, depuis 1992, se posent les premières réflexions sur la saturation des adresses IP, par l'Internet Engineering Task Force. En 1994, premières recommandations. En 1996, les premiers prototypes d'IPv6 voient le jour. En 2003, on devrait commencer à voir migrer les segments IPv4 vers v6.

Technique

La norme actuelle IPv4 commence à montrer de sérieuses limitations. Tout d'abord le nombre d'adresses IP disponibles, manque de robustesse pour ce qui est de la sécurité et manque de finesse pour les connexions temps réel.

C'est là qu'interviendra IPv6 ou IP ng pour "next generation", enjeu capital pour la survie d'Internet. Puisque les 2 objectifs capitaux sont :

- régler le problème d'espace d'adressage pour l'Internet, mais aussi pour la domotique, votre voiture, votre chien, votre femme, enfin tout quoi !

- Anticiper sur les besoins futurs de la communication avec les applications multimédia, la mobilité des postes, etc...

Mais cette nouvelle norme doit permettre une mise à jour des plus progressives des routeurs, avec une coexistence transparente (si, si j'insiste) avec la version IP actuelle (la V4).

Parlons (peu mais bien des adresses IP, elles vont passer de 4 octets à 16 (soit 128 bits). Notons que les adresses commençant par 010 (soit 1/8 de l'espace total) seront affectées aux machines connectées et conservant la hiérarchie des 125 bits restants. La taille des portions réservées étant variable, la notion des classes avec un nombre de bits fixes, est corrigée ; j'espère que ça vous arrange, parce que sinon !x=?$*µ: .

De plus, IPv6 prévoit la notion de réseau autonome en prévoyant que les adresses commençant par 1111 1110 1 seront des adresses locales et pourront être utilisées librement dans un réseau local, les bits de poids faibles seront utilisés pour identifier le masque et l'adresse de la station qui voudrait "sortir".

IPv4, ne garantit aucun délai sur l'acheminement des paquets et l'on doit déborder d'astuces pour faire tourner des applications comme Windows Média Player et/ou autre soft du même style en « buffeurisant ». C'est pourquoi IPv6 instaure les champs "identification de flux" et "priorité". Le principe général est le suivant, à l'heure où je vous parle, ce n'est peut être plus tout à fait pareil, mais bon :

Lorsqu'un émetteur désire transmettre un flux de données (audio, vidéo,...) vers un destinataire (unique ou pas) il attribue un identifiant unique à tous ces paquets (un peu de respect svp). Il signifie aux routeurs qu'il requiert (oui les paquets, faut suivre un peu), un traitement uniforme de leur part. Les caractéristiques de ce traitement (par exemple réserver une capacité de transmission déterminée) pourront être transmises par le protocole de gestion de réseau soit par les paquets eux-mêmes (extension de l'en-tête). Le champ "priorité" vient ajouter un autre paramètre qui peut être utilisé par un émetteur, affecter le traitement des paquets émis par lui. Cette priorité n'est pas absolue, mais relative à un émetteur déterminé: 0 a 7 pour un trafic normal, 8 à15 pour les flots temps réel. Dans ce cas c'est le récepteur qui a en charge d'effectuer les acquittements et de prévenir l'émetteur des éventuelles pertes de paquets.

D'après les concepteurs, l'utilisation conjointe de ces 2 champs permet de gérer correctement la hiérarchie des priorités entre les différents flux de données que le réseau doit router en respectant 2 grands principes d'Internet, pas de réservation de bande passante pour une liaison particulière - propre cependant - (VLAN, mais non pas vlan, plutôt: Virtual Lan Area Network) et une autonomie de chaque nœud du réseau (pas de supervision générale, hein Billou !)

Les informations optionnelles ne figurent plus dans l'en-tête (à la dif de IPv4) mais dans des extensions spécifiques à la suite de celui-ci qui reste donc de longueur fixe. La longueur de ces extensions est extensible par multiple de 8 et non limitées (ex: routage imposé, encapsulation, info sur la fragmentation,...), tout ce que vous voulez tant que ce soit propre !.

Pour la sécurité, l'authentification garantit l'authentification et l'intégrité des transmissions. L'encapsulation, utilise l'algorithme DES (Data Encryption Standard), mais tout ceci est voué à l'évolution compte tenu des législations et droits d'utilisations.

C'est bien beau, mais le problème c'est de passer de la v4 à la v6 (la v5 ou ST Datagram mode quasiment inutilisée (http://www.olympus-zone.net/00-Home/04-Protocoles/05-IPv5/?Theme=Blue&langue=fr) ou comment faire cohabiter 2 protocoles sur le réseau AIE, AIE !!! Eh oui car les nouvelles machines posséderont une adresse sur 16 octets, ce qui signifie que les routeurs et machines autres devront pouvoir retransmettre des paquets émis en IPv4 et réciproquement.

Plusieurs phases à ceci :

- Implémentation totale de la v4 et v6

- @v4 contenue dans @v6 et encapsulation de paquet v6 dans v4

- Puis traduction des en-têtes pour router nœud à nœud

La seule contrainte apparente, est la mise à niveau des serveurs DNS (Domain Name Server : machine hébergeant les répertoires qui permettent de convertir les identifiant alphabétiques en adresses IP).

On n'a pas fini d'en entendre parler ! Et je j'imagine déjà pas mal de SSII et autres prestataires ainsi que les équipementiers réseau se faire de joli bénéfice.

Liens annexes :

Pour finir, les personnes qui désirent avoir d'autre détail et consulter les RFC entre autre je recommande ces adresses :

http://www.urec.cnrs.fr/ipv6/RFC.html (il s'agit d'une page du site du CNRS, ou toutes les RFC concernant l'IPv6 sont disponible, et elles sont très nombreuses).

http://www.microsoft.com/ipv6

http://www.olympus-zone.net

http://abcdrfc.free.fr/rfc-vf/rfc2460.html Traduction de la RFC 2460 en Français, merci à son auteur.