RFC 8517 : An Inventory of Transport-centric Functions Provided by Middleboxes: An Operator Perspective

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 mai 2019

Date de publication du RFC : Février 2019

https://www.bortzmeyer.org/8517.html

À l'IETF, ou, d'une manière générale, chez les gens qui défendent un réseau neutre <https://www.bortzmeyer.org/neutralite.html>, les boitiers intermédiaires, les "*middleboxes*", sont mal vus. Ces boitiers contrarient le modèle de bout en bout et empêchent souvent deux machines consentantes de communiquer comme elles le veulent. Des simples routeurs, OK, qui ne font que transmettre les paquets, mais pas de "*middleboxes*" s'arrogeant des fonctions supplémentaires. Au contraire, ce RFC écrit par des employés d'Orange, défend l'idée de "*middlebox*" et explique leurs avantages pour un opérateur. Ce n'est pas par hasard qu'il est publié alors que les discussions font toujours rage à l'IETF autour du protocole QUIC <https://www.bortzmeyer.org/quic.html>, qui obscurcira délibérement une partie de son fonctionnement, pour éviter ces interférences par les "*middleboxes*".

Le terme de "*middlebox*" est défini dans le RFC 3234 [1]. Au sens littéral, un routeur IP est une "*middlebox*" (il est situé entre les deux machines qui communiquent, et tout le trafic passe par lui) mais, en pratique, ce terme est utilisé uniquement pour les boitiers qui assurent des fonctions **en plus de la transmission de paquets IP**. Ces fonctions sont par exemple le pare-feu, la traduction d'adresses, la surveillance, etc. (Le RFC parle de "*advanced service functions*", ce qui est de la pure publicité.) Ces boitiers intermédiaires sont en général situés là où on peut observer et contrôler tout le trafic donc en général à la connexion d'un réseau local avec l'Internet, par exemple dans la "*box*" qu'imposent certains FAI, ou bien, dans les réseaux pour mobiles, là où le GGSN se connecte au PDN (RFC 6459, section 3.1.) Mais, parfois, ces boitiers sont en plein milieu du réseau de l'opérateur.

L'Internet suit normalement un modèle de bout en bout (RFC 1958.) Ce modèle dit que les équipements intermédiaires entre deux machines qui communiquent ne doivent faire que le strict minimum, laissant

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3234.txt

aux deux machines terminales <https://www.bortzmeyer.org/terminal-host.html> l'essentiel des fonctions. Cela assure la capacité de changement (il est plus facile de modifier les extrémités que le réseau), ainsi le Web a pu être déployé sans avoir besoin de demander la permission aux opérateurs, contrairement à ce qui se passe dans le monde des télécommunications traditionnelles. Et, politiquement, ce modèle de bout en bout permet la neutralité <https://www.bortzmeyer.org/neutralite.html> du réseau. Il n'est donc pas étonnant que les opérateurs de télécommunication traditionnels, dont les PDG ne ratent jamais une occasion de critiquer cette neutralité, n'aiment pas ce modèle. Truffer l'Internet de "*middleboxes*" de plus en plus intrusives est une tentative de revenir à un réseau de télécommunications comme avant, où tout était contrôlé par l'opérateur. Comme le RFC 8404, ce RFC est donc très politique.

Et, comme le RFC 8404, cela se manifeste par des affirmations outrageusement publicitaires, comme de prétendre que les opérateurs réseaux sont « les premiers appelés quand il y a un problème applicatif ». Faites l'expérience : si vlc a du mal à afficher une vidéo distante, appelez votre FAI et regardez si vous aurez réellement de l'aide...C'est pourtant ce que prétend ce RFC, qui affirme que l'opérateur veut accéder aux informations applicatives « pour aider ».

Le RFC note aussi que certaines des fonctions assurées par les boitiers intermédiaires ne sont pas réellement du choix de l'opérateur : contraintes légales (« boîtes noires » imposées par l'État) ou bien réalités de l'Internet (manque d'adresses IPv4 - cf. RFC 6269, fonctions liées aux attaques par déni de service, par exemple).

Les "*middleboxes*" travaillent parfois avec les informations de la couche 7 (ce qu'on nomme typiquement le DPI) mais le RFC se limite au travail sur les fonctions de la couche 4, une sorte de « DPI léger ».

Voyons maintenant ces utilisations des "*middleboxes*", et commençons par les mesures (section 2 du RFC), activité passive et qui ne modifie pas les paquets, donc n'entre pas forcément en conflit avec le principe de neutralité. Par exemple, mesurer le taux de perte de paquets (RFC 7680) est certainement quelque chose d'intéressant : s'il augmente, il peut indiquer un engorgement quelque part sur le trajet (pas forcément chez l'opérateur qui mesure). Chez l'opérateur, qui ne contrôle pas les machines terminales, on peut mesurer ce taux en observant les réémissions TCP (ce qui indique une perte en aval du point d'observation), les trous dans les numéros de séquence (ce qui indique une perte en amont), ou bien les options SACK (RFC 2018). Cela marche avec TCP, moins bien avec QUIC <https://www.bortzmeyer.org/quic.html>, où ces informations sont typiquement chiffrées. Comme l'observation des options ECN (RFC 3168), le taux de pertes permet de détecter la congestion.

Et le RTT (RFC 2681) ? Il donne accès à la latence <https://www.bortzmeyer.org/latence.html>, une information certainement intéressante. L'opérateur peut le mesurer par exemple en regardant le délai avant le passage d'un accusé de réception TCP. Plusieurs autres mesures sont possibles et utiles en étant « au milieu » et le RFC les détaille. Arrêtons-nous un moment sur celles liées à la sécurité : l'observation du réseau peut permettre de détecter certaines attaques, mais le RFC note (et déplore) que l'évolution des protocoles réseau tend à rendre cela plus difficile, puisque les protocoles annoncent de moins en moins d'information au réseau (en terme du RFC 8546, ils réduisent la vue depuis le réseau). Cela se fait par la diminution de l'entropie pour éviter le "*fingerprinting*" et par le chiffrement (cf. RFC 8404, qui critiquait déjà le chiffrement de ce point de vue). Évidemment, les utilisateurs diront que c'est fait exprès : on souhaite en effet réduire les possibilités de surveillance. Mais tout le monde n'a pas les mêmes intérêts.

Le RFC parle également des mesures effectuées au niveau applicatif. Ainsi, il note que les opérateurs peuvent tirer des conclusions de l'analyse des temps de réponse DNS.

Il y a bien sûr plein d'autres choses que les boitiers intermédiaires peuvent faire, à part mesurer. La section 3 du RFC les examine, et c'est le gros de ce RFC. L'une des plus connues est la traduction d'adresses. Celle-ci est souvent un grave obstacle sur le chemin des communications, malgré les recommandations (pas toujours suivies) des RFC 4787 et RFC 7857.

Après la traduction d'adresses, la fonction « pare-feu » est sans doute la plus connue des fonctions assurées par les "*middleboxes*". Par définition, elle est intrusive : il s'agit de bloquer des communications jugées non souhaitées, voire dangereuses. La question de fond est évidemment « qui décide de la politique du pare-feu ? » Du point de vue technique, le RFC note qu'il est très fréquent de différencier les communications initiées depuis l'intérieur de celles initiées depuis l'extérieur. Cela nécessite d'observer la totalité du trafic pour détecter, par exemple, quel paquet avait commencé la session.

Les autres fonctions des "*middleboxes*" citées par ce RFC sont moins connues. Il y a le « nettoyage <https://www.youtube.com/watch?v=GU7Tu0CJsGU> » ("*dDoS scrubbing*") qui consiste à classifier les paquets en fonction de s'ils font partie d'une attaque par déni de service ou pas, et de les jeter si c'est le cas (cf. par exemple RFC 8811). Le RFC explique que c'est une action positive, puisque personne (à part l'attaquant) n'a intérêt à ce que le réseau soit ralenti, voire rendu inutilisable, par une telle attaque. Le cas est compliqué, comme souvent en sécurité <https://www.bortzmeyer.org/jsecin-2018.html>. Bien sûr, personne ne va défendre l'idée que le principe de neutralité va jusqu'à laisser les attaques se dérouler tranquillement. Mais, d'un autre côté, **toutes** les classifications (un préalable indispensable au nettoyage) ont des faux positifs, et la sécurité peut donc avoir des conséquences néfastes (le RFC regrette que la protection de la vie privée a pour conséquence qu'il est plus difficile de reconnaitre les « paquets honnêtes »). La vraie question, ici comme ailleurs est « qui va décider ? ».

Autre utilisation, cette fois franchement problématique, l'identification implicite. Il s'agit d'identifier un utilisateur donné sans qu'il ait d'action explicite à faire, par exemple en ajoutant à ses requêtes HTTP un élément d'identification (comme expliqué dans un article fameux <https://www.bortzmeyer.org/enrichir-qui.html>) ou bien en jouant avec les options TCP (RFC 7974). Il s'agit là clairement de prise de contrôle par le boitier intermédiaire, qui se permet non seulement de modifier les données pendant qu'elles circulent, mais également prétend gérer l'identification des utilisateurs.

Autre fonction des boitiers intermédiaires, l'amélioration des performances en faisant assurer par ces "*middleboxes*" des fonctions qui étaient normalement assurées par les machines terminales, mais où l'opérateur estime qu'il est mieux placé pour le faire. Ces PEP ("*Performance-Enhancing Proxies*") sont notamment courants dans les réseaux pour mobiles (cf. RFC 3135, notamment sa section 2.1.1 ou bien cet exposé <https://datatracker.ietf.org/meeting/100/materials/slides-100-iccrg-mptcp-and-bbr-p
Cette fonction nécessite de pouvoir tripoter les en-têtes TCP.

Bien sûr, comme ce RFC exprime le point de vue des gros intermédiaires, il reprend l'élément de langage courant comme quoi il est nécessaire de prioriser certains types de trafic par rapport à d'autres. On aurait une voie rapide pour certains et des lentes pour les autres. Tout le monde est d'accord que la prioritisation est utile (la vidéo YouTube est moins importante que mon courrier professionnel) mais la question est encore « qui décide de ce qu'on priorise, et donc de ce qu'on ralentit ? » Ici, le RFC dit sans hésiter que c'est aux "*middleboxes*" de décider, après examen du trafic. L'exemple donné est amusant « on peut ainsi décider de donner la priorité aux jeux en ligne sur les mises à jour de logiciels ». Les gens de la sécurité, qui essaient toujours d'obtenir que les mises à jour de sécurité soient déployées plus rapidement, apprécieront…

On peut prioriser sans avoir accès à toutes les données (par exemple, en se basant uniquement sur les adresses IP) mais le RFC estime que, sans cet accès à tout, les décisions seront forcément moins efficaces.

Les auteurs du RFC sont manifestement conscients que beaucoup de leurs propositions vont énerver les utilisateurs. Alors, ils tentent de temps en temps d'expliquer que c'est pour leur bien qu'on viole la neutralité du réseau. Ainsi, le RFC cite l'exemple d'un réseau qui ralentirait le téléchargement d'une vidéo, pour épargner à l'abonné l'épuisement de son « forfait » « illimité ». Après tout, la vidéo ne sera peut-être pas regardée en entier, donc il n'est pas nécessaire de la charger tout de suite...

Voilà, nous sommes arrivés au bout de la liste des fonctions assurées par les boitiers intermédiaires (je ne les ai pas toutes citées dans ce court article). Il reste à voir les conséquences de ces fonctions pour la sécurité, et c'est le rôle de la section 5 du RFC. Elle estime d'abord que les fonctions décrites ne violent pas forcément la vie privée (RFC 6973) mais note quand même que même les champs « purement techniques » comme l'en-tête TCP, peuvent poser des risques pour la confidentialité des communications.

Et cette section 5 note aussi que l'information observée dans les en-têtes de couche 4 peuvent rendre certaines attaques plus faciles, par exemple en fabriquant un paquet TCP qui sera accepté par la machine terminale. On peut alors mener une attaque par déni de service en envoyant un faux RST (qui coupe la connexion, une attaque que les opérateurs ont déjà pratiquée <https://www.nextinpact.com/archive/39594-comcast-bittorrent-filtrage.htm>.) La solution citée est l'utilisation du RFC 5925, qui protège l'intégrité de la connexion TCP mais pas sa confidentialité...