Elements of a Framework for PSAMP

Nick Duffield

AT&T Labs

nduffield@att.com

Aims and Focus

- Scope out requirements for PSAMP
- Position PSAMP as a supplier of packet measurements
  - support applications, but they are done elsewhere
  - main work for PSAMP is to define packet selection operations
- Need to get measurements to applications
  - hence requirements for information model, export
  - can use existing protocols (IPFIX the obvious candidate)
    - if PSAMP requirements match existing protocol capabilities

Elements

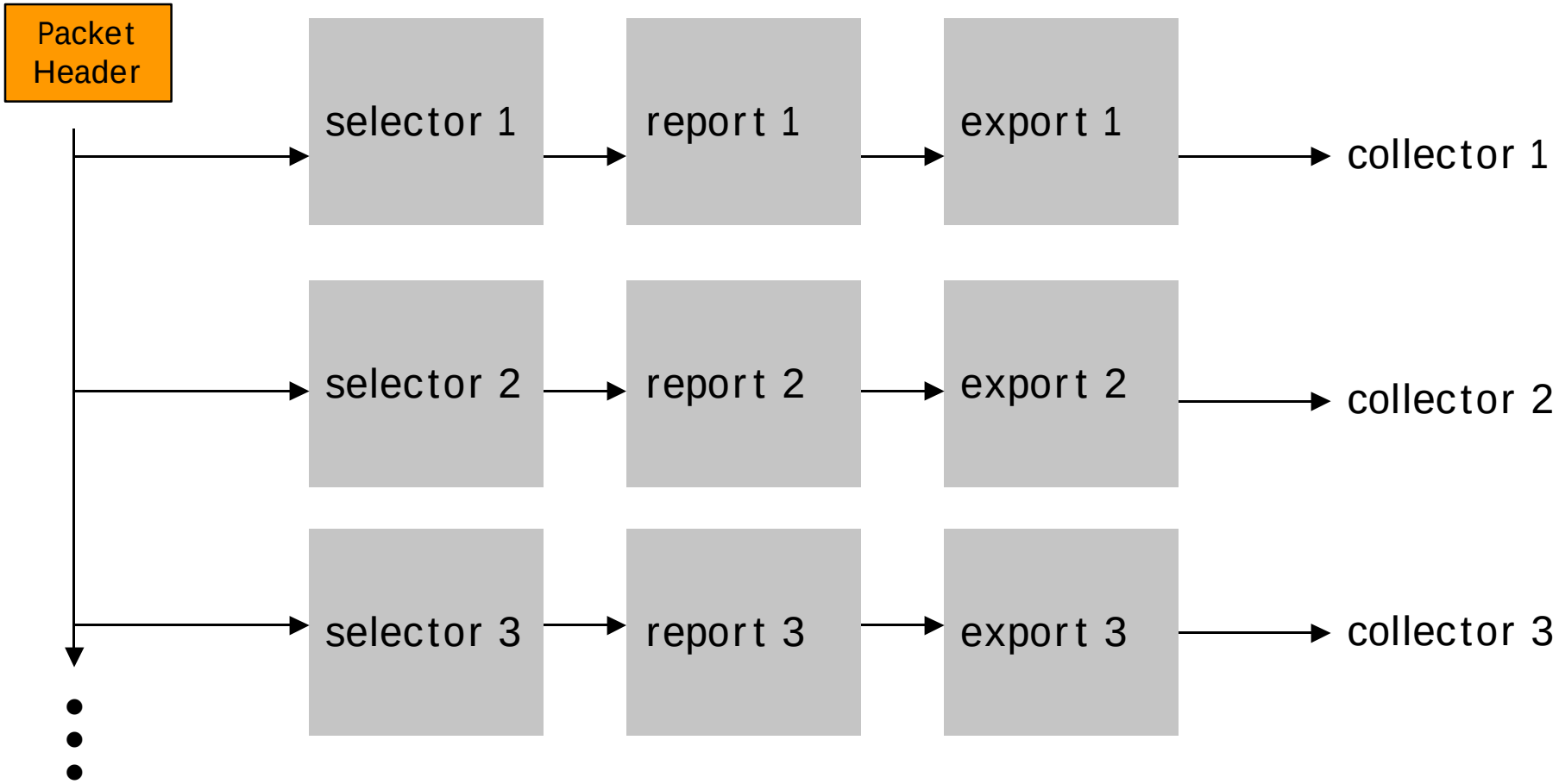
- Packet selection
- Parallel measurement
- Report content
- Self-defining report stream
- Remote and local export
- Robustness and information loss
- Configuration and management

Packet Selection Primitives

- Requirement: sufficiently rich set of packet selection operations
- Filter
  - e.g., match/mask on source/destination prefix, port numbers, protocol, … + tags to indicate the associated (sub)interface
- Sample
  - e.g., 1 in N deterministic, random, or hash-based
- Combinations
  - e.g., filter, then sample 1 in N
- Scope
  - selection based on packet content: availability of router state not assumed
- Counters
  - packets/bytes of full packet stream, and of selected packets
  - available for export, or polling
  - used directly by applications, e.g., filter, then count for billing
  - provide robustness w.r.t. information loss, e.g., from report stream

Parallel Measurement

- Requirement: parallel configurable information flows



Resource Issues for Parallel Measurements

- Bounded processing resources per packet in router
- Packet may match several selectors
  - e.g. coarse AS filter for billing, narrow subfilter for engineerng
- If packet matches too many selectors:
  - not possible to fully report all resulting measurements
- Want graceful degradation from full reporting
  - e.g., reflecting user priorities
- Information model design:
  - should provide inherent robustness to such information loss

Report Content

- Requirement: per packet reporting with sufficient detail
- Classes of information available for inclusion
  - header fields, e.g., IP src/dst address, TCP/UDP ports, sizes, ToS, ...
  - sub-IP level identifiers, e.g., i/o interfaces, MPLS label stack, ...
  - router state, e.g, routing prefix, AS numbers, next hop, timestamps,...
  - derived quantities, e.g., hash values
  - packet/byte counters from originating selector

Self-defining Report Stream

- Requirement: transparent interpretation of data
- Include selector parameters for data interpretation
  - e.g., sampling: use N to estimate actual traffic intensity
  - e.g., filtering: what is possible universe of a given packet
  - e.g.., hash function parameters: for ICMP traceback matching
- Attribution
  - multiple selectors: which one(s) selected packet?
- Self-defining report stream
  - include selector parameters, report format, …
    - e.g. periodically, upon change, upon command, …
  - robust: data and its interpretation bound together
- Alternative that we don't like:
  - collector keeps independent track of selection parameters
    - e.g. parameter management system, or by polling router
  - joining data painful, especially synchronization
  - multiple systems to interpret one data source = architectural hostage
  - impact of undocumented changes, e.g., through CLI

Remote and Local Export

- Requirement:
  - reporting to on-board and off-board applications
- Flexibility of different export destinations per selector
  - different measurement applications, on different or same host
- Allow local export to on-board applications
  - e.g. security applications
    - local export of hashes to ICMP traceback application
  - e.g. multiple-packet measurement operations
    - interpacket delay jitter, flow formation
- Rate limiting export
  - e.g. rate limit supply of measurements to transport

Robustness and Information Loss

- Requirement: robustness to information loss
- Causes of information loss:
  - incomplete information if packet matches multiple selectors
  - report loss in transit
  - collector failure
- Inherent robustness in packet measurement model:
  - small information content in a single measurement
    - relative to whole data stream
- Enhance robustness of measurement report stream:
  - enable interpolation/correction for missing data
    - e.g., include packet/byte counters, sequence numbers
  - decouples from and reduces need for reliability at other levels

Configuration and Management

- Motivation: enable reliable configuration by external applications
  - (not as part of the export protocol!)
  - of selector parameters, report format, export destination
  - configuration of selectors in large number of device
- Applications:
  - e.g., setup of large number of filters/counters for billing
  - e.g., collector failure: redirection of export to secondary collector
  - e.g., ongoing 1 in N baseline measurements to NOC
    - automated detection of DoS attack signature at NOC
    - automated reconfiguration of router filter to focus on attack traffic
  - e.g., dynamic selector reconfiguration by on-board applications
- Requirement: MIB for configuration parameters, SNMP to read/write
  - secure, reliable, widespread experience, easy to build clients
  - vendor neutral, standardized
  - easy to reconfigure from on-board application