

RFC 2914 : Congestion Control Principles

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 septembre 2007

Date de publication du RFC : Septembre 2000

<https://www.bortzmeyer.org/2914.html>

L'Internet ne continue à fonctionner que parce que chaque machine qui y est connectée « fait attention », entre autre parce que les logiciels qui y sont installés essaient d'éviter de congestionner le réseau. Sur quels principes repose ce contrôle de la congestion ?

D'abord, ce contrôle de congestion n'est pas fait par IP (et donc pas par les routeurs) mais dans les protocoles au dessus, TCP étant le plus utilisé. Le contrôle de congestion est donc **de bout en bout** entre deux machines qui communiquent et n'est pas du ressort du réseau lui-même. Cela le rend très souple et très adapté à l'innovation mais cela met une lourde responsabilité sur chaque machine de l'Internet. Comme discuté dans la section 3.2 du RFC, une machine incivile qui voudrait s'allouer le maximum de bande passante peut le faire. Et, pour l'instant, il n'existe pas de protocoles IETF pour détecter ce comportement (certains travaux de recherche ont eu lieu sur ce sujet).

Le plus gros risque si le contrôle de congestion défaillait, risque décrit dans la section 3.1, ainsi que dans la section 5, est celui d'**effondrement** : dans un effondrement dû à la congestion, le débit diminue si on augmente le nombre de paquets. Le réseau passe alors tout son temps à tenter de transmettre des paquets qui seront finalement perdus, retransmis, le tout sans bénéfice pour personne. L'Internet est passé plusieurs fois près de l'effondrement (cf. RFC 896¹, qui était également le premier à pointer le danger des machines inciviles ou boguées, qui ne réagissent pas en cas de congestion) et seule l'amélioration continue des protocoles de transport a permis de continuer la croissance du trafic.

En effet, à partir de 1986, TCP a commencé, notamment sous l'impulsion de Van Jacobson, à prêter sérieusement attention à la congestion (voir le RFC 2001 pour une description "*a posteriori*" de cet effort), notamment via le mécanisme de **retraite**, où l'émetteur cherche s'il y a congestion et ralentit son débit si c'est le cas.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc896.txt>

Aujourd'hui, tout **flot** de données (un flot n'a pas de définition unique et rigoureuse, disons que c'est un ensemble de paquets appartenant au même échange de données, et gérés ensemble, pour ce qui concerne la congestion) doit mettre en œuvre des techniques de détection et de réponse à la congestion. Pour une application utilisant TCP, c'est fait automatiquement dans ce protocole mais une application utilisant UDP doit s'en charger elle-même. (D'autres RFC sont sortis depuis comme le RFC 5681 pour TCP.)

Outre l'effondrement, l'absence de contrôle de congestion présente un autre risque, qui fait l'objet de la section 3.2, le risque d'**injustice**. Si plusieurs flots se battent pour une bande passante limitée, le risque est que le mauvais citoyen, qui ne diminue pas son débit en cas de congestion, emporte une plus grosse part du gâteau que les autres. Une implémentation de TCP qui se comporterait ainsi pourrait même permettre à son vendeur de prétendre qu'il a un « TCP accéléré ». C'est une méthode analogue, mais au niveau applicatif, qu'avait utilisé le navigateur Web Netscape 1, en ouvrant plusieurs connexions TCP simultanées vers le même serveur HTTP.

La section 6 de notre RFC est ensuite dédiée aux démarches à adopter : avoir un contrôle de congestion est la principale. La section 9, en annexe, décrit plus spécifiquement les responsabilités de TCP. De nombreux RFC (par exemple le RFC 4907), référencent ce document, auquel tous les nouveaux protocoles doivent se conformer. Mais, en 2011, la question du contrôle de la congestion restait toujours largement ouverte, comme le montre le RFC 6077.