RFC 7012 : Information Model for IP Flow Information eXport (IPFIX)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 septembre 2013

Date de publication du RFC : Unknown month 2013 September

https://www.bortzmeyer.org/7012.html

Le protocole IPFIX d'envoi par un routeur de résumés statistiques sur le trafic qu'il voit passer (RFC 7011 [1]), dépend d'un modèle de données, que décrit notre RFC, qui remplace l'ancien RFC 5102.

Le RFC 7011 qui normalise 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 assez simple (son prédécesseur, le RFC 5102 était très long, mais c'est parce qu'il intégrait la liste des éléments d'information disponibles, elle est désormais dans un registre IANA). 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 de différentes factures, booléens, adresses MAC, chaînes de caractères en Unicode, etc). Plus originaux sont les sémantiques de la section 3.2. Si les éléments ont par défaut la sémantique `quantity` (ils affichent la valeur actuellement mesurée), d'autres sont différents, par exemple en indiquant un total (sémantique d'odomètre). Ainsi, les éléments ayant une sémantique de `totalCounter` repartent de zéro lorsqu'ils ont atteint leur valeur maximale. Ceux ayant la sémantique `identifier` ne sont pas des nombres (même quand leur valeur est numérique, comme les numéros d'AS) et ne doivent donc pas être additionnés.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7011.txt`

Voici un exemple complet, tiré du registre <https://www.iana.org/assignments/ipfix/ipfix.xhtml>. Certains champs sont obligatoires, comme le nom, la description, le type (ici un entier non signé de 64 bits) ou l'ElementID (qui peut être un nombre simple attribué par l'IANA, pour les éléments « officiels » comme le 85 montré ici, ou bien complété par un numéro d'organisation pour les autres). D'autres sont facultatifs comme l'unité (ici, des octets ; une erreur dans les unités a déjà entraîné la perte d'une sonde spatiale). Le nom suit parfois des conventions de nommage (section 2.3). Par exemple, les éléments dont le nom commence par post identifient une mesure faite **après** un traitement par une "*middlebox*", par exemple une traduction d'adresse. Voici l'élément octetTotalCount :

```
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
```

Le vrai format source du registre (regardez <https://www.iana.org/assignments/ipfix/ipfix.xml> depuis autre chose qu'un navigateur Web) est XML (section 7.3), avec un schéma en Relax NG. La définition ci-dessus est en fait :

```
<record>
<name>octetTotalCount</name>
<dataType>unsigned64</dataType>
<group>flowCounter</group>
<dataTypeSemantics>totalCounter</dataTypeSemantics>
<elementId>85</elementId>
<applicability>all</applicability>
<status>current</status>
<description>
<paragraph>
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 includes IP header(s) and IP payload.
</paragraph>
</description>
<units>octets</units>
<xref type="rfc" data="rfc5102"/>
<revision>0</revision>
<date>2013-02-18</date>
</record>
```

Les éléments dans le registre IANA sont décrits en XML car cela permet de produire automatiquement du code ou des fichiers de configuration à partir du registre. Mais le protocole IPFIX lui-même n'utilise pas du tout XML.

Les changements depuis le RFC 5102 sont décrits en section 1.1. Le principal est que la liste des éléments d'information, au lieu d'être listée dans le RFC, est désormais dans un registre IANA <https://www.iana.org/assignments/ipfix/ipfix.xml>. D'autre part, le mécanisme pour modifier cette liste a été légèrement changé (section 7.4). Il est décrit en détail dans le RFC 7013. En gros, pour ajouter un nouvel élément d'information, il faut un examen par un expert (le RFC 5226 décrit toutes ces procédures).