RFC 8883 : ICMPv6 Errors for Discarding packets Due to Processing Limits

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 septembre 2020

Date de publication du RFC : Septembre 2020

https://www.bortzmeyer.org/8883.html

Dans l'Internet, un routeur est toujours autorisé à jeter un paquet quand il ne peut pas le traiter, parce que ses files d'attente sont pleines, par exemple. Après tout, à l'impossible, nul n'est tenu, et les protocoles de transport et d'application savent à quoi s'attendre, et qu'ils devront peut-être gérer ces paquets perdus. Mais un routeur peut aussi jeter un paquet parce que des caractéristiques du paquet rendent impossible le traitement. Dans ce cas, il serait sympa de prévenir l'émetteur du paquet, pour qu'il puisse savoir que ses paquets, quoique légaux, ne peuvent pas être traités par certains routeurs. Notre nouveau RFC crée donc plusieurs nouveaux messages ICMP pour signaler à l'émetteur d'un paquet IPv6 qu'il en demande trop au routeur, par les en-têtes d'extension IPv6 qu'il ajoute.

La section 1 du RFC commence par lister les cas où un routeur peut légitimement jeter des paquets IPv6, même si les ressources matérielles du routeur ne sont pas épuisées :

— Voyons d'abord le cas des en-têtes d'extension pris individuellement. IPv6 permet d'ajouter aux paquets une chaîne d'en-têtes successifs (RFC 8200 [1], section 4). Ces en-têtes peuvent être de taille variable (c'est le cas de "*Destination Options*", qui peut contenir plusieurs options). Il n'y a pas de limite absolue à leur nombre, uniquement la contrainte qu'ils doivent tenir dans un datagramme, donc la taille de cette chaîne doit être inférieure à la MTU du chemin. Normalement, les routeurs ne regardent pas ces en-têtes (sauf "*Hop by Hop Options*") mais certains équipements réseau le font (cf. RFC 7045). Si, par exemple, l'équipement a, dans son code, une limite du genre « maximum 100 octets par en-tête et au plus trois options dans les en-têtes à options », alors, il jettera les paquets excédant ces limites. (S'il n'a pas de limites, cela peut augmenter sa vulnérabilité à certaines attaques par déni de service.)
— Il peut aussi y avoir une limite portant sur la taille totale de la chaîne, pour les mêmes raisons, et avec les mêmes conséquences.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8200.txt

— Dans certains cas, les routeurs qui jettent le paquet ont tort, mais cela ne change rien en pratique : comme ils vont continuer à le faire, autant qu'ils puissent signaler qu'ils l'ont fait, ce qui est le but de ce RFC.

La section 2 du RFC définit donc six nouveaux codes pour indiquer les problèmes, à utiliser avec le type ICMP 4 ("*Parameter Problem*", cf. RFC 4443, section 3.4). Petit rappel : les messages ICMP ont un **type** (ici, 4) et les messages d'erreur d'un même type sont différenciés par un **code** qui apporte des précisions. Ainsi, le type 1, "*Destination Unreachable*", peut servir par exemple pour des messages d'erreur ICMP de code 1 (filtrage par décision délibérée), 4 (port injoignable), etc. Les codes de notre RFC sont dans le registre IANA <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml#icmpv6-parameters-codes-5>. Les voici :

— 5, en-tête suivant inconnu ("*Unrecognized Next Header type encountered by intermediate node*") : normalement, les routeurs ne doivent pas rejeter les en-têtes inconnus, juste les passer tel quels mais, s'ils le font, qu'au moins ils l'indiquent, avec ce code. (On a vu que l'approche de ce RFC est pragmatique.)
— 6, en-tête trop gros ("*Extension header too big*").
— 7, chaîne d'en-têtes trop longue ("*Extension header chain too long*").
— 8, trop d'en-têtes ("*Too many extension headers*").
— 9, trop d'options dans un en-tête ("*Too many options in extension header*") : à envoyer si le nombre d'options dans, par exemple, l'en-tête "*Hop-by-hop options*", est trop élevé. Petit rappel : certains en-têtes ("*Destination Options*" et "*Hop-by-hop Options*") sont composites : ils comportent une liste d'une ou plusieurs options.
— 10, option trop grosse ("*Option too big*") : à envoyer si on rencontre une option de taille trop importante dans un en-tête comme "*Destination options*".

Et la section 3 définit un nouveau code pour le type d'erreur "*Destination Unreachable*", le code 8, en-têtes trop longs ("*Headers too long*"). Il a également été mis dans le registre IANA <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml#icmpv6-parameters-codes-2
Les messages utilisant ce code suivent le format du RFC 4884.

Et que fait-on quand on envoie ou reçoit des erreurs ICMP liées au traitement des en-têtes ? La section 4 du RFC rappelle les règles. D'abord, il faut évidemment suivre le RFC 4443, par exemple la limitation du rythme d'envoi des erreurs (RFC 4443, section 2.4f). Et, à la réception d'un message d'erreur ICMP, il est crucial de le valider (n'importe quelle machine sur l'Internet a pu générer ce message, en mentant sur son adresse IP source). Pour cela, on peut utiliser la portion du paquet original qui a été incluse dans le message d'erreur : il faut vérifier qu'elle correspond à une conversation en cours (connexion TCP existante, par exemple). Ensuite, il y a des règles spécifiques aux erreurs de ce RFC :

— On n'envoie qu'une erreur ICMP, même si plusieurs problèmes étaient survenus pendant le traitement d'un paquet (par exemple trop d'en-têtes **et** un total trop long). La section 4.1 donne la priorité à suivre pour savoir quelle erreur privilégier.
— À la réception, on peut ajuster son comportement en fonction de l'erreur signalée, par exemple envoyer moins d'en-têtes si l'erreur était le code 8, "*Too many extension headers*". Si les en-têtes IPv6 ont été gérés par l'application, il faut la prévenir, qu'elle puisse éventuellement changer son comportement. Et s'ils ont été ajouté par le noyau, c'est à celui-ci d'agir différemment.

La section 5 rappelle un point d'ICMP qu'il vaut mieux garder en tête. ICMP n'est **pas fiable**. Les messages d'erreur ICMP peuvent se perdre, soit, comme tout paquet IP, parce qu'un routeur n'arrivait pas à suivre le rythme, soit parce qu'une "*middlebox*" sur le trajet jette tous les paquets ICMP (une erreur de configuration fréquente quand les amateurs configurent un pare-feu cf. RFC 8504). Bref, il ne faut pas compter que vous recevrez forcément les messages indiqués dans ce RFC, si vos paquets avec en-têtes d'extension ne sont pas transmis.

La même section 5 explique les motivations pour ce RFC : on constate une tendance à augmenter le nombre et la taille des en-têtes d'extension IPv6. Cela peut être pour faire du routage influencé par la source, pour de l'OAM, ou pour d'autres innovations récentes.

Comme indiqué au début, cette augmentation peut se heurter aux limites des routeurs. La section 5.2.3 donne des exemples concrets. Les routeurs ne sont pas du pur logiciel, beaucoup de fonctions sont

mises dans du matériel spécialisé. Ainsi, les circuits de traitement des paquets peuvent ne pas avoir de notion de boucle. Pour traiter les en-têtes d'extension ou les options dans un en-tête, la solution évidente qu'est la boucle n'est pas disponible, et on fait donc un petit nombre de tests suivis d'un saut. Le nombre maximal de tests est donc limité.

Enfin, la section 6 de notre RFC discute des questions de sécurité. Il y a le problème du filtrage par les pare-feux (voir le RFC 4890) mais aussi le risque (assez lointain, je trouve) que l'observation de la génération de ces nouveaux messages d'erreur donnent des indications à un observateur sur le logiciel utilisé. C'est un problème commun à tous les choix optionnels. En tout cas, le RFC recommande que l'envoi de ces messages d'erreur soit configurable.

Actuellement, il ne semble pas qu'il existe déjà de mise en œuvre de ce RFC.