IPFIX Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 25, 2008

E. Boschi
Hitachi Europe
B. Trammell
CERT/NetSA
L. Mark
T. Zseby
Fraunhofer FOKUS

August 24, 2007

# Exporting Type Information for IPFIX Information Elements
## draft-boschi-ipfix-exporting-type-00.txt

Status of this Memo



Copyright Notice



Abstract

This document describes an extension to IPFIX to allow the encoding of IPFIX Information Model properties within an IPFIX Message stream, to allow the export of extended type information for enterprise-specific Information Elements. This format is designed to facilitate

interoperability and reusability among a wide variety of applications and tools.

Table of Contents

## 1. Introduction

The IPFIX protocol specification allows the creation of enterprise-specific Information Elements to easily extend the protocol to meet requirements which aren't covered by the existing Information Model. However, IPFIX Templates provide only the ability to export the size of the fields defined by these Information Elements; there is no mechanism to provide full type information for these Information Elements as is defined for the Information Elements in the IPFIX Information Model.

This limits the interoperability of enterprise-specific Information Elements. It is not possible to use analysis tools on IPFIX records containing these partially defined Information Elements that have not been developed with a priori knowledge of their types, since such tools will not be able to decode them; these tools can only treat and store them as opaque octet arrays. However, if richer information is available, additional operations such as efficient storage, display, and limited analysis of records containing enterprise-specific Information Elements become possible, even for Collecting Processes that had not been specifically developed to understand them.

This document proposes a mechanism to encode the full set of properties available for the definition of Information Elements within the IPFIX Information Model inline within an IPFIX Message stream using IPFIX Options. This mechanism may be used to fully define type information for Information Elements used within a message stream, without resort to an external reference or reliance on out-of-band configuration.

## 2. Terminology

Terms used in this document that are defined in the Terminology section of the IPFIX Protocol [I-D.ietf-ipfix-protocol] document are to be interpreted as defined there.

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].

## 3. Type Information Export

This section describes the mechanism used to encode Information Element type information within an IPFIX Message stream. This mechanism consists of an Options Template Record used to define Information Element type records, and a set of Information Elements

required by these type records. We first specify the necessary Information Elements, followed by the Information Element Type Options Template itself. Note that Information Element type records require one Information Element, informationElementId, that is defined in the PSAMP Information Model [I-D.ietf-psamp-info].

## 3.1. informationElementDataType

Description: A description of the storage type of an IPFIX information element. These correspond to the abstract data types defined in section 3.1 of the IPFIX Information Model [I-D.ietf-ipfix-info]; see that section for more information on the types described below. This field may take the following values:

| Value | Description |
|---|---|
| 0x00 | octetArray |
| 0x01 | unsigned8 |
| 0x02 | unsigned16 |
| 0x03 | unsigned32 |
| 0x04 | unsigned64 |
| 0x05 | signed8 |
| 0x06 | signed16 |
| 0x07 | signed32 |
| 0x08 | signed64 |
| 0x09 | float32 |
| 0x0A | float64 |
| 0x0B | boolean |
| 0x0C | macAddress |
| 0x0D | string |
| 0x0E | dateTimeSeconds |
| 0x0F | dateTimeMilliseconds |
| 0x10 | dateTimeMicroseconds |
| 0x11 | dateTimeNanoseconds |
| 0x12 | ipv4Address |
| 0x13 | ipv6Address |

These types are registered in the IANA IPFIX Information Element Data Type subregistry; new types may be added subject to Expert Review [RFC2434].

Abstract Data Type: unsigned8

ElementId: TBD1

Status: Proposed

Reference: Section 3.1 of the IPFIX Information Model

### 3.2. informationElementDescription

Description: A string containing a human-readable description of an Information Element.

Abstract Data Type: string

Data Type Semantics: identifier

ElementId: TBD2

Status: Proposed

### 3.3. informationElementName

Description: A string containing the name of an Information Element.

Abstract Data Type: string

Data Type Semantics: identifier

ElementId: TBD3

Status: Proposed

### 3.4. informationElementRangeBegin

Description: Contains the inclusive low end of the range of acceptable values for an Information Element. Not valid and SHOULD be ignored by a Collecting Process unless informationElementRangeEnd is also available for the same Information Element.

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: TBD4

Status: Proposed

### 3.5. informationElementRangeEnd

Description: Contains the inclusive high end of the range of acceptable values for an Information Element. Not valid and SHOULD be ignored by a Collecting Process unless informationElementRangeBegin is also available for the same Information Element.

Abstract Data Type: unsigned64

Data Type Semantics: quantity

ElementId: TBD5

Status: Proposed

### 3.6. informationElementSemantics

Description: A description of the semantics of an IPFIX information element. These correspond to the data type semantics defined in section 3.2 of the IPFIX Information Model [I-D.ietf-ipfix-info]; see that section for more information on the types described below. This field may take the following values; the special value 0x00 (none) is used to note that no semantics apply to the field; it cannot be manipulated by a Collecting Process or File Reader that does not understand it a priori.

| Value | Description |
|---|---|
| 0x00 | none |
| 0x01 | quantity |
| 0x02 | totalCounter |
| 0x03 | deltaCounter |
| 0x04 | identifier |
| 0x05 | flags |

These types are registered in the IANA IPFIX Information Element Semantics subregistry; new types may be added subject to Expert Review [RFC2434].

Abstract Data Type: unsigned8

ElementId: TBD6

Status: Proposed

Reference: Section 3.2 of the IPFIX Information Model

### 3.7. informationElementUnits

Description: A description of the units of an IPFIX Information Element. These correspond to the units implicitly defined in the Information Element definitions in section 5 of the IPFIX Information Model [I-D.ietf-ipfix-info]; see that section for more information on the types described below. This field may take the following values; the special value 0x00 (none) is used to note that the field is unitless.

| Value | Name | Notes |
|---|---|---|
| 0x0000 | none | |
| 0x0001 | bits | |
| 0x0002 | octets | |
| 0x0003 | packets | |
| 0x0004 | flows | |
| 0x0005 | seconds | |
| 0x0006 | milliseconds | |
| 0x0007 | microseconds | |
| 0x0008 | nanoseconds | |
| 0x0009 | 4-octet words | for IPv4 header length |
| 0x000A | messages | for reliability reporting |
| 0x000B | hops | for TTL |
| 0x000C | entries | for MPLS label stack |

These types are registered in the IANA IPFIX Information Element Units subregistry; new types may be added on a First Come First Served [RFC2434] basis.

Abstract Data Type: unsigned16

ElementId: TBD7

Status: Proposed

Reference: Section 5 of the IPFIX Information Model

### 3.8. privateEnterpriseNumber

Description: A private enterprise number used to scope an informationElementID, as would appear in an IPFIX Template Record. This element can be used to scope properties to a specific Information Element. If the Enterprise ID bit of the corresponding Information Element is cleared (has the value 0), this IE should be set to 0. The presence of a non-zero value in this IE implies that the Enterprise ID bit of the corresponding Information Element is set (has the value 1).

Abstract Data Type: unsigned32

Data Type Semantics: identifier

ElementId: TBD8

Status: Proposed

Reference: Section 3.4.1 of the IPFIX Protocol draft

### 3.9. Information Element Type Options Template

The Information Element Type Options Template attaches type information to Information Elements used within Template Records, as scoped to an Observation Domain within a Transport Session. This provides a mechanism for representing an IPFIX Information Model inline within an IPFIX Message stream. Data Records described by this template are referred to as Information Element type records.

In deployments in which interoperability across vendor implementations of IPFIX is important, an Exporting Process exporting data using Templates containing enterprise-specific Information Elements SHOULD export an Information Element type record for each enterprise-specific Information Element it exports. Collecting Processes MAY use these type records to improve handling of unknown enterprise-specific Information Elements. Exporting Processes using enterprise-specific Information Elements to implement proprietary features MAY omit type records for those Information Elements.

Information Element type records MUST be handled by Collecting Processes as scoped to the Transport Session in which they are sent; this facility is not intended to provide a method for the permanent definition of Information Elements.

Similarly, for security reasons, type information for a given Information Element MUST NOT be re-defined by Information Element type records. Once an Information Element type record has been

exported for a given Information Element within a given Transport Session, all subsequent type records for that Information Element MUST be identical. If conflicting semantic or type information is received in multiple semantics records by a Collecting Process, the Collecting Process MUST reset the Transport Session.

The template SHOULD contain the following Information Elements as defined in the PSAMP Information Model [I-D.ietf-psamp-info] and in this document, above:

| IE | Description |
|---|---|
| informationElementID | The Information Element identifier of the Information Element within the specified Template this record describes. This Information Element MUST be defined as a Scope Field. See the PSAMP Information Model [I-D.ietf-psamp-info] for a definition of this field. |
| privateEnterpriseNumber | The Private Enterprise number of the Information Element within the specified Template this record describes. This Information Element MUST be defined as a Scope Field. |
| informationElementDataType | The storage type of the specified Information Element. |
| informationElementSemantics | The semantic type of the specified Information Element. |
| informationElementUnits | The units of the specified Information Element. This element MAY be omitted if the Information Element is a unitless quantity, or a not a quantity or counter. |
| informationElementRangeBegin | The low end of the range of acceptable values for the specified Information Element. This element MAY be omitted if the Information Element's acceptable range is defined by its data type. |

| informationElementRangeEnd | The high end of the range of acceptable values for the specified Information Element. This element MAY be omitted if the Information Element's acceptable range is defined by its data type. |
|---|---|
| informationElementName | The name of the specified Information Element. |
| informationElementDescription | A human readable description of the specified Information Element. This element MAY be omitted in the interest of export efficiency. |

## 4. Security Considerations

The same security considerations as for the IPFIX Protocol [I-D.ietf-ipfix-protocol] apply.

## 5. IANA Considerations

This document specifies the creation of several new IPFIX Information Elements in the IPFIX Information Element registry located at http://www.iana.org/assignments/ipfix, as defined in section 3 above. IANA has assigned the following Information Element numbers for their respective Information Elements as specified below:

- Information Element Number TBD1 for the informationElementDataType Information Element
- Information Element Number TBD2 for the informationElementDescription Information Element
- Information Element Number TBD3 for the informationElementName Information Element
- Information Element Number TBD4 for the informationElementRangeBegin Information Element
- Information Element Number TBD5 for the informationElementRangeEnd Information Element
- Information Element Number TBD6 for the informationElementSemantics Information Element

- Information Element Number TBD7 for the informationElementUnits Information Element

- Information Element Number TBD8 for the privateEnterpriseNumber Information Element

- [NOTE for IANA: The text TBD1, TBD2, TBD3, TBD4, TBD5, TBD6, TBD7, and TBD8 should be replaced with the respective assigned Information Element numbers where they appear in this document.]

IANA has created an Information Element Data Type subregistry for the values defined for the informationElementSemantics Information Element. Entries may be added to this subregistry subject to Expert Review [RFC2434].

[NOTE for IANA: Please create a new Information Element Data Type subregistry as specified in the paragraph above, with initial values taken from section 3.1 of this document.]

IANA has created an Information Element Semantics subregistry for the values defined for the informationElementSemantics Information Element. Entries may be added to this subregistry subject to Expert Review [RFC2434].

[NOTE for IANA: Please create a new Information Element Semantics subregistry as specified in the paragraph above, with initial values taken from section 3.6 of this document.]

IANA has created an Information Element Units subregistry for the values defined for the informationElementUnits Information Element. Entries may be added to this subregistry on a First Come First Served [RFC2434] basis.

[NOTE for IANA: Please create a new Information Element Units subregistry as specified in the paragraph above, with initial values taken from section 3.7 of this document.]

## 6. Acknowledgements

Thanks to Paul Aitken for the detailed technical review, and to David Moore for first raising this issue to the IPFIX mailing list.

## 7. References

## 7.1. Normative References

[I-D.ietf-ipfix-protocol]
Claise, B., "Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information", draft-ietf-ipfix-protocol-25 (work in progress), August 2007.

[I-D.ietf-ipfix-info]
Quittek, J., "Information Model for IP Flow Information Export", draft-ietf-ipfix-info-15 (work in progress), February 2007.

[I-D.ietf-psamp-info]
Dietz, T., "Information Model for Packet Sampling Exports", draft-ietf-psamp-info-06 (work in progress), June 2007.

## 7.2. Informative References

[I-D.ietf-ipfix-biflow]
Trammell, B. and E. Boschi, "Bidirectional Flow Export using IPFIX", draft-ietf-ipfix-biflow-05 (work in progress), June 2007.

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

## Appendix A. Examples

The following example illustrates how the type information extension mechanism defined in this document may be used to describe the semantics of enterprise-specific Information Elements. The Information Elements used in this example are as follows:

- initialTCPFlags, CERT (PEN 6871) private IE 14, 1 octet, the TCP flags on the first TCP packet in the flow.

- unionTCPFlags, CERT (PEN 6871) private IE 15, 1 octet, the union of the TCP flags on all packets after the first TCP packet in the flow.

An Exporting Process exporting flows containing these Information

Elements might use a Template like the following:

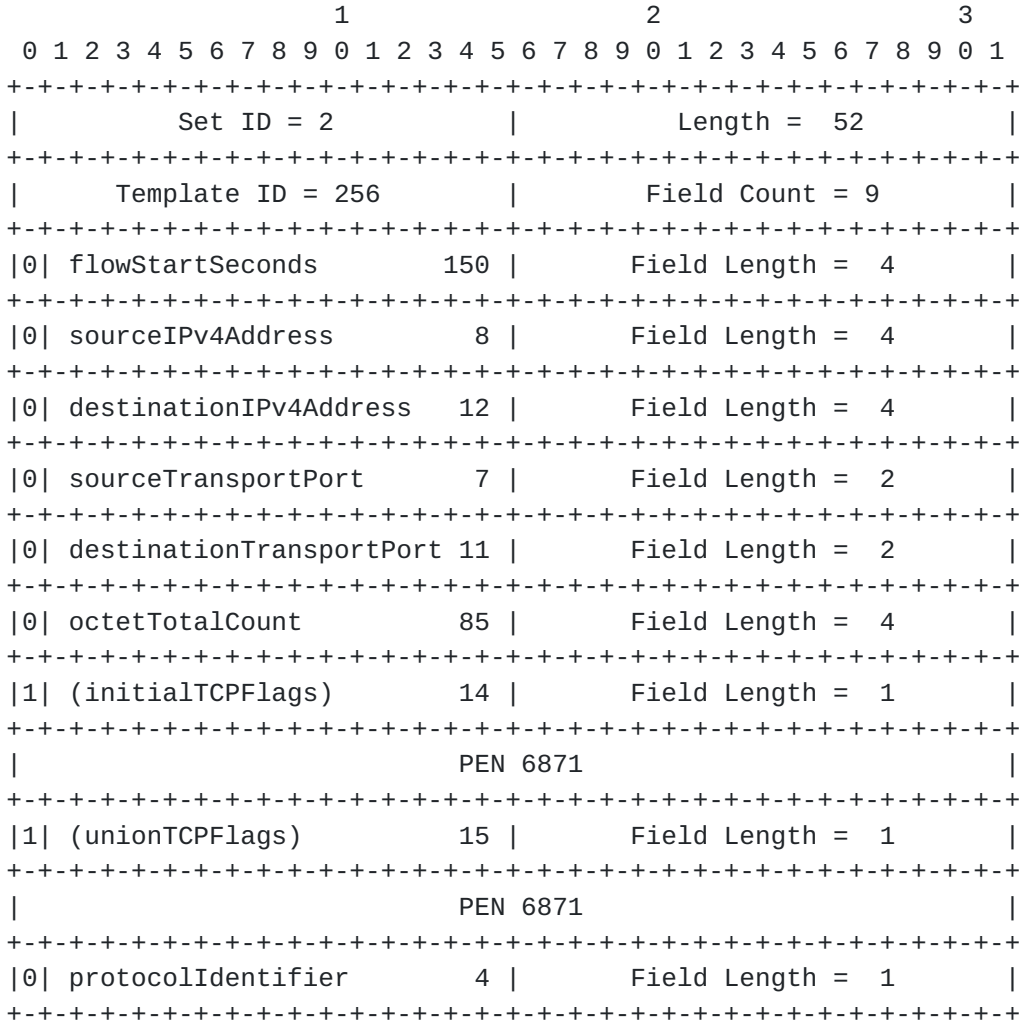


Figure 1: Template with Enterprise-Specific IEs

However, a Collecting Process receiving Data Sets described by this Template can only treat the enterprise-specific Information Elements as opaque octets; specifically, there is no hint to the collector that they contain flag information. To use the type information extension mechanism to address this problem, the Exporting Process would first export the Information Element Type Options Template described in section 3.9 above:

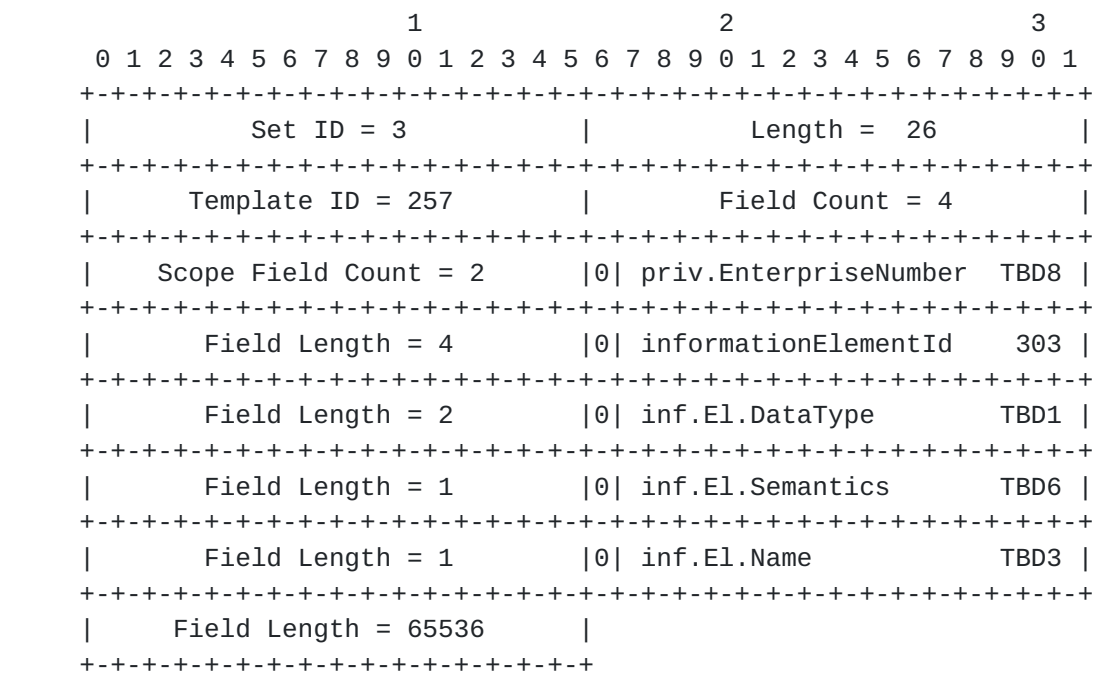


Figure 2: Example Information Element Type Options Template

Then, the Exporting Process would then export two records described by the Example Information Element Type Options Template to describe the enterprise-specific Information Elements:


Figure 3: Type Information Extension Example

## Authors' Addresses

Elisa Boschi
Hitachi Europe SAS
Immeuble Le Theleme
1503 Route des Dolines
06560 Valbonne
France

Phone: +33 4 89874100
Email: elisa.boschi@hitachi-eu.com

Brian H. Trammell
CERT Network Situational Awareness
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, Pennsylvania 15213
United States

Phone: +1 412 268 9748
Email: bht@cert.org

Lutz Mark
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

Phone: +49 30 3463 7306
Email: lutz.mark@fokus.fraunhofer.de

Tanja Zseby
Fraunhofer Institute for Open Communication Systems
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

Phone: +49 30 3463 7153
Email: tanja.zseby@fokus.fraunhofer.de

## Full Copyright Statement



## Intellectual Property



## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).