Internet Engineering Task Force (IETF)
Request for Comments: 6183
Updates: 5470
Category: Informational
ISSN: 2070-1721

A. Kobayashi
NTT
B. Claise
Cisco Systems, Inc.
G. Muenz
TU Muenchen
K. Ishibashi
NTT

April 2011

IP Flow Information Export (IPFIX) Mediation: Framework

Abstract

This document describes a framework for IP Flow Information Export (IPFIX) Mediation. This framework extends the IPFIX reference model specified in RFC 5470 by defining the IPFIX Mediator components.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The IP Flow Information Export (IPFIX) architectural components in [RFC5470] consist of IPFIX Devices and IPFIX Collectors communicating using the IPFIX protocol. Due to the sustained growth of IP traffic in heterogeneous network environments, this Exporter-Collector architecture may lead to scalability problems. In addition, it does not provide the flexibility required by a wide variety of measurement applications. A detailed descriptions of these problems is given in [RFC5982].

To fulfill application requirements with limited system resources, the IPFIX architecture needs to introduce an intermediate entity between Exporters and Collectors. From a data manipulation point of view, this intermediate entity may provide the aggregation, correlation, filtering, and modification of Flow Records and/or Packet Sampling (PSAMP) Packet Reports to save measurement system resources and to perform preprocessing tasks for the Collector. From a protocol conversion point of view, this intermediate entity may provide conversion into IPFIX, or conversion of IPFIX transport protocols (e.g., from UDP to the Stream Control Transmission Protocol (SCTP)) to improve the export reliability.

This document introduces a generalized concept for such intermediate entities and describes the high-level architecture of IPFIX Mediation, key IPFIX Mediation architectural components, and characteristics of IPFIX Mediation.

This document is structured as follows: Section 2 describes the terminology used in this document, Section 3 gives an IPFIX/PSAMP document overview, Section 4 describes a high-level reference model, Section 5 describes functional features related to IPFIX Mediation, Section 6 describes combinations of components along with some application examples, Section 7 describes consideration points of the encoding for IPFIX Message Headers, Section 8 describes the Information Elements used in an IPFIX Mediator, and Section 9 describes the security issues raised by IPFIX Mediation.

2. Terminology and Definitions

The IPFIX-specific and PSAMP-specific terminology used in this document is defined in [RFC5101] and [RFC5476], respectively. The IPFIX-Mediation-specific terminology used in this document is defined in [RFC5982]. However, as reading the problem statements document is not a prerequisite to reading this framework document, the definitions have been reproduced here along with additional definitions. In this document, as in [RFC5101] and [RFC5476], the first letter of each IPFIX-specific and PSAMP-specific term is capitalized along with the IPFIX-Mediation-specific terms defined here. The use of the terms "must", "should", and "may" in this document is informational only.

In this document, we use the term "record stream" to mean a stream of records carrying flow-based or packet-based information. The records may be encoded as IPFIX Data Records or in any other format.

Transport Session Information

The Transport Session Information contains information that allows the identification of an individual Transport Session as defined in [RFC5101]. If SCTP is used as transport protocol, the Transport Session Information identifies the SCTP association. If TCP or UDP is used as transport protocol, the Transport Session Information corresponds to the 5-tuple {Exporter IP address, Collector IP address, Exporter transport port, Collector transport port, transport protocol}. The Transport Session Information may include further details about how Transport Layer Security (TLS) [RFC5246] or Datagram Transport Layer Security (DTLS) [RFC4347] is used for encryption and authentication.

Original Exporter

An Original Exporter is an IPFIX Device that hosts the Observation Points where the metered IP packets are observed.

IPFIX Mediation

IPFIX Mediation is the manipulation and conversion of a record stream for subsequent export using the IPFIX protocol.

The following terms are used in this document to describe the architectural entities used by IPFIX Mediation.

Intermediate Process

An Intermediate Process takes a record stream as its input from Collecting Processes, Metering Processes, IPFIX File Readers, other Intermediate Processes, or other record sources; performs some transformations on this stream based upon the content of each record, states maintained across multiple records, or other data sources; and passes the transformed record stream as its output to Exporting Processes, IPFIX File Writers, or other Intermediate Processes in order to perform IPFIX Mediation. Typically, an Intermediate Process is hosted by an IPFIX Mediator. Alternatively, an Intermediate Process may be hosted by an Original Exporter.

Specific Intermediate Processes are described below. However, this is not an exhaustive list.

Intermediate Conversion Process

An Intermediate Conversion Process is an Intermediate Process that transforms non-IPFIX into IPFIX or manages the relation among Templates and states of incoming/outgoing transport sessions in the case of transport protocol conversion (e.g., from UDP to SCTP).

Intermediate Aggregation Process

An Intermediate Aggregation Process is an Intermediate Process that aggregates records based upon a set of Flow Keys or functions applied to fields from the record (e.g., data binning and subnet aggregation).

Intermediate Correlation Process

An Intermediate Correlation Process is an Intermediate Process that adds information to records, noting correlations among them, or generates new records with correlated data from multiple records (e.g., the production of bidirectional flow records from unidirectional flow records).

Intermediate Selection Process

An Intermediate Selection Process is an Intermediate Process that selects records from a sequence based upon criteria-evaluated record values and passes only those records that match the criteria (e.g., filtering only records from a given network to a given Collector).

Intermediate Anonymization Process

An Intermediate Anonymization Process is an Intermediate Process that transforms records in order to anonymize them, to protect the identity of the entities described by the records (e.g., by applying prefix-preserving pseudonymization of IP addresses).

IPFIX Mediator

An IPFIX Mediator is an IPFIX Device that provides IPFIX Mediation by receiving a record stream from some data sources, hosting one or more Intermediate Processes to transform that stream, and exporting the transformed record stream into IPFIX Messages via an Exporting Process. In the common case, an IPFIX Mediator receives a record stream from a Collecting Process, but it could also receive a record stream from data sources not encoded using IPFIX, e.g., in the case of conversion from the NetFlow V9 protocol [RFC3954] to the IPFIX protocol.

Note that the IPFIX Mediator is a generalization of the concentrator and proxy elements envisioned in the IPFIX requirements [RFC3917]. IPFIX Mediators running appropriate Intermediate Processes provide the functionality specified therein.

3. IPFIX/PSAMP Documents Overview

IPFIX Mediation can be applied to flow-based or packet-based information. The flow-based information is encoded as IPFIX Flow Records by the IPFIX protocol, and the packet-based information is extracted by some packet selection techniques and then encoded as PSAMP Packet Reports by the PSAMP protocol. Thus, this section describes relevant documents for both protocols.

3.1. IPFIX Documents Overview

The IPFIX protocol [RFC5101] provides network administrators with access to IP Flow information. The architecture for the export of measured IP Flow information from an IPFIX Exporting Process to a Collecting Process is defined in [RFC5470], per the requirements defined in [RFC3917]. The IPFIX protocol [RFC5101] specifies how IPFIX Data Records and Templates are carried via a number of transport protocols from IPFIX Exporting Processes to IPFIX Collecting Processes. IPFIX has a formal description of IPFIX Information Elements, their names, types, and additional semantic information, as specified in [RFC5102]. The IPFIX Management Information Base is defined in [RFC5815]. Finally, [RFC5472] describes what types of applications can use the IPFIX protocol and how they can use the information provided. Furthermore, it shows how the IPFIX framework relates to other architectures and frameworks. The storage of IPFIX Messages in a file is specified in [RFC5655].

3.2. PSAMP Documents Overview

The framework for packet selection and reporting [RFC5474] enables 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. The set of packet selection techniques (Sampling and Filtering) standardized by PSAMP is described in [RFC5475]. The PSAMP protocol [RFC5476] specifies the export of packet information from a PSAMP Exporting Process to a Collector. Like IPFIX, PSAMP has a formal description of its Information

Elements, their names, types, and additional semantic information. The PSAMP information model is defined in [RFC5477]. The PSAMP Management Information Base is described in [PSAMP-MIB].

4. IPFIX Mediation Reference Model

Figure A shows the high-level IPFIX Mediation reference model as an extension of the IPFIX reference model presented in [RFC5470]. This figure covers the various possible scenarios that can exist in an IPFIX measurement system.

```
       +----------------+  +---------------+    +---------------+
       | Collector 1    |  | Collector 2   |    | Collector N   |
       |[Collecting     |  |[Collecting    |    |[Collecting    |
       |   Process(es)] |  |  Process(es)] |... |  Process(es)] |
       +----^-----------+  +---^--------^--+    +--------^------+
            |                 /          \               |
            |                /            \              |
     Flow Records     Flow Records   Flow Records   Flow Records
            |              /               \            |
     +------+-------------+------+    +------+-----------+--------+
     |IPFIX Mediator N+1         |    |IPFIX Mediator Z           |
     |[Exporting Process(es)]    |    |[Exporting Process(es)]    |
     |[Intermediate Process(es)] |    |[Intermediate Process(es)] |
     |[Collecting Process(es)]   |... |[Collecting Process(es)]   |
     +----^----------------^-----+    +------^----------------^---+
          |                |                 |                |
     Flow Records     Flow Records      Packet Reports  record stream
          |                |                 |                |
   +------+------+  +------+-------+  +------+-------+  +-----+-----+
   |IPFIX        |  |IPFIX Original|  |PSAMP Original|  |Other      |
   |  Mediator 1 |  |   Exporter 1 |  |   Exporter 1 |  |  Source 1 |
   |+-------------+ |+--------------+ |+--------------+ |+-----------+
   +|IPFIX        | +|IPFIX Original| +|PSAMP Original| +|Other      |
    |  Mediator N |  |   Exporter N |  |   Exporter N |  |  Source N |
    |[Exporting   |  |[Exporting    |  |[Exporting    |  |           |
    | Process(es)]|  |  Process(es)]|  |  Process(es)]|  |           |
    |[Intermediate|  |[Metering     |  |[Metering     |  |           |
    | Process(es)]|  |  Process(es)]|  |  Process(es)]|  |           |
    |[Collecting  |  |[Observation  |  |[Observation  |  |           |
    | Process(es)]|  |     Point(s)]|  |     Point(s)]|  |           |
    +------^------+  +-----^-^------+  +-----^-^------+  +-----------+
           |               | |               | |
      Flow Records   Packets coming    Packets coming
                    into Observation  into Observation
                          Points            Points
```

Figure A: IPFIX Mediation Reference Model Overview

The functional components within each entity are indicated within brackets []. An IPFIX Mediator receives IPFIX Flow Records or PSAMP Packet Reports from other IPFIX Mediators, IPFIX Flow Records from IPFIX Original Exporters, PSAMP Packet Reports from PSAMP Original Exporters, and/or a record stream from other sources. The IPFIX Mediator then exports IPFIX Flow Records and/or PSAMP Packet Reports to one or multiple Collectors and/or other IPFIX Mediators.

Figure B shows the basic IPFIX Mediator component model. An IPFIX Mediator contains one or more Intermediate Processes and one or more Exporting Processes. Typically, it also contains a Collecting Process but might contain several Collecting Processes, as described in Figure B.

```
                  IPFIX (Data Records)
                              ^
                            ^ |
   +------------------------|-|---------------------+
   | IPFIX Mediator         | |                     |
   |                        | |                     |
   |  .---------------------|-+-------------------. |
   | .----------------------+--------------------.| |
   | |          Exporting Process(es)            |' |
   | '----------------------^--------------------'  |
   |                        | |                     |
   |  .---------------------|-+-------------------. |
   | .----------------------+--------------------.| |
   | |          Intermediate Process(es)         |' |
   | '----------------------^--------------------'  |
   |                        | |                     |
   |  .---------------------|-+-------------------. |
   | .----------------------+--------------------.| |
   | |          Collecting Process(es)           |' |
   | '----------------------^--------------------'  |
   +------------------------|-|---------------------+
                            |
                  IPFIX (Data Records)
```

Figure B: Basic IPFIX Mediator Component Model

However, other data sources are also possible: an IPFIX Mediator can receive a record stream from non-IPFIX protocols such as NetFlow [RFC3954] exporter(s). This document does not make any particular assumption on how a record stream is transferred to an IPFIX Mediator. Figure C shows the IPFIX Mediator component model in the case of IPFIX protocol conversion from non-IPFIX exporters.

```
                  IPFIX (Data Records)
                              ^
                            ^ |
   +------------------------|-|---------------------+
   | IPFIX Mediator         | |                     |
   |  .---------------------|-+-------------------. |
   | .----------------------+--------------------.| |
   | |          Exporting Process(es)            |' |
   | '----------------------^--------------------'  |
   |  .---------------------|-+-------------------. |
   | .----------------------+--------------------.| |
   | |          Intermediate Process(es)         |' |
   | '----------------------^--------------------'  |
   +------------------------|-----------------------+
                            | record stream
   +------------------------|-----------------------+
   | Non-IPFIX exporter     |                       |
   |          +-------------+----------+            |
   |          |                        |            |
   +----------|------------------------|------------+
              |                        |
            Packets coming into observation points
```

Figure C: IPFIX Mediator Component Model in IPFIX
Protocol Conversion

Alternatively, an Original Exporter may provide IPFIX Mediation by hosting one or more Intermediate Processes. The component model in Figure D adds Intermediate Process(es) to the IPFIX Device model illustrated in [RFC5470]. In comparison with Figures 1 or 2 in [RFC5470], the Intermediate Process is located between Exporting Process(es) and IPFIX or PSAMP Metering Process(es).

```
                     IPFIX (Data Records)
                               ^ ^
   +---------------------------|-|------------------------+
   | Original Exporter         | |                        |
   |                           | |                        |
   |     .---------------------|-+-------------------.    |
   |    .----------------------+--------------------.|    |
   |    |           Exporting Process(es)           |'    |
   |    '----------------------^--------------------'     |
   |                           | |                        |
   |     .---------------------|-+-------------------.    |
   |    .----------------------+--------------------.|    |
   |    |          Intermediate Process(es)         |'    |
   |    '---------^-----------------------^---------'     |
   |              |      Data Records     |               |
   |   .----------+---------.   .---------+----------.    |
   |   | Metering Process 1 |...| Metering Process N |    |
   |   '----------^---------'   '---------^----------'    |
   |              |                       |               |
   |  .-----------+---------.   .---------+-----------.   |
   |  | Observation Point 1 |...| Observation Point N |   |
   |  '-----------^---------'   '---------^-----------'   |
   +--------------|-----------------------|---------------+
                  |                       |
            Packets coming into Observation Points
```

Figure D: IPFIX Mediation Component Model at Original Exporter

In addition, an Intermediate Process may be collocated with an IPFIX File Reader and/or Writer. Figure E shows an IPFIX Mediation component model with an IPFIX File Writer and/or Reader.

```
                   IPFIX (Data Records)
                               ^
                             ^ |
      .----------------------|-+--------------------.
     .-----------------------+---------------------.|
     |              IPFIX File Writer              |'
     '-----------------------^---------------------'
                             | |
      .----------------------|-+--------------------.
     .-----------------------+---------------------.|
     |          Intermediate Process(es)           |'
     '-----------------------^---------------------'
                             | |
      .----------------------|-+--------------------.
     .-----------------------+---------------------.|
     |              IPFIX File Reader              |'
     '-----------------------^---------------------'
                             |
                   IPFIX (Data Records)
```

Figure E: IPFIX Mediation Component Model Collocated
with IPFIX File Writer/Reader

5. IPFIX Mediation Functional Blocks

Figure F shows a functional block diagram example in an IPFIX Mediator that has different Intermediate Process types.

```
                         IPFIX           IPFIX               IPFIX
                           ^               ^                   ^
                           |               |                   |
     .------------.  .-----+-------. .-----+-------.    .------+------.
     | IPFIX File |  | Exporting   | | Exporting   |    | Exporting   |
     | Writer     |  | Process 1   | | Process 2   |....| Process N   |
     '-----^-^----'  '-----^-------' '-----^-------'    '------^------'
           | |             |               |                   |
           | +-------------+               |                   |
           :          Flow Records / Packet Reports            :
    .------+-------. .-----+--------. .----+---------. .--------------.
    | Intermediate | | Intermediate | | Intermediate | | Intermediate |
    | Anonymization| | Correlation  | | Aggregation  | | Selection    |
    | Process N    | | Process N    | | Process N    | | Process N    |
    '------|-------' '------|-------' '-----|-|------' '-------|------'
           |                +---------------+ |                |
           :                :                 :                :
    .------+-------. .------+-------. .-------+------. .-------+------.
    | Intermediate | | Intermediate | | Intermediate | | Intermediate |
    | Selection    | | Selection    | | Selection    | | Selection    |
    | Process 1    | | Process 2    | | Process 3    | | Process 4    |
    '------|-|-----' '------|-------' '-----|--------' '-------|------'
           | +--------------+               | +----------------+
           |                |               | |                |
           :          Flow Records / Packet Reports            :
    .------+------. .-------+-----.   .-----+-+-----.    .-----+------.
    | Collecting  | | Collecting  |   | Collecting  |    | IPFIX File |
    | Process 1   | | Process 2   |...| Process N   |    | Reader     |
    '------^------' '------^------'   '------^------'    '------------'
           |               |                 |
      Flow Records   Flow Records      Flow Records
```

Figure F: IPFIX Mediation Functional Block Diagram

5.1. Collecting Process

A Collecting Process in an IPFIX Mediator is not different from the Collecting Process described in [RFC5101]. Additional functions in an IPFIX Mediator include transmitting the set of Data Records and Control Information to one or more components, i.e., Intermediate Processes and other applications. In other words, a Collecting Process may duplicate the set and transmit it to one or more components in sequence or in parallel. In the case of an IPFIX

Mediator, the Control Information described in [RFC5470] includes IPFIX Message Header information and Transport Session Information along with information about the Metering Process and the Exporting Process in an Original Exporter, e.g., Sampling parameters.

5.2. Exporting Process

An Exporting Process in an IPFIX Mediator is not different from the Exporting Process described in [RFC5101]. Additional functions in an IPFIX Mediator may include the following:

- o Receiving the trigger to transmit the Template Withdrawal Messages from Intermediate Process(es) when relevant Templates become invalid due to, for example, incoming session failure.
- o Transmitting the origin (e.g., Observation Point, Observation Domain ID, Original Exporter IP address, etc.) of the data in additional Data Record fields or additional Data Records. The parameters that represent the origin should be configurable.

5.3. Intermediate Process

An Intermediate Process is a key functional block for IPFIX Mediation. Its typical functions include the following:

- o Generating a new record stream from an input record stream including context information (e.g., Observation Domain ID and Transport Session Information) and transmitting it to other components.
- o Reporting statistics and interpretations for IPFIX Metering Processes, PSAMP Metering Processes, and Exporting Processes from an Original Exporter. See Section 4 of [RFC5101] and Section 6 of [RFC5476] for relevant statistics data structures and interpretations, respectively. Activation of this function should be configurable.
- o Maintaining the configurable relation between Collecting Process(es)/Metering Process(es) and Exporting Process(es)/other Intermediate Process(es).
- o Maintaining database(s) of Data Records in the case of an Intermediate Aggregation Process and an Intermediate Correlation Process. The function has the Data Record expiration rules described in the next subsection.
- o Maintaining statistics on the Intermediate Process itself, such as the number of input/output Data Records, etc.

- Maintaining additional information about output record streams, which includes information related to the Original Exporters, Observation Domain, and administrative domain as well as some configuration parameters related to each function.

In the case of an Intermediate Aggregation Process, Intermediate Anonymization Process, and Intermediate Correlation Process, the value of the "flowKeyIndicator" needs to be modified when modifying the data structure defined by an original Template.

For example, an Intermediate Aggregation Process aggregating incoming Flow Records composed of the sourceIPv4Address and destinationIPv4Address Flow Keys into outgoing Flow Records with the destinationIPv4Address Flow Key must modify the incoming flowKeyIndicator to contain only the destinationIPv4Address.

5.3.1. Data Record Expiration

An Intermediate Aggregation Process and Intermediate Correlation Process need to have expiration conditions to export cached Data Records. In the case of the Metering Process in an Original Exporter, these conditions are described in [RFC5470]. In the case of the Intermediate Process, these conditions are as follows:

- If there are no input Data Records belonging to a cached Flow for a certain time period, aggregated Flow Records will expire. This time period should be configurable at the Intermediate Process.

- If the Intermediate Process experiences resource constraints (e.g., lack of memory to store Flow Records), aggregated Flow Records may prematurely expire.

- For long-running Flows, the Intermediate Process should cause the Flow to expire on a regular basis or on the basis of an expiration policy. This periodicity or expiration policy should be configurable at the Intermediate Process.

In the case of an Intermediate Correlation Process, a cached Data Record may be prematurely expired (and discarded) when no correlation can be computed with newly received Data Records. For example, an Intermediate Correlation Process computing one-way delay may discard the cached Packet Report when no other matching Packet Report are observed within a certain time period.

5.3.2. Specific Intermediate Processes

This section describes the functional blocks of specific Intermediate Processes.

5.3.2.1. Intermediate Conversion Process

When receiving a non-IPFIX record stream, the Intermediate Conversion Process covers the following functions:

- Determining the IPFIX Information Element identifiers that correspond to the fields of the non-IPFIX records (e.g., converting the NetFlow V9 protocol [RFC3954] to the IPFIX Information Model [RFC5102]).

- Transforming the non-IPFIX records into Data Records, (Options) Template Records, and/or Data Records defined by Options Templates.

- Converting additional information (e.g., sampling rate, sampling algorithm, and observation information) into appropriate fields in the existing Data Records or into Data Records defined by new Options Templates.

IPFIX transport protocol conversion can be used to enhance the export reliability, for example, for data retention and accounting. In this case, the Intermediate Conversion Process covers the following functions:

- Relaying Data Records, (Options) Template Records, and Data Records defined by Options Templates.

- Setting the trigger for the Exporting Process in order to export IPFIX Template Withdrawal Messages relevant to the Templates when Templates becomes invalid due to, for example, incoming session failure. This case applies to SCTP and TCP Transport Sessions on the outgoing side only.

- Maintaining the mapping information about Transport Sessions, Observation Domain IDs, and Template IDs on the incoming and outgoing sides in order to ensure the consistency of scope field values of incoming and outgoing Data Records defined by Options Templates and of Template IDs of incoming and outgoing IPFIX Template Withdrawal Messages.

5.3.2.2. Intermediate Selection Process

An Intermediate Selection Process has analogous functions to the PSAMP Selection Process described in [RFC5475]. The difference is that the Intermediate Selection Process takes a record stream, e.g., Flow Records or Packet Reports, instead of observed packets as its input.

The typical function is property match filtering that retrieves a record stream of interest. The function selects a Data Record if the value of a specific field in the Data Record equals a configured value or falls within a configured range.

5.3.2.3. Intermediate Aggregation Process

An Intermediate Aggregation Process covers the following functions:

- Merging a set of Data Records within a certain time period into one Flow Record by summing up the counters where appropriate.

- Maintaining statistics and additional information about aggregated Flow Records.

  The statistics for an aggregated Flow Record may include the number of original Data Records and the maximum and minimum values of per-flow counters. Additional information may include an aggregation time period, a new set of Flow Keys, and observation location information involved in the Flow aggregation. Observation location information can be tuples of (Observation Point, Observation Domain ID, Original Exporter IP address) or another identifier indicating the location where the measured traffic has been observed.

- Aggregation of Data Records, which can be done in the following ways:

  * Spatial composition

    With spatial composition, Data Records sharing common properties are merged into one Flow Record within a certain time period. One typical aggregation can be based on a new set of Flow Keys. Generally, a set of common properties smaller than an original set of Flow Keys results in a higher level of aggregation. Another aggregation can be based on a set of Observation Points within an Observation Domain, on a set of Observation Domains within an Exporter, or on a set of Exporters.

    If some fields do not serve as Flow Keys or per-Flow counters, their values may change from Data Records to Data Records within an aggregated Flow Record. The Intermediate Aggregation Process determines their values by the first Data Record received, a specific Exporter IP address, or other appropriate decisions.

Furthermore, a new identifier indicating a group of observation locations can be introduced, for example, to indicate PoPs (Points of Presence) in a large network, or a logical interface composed of physical interfaces with link aggregation.

* Temporal composition

  With temporal composition, multiple Flow Records with identical Flow Key values are merged into a single Flow Record of longer Flow duration if they arrive within a certain time interval. The main difference to spatial composition is that Flow Records are only merged if they originate from the same Observation Point and if the Flow Key values are identical. For example, multiple Flow Records with a Flow duration of less than one minute can be merged into a single Flow Record with more than ten minutes Flow duration.

  In addition, the Intermediate Aggregation Process with temporal composition produces aggregated counters while reducing the number of Flow Records on a Collector. Some specific non-key fields, such as the minimumIpTotalLength/maximumIpTotalLength or minimumTTL/maximumTTL, will contain the minimum and maximum values for the new aggregated Flow.

Spatial and temporal composition can be combined in a single Intermediate Aggregation Process. The Intermediate Aggregation Process can be combined with the Intermediate Selection Process in order to aggregate only a subset of the original Flow Records, for example, Flow Records with small numbers of packets as described in Section 6.2.

5.3.2.4. Intermediate Anonymization Process

An Intermediate Anonymization Process covers the following typical functions:

o Deleting specified fields

  The function deletes existing fields in accordance with some instruction rules. Examples include hiding network topology information and private information. In the case of feeding Data Records to end customers, disclosing vulnerabilities is avoided by deleting fields, e.g., "ipNextHopIP{v4|v6}Address", "bgpNextHopIP{v4|v6}Address", "bgp{Next|Prev}AdjacentAsNumber", and "mplsLabelStackSection", as described in [RFC5102].

- Anonymizing values of specified fields

  The function modifies the values of specified fields. Examples include anonymizing customers’ private information, such as IP address and port number, in accordance with a privacy protection policy. The Intermediate Anonymization Process may also report anonymized fields and the anonymization method as additional information.

5.3.2.5. Intermediate Correlation Process

An Intermediate Correlation Process can be viewed as a special case of the Intermediate Aggregation Process, covering the following typical functions:

- Producing new information including metrics, counters, attributes, or packet property parameters by evaluating the correlation among sets of Data Records or among Data Records and other meta data after gathering sets of Data Records within a certain time period.

- Adding new fields into a Data Record or creating a new Data Record.

A correlation of Data Records can be done in the following ways, which can be implemented individually or in combinations.

- One-to-one correlation between Data Records, with the following examples:

  * One-way delay, Packet delay variation in [RFC5481]
    The metrics come from the correlation of the timestamp value on a pair of Packet Reports indicating an identical packet at different Observation Points in the network.

  * Packet inter-arrival time
    The metrics come from the correlation of the timestamp value on consecutive Packet Reports from a single Exporter.

  * Rate-limiting ratio, compression ratio, optimization ratio, etc.
    The data values come from the correlation of Data Records indicating an identical Flow observed on the incoming/outgoing points of a WAN interface.

- Correlation amongst Data Records, with the following examples:

  - Bidirectional Flow composition
    The method of exporting and representing a Bidirectional Flow (Biflow) is described in [RFC5103]. The Bidirectional Flow composition is a special case of Flow Key aggregation. The Flow Records are merged into one Flow Record as Biflow if Non-directional Key Fields match and the Directional Key Fields match their reverse direction counterparts. The direction assignment method to assign the Biflow Source and Destination as additional information may be reported. In the case of an Intermediate Aggregation Process, the direction may be assigned arbitrarily (see [RFC5103], Section 5.3).

  - Average/maximum/minimum for packets, bytes, one-way delay, packet loss, etc.
    The data values come from the correlation of multiple Data Records gathered in a certain time interval.

- Correlation between Data Record and other meta data

  Typical examples are derived packet property parameters described in [RFC5102]. The parameters are retrieved based on the value of the specified field in an input Data Record, compensating for traditional exporting devices or probes that are unable to add packet property parameters. Typical derived packet property parameters are as follows:

  - "bgpNextHop{IPv4|IPv6}Address" described in [RFC5102]
    This value indicates the egress router of a network domain. It is useful for making a traffic matrix that covers the whole network domain.

  - BGP community attributes
    This attribute indicates tagging for routes of geographical and topological information and source types (e.g., transit, peer, or customer) as described in [RFC4384]. Therefore, network administrators can monitor the geographically-based or source-type-based traffic volume by correlating the attribute.

  - "mplsVpnRouteDistinguisher" described in [RFC5102]
    This value indicates the VPN customer’s identification, which cannot be extracted from the core router in MPLS networks. Thanks to this correlation, network administrators can monitor the customer-based traffic volume even on core routers.

6. Component Combination

An IPFIX Mediator may be able to simultaneously support more than one Intermediate Process. Multiple Intermediate Processes generally are configured in the following ways.

- Parallel Intermediate Processes

  A record stream is processed by multiple Intermediate Processes in parallel to fulfill the requirements of different applications. In this setup, every Intermediate Process receives a copy of the entire record stream as its input.

- Serial Intermediate Processes

  To execute flexible manipulation of a record stream, the Intermediate Processes are connected serially. In that case, an output record stream from one Intermediate Process forms an input record stream for a succeeding Intermediate Process.

In addition to the combination of Intermediate Processes, the combination of some components (Exporting Process, Collecting Process, IPFIX File Writer and Reader) can be applied to provide various data reduction techniques. This section shows some combinations along with examples.

6.1. Data-Based Collector Selection

The combination of one or more Intermediate Selection Processes and Exporting Processes can determine to which Collector input Data Records are exported. Applicable examples include exporting Data Records to a dedicated Collector on the basis of a customer or an organization. For example, an Intermediate Selection Process selects Data Records from a record stream on the basis of the peering autonomous system number, and an Exporting Process sends them to a dedicated Collector, as shown in the Figure G.

```
             .----------------------.   .------------.
             | Intermediate         |   | Exporting  |
             |  Selection Process 1 |   |  Process 1 |
          +--+--- Peering AS #10 ---+-->|            +--> Collector 1
          |  '----------------------'   '------------'
          |  .----------------------.   .------------.
   record |  | Intermediate         |   | Exporting  |
   stream |  |  Selection Process 2 |   |  Process 2 |
   -------+--+--- Peering AS #20 ---+-->|            +--> Collector 2
          |  '----------------------'   '------------'
          |  .----------------------.   .------------.
          |  | Intermediate         |   | Exporting  |
          |  |  Selection Process 3 |   |  Process 3 |
          +--+--- Peering AS #30 ---+-->|            +--> Collector 3
             '----------------------'   '------------'
```

Figure G: Data-Based Collector Selection

6.2. Flow Selection and Aggregation

The combination of one or more Intermediate Selection Processes and Intermediate Aggregation Processes can efficiently reduce the amount of Flow Records. The combination structure is similar to the concept of the Composite Selector described in [RFC5474]. For example, an Intermediate Selection Process selects Flows consisting of a small number of packets and then transmits them to an Intermediate Aggregation Process. Another Intermediate Selection Process selects other Flow Records and then transmits them to an Exporting Process, as shown in Figure H. This results in aggregation on the basis of the distribution of the number of packets per Flow.

```
            .------------------.  .--------------.  .------------.
            | Intermediate     |  | Intermediate |  | Exporting  |
            |   Selection      |  |  Aggregation |  |    Process |
            |        Process 1 |  |     Process  |  |            |
          +-+ packetDeltaCount +->|              +->|            |
          | |             <= 5 |  |              |  |            |
   record | '------------------'  '--------------'  |            |
   stream | .------------------.                    |            |
   -------+ | Intermediate     |                    |            |
          | |   Selection      |                    |            |
          | |        Process 2 |                    |            |
          +-+ packetDeltaCount +------------------->|            |
            |              > 5 |                    |            |
            '------------------'                    '------------'
```

Figure H: Flow Selection and Aggregation Example

6.3. IPFIX File Writer/Reader

An IPFIX File Writer [RFC5655] stores Data Records in a file system. When Data Records include problematic Information Elements, an Intermediate Anonymization Process can delete these fields before the IPFIX File Writer handles them, as shown in Figure I.

```
          .---------------.  .---------------.  .-------------.
          | Collecting    |  | Intermediate  |  | IPFIX       |
    IPFIX |      Process  |  | Anonymization |  |   File      |
    ----->|               +->|       Process +->|      Writer |
          '---------------'  '---------------'  '-------------'
```

Figure I: IPFIX Mediation Example with IPFIX File Writer

In contrast, an IPFIX File Reader [RFC5655] retrieves stored Data Records when administrators want to retrieve past Data Records from a given time period. If the data structure of the Data Records from the IPFIX File Reader is different from what administrators want, an Intermediate Anonymization Process and Intermediate Correlation Process can modify the data structure, as shown in Figure J.

```
    .-------------.  .---------------.  .---------------.  .-----------.
    | IPFIX       |  | Intermediate  |  | Intermediate  |  | Exporting |
    |   File      |  | Anonymization |  |   Correlation |  |   Process |
    |      Reader +->|       Process +->|       Process +->|           |
    '-------------'  '---------------'  '---------------'  '-----------'
```

Figure J: IPFIX Mediation Example with IPFIX File Reader

In the case where distributed IPFIX Mediators enable on-demand export of Data Records that have been previously stored by a File Writer, a collecting infrastructure with huge storage capacity for data retention can be set up.

7. Encoding for IPFIX Message Header

The IPFIX Message Header [RFC5101] includes Export Time, Sequence Number, and Observation Domain ID fields. This section describes some consideration points for the IPFIX Message Header encoding in the context of IPFIX Mediation.

Export Time

An IPFIX Mediator can set the Export Time in two ways.

* Case 1: keeping the field value of incoming Transport Sessions

- Case 2: setting the time at which an IPFIX Message leaves the IPFIX Mediator

Case 1 can be applied when an IPFIX Mediator operates as a proxy at the IPFIX Message level rather than the Data Record level. In case 2, the IPFIX Mediator needs to handle any delta timestamp fields described in [RFC5102], such as "flowStartDeltaMicroseconds" and "flowEndDeltaMicroseconds".

Sequence Number

In the case where an IPFIX Mediator relays IPFIX Messages from one Transport Session to another Transport Session, the IPFIX Mediator needs to handle the Sequence Number properly. In particular, the Sequence Number in the outgoing session is not allowed to be re-initialized, even when the incoming session shuts down and restarts.

Observation Domain ID

According to [RFC5101], the Observation Domain ID in the IPFIX Message Header is locally unique per Exporting Process. In contrast to the Observation Domain ID used by an Original Exporter, the Observation Domain ID used by an IPFIX Mediator does not necessarily represent a set of Observation Points located at the IPFIX Mediator itself.

An IPFIX Mediator may act as a proxy by relaying entire IPFIX Messages. In this case, it may report information about the Original Exporters by using the Observation Domain ID of the outgoing Messages as the scope field in an Options Template Record.

Otherwise, the IPFIX Mediator should have a function to export the observation location information regarding the Original Exporter. The information contains the IP addresses and Observation Domain IDs used by the Original Exporters and some information about the Transport Session, for example, the source port number, so that different Exporting Processes on the same Original Exporter can be identified. As far as privacy policy permits, an IPFIX Mediator reports the information to an IPFIX Collector.

If information about a set of Original Exporters needs to be reported, it can be useful to export it as Common Properties as specified in [RFC5473]. The commonPropertiesID may then serve as a scope for the set of Original Exporters. The Common Properties

Withdrawal Message [RFC5473] can be used to indicate that an incoming Transport Session from one of the Original Exporters was closed.

8. Information Model

IPFIX Mediation reuses the general information models from [RFC5102] and [RFC5477], and, depending on the Intermediate Processes type, potentially Information Elements such as:

- Original Exporter IP address, Observation Domain ID, and source port number about the Transport Session at the Original Exporter, in the case where an IPFIX Mediator reports original observation location information in Section 7. The Information Elements contained in the Export Session Details Options Template in [RFC5655] may be utilized for this purpose.

- Report on the applied IPFIX Mediation functions as described in Section 6.7. in [RFC5982].

- Certificate of an Original Exporter in Section 9. The Information Element exporterCertificate in [RFC5655] may be utilized for this purpose.

9. Security Considerations

As Mediators act as both IPFIX Collecting Processes and Exporting Processes, the Security Considerations for IPFIX [RFC5101] also apply to Mediators. The Security Considerations for IPFIX Files [RFC5655] also apply to IPFIX Mediators that write IPFIX Files or use them for internal storage. In addition, there are a few specific considerations that IPFIX Mediator implementations must take into account.

By design, IPFIX Mediators are "men-in-the-middle": they intercede in the communication between an Original Exporter (or another upstream Mediator) and a downstream Collecting Process. TLS provides no way to connect the session between the Mediator and the Original Exporter to the session between the Mediator and the downstream Collecting Process; indeed, this is by design. This has important implications for the level of confidentiality provided across an IPFIX Mediator and the ability to protect data integrity and Original Exporter authenticity across a Mediator. In general, a Mediator should maintain the same level of integrity and confidentiality protection on both sides of the mediation operation, except in situations where the Mediator is explicitly deployed as a gateway between trusted and untrusted networks.

Subsequent subsections deal with specific security issues raised by IPFIX Mediation.

9.1. Avoiding Security Level Downgrade

An IPFIX Mediator that accepts IPFIX Messages over a Transport Session protected by TLS [RFC5246] or DTLS [RFC4347] and that then exports IPFIX Messages derived therefrom in cleartext is a potentially serious vulnerability in an IPFIX infrastructure. The concern here is that confidentiality protection may be lost across a Mediator.

Therefore, an IPFIX Mediator that receives IPFIX Messages from an upstream Exporting Process protected using TLS or DTLS must provide for sending of IPFIX Messages resulting from the operation of the Intermediate Process(es) to a downstream Collecting Process using TLS or DTLS by default. It may be configurable to export records derived from protected records in cleartext but only when application requirements allow.

There are two common use cases for this. First, a Mediator performing a transformation that leads to a reduction in the required level of security (e.g., by removing all information requiring confidentiality from the output records) may export records downstream without confidentiality protection. Second, a mediator that acts as a proxy between an external (untrusted) network and an internal (trusted) network may export records without TLS when the additional overhead of TLS is unnecessary (e.g., on a physically protected network in the same locked equipment rack).

9.2. Avoiding Security Level Upgrade

There is a similar problem in the opposite direction: as an IPFIX Mediator’s signature on a TLS session to a downstream Collecting Process acts as an implicit assertion of the trustworthiness of the data within the session, a poorly deployed IPFIX Mediator could be used to "legitimize" records derived from untrusted sources. Unprotected sessions from the Original Exporter are generally untrusted, because they could have been tampered with or forged by an unauthorized third party. The concern here is that a Mediator could be used to add inappropriate trust to external information whose integrity cannot be guaranteed.

When specific deployment requirements allow, an IPFIX Mediator may export signed IPFIX Messages containing records derived from records received without integrity protection via TLS. One such deployment consideration would be the reverse of the second case above: when the Mediator acts as a proxy between an internal (trusted) and an external (untrusted) network and when the path from the Original Exporter is protected using some other method and the overhead of a TLS session is unnecessary.

In such cases, the IPFIX Mediator should notify the downstream Collector about the missing protection of all or part of the original record stream as part of the Transport Session Information.

9.3. Approximating End-to-End Assertions for IPFIX Mediators

Because the Transport Session between an IPFIX Mediator and an Original Exporter is independent from the Transport Session between the Mediator and the downstream Collecting Process, there is no existing method via TLS to assert the identity of the original Exporting Process downstream. However, an IPFIX Mediator, which modifies the stream of IPFIX Messages sent to it, is by definition a trusted entity in the infrastructure. Therefore, the IPFIX Mediator’s signature on an outgoing Transport Session can be treated as an implicit assertion that the Original Exporter was positively identified by the Mediator and that the source information it received was trustworthy. However, as noted in the previous section, IPFIX Mediators must in this circumstance take care not to provide an inappropriate upgrade of trust.

If the X.509 certificates [RFC5280] used to protect a Transport Session between an Original Exporter and an IPFIX Mediator are required downstream, an IPFIX Mediator may export Transport Session Information, including the exporterCertificate and the collectorCertificate Information Elements, with the Export Session Details Options Template defined in Section 8.1.3 of [RFC5655] or the Message Details Options Template defined in Section 8.1.4 of [RFC5655] in order to export this information downstream. However, in this case, the IPFIX Mediator is making an implicit assertion that the upstream session was properly protected and therefore trustworthy or that the Mediator has otherwise been configured to trust the information from the Original Exporter and, as such, must protect the Transport Session to the downstream Collector using TLS or DTLS as well.

9.4. Multiple Tenancy

Information from multiple sources may only be combined within a Mediator when that Mediator is applied for that specific purpose (e.g., spatial aggregation or concentration of records). In all other cases, an IPFIX Mediator must provide for keeping traffic data from multiple sources separate. Though the details of this are application-specific, this generally entails separating Transport

Sessions within the Mediator and associating them with information related to the source or purpose, e.g., network or hardware address range, virtual LAN tag, interface identifiers, and so on.

10. References

10.1. Normative References

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

[RFC5470] Sadasivan, G., Brownlee, N., Claise, B., and J. Quittek, "Architecture for IP Flow Information Export", RFC 5470, March 2009.

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

[RFC5655] Trammell, B., Boschi, E., Mark, L., Zseby, T., and A. Wagner, "Specification of the IP Flow Information Export (IPFIX) File Format", RFC 5655, October 2009.

10.2. Informative References

[PSAMP-MIB] Dietz, T., Claise, B., and J. Quittek, "Definitions of Managed Objects for Packet Sampling", Work in Progress, March 2011.

[RFC3917] Quittek, J., Zseby, T., Claise, B., and S. Zander, "Requirements for IP Flow Information Export (IPFIX)", RFC 3917, October 2004.

[RFC3954] Claise, B., Ed., "Cisco Systems NetFlow Services Export Version 9", RFC 3954, October 2004.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4384] Meyer, D., "BGP Communities for Data Collection", BCP 114, RFC 4384, February 2006.

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

[RFC5103] Trammell, B. and E. Boschi, "Bidirectional Flow Export Using IP Flow Information Export (IPFIX)", RFC 5103, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5472] Zseby, T., Boschi, E., Brownlee, N., and B. Claise, "IP Flow Information Export (IPFIX) Applicability", RFC 5472, March 2009.

[RFC5473] Boschi, E., Mark, L., and B. Claise, "Reducing Redundancy in IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) Reports", RFC 5473, March 2009.

[RFC5474] Duffield, N., Ed., Chiou, D., Claise, B., Greenberg, A., Grossglauser, M., and J. Rexford, "A Framework for Packet Selection and Reporting", RFC 5474, March 2009.

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

[RFC5477] Dietz, T., Claise, B., Aitken, P., Dressler, F., and G. Carle, "Information Model for Packet Sampling Exports", RFC 5477, March 2009.

[RFC5481] Morton, A. and B. Claise, "Packet Delay Variation Applicability Statement", RFC 5481, March 2009.

[RFC5815] Dietz, T., Ed., Kobayashi, A., Claise, B., and G. Muenz, "Definitions of Managed Objects for IP Flow Information Export", RFC 5815, April 2010.

[RFC5982] Kobayashi, A., Ed., and B. Claise, Ed., "IP Flow Information Export (IPFIX) Mediation: Problem Statement", RFC 5982, August 2010.

11. Acknowledgements

We would like to thank the following persons: Brian Trammell for his contribution regarding the improvement of the terminology section and the security considerations section; Daisuke Matsubara, Tsuyoshi Kondoh, Hiroshi Kurakami, and Haruhiko Nishida for their contribution during the initial phases of the document; Nevil Brownlee and Juergen Quittek for their technical reviews and feedback.

Authors’ Addresses

Atsushi Kobayashi
Nippon Telegraph and Telephone East Corporation
26F 3-20-2, Nishi-shinjuku 3-chome
Shinjuku, Tokyo 163-8019
Japan
Phone: +81-3-5353-3636
EMail: akoba@orange.plala.or.jp

Benoit Claise
Cisco Systems, Inc.
De Kleetlaan 6a b1
Diegem 1831
Belgium
Phone: +32 2 704 5622
EMail: bclaise@cisco.com

Gerhard Muenz
Technische Universitaet Muenchen
Boltzmannstr. 3
Garching 85748
Germany
EMail: muenz@net.in.tum.de
URI: http://www.net.in.tum.de/˜muenz

Keisuke Ishibashi
NTT Service Integration Platform Laboratories
3-9-11 Midori-cho
Musashino-shi 180-8585
Japan
Phone: +81-422-59-3407
EMail: ishibashi.keisuke@lab.ntt.co.jp