RFC 6935 : IPv6 and UDP Checksums for Tunneled Packets

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 mai 2013

Date de publication du RFC : Avril 2013

https://www.bortzmeyer.org/6935.html

Ne dites plus qu'en IPv6, la somme de contrôle est toujours obligatoire dans les en-têtes des paquets UDP. Depuis ce RFC 6935 [1], ce n'est plus vrai dans tous les cas. Lors de l'encapsulation de paquets dans un tunnel UDP, on a désormais le droit de ne pas mettre de somme de contrôle dans les paquets UDP, essentiellement pour des raisons de performance.

Le principal demandeur de cette modification était le protocole LISP (RFC 9300), qui dépend énormement de tunnels UDP. Même si le calcul de la somme de contrôle Internet est rapide (RFC 1071), comme ce calcul peut se faire des millions de fois par seconde pour un routeur très actif, on peut chercher à l'économiser. D'autant plus qu'il n'est pas forcément utile puisque, dans le cas d'un tunnel, le protocole qui circule dans le tunnel est déjà protégé par une somme de contrôle. À noter que d'autres protocoles que LISP (comme ceux utilisés pour le "*multicast*") peuvent bénéficier de cette nouvelle indulgence. Mais elle ne s'applique pas aveuglément à tout UDP (comme l'avaient proposé certains au début de la discussion), uniquement aux tunnels.

La norme actuelle sur IPv6, le RFC 2460, imposait (dans sa section 8.1) une somme de contrôle pour les paquets UDP (en IPv4, elle était facultative). En effet, IPv6 n'a pas de somme de contrôle dans la couche 3 (contrairement à son prédecesseur).

Ce RFC est un produit du groupe de travail IETF 6man <http://tools.ietf.org/wg/6man>, qui produit inlassablement d'innombrables RFC </search?pattern=6man> pour combler tous les petits problèmes qui trainent encore dans IPv6 et sont révélés par son utilisation dans le vrai monde.

Notez bien que cette dispense de somme de contrôle n'est pas générale : elle concerne les cas où il y a un tunnel et où il utilise UDP. Pourquoi UDP, alors qu'il existe des protocoles de tunnel qui s'en

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6935.txt

dispensent ? Parce que l'Internet est hélas de plus en plus ossifié, et que des "*middleboxes*" stupides et boguées sont partout sur le trajet des pauvres paquets. Les techniques de tunnel directement sur IP (comme l'excellent GRE du RFC 2784) sont souvent bloquées, alors qu'UDP passe partout. On aura donc un protocole X (LISP ou un autre) à l'intérieur du tunnel et de l'UDP à l'extérieur. Hier, cet UDP à l'extérieur était forcément protégé par une somme de contrôle. Pour un routeur qui sert de terminaison à des dizaines de milliers de tunnels (ce qui n'aurait rien d'étonnant avec LISP), calculer et vérifier ces sommes peut être très douloureux. D'autant plus que le protocole X a souvent sa propre somme de contrôle : ne serait-ce pas mieux pour tout le monde que le tunnel soit non sécurisé, ses éventuelles corruptions de paquets étant détectées par le protocole X uniquement ?

La section 4 discute plus en détail de certains aspects du problème mais il vaut mieux consulter le RFC 6936 pour tout savoir. Cet autre RFC précise notamment dans quels cas supprimer la somme de contrôle est une bonne idée et dans quels cas il vaut mieux la garder. La section 4 de notre RFC note particulièrement que les paquets de **contrôle** du tunnel, ceux qui servent à la signalisation, devraient rester protégés (s'ils sont corrompus, le tunnel peut cesser de fonctionner, c'est-à-dire que la corruption d'**un** paquet va affecter d'autres paquets). Notons que certains protocoles de tunnel comme GRE n'ont aucun mécanisme de contrôle. Lorsqu'il y en a un, il est souvent utilisé pour établir un contexte au début, avec choix des paramètres pour le tunnel : ce peut être le bon moment pour négocier le non-usage des sommes de contrôle sur les paquets de données.

Autre piège rigolo : certaines "*middleboxes*" vont tiquer en voyant les paquets UDP sans somme de contrôle (bien que, normalement, la somme de contrôle soit de bout en bout et ne regarde pas ces équipements intermédiaires). Bien que ce soit désormais légal, il va falloir attendre longtemps avant que tous ces engins soient mis à jour (section 4.3). En attendant ce jour, il est prudent que le tunnel détecte les problèmes en envoyant des paquets avec et sans somme de contrôle au début : si seuls les premiers passent, c'est qu'on a une "*middlebox*" agressive sur le trajet et qu'il faut renoncer à appliquer ce RFC 6935. Le test est d'ailleurs à répéter de temps en temps : la route peut changer et on peut donc se retrouver soudain à traverser une nouvelle "*middlebox*".

La section 4.1 conseille également de tenter de détecter la corruption avant de décapsuler, par exemple en examinant l'adresse IP source, pour minimiser le risque d'envoyer au protocole encapsulé un paquet reçu corrompu. Mais cette détection ne marchera pas à tous les cas (sinon, on pourrait supprimer les sommes de contrôle dans tous les cas) et le protocole encapsulé doit donc être robuste et réagit proprement lorsque ces paquets corrompus sont injectés dans un flux existant (section 4.2).

La section 5 contient la nouvelle norme pour les sommes de contrôle UDP. Elle remplace le texte du RFC 2460 (qui disait que la somme de contrôle UDP était toujours obligatoire en IPv6) par un texte plus nuancé : par **défaut**, la somme de contrôle **doit** être calculée et mise dans le paquet. Mais on **peut** s'en dispenser dans le cas de **tunnels** (et uniquement celui-ci), sur le paquet extérieur. Le protocole à l'intérieur du paquet (qui n'est pas forcément de l'UDP et même pas forcément de l'IPv6) doit rester protégé par sa propre somme de contrôle. Cela ne doit s'appliquer que pour une liste explicite de ports (ceux utilisés par le tunnel) et pas pour tout le trafic UDP de la machine. Et le tout doit se faire en lisant le RFC 6936 qui précise les conditions d'application de cette nouvelle règle.

Les curieux et les chercheurs en informatique noteront que la section 6 liste des points qui mériteraient davantage d'étude. Ainsi, il n'y a pas eu d'étude systématique de la corruption de paquets sur l'Internet depuis 2000 et personne ne sait donc trop si c'est un phénomène fréquent ou pas. Cette section note aussi qu'il existe en théorie une meilleure solution pour les tunnels, UDP Lite (RFC 3828), mais que sa probabilité de passer les "*middleboxes*" est plus faible que celle d'UDP.

Plusieurs des mises en œuvre de LISP envoient déjà des paquets UDP sans somme de contrôle (ou plus exactement avec une somme à zéro).