RFC 7066 : IPv6 for 3GPP Cellular Hosts

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 novembre 2013

Date de publication du RFC : Novembre 2013

http://www.bortzmeyer.org/7066.html

Il y a désormais des tas d'engins mobiles connectés à l'Internet, par la 3G ou bientôt par la 4G (mon Dieu, je mets des termes marketroïdo-publicitaires sur mon blog...) Les spécifications de ces protocoles imposent normalement IPv6 mais, en pratique, on ne trouve quasiment jamais d'IPv6 sur ces réseaux mobiles (tiens, le RFC utilise le terme états-unien, "*cellular*"). D'ailleurs, ça veut dire quoi « gérer IPv6 » pour ces engins ? Quels sont, parmi les nombreux RFC sur IPv6, ceux qu'il faut absolument mettre en œuvre ? Les caractéristiques du monde mobile (capacité réseau très limitée, par exemple) ont-elles des conséquences particulières pour IPv6 ? Ce RFC fait le point sur « IPv6 sur réseaux mobiles ». Il succède au RFC 3316 [1], qui avait été le premier, en 2003, à se lancer dans ce travail.

Ces technologies de réseaux mobiles permettent à un appareil comme le "*smartphone*" d'avoir, lui aussi, une connexion permanente à l'Internet, comme l'ADSL le permet aux machines fixes. Cela a commencé avec le GPRS, puis l'UMTS et quelques autres techniques. Résultat, des centaines de millions d'engins mobiles sont connectés et chacun a besoin d'une adresse IP. IPv4 n'y suffit plus depuis longtemps, et, aujourd'hui, avoir un accès Internet sur son mobile impose quasiment toujours d'être coincé avec une adresse privée (RFC 1918). D'où l'intérêt d'IPv6, qui permettra à chaque machine d'avoir son adresse publique. UMTS a apparemment été le premier réseau mobile où IPv6 était mentionné dans la spécification. Pour les réseaux EPS/LTE, voir le RFC 6459.

Normalement, « avoir IPv6 », pour une machine terminale <http://www.bortzmeyer.org/terminal-host.html>, est facile à définir. Cela veut dire respecter les règles du RFC 6434, qui rassemble en un document la liste des exigences. D'ailleurs, notre RFC 7066 ne prétend pas remplacer ce RFC 6434 : il le complète, pour préciser les points spécifiques aux réseaux mobiles (« cellulaires », comme si on était en prison). Il vise surtout les programmeurs qui vont mettre ou maintenir IPv6 dans Android, iOS, etc. À noter que le RFC distingue trois types de machines terminales connectées aux réseaux mobiles :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3316.txt

— Celles complètement fermées, où l'utilisateur ne peut rien changer (un téléphone classique),
— Celles où l'utilisateur peut ajouter des applications (le "*smartphone*" typique),
— Celles où l'accès 3G est extérieur à la machine, par exemple un ordinateur portable muni d'une clé 3G, où les applications (et même une bonne partie du système) ne savent pas qu'elles utilisent la 3G.

Ce RFC se focalise sur l'IPv6, pas sur les techniques de transition d'IPv4 vers IPv6 ou de coexistence temporaire entre les deux protocoles. Il rappelle que la meilleure technique est la « double-pile » du RFC 4213 : que chaque machine ait deux adresses, une v4 et une v6, le temps de la transition.

Le RFC commence par les exigences de base ("*Basic IP*"), celles qui s'appliquent dans tous les cas (section 2). La machine doit évidemment mettre en œuvre la norme IPv6 de base (RFC 2460), ainsi que les mécanismes de découverte du voisin du RFC 4861.

Toutefois, il faut nuancer. Dans les réseaux GPRS, UMTS et EPS, la liaison est point-à-point : une machine n'a qu'un seul voisin, déjà connu car il s'annonce comme routeur (ce routeur est appelé par des sigles pittoresques qui dépendent de la technologie utilisée, comme GGSN ou PGW). Et donc, logiquement, il n'y a pas d'adresse de niveau 2, donc pas besoin d'un protocole pour résoudre les adresses IP en adresses de niveau 2, comme le fait NDP. Même si le routeur répondait aux messages "*Neighbor Solicitation*", sa réponse ne contiendrait pas d'adresses de niveau 2. Le mécanisme NUD ("*Neighor Unreachability Detection*") du RFC 4861, section 7.3, reste nécessaire (des détails dans l'annexe A). Ces messages permettent de s'assurer que le voisin répond bien. Mais il ne faut pas en abuser : les engins connectés à un réseau mobile ont en général une batterie à capacité limitée. Notre RFC recommande donc, pour s'assurer que le voisin est toujours vivant, de compter avant tout sur des indications indirectes, comme le retour des paquets TCP, ou comme les réponses DNS lorsqu'on a utilisé UDP pour les questions. Avec les protocoles de téléphonie comme RTP (RFC 3550) ou SIP (RFC 3261), il faut se servir des mécanismes de rétroaction de ces protocoles, pour confirmer la joignabilité. On ne doit faire du NUD qu'en dernier recours.

Le mobile ainsi connecté doit configurer sa propre adresse IPv6 avec SLAAC ("*StateLess Address AutoConfiguration*", RFC 4862), ce qui veut dire qu'il doit accepter les RA ("*Router Advertisment*") envoyés d'en face. Aucun besoin de faire de la détection d'adresses dupliquées (RFC 4862, section 5.4) puisqu'on est seul sur le lien (avec le routeur). En revanche, DHCP (RFC 3315) n'est pas obligatoire, mais on peut l'utiliser, par exemple pour récupérer les adresses des serveurs SIP (RFC 3736 et RFC 3319) ou pour obtenir la délégation d'un préfixe à utiliser sur le réseau local (RFC 3633, au cas où le mobile serve lui-même de routeur pour un tel réseau, par exemple en WiFi).

Le mécanisme d'adressage est très différent de celui des réseaux fixes. Le préfixe de l'adresse est fourni par le routeur et est unique par connexion 3G. Le suffixe est également choisi par le routeur, en général au hasard, il n'y a pas d'adresse MAC en dur dans l'engin mobile. L'annexe A rappele les particularités de l'adressessage IPv6 en 3G.

Le mobile doit également savoir trouver les adresses des résolveurs DNS avec SLAAC, comme normalisé dans le RFC 8106. Certes, ces adresses sont normalement transmises au mobile en 3G, sans passer par un protocole IP, mais il peut y avoir sur le trajet des intermédiaires qui ont du mal à passer cette option.

À ce sujet, on a parfois du PPP (RFC 1661) entre le mobile et un autre équipement, notamment dans le cas d'ordinateurs avec clé 3G. Dans ce cas, il faut utiliser le protocole de contrôle PPP pour IPv6, IPv6CP, normalisé dans le RFC 5072.

Des problèmes de vie privée ? Forcément, oui. Un mobile étant mobile, pouvoir le suivre à la trace serait très intéressant pour certains, et néfaste pour la vie privée de son propriétaire. Il est donc recommandé de mettre en œuvre les adresses temporaires du RFC 4941 mais lisez plus loin, la question de

l'adressage IPv6 sur les réseaux 3G est plus compliquée qu'elle n'en a l'air. Comme le rappelle la section 7, la partie spécifique à la machine ("*Interface Identifier*") de l'adresse IPv6 est donnée par le réseau, elle n'est pas une propriété constante de la machine (comme l'est une adresse Ethernet) et le suivi à la trace via les adresses 3G est donc nettement moins possible. En fait, c'est plutôt le préfixe et pas le suffixe qui identifie une machine, car il reste constant pendant le déplacement.

Et une dernière chose à bien garder en tête : la MTU. Les réseaux mobiles utilisent beaucoup de tunnels et les paquets peuvent donc avoir une taille maximum plus faible que prévue. Il est donc impératif que les mobiles tiennent compte de l'option MTU dans les messages RA (section 4.6.4 du RFC 4861).

Une fois ces questions de base réglées et correctement mises en œuvre dans le mobile, le RFC a encore deux courtes sections. La section 3 concerne la sécurité. Elle rappelle qu'IPsec n'est pas obligatoire (bien que, évidemment, son usage sécuriserait tout le trafic du mobile, avant son envoi sur les ondes radio). Elle note aussi qu'un mobile peut s'attendre à recevoir des paquets fragmentés, que ceux-ci posent des problèmes de sécurité fréquents, et qu'il faut donc suivre les RFC 5722 et RFC 6980. La sécurité est également discutée en section 7.

La dernière section d'exigences, la section 4, concerne la mobilité. Dans le monde 3G, elle est gérée par les couches basses et il n'est donc pas du tout nécessaire de mettre en œuvre les techniques de mobilité IP (par exemple celles du RFC 5555).

L'annexe B résume les changements depuis le RFC 3316. Rien de révolutionnaire, essentiellement des clarifications, l'ajout de technologies récentes comme la découverte des résolveurs DNS par le RFC 6106, beaucoup de points liés à la sécurité, suite au RFC 6583, etc.

Je ne fournis dans cet article aucun exemple concret : c'est parce que les opérateurs qui font de l'IPv6 sur la 3G sont en nombre infime (aucun en France). Par exemple, regardez le dernier point `<http://www.sfr.com/reseaux/nos-technologies/06072012-1701-le-passage-lipv6-chez-sfr>` fait par SFR, aucune date n'était annoncée.

Si vous avez le courage de lire les normes 3GPP, elles sont disponibles en ligne `<http://www.3gpp.org/specifications>`. Voyez notamment "*TS 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*" `<http://www.3gpp.org/ftp/Specs/html-info/23401.htm>`.