RFC 7045 : Transmission and Processing of IPv6 Extension Headers

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 décembre 2013

Date de publication du RFC : Décembre 2013

https://www.bortzmeyer.org/7045.html

Encore un RFC de clarification sur IPv6. Le déploiement effectif de ce protocole a en effet suscité des questions qui n'étaient pas évidentes avant. Ce RFC s'occupe des en-têtes d'extension que peut contenir un datagramme IPv6. Les règles de traitement de ces en-têtes dans la section 4 du RFC 2460 [1] n'étaient en effet pas d'une clarté limpide. Ce RFC précise aussi les règles d'enregistrement de nouveaux en-têtes à l'IANA, puisqu'il n'existait malheureusement pas de liste faisant autorité.

Petit rappel, d'abord (section 1 du RFC) : l'en-tête normal d'un datagramme IPv6 est de taille fixe (40 octets) contrairement à ce qui se passe en IPv4. Mais entre cet en-tête et le contenu du paquet (qui peut être du TCP, de l'ICMP, de l'UDP ou même être vide), peuvent se glisser plusieurs en-têtes d'extension. Il y a donc une chaîne d'en-têtes, reliés par le champ "*Next header*" qui identifie le type de l'en-tête d'extension ou du contenu qui suit. Par exemple, un "*Next header*" à 60 signifie que cet en-tête est suivi par un en-tête "*Destination options*" <https://www.bortzmeyer.org/destination-options-ipv6.html> alors qu'un "*Next header*" à 6 indique que l'en-tête est suivi par du contenu TCP.

La norme IPv6, le RFC 2460, spécifiait dans sa section 4 un jeu initial d'en-têtes d'extension, ainsi que la façon de les traiter. À l'exception de l'en-tête "*Hop-by-Hop Options*", les en-têtes d'extension devaient être ignorés par les routeurs intermédiaires, et traités uniquement dans la machine de destination finale. Ainsi, de nouveaux en-têtes pouvaient être introduits sans affecter les routeurs et sans que ceux-ci aient besoin d'être mis à jour.

Ce schéma correspondait à l'architecture originale de l'Internet : le moins de traitements possible dans les nœuds intermédiaires, et toute l'intelligence aux extrémités. Mais ce modèle est désormais menacé par l'invasion de "*middleboxes*" plus ou moins invasives. Par exemple, pare-feux et répartiteurs de

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2460.txt

charge inspectent le paquet et prennent des décisions en fonction d'autres informations que l'en-tête initial (en général, elles regardent au moins l'en-tête TCP). Résultat, on ne peut plus prétendre que le réseau est transparent pour les en-têtes d'extension. Ces "*middleboxes*" doivent suivre toute la chaîne des en-têtes et ce travail est plutôt compliqué <https://www.bortzmeyer.org/analyse-pcap-ipv6.html>, car il n'existait pas (jusqu'au RFC 6564) de format uniforme pour les en-têtes. Il est donc difficile de l'accomplir à la vitesse du réseau, lorsque celui-ci est du 100 Gb/s! Ce problème n'a pas de solution simple (il découle d'un mauvais choix lors de la création d'IPv6) mais on peut au moins spécifier rigoureusement ce qu'on attend de ces "*middleboxes*".

En effet, certaines "*middleboxes*", notamment les pare-feux, ont un comportement anormal. Un pare-feu est, par profession, paranoïaque : il rejette tout ce qu'il ne connait pas. Un en-tête inconnu et, hop, tout le paquet est jeté. Les en-têtes nouveaux ont donc peu de chances de réussir à se frayer un chemin dans l'Internet. Mais il y a pire : bien des pare-feux programmés avec les pieds par des gens qui n'ont jamais lu le RFC 2460 ne reconnaissent même pas la totalité des en-têtes d'extension originels. Ainsi, certaines fonctions d'IPv6, pourtant normalisées dès le début, comme la fragmentation, ont du mal à fonctionner.

Même si le programmeur de la "*middlebox*" a lu le RFC 2460, il risque de s'être simplifié la vie en ignorant la possibilité que de nouveaux en-têtes soient définis. L'IETF ne leur facilitait pas la tâche en ne fournissant pas de liste faisant autorité de tous les en-têtes déclarés. En effet, les numéros d'en-tête sont issus du même espace que les protocoles de transport (voir le registre <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>). Et il n'y avait pas de moyen simple de savoir si le numéro N dans cet espace désigne un protocole de transport ou un en-tête d'extension, si l'application ne connait pas ce qui est désigné par ce N. Résultat, les nouveaux en-têtes ont peu de chance d'être déployés (ils se heurteront à toutes les "*middleboxes*"). On voit donc peu d'applications qui tentent d'utiliser des nouveaux en-têtes... ce qui ne motive pas les développeurs de "*middleboxes*" à réparer leurs engins. Le format uniforme des en-têtes, décrit dans le RFC 6564, arrangera un peu les choses, en permettant de passer un en-tête, même inconnu.

Après ces préliminaires, les exigences (section 2 de notre RFC). D'abord, un rappel, le traitement des en-têtes d'extension n'est pas une cerise sur le gâteau, c'est un composant indispensable d'IPv6 et toute machine qui prétend traiter l'IPv6 doit traiter ces en-têtes et, si elle veut accéder au contenu du paquet, doit être capable de traiter la chaîne complète des en-têtes. Un simple routeur (qui ne regarde pas le contenu des paquets) doit transmettre les paquets qu'ils aient des en-têtes d'extension ou pas (ce routeur n'a que l'en-tête fixe à regarder). Un engin qui a des fonctions supplémentaires (comme un pare-feu) doit examiner toute la chaîne si elle ne comprend que des en-têtes normalisés et notre RFC recommande que cela soit possible même s'il existe des en-têtes inconnus dans la chaîne. Maintenant qu'une liste des en-têtes normalisés <https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#extension-header> est publiée, les programmeurs n'ont plus d'excuse.

Le RFC 2460 demandait que les machines de destination jettent les paquets contenant des en-têtes inconnus. Mais cela ne s'applique qu'aux machines de destination. Les machines intermédiaires, comme les pare-feux, ne doivent pas en faire autant, sinon il ne sera jamais possible de déployer de nouveaux en-têtes (je crains que cette excellente recommandation ne soit largement ignorée, dans un Internet de plus en plus ossifié).

Une machine intermédiaire peut avoir une option configurable pour jeter les paquets contenant des en-têtes normalisés mais cela doit être une option, non activée par défaut. (Pour les en-têtes inconnus, le choix par défaut peut être de les jeter.)

Une mention spéciale pour l'en-tête de routage (section 4.4 du RFC 2460). Il existe en plusieurs variantes, identifiées par un numéro de type. Si les types 0 et 1 ont été officiellement abandonnés pour

des raisons de sécurité (RFC 5095), il n'y a aucune bonne raison de jeter les paquets contenant d'autres types, comme le type 2 (RFC 6275) ou le type 3 (RFC 6554).

Une autre mention concerne l'en-tête "*hop by hop*", le seul que tous les routeurs sur le trajet sont censés examiner (c'est pour cela qu'il est obligatoirement en premier). Comme c'est très difficile à faire à pleine vitesse, notre RFC adopte une position réaliste en notant qu'il ne faut pas s'attendre à ce que tous les routeurs le fassent effectivement, et que ceux qui le feront utiliseront sans doute un chemin plus lent à l'intérieur du routeur.

La section 3 revient sur des questions de sécurité générales. Par exemple, elle rappelle que des en-têtes utilisant les valeurs marquées comme expérimentales (253 et 254) auront encore plus de problèmes que les autres à passer (RFC 4727).

Quant à la section 4, elle spécifie les changements à l'IANA visant à faciliter la tâche des programmeurs de code IPv6. D'abord, dans le registre des numéros de protocole <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>, ajouter une colonne pour indiquer s'il s'agit d'un en-tête d'extension IPv6 (la nouvelle colonne « "*IPv6 Extension Header*" »). Ensuite, créer un nouveau registre <https://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xhtml#extension-header> ne contenant que ces numéros. L'enregistrement de nouveaux en-têtes continue à suivre les règles du RFC 2780.