IPFIX Mediation: Problem Statement

draft-ietf-ipfix-mediators-problem-statement-02

<u>Atsushi Kobayashi</u> and Haruhiko Nishida (NTT) Christoph Sommer and Falko Dressler (Univ. Erlangen) Emile Stephan (France Telecom) Benoit Claise (Cisco Systems)

Feedback received for -01

- Thank you to reviewers:
 - □ Gerhard Muenz
 - Nevil Brownlee

Resolved issues in -02:

- □ What are present problems in IPFIX? (Gerhard)
 - →Added "Problem Statement" section.
- □ Why IPFIX Mediation is needed? (Gerhard)
 - →An implementation analysis in applicable examples argues the necessity for Mediation.
- Eliminate ambiguity on Mediation terminologies.
 (Gerhard, Benoit, Christoph)

→ Improved them based on feedback from mailing-list

Feedback received for -01

Resolved issues in -02:

- Delete informative references to three drafts (flow anonymisation, aggregation, and flow selection techniques)
 - (Nevil)
 - →Added summary of three drafts

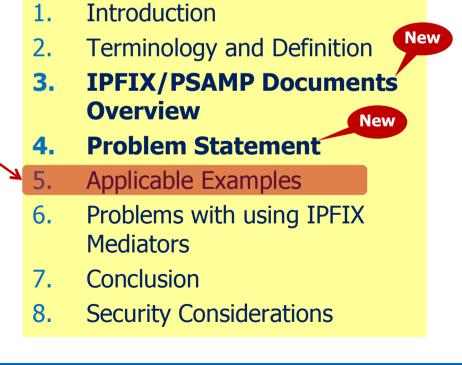
Changes in -02: Reorganization

- New Section: "IPFIX/PSAMP Document Overview" and "Problem Statement"
- * "Approaches to Scalability" is included in "Applicable Examples"

-01

- 1. Introduction
- 2. Terminology and Definition
- 3. Flow-Based Mediation: Applicability Examples
- 4. Approaches to Scalability
- 5. Problems with using IPFIX Mediators
- 6. Conclusion
- 7. Security Considerations

-02



Changes in -02: Terminology

***IPFIX** Mediation

□IPFIX Mediation is a function that can be applied to individual Data Records and/or Template Records or to entire IPFIX Messages. IPFIX Mediation offers one or multiple capabilities.

***IPFIX** Mediator

■ An IPFIX Mediator is an IPFIX Device that contains one or more IPFIX Mediation capabilities.

□IPFIX Proxy, Distributor etc. indicate the capability of the device.

Distinction between IPFIX Proxy and Distributor

- □ IPFIX Proxy converts legacy protocol to IPFIX, or transport protocol to another transport protocol.
- IPFIX Distributor determines a Collector, to which a Data Record is exported, based on its content.

Changes in -02: Problem Statement

***Operators pursue appropriate conditions:**

- **□** Capacity of measurement system
- **D** Requirement for given application

More complex situation comes from:

- □ IP traffic growth
 - → How to build a large-scale collecting infrastructure?
- □ Multi-purpose Traffic Measurement
 - Traffic engineering, security, accounting, and QoS performance
 - → How to transmit traffic data to specific applications?
- Heterogeneous Environment
 - Traditional Exporters or state-of-the-art Exporters
 - Probe, router or switch
 - → How to absorb the differences of Exporter capabilities?

Changes in -02: Applicable Examples

List of applicability examples to cope with complex situations

- □ Adjusting Flow Granularity
- □ Hierarchical Collecting Infrastructure
- Correlation of Data Records
- □ Time/Spatial Composition
- Data Retention
- □ IPFIX Export from Branch Office
- Distributing Data Records
- IPFIX Export Across Domains
- □ Flow-based Sampling and Selection
- □ Interoperability between Legacy Protocols and IPFIX

Implementation analysis argues the solutions with or without Mediation.

Further Changes in -02

Summaries for three drafts

Anonymization described in "IPFIX Export Across Domains"
 Flow selection described in "Flow-based Sampling and Selection"
 Aggregation described in "Adjusting Flow Granularity"

*****Use "Data Record" as a generic term for Flow Record and Packet Report when possible

Added specific security threats related to Mediator

- □ Attacks against IPFIX Mediator
- Man-in-the-middle attack by untrusted IPFIX Mediator
- □ Configuration on IPFIX Mediation

Open Issue

Should Mediator send the function done on Data Record to Top Collector? (Benoit)

- Top Collector should sometimes know what the Mediation has done on the Data Records (for example, sum, average, etc...).
 - It is difficult to deduce the distinction between time composition, spatial composition and Flow Key aggregation.



The draft was stabilized thanks to Gerhard's detailed review.
It will be ready for WG last call after improving the wording.