Network Working Group
Request for Comments: 5477
Category: Standards Track

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

March 2009

Information Model for Packet Sampling Exports

Status of This Memo

Copyright Notice

Abstract

This memo defines an information model for the Packet SAMPling (PSAMP) protocol. It is used by the PSAMP protocol for encoding sampled packet data and information related to the Sampling process. As the PSAMP protocol is based on the IP Flow Information eXport (IPFIX) protocol, this information model is an extension to the IPFIX information model.

Table of Contents

1. Introduction

Packet Sampling techniques are required for various measurement scenarios. The Packet Sampling (PSAMP) protocol provides mechanisms for packet selection using different Filtering and Sampling techniques. A standardized way for the export and storage of the Information Elements defined in Section 8 is required. The definition of the PSAMP information and data model is based on the IPFIX information model [RFC5102]. The PSAMP protocol document [RFC5476] specifies how to use the IPFIX protocol in the PSAMP context.

This document examines the IPFIX information model [RFC5102] and extends it to meet the PSAMP requirements. Therefore, the structure of this document is strongly based on the IPFIX document. It complements the PSAMP protocol specification by providing an appropriate PSAMP information model. The main part of this document, Section 8, defines the list of Information Elements to be transmitted by the PSAMP protocol. Sections 5 and 6 describe the data types and Information Element properties used within this document and their relationship to the IPFIX information model.

Although the PSAMP charter specified no requirements for measuring packet errors (such as drops, malformed, etc.), and this document does not cover such data, if there is need for collecting and exporting packet error information, the appropriate Information

Elements can be requested from IANA, and exported with the PSAMP protocol.

The main body of Section 8 was generated from an XML document. The XML-based specification of the PSAMP Information Elements can be used for automatically checking syntactical correctness of the specification. Furthermore it can be used -- in combination with the IPFIX information model -- for automated code generation. The resulting code can be used in PSAMP protocol implementations to deal with processing PSAMP information elements.

For that reason, the XML document that served as the source for Section 8 is attached to this document in Appendix A.

Note that although partially generated from the attached XML documents, the main body of this document is normative while the appendix is informational.

2. PSAMP Documents Overview

This document is one out of a series of documents from the PSAMP group.

[RFC5474]: "A Framework for Packet Selection and Reporting" describes the PSAMP framework for network elements to select subsets of packets by statistical and other methods, and to export a stream of reports on the selected packets to a Collector.

[RFC5475]: "Sampling and Filtering Techniques for IP Packet Selection" describes the set of packet selection techniques supported by PSAMP.

[RFC5476]: "Packet Sampling (PSAMP) Protocol Specifications" specifies the export of packet information from a PSAMP Exporting Process to a PSAMP Collecting Process.

RFC 5477 (this document): "Information Model for Packet Sampling Exports" defines an information and data model for PSAMP.

3. Terminology

IPFIX-specific terminology used in this document is defined in Section 2 of [RFC5101]. PSAMP-specific terminology used in this document is defined in Section 3.2 of [RFC5476]. In this document, as in [RFC5101] and [RFC5476], the first letter of each IPFIX- and PSAMP-specific term is capitalized.

3.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

4. Relationship between PSAMP and IPFIX

As described in the PSAMP protocol [RFC5476], a PSAMP Report can be seen as a very special IPFIX Data Record. It represents an IPFIX Flow containing only a single packet. Therefore, the IPFIX information model can be used as a basis for PSAMP Reports.

Nevertheless, there are properties required in PSAMP Reports that cannot be modeled using the current IPFIX information model. This document describes extensions to the IPFIX information model that allow the modeling of information and data required by PSAMP.

Some of these extensions allow the export of what may be considered sensitive information. Refer to the Security Considerations section for a fuller discussion.

Note that the export of sampled or filtered PSAMP Reports may not need all the Information Elements defined by the IPFIX information model [RFC5102], as discussed in Sections 6.2 and 6.3 of the PSAMP Framework [RFC5474].

5. Properties of a PSAMP Information Element

The PSAMP Information Elements are defined in accordance with Sections 2.1 to 2.3 of the IPFIX information model [RFC5102] to which reference should be made for more information. Nevertheless, we strongly recommend defining the optional "units" property for every Information Element (if applicable).

The Data Types defined in Section 3.1 of the IPFIX information model [RFC5102] are also used for the PSAMP Information Elements.

6. Type Space

The PSAMP Information Elements MUST be constructed from the basic abstract data types and data type semantics described in Section 3 of the IPFIX information model [RFC5102]. To ensure consistency between IPFIX and PSAMP, the data types are not repeated in this document. The encoding of these data types is described in the IPFIX protocol [RFC5101].

7. Overloading Information Elements

Information Elements SHOULD NOT be overloaded with multiple meanings or re-used for multiple purposes. Different Information Elements SHOULD be allocated for each requirement.

Although the presence of certain other Information Elements allows the selection method to be inferred, a separate Information Element is provided for the selectorAlgorithm to include as scope for the Selector Report Interpretation [RFC5476].

Even if the Information Elements are specified with a specific selection method (i.e., a specific value of selectorAlgorithm) in mind, these Information Elements are not restricted to the selection method and MAY be used for different selection methods in the future.

8. The PSAMP Information Elements

This section describes the Information Elements used by the PSAMP protocol.

For each Information Element specified in Sections 8.1 - 8.6 below, a unique identifier is allocated in accordance with Section 4 of the IPFIX information model [RFC5102]. The assignments are controlled by IANA as an extension of the IPFIX information model.

The Information Elements specified by the IPFIX information model [RFC5102] are used by the PSAMP protocol where applicable. To avoid inconsistencies between the IPFIX and the PSAMP information and data models, only those Information Elements that are not already described by the IPFIX information model are defined here.

Below is the list of additional PSAMP Information Elements:

ID	Name	ID	Name
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. Identifiers (301-303)

Information Elements in this section serve as identifiers. All of them have an integral abstract data type and data type semantics "identifier".

ID	Name	ID	Name
301	selectionSequenceId	303	informationElementId
302	selectorId		

8.1.1. selectionSequenceId

Description:

From all the packets observed at an Observation Point, a subset of the packets is selected by a sequence of one or more Selectors. The selectionSequenceId is a unique value per Observation Domain, specifying the Observation Point and the sequence of Selectors through which the packets are selected.

Abstract Data Type: unsigned64

Data Type Semantics: identifier

ElementId: 301

Status: current

8.1.2. selectorId

Description:

The Selector ID is the unique ID identifying a Primitive Selector. Each Primitive Selector must have a unique ID in the Observation Domain.

Abstract Data Type: unsigned16

Data Type Semantics: identifier

ElementId: 302

Status: current

8.1.3. informationElementId

Description:

This Information Element contains the ID of another Information Element.

Abstract Data Type: unsigned16

Data Type Semantics: identifier

ElementId: 303

Status: current

8.2. Sampling Configuration (304-311)

Information Elements in this section can be used for describing the Sampling configuration of a Selection Process.

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

8.2.1. selectorAlgorithm

Description:

This Information Element identifies the packet selection methods (e.g., Filtering, Sampling) that are applied by the Selection Process.

Most of these methods have parameters. Further Information Elements are needed to fully specify packet selection with these methods and all their parameters.

The methods listed below are defined in [RFC5475]. For their parameters, Information Elements are defined in the information model document. The names of these Information Elements are listed for each method identifier.

Further method identifiers may be added to the list below. It might be necessary to define new Information Elements to specify their parameters.

The selectorAlgorithm registry is maintained by IANA. New assignments for the registry will be administered by IANA and are subject to Expert Review [RFC5226].

The registry can be updated when specifications of the new method(s) and any new Information Elements are provided.

The group of experts must double check the selectorAlgorithm definitions and Information Elements with already defined selectorAlgorithms and Information Elements for completeness, accuracy, and redundancy. Those experts will initially be drawn from the Working Group Chairs and document editors of the IPFIX and PSAMP Working Groups.

The following packet selection methods identifiers are defined here:

ID	Method	Parameters
1	Systematic count-based Sampling	samplingPacketInterval samplingPacketSpace
2	Systematic time-based Sampling	samplingTimeInterval samplingTimeSpace
3	Random n-out-of-N Sampling	samplingSize samplingPopulation
4	Uniform probabilistic Sampling	samplingProbability
5	Property Match Filtering	no agreed parameters
	Hash-based Filtering	hashInitialiserValue hashIPPayloadOffset hashIPPayloadSize hashSelectedRangeMin hashSelectedRangeMax hashOutputRangeMin hashOutputRangeMax
6	using BOB	
7	using IPSX	
8	using CRC	

There is a broad variety of possible parameters that could be used for Property match Filtering (5), but currently there are no agreed parameters specified.

Abstract Data Type: unsigned16

Data Type Semantics: identifier

ElementId: 304

Status: current

8.2.2. samplingPacketInterval

Description:

This Information Element specifies the number of packets that are consecutively sampled. A value of 100 means that 100 consecutive packets are sampled.

For example, this Information Element may be used to describe the configuration of a systematic count-based Sampling Selector.

Abstract Data Type: unsigned32

Data Type Semantics: quantity

ElementId: 305

Status: current

Units: packets

8.2.3. samplingPacketSpace

Description:

This Information Element specifies the number of packets between two "samplingPacketInterval"s. A value of 100 means that the next interval starts 100 packets (which are not sampled) after the current "samplingPacketInterval" is over.

For example, this Information Element may be used to describe the configuration of a systematic count-based Sampling Selector.

Abstract Data Type: unsigned32

Data Type Semantics: quantity

ElementId: 306

Status: current

Units: packets

8.2.4. samplingTimeInterval

Description:

This Information Element specifies the time interval in microseconds during which all arriving packets are sampled.

For example, this Information Element may be used to describe the configuration of a systematic time-based Sampling Selector.

Abstract Data Type: unsigned32

Data Type Semantics: quantity

ElementId: 307

Status: current

Units: microseconds

8.2.5. samplingTimeSpace

Description:

This Information Element specifies the time interval in microseconds between two "samplingTimeInterval"s. A value of 100 means that the next interval starts 100 microseconds (during which no packets are sampled) after the current "samplingTimeInterval" is over.

For example, this Information Element may used to describe the configuration of a systematic time-based Sampling Selector.

Abstract Data Type: unsigned32

Data Type Semantics: quantity

ElementId: 308

Status: current

Units: microseconds

8.2.6. samplingSize

Description:

This Information Element specifies the number of elements taken from the parent Population for random Sampling methods.

For example, this Information Element may be used to describe the configuration of a random n-out-of-N Sampling Selector.

Abstract Data Type: unsigned32

Data Type Semantics: quantity

ElementId: 309

Status: current

Units: packets

8.2.7. samplingPopulation

Description:

This Information Element specifies the number of elements in the parent Population for random Sampling methods.

For example, this Information Element may be used to describe the configuration of a random n-out-of-N Sampling Selector.

Abstract Data Type: unsigned32

Data Type Semantics: quantity

ElementId: 310

Status: current

Units: packets

8.2.8. samplingProbability

Description:

This Information Element specifies the probability that a packet is sampled, expressed as a value between 0 and 1. The probability is equal for every packet. A value of 0 means no packet was sampled since the probability is 0.

For example, this Information Element may be used to describe the configuration of a uniform probabilistic Sampling Selector.

Abstract Data Type: float64

Data Type Semantics: quantity

ElementId: 311

Status: current

8.3. Hash Configuration (326-334)

The following Information Elements can be used for describing the Sampling configuration of a Selection Process. The individual parameters are explained in more detail in Sections 6.2, 3.8, and 7.1 of [RFC5475].

ID	Name	ID	Name
326	digestHashValue	331	hashSelectedRangeMin
327	hashIPPayloadOffset	332	hashSelectedRangeMax
328	hashIPPayloadSize	333	hashDigestOutput
329	hashOutputRangeMin	334	hashInitialiserValue
330	hashOutputRangeMax		

8.3.1. digestHashValue

Description:

This Information Element specifies the value from the digest hash function.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 326

Status: current

8.3.2. hashIPPayloadOffset

Description:

This Information Element specifies the IP payload offset used by a Hash-based Selection Selector.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 327

Status: current

8.3.3. hashIPPayloadSize

Description:

This Information Element specifies the IP payload size used by a Hash-based Selection Selector.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 328

Status: current

8.3.4. hashOutputRangeMin

Description:

This Information Element specifies the value for the beginning of a hash function’s potential output range.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 329

Status: current

8.3.5. hashOutputRangeMax

Description:

This Information Element specifies the value for the end of a hash function’s potential output range.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 330

Status: current

8.3.6. hashSelectedRangeMin

Description:

This Information Element specifies the value for the beginning of a hash function’s selected range.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 331

Status: current

8.3.7. hashSelectedRangeMax

Description:

This Information Element specifies the value for the end of a hash function’s selected range.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 332

Status: current

8.3.8. hashDigestOutput

Description:

This Information Element contains a boolean value that is TRUE if the output from this hash Selector has been configured to be included in the packet report as a packet digest, else FALSE.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: boolean

Data Type Semantics: quantity

ElementId: 333

Status: current

8.3.9. hashInitialiserValue

Description:

This Information Element specifies the initialiser value to the hash function.

See also Sections 6.2, 3.8, and 7.1 of [RFC5475].

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: 334

Status: current

8.4. Timestamps (322-325)

The Information Elements listed below contain timestamps. They can be used for reporting the observation time of a single packet.

ID	Name	ID	Name
322	observationTimeSeconds	324	observationTimeMicroseconds
323	observationTimeMilliseconds	325	observationTimeNanoseconds

8.4.1. observationTimeSeconds

Description:

This Information Element specifies the absolute time in seconds of an observation.

Abstract Data Type: dateTimeSeconds

Data Type Semantics: quantity

ElementId: 322

Status: current

Units: seconds

8.4.2. observationTimeMilliseconds

Description:

This Information Element specifies the absolute time in milliseconds of an observation.

Abstract Data Type: dateTimeMilliseconds

Data Type Semantics: quantity

ElementId: 323

Status: current

Units: milliseconds

8.4.3. observationTimeMicroseconds

Description:

This Information Element specifies the absolute time in microseconds of an observation.

Abstract Data Type: dateTimeMicroseconds

Data Type Semantics: quantity

ElementId: 324

Status: current

Units: microseconds

8.4.4. observationTimeNanoseconds

Description:

This Information Element specifies the absolute time in nanoseconds of an observation.

Abstract Data Type: dateTimeNanoseconds

Data Type Semantics: quantity

ElementId: 325

Status: current

Units: nanoseconds

8.5. Packet Data (313-314, 316-317)

The following Information Elements are all used for reporting raw content of a packet. All Information Elements containing sections of the observed packet can also be used in IPFIX [RFC5101]. If the values for those sections vary for different packets in a Flow, then the Flow Report will contain the value observed in the first packet of the Flow.

ID	Name	ID	Name
313	ipHeaderPacketSection	316	mplsLabelStackSection
314	ipPayloadPacketSection	317	mplsPayloadPacketSection

8.5.1. ipHeaderPacketSection

Description:

This Information Element, which may have a variable length, carries a series of octets from the start of the IP header of a sampled packet.

With sufficient length, this element also reports octets from the IP payload, subject to [RFC2804]. See the Security Considerations section.

The size of the exported section may be constrained due to limitations in the IPFIX protocol.

The data for this field MUST NOT be padded.

Abstract Data Type: octetArray

ElementId: 313

Status: current

8.5.2. ipPayloadPacketSection

Description:

This Information Element, which may have a variable length, carries a series of octets from the start of the IP payload of a sampled packet.

The IPv4 payload is that part of the packet that follows the IPv4 header and any options, which [RFC0791] refers to as "data" or "data octets". For example, see the examples in [RFC0791], Appendix A.

The IPv6 payload is the rest of the packet following the 40-octet IPv6 header. Note that any extension headers present are considered part of the payload. See [RFC2460] for the IPv6 specification.

The size of the exported section may be constrained due to limitations in the IPFIX protocol.

The data for this field MUST NOT be padded.

Abstract Data Type: octetArray

ElementId: 314

Status: current

8.5.3. mplsLabelStackSection

Description:

This Information Element, which may have a variable length, carries the first n octets from the MPLS label stack of a sampled packet.

With sufficient length, this element also reports octets from the MPLS payload, subject to [RFC2804]. See the Security Considerations section.

See [RFC3031] for the specification of MPLS packets.

See [RFC3032] for the specification of the MPLS label stack.

The size of the exported section may be constrained due to limitations in the IPFIX protocol.

The data for this field MUST NOT be padded.

Abstract Data Type: octetArray

ElementId: 316

Status: current

8.5.4. mplsPayloadPacketSection

Description:

This Information Element, which may have a variable length, carries the first n octets from the MPLS payload of a sampled packet, being data that follows immediately after the MPLS label stack.

See [RFC3031] for the specification of MPLS packets.

See [RFC3032] for the specification of the MPLS label stack.

The size of the exported section may be constrained due to limitations in the IPFIX protocol.

The data for this field MUST NOT be padded.

Abstract Data Type: octetArray

ElementId: 317

Status: current

8.6. Statistics (318-321, 336-338)

Information Elements in this section can be used for reporting statistics from the Metering Process.

ID	Name	ID	Name
318	selectorIdTotalPktsObserved	336	upperCILimit
319	selectorIdTotalPktsSelected	337	lowerCILimit
320	absoluteError	338	confidenceLevel
321	relativeError		

8.6.1. selectorIdTotalPktsObserved

Description:

This Information Element specifies the total number of packets observed by a Selector, for a specific value of SelectorId.

This Information Element should be used in an Options Template scoped to the observation to which it refers. See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Abstract Data Type: unsigned64

Data Type Semantics: totalCounter

ElementId: 318

Status: current

Units: packets

8.6.2. selectorIdTotalPktsSelected

Description:

This Information Element specifies the total number of packets selected by a Selector, for a specific value of SelectorId.

This Information Element should be used in an Options Template scoped to the observation to which it refers. See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Abstract Data Type: unsigned64

Data Type Semantics: totalCounter

ElementId: 319

Status: current

Units: packets

8.6.3. absoluteError

Description:

This Information Element specifies the maximum possible measurement error of the reported value for a given Information Element. The absoluteError has the same unit as the Information Element with which it is associated. The real value of the metric can differ by absoluteError (positive or negative) from the measured value.

This Information Element provides only the error for measured values. If an Information Element contains an estimated value (from Sampling), the confidence boundaries and confidence level have to be provided instead, using the upperCILimit, lowerCILimit, and confidenceLevel Information Elements.

This Information Element should be used in an Options Template scoped to the observation to which it refers. See section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Abstract Data Type: float64

Data Type Semantics: quantity

ElementId: 320

Status: current

Units: The units of the Information Element for which the error is specified.

8.6.4. relativeError

Description:

This Information Element specifies the maximum possible positive or negative error ratio for the reported value for a given Information Element as a percentage of the measured value. The real value of the metric can differ by relativeError percent (positive or negative) from the measured value.

This Information Element provides only the error for measured values. If an Information Element contains an estimated value (from Sampling), the confidence boundaries and confidence level have to be provided instead, using the upperCILimit, lowerCILimit, and confidenceLevel Information Elements.

This Information Element should be used in an Options Template scoped to the observation to which it refers. See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Abstract Data Type: float64

Data Type Semantics: quantity

ElementId: 321

Status: current

8.6.5. upperCILimit

Description:

This Information Element specifies the upper limit of a confidence interval. It is used to provide an accuracy statement for an estimated value. The confidence limits define the range in which the real value is assumed to be with a certain probability p. Confidence limits always need to be associated with a confidence level that defines this probability p. Please note that a confidence interval only provides a probability that the real value lies within the limits. That means the real value can lie outside the confidence limits.

The upperCILimit, lowerCILimit, and confidenceLevel Information Elements should all be used in an Options Template scoped to the observation to which they refer. See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Note that the upperCILimit, lowerCILimit, and confidenceLevel are all required to specify confidence, and should be disregarded unless all three are specified together.

Abstract Data Type: float64

Data Type Semantics: quantity

ElementId: 336

Status: current

8.6.6. lowerCILimit

Description:

This Information Element specifies the lower limit of a confidence interval. For further information, see the description of upperCILimit.

The upperCILimit, lowerCILimit, and confidenceLevel Information Elements should all be used in an Options Template scoped to the observation to which they refer. See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Note that the upperCILimit, lowerCILimit, and confidenceLevel are all required to specify confidence, and should be disregarded unless all three are specified together.

Abstract Data Type: float64

Data Type Semantics: quantity

ElementId: 337

Status: current

8.6.7. confidenceLevel

Description:

This Information Element specifies the confidence level. It is used to provide an accuracy statement for estimated values. The confidence level provides the probability p with which the real value lies within a given range. A confidence level always needs to be associated with confidence limits that define the range in which the real value is assumed to be.

The upperCILimit, lowerCILimit, and confidenceLevel Information Elements should all be used in an Options Template scoped to the observation to which they refer. See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

Note that the upperCILimit, lowerCILimit, and confidenceLevel are all required to specify confidence, and should be disregarded unless all three are specified together.

Abstract Data Type: float64

Data Type Semantics: quantity

ElementId: 338

Status: current

9. Security Considerations

The PSAMP information model itself does not directly introduce security issues. Rather, it defines a set of attributes that may for privacy or business issues be considered sensitive information.

For example, exporting values of header fields may make attacks possible for the receiver of this information, which would otherwise only be possible for direct observers of the reported Flows along the data path. Specifically, the Information Elements pertaining to packet sections MUST target no more than the packet header, some subsequent bytes of the packet, and encapsulating headers if present. Full packet capture of arbitrary packet streams is explicitly out of scope, per [RFC2804].

The underlying protocol used to exchange the information described here MUST therefore apply appropriate procedures to guarantee the integrity and confidentiality of the exported information. Such procedures are defined in separate documents, specifically the IPFIX protocol document [RFC5101].

10. IANA Considerations

The PSAMP information model, as set out in this document, has two sets of assigned numbers. Considerations for assigning them are discussed in this section, using the example policies as set out in the "Guidelines for IANA Considerations" document [RFC5226].

10.1. Related Considerations

As the PSAMP protocol uses the IPFIX protocol, refer to the IANA Considerations section in [RFC5102] for the assignments of numbers used in the protocol and for the numbers used in the information model.

10.2. PSAMP-Related Considerations

This document specifies an initial set of PSAMP Information Elements fulfilling the needs specified in [RFC5475], as an extension to the IPFIX Information Elements [RFC5102].

Note that the PSAMP Information Element IDs were initially started at value 301, in order to leave a gap for any ongoing IPFIX work requiring new Information Elements. It is expected that this gap in the Information Element numbering will be filled in by IANA with new IPFIX Information Elements.

Each new selection method MUST be assigned a unique value in the selectorAlgorithm registry. Its configuration parameter(s), along with the way to report them with an Options Template, MUST be clearly specified. The initial content of the selectorAlgorithm registry is found in Section 8.2.1.

New assignments for the PSAMP selection method will be administered by IANA and are subject to Expert Review [RFC5226]. The group of experts must double check the Information Elements definitions with already defined Information Elements for completeness, accuracy, and redundancy. Those experts will initially be drawn from the Working Group Chairs and document editors of the IPFIX and PSAMP Working Groups. The selectorAlgorithm registry is maintained by IANA and can be updated as long as specifications of the new method(s) and any new Information Elements are provided.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5101] Claise, B., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, January 2008.

[RFC5475] Zseby, T., Molina, M., Duffield, D., Niccolini, S., and F. Rapall, "Sampling and Filtering Techniques for IP Packet Selection", RFC 5475, March 2009.

[RFC5476] Claise, B., Ed., "Packet Sampling (PSAMP) Protocol Specifications", RFC 5476, March 2009.

11.2. Informative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC2804] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[RFC5474] Duffield, N., Ed., "A Framework for Packet Selection and Reporting", RFC 5474, March 2009.

Appendix A. Formal Specification of PSAMP Information Elements

This appendix contains a formal description of the PSAMP information model XML document. Note that this appendix is of informational nature, while the text in Section 8 generated from this appendix is normative.

Using a formal and machine-readable syntax for the information model enables the creation of PSAMP-aware tools that can automatically adapt to extensions to the information model, by simply reading updated information model specifications.

The wide availability of XML-aware tools and libraries for client devices is a primary consideration for this choice. In particular, libraries for parsing XML documents are readily available. Also, mechanisms such as the Extensible Stylesheet Language (XSL) allow for transforming a source XML document into other documents. This draft was authored in XML and transformed according to [RFC2629].

It should be noted that the use of XML in Exporters, Collectors, or other tools is not mandatory for the deployment of PSAMP. In particular, exporting processes do not produce or consume XML as part of their operation. It is expected that PSAMP Collectors MAY take advantage of the machine readability of the information model vs. hardcoding their behavior or inventing proprietary means for accommodating extensions.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  This XML document is a product of the IETF IPFIX Working Group.
  Contact information:
    WG charter:
      http://www.ietf.org/html.charters/ipfix-charter.html

    Mailing Lists:
      General Discussion: ipfix@ietf.org
      To Subscribe: http://www1.ietf.org/mailman/listinfo/ipfix
      Archive:
        http://www1.ietf.org/mail-archive/web/ipfix/current/index.html

    Editor:
      Thomas Dietz
      NEC Europe Ltd.
      NEC Laboratories Europe
      Network Research Division
      Kurfuersten-Anlage 36
      Heidelberg 69115
      Germany
```

Phone: +49 6221 4342-128
Email: Thomas.Dietz@nw.neclab.eu

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

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

Falko Dressler
University of Erlangen-Nuremberg
Dept. of Computer Sciences
Martensstr. 3
Erlangen 91058
Germany
Phone: +49 9131 85-27914
Email: 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
Phone: +49 89 289-18030
EMail: carle@in.tum.de
URI: http://www.net.in.tum.de/˜carle/

Abstract:

This memo defines an information model for the Packet SAMPling (PSAMP) protocol. It is used by the PSAMP protocol for encoding sampled packet data and information related to the Sampling process. As the PSAMP protocol is based on the IPFIX protocol, this information model is an extension to the IPFIX information model.

```
   Copyright (c) 2009 IETF Trust and the persons identified as
   authors of the code.  All rights reserved.

   Redistribution and use in source and binary forms, with or without
   modification, are permitted provided that the following conditions
   are met:

   - Redistributions of source code must retain the above copyright
     notice, this list of conditions and the following disclaimer.

   - Redistributions in binary form must reproduce the above copyright
     notice, this list of conditions and the following disclaimer in
     the documentation and/or other materials provided with the
     distribution.

   - Neither the name of Internet Society, IETF or IETF Trust, nor the
     names of specific contributors, may be used to endorse or promote
     products derived from this software without specific prior
     written permission.

   THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
   'AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
   LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
   A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
   OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
   SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
   LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
   DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
   THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
   (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
   OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

   This version of the XML document is part of RFC 5477;
   see the RFC itself for full legal notices.
-->
<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-info
             ipfix-info.xsd">
  <field name="selectionSequenceId" dataType="unsigned64"
    dataTypeSemantics="identifier" elementId="301" status="current"
    group="identifiers">
    <description>
      <paragraph>
        From all the packets observed at an Observation Point, a subset
        of the packets is selected by a sequence of one or more
        Selectors.  The selectionSequenceId is a unique value per
        Observation Domain, specifying the Observation Point and the
        sequence of Selectors through which the packets are selected.
      </paragraph>
    </description>
  </field>

  <field name="selectorId" dataType="unsigned16"
    dataTypeSemantics="identifier" elementId="302" status="current"
    group="identifiers">
    <description>
      <paragraph>
        The Selector ID is the unique ID identifying a Primitive
        Selector.  Each Primitive Selector must have a unique ID in the
        Observation Domain.
      </paragraph>
    </description>
  </field>

  <field name="informationElementId" dataType="unsigned16"
    dataTypeSemantics="identifier" elementId="303" status="current"
    group="identifiers">
    <description>
      <paragraph>
        This Information Element contains the ID of another Information
        Element.
      </paragraph>
    </description>
  </field>

  <field name="selectorAlgorithm" dataType="unsigned16"
    dataTypeSemantics="identifier" elementId="304" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element identifies the packet selection
        methods (e.g., Filtering, Sampling) that are applied by
        the Selection Process.

        Most of these methods have parameters.  Further
        Information Elements are needed to fully specify packet
        selection with these methods and all their parameters.

        The methods listed below are defined in
        [RFC5475].  For their parameters,
        Information Elements are defined in the information model
        document.  The names of these Information Elements are
        listed for each method identifier.
```

Further method identifiers may be added to the list below. It might be necessary to define new Information Elements to specify their parameters.

The selectorAlgorithm registry is maintained by IANA. New assignments for the registry will be administered by IANA and are subject to Expert Review [RFC5226].

The registry can be updated when specifications of the new method(s) and any new Information Elements are provided.

The group of experts must double check the selectorAlgorithm definitions and Information Elements with already defined selectorAlgorithms and Information Elements for completeness, accuracy, and redundancy. Those experts will initially be drawn from the Working Group Chairs and document editors of the IPFIX and PSAMP Working Groups.

The following packet selection methods identifiers are defined here:

ID	Method	Parameters
1	Systematic count-based Sampling	samplingPacketInterval samplingPacketSpace
2	Systematic time-based Sampling	samplingTimeInterval samplingTimeSpace
3	Random n-out-of-N Sampling	samplingSize samplingPopulation
4	Uniform probabilistic Sampling	samplingProbability
5	Property Match Filtering	no agreed parameters
Hash-based Filtering		hashInitialiserValue hashIPPayloadOffset hashIPPayloadSize hashSelectedRangeMin hashSelectedRangeMax hashOutputRangeMin hashOutputRangeMax
6	using BOB	
7	using IPSX	
8	using CRC	

```
        There is a broad variety of possible parameters that could be
        used for Property Match Filtering (5), but currently there are
        no agreed parameters specified.
      </paragraph>
    </description>
  </field>

  <field name="samplingPacketInterval" dataType="unsigned32"
    dataTypeSemantics="quantity" elementId="305" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the number of packets that
        are consecutively sampled.  A value of 100 means that
        100 consecutive packets are sampled.

        For example, this Information Element may be used to describe
        the configuration of a systematic count-based Sampling Selector.
      </paragraph>
    </description>
    <units>packets</units>
  </field>

  <field name="samplingPacketSpace" dataType="unsigned32"
    dataTypeSemantics="quantity" elementId="306" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the number of packets between
        two "samplingPacketInterval"s.  A value of 100 means that the
        next interval starts 100 packets (which are not sampled)
        after the current "samplingPacketInterval" is over.

        For example, this Information Element may be used to describe
        the configuration of a systematic count-based Sampling Selector.
      </paragraph>
    </description>
    <units>packets</units>
  </field>

  <field name="samplingTimeInterval" dataType="unsigned32"
    dataTypeSemantics="quantity" elementId="307" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the time interval in
        microseconds during which all arriving packets are sampled.
        For example, this Information Element may be used to describe
        the configuration of a systematic time-based Sampling Selector.
      </paragraph>
    </description>
    <units>microseconds</units>
  </field>

  <field name="samplingTimeSpace" dataType="unsigned32"
    dataTypeSemantics="quantity" elementId="308" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the time interval in
        microseconds between two "samplingTimeInterval"s.  A value of 100
        means that the next interval starts 100 microseconds
        (during which no packets are sampled) after the current
        "samplingTimeInterval" is over.

        For example, this Information Element may used to describe the
        configuration of a systematic time-based Sampling Selector.
      </paragraph>
    </description>
    <units>microseconds</units>
  </field>

  <field name="samplingSize" dataType="unsigned32"
    dataTypeSemantics="quantity" elementId="309" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the number of elements taken
        from the parent Population for random Sampling methods.

        For example, this Information Element may be used to describe
        the configuration of a random n-out-of-N Sampling Selector.
      </paragraph>
    </description>
    <units>packets</units>
  </field>

  <field name="samplingPopulation" dataType="unsigned32"
    dataTypeSemantics="quantity" elementId="310" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the number of elements in the
        parent Population for random Sampling methods.
        For example, this Information Element may be used to describe
        the configuration of a random n-out-of-N Sampling Selector.
      </paragraph>
    </description>
    <units>packets</units>
  </field>

  <field name="samplingProbability" dataType="float64"
    dataTypeSemantics="quantity" elementId="311" status="current"
    group="sampling configuration">
    <description>
      <paragraph>
        This Information Element specifies the probability that a packet
        is sampled, expressed as a value between 0 and 1.  The
        probability is equal for every packet.  A value of 0 means no
        packet was sampled since the probability is 0.

        For example, this Information Element may be used to describe
        the configuration of a uniform probabilistic Sampling Selector.
      </paragraph>
    </description>
  </field>

  <field name="ipHeaderPacketSection" dataType="octetArray"
    elementId="313" status="current" group="packet data">
    <description>
      <paragraph>
        This Information Element, which may have a variable length,
        carries a series of octets from the start of the IP header of a
        sampled packet.

        With sufficient length, this element also reports octets from
        the IP payload, subject to [RFC2804].  See the Security
        Considerations section.

        The size of the exported section may be constrained due to
        limitations in the IPFIX protocol.

        The data for this field MUST NOT be padded.
      </paragraph>
    </description>
  </field>

  <field name="ipPayloadPacketSection" dataType="octetArray"
    elementId="314" status="current" group="packet data">
    <description>
      <paragraph>
        This Information Element, which may have a variable length,
        carries a series of octets from the start of the IP payload of a
        sampled packet.

        The IPv4 payload is that part of the packet that follows the
        IPv4 header and any options, which [RFC0791] refers to as "data"
        or "data octets".  For example, see the examples in [RFC0791],
        Appendix A.

        The IPv6 payload is the rest of the packet following the
        40-octet IPv6 header.  Note that any extension headers present
        are considered part of the payload.  See [RFC2460] for the IPv6
        specification.

        The size of the exported section may be constrained due to
        limitations in the IPFIX protocol.

        The data for this field MUST NOT be padded.
      </paragraph>
    </description>
  </field>

  <field name="mplsLabelStackSection" dataType="octetArray"
    elementId="316" status="current" group="packet data">
    <description>
      <paragraph>
        This Information Element, which may have a variable length,
        carries the first n octets from the MPLS label stack of a
        sampled packet.

        With sufficient length, this element also reports octets from
        the MPLS payload, subject to [RFC2804].  See the Security
        Considerations section.

        See [RFC3031] for the specification of MPLS packets.

        See [RFC3032] for the specification of the MPLS label stack.

        The size of the exported section may be constrained due to
        limitations in the IPFIX protocol.

        The data for this field MUST NOT be padded.
      </paragraph>
    </description>
  </field>

  <field name="mplsPayloadPacketSection" dataType="octetArray"
    elementId="317" status="current" group="packet data">
    <description>
```

```
      <paragraph>
        This Information Element, which may have a variable length,
        carries the first n octets from the MPLS payload of a sampled
        packet, being data that follows immediately after the MPLS label
        stack.

        See [RFC3031] for the specification of MPLS packets.

        See [RFC3032] for the specification of the MPLS label stack.

        The size of the exported section may be constrained due to
        limitations in the IPFIX protocol.

        The data for this field MUST NOT be padded.
      </paragraph>
    </description>
  </field>

  <field name="selectorIdTotalPktsObserved" dataType="unsigned64"
    dataTypeSemantics="totalCounter" elementId="318" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the total number of packets
        observed by a Selector, for a specific value of SelectorId.

        This Information Element should be used in an Options Template
        scoped to the observation to which it refers.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].
      </paragraph>
    </description>
    <units>packets</units>
  </field>

  <field name="selectorIdTotalPktsSelected" dataType="unsigned64"
    dataTypeSemantics="totalCounter" elementId="319" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the total number of packets
        selected by a Selector, for a specific value of SelectorId.

        This Information Element should be used in an Options Template
        scoped to the observation to which it refers.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].
        </paragraph>
    </description>
    <units>packets</units>
```

```xml
  </field>

  <field name="absoluteError" dataType="float64"
    dataTypeSemantics="quantity" elementId="320" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the maximum possible
        measurement error of the reported value for a given Information
        Element.  The absoluteError has the same unit as the Information
        Element with which it is associated.  The real value of the
        metric can differ by absoluteError (positive or negative) from
        the measured value.

        This Information Element provides only the
        error for measured values.  If an Information Element contains
        an estimated value (from Sampling), the confidence boundaries
        and confidence level have to be provided instead, using the
        upperCILimit, lowerCILimit, and confidenceLevel Information
        Elements.

        This Information Element should be used in an Options Template
        scoped to the observation to which it refers.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].
      </paragraph>
    </description>
    <units>
      The units of the Information Element for which the error is
      specified.
    </units>
  </field>

  <field name="relativeError" dataType="float64"
    dataTypeSemantics="quantity" elementId="321" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the maximum possible positive
        or negative error ratio for the reported value for a given
        Information Element as a percentage of the measured value.
        The real value of the metric can differ by relativeError percent
        (positive or negative) from the measured value.

        This Information Element provides only the error for measured
        values.  If an Information Element contains an estimated value
        (from Sampling), the confidence boundaries and confidence
        level have to be provided instead, using the upperCILimit,
        lowerCILimit, and confidenceLevel Information Elements.
        This Information Element should be used in an Options Template
        scoped to the observation to which it refers.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].
      </paragraph>
    </description>
  </field>

  <field name="observationTimeSeconds" dataType="dateTimeSeconds"
    dataTypeSemantics="quantity" elementId="322" status="current"
    group="timestamps">
    <description>
      <paragraph>
        This Information Element specifies the absolute time in seconds
        of an observation.
      </paragraph>
    </description>
    <units>seconds</units>
  </field>

  <field name="observationTimeMilliseconds"
    dataType="dateTimeMilliseconds" dataTypeSemantics="quantity"
    elementId="323" status="current" group="timestamps">
    <description>
      <paragraph>
        This Information Element specifies the absolute time in
        milliseconds of an observation.
      </paragraph>
    </description>
    <units>milliseconds</units>
  </field>

  <field name="observationTimeMicroseconds"
    dataType="dateTimeMicroseconds" dataTypeSemantics="quantity"
    elementId="324" status="current" group="timestamps">
    <description>
      <paragraph>
        This Information Element specifies the absolute time in
        microseconds of an observation.
      </paragraph>
    </description>
    <units>microseconds</units>
  </field>

  <field name="observationTimeNanoseconds"
    dataType="dateTimeNanoseconds" dataTypeSemantics="quantity"
    elementId="325" status="current" group="timestamps">
    <description>
      <paragraph>
```

```
        This Information Element specifies the absolute time in
        nanoseconds of an observation.
      </paragraph>
    </description>
    <units>nanoseconds</units>
  </field>

  <field name="digestHashValue" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="326" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the value from the digest
        hash function.

        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashIPPayloadOffset" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="327" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the IP payload offset used by
        a Hash-based Selection Selector.

        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashIPPayloadSize" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="328" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the IP payload size used by a
        Hash-based Selection Selector.
        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475]
      </paragraph>
    </description>
  </field>
  <field name="hashOutputRangeMin" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="329" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the value for the beginning
        of a hash function’s potential output range.
        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashOutputRangeMax" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="330" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the value for the end of a
        hash function’s potential output range.

        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashSelectedRangeMin" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="331" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the value for the beginning
        of a hash function’s selected range.

        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashSelectedRangeMax" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="332" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the value for the end of a
        hash function’s selected range.
        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashDigestOutput" dataType="boolean"
    dataTypeSemantics="quantity" elementId="333" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element contains a boolean value that is TRUE
        if the output from this hash Selector has been configured to be
        included in the packet report as a packet digest, else FALSE.

        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="hashInitialiserValue" dataType="unsigned64"
    dataTypeSemantics="quantity" elementId="334" status="current"
    group="hash configuration">
    <description>
      <paragraph>
        This Information Element specifies the initialiser value to the
        hash function.

        See also Sections 6.2, 3.8, and 7.1 of
        [RFC5475].
      </paragraph>
    </description>
  </field>

  <field name="upperCILimit" dataType="float64"
    dataTypeSemantics="quantity" elementId="336" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the upper limit of a
        confidence interval.  It is used to provide an accuracy
        statement for an estimated value.  The confidence limits
        define the range in which the real value is assumed to be
        with a certain probability p.  Confidence limits always need
        to be associated with a confidence level that defines this
        probability p.  Please note that a confidence interval only
        provides a probability that the real value lies within the
        limits.  That means the real value can lie outside the
        confidence limits.

        The upperCILimit, lowerCILimit, and confidenceLevel
        Information Elements should all be used in an Options Template
        scoped to the observation to which they refer.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

        Note that the upperCILimit, lowerCILimit, and confidenceLevel
        are all required to specify confidence, and should be
        disregarded unless all three are specified together.
      </paragraph>
    </description>
    </field>

  <field name="lowerCILimit" dataType="float64"
    dataTypeSemantics="quantity" elementId="337" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the lower limit of a
        confidence interval.  For further information, see the
        description of upperCILimit.

        The upperCILimit, lowerCILimit, and confidenceLevel
        Information Elements should all be used in an Options Template
        scoped to the observation to which they refer.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

        Note that the upperCILimit, lowerCILimit, and confidenceLevel
        are all required to specify confidence, and should be
        disregarded unless all three are specified together.
      </paragraph>
    </description>
  </field>

  <field name="confidenceLevel" dataType="float64"
    dataTypeSemantics="quantity" elementId="338" status="current"
    group="statistics">
    <description>
      <paragraph>
        This Information Element specifies the confidence level.  It is
        used to provide an accuracy statement for estimated values.
        The confidence level provides the probability p with which the
        real value lies within a given range.  A confidence level
        always needs to be associated with confidence limits that
        define the range in which the real value is assumed to be.
        The upperCILimit, lowerCILimit, and confidenceLevel
        Information Elements should all be used in an Options Template
        scoped to the observation to which they refer.
        See Section 3.4.2.1 of the IPFIX protocol document [RFC5101].

        Note that the upperCILimit, lowerCILimit, and confidenceLevel
        are all required to specify confidence, and should be
        disregarded unless all three are specified together.
      </paragraph>
    </description>
  </field>

</fieldDefinitions>
```

Authors’ Addresses

Thomas Dietz
NEC Europe Ltd.
NEC Laboratories Europe
Network Research Division
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342-128
EMail: Thomas.Dietz@nw.neclab.eu
URI: http://www.nw.neclab.eu

Benoit Claise
Cisco Systems, Inc.
De Kleetlaan 6a b1
Degem 1813
Belgium

Phone: +32 2 704 5622
EMail: bclaise@cisco.com

Paul Aitken
Cisco Systems, Inc.
96 Commercial Quay
Edinburgh EH6 6LX
Scotland

Phone: +44 131 561 3616
EMail: paitken@cisco.com
URI: http://www.cisco.com/

Falko Dressler
University of Erlangen-Nuremberg
Dept. of Computer Sciences
Martensstr. 3
Erlangen 91058
Germany

Phone: +49 9131 85-27914
EMail: 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

Phone: +49 89 289-18030
EMail: carle@in.tum.de
URI: http://www.net.in.tum.de/˜carle/