RFC 6434 : IPv6 Node Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 décembre 2011

Date de publication du RFC : Décembre 2011

https://www.bortzmeyer.org/6434.html

Il existe des tas de RFC qui concernent IPv6 et le programmeur qui met en œuvre ce protocole dans une machine risque fort d'en rater certains, ou bien d'implémenter certains qu'il aurait pu éviter. Ce RFC était donc un méta-RFC, chargé de dresser la liste de ce qui est **indispensable** dans une machine IPv6. Il a été remplacé depuis par le RFC 8504 [1]. Les deux points les plus chauds concernaient la configuration (par DHCP ou par RA - "*Router Advertisment*" ?) et la gestion d'IPsec, désormais officiellement facultative.

Ce document remplace son prédécesseur, le RFC 4294 (et est lui-même remplacé par le RFC 8504. Il vise le même but, servir de carte au développeur qui veut doter un système de capacités IPv6 et qui se demande s'il doit vraiment tout faire (réponse : non). Ce RFC explique clairement quels sont les points d'IPv6 qu'on ne peut **pas** négliger, sous peine de ne pas pouvoir interagir avec les autres machines IPv6. Le reste est laissé à l'appréciation du développeur. La section 2 résume ce but.

Les deux gros changements par rapport au RFC 4294 sont :
— DHCP monte en grade, bien que restant derrière les RA pour la configuration des machines IPv6,
— IPsec n'est plus obligatoire.
Ce RFC s'applique à tous les **nœuds** IPv6, aussi bien les **routeurs** (ceux qui transmettent des paquets IPv6 reçus qui ne leur étaient pas destinés) que les **machines terminales <https://www.bortzmeyer.org/terminal-host.html>** (toutes les autres).

Bien, maintenant, les obligations d'une machine IPv6, dans l'ordre. D'abord, la couche 2 (section 4 du RFC). Comme IPv4, IPv6 peut tourner sur des tas de couches de liaison différentes et d'autres apparaîtront certainement dans le futur. En attendant, on en a déjà beaucoup, Ethernet (RFC 2464), 802.16 (RFC 5121), PPP (RFC 5072) et bien d'autres, sans compter les tunnels.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8504.txt

Ensuite, la couche 3 (section 5 du RFC) qui est évidemment le gros morceau puisque c'est la couche d'IP. Le cœur d'IPv6 est normalisé dans le RFC 2460 et ce dernier RFC doit donc être intégralement implémenté, à l'exception de l'en-tête de routage de type 0, qui a été abandonné par le RFC 5095.

Comme IPv6, contrairement à IPv4, ne permet pas aux routeurs intermédiaires de fragmenter les paquets, la découverte de la MTU du chemin est particulièrement cruciale. La mise en œuvre du RFC 1981 est donc recommandée. Seules les machines ayant des ressources très limitées (genre où tout doit tenir dans la ROM de démarrage) sont dispensées. Mais le RFC se doit de rappeler que la détection de la MTU du chemin est malheuresement peu fiable dans l'Internet actuel, en raison du grand nombre de pare-feux configurés avec les pieds et qui bloquent tout l'ICMP. Il peut être donc nécessaire de se rabattre sur les techniques du RFC 4821).

Le RFC 2460 décrit le format des paquets et leur traitement. Les adresses y sont simplement mentionnées comme des champs de 128 bits de long. Leur architecture est normalisée dans le RFC 4291, qui est obligatoire.

Également indispensable à toute machine IPv6, l'autoconfiguration sans état du RFC 4862, ainsi que ses protocoles auxiliaires comme la détection d'une adresse déjà utilisée.

ICMP (RFC 4443) est évidemment obligatoire, c'est le protocole de signalisation d'IP (une des erreurs les plus courantes des administrateurs réseaux incompétents est de bloquer ICMP sur les pare-feux).

Dernier protocole obligatoire, la sélection de l'adresse source selon les règles du RFC 3484 (depuis remplacé par le RFC 6724), pour le cas où la machine aurait le choix entre plusieurs adresses (ce qui est plus fréquent en IPv6 qu'en IPv4).

Le reste n'est en général pas absolument obligatoire mais recommandé (le terme a un sens précis dans les RFC, définie dans le RFC 2119 : ce qui est marqué d'un "*SHOULD*" doit être mis œuvre, sauf si on a une bonne raison explicite et qu'on sait exactement ce qu'on fait). Par exemple, la découverte des voisins (NDP, RFC 4861) est recommandée. Toutes les machines IPv6 en ont besoin, sauf si elles utilisent les liens ne permettant pas la diffusion.

Moins générale, la sélection d'une route par défaut s'il en existe plusieurs, telle que la normalise le RFC 4191. Elle est particulièrement importante pour les environnements SOHO (RFC 7084).

On a vu que l'autoconfiguration sans état (sans qu'un serveur doive se souvenir de qui a quelle adresse) était obligatoire. DHCP (RFC 8415), lui, n'est que recommandé.

Une extension utile (mais pas obligatoire) d'IP est celle des adresses IP temporaires du RFC 8981, permettant de résoudre certains problèmes de protection de la vie privée. Évidemment, elle n'a pas de sens pour toutes les machines (par exemple, un serveur dans son "*rack*" n'en a typiquement pas besoin). Elle est par contre recommandée pour les autres.

Encore moins d'usage général, la sécurisation des annonces de route (et des résolutions d'adresses des voisins) avec le protocole SEND (RFC 3971). Le déploiement effectif de SEND est très faible et le RFC ne peut donc pas recommander cette technique pour laquelle on n'a pas d'expérience, et qui reste simplement optionnelle.

L'une des grandes questions que se pose l'administrateur réseaux avec IPv6 a toujours été « autoconfiguration RA - "*Router Advertisment*" - ou bien DHCP ? » C'est l'un des gros points de ce RFC et

la section 6 le discute en détail. Au début d'IPv6, DHCP n'existait pas encore pour IPv6 et les RA ne permettaient pas encore de transmettre des informations pourtant indispensables comme les adresses des résolveurs DNS (le RFC 6106 a résolu cela). Aujourd'hui, les deux protocoles ont à peu près des capacités équivalentes. RA a l'avantage d'être sans état, DHCP a l'avantage de permettre des options de configuration différentes par machine. Alors, quel protocole choisir ? Le problème de l'IETF est que si on en normalise deux, en laissant les administrateurs du réseau choisir, on court le risque de se trouver dans des situations où le réseau a choisi DHCP alors que la machine attend du RA ou bien le contraire. Bref, on n'aurait pas d'interopérabilité, ce qui est le but premier des normes Internet. Lorsque l'environnement est très fermé (un seul fournisseur, machines toutes choisies par l'administrateur réseaux), ce n'est pas un gros problème. Mais dans un environnement ouvert, par exemple un campus universitaire ou un "*hotspot*" Wifi, que faire ? Comme l'indiquent les sections 5.9.2 et 5.9.5, seul RA est obligatoire, DHCP ne l'est pas. RA est donc toujours la méthode recommandée si on doit n'en choisir qu'une, c'est la seule qui garantit l'interopérabilité. (Voir aussi la section 7.2 sur DHCP.)

Continuons à grimper vers les couches hautes. La section 7 est consacrée aux questions DNS. Une machine IPv6 devrait pouvoir suivre le RFC 3596 et donc avoir la possibilité de gérer des enregistrements DNS de type AAAA (les adresses IPv6) et la résolution d'adresses en noms grâce à des enregistrements PTR dans `ip6.arpa`. Les anciens enregistrements A6 (RFC 3363) ont été abandonnés mais on constate que ces enregistrements sont toujours très demandés lors des requêtes à des serveurs DNS faisant autorité, comme ceux de `.fr` (dans les 0,5 % des requêtes, soit davantage que SRV ou DS).

À noter qu'une machine IPv6, aujourd'hui, a de fortes chances de se retrouver dans un environnement où il y aura une majorité du trafic en IPv4 (c'est certainement le cas si cet environnement est l'Internet). La section 8 rappelle donc qu'une machine IPv6 peut avoir intérêt à avoir également IPv4 et à déployer des techniques de transition comme la double-pile du RFC 4213.

Encore juste une étape et nous en sommes à la couche 7, à laquelle la section 9 est consacrée. Si elle parle de certains détails de présentation des adresses (RFC 5952), elle est surtout consacrée à la question des API. En 2011, on peut dire que la grande majorité des machines a IPv6, côté couche 3 (ce qui ne veut pas dire que c'est activé, ni que le réseau le route). Mais les applications sont souvent en retard et beaucoup ne peuvent tout simplement pas communiquer avec une autre machine en IPv6. L'IETF ne normalise pas traditionnellement les API donc il n'y a pas d'API recommandée ou officielle dans ce RFC, juste de l'insistance sur le fait qu'il faut fournir une API IPv6 aux applications, si on veut qu'elles utilisent cette version d'IP, et qu'il en existe déjà, dans les RFC 3493 (fonctions de base) et RFC 3542 (fonctions avancées).

La sécurité d'IPv6 a fait bouger beaucoup d'électrons, longtemps avant que le protocole ne soit suffisamment déployé pour qu'on puisse avoir des retours d'expérience. Certains ont survendu IPv6 en prétendant que, contrairement à IPv4, il avait la sécurité intégrée dès le début et était donc plus sûr. Cette légende vient du fait qu'en théorie, IPsec était obligatoire pour toute mise en œuvre d'IPv6. Ce point n'a jamais été respecté par les implémentations (et puis, de toute façon, avoir IPsec est une chose, l'activer, avec sa complexe configuration, en est une autre). Désormais, depuis la sortie de notre RFC 6434, ce point n'est même plus vrai en théorie, IPsec (RFC 4301) est officiellement simplement recommandé.

Le RFC note donc bien que la sécurité est un processus complexe, qui ne dépend certainement pas que d'une technique magique (« IPsec est intégré donc il n'y a pas de problème de sécurité ») et qu'aucun clair gagnant n'émerge de la liste des solutions de sécurité (IPsec, TLS, SSH, etc). D'autant plus qu'IPv6 vise à être déployé dans des contextes comme « l'Internet des Trucs » où beaucoup de machines n'auront pas forcément les ressources nécessaires pour faire de l'IPsec.

Toutes les règles et recommandations précédentes étaient pour tous les nœuds IPv6. La section 12 expose les règles spécifiques aux routeurs. Ils doivent être capables d'envoyer les "*Router Advertisment*"

et de répondre aux "*Router Solicitation*" du RFC 4861 et on suggère aux routeurs SOHO d'envisager sérieusement d'inclure un serveur DHCP (RFC 7084) et aux routeurs de réseaux locaux de permettre le relayage des requêtes DHCP.

Enfin, la section 13 se penche sur la gestion des réseaux IPv6 en notant que deux MIB sont obligatoires, celle du RFC 4292 sur la table de routage, et celle du RFC 4293 sur IP en général.

Les changements par rapport au RFC 4294 sont résumés dans l'annexe 16. Les deux plus importants, comme déjà noté, sont IPsec et DHCP, un qui descend, l'autre qui monte. Mais on y trouve aussi l'arrivée de SEND (mais en option), celle des options DNS du RFC 6106, et beaucoup de détails et de clarifications. Depuis, le RFC 8504 a aussi apporté ses changements.