Flow Selection Techniques

draft-ietf-ipfix-flow-selection-tech-02.txt

Lorenzo Peluso, Tanja Zseby,

Salvatore D'Antonio, Maurizio Molina

IETF 78, Maastricht, July 2010

Background

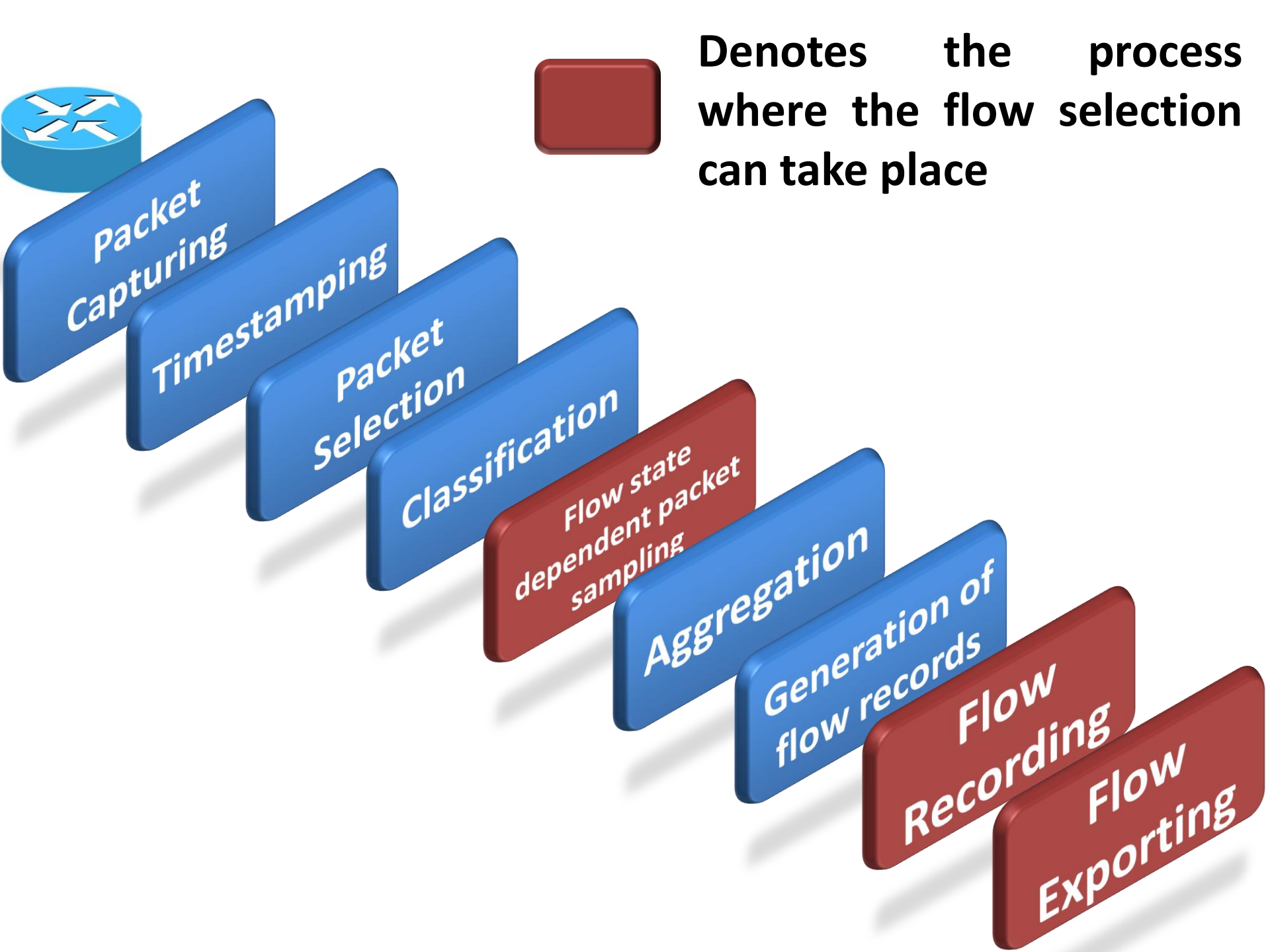
- Motivation
- Flow selection techniques
- Use of flow selection along the flow monitoring work flow

Motivation

- Resource optimization
  - Use and management of computing, memory, and network resources can be optimized thanks to the use of flow selection techniques
- Application requirements
  - A flexible flow monitoring system can underpin various applications with diverse requirements by properly selecting flows of interest
- Dynamic traffic analysis
  - Fine-grained or coarse-grained traffic analysis benefits from the use of flow selection strategies

Flow selection techniques

- Flow selection based on the content of the flow record
- Flow selection based on flow record arrival time
- Flow selection based on external events like the exhaustion of local resources


Denotes the process where the flow selection can take place
Packet Capturing
Timestamping
Packet Selection
Classification
Flow state dependent packet sampling
Aggregation
Generation of flow records
Flow Recording
Flow Exporting

Changes since -01 version

- Feedback from IETF 77
  - How does flow selection fit in with the IPFIX mediation framework?
- -02 version approach
  - Flow selection is integrated into the reference model of the IPFIX Mediation framework as an Intermediate Process (draft-ietf-ipfix-mediators-framework-07)
  - The selection function is performed at two different levels of the IPFIX framework architecture:
    - IPFIX Original Exporter
    - IPFIX Mediator

Flow selection as a function of the IPFIX Original Exporter

- Flow selection can apply during:
  - The metering process
  - The recording process
  - The exporting process

Flow selection during the metering process

- Flow state dependent packet sampling. Two examples:
  - If sampled packets belong to a flow of interest, then they are assigned to the corresponding flow, thus contributing to increase metrics in the flow record, otherwise they are discarded
  - In case sampled packets are the first packets of a new flow, they are discarded so as to avoid the generation of a new flow record and then the consumption of either memory or computing resources

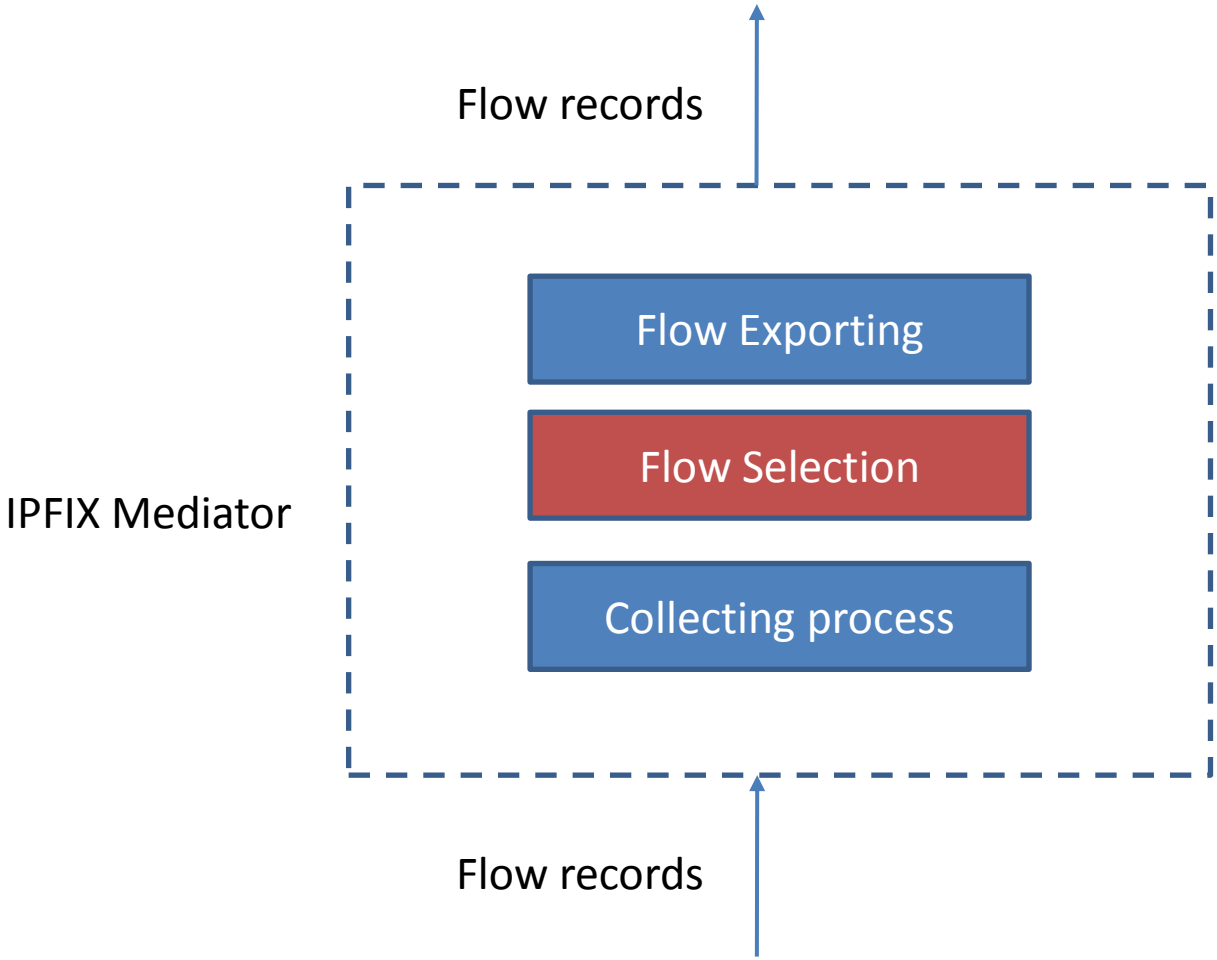
Flow selection during the recording process

- Flow selection applies to the flow records stored in the flow cache
  - Flow records are selected and removed from the flow cache in order to make room to newly generated records
  - Timed-out flows are selected for being removed from the memory area devoted to containing flow information

Flow selection during the exporting process

- A subset of the flow records stored in the flow cache is selected to be exported and provided to the application
  - According to flow state dependent criteria/policies some flow records are moved from the flow cache to the collector
  - Depending on the application requirements some flow state parameters are assessed in order to identify worth exporting flow records

Flow selection as a mediation function



Flow selection at mediator's level

- The IPFIX mediator is in charge of further selecting flows within the subset of flow records being exported by the IPFIX exporter
  - More complex selection criteria
  - More fine-grained selection of the flow records to be exported
  - If an IPFIX Mediator interacts with a set of IPFIX Collectors, flow records arriving at the IPFIX Mediator might be selected based on the IPFIX Collector requesting flow information

Information model for exporting of flow selection information

- The information elements are defined in accordance with the IPFIX information model [RFC5102]
- Examples of information elements are:
  - FsMeter_UnmeasPacketCount, which counts the number of packets that have not been metered (due to the application of flow state dependent packet sampling)
  - FsExp_UnexportedPacketCount, which counts the number of packets contained in the not-exported flow records

Information model for configuration of flow selection techniques

- selectionMethod,
  - identifies the method applied by the flow selection process
- flowMaxAdmitFlowRecords
  - specifies the maximum number of eligible flow records which might be created in the flow cache
- flowRecordBytesSize
  - specifies the minimum number of bytes which must be contained in a flow record in order that it is considered not eligible for removal

Way forward

- Better explain the motivation why flow state dependent packet sampling is in scope
- Provide more details about the role of flow selection in the mediation framework
- Solicit additional feedback/comments from WG
- Send the draft to the IESG