Exporting Aggregated Flow Data using IPFIX (draft-trammell-ipfix-a9n-03)

B. Trammell, E. Boschi, A. Wagner, B. Claise

IETF 81 – Québec, Canada – 27 July 2011

a9n in a nutshell

- Draft defines a general purpose architecture operational model for an Intermediate Aggregation Process (IAP), and support for aggregated flow export.
- Minimal changes since Prague:
  - Noted open issues raised in hallway conversations (not addressed)
  - Wrote first example in detail

Contents

- 1. Introduction
- 2. Terminology
  - **Aggregated Flow**: *A Flow, as defined by [RFC5101], derived from a set of zero or more original Flows within a defined Aggregation Interval.*
- 3. Use Cases
  - Time series generation
  - Adaptive resolution of flow data
  - Anonymizing effects of aggregation
  - *This section requires some expansion, and harmonization with section 8 (Examples)*

More Contents

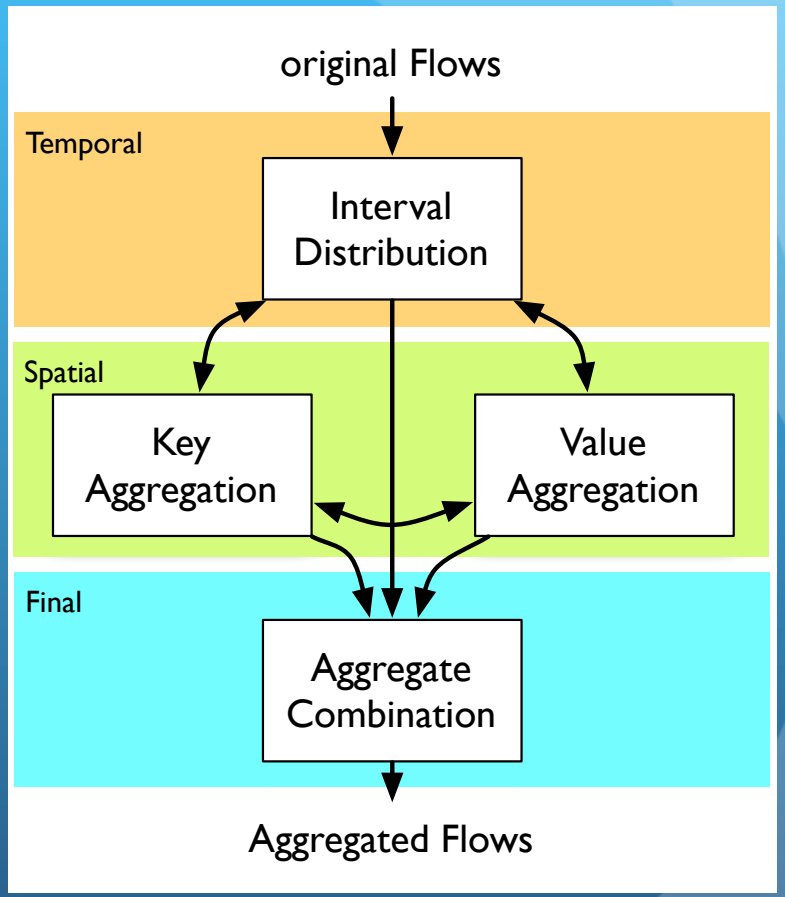
- 4. Architecture
  - How an Intermediate Aggregation Process fits into a Mediator, and with other IPFIX Architecture entities
  - A generalized, descriptive model for the internal arrangement of an Intermediate Aggregation Process
- 5. Operations
  - Detailed description of each of the operations outlined in the internal architecture
- 6. Additional Considerations
  - Exact versus Approximate Counting
  - Considerations for Aggregation of Sampled Data

Yet More Contents

- 7. Export
  - Guidelines, IEs, and options templates for exporting according to the model in sections 4-6
- 8. Examples
  - New in -03: introduce conventions and toy data set used by all examples
  - Traffic Time-Series per Source
  - Core Traffic Matrix
  - Distinct Source Count
  - Traffic Time-Series with Counter Distribution
- 9. Security
- 10. IANA

IAP Architecture

- Decomposition into iterative temporal and spatial steps
- Spatial aggregation implies temporal aggregation
  - interdependency due to special treatment of intervals in IPFIX



Next steps

- Continued improvement of examples and use cases.
- Continue eliciting feedback and incorporating improvements from WG members.
  - One complete review of -03 already received (thanks, Christian Henke!) as well as comments on interval distribution (thanks, Lothar Braun!)
- WG adoption; to IESG in Taipei-Paris timeframe