RFC 3917 : Requirements for IP Flow Information Export (IPFIX)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 décembre 2006. Dernière mise à jour le 1 février 2008

Date de publication du RFC : Octobre 2004

https://www.bortzmeyer.org/3917.html

Depuis longtemps, les opérateurs des réseaux ont besoin de récolter des informations agrégées sur le trafic que voient passer leurs routeurs. IPFIX, dont le cahier des charges figure dans ce RFC, sera le protocole IETF pour cela.

Compter chaque paquet IP est clairement irréaliste. Cela reproduirait le problème de X.25 où les routeurs passaient plus de temps à faire de la facturation qu'à faire circuler les paquets. Il faut donc agréger en **flots**. Un flot est un ensemble de paquets, qui partagent des caractéristiques communes par exemple, appartenance à la même connexion TCP. Le protocole Netflow, de Cisco (décrit dans le RFC 3954 [1]), a été le premier à avoir la possibilité de compter par flot et non plus par paquets, et aussi le premier à formaliser la différence entre l'**observateur**, qui voit les flots et produit l'information agrégée, et le **récolteur** qui reçoit ces chiffres et les traite. Il existe aujourd'hui une offre logicielle abondante pour récolter et traiter les flots Netflow. IPFIX sera un descendant direct de Netflow.

Notre RFC met donc par écrit le cahier des charges du nouveau protocole : le modèle de données, la terminologie, ... Il précise quelles catactéristique on peut utiliser pour définir un flot. Une liste des données minimales que IPFIX doit permettre de transmettre est aussi donnée (adresses IP, numéros de port, nombre de paquets transmis, etc).

Une part importante est consacrée aux questions de sécurité : les flots contiennent typiquement des informations assez sensibles et qui ne doivent pas être révélées.

Les RFC normalisant IPFIX sont aujourd'hui tous finis, le RFC 5470 sur l'architecture, le RFC 5472 sur les considérations générales d'applicabilité, le RFC 5101 sur le protocole, le RFC 5102 sur le modèle de données, le RFC 5471 sur les tests du protocole et le RFC 5153 sur les détails d'implémentation ont été publiés. Ils ont été remplacés en septembre 2013 par une seconde série, avec le RFC 7011 sur le protocole et le RFC 7012 sur le modèle de données.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3954.txt