IPFIX Mediation: Framework

draft-ietf-ipfix-mediators-framework-02

Atsushi Kobayashi and Haruhiko Nishida (NTT)
Benoit Claise (Cisco Systems)

Feedback received for -01

- Thank you to reviewers:
  - Gerhard Muenz
    - This draft is in a very good shape.
    - The description of different mediation functions is comprehensive.
  - Nevil Brownlee

Feedback received for -01

- Resolved issues in -02:
  - Delete informative references to three drafts (flow anonymisation, aggregation, and flow selection techniques)
    - → Deleted references for three drafts
  - Should not define the Information Elements
    - → Deleted Information Elements.

  Maximum and minimum count elements could be included in future document.

Changes in -02: Selection Function

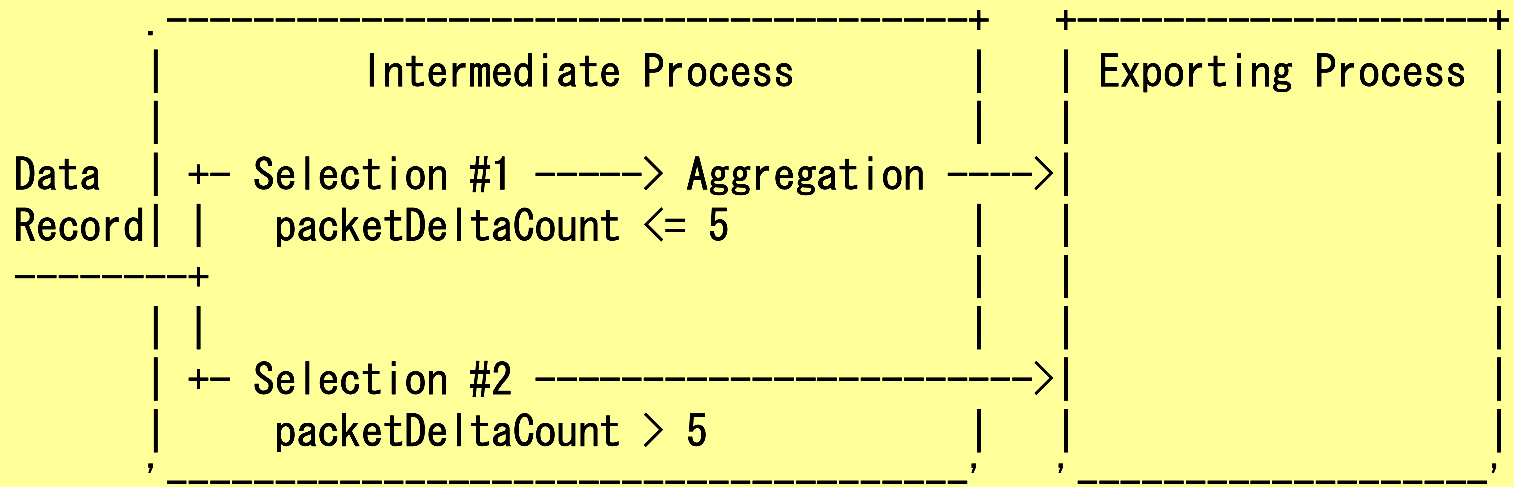
- "Flow-based Collector Selection" should not be a function of its own. (Gerhard)
  - Described as a use-case of one or more Selection Functions and Exporting Processes.

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

      Figure D: Exporting classified Data Records to dedicated Collector.
```

Changes in -02: use-case

- Also added a use-case of the Selection Functions and other functions



```
      .--------------------------------------+   +-------------------+
      |         Intermediate Process         |   | Exporting Process |
      |                                      |   |                   |
Data  | +- Selection #1 -----> Aggregation ----->|                   |
Record| |   packetDeltaCount <= 5            |   |                   |
--------+                                    |   |                   |
      | |                                    |   |                   |
      | +- Selection #2 ------------------------>|                   |
      |     packetDeltaCount > 5             |   |                   |
      '--------------------------------------'   '-------------------'
```

Figure E: Flow Selection and Aggregation

Changes in -02: Time Composition

- Improved the paragraph to avoid confusion.
  - Time composition advantages:
    - **Reducing the number of Flow Records**
    - **Computing the active time period for long-running Flows**
    - **Revealing the up-and-down traffic volume within an active time**
      - Short period Flow Records created by configuring a short active time, e.g., 1 or 10 sec, are merged within a certain time period, e.g., 60 or 300 sec, at an IPFIX Mediator. While merging, the IPFIX Mediator computes new metrics such as maximum and minimum.

Changes in -02: Security Considerations

- Added some solutions to specific security threats related to Mediator
  - **Attacks against IPFIX Mediator**
    - IPFIX Mediators host the packet filter function to reject malicious packets at an outside interface.
  - **Man-in-the-middle attack by untrusted Mediator**
    - IPFIX Collectors and Exporters must verify trusted Mediators to prevent connection to untrusted Mediators.
  - **Configuration on IPFIX Mediation**
    - To eliminate the risks, IPFIX Mediators must provide an authentication function for authorized administrators and facilities for tracing configuration changes to their origin.

Open Issue

- **New observation group (Benoit)**
  - In case of aggregation (for example all routers in Japan), where should we encode the information?
    - In a new Observation Point as a Flow Key in the Flow Record?
    - Or with a new Mediator Observation Domain ID?
  - → Is this a framework issue or a protocol issue?

Next Steps

- The draft was stabilized thanks to Gerhard’s detailed review.
- A new version will be produced (some editorial comments)
- Then it will be ready for WG last call