IPFIX Applicability

draft-zseby-ipfix-applicability-00.txt

Tanja Zseby, FhG FOKUS
Reinaldo Penno, Nortel Networks
Nevil Brownlee, CAIDA

Applicability Draft

- Motivation
  - Rough idea about target applications (req. draft) but no concrete scenarios
    - e.g. accounting: different charging schemes
    - e.g. QoS monitoring: different metrics
  - Other frameworks and WG (e.g. RTFM, IPPM, AAA)
    - Need to clarify relations and potential interfaces
- Objectives:
  - Show how (target) applications can use IPFIX
    - How can IPFIX be deployed in concrete scenarios
    - When are which optional features useful
    - What else can we do with IPFIX (further applications ?)
  - Describe relations and potential interfaces to other frameworks/ working groups
    - What is the relation between IPFIX and other WGs/frameworks
    - How would IPFIX fit into existing frameworks (potential integration/interfaces)

Current Table of Content

- Applications of IPFIX
  - Accounting with IPFIX
  - Intrusion Detection with IPFIX
  - QoS Monitoring with IPFIX
    - Measurement of Round-trip-time (RTT) with IPFIX
    - Measurement of One-way-delay (OWD) with IPFIX
    - Measurement of Loss with IPFIX
    - Measurement of delay variation with IPFIX
    - Sampling for QoS Monitoring
- Relations to other Frameworks
  - IPFIX and AAA
  - IPFIX and RTFM
  - IPFIX considerations for middleboxes

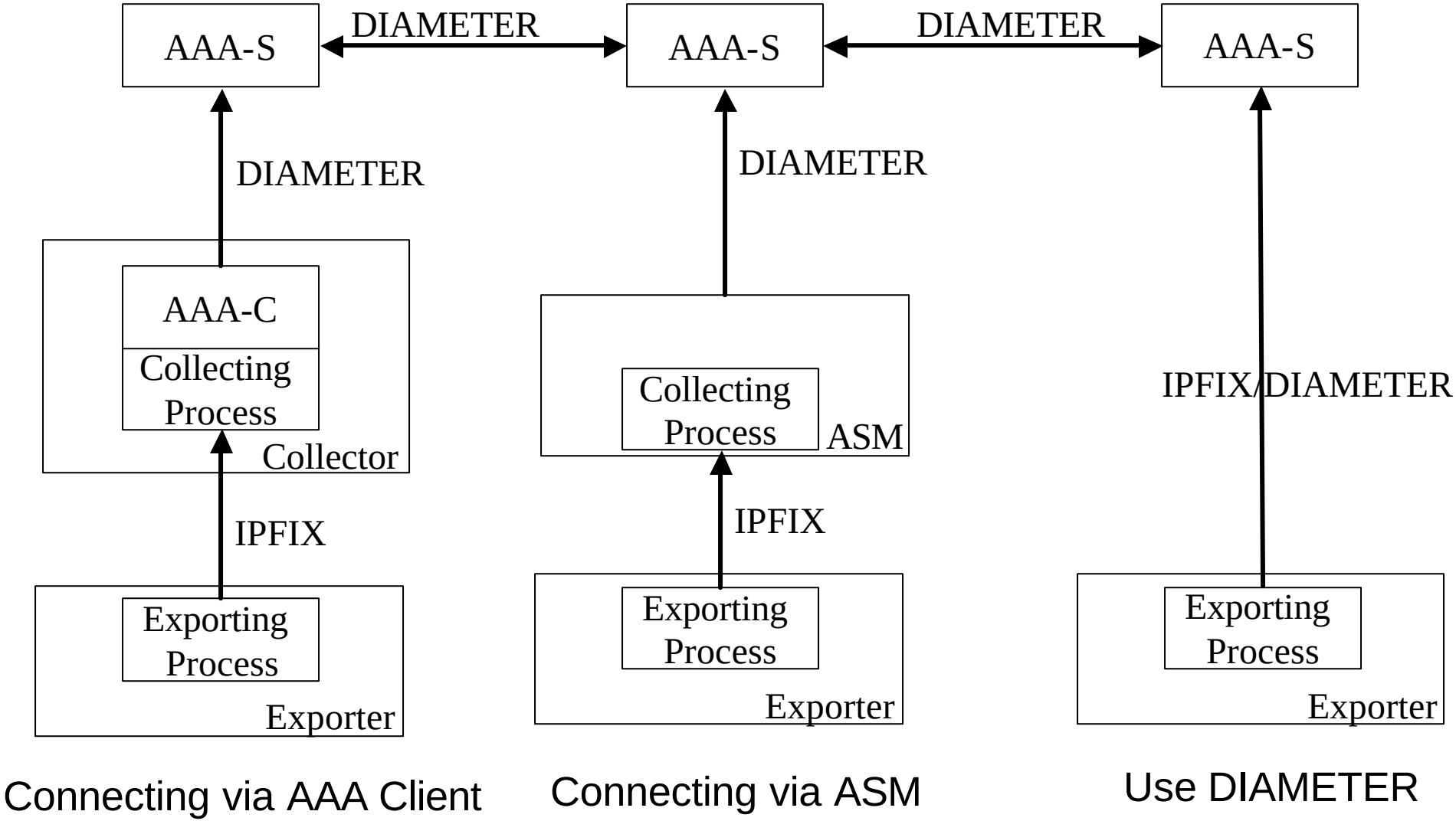
QoS Monitoring with IPFIX

- Round-trip-time
  - Packet pair matching (e.g. for DNS, TCP, ICMP,SNMP)
    - Measure both directions
    - Classification of protocols
    - Recognize request/response
    - Timestamping
  - Calculation at exporter or collector
  - Probably possible with optional IPFIX features
- One-way-delay
  - Correlation of packet arrival events at 2 measurement points
    - Calculation of unique packet ID
  - Probably possible with optional IPFIX features
- Loss
  - Utilization of sequence numbers or
  - 2 point measurement (like one-way-delay)
- Sampling useful and possible
- PSAMP support highly valuable

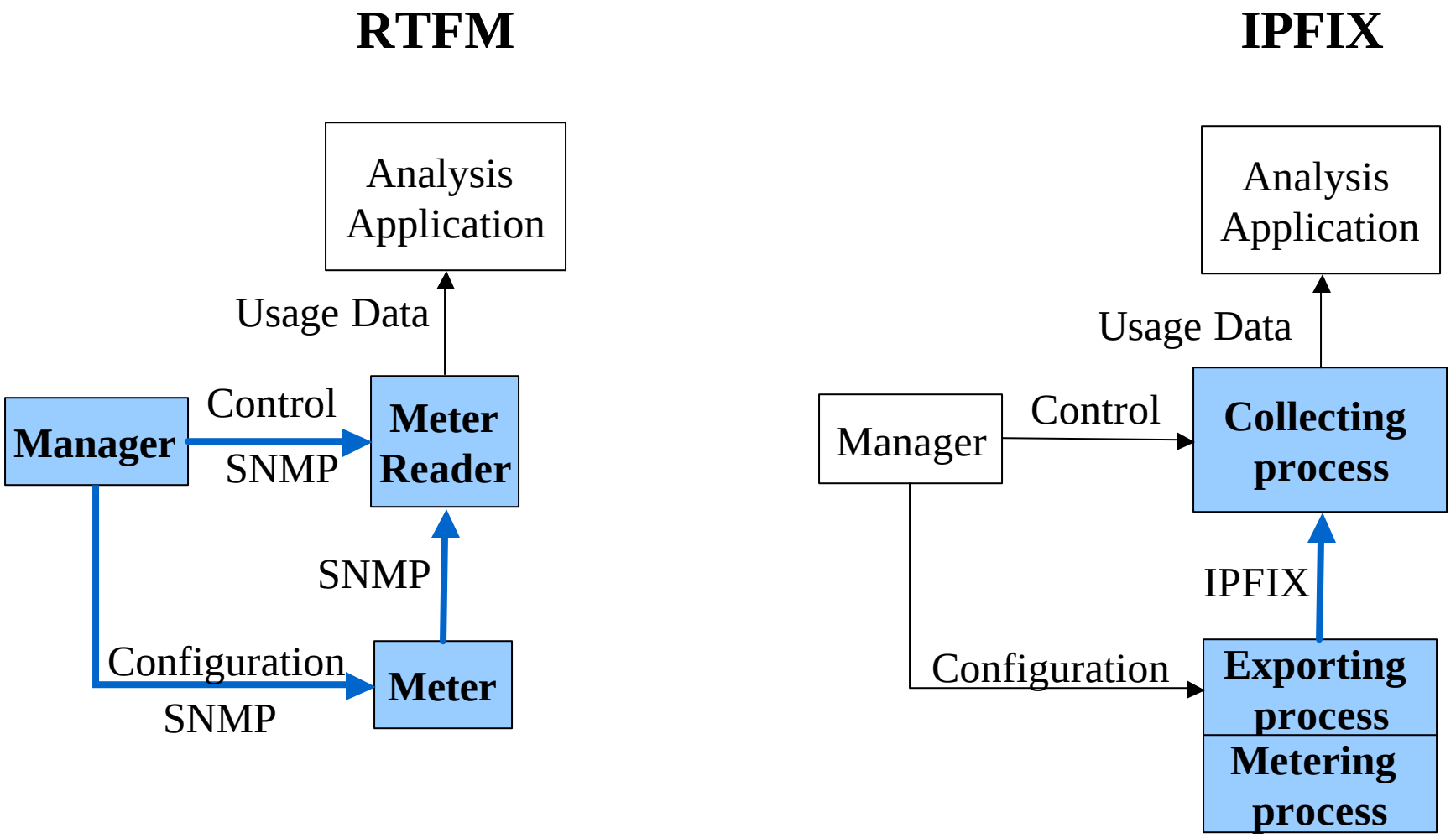
IPFIX and AAA

- IPFIX Accounting can be realized without AAA
- If AAA Infrastructure is present:
  - Accounting data collection with IPFIX
  - Generation of DIAMETER accounting records
  - Secure exchange of accounting data between domains
  - Mapping of user ID to flow information
- Possibilities for interoperation between IPFIX and AAA
  - Connecting via AAA Client
  - Connecting via Application Specific Modul (ASM) (IRTF AAARCH group)
  - Use DIAMETER for IPFIX transport

IPFIX and AAA



IPFIX and RTFM



IPFIX and RTFM

- RTFM
  - Meters, Meter reader, Manager
  - Bidirectional flows
  - Meterconfiguration via SNMP
  - Meter MIB
  - Data Collection
    - Pull Mode
    - SNMP
  - Multiple rulesets allowed
  - No duplicate counting within ruleset (Count in one bucket)
  - Continously incrementing counters
  - Systematic Sampling (selection of every Nth packet) supported
- IPFIX
  - Metering, exporting and collecting process
  - Flow direction: open issue
  - Configuration: out of scope
  - Data Collection
    - Push Mode (Pull optional)
    - IPFIX Protocol
  - Counters: delta or absolute ?
  - Sampling: optional

Considerations for Middleboxes

- Implications on IPFIX exporting/metering processes that are co-located with middlebox functions (Firewalls, NAT, etc.)
- Firewall: How to report dropped packets ?
  - Discard silently
  - Discard and send flow record
  - Discard and send flow record with discard information
- NAT: Export private or public address ?
  - Traditonal NAT (private to public)
    - source or destination address may be changed
    - Suggestion: private and public SHOULD be reported
  - Bi-directional NAT (private to public or public to private)
    - Source or destination address may be changed
  - Twice NAT
    - Source and destination address may be changed
    - Suggestion: private and public MUST be reported

Considerations for Middleboxes

- Traffic Conditioners
  - Marker: Which flow should be reported ? (Marked, Unmarked, Both)
  - Shapers: No report on discarded packets
  - Droppers: Like firewall options
- Tunneling: Report before and/or after tunneling ?
  - Dependent on location and data access of exporting process
- VPNs
  - Layer 3 Provider-Edge-based VPN
    - IP Level forwarding
    - Exporting process in provider edge device
    - Distinguish VPNs with overlapping private address realms by key
  - Layer 2 Provider-Edge-based VPN
    - Layer 2 Services
    - No recommendation yet

Open Issues, Missing Parts

- Extend existing sections
- Many things clearer, when protocol is selected
- Furher sections
  - Traffic Profiling with IPFIX
  - Traffic Engineering with IPFIX
  - Intrusion detection with IPFIX
  - IPFIX and IPPM
  - IPFIX and PSAMP
  - IPFIX and RMON

Document: http://ipfix.doit.wisc.edu/app/draft-zseby-ipfix-applicability-00.txt
Mailing-list: ipfix-app@net.doit.wisc.edu

Thank you for your attention !

Questions ?

Comments ?

Volunteers ?