Exporting Aggregated Flow Data using IPFIX (draft-trammell-ipfix-a9n-04)

B. Trammell, A. Wagner, B. Claise

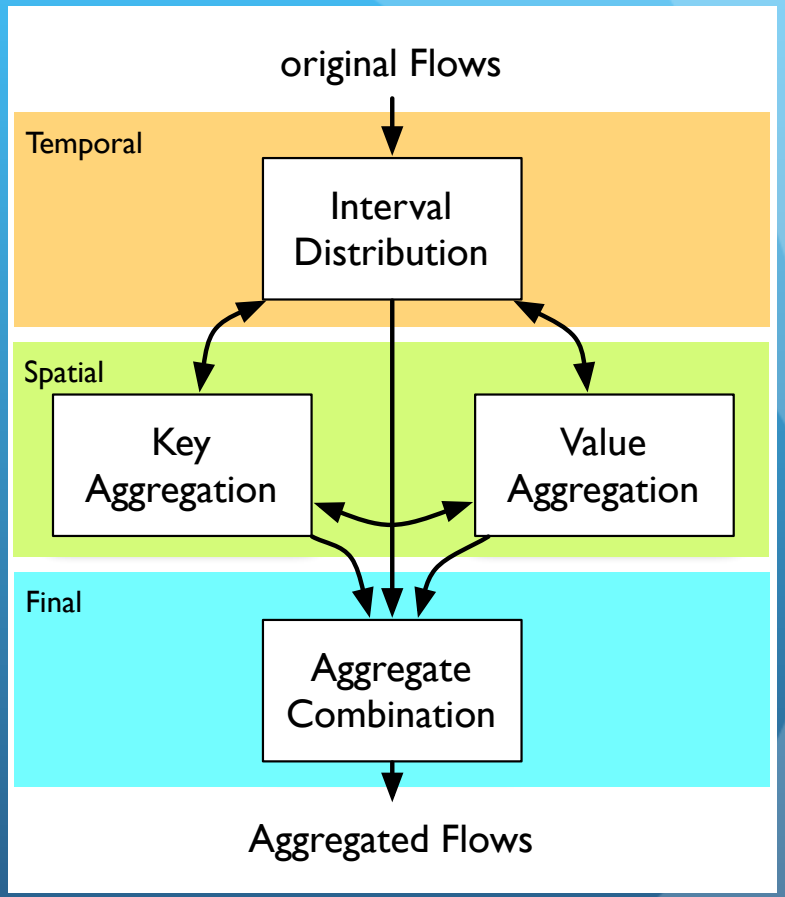
IETF 81 – Québec, Canada – 27 July 2011

a9n in a nutshell

- Defines a general purpose architecture operational model for an Intermediate Aggregation Process (IAP)
- Defines support for aggregated flow export based upon this model
- Provides examples of aggregated flows

IAP Architecture

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



Changes since trammell-03

- §5.3.2: new section on derived non-key fields
- §6.3: add considerations for heterogeneous flow aggregation
  - Flows of different types or from different sources must be
    - correlated in order to homogenize them before aggregation, or
    - kept completely separate, identified by Observation Domain.
- §7.2.4: change `originalFlows` to `deltaFlowCount` (IE 3) for compatibility with NetFlow v9 IEs
- §7.3: add new `distinctCountOf[Source,Destination]Address` for counting addresses without regard to address version.

Additions / editorial since -03

- Completed examples
- Completed Security Considerations
  - reference to 5101, 6183
  - reference to 6235 when used with anonymization
- First-pass terminology review and cleanup
- Improved illustrations in architecture section
  - Clarify potential deployment locations of IAP
  - New illustration showing application of aggregation together with a (yet-undefined) correlation process

Next steps

- Submit –ietf-00
  - Unless we get more review comments in the meantime, this is essentially identical to –trammell-04
- WGLC before Paris