RFC 5102 : Information Model for IP Flow Information Export

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 février 2008

Date de publication du RFC : Janvier 2008

https://www.bortzmeyer.org/5102.html

Le protocole IPFIX d'envoi par un routeur de résumés statistiques sur le trafic qu'il voit passer (RFC 5101 [1], depuis remplacé par le RFC 7011), dépend d'un modèle de données, que décrivait notre RFC (depuis remplacé par le RFC 7012).

Le RFC 5101 qui normalisait le protocole IPFIX indique **comment** transporter les données de l'**exporteur** (typiquement un routeur) vers le **récolteur** (typiquement la machine d'administration du réseau) mais n'indique pas **quelles** données sont transportées. Notre RFC va jouer ce rôle, équivalent à celui du SMI du RFC 2578 pour SNMP.

Notre RFC est très long mais il est surtout composé d'une longue liste (section 5) des informations qui peuvent être transmises en IPFIX. En fait, il est assez simple. Un élément d'information a un nom (par exemple `destinationTransportPort`), une description (cet élément indique le port de destination du flot), un type (ici `unsigned16`, nombre entier sur 16 bits) et d'autres informations utiles comme un "*ElementID*" qui identifie de manière unique un élément d'information. Les types sont décrits en détail dans la section 3 mais sont très classiques (entiers, booléens, adresses MAC, etc). Plus originaux sont les sémantiques de la section 3.2, qui précisent, par exemple, que les éléments ayant une sémantique de `totalCounter` repartent de zéro lorsqu'ils ont atteint leur valeur maximale.

Voici un exemple complet, tiré de la section 5.10.4 :

```
octetTotalCount
   Description:
      The total number of octets in incoming packets for this Flow at
      the Observation Point since the Metering Process
      (re-)initialization for this Observation Point.  The number of
      octets include IP header(s) and IP payload.
   Abstract Data Type: unsigned64
   Data Type Semantics: totalCounter
   ElementId: 85
   Status: current
   Units: octets
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5101.txt`