RFC 8504 : IPv6 Node Requirements

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 janvier 2019

Date de publication du RFC : Janvier 2019

https://www.bortzmeyer.org/8504.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 est donc un méta-RFC, chargé de dresser la liste de ce qui est **indispensable** dans une machine IPv6. Pas de changements spectaculaires par rapport au précédent RFC mais beaucoup de détails.

Ce document remplace son prédécesseur, le RFC 6434[1]. 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, ou à celle de profils spécifiques à un usage ou à une organisation (comme dans le cas du « "*Profile for IPv6 in the U.S. Government*" <https://www.nist.gov/programs-projects/usgv6-program> »). La section 1 résume ce but.

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, voyons 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), les réseaux pour objets connectés LowPAN 802.15.4 (RFC 4944), 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/rfc6434.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 8200 et ce dernier RFC doit donc être intégralement implémenté.

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 8201 est donc recommandée. Seules les machines ayant des ressources très limitées (du 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 malheureusement 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 recommande également de ne pas trop fragmenter les paquets, pour ne pas tenter le diable, un certain nombre de machines intermédiaires bloquant les fragments. Cela concerne notamment les protocoles utilisant UDP, comme le DNS, qui n'ont pas de négociation de la taille des messages, contrairement à TCP.

En parlant de fragmentation, notre RFC rappelle également qu'on ne doit pas générer de fragments atomiques (un datagramme marqué comme fragmenté alors que toutes les données sont dans un seul datagramme), pour les raisons expliquées dans le RFC 8021. Et il ne faut pas utiliser d'identificateurs de fragment prévisibles (RFC 7739), afin d'empêcher certaines attaques comme l'attaque Shulman sur le DNS <https://www.bortzmeyer.org/dns-attaques-shulman.html>.

Le RFC 8200 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. (Une tentative de mise à jour de ce RFC 4291 avait eu lieu mais a été abandonnée sous les protestations <https://www.ietf.org/mail-archive/web/ipv6/current/msg26235.html>.) La règle actuelle (RFC 7421) est que le réseau local a une longueur de préfixe de 64 bits (mais il y a au moins une exception, cf. RFC 6164.)

Également indispensable à toute machine IPv6, l'autoconfiguration sans état du RFC 4862 (SLAAC, "*StateLess Address AutoConfiguration*"), ainsi que ses protocoles auxiliaires comme la détection d'une adresse déjà utilisée. D'autre part, il est recommandé d'accepter l'allocation d'un préfixe entier à une machine (RFC 8273).

Les en-têtes d'extension (RFC 8200, section 4) sont un élément de base d'IPv6 et doivent donc être acceptés et traités par toutes les machines terminales. Notez que la création de nouveaux en-têtes est désormais déconseillée donc qu'une mise en œuvre d'IPv6 a des chances de ne pas voir apparaitre de nouveaux en-têtes. Même si c'était le cas, ils devront suivre le format générique du RFC 6564, ce qui devrait faciliter leur traitement.

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 <http://shouldiblockicmp.com/> sur les pare-feux).

Dernier protocole obligatoire, la sélection de l'adresse source selon les règles du 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). Et si la machine IPv6 a plusieurs adresses IP, et qu'il y a plusieurs routeurs, elle doit choisir le routeur en fonction de l'adresse source (RFC 8028).

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. Notez que DHCP ne permet pas d'indiquer le routeur à utiliser, cette information ne peut être obtenue qu'en écoutant les RA ("*Router Advertisements*").

Une extension utile (mais pas obligatoire) d'IP est celle des adresses IP temporaires du RFC 4941, 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. Le RFC 7721 fait un tour d'horizon plus général de la sécurité d'IPv6.

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 SLAAC - "*StateLess Address AutoConfiguration*" - / RA - "*Router Advertisement*" - ou bien DHCP ? » C'est l'un des gros points de ce RFC et la section 8.4 le discute en détail. Au début d'IPv6, DHCP n'existait pas encore pour IPv6 et les RA utilisés par SLAAC ne permettaient pas encore de transmettre des informations pourtant indispensables comme les adresses des résolveurs DNS (c'est maintenant possible, cf. RFC 8106). 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. Mais DHCP ne permet pas d'indiquer le routeur à utiliser. 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 6.3 et 6.5, 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.

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`.

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 10 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 11 est consacrée. Si elle parle de certains détails de présentation des adresses (RFC 5952), elle est surtout consacrée à la question des API. En 2019, on peut dire que la très 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. Le RFC note donc bien que la sécurité est un processus complexe, qui ne dépend certainement pas que d'une technique magique 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 14 expose les règles spécifiques aux routeurs. Ils doivent évidemment router les paquets (cf. RFC 7608). Ils doivent aussi être capables d'envoyer les "*Router Advertisement*" 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.

Nouveauté de ce RFC, la section 15 se penche sur le cas des objets contraints, ces tout petits ordinateurs avec peu de ressources, pour lesquels il a parfois été dit qu'IPv6 n'était pas réaliste. Le groupe de travail de l'IETF 6LowPAN <https://datatracker.ietf.org/wg/6lowpan> a beaucoup travaillé pour faire en sorte qu'IPv6 tourne bien sur ces objets contraints (RFC 4919). Pour la question de la consommation énergétique, voir le RFC 7772.

Enfin, la section 16 se penche sur la gestion des réseaux IPv6 en notant qu'au moins deux MIB sont recommandées, celle du RFC 4292 sur la table de routage, et celle du RFC 4293 sur IP en général. SNMP n'est plus le seul protocole cité, Netconf (RFC 6241) et Restconf (RFC 8040) apparaissent.

Les changements par rapport au RFC 6434 sont résumés dans l'annexe A. Pas mal de changements pendant les sept ans écoulés depuis le RFC 6434 mais aucun n'est dramatique :

— Ajout des objets contraints, et des questions liées à la consommation eléctrique,
— L'indication du résolveur DNS par les RA, devient obligatoire (section 8.3),
— Ajout de Netconf et Restconf pour la gestion des réseaux,
— Les questions liées à la vie privée sont plus nombreuses, avec par exemple le profil DHCP du RFC 7844,
— Les "*jumbograms*" du RFC 2675, peu déployés, ont été abandonnés,
— Autre abandon, celui d'ATM, un échec complet,
— Conseils sur la fragmentation, notamment pour le DNS.