RFC 9287 : Greasing the QUIC bit

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 août 2022

Date de publication du RFC : Août 2022

https://www.bortzmeyer.org/9287.html

Dans un monde idéal, nos flux de données sur l'Internet passeraient sans problème et sans être maltraitées par les éléments intermédiaires du réseau. Mais dans le monde réel, de nombreuses "*middleboxes*" examinent le trafic et interfèrent avec lui. Les machines émettrices de trafic doivent donc se protéger et une des techniques les plus courantes est le chiffrement : si la "*middlebox*" ne peut pas comprendre ce qui est envoyé, elle ne pourra pas interférer. Le protocole de transport QUIC <https://www.bortzmeyer.org/quic.html> chiffre donc le plus possible. Mais une partie du trafic reste non chiffrée. Une des techniques pour empêcher que les "*middleboxes*" ne le lisent et ne prennent des décisions déplorables fondées sur ces informations transmises en clair est le **graissage** : on fait varier les données le plus possible. Ce RFC normalise une possibilité de graisser un bit de l'en-tête QUIC qui était fixe auparavant.

L'un des principes de conception de QUIC <https://www.bortzmeyer.org/quic.html> est de diminuer le plus possible la vue depuis le réseau (RFC 8546 [1]) ; les éléments intermédiaires, comme les routeurs ne doivent avoir accès qu'à ce qui leur est strictement nécessaire, le reste étant chiffré, pour leur éviter toute tentation. QUIC définit (dans le RFC 8999) des invariants, des informations qui seront toujours vraies même pour les futures versions de QUIC (le RFC 9000 définit QUIC version 1, pour l'instant la seule version). En dehors de ces invariants, tout peut...varier et les équipements intermédiaires du réseau ne doivent pas en tenir compte. Si tous suivaient ce principe, on préserverait la neutralité du réseau <https://www.bortzmeyer.org/neutralite.html>, et on éviterait l'ossification (cf. RFC 9170). Mais, en pratique, on sait que ce n'est pas le cas et que toute information visible depuis le réseau sera utilisée par les "*middleboxes*", ce qui peut rendre difficile les évolutions futures (TLS a par exemple beaucoup souffert de ce problème, d'où le RFC 8701, le premier à avoir formalisé ce concept de graissage).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8546.txt

Or, QUIC a un bit qui n'est pas cité dans les invariants du RFC 8999 mais qui est fixe et peur servir à différencier QUIC d'autres protocoles. On l'appele d'ailleurs souvent le « bit QUIC » (même si ça n'est pas son nom officiel, qui est "*fixed bit*", cf. RFC 9000, sections 17.2 et 17.3). Si les "*middleboxes*" s'en servent pour appliquer un traitement particulier à QUIC, les futures versions de QUIC ne pourront pas utiliser ce bit pour autre chose (rappelez-vous qu'il ne fait pas partie des invariants).

Notre RFC ajoute donc à QUIC une option pour graisser ce bit, c'est-à-dire pour le faire varier au hasard, décourageant ainsi les "*middleboxes*" d'en tenir compte. Un nouveau paramètre de transport QUIC (ces paramètres sont définis dans le RFC 9000, section 7.4) est créé, `grease_quic_bit` (et ajouté au registre IANA <https://www.iana.org/assignments/quic/quic.xml#quic-transport>). Lorsqu'il est annoncé à l'ouverture de la connexion QUIC, il indique que ce bit est ignoré et que le pair à tout intérêt à le faire varier.

Les paquets initiaux de la connexion (`Initial` et `Handshake`) doivent garder le bit QUIC à 1 (puisqu'on n'a pas encore les paramètres de la connexion), sauf si on reprend une ancienne connexion (en envoyant un jeton, cf. RFC 9000, section 19.7).

Tout le but de ce graissage est de permettre aux futures versions de QUIC (v2, 3, etc) d'utiliser ce bit qui était originellement fixe. Ces futures versions, ou tout simplement des extensions à QUIC négociées au démarrage de la connexion, pourront donc utiliser ce bit (lui donner une sémantique). Le RFC leur recommande d'annoncer quand même le paramètre `grease_quic_bit`, ce qui permettra de graisser même si la future extension n'est pas gérée par le partenaire.

Le RFC note enfin que ce graissage rend plus difficile d'identifier les flux de données QUIC au milieu de tout le trafic. C'est bien sûr le but, mais cela peut compliquer certains activités d'administration réseau. Un futur RFC <https://datatracker.ietf.org/doc/draft-ietf-quic-manageability/> explique plus en détail cette situation.

Apparemment, plusieurs mises en œuvre de QUIC gèrent déjà ce graissage.