Fraunhofer Institute for Open Communication Systems

Standardizing IP Traffic Flow Measurement at the IETF

Tanja Zseby (FhG FOKUS, zseby@fokus.fhg.de)

Jürgen Quittek (NEC Europe Ltd., quittek@ccrle.nec.de)

Outline

- FhG FOKUS
- Standardization of IP Traffic Flow Measurements in the IETF and IRTF
  - Real Time Traffic Flow Measurement (RTFM)
  - IP Flow Information Export (IPFIX) ←
  - Packet Sampling (PSAMP) ←
  - IP Perfomance Metrics (IPPM)
  - IRTF Internet Measurement Research Group (IMRG)
  - Authentication, Authorization, Accounting (AAA) and IRTF AAAARCH
- Related EU projects at FOKUS
  - InterMon
  - 6QM

FOKUS Measurement Activities

- Fraunhofer Institute for Open Communication Systems (FhG FOKUS), Berlin,Germany
  - Measurement group at Competence Center for Global Networking (GLONE)
  - Since 01.01.03: New Competence Center for Measurement Technologies and Network Research (METEOR)

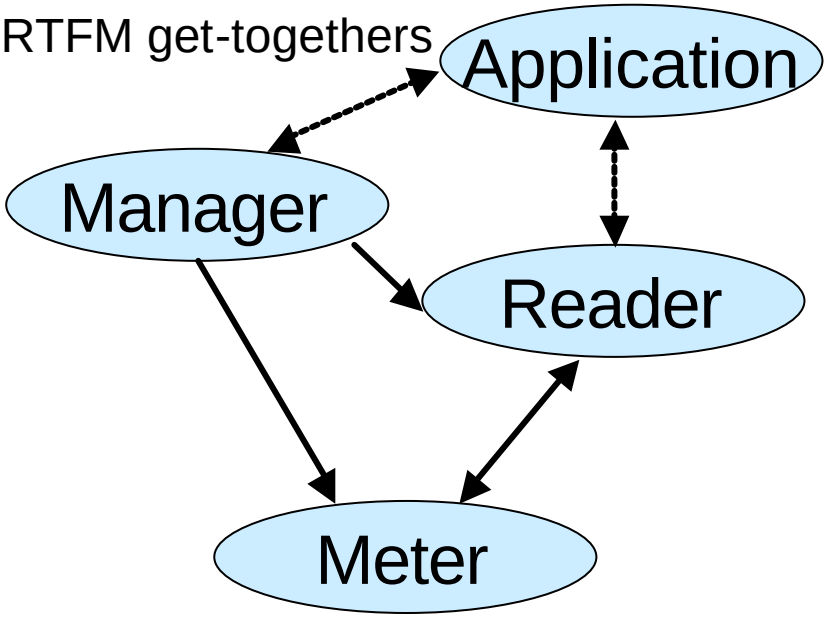
www.fokus.fhg.de

- Measurement Activities
  - Passive and active measurement components
  - Control of distributed heterogeneous measurement platform
  - Resource efficient measurements (e.g. sampling)
  - Standardization
    - IETF IPFIX (requirements, applicability)
    - IETF PSAMP (sampling information model)
    - IRTF AAAARCH (policy-based accounting RFC3334)
    - IRTF IMRG (planed; measurement configuration)

RTFM

Real Time Traffic Flow Measurement (RTFM)

- Former IETF working group
  - Outcome:
    - RFCs 2720-2724
    - Measurement Architecture
    - Meter NeTraMet
  - Was continued as RTFM get-togethers



RTFM Meter NeTraMet

- Very flexible and powerful meter
  - Programmable rule sets
  - Meter can serve several readers
  - Manger can control multiple meters
- Reader polls meter
- Meter configuration via SNMPv2 (Meter MIB)
  - which flows should be measured
  - which attributes should be stored
- Realization by SNMP Meter MIB
- Free software implementation NeTraMet 4.3
- Extensions:
  - Support for DiffServ codepoint
  - Support for IPv6 addresses
  - RSVP Message Parser from CEFRIEL
  - Passive RTT measurements based on packet pairs
- No acceptance at manufacturers
- Complicated to use (too powerful)

IPFIX

IETF IPFIX Working Group

- IP Flow Information eXport (IPFIX)
  - BoF sessions 12/00 and 08/01
  - active since 10/01
- Successor of RTFM (Real-Time Flow Measurement) working group
- Target (official): standardizing current practice
  - Target (unofficial): standardizing (something like) Cisco NetFlow
- Chairs
  - Nevil Brownlee, CAIDA
  - David Plonka, University of Wisconsin

IPFIX Scope and General Requirements

Goal: Find or develop a basic common IP Traffic Flow measurement technology to be available on (almost) all future routers

- Fulfilling requirements of many applications
- Low hardware/software costs
- Simple and scalable
- Metering to be integrated in general purpose IP routers and other devices (probes, middleboxes)
- Data processing to be integrated into various applications
- Interoperability by openness or standardization

IPFIX WG: Expected Output

- Planned documents
  - Requirements RFC (almost completed)
  - Architecture RFC (just starting!)
  - Data model RFC (getting mature)
  - Applicability RFC (initial ideas, some text)
- Protocol development? Protocol selection!
- Configuration of measurements will not be standardized

IPFIX WG: Current Status

- Good support from IESG (Internet Engineering Steering Group)
- High interest from equipment manufacturers
  - Cisco designed NetFlow v9 compliant to IPFIX requirements
  - Cisco proposes to standardize NetFlow v9
  - NEC/Riverstone/Enterasys contributing much
  - Juniper is closely monitoring progress
- Highly skilled design team
  - approx. 15 people from Cisco, NEC, Riverstone, CAIDA, XACCT, …
- More information at http://ipfix.doit.wisc.edu

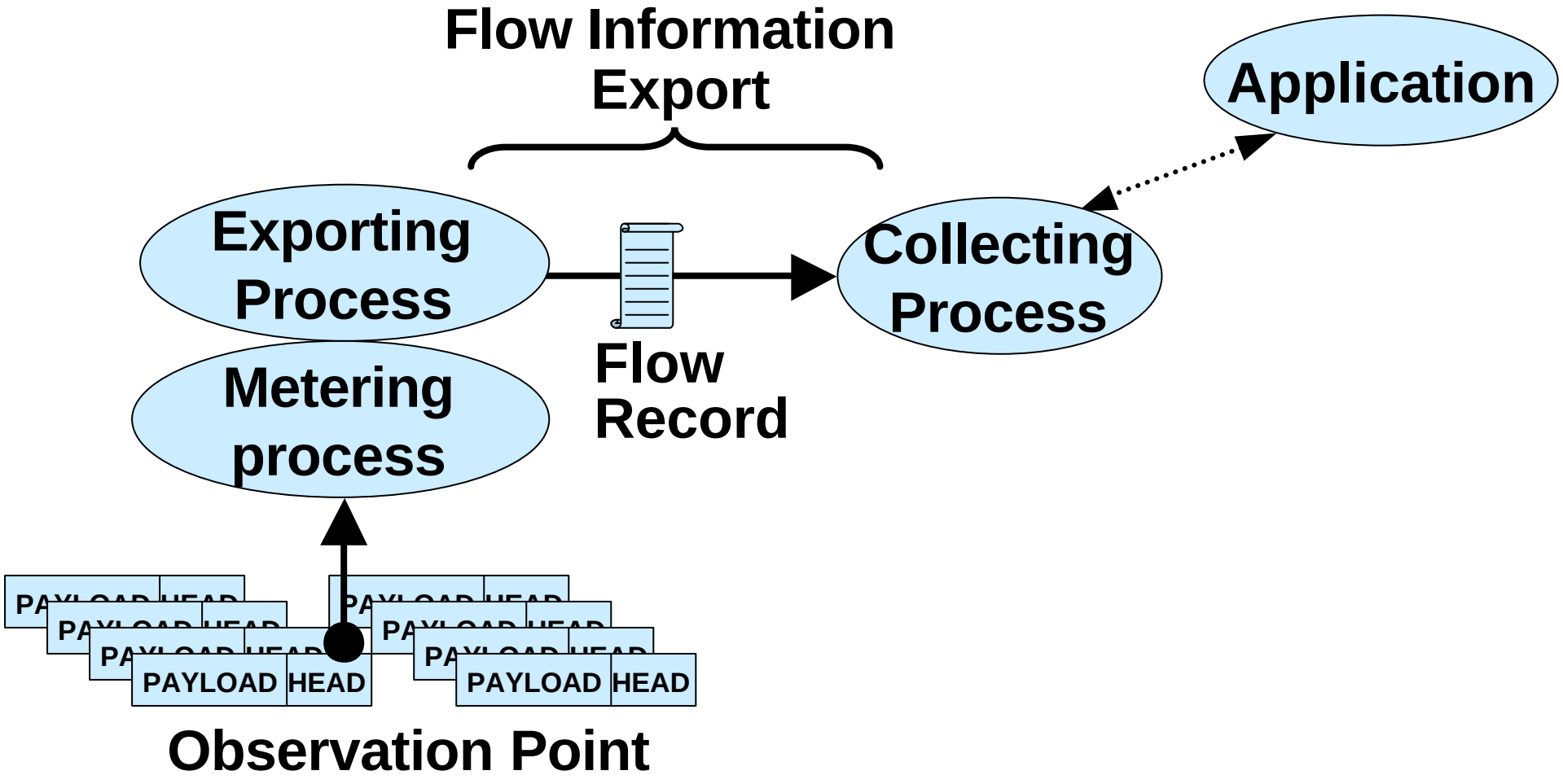
Target Applications (1)

- Usage-based accounting
  - input to charging and billing
  - various business model
    - time-based, volume-based, QoS class-based
    - per application, per user, per user group
- Traffic engineering
  - optimizing network usage
  - traffic analysis on congested links
    - origin of traffic
    - type of traffic
    - dynamic behavior (bursty, adaptive, …)
- Traffic profiling

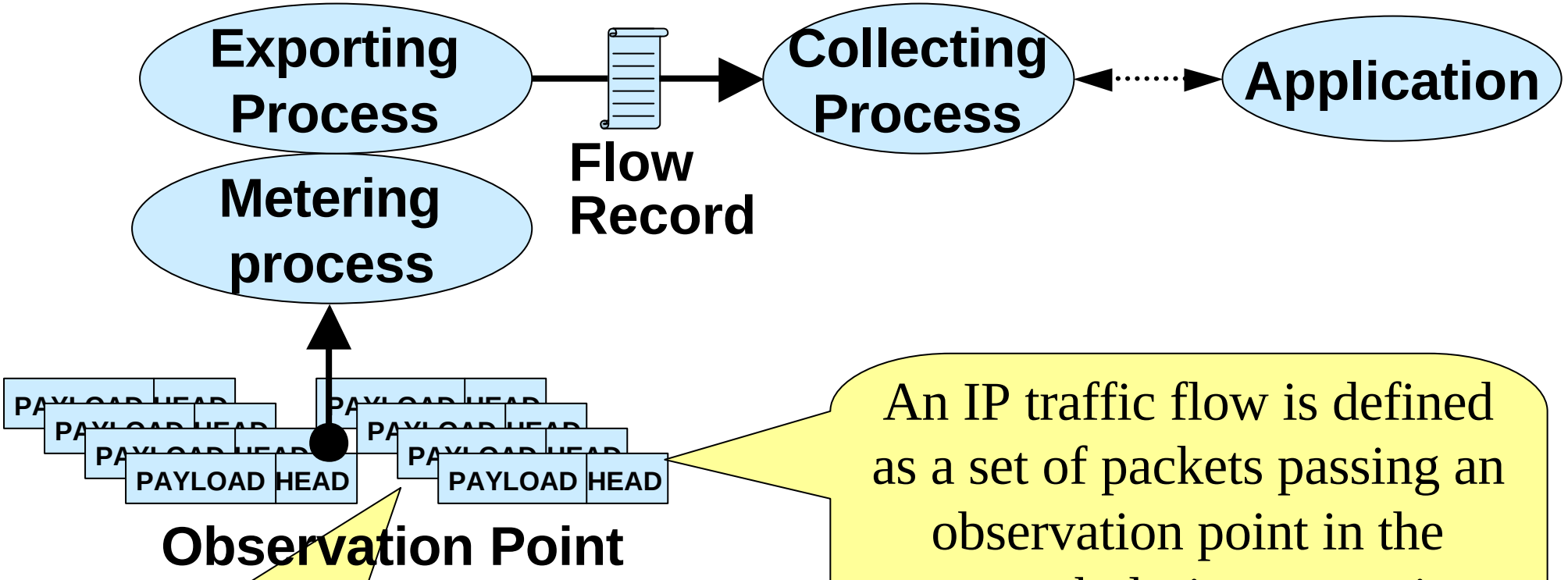
Target Applications (2)

- QoS monitoring
  - (passive) measurement of QoS properties
  - validating Service Level Agreements
- Attack detection and analysis
  - detecting (high volume) traffic patterns
  - investigation of origin of attacks
- Intrusion detection
  - detecting unexpected or illegal packets
- …

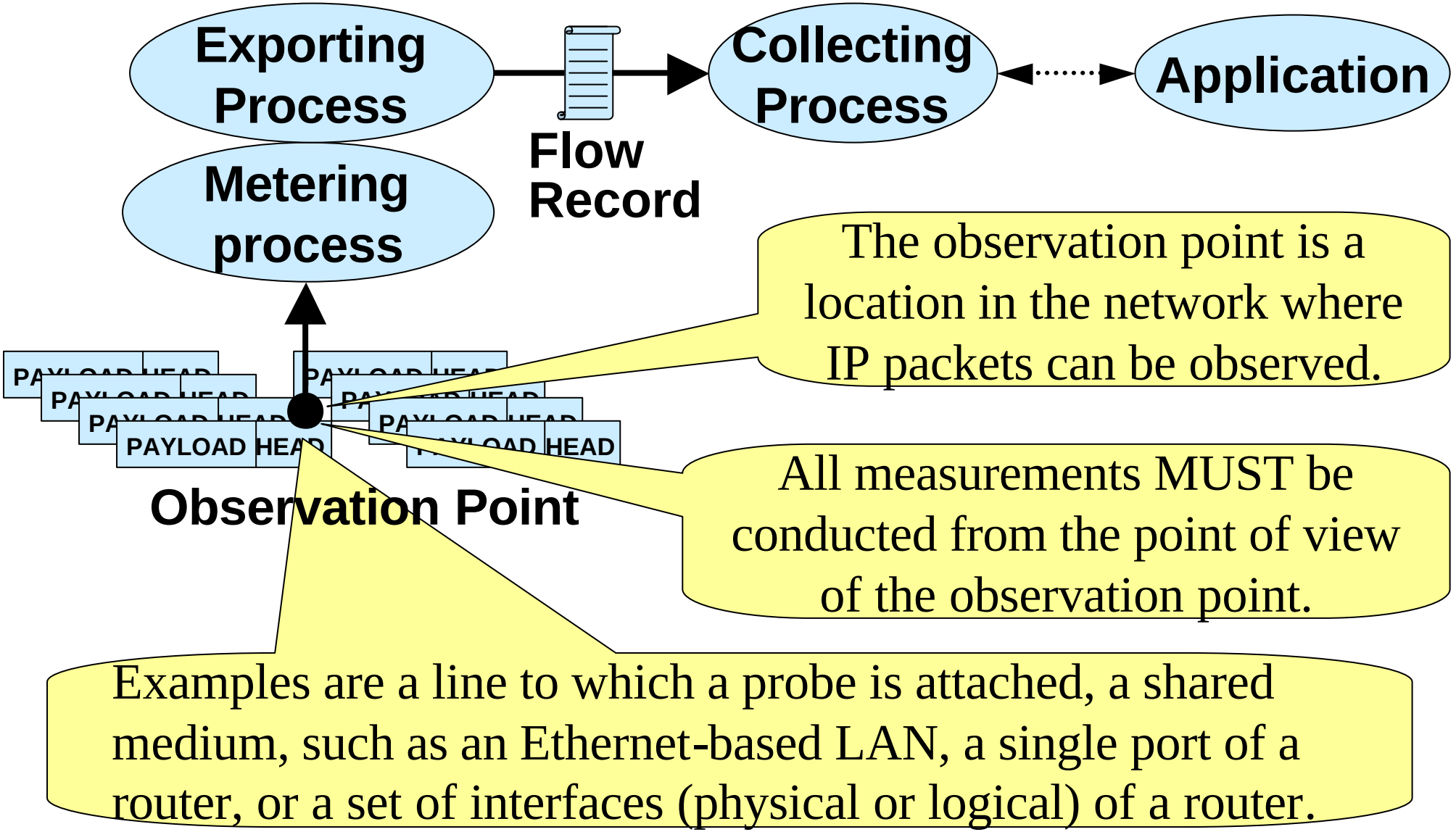
IPFIX Architecture Overview



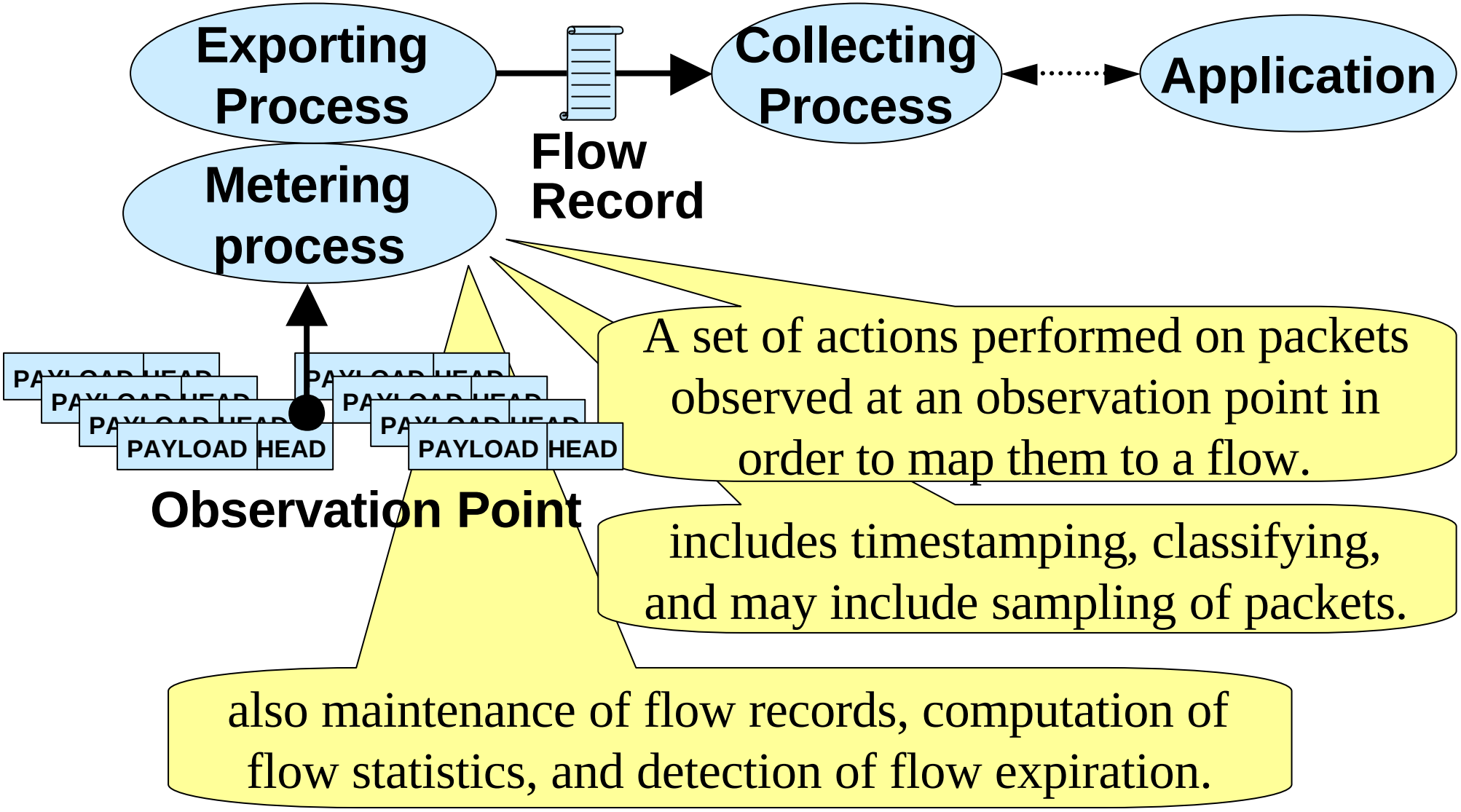
IPFIX Terminology: IP Traffic Flow



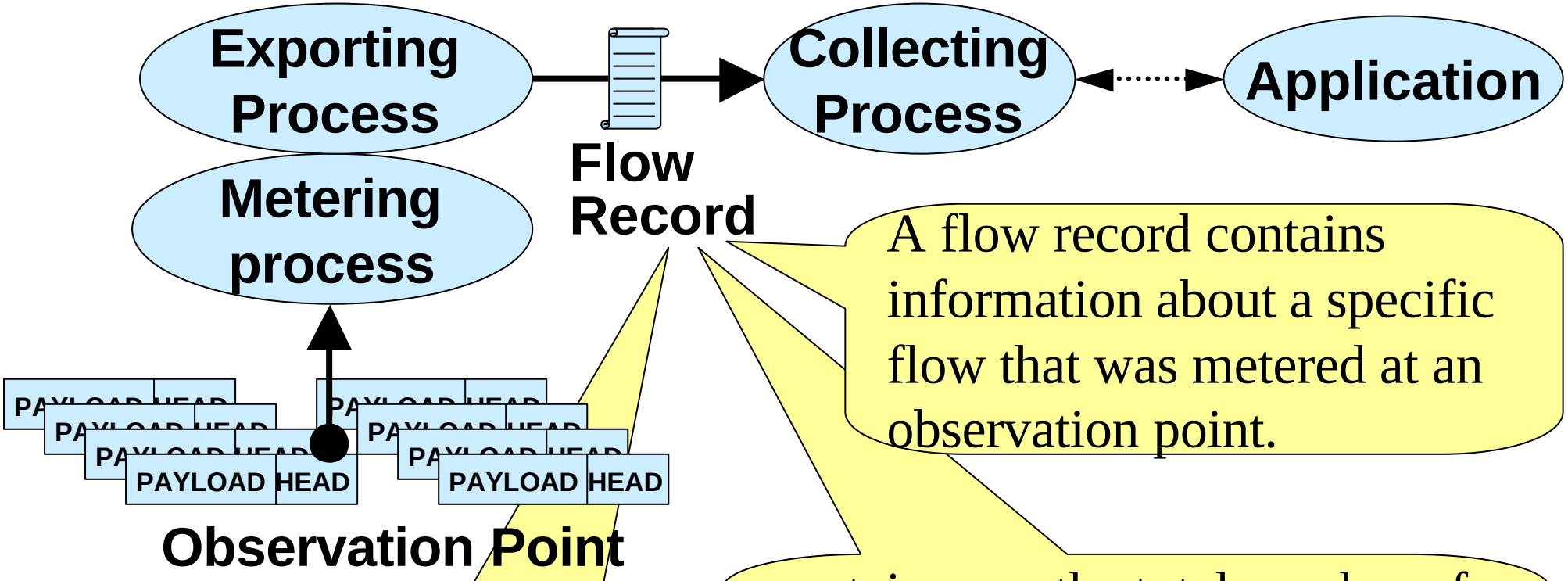
IPFIX Terminology: Observation Point



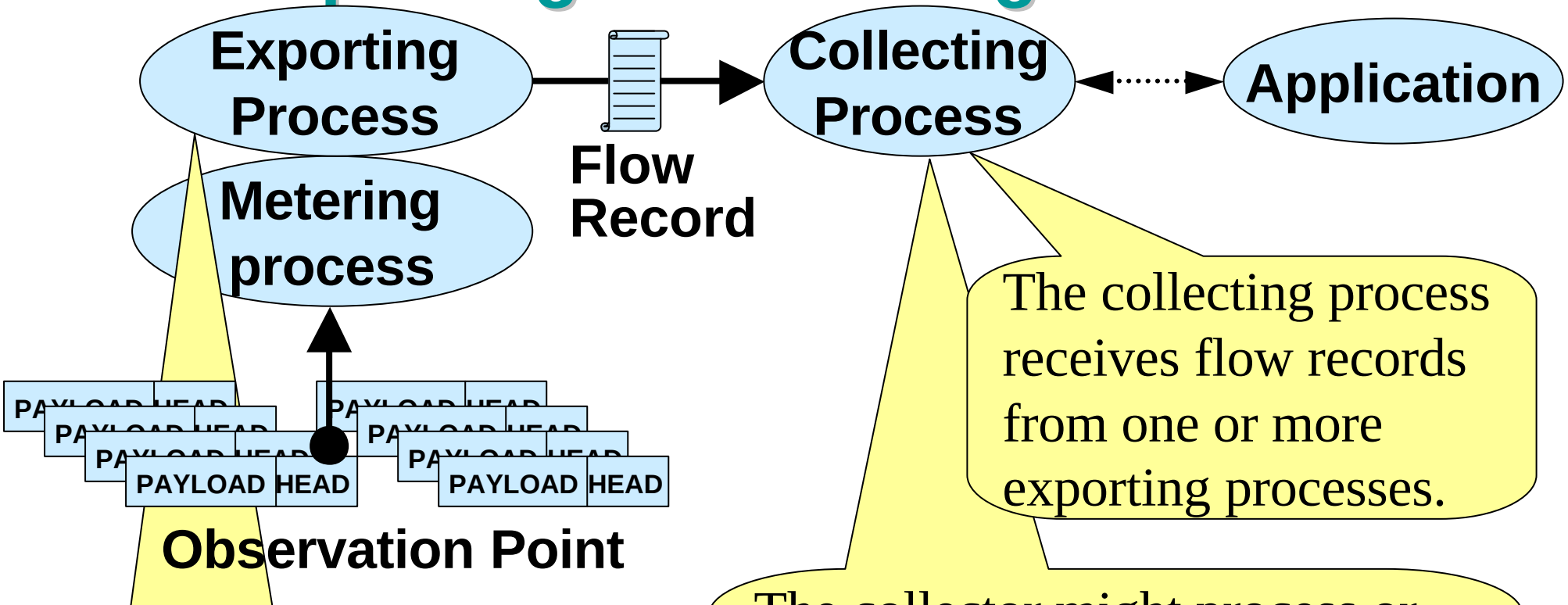
IPFIX Terminology: Metering Process



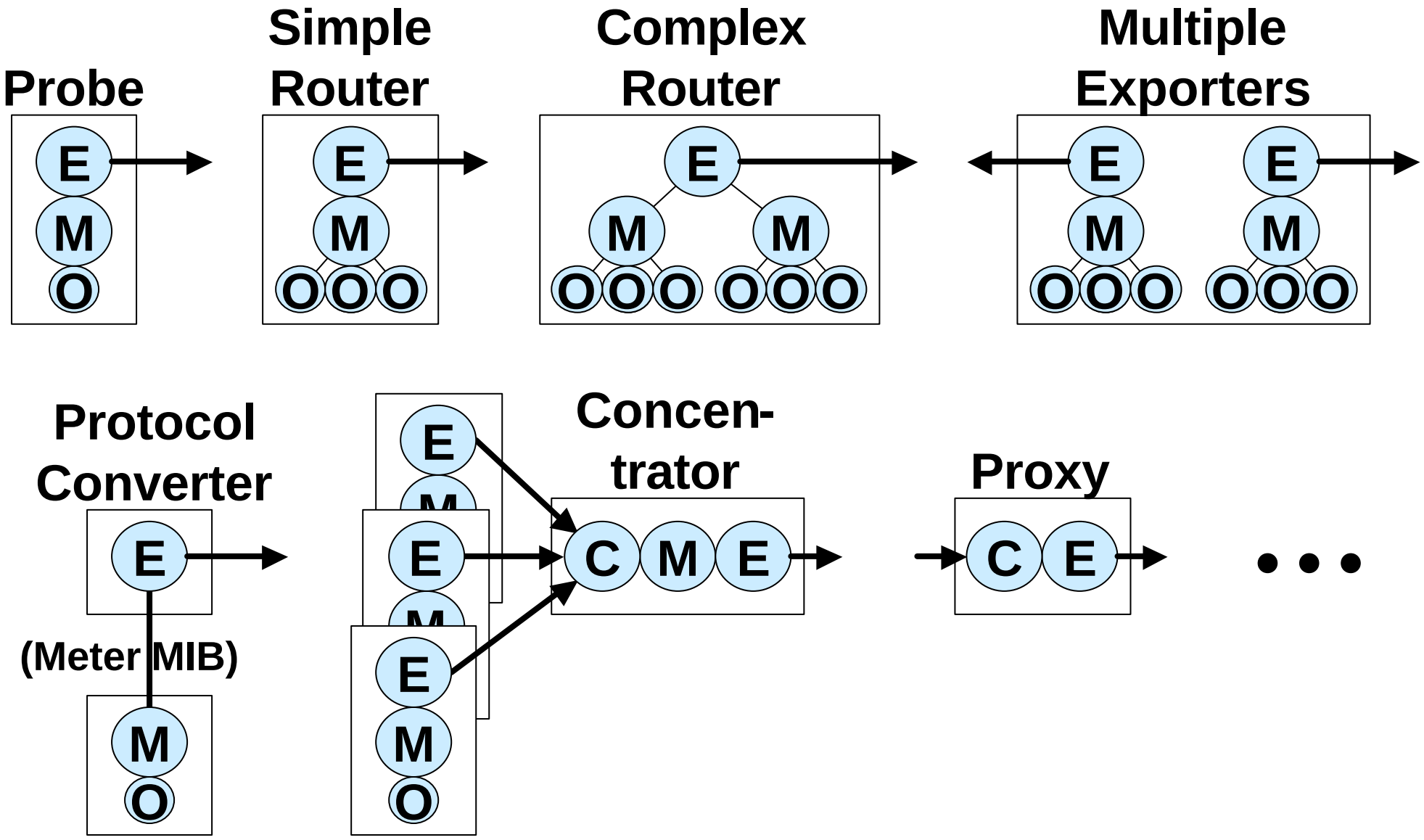
IPFIX Terminology: Flow Record



IPFIX Terminology: Exporting & Collecting Process



IPFIX-related Devices



Protocol Evaluation Process

- Candidate protocols
  - Need advocate person (no advocate, no evaluation)
  - Evaluation document (with regard to IPFIX requirements)
- Evaluation team
  - No members from companies proposing protocols
  - Preparing guidelines for advocates
  - Selecting and discussing individual evaluations with the advocates
  - Producing a joint evaluation document covering all candidate protocols

Existing Technologies

- IETF standards
  - RTFM
  - RMON, RMON2
- Proprietary technologies
  - NetFlow (Cisco)
  - sFlow (InMon)
  - LFAP (Riverstone)
  - Crane (XACCT)
  - DIAMETER

Critical Outlook: Potential Problems Still Ahead

- Is IPFIX already too complicated?
  - Flexible flow definition
  - Reliability
  - Congestion awareness
  - Flexible data format
- Many people might not be satisfied with not using UDP
- Cisco expects NetFlow v9 to be come standard
  - What if NetFlow v9 will not be the selected protocol?
- Of course - and always: Security issues

PSAMP

IETF PSAMP Working Group

- Packet Sampling (PSAMP)
  - BoF session in March 02, WG since July 02
- Focus on sampling and capturing packets and on transferring them to data collectors
- Target applications
  - Traffic profiling, monitoring network behavior
- Initiator: Nick Duffield, AT&T
- Closely Related to IPFIX
- Chairs
  - Andy Bierman, Cisco
  - Juergen Quittek, NEC
- Hot issues
  - (partial) export of payload
  - existing patents held by AT&T and HP

PSAMP Objectives

- Objectives (from charter)
  - Define standard set of capabilities for NW elements for supporting packet sampling
  - Domain-wide consistency of sampling schemes ➔consistent interpretation
  - Self-defining report format
  - Configuration of packet selectors
- Work Plan (from charter)
  - Specify packet sampling schemes
  - Define report structure (which includes packet fields)
  - Report stream: stream of reports of same type (format, sampling parameters,..)
  - Configuration MIB (sampling parameters,etc.)
- Differences to IPFIX unclear
  - Full packet capturing not in scope
  - Definition of standard sampling and classification rules
  - Use IPFIX as one option for transport
  - draft-quittek-psamp-ipfix-00.txt
- Documents
  - Framework: draft-ietf-psamp-framework-00.txt
  - Sampling and Filtering Techniques: draft-ietf-psamp-sample-tech-00.txt

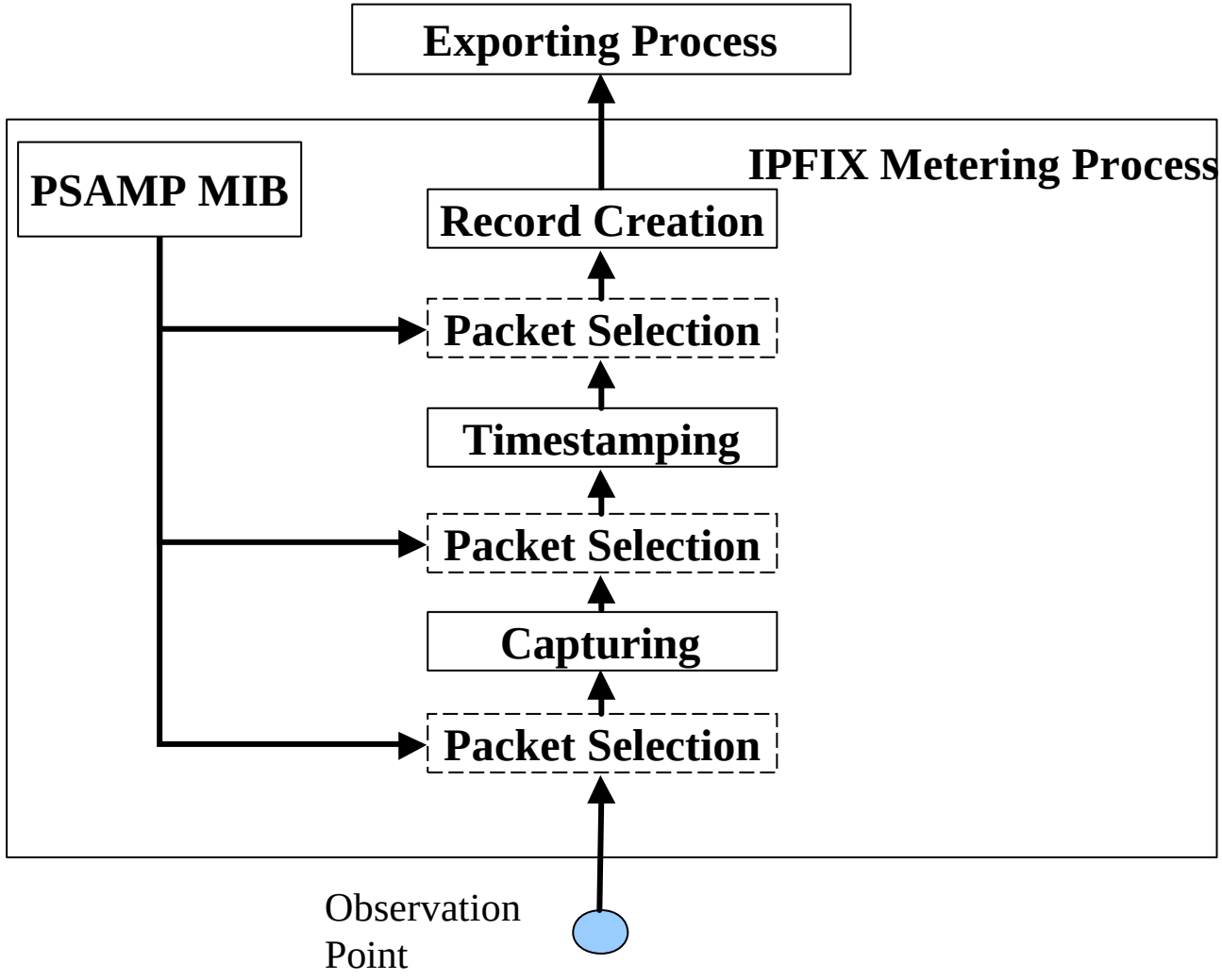
Information Models

- Information Models for Packet selection methods
  - What information needs to be provided to describe the method
  - Basis for
    - Configuration of methods
    - Reporting of technique in use to collector

Proposed Terminology

- Use IPFIX terms:
  - Metering, Exporting and Collection Process
  - Observation Point
  - Flow
- Packet Selection
  - Filtering
  - Sampling
  - Combinations
- Filtering
  - ***Deterministic*** function on parts of the ***packet content*** (header, payload)
  - can emulate a pseudo random selection
  - ➔ needs to process the packet for selection decision
- Sampling
  - ***Deterministic*** or ***random*** function on temporal or spatial ***packet position*** or
  - By performing ***random calculations*** per packet
  - ➔ may need packet position
- Packet Stream
  - Input stream for selector
  - Differs from IPFIX flow definition

Relation to IPFIX (my view)



Parameters

- Sampling
  - Random Sampling
    - n-out-of-N
      - Sample fraction n/N
    - Probabilistic
      - Sampling probability p
  - Systematic Sampling (equally spaced)
    - Time Based (temporal packet position)
      - Interval length (in time)
      - Spacing
    - Position based (spatial packet position)
      - Interval length (in packets)
      - Spacing

Parameters

- Filtering
  - Matching
    - Bitmask or interval
    - For header, payload or both
  - Hashing
    - Considered bits
    - Hash function and parameters
  - Router State
    - Router state/treatment that triggers selection
- Composite Schemes
  - Combination of basis schemes
  - Concatenated via STREAM_ID definition

Open Issues

- Focus on few standard selection methods ?
  - Which ?
  - How many ?
- Combined schemes
  - Linked
  - Or define as separate scheme
- Which aspects should be standardized ?
  - Schemes and Parameters
  - Configuration format
  - Reporting format
  - Configuration Protocol? SNMP ?
  - Reporting protocol ? IPFIX ?

Open Issues

- Categorization
  - Specify what input is required for the selection process
    - Filtering needs packet content
    - Sampling may need packet position
    - 3rd category for router state based filtering ?
  - Hashing
    - Would be a form of filtering
    - But: pseudo random sampling can be achieved with hashing
  - Useful categorization ? Other proposals ? Needed at all ?
- Relation to IPFIX
  - Packet selection as part of the IPFIX metering process
  - Associated IPFIX process
  - Alternative reporting protocols ?
  - will there be identifiers for observation points and IPFIX processes ?
  - Specify location of packet selection component in metering process
    - Document: draft-quittek-psamp-ipfix-00.txt

Further Groups

IP Performance Metrics (IPPM)

- Goal: Definition of Standard Metrics
  - Connectivity (RFC 2678)
  - One-way Delay (RFC 2679)
  - One-way Packet Loss (RFC 2680)
  - Round-trip Delay (RFC 2681)
  - One-way Loss Pattern Sample Metrics (RFC 3357)
  - IP Packet Delay Variation (RFC 3393)
- Current issues
  - Packet Reordering Metric
  - IPPM Reporting MIB
  - One-way-active Measurement Protocol
  - IP Measurement Protocol (IPMP)

Internet Measurement Research Group (IMRG)

- New IRTF group
- Measurement infrastructures (e.g., Surveyor, NIMI)
  - Scalability of meshes
  - Security of measurement tools
  - Access control, resource control, scheduling issues.
- Sharing measurement data within the community
  - Systematic way for storing measurements
  - Systems for remote sharing of measurement results
  - Remote configuration of measurements, analysis, and anonymization
- New measurement techniques
  - Forum for sharing preliminary findings
  - Encourage further work and collaboration
- Developing models based on network measurements
  - Understand network dynamics
  - Aiding researchers
  - Conduct useful simulations of the network.
- Foster communication between the research and operations communities
  - Requirements from operators
  - Core problems that need to be addressed
  - "wish list" of outstanding problems

Authentictaion Authorization and Accounting (AAA, AAAARCH)

- AAA
  - IETF group
  - Focus on network access (e.g. mobile IP)
  - Standardization of DIAMETER protocol
  - Accounting RFCs:
    - Introduction to Accounting Management (RFC 2975)
    - Accounting Attributes and Record Formats (RFC 2924)
- AAAARCH
  - IRTF group
  - Generic Architecture for AAA
  - Policy-based Accounting (RFC3334)

Related EU Projects

InterMon – Advanced architecture for INTER-domain quality of service MONitoring, modelling and visualisation

- **Target**: Inter-domain QoS measurement + analysis + visualization
- **Solution**: Develop a scalable inter-domain QoS control architecture with integrated components for:
  - *topology discovery* by analyzing routing advertisements
  - *measurement / monitoring* of network traffic
  - *traffic modeling* based on measurement data
  - *simulation* of data traffic / network behavior
  - *data mining* aggregation of collected information
  - *visualization* with interactive data exploration
- **Targeted customers**: Internet service providers, QoS enabled end system developers, network operators
- **Purpose**: operative control, planning and optimisation, experiments with traffic QoS classes

InterMon Workshop: February 20-21, 2003 Salzburg, Austria

www.ist-intermon.org

6QM - IPv6
Quality of Service Measurement

- Measurement Requirements for IPv6 networks
  - Accounting
  - SLA validation
- Development of Measurement components for IPv6 networks
  - Passive and active measurements
  - Measurement configuration
  - IPFIX reporting
- Dissemination and Linkage with other related Foras and Projects, in order to publicize the project results.
  - Deployment of measurement components in IPv6 research networks (6net, Euro6, etc.)

www.6qm.org

Thank You