

# RFC 6633 : Deprecation of ICMP Source Quench messages

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mai 2012

Date de publication du RFC : Mai 2012

<https://www.bortzmeyer.org/6633.html>

---

Il y avait belle lurette que les messages ICMP « Répression de la source » ("*Source Quench*") n'étaient plus utilisés. Ces messages devaient servir, à l'origine, à signaler à un émetteur qu'il exagérait et qu'il devrait ralentir l'envoi de données. Divers problèmes, notamment de sécurité, font que ces messages sont désormais ignorés par toutes les mises en œuvre de TCP/IP. Mais cet abandon de fait n'avait jamais été documenté. Voilà qui est fait, ce RFC 6633<sup>1</sup> marque donc l'abandon officiel de la répression de la source.

À l'origine, cette répression ("*quench*") avait été normalisée dans le RFC sur ICMP pour IPv4, le RFC 792. De type 4 et de code 0, le message "*Source Quench*" était censé limiter la congestion en disant à l'émetteur qu'un récepteur n'arrivait plus à suivre. Inefficace et injuste, le "*Source Quench*" n'a jamais été très utilisé. Les routeurs ont officiellement arrêté de s'en servir avec le RFC 1812, dès 1995. Ce RFC notait déjà les limites et problèmes du "*Source Quench*" (dans sa section 4.3.3.3, qui fournissait des références).

En outre, les messages "*Source Quench*", n'étant pas authentifiés, posaient un gros problème de sécurité : un méchant pouvait générer de faux messages pour réduire le débit de son ennemi, comme expliqué dans le RFC 5927 (et la section 8 de notre RFC). C'est d'ailleurs à cause de cela que des IDS comme Snort couinent lorsqu'ils voient passer des messages de répression de la source (voir Anderson, D., Fong, M., et A. Valdes, « "*Heterogeneous Sensor Correlation : A Case Study of Live Traffic Analysis*" », Proceedings of the 3rd Annual IEEE Information Assurance Workshop New York, NY, USA, 2002).

Restaient les protocoles de transport. Le RFC 1122 disait dans sa section 4.2.3.9 que les machines terminales **devaient** réagir aux "*Source Quench*" en diminuant le débit émis. La méthode recommandée pour TCP était de revenir au démarrage en douceur (RFC 5681).

De fait, le problème est réglé depuis longtemps, comme le documentait le RFC 5927 : les mises en œuvre de TCP et autres protocoles de transport ignorent les messages "*Source Quench*" depuis au moins 2005, RFC 1122 ou pas RFC 1122. L'annexe A de notre RFC 6633 fait le tour des implémentations TCP/IP et note que Linux a commencé à ignorer ces messages en 2004, FreeBSD, NetBSD et Solaris depuis 2005, etc. Voici par exemple ce que fait NetBSD (fichier `sys/netinet/tcp_subr.c`, routine `tcp_ctlinput()`) :

---

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc6633.txt>

```
if (cmd == PRC_QUENCH)
/*
 * Don't honor ICMP Source Quench messages meant for
 * TCP connections.
 */
return NULL;
```

Bref, ce RFC ne fait que documenter l'état des choses déjà existant.

En outre, ces messages "*Source Quench*" sont largement filtrés et ont donc peu de chances d'atteindre les machines qui émettent les données. Une étude de 1994 (Floyd, S., « "*TCP and Explicit Congestion Notification*" », ACM CCR Volume 24, Issue 5) notait déjà qu'on trouvait très peu de tels messages dans la nature. À la place, les routeurs sont censés utiliser ECN (RFC 3168) et (même si le RFC ne le rappelle pas), les machines terminales doivent de toute façon réagir aux pertes de paquets en ralentissant leur émission (RFC 5681).

Donc, le "*Source Quench*" est désormais officiellement abandonné. La section 3 de notre RFC modifie le RFC 1122 en demandant aux machines terminales de ne pas émettre de tels messages et d'ignorer ceux qu'elles recevraient. La section 4 fait de même pour les routeurs. La section 9 demande à l'IANA de marquer ces messages comme abandonnés dans le registre ICMP <<https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml#icmp-parameters-codes-4>>.

Il n'y avait pas de règle précise dans le passé pour d'autres protocoles de transport comme UDP ou SCTP. Les sections 5 et 6 de notre RFC leur applique la même règle : il faut ignorer complètement les messages de répression de la source qu'on pourrait recevoir.

Ah, et puis quelqu'un avait proposé une utilisation des messages "*Source Quench*" dans le RFC 1016. Suivant l'idée générale d'abandonner ces messages, la mise en œuvre de ce RFC est donc désormais déconseillée (cf. section 7).

De toute façon, le problème aurait disparu avec IPv4 : IPv6, lui, n'a jamais eu de message "*Source Quench*" (RFC 4443).