RFC 8300 : Network Service Header (NSH)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 janvier 2018

Date de publication du RFC : Janvier 2018

https://www.bortzmeyer.org/8300.html

Ce "*Network Service Header*" est un mécanisme concret pour faire passer sur le réseau les paquets destinés à une SF ("*Service Function*", voir RFC 7665 [1] pour l'architecture et les définitions). On colle un NSH, stockant plusieurs métadonnées, au paquet à traiter, on encapsule ce paquet à traiter et on l'envoie au dispositif de traitement via un réseau "*overlay*". Et on fait l'opération inverse au retour. L'encapsulation peut se faire dans IP (par exemple avec GRE) ou dans un autre protocole.

Les métadonnées mises dans le NSH sont le résultat d'un processus de classification où le réseau décide ce qu'on va faire au paquet. Par exemple, en cas de dDoS, le classificateur décide de faire passer tous les paquets ayant telle adresse source par un équipement de filtrage plus fin, et met donc cette décision dans le NSH (section 7.1). Le NSH contient les informations nécessaires pour le SFC ("*Service Function Chain*", RFC 7665). Sa lecture est donc très utile pour l'opérateur du réseau (elle contient la liste des traitements choisis, et cette liste peut permettre de déduire des informations sur le trafic en cours) et c'est donc une information plutôt sensible (voir aussi le RFC 8165).

Le NSH ne s'utilise qu'à l'intérieur de votre propre réseau (il n'offre, par défaut, aucune authentification et aucune confidentialité, voir section 8 du RFC). C'est à l'opérateur de prendre les mesures nécessaires, par exemple en chiffrant tout son trafic interne. Cette limitation à un seul domaine permet également de régler le problème de la fragmentation, si ennuyeux dès qu'on encapsule, ajoutant donc des octets. Au sein d'un même réseau, on peut contrôler tous les équipements et donc s'assurer que la MTU sera suffisante, ou, sinon, que la fragmentation se passera bien (section 5 du RFC).

Tout le projet SFC <https://datatracker.ietf.org/wg/sfc/about/> (dont c'est le troisième RFC) repose sur une vision de l'Internet comme étant un ensemble de "*middleboxes*" tripotant les paquets au passage, plutôt qu'étant un ensemble de machines terminales se parlant suivant le principe de bout en bout. C'est un point important à noter pour comprendre les débats au sein de l'IETF.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7665.txt