

Groupe de travail Réseau
Request for Comments : 5477
 Catégorie : sur la voie de la normalisation

T. Dietz, NEC Europe Ltd.
 B. Claise, Cisco Systems, Inc. Catégorie :
 P. Aitken, Cisco Systems, Inc.
 F. Dressler, University of Erlangen-Nuremberg
 G. Carle, Technical University of Munich
 mars 2009

Traduction Claude Brière de L'Isle

Modèle d'information pour les exportations d'échantillons de paquets

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de droits de reproduction

Copyright (c) 2009 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

Le présent document peut contenir des matériaux provenant de documents de l'IETF ou de contributions à l'IETF publiées ou rendues disponibles au public avant le 10 novembre 2008. La ou les personnes qui ont le contrôle des droits de reproduction sur tout ou partie de ces matériaux peuvent n'avoir pas accordé à l'IETF Trust le droit de permettre des modifications de ces matériaux en dehors du processus de normalisation de l'IETF. Sans l'obtention d'une licence adéquate de la part de la ou des personnes qui ont le contrôle des droits de reproduction de ces matériaux, le présent document ne peut pas être modifié en dehors du processus de normalisation de l'IETF, et des travaux dérivés ne peuvent pas être créés en dehors du processus de normalisation de l'IETF, excepté pour le formater en vue de sa publication comme RFC ou pour le traduire dans une autre langue que l'anglais.

Résumé

Le présent mémoire définit un modèle d'information pour le protocole d'échantillonnage de paquets (PSAMP, *Packet SAMPling*). Il est utilisé par le protocole PSAMP pour coder les données de paquets échantillonnés et les informations relatives au processus d'échantillonnage. Comme le protocole PSAMP se fonde sur le protocole d'exportation d'informations de flux IP (IPFIX, *IP Flow Information eXport*) ce modèle d'information est une extension du modèle d'information IPFIX.

Table des matières

1. Introduction.....	2
2. Vue d'ensemble des documents PSAMP.....	2
3. Terminologie.....	3
3.1 Conventions utilisées dans le document.....	3
4. Relations entre PSAMP et IPFIX.....	3
5. Propriétés d'un élément d'information PSAMP.....	3
6. Espace de type.....	3
7. Surcharge des éléments d'information.....	3
8. Éléments d'information PSAMP.....	4
8.1 Identifiants (301-303).....	4
8.2 Configuration d'échantillonnage (304-311).....	5
8.3 Configuration de hachage (326-334).....	8
8.4 Horodatages (322-325).....	9
8.5 Données de paquet (313-314, 316-317).....	10
8.6 Statistiques (318-321, 336-338).....	12

9. Considérations sur la sécurité.....	14
10. Considérations relatives à l'IANA.....	14
10.1 Considérations en rapport.....	14
10.2 Considérations relatives à PSAMP.....	14
11. Références.....	15
11.1 Références normatives.....	15
11.2 Références pour information.....	15
Appendice A. Spécification formelle des éléments d'information PSAMP.....	15
Adresse des auteurs.....	25

1. Introduction

Des techniques d'échantillonnage de paquet sont nécessaires pour divers scénarios de mesures. Le protocole d'échantillonnage de paquet (PSAMP) fournit des mécanismes pour la sélection de paquets en utilisant différentes techniques de filtrage et d'échantillonnage. Une façon normalisée pour l'exportation et la mémorisation des éléments d'information définis à la Section 8 est requise. La définition du modèle d'information et de données de PSAMP se fonde sur le modèle d'information IPFIX [RFC5102]. Le document du protocole PSAMP [RFC5476] spécifie comment utiliser le protocole IPFIX dans le contexte de PSAMP.

Le présent document examine le modèle d'information IPFIX [RFC5102] et l'étend pour satisfaire les exigences de PSAMP. Donc, la structure de ce document est fortement fondée sur le document IPFIX. Il complète la spécification du protocole PSAMP en fournissant un modèle d'information PSAMP approprié. La partie principale de ce document, la Section 8, définit la liste des éléments d'information à transmettre par le protocole PSAMP. Les sections 5 et 6 décrivent les types de données et les propriétés d'éléments d'information utilisés dans le présent document et leurs relations avec le modèle d'information IPFIX.

Bien que le mandat du groupe de travail PSAMP ne spécifie pas d'exigences pour les erreurs de mesure de paquet (comme les abandons, les mals formés, etc.) et que le présent document ne traite pas de telles données, si il y a un besoin de collecte et d'exportation des informations sur les erreurs de paquet, les éléments d'information appropriés peuvent être demandés à l'IANA, et exportés avec le protocole PSAMP.

Le corps principal de la Section 8 a été généré à partir d'un document XML. La spécification fondée sur XML des éléments d'information PSAMP peut être utilisée pour vérifier automatiquement la correction syntaxique de la spécification. De plus, il peut être utilisé -- en combinaison avec le modèle d'information IPFIX -- pour automatiser la génération de code. Le code résultant peut être utilisé dans les mises en œuvre du protocole PSAMP pour le traitement des éléments d'information PSAMP.

Pour cette raison, le document XML qui a servi de source à la Section 8 est attaché au présent document à l'Appendice A.

Noter que bien que partiellement généré à partir des documents XML rattachés, le corps principal de ce document est normatif tandis que l'appendice est pour information.

2. Vue d'ensemble des documents PSAMP

Le présent document fait partie d'une série de documents du groupe PSAMP.

[RFC5474] : "Cadre de travail pour la sélection et le rapport de paquet" décrit le cadre de PSAMP pour que les éléments de réseau choisissent des sous ensembles de paquets par des méthodes statistiques et autres, et pour exporter un flux de rapports sur les paquets choisis à un collecteur.

RFC 5475 : "Techniques d'échantillonnage et de filtrage pour la sélection de paquets IP" décrit l'ensemble de techniques de sélection de paquets prise en charge par PSAMP.

[RFC5476] : "Spécification du protocole d'échantillonnage de paquet (PSAMP)" spécifie l'exportation des informations de paquet d'un processus d'exportation PSAMP à un processus de collecte PSAMP.

[RFC5477] (ce document) : "Modèle d'information pour l'exportation d'échantillonnage de paquet" définit un modèle

d'information et de données pour PSAMP.

3. Terminologie

La terminologie spécifique de IPFIX utilisée dans ce document est définie à la Section 2 de la [RFC5101]. La terminologie spécifique de PSAMP utilisée dans ce document est définie au paragraphe 3.2 de la [RFC5476]. Dans ce document, comme dans les [RFC5101] et [RFC5476] (*dans la seule version anglaise*) la première lettre de chaque terme spécifique de IPFIX et de PSAMP est en majuscule.

3.1 Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

4. Relations entre PSAMP et IPFIX

Comme décrit dans le protocole PSAMP [RFC5476], un rapport PSAMP peut être vu comme un enregistrement de données IPFIX très particulier. Il représente un flux IPFIX contenant un seul paquet. Donc, le modèle d'information IPFIX peut être utilisé comme base pour les rapports PSAMP.

Néanmoins, il y a des propriétés exigées dans les rapports PSAMP qui ne peuvent pas être modélisées en utilisant le modèle d'information IPFIX actuel. Le présent document décrit les extensions au modèle d'information IPFIX qui permettent la modélisation des informations et données requises par PSAMP.

Certaines de ces extensions permettent l'exportation de ce qui peut être considéré comme des informations sensibles. Se référer à la section des considérations sur la sécurité pour une discussion plus poussée.

Noter que l'exportation de rapports PSAMP d'échantillonnage ou de filtrage peut n'avoir pas besoin de tous les éléments d'information définis par le modèle d'information IPFIX [RFC5102], comme discuté aux paragraphes 6.2 et 6.3 du cadre PSAMP [RFC5474].

5. Propriétés d'un élément d'information PSAMP

Les éléments d'information PSAMP sont définis conformément aux paragraphes 2.1 à 2.3 du modèle d'information IPFIX [RFC5102] auxquels une référence devrait être faite pour plus d'informations. Néanmoins, on recommande fortement de définir la propriété facultative "unité" pour chaque élément d'information (si c'est applicable).

Les types Data définis au paragraphe 3.1 du modèle d'information IPFIX [RFC5102] sont aussi utilisés pour les éléments d'information PSAMP.

6. Espace de type

Les éléments d'information PSAMP DOIVENT être construits à partir des types de données abstraits de base et de la sémantique de type de données décrits à la Section 3 du modèle d'information IPFIX [RFC5102]. Pour assurer la cohérence entre IPFIX et PSAMP, les types de données ne sont pas répétés dans ce document. Le codage de ces types de données est décrit dans le protocole IPFIX [RFC5101].

7. Surcharge des éléments d'information

Les éléments d'information NE DEVRAIENT PAS être surchargés avec plusieurs significations ou ré-utilisés pour

plusieurs objets. Des éléments d'information différents DEVRAIENT être alloués pour chaque exigence.

Bien que la présence de certains autres éléments d'information permette de déduire la méthode de choix, un élément d'information séparé est fourni pour le selectorAlgorithm pour l'inclure comme portée pour l'interprétation de rapport de sélecteur [RFC5476].

Même si les éléments d'information sont spécifiés avec une méthode de choix spécifique (c'est-à-dire, une valeur spécifique de selectorAlgorithm) ces éléments d'information ne sont pas restreints à la méthode de choix et PEUVENT être utilisés à l'avenir pour des méthodes de choix différentes.

8. Éléments d'information PSAMP

Cette section décrit les éléments d'information utilisés par le protocole PSAMP.

Pour chaque élément d'information spécifié dans les paragraphes 8.1 à 8.6 ci-dessous, un identifiant univoque est alloué en accord avec la Section 4 du modèle d'information IPFIX [RFC5102]. Les allocations sont contrôlées par l'IANA comme une extension au modèle d'information IPFIX.

Les éléments d'information spécifiés par le modèle d'information IPFIX [RFC5102] sont utilisés par le protocole PSAMP lorsque applicables. Pour éviter des incohérences entre les modèles d'information et de données IPFIX et PSAMP, seuls les éléments d'information qui ne sont pas déjà décrits par le modèle d'information IPFIX sont définis ici.

Voici la liste des éléments d'information PSAMP supplémentaires :

Identifiant	Nom	Identifiant	Nom
301	selectionSequenceId	321	relativeError
302	selectorId	322	observationTimeSeconds
303	informationElementId	323	observationTimeMilliseconds
304	selectorAlgorithm	324	observationTimeMicroseconds
305	samplingPacketInterval	325	observationTimeNanoseconds
306	samplingPacketSpace	326	digestHashValue
307	samplingTimeInterval	327	hashIPPayloadOffset
308	samplingTimeSpace	328	hashIPPayloadSize
309	samplingSize	329	hashOutputRangeMin
310	samplingPopulation	330	hashOutputRangeMax
311	samplingProbability	331	hashSelectedRangeMin
313	ipHeaderPacketSection	332	hashSelectedRangeMax
314	ipPayloadPacketSection	333	hashDigestOutput
316	mplsLabelStackSection	334	hashInitialiserValue
317	mplsPayloadPacketSection	336	upperCILimit
318	selectorIdTotalPktsObserved	337	lowerCILimit
319	selectorIdTotalPktsSelected	338	confidenceLevel
320	absoluteError		

8.1 Identifiants (301-303)

Les éléments d'information de ce paragraphe servent d'identifiants. Tous ont un type de données abstrait entier et une sémantique de type de données de "identifier".

Identifiant	Nom
301	selectionSequenceId
302	selectorId
303	informationElementId

8.1.1 selectionSequenceId

Description : à partir de tous les paquets observés à un point d'observation, un sous ensemble des paquets est choisi par une séquence d'un ou plusieurs sélecteurs. Le selectionSequenceId est une valeur unique par domaine

d'observation, spécifiant le point d'observation et la séquence de sélecteurs à travers laquelle les paquets sont choisis.

Type de données abstrait : unsigned64
Sémantique du type de données : identifiant
ElementId : 301
Statut : courant

8.1.2 selectorId

Description : l'identifiant de sélecteur est l'identifiant unique qui identifie un sélecteur primaire. Chaque sélecteur primaire doit avoir un identifiant unique dans le domaine d'observation.

Type de données abstrait : unsigned16
Sémantique du type de données : identifiant
ElementId : 302
Statut : courant

8.1.3 informationElementId

Description : cet élément d'information contient l'identifiant d'un autre élément d'information.

Type de données abstrait : unsigned16
Sémantique du type de données : identifiant
ElementId: 303
Statut : courant

8.2 Configuration d'échantillonnage (304-311)

Les éléments d'information de ce paragraphe peuvent être utilisés pour décrire la configuration d'échantillonnage d'un processus de choix.

Identifiant	Nom	Identifiant	Nom
304	selectorAlgorithm	308	samplingTimeSpace
305	samplingPacketInterval	309	samplingSize
306	samplingPacketSpace	310	samplingPopulation
307	samplingTimeInterval	311	samplingProbability

8.2.1 selectorAlgorithm

Description : Cet élément d'information identifie les méthodes de choix de paquet (par exemple, filtrage, échantillonnage) qui sont appliquées par le processus de choix. La plupart de ces méthodes ont des paramètres. D'autres éléments d'information sont nécessaires pour spécifier pleinement le choix de paquet avec ces méthodes et tous leurs paramètres. Les méthodes mentionnées ci-dessous sont définies dans la [RFC5475]. Pour leurs paramètres, les éléments d'information sont définis dans le document de modèle d'information. Les noms de ces éléments d'information sont mentionnés pour chaque identifiant de méthode. D'autres identifiants de méthode peuvent être ajoutés à cette liste.

Il pourrait être nécessaire de définir de nouveaux éléments d'information pour spécifier leurs paramètres. Le registre selectorAlgorithm est tenu par l'IANA. Les nouvelles allocations dans le registre seront administrées par l'IANA et sont soumises à revue d'expert [RFC5226]. Le registre peut être mis à jour quand des spécifications de la ou les nouvelles méthodes et tous nouveaux éléments d'information sont fournis. Le groupe d'experts doit faire une double vérification des définitions de selectorAlgorithm et des éléments d'information avec les selectorAlgorithm et éléments d'information déjà définis quant à leur complétude, précision, et redondance. Ces experts vont initialement être pris parmi les présidents du groupe de travail et les éditeurs de document des groupes IPFIX et PSAMP.

Les identifiants de méthodes de choix de paquet suivants sont définis ici :

Identifiant	Méthode	Paramètres
1	échantillonnage systématique fondé sur le compte	samplingPacketInterval, samplingPacketSpace
2	échantillonnage systématique fondé sur le temps	samplingTimeInterval, samplingTimeSpace
3	échantillonnage aléatoire de n parmi N	samplingSize, samplingPopulation
4	échantillonnage probabiliste uniforme	samplingProbability
5	filtrage sur la correspondance de propriété	pas d' accord sur les paramètres
Filtrage fondé sur le hachage		hashInitialiserValue, hashIPPayloadOffset,
6	utilisant BOB	hashIPPayloadSize, hashSelectedRangeMin,
7	utilisant IPSX	hashSelectedRangeMax, hashOutputRangeMin,
8	utilisant CRC	hashOutputRangeMax

Il y a un grand nombre de paramètres possibles qui pourraient être utilisés pour le filtrage sur la correspondance de propriété (5) mais il n'y a actuellement pas d'accord sur les paramètres à spécifier.

Type de données abstrait : unsigned16
 Sémantique du type de données : identifiant
 ElementId : 304
 Statut : courant

8.2.2 samplingPacketInterval

Description : Cet élément d'information spécifie le nombre de paquets qui sont échantillonnés consécutivement. Une valeur de 100 signifie que 100 paquets consécutifs sont échantillonnés. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le compte.

Type de données abstrait : unsigned32
 Sémantique du type de données : quantité
 ElementId : 305
 Statut : courant
 Unité : paquets

8.2.3 samplingPacketSpace

Description : Cet élément d'information spécifie le nombre de paquets entre deux "samplingPacketInterval". Une valeur de 100 signifie que le prochain intervalle commence 100 paquets (qui ne seront pas échantillonnés) après que le "samplingPacketInterval" actuel sera terminé. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le compte.

Type de données abstrait : unsigned32
 Sémantique du type de données : quantité
 ElementId : 306
 Statut : courant
 Unité : paquets

8.2.4 samplingTimeInterval

Description : cet élément d'information spécifie en microsecondes l'intervalle de temps durant lequel tous les paquets arrivants sont échantillonnés. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le temps.

Type de données abstrait : unsigned32
 Sémantique du type de données : quantité
 ElementId : 307
 Statut : courant
 Unité: microseconde

8.2.5 **samplingTimeSpace**

Description : cet élément d'information spécifie en microsecondes l'intervalle de temps entre deux "samplingTimeInterval". Une valeur de 100 signifie que le prochain intervalle commence 100 microsecondes (durant lesquelles aucun paquet ne sera échantillonné) après que le "samplingTimeInterval" en cours est terminé. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le temps.

Type de données abstrait : unsigned32
 Sémantique du type de données : quantité
 ElementId : 308
 Statut : courant
 Unité : microseconde

8.2.6 **samplingSize**

Description : Cet élément d'information spécifie le nombre d'éléments pris dans la population parente pour les méthodes d'échantillonnage aléatoires. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage aléatoire de n parmi N.

Type de données abstrait : unsigned32
 Sémantique du type de données : quantité
 ElementId : 309
 Statut : courant
 Unité : paquets

8.2.7 **samplingPopulation**

Description : cet élément d'information spécifie le nombre d'éléments dans la population parente pour les méthodes d'échantillonnage aléatoire. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage aléatoire de n parmi N.

Type de données abstrait : unsigned32
 Sémantique du type de données : quantité
 ElementId : 310
 Statut : courant
 Unité : paquets

8.2.8 **samplingProbability**

Description : cet élément d'information spécifie la probabilité qu'un paquet soit échantillonné, exprimée comme une valeur entre 0 et 1. La probabilité est égale pour chaque paquet. Une valeur de 0 signifie qu'aucun paquet n'a été échantillonné car la probabilité est 0. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage probabiliste uniforme.

Type de données abstrait : float64
 Sémantique du type de données : quantité
 ElementId : 311
 Statut : courant

8.3 **Configuration de hachage (326-334)**

Les éléments d'information suivants peuvent être utilisés pour décrire la configuration d'échantillonnage d'un processus de sélection. Les paramètres individuels sont expliqués plus en détails aux paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Identifiant	Nom	Identifiant	Nom
326	digestHashValue	331	hashSelectedRangeMin
327	hashIPPayloadOffset	332	hashSelectedRangeMax
328	hashIPPayloadSize	333	hashDigestOutput

329	hashOutputRangeMin	334	hashInitialiserValue
330	hashOutputRangeMax		

8.3.1 digestHashValue

Description : cet élément d'information spécifie la valeur provenant de la fonction de hachage de résumé. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
Sémantique du type de données : quantité
ElementId : 326
Statut : courant

8.3.2 hashIPPayloadOffset

Description : cet élément d'information spécifie le décalage de la charge utile IP utilisée par un sélecteur de choix fondé sur le hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
Sémantique du type de données : quantité
ElementId : 327
Statut : courant

8.3.3 hashIPPayloadSize

Description : cet élément d'information spécifie la charge utile IP utilisée par une sélecteur de choix fondé sur le hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
Sémantique du type de données : quantité
ElementId : 328
Statut : courant

8.3.4 hashOutputRangeMin

Description : cet élément d'information spécifie la valeur du début de la gamme de résultats potentiels d'une fonction de hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
Sémantique du type de données : quantité
ElementId : 329
Statut : courant

8.3.5 hashOutputRangeMax

Description : cet élément d'information spécifie la valeur de la fin de la gamme de résultats potentiels d'une fonction de hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
Sémantique du type de données : quantité
ElementId : 330
Statut : courant

8.3.6 hashSelectedRangeMin

Description : cet élément d'information spécifie la valeur du début de la gamme de choix d'une fonction de hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
 Sémantique du type de données : quantité
 ElementId : 331
 Statut : courant

8.3.7 hashSelectedRangeMax

Description : cet élément d'information spécifie la valeur de la fin de la gamme de choix d'une fonction de hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
 Sémantique du type de données : quantité
 ElementId : 332
 Statut : courant

8.3.8 hashDigestOutput

Description : cet élément d'information contient une valeur booléenne qui est VRAIE si le résultat de ce sélecteur de hachage a été configuré à être inclus dans le rapport de paquet comme résumé de paquet, autrement elle est FAUSSE. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : booléen
 Sémantique du type de données : quantité
 ElementId : 333
 Statut : courant

8.3.9 hashInitialiserValue

Description : cet élément d'information spécifie la valeur d'initialisation de la fonction de hachage. Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].

Type de données abstrait : unsigned64
 Sémantique du type de données : quantité
 ElementId : 334
 Statut : courant

8.4 Horodatages (322-325)

Les éléments d'information mentionnés ci-dessous contiennent des horodatages. Ils peuvent être utilisés pour rapporter l'heure d'observation d'un seul paquet.

Identifiant	Nom	Identifiant	Nom
322	observationTimeSeconds	324	observationTimeMicroseconds
323	observationTimeMilliseconds	325	observationTimeNanoseconds

8.4.1 observationTimeSeconds

Description : cet élément d'information spécifie en secondes le temps absolu d'une observation.

Type de données abstrait : dateTimeSeconds
 Sémantique du type de données : quantité
 ElementId : 322
 Statut : courant
 Unité : secondes

8.4.2 **observationTimeMilliseconds**

Description : cet élément d'information spécifie en millisecondes le temps absolu d'une observation.

Type de données abstrait : `dateTimeMilliseconds`

Sémantique du type de données : quantité

ElementId : 323

Statut : courant

Unité : millisecondes

8.4.3 **observationTimeMicroseconds**

Description : cet élément d'information spécifie en microsecondes le temps absolu d'une observation.

Type de données abstrait : `dateTimeMicroseconds`

Sémantique du type de données : quantité

ElementId : 324

Statut : courant

Unité : microsecondes

8.4.4 **observationTimeNanoseconds**

Description : Cet élément d'information spécifie en nanosecondes le temps absolu d'une observation.

Type de données abstrait : `dateTimeNanoseconds`

Sémantique du type de données : quantité

ElementId : 325

Statut : courant

Unité : nanoseconde

8.5 **Données de paquet (313-314, 316-317)**

Les éléments d'information suivants sont tous utilisés pour rapporter le contenu brut d'un paquet. Tous les éléments d'information contenant des sections du paquet observé peuvent aussi être utilisés dans IPFIX [RFC5101]. Si les valeurs pour ces sections varient pour les différents paquets d'un flux, alors le rapport de flux va contenir la valeur observée dans le premier paquet du flux.

Identifiant	Nom	Identifiant	Nom
313	<code>ipHeaderPacketSection</code>	316	<code>mplsLabelStackSection</code>
314	<code>ipPayloadPacketSection</code>	317	<code>mplsPayloadPacketSection</code>

8.5.1 **ipHeaderPacketSection**

Description : cet élément d'information, qui peut avoir une longueur variable, porte une série d'octets depuis le début de l'en-tête IP d'un paquet échantillonné. Avec une longueur suffisante, cet élément rapporte aussi les octets de la charge utile IP, sous réserve de la [RFC2804]. Voir la section des considérations sur la sécurité. La taille de la section exportée peut être contrainte par des limitations du protocole IPFIX. Les données de ce champ NE DOIVENT PAS avoir de bourrage.

Type de données abstrait : `octetArray`

ElementId : 313

Statut : courant

8.5.2 **ipPayloadPacketSection**

Description : cet élément d'information, qui peut avoir une longueur variable, porte une série d'octets provenant du début de la charge utile IP d'un paquet échantillonné. La charge utile IPv4 est la partie du paquet qui suit l'en-tête IPv4 et toute option, à laquelle la [RFC0791] se réfère comme les "données" ou les "octets de données". Voir les

exemples à l'Appendice A de la [RFC0791]. La charge utile IPv6 est le reste du paquet qui suit les 40 octets de l'en-tête IPv6. Noter que tous les en-tête d'extension présents sont considérés faire partie de la charge utile. Voir la spécification IPv6 dans la [RFC2460]. La taille de la section exportée peut être contrainte par des limitations du protocole IPFIX. Les données de ce champ NE DOIVENT PAS avoir de bourrage.

Type de données abstrait : octetArray

ElementId : 314

Statut : courant

8.5.3 mplsLabelStackSection

Description : cet élément d'information, qui peut avoir une longueur variable, porte les n premiers octets de la pile d'étiquettes MPLS d'un paquet échantillonné. Avec une longueur suffisante, cet élément rapporte aussi les octets provenant de la charge utile MPLS, sous réserve de la [RFC2804]. Voir la section des considérations sur la sécurité. Voir la [RFC3031] pour la spécification des paquets MPLS. Voir la [RFC3032] pour la spécification de la pile d'étiquettes MPLS. La taille de la section exportée peut être contrainte par des limitations du protocole IPFIX. Les données de ce champ NE DOIVENT PAS avoir de bourrage.

Type de données abstrait : octetArray

ElementId : 316

Statut : courant

8.5.4 mplsPayloadPacketSection

Description : cet élément d'information, qui peut avoir une longueur variable, porte les n premiers octets de la charge utile MPLS d'un paquet échantillonné, qui sont les données suivant immédiatement la pile d'étiquettes MPLS. Voir la [RFC3031] pour la spécification des paquets MPLS. Voir la [RFC3032] pour la spécification de la pile d'étiquettes MPLS. La taille de la section exportée peut être contrainte par des limitations du protocole IPFIX. Les données de ce champ NE DOIVENT PAS avoir de bourrage.

Type de données abstrait : octetArray

ElementId : 317

Statut : courant

8.6 Statistiques (318-321, 336-338)

Les éléments d'information dans cette section peuvent être utilisés pour rapporter des statistiques provenant du processus de mesure.

Identifiant	Nom	Identifiant	Nom
318	selectorIdTotalPktsObserved	336	upperCILimit
319	selectorIdTotalPktsSelected	337	lowerCILimit
320	absoluteError	338	confidenceLevel
321	relativeError		

8.6.1 selectorIdTotalPktsObserved

Description : cet élément d'information spécifie le nombre total de paquets observés par un sélecteur, pour une valeur spécifique de SelectorId. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].

Type de données abstrait : unsigned64

Sémantique du type de données : totalCounter

ElementId : 318

Statut : courant

Unité : paquets

8.6.2 selectorIdTotalPktsSelected

Description : cet élément d'information spécifie le nombre total de paquets choisis par un sélecteur, pour une valeur spécifique du SelectorId. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].

Type de données abstrait : unsigned64

Sémantique du type de données : totalCounter

ElementId : 319

Statut : courant

Unité : paquets

8.6.3 absoluteError

Description : cet élément d'information spécifie l'erreur de mesure maximum possible de la valeur rapportée pour un élément d'information donné. "absoluteError" a la même unité que l'élément d'information auquel il est associé. La valeur réelle de la métrique peut différer de absoluteError (positive ou négative) de la valeur mesurée. Cet élément d'information donne seulement l'erreur pour les valeurs mesurées. Si un élément d'information contient une valeur estimée (provenant de l'échantillonnage) les limites de confiance et le niveau de confiance doivent être fournis à la place, en utilisant les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].

Type de données abstrait : float64

Sémantique du type de données : quantité

ElementId : 320

Statut : courant

Unité : unités de l'élément d'information pour lequel l'erreur est spécifiée.

8.6.4 relativeError

Description : cet élément d'information spécifie le ratio d'erreur maximum possible positive ou négative pour la valeur rapportée pour un élément d'information donné comme un pourcentage de la valeur mesurée. La valeur réelle de la métrique peut différer de relativeError pourcent (positif ou négatif) de la valeur mesurée. Cet élément d'information donne seulement l'erreur pour les valeurs mesurées. Si un élément d'information contient une valeur estimée (à partir de l'échantillonnage) les limites de confiance et le niveau de confiance doivent être fournis à la place, en utilisant les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].

Type de données abstrait : float64

Sémantique du type de données : quantité

ElementId : 321

Statut : courant

8.6.5 upperCILimit

Description : cet élément d'information spécifie la limite supérieure d'un intervalle de confiance. Il est utilisé pour fournir une déclaration de précision pour une valeur estimée. Les limites de confiance définissent la gamme dans laquelle la valeur réelle est supposée être avec une certaine probabilité p. Les limites de confiance doivent toujours être associées à un niveau de confiance qui définit cette probabilité p. On notera qu'un intervalle de confiance donne seulement une probabilité que la valeur réelle soit dans ces limites. Cela signifie que la valeur réelle peut être en-dehors des limites de confiance. Les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel devraient tous être utilisés dans un gabarit d'options dont la portée est l'observation à laquelle ils se réfèrent. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101]. Noter qu'il est exigé que upperCILimit, lowerCILimit, et confidenceLevel spécifient tous la confiance, et ils ne devraient être pris en compte que si ils sont tous trois spécifiés.

Type de données abstrait : float64
Sémantique du type de données : quantité
ElementId : 336
Statut : courant

8.6.6 lowerCILimit

Description : cet élément d'information spécifie la limite inférieure d'un intervalle de confiance. Pour plus d'informations, voir la description de upperCILimit. Les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel devraient tous être utilisés dans un gabarit d'options dont la portée est l'observation à laquelle ils se réfèrent. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101]. Noter qu'il est exigé de upperCILimit, lowerCILimit, et confidenceLevel qu'ils spécifient tous la confiance, et ils ne devraient être pris en compte que si ils sont tous trois spécifiés.

Type de données abstrait : float64
Sémantique du type de données : quantité
ElementId : 337
Statut : courant

8.6.7 confidenceLevel

Description : cet élément d'information spécifie le niveau de confiance. Il est utilisé pour fournir une déclaration sur la précision des valeurs estimées. Le niveau de confiance donne la probabilité p avec laquelle la valeur réelle se tient dans une gamme donnée. Un niveau de confiance doit toujours être associé aux limites de confiance qui définissent la gamme dans laquelle la valeur réelle est supposée être. Les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel devraient tous être utilisés dans un gabarit d'options dont la portée est l'observation à laquelle ils se réfèrent. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101]. Noter qu'il est exigé de upperCILimit, lowerCILimit, et confidenceLevel qu'ils spécifient tous la confiance, et ils ne devraient être pris en compte que si ils sont tous trois spécifiés.

Type de données abstrait : float64
Sémantique du type de données : quantité
ElementId : 338
Statut : courant

9. Considérations sur la sécurité

Le modèle d'information PSAMP n'introduit pas directement par lui-même de problème de sécurité. Il définit plutôt un ensemble d'attributs qui peuvent être considérés pour des questions de vie privée ou d'affaires comme des informations sensibles.

Par exemple, exporter les valeur des champs d'en-tête peut rendre des attaques possible pour le receveur de ces informations, qui ne seraient autrement possibles que pour des observateurs directs des flux rapportés le long du chemin des données. Précisément, les éléments d'information relevant des sections du paquet DOIVENT cibler pas plus que l'en-tête du paquet, quelques octets suivants du paquet, et les en-têtes encapsulants si il en est de présent. La capture complète de paquet du flux de paquet est explicitement hors du champ de ce document, conformément à la [RFC2804].

Le protocole sous-jacent utilisé pour échanger les informations décrites ici DOIT donc appliquer les procédures appropriées pour garantir l'intégrité et la confidentialité des informations exportées. De telles procédures sont définies dans des documents séparés, spécifiquement le document de protocole IPFIX [RFC5101].

10. Considérations relatives à l'IANA

Le modèle d'information PSAMP, comme décrit dans le présent document, a deux ensembles de numéros alloués. Les considérations sur leur allocation sont discutées dans cette section, en utilisant les exemples de politiques décrits dans le

document "Lignes directrices pour la rédaction d'une section de considérations relatives à l'IANA" [RFC5226].

10.1 Considérations en rapport

Comme le protocole PSAMP utilise le protocole IPFIX, se référer à la section des considérations relatives à l'IANA de la [RFC5102] pour les allocations de numéros utilisés dans le protocole et pour les numéros utilisés dans le modèle d'information.

10.2 Considérations relatives à PSAMP

Le présent document spécifie un ensemble initial d'éléments d'information PSAMP satisfaisant les besoins spécifiés dans la [RFC5475], comme une extension aux éléments d'information IPFIX [RFC5102].

Noter que les identifiants d'élément d'information PSAMP débutaient initialement à la valeur de 301, afin de laisser de la place pour tout travail en cours sur IPFIX exigeant de nouveaux éléments d'information. On suppose que ce trou dans la numérotation d'élément d'information va être comblé par l'IANA avec de nouveaux éléments d'information IPFIX.

Chaque nouvelle méthode de sélection DOIT recevoir une valeur unique dans le registre selectorAlgorithm. Ses paramètres de configuration, avec la façon de les rapporter avec un gabarit d'options, DOIVENT être clairement spécifiés. Le contenu initial du registre selectorAlgorithm se trouve au paragraphe 8.2.1.

Les nouvelles allocations pour la méthode de sélection PSAMP vont être administrées par l'IANA et sont soumises à une revue par expert [RFC5226]. Le groupe d'experts doit faire une double vérification des définitions d'éléments d'information avec les éléments d'information déjà définis quant à leur complétude, précision, et redondance. Ces experts vont initialement être pris parmi les présidents du groupe de travail et les éditeurs de document des groupes de travail IPFIX et PSAMP. Le registre selectorAlgorithm est tenu par l'IANA et peut être mis à jour lorsque des spécifications de nouvelles méthodes et tous nouveaux éléments d'information sont fournis.

11. Références

11.1 Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, (MàJ par [RFC8174](#))
- [RFC5101] B. Claise, éd., "[Spécification du protocole d'exportation d'informations](#) de flux IP (IPFIX) pour l'échange d'informations de flux de trafic IP", janvier 2008. (P.S.) (Obsolète, voir [RFC7011](#), STD77)
- [RFC5102] J. Quittek et autres, "Modèle d'informations pour l'exportation d'informations de flux IP", janvier 2008. (P.S.) (Remplacée par [RFC7012](#))
- [RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (Remplace [RFC2434](#) ; remplacée par [RFC8126](#))
- [RFC5475] T. Zseby et autres, "[Techniques d'échantillonnage](#) et de filtrage pour sélection de paquet IP", mars 2009. (P.S.)
- [RFC5476] B. Claise et autres "Spécification du [protocole d'échantillonnage de paquet](#) (PSAMP)", mars 2009. (P.S.)

11.2 Références pour information

- [RFC0791] J. Postel, éd., "Protocole Internet - Spécification du [protocole du programme Internet](#)", STD 5, septembre 1981.
- [RFC2460] S. Deering et R. Hinden, "Spécification du [protocole Internet, version 6](#) (IPv6)", décembre 1998. (MàJ par [5095](#), [6564](#) ; D.S ; Remplacée par [RFC8200](#), STD 86)

- [RFC2629] M. Rose, "Écrire des I-D et des RFC en utilisant XML", juin 1999. (*Information ; Remplacée par RFC7749*)
- [RFC2804] IAB, IESG, "[Politique de l'IETF en matière d'écoutes](#)", mai 2000. (*Information*)
- [RFC3031] E. Rosen, A. Viswanathan, R. Callon, "Architecture de [commutation d'étiquettes multi protocoles](#)", janvier 2001. (*P.S.*) (*MàJ par la RFC6790*)
- [RFC3032] E. Rosen et autres, "[Codage de pile d'étiquettes MPLS](#)", janvier 2001. (*Info. ; MàJ par RFC9017*)
- [RFC5474] N. Duffield et autres, "[Cadre de travail pour la sélection](#) et le rapport de paquet", mars 2009. (*Information*)

Appendice A. Spécification formelle des éléments d'information PSAMP

Le présent appendice contient une description formelle du document XML de modèle d'information PSAMP. Noter que cet appendice est de nature informative, tandis que le texte de la Section 8 généré à partir de cet appendice est normatif.

Utiliser une syntaxe formelle et lisible par la machine pour le modèle d'information permet la création d'outils à capacité PSAMP qui peuvent adapter automatiquement les extensions au modèle d'information, en lisant simplement les mises à jour des spécifications du modèle d'information.

La large disponibilité d'outils et bibliothèques à capacité XML pour les appareils clients est la principale considération de ce choix. En particulier, les bibliothèques pour l'analyse des documents XML sont directement disponibles. Aussi, des mécanismes comme le langage extensible de feuille de style (XSL, *Extensible Stylesheet Language*) permettent de transformer un document source XML en d'autres documents. Ce projet a été rédigé en XML et transformé en accord avec la [RFC2629].

On devrait noter que l'utilisation de XML dans les exportateurs, collecteurs, ou autres outils n'est pas obligatoire pour le déploiement de PSAMP. En particulier, les processus d'exportation ne produisent ni ne consomment XML au titre de leur fonctionnement. On s'attend à ce que les collecteurs PSAMP PUISSENT tirer parti de la lisibilité du modèle d'information par la machine plutôt que de coder leur comportement ou d'inventer des moyens propriétaires pour traiter les extensions.

```
<?xml version="1.0" codage="UTF-8"?>
```

```
<!--
```

Ce document XML est un produit du groupe de travail IPFIX de l'IETF.

Contact : mandat du groupe de travail : <http://www.ietf.org/html.charters/ipfix-charter.html>

Listes de diffusion :

Discussion générale : ipfix@ietf.org

Pour s'abonner : <http://www1.ietf.org/mailman/listinfo/ipfix>

Archive : <http://www1.ietf.org/mail-archive/web/ipfix/current/index.html>

Éditeur :

Thomas Dietz

NEC Europe Ltd.

NEC Laboratories Europe

Network Research Division

Kurfuersten-Anlage 36

Heidelberg 69115

Germany

téléphone : +49 6221 4342-128

mél : Thomas.Dietz@nw.neclab.eu

Benoit Claise

Cisco Systems, Inc.

De Kleetlaan 6a b1

Degem 1813

Belgium

téléphone : +32 2 704 5622

mél : bclaise@cisco.com

Paul Aitken
Cisco Systems, Inc.
96 Commercial Quay
Edinburgh EH6 6LX
Scotland
téléphone : +44 131 561 3616
mél : paitken@cisco.com
URI: <http://www.cisco.com>

Falko Dressler
University of Erlangen-Nuremberg
Dept. of Computer Sciences
Martensstr. 3
Erlangen 91058
Germany
téléphone : +49 9131 85-27914
mél : dressler@informatik.uni-erlangen.de
URI: <http://www7.informatik.uni-erlangen.de/~dressler>

Georg Carle
Technical University of Munich
Institute for Informatics
Boltzmannstr. 3
Garching bei Muenchen 85737
Germany
téléphone : +49 89 289-18030
mél : carle@in.tum.de
URI : <http://www.net.in.tum.de/~carle/>

Résumé :

Le présent mémoire définit un modèle d'information pour le protocole d'échantillonnage de paquet (PSAMP, *Packet SAMPLing*). Il est utilisé par le protocole PSAMP pour coder les données et informations de paquet échantillonné relatives au processus d'échantillonnage. Comme le protocole PSAMP est fondé sur le protocole IPFIX, ce modèle d'information est une extension du modèle d'information IPFIX.

Copyright (c) 2009 IETF Trust et les personnes identifiées comme auteurs du code. Tous droits réservés.

La redistribution et l'usage en formes source et binaire, avec ou sans modification, sont permis pourvu que les conditions suivantes soient satisfaites :

- La redistribution du code source doit conserver la notice de droits de reproduction ci-dessus, cette liste de conditions et le déclinatoire de responsabilité suivant.
- La redistribution en forme binaire doit reproduire la notice de droits de reproduction ci-dessus, cette liste de conditions et le déclinatoire de responsabilité dans la documentation et/ou autres matériaux fournis avec la distribution.
- Ni le nom de la Internet Society, IETF ou IETF Trust, ni les noms des contributeurs spécifiques, ne peuvent être utilisés pour endosser ou promouvoir des produits dérivés de ce logiciel sans une permission écrite spécifique préalable.

Le présent logiciel est fourni par les détenteurs du droit de reproduction et les contributeurs "tel quel" et toutes garanties expresses ou implicites, incluant, mais sans s'y limiter, la garantie implicite de mise sur le marché et de convenance pour un objet particulier sont déclinées. En aucun cas le détenteur du droit de reproduction ou contributeurs ne sera responsable de dommages directs, indirects, incidents, spéciaux, exemplaires, ou conséquents (incluant, mais sans s'y limiter, la fourniture de biens ou services de substitution, perte d'usage, données, ou profits, ou interruption d'affaires) cependant causées et sur toute théorie de responsabilité, contractuelle, responsabilité stricte, ou tort (incluant par négligence ou autrement) survenant d'une façon ou d'une autre de l'utilisation de ce logiciel, même si il est avisé de la possibilité d'un tel dommage.

Cette version du document XML fait partie de la RFC 5477 ; voir la RFC elle-même pour les notices légales complètes.

-->

```
<fieldDefinitions xmlns="urn:ietf:params:xml:ns:ipfix-info"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:ipfix-infoipfix-info.xsd">
```

```
<field name="selectionSequenceId" dataType="unsigned64"
dataTypeSemantics="identifiant" elementId="301" status="current" group="identifiants">
<description>
<paragraph>
À partir de tous les paquets observés à un point d'observation, un sous ensemble des paquets est choisi par une séquence
d'un ou plusieurs sélecteurs. Le selectionSequenceId est une valeur unique par domaine d'observation, spécifiant le point
d'observation et la séquence de sélecteurs à travers laquelle les paquets sont choisis.
</paragraph>
</description>
</field>
```

```
<field name="selectorId" dataType="unsigned16"
dataTypeSemantics="identifiant" elementId="302" status="current"
group="identifiants">
<description>
<paragraph>
L'identifiant de sélecteur est l'identifiant unique qui identifie un sélecteur primaire. Chaque sélecteur primaire doit avoir
un identifiant unique dans le domaine d'observation.
</paragraph>
</description>
</field>
```

```
<field name="informationElementId" dataType="unsigned16"
dataTypeSemantics="identifiant" elementId="303" status="current"
group="identifiants">
<description>
<paragraph>
Cet élément d'information contient l'identifiant d'un autre élément d'information.
</paragraph>
</description>
</field>
```

```
<field name="selectorAlgorithm" dataType="unsigned16"
dataTypeSemantics="identifiant" elementId="304" status="current"
group="sampling configuration">
<description>
<paragraph>
Cet élément d'information identifie les méthodes de choix de paquet (par exemple, filtrage, échantillonnage) qui sont
appliquées par le processus de choix.
```

La plupart de ces méthodes ont des paramètres. D'autres éléments d'information sont nécessaires pour spécifier complètement le choix de paquet avec ces méthodes et tous leurs paramètres.

Les méthodes mentionnées ci-dessous sont définies dans la [RFC5475]. Pour leurs paramètres, les éléments d'information sont définis dans le document de modèle d'information. Les noms de ces éléments d'information sont mentionnés pour chaque identifiant de méthode.

D'autres identifiants de méthode peuvent être ajoutés à la liste ci-dessous. Il pourrait être nécessaire de définir de nouveaux éléments d'information pour spécifier leurs paramètres.

Le registre selectorAlgorithm est tenu par l'IANA. Les nouvelles allocations dans le registre seront administrées par l'IANA et sont soumises à revue d'expert [RFC5226].

Le registre peut être mis à jour quand des spécifications de nouvelles méthodes et tous nouveaux éléments d'information sont fournis.

Le groupe d'experts doit faire une double vérification des définitions et éléments d'information de selectorAlgorithm avec les selectorAlgorithm et éléments d'information déjà définis quant à leur complétude, précision, et redondance. Ces experts vont initialement être pris parmi les présidents du groupe de travail et éditeurs de document des groupes de travail IPFIX et PSAMP.

Les identifiants de méthodes de choix de paquet suivantes sont définies ici :

Identifiant	Méthode	Paramètres
1	échantillonnage systématique fondé sur le compte	samplingPacketInterval, samplingPacketSpace
2	échantillonnage systématique fondé sur le temps	samplingTimeInterval, samplingTimeSpace
3	échantillonnage aléatoire de n parmi N	samplingSize, samplingPopulation
4	échantillonnage probabiliste uniforme	samplingProbability
5	filtrage sur la correspondance de propriété	pas d' accord sur les paramètres
Filtrage fondé sur le hachage		hashInitialiserValue, hashIPPayloadOffset,
6	utilisant BOB	hashIPPayloadSize, hashSelectedRangeMin,
7	utilisant IPSX	hashSelectedRangeMax, hashOutputRangeMin,
8	utilisant CRC	hashOutputRangeMax

Il y a une grande diversité de paramètres possibles qui pourraient être utilisés pour le filtrage sur la correspondance de propriété (5), mais il n'y a actuellement pas d'accord sur les paramètres à spécifier.

```
</paragraph>
</description>
</field>
```

```
<field name="samplingPacketInterval" dataType="unsigned32"
dataTypeSemantics="quantity" elementId="305" status="current"
group="sampling configuration">
<description>
<paragraph>
Cet élément d'information spécifie le nombre de paquets qui sont consécutivement échantillonnés. Une valeur de 100 signifie que 100 paquets consécutifs sont échantillonnés. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le compte.
</paragraph>
</description>
<units>packets</units>
</field>
```

```
<field name="samplingPacketSpace" dataType="unsigned32"
dataTypeSemantics="quantity" elementId="306" status="current"
group="sampling configuration">
<description>
<paragraph>
Cet élément d'information spécifie le nombre de paquets entre deux "samplingPacketInterval". Une valeur de 100 signifie que le prochain intervalle commence 100 paquets (qui ne sont pas échantillonnés) après que le "samplingPacketInterval" en cours est terminé. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le compte.
</paragraph>
</description>
<units>packets</units>
</field>
```

```
<field name="samplingTimeInterval" dataType="unsigned32"
dataTypeSemantics="quantity" elementId="307" status="current"
group="sampling configuration">
<description>
<paragraph>
Cet élément d'information spécifie l'intervalle de temps en microsecondes durant lequel tous les paquets arrivants sont échantillonnés. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le temps.
</paragraph>
</description>
<units>microseconds</units>
</field>
```

```
<field name="samplingTimeSpace" dataType="unsigned32"
dataTypeSemantics="quantity" elementId="308" status="current"
group="sampling configuration">
```

```

<description>
  <paragraph>
    Cet élément d'information spécifie l'intervalle de temps en microsecondes entre deux "samplingTimeInterval". Une
    valeur de 100 signifie que le prochain intervalle débute 100 microsecondes (durant lesquelles aucun paquet n'est
    échantillonné) après que le "samplingTimeInterval" en cours est terminé. Par exemple, cet élément d'information peut
    être utilisé pour décrire la configuration d'un sélecteur d'échantillonnage systématique fondé sur le temps.
  </paragraph>
</description>
<units>microseconds</units>
</field>

```

```

field name="samplingSize" dataType="unsigned32"
  dataTypeSemantics="quantity" elementId="309" status="current"
  group="sampling configuration">
  <description>
    <paragraph>
      Cet élément d'information spécifie le nombre d'éléments pris dans la population parente pour des méthodes
      d'échantillonnage aléatoires. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un
      sélecteur d'échantillonnage aléatoire de n parmi N.
    </paragraph>
  </description>
  <units>packets</units>
</field>

```

```

<field name="samplingPopulation" dataType="unsigned32"
  dataTypeSemantics="quantity" elementId="310" status="current"
  group="sampling configuration">
  <description>
    <paragraph>
      Cet élément d'information spécifie le nombre d'éléments dans la population parente pour les méthodes d'échantillonnage
      aléatoires. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur
      d'échantillonnage aléatoire de n parmi N.
    </paragraph>
  </description>
  <units>packets</units>
</field>

```

```

<field name="samplingProbability" dataType="float64"
  dataTypeSemantics="quantity" elementId="311" status="current"
  group="sampling configuration">
  <description>
    <paragraph>
      Cet élément d'information spécifie la probabilité qu'un paquet soit échantillonné, exprimée par une valeur entre 0 et 1. La
      probabilité est égale pour chaque paquet. Une valeur de 0 signifie qu'aucun paquet n'a été échantillonné car la probabilité
      est 0. Par exemple, cet élément d'information peut être utilisé pour décrire la configuration d'un sélecteur
      d'échantillonnage probabiliste uniforme.
    </paragraph>
  </description>
</field>

```

```

<field name="ipHeaderPacketSection" dataType="octetArray"
  elementId="313" status="current" group="packet data">
  <description>
    <paragraph>
      Cet élément d'information, qui peut avoir une longueur variable, porte une série d'octets depuis le début de l'en-tête IP
      d'un paquet échantillonné. Avec une longueur suffisante, cet élément rapporte aussi les octets de la charge utile IP, sous
      réserve de la [RFC2804]. Voir la section des considérations sur la sécurité. La taille de la section exportée peut être
      contrainte par les limitations du protocole IPFIX. Les données de ce champ NE DOIVENT PAS avoir de bourrage.
    </paragraph>
  </description>
</field>

```

```
<field name="ipPayloadPacketSection" dataType="octetArray"
elementId="314" status="current" group="packet data">
<description>
<paragraph>
Cet élément d'information, qui peut avoir une longueur variable, porte une série d'octets depuis le début de la charge utile
IP d'un paquet échantillonné. La charge utile IPv4 est la partie du paquet qui suit l'en-tête IPv4 et toutes les options,
auxquelles la [RFC0791] se réfère comme des "données" ou "octets de données". Par exemple, voir les exemples de la
[RFC0791], Appendice A. La charge utile IPv6 est le reste du paquet qui suit les 40 octets de l'en-tête IPv6. Noter que
tous les en-têtes d'extension présents sont considérés faire partie de la charge utile. Voir la [RFC2460] pour la
spécification de IPv6. La taille de la section exportée peut être contrainte par des limitations du protocole IPFIX. Les
données de ce champ NE DOIVENT PAS avoir de bourrage.
</paragraph>
</description>
</field>
```

```
<field name="mplsLabelStackSection" dataType="octetArray"
elementId="316" status="current" group="packet data">
<description>
<paragraph>
Cet élément d'information, qui peut avoir une longueur variable, porte les n premiers octets de la pile d'étiquettes MPLS
d'un paquet échantillonné. Avec une longueur suffisante, cet élément rapporte aussi les octets provenant de la charge
utile MPLS, sous réserve de la [RFC2804]. Voir la section des considérations sur la sécurité. Voir la [RFC3031] pour la
spécification des paquets MPLS. Voir la [RFC3032] pour la spécification de la pile d'étiquettes MPLS. La taille de la
section exportée peut être contrainte par des limitations du protocole IPFIX. Les données de ce champ NE DOIVENT
PAS avoir de bourrage.
</paragraph>
</description>
</field>
```

```
<field name="mplsPayloadPacketSection" dataType="octetArray"
elementId="317" status="current" group="packet data">
<description>
<paragraph>
Cet élément d'information, qui peut avoir une longueur variable, porte les n premiers octets de la charge utile MPLS d'un
paquet échantillonné, qui sont les données suivant immédiatement la pile d'étiquettes MPLS. Voir la [RFC3031] pour la
spécification des paquets MPLS. Voir la [RFC3032] pour la spécification de la pile d'étiquettes MPLS. La taille de la
section exportée peut être contrainte par des limitations du protocole IPFIX. Les données de ce champ NE DOIVENT
PAS avoir de bourrage
</paragraph>
</description>
</field>
```

```
<field name="selectorIdTotalPktsObserved" dataType="unsigned64"
dataTypeSemantics="totalCounter" elementId="318" status="current"
group="statistics">
<description>
<paragraph>
Cet élément d'information spécifie le nombre total de paquets observés par un sélecteur, pour une valeur spécifique de
SelectorId. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à
laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].
</paragraph>
</description>
<units>packets</units>
</field>
```

```
<field name="selectorIdTotalPktsSelected" dataType="unsigned64"
dataTypeSemantics="totalCounter" elementId="319" status="current"
group="statistics">
<description>
<paragraph>
```

Cet élément d'information spécifie le nombre total de paquets choisis par un sélecteur, pour une valeur spécifique de SelectorId. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].

```
</paragraph>
</description>
<units>packets</units>
</field>
```

```
<field name="absoluteError" dataType="float64"
dataTypeSemantics="quantity" elementId="320" status="current"
group="statistics">
```

```
<description>
<paragraph>
Cet élément d'information spécifie l'erreur de mesure maximum possible de la valeur rapportée pour un élément d'information donné. Le absoluteError a les mêmes unités que l'élément d'information auquel il est associé. La valeur réelle de la métrique peut différer de la absoluteError (positive ou négative) de la valeur mesurée. Cet élément d'information donne seulement l'erreur pour les valeurs mesurées. Si un élément d'information contient une valeur estimée (provenant de l'échantillonnage) les limites de confiance et le niveau de confiance doivent être fournis à la place, en utilisant les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].
```

```
</paragraph>
</description>
<units>Les unités de l'élément d'information pour lequel l'erreur est spécifiée.</units>
</field>
```

```
<field name="relativeError" dataType="float64"
dataTypeSemantics="quantity" elementId="321" status="current"
group="statistics">
```

```
<description>
<paragraph>
Cet élément d'information spécifie le taux d'erreur positive ou négative maximum possible pour la valeur rapportée pour un élément d'information donné comme pourcentage de la valeur mesurée. La valeur réelle de la métrique peut différer de relativeError pourcent (positif ou négatif) de la valeur mesurée. Cet élément d'information donne seulement l'erreur pour les valeurs mesurées. Si un élément d'information contient une valeur estimée (provenant de l'échantillonnage) les limites de confiance et le niveau de confiance doivent être fournis à la place, en utilisant les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel. Cet élément d'information devrait être utilisé dans un gabarit d'options dont la portée est l'observation à laquelle il se réfère. Voir le paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101].
```

```
</paragraph>
</description>
</field>
```

```
<field name="observationTimeSeconds" dataType="dateTimeSeconds"
dataTypeSemantics="quantity" elementId="322" status="current"
group="timestamps">
```

```
<description>
<paragraph>
Cet élément d'information spécifie en secondes le temps absolu d'une observation.
```

```
</paragraph>
</description>
<units>seconds</units>
</field>
```

```
<field name="observationTimeMilliseconds"
dataType="dateTimeMilliseconds" dataTypeSemantics="quantity"
elementId="323" status="current" group="timestamps">
```

```
<description>
<paragraph>
Cet élément d'information spécifie en millisecondes le temps absolu d'une observation.
</paragraph>
```

```
</description>
<units>milliseconds</units>
</field>
```

```
<field name="observationTimeMicroseconds"
  dataType="dateTimeMicroseconds" dataTypeSemantics="quantity"
  elementId="324" status="current" group="timestamps">
  <description>
    <paragraph>
      Cet élément d'information spécifie en microsecondes le temps absolu d'une observation.
    </paragraph>
  </description>
  <units>microseconds</units>
</field>
```

```
<field name="observationTimeNanoseconds"
  dataType="dateTimeNanoseconds" dataTypeSemantics="quantity"
  elementId="325" status="current" group="timestamps">
  <description>
    <paragraph>
      Cet élément d'information spécifie en nanosecondes le temps absolu d'une observation.
    </paragraph>
  </description>
  <units>nanoseconds</units>
</field>
```

```
<field name="digestHashValue" dataType="unsigned64"
  dataTypeSemantics="quantity" elementId="326" status="current"
  group="hash configuration">
  <description>
    <paragraph>
      Cet élément d'information spécifie la valeur provenant de la fonction de hachage de résumé. Voir aussi les paragraphes
      6.2, 3.8, et 7.1 de la [RFC5475].
    </paragraph>
  </description>
</field>
```

```
<field name="hashIPPayloadOffset" dataType="unsigned64"
  dataTypeSemantics="quantity" elementId="327" status="current"
  group="hash configuration">
  <description>
    <paragraph>
      Cet élément d'information spécifie le décalage de la charge utile IP utilisé par un sélecteur de choix fondé sur le hachage.
      Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
    </paragraph>
  </description>
</field>
```

```
<field name="hashIPPayloadSize" dataType="unsigned64"
  dataTypeSemantics="quantity" elementId="328" status="current"
  group="hash configuration">
  <description>
    <paragraph>
      Cet élément d'information spécifie la taille de la charge utile IP utilisée par un sélecteur de choix fondé sur le hachage.
      Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
    </paragraph>
  </description>
</field>
```

```
<field name="hashOutputRangeMin" dataType="unsigned64"
  dataTypeSemantics="quantity" elementId="329" status="current"
```

```
group="hash configuration">
<description>
<paragraph>
Cet élément d'information spécifie la valeur pour le début de la gamme de résultats potentiels d'une fonction de hachage.
Voir aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
</paragraph>
</description>
</field>

<field name="hashOutputRangeMax" dataType="unsigned64"
dataTypeSemantics="quantity" elementId="330" status="current"
group="hash configuration">
<description>
<paragraph>
Cet élément d'information spécifie la valeur de la fin de la gamme de résultats potentiels d'une fonction de hachage. Voir
aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
</paragraph>
</description>
</field>

<field name="hashSelectedRangeMin" dataType="unsigned64"
dataTypeSemantics="quantity" elementId="331" status="current"
group="hash configuration">
<description>
<paragraph>
Cet élément d'information spécifie la valeur pour le début de la gamme choisie d'une fonction de hachage. Voir aussi les
paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
</paragraph>
</description>
</field>

<field name="hashSelectedRangeMax" dataType="unsigned64"
dataTypeSemantics="quantity" elementId="332" status="current"
group="hash configuration">
<description>
<paragraph>
Cet élément d'information spécifie la valeur pour la fin de la gamme choisie d'une fonction de hachage. Voir aussi les
paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
</paragraph>
</description>
</field>

<field name="hashDigestOutput" dataType="boolean"
dataTypeSemantics="quantity" elementId="333" status="current"
group="hash configuration">
<description>
<paragraph>
Cet élément d'information contient une valeur booléenne qui est VRAIE si le résultat provenant de ce sélecteur de
hachage a été configuré à être inclus dans le rapport de paquet comme un résumé de paquet, et FAUX autrement. Voir
aussi les paragraphes 6.2, 3.8, et 7.1 de la [RFC5475].
</paragraph>
</description>
</field>

<field name="hashInitialiserValue" dataType="unsigned64"
dataTypeSemantics="quantity" elementId="334" status="current"
group="hash configuration">
<description>
<paragraph>
Cet élément d'information spécifie tla valeur d'initialisation de la fonction de hachage. Voir aussi les paragraphes 6.2,
3.8, et 7.1 de la [RFC5475].
```

```
</paragraph>
</description>
</field>
```

```
<field name="upperCILimit" dataType="float64"
  dataTypeSemantics="quantity" elementId="336" status="current"
  group="statistics">
  <description>
  <paragraph>
  Cet élément d'information spécifie la limite supérieure d'un intervalle de confiance. Il est utilisé pour fournir une
  déclaration de précision pour une valeur estimée. Les limites de confiance définissent la gamme dans laquelle la valeur
  réelle est supposée être avec une certaine probabilité p. Les limites de confiance doivent toujours être associées à un
  niveau de confiance qui définit cette probabilité p. Noter qu'un intervalle de confiance ne fournit qu'une probabilité que
  la valeur réelle se tienne dans les limites. Cela signifie que la valeur réelle peut être en-dehors des limites de confiance.
  Les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel devraient tous être utilisés dans un gabarit
  d'options dont la portée est l'observation à laquelle ils se réfèrent. Voir le paragraphe 3.4.2.1 du document de protocole
  IPFIX [RFC5101]. Noter que upperCILimit, lowerCILimit, et confidenceLevel sont tous obligés de spécifier le niveau
  de confiance, et devraient être ignorés si tous ne sont pas spécifiés ensemble.
  </paragraph>
  </description>
</field>
```

```
<field name="lowerCILimit" dataType="float64"
  dataTypeSemantics="quantity" elementId="337" status="current"
  group="statistics">
  <description>
  <paragraph>
  Cet élément d'information spécifie la limite inférieure d'un intervalle de confiance. Pour plus d'information, voir la
  description de upperCILimit. Les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel devraient tous
  être utilisés dans un gabarit d'options dont la portée est l'observation à laquelle ils se réfèrent. Voir le paragraphe 3.4.2.1
  du document de protocole IPFIX [RFC5101]. Noter que upperCILimit, lowerCILimit, et confidenceLevel sont tous
  obligés de spécifier le niveau de confiance, et devraient être ignorés si tous ne sont pas spécifiés ensemble.
  </paragraph>
  </description>
</field>
```

```
<field name="confidenceLevel" dataType="float64"
  dataTypeSemantics="quantity" elementId="338" status="current"
  group="statistics">
  <description>
  <paragraph>
  Cet élément d'information spécifie le niveau de confiance. Il est utilisé pour fournir une déclaration de précision sur les
  valeurs estimées. Le niveau de confiance donne la probabilité p avec laquelle la valeur réelle se tient dans une gamme
  donnée. Un niveau de confiance doit toujours être associé à des limites de confiance qui définissent la gamme dans
  laquelle la valeur réelle est supposée être. Les éléments d'information upperCILimit, lowerCILimit, et confidenceLevel
  devraient tous être utilisés dans un gabarit d'options dont la portée est l'observation à laquelle ils se réfèrent. Voir le
  paragraphe 3.4.2.1 du document de protocole IPFIX [RFC5101]. Noter que upperCILimit, lowerCILimit, et
  confidenceLevel sont tous obligés de spécifier le niveau de confiance, et devraient être ignorés si tous ne sont pas
  spécifiés ensemble.
  </paragraph>
  </description>
</field>
```

```
</fieldDefinitions>
```

Adresse des auteurs

Thomas Dietz
NEC Europe Ltd.
NEC Laboratories Europe
Network Research Division
Kurfuersten-Anlage 36
Heidelberg 69115
Germany
téléphone : +49 6221 4342-128
mél : Thomas.Dietz@nw.neclab.eu

Benoit Claise
Cisco Systems, Inc.
De Kleetlaan 6a b1
Degem 1813
Belgium
téléphone : +32 2 704 5622
mél : bclaise@cisco.com

Paul Aitken
Cisco Systems, Inc.
96 Commercial Quay
Edinburgh EH6 6LX
Scotland
téléphone : +44 131 561 3616
mél : paitken@cisco.com
URI : <http://www.cisco.com>

Falko Dressler
University of Erlangen-Nuremberg
Dept. of Computer Sciences
Martensstr. 3
Erlangen 91058
Germany
téléphone : +49 9131 85-27914
mél : dressler@informatik.uni-erlangen.de
URI: <http://www7.informatik.uni-erlangen.de/~dressler>

Georg Carle
Technical University of Munich
Institute for Informatics
Boltzmannstr. 3
Garching bei Muenchen 85737
Germany
téléphone : +49 89 289-18030
mél : carle@in.tum.de
URI : <http://www.net.in.tum.de/~carle/>