

IP Flow Information eXport (IPFIX)

Carsten Schmoll
carsten.schmoll@fokus.fraunhofer.de

IPFIX – IETF Working Group



- IP Flow Information eXport (IPFIX) WG
 - Successor of RTFM (Real-Time Flow Measurement) WG
 - IPFIX BoF sessions 12/2000 and 08/2001
 - WG active since 10/2001
- Target
 - (official): standardizing current practice in flow data export
 - define “IP flow” and specify a transport mapping for it
 - (unofficial): standardizing (something like) Cisco NetFlow
- Chairs
 - Nevil Brownlee, CAIDA
 - David Plonka, University of Wisconsin

IPFIX - Motivation

- **IP packet flow** information is often gathered and exported
- **from** IP devices such as routers or measurement stations
- **to** mediation, accounting, and network management systems
- **including** (a) those attributes derived from the IP packet headers and (b) attributes known only to the exporter (e.g. ingress and egress ports, network prefix)
- **for** the purposes of Internet research, measurement, accounting, and billing.

- **IPFIX WG goal:** develop and standardize a generalized flow export methodology (easier than to support N export protocols)
- develop a data model, which represents the flow information
- select a (congestion-aware) transport protocol by which IP flow information can be transferred in a timely fashion

IPFIX Scope

- Select or develop a basic common IP Traffic Flow measurement technology
- Goal to have it implemented on (almost) all future routers (vendor support)
- Simple and scalable
- Low hardware/software costs (overhead)
- Metering to be integrated in IP routers as well as other devices (software probes, middleboxes)
- Data processing to be integrated into various applications
- Interoperability by standardization and openness

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, ...)

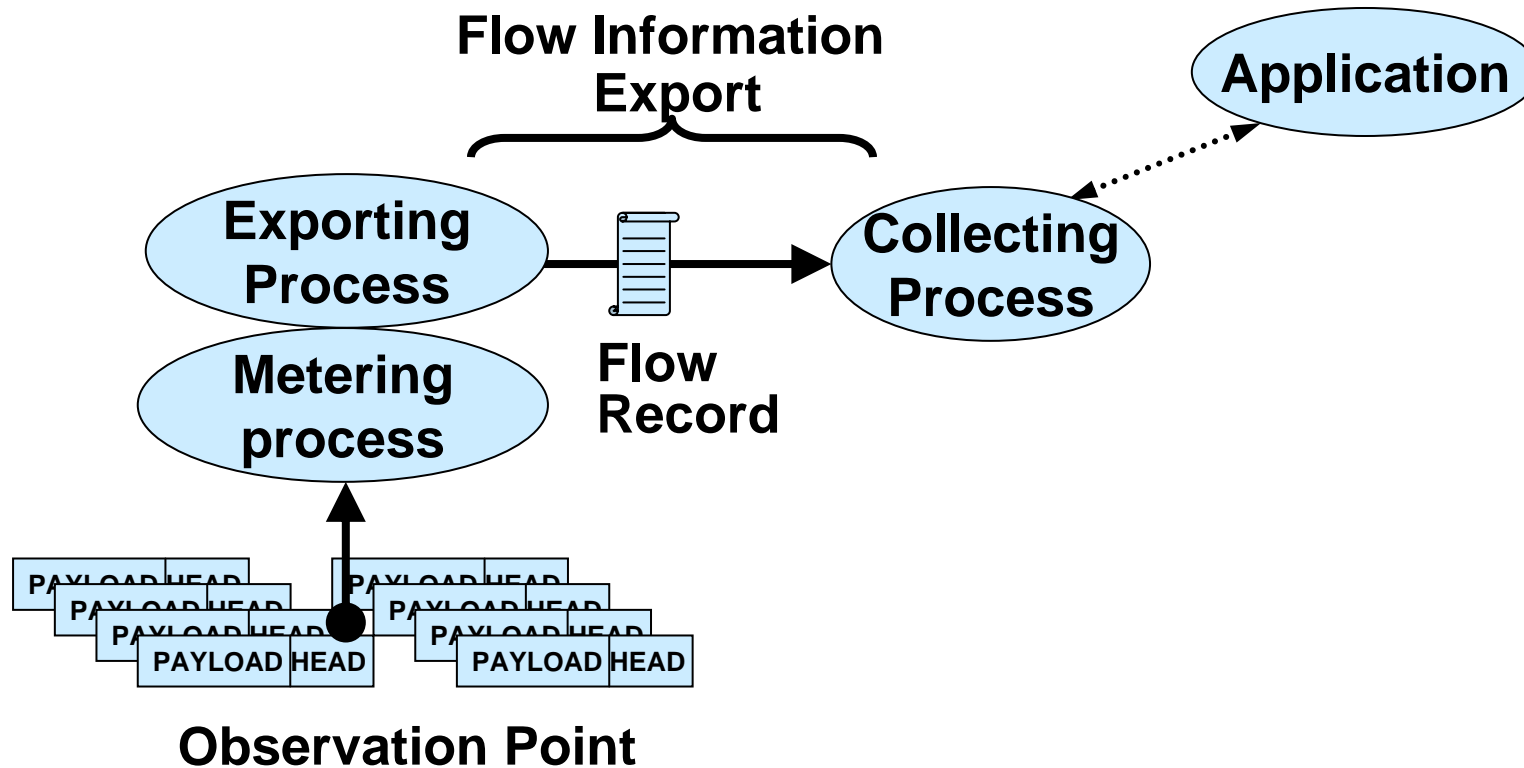
Target Applications (2)

- Traffic profiling
- 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
- more conceivable (even non-IP flow related)

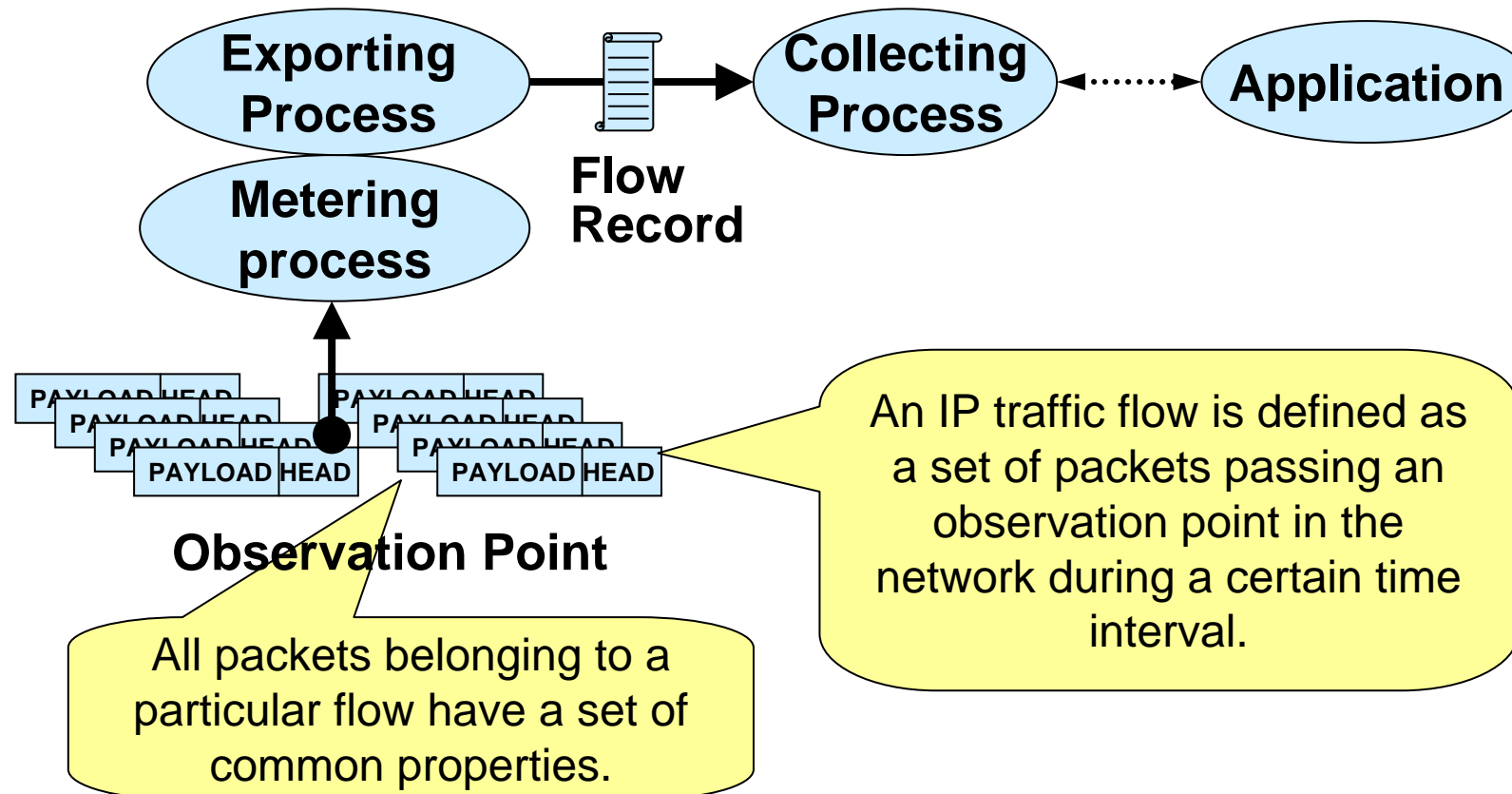
Existing Technologies

- IETF standards:
 - RTFM (NeTraMet)
 - RMON, RMON2
 - DIAMETER
- Proprietary technologies:
 - NetFlow v4/5/9 (Cisco)
 - sFlow (InMon)
 - LFAP (Riverstone)
 - Crane (XACCT)

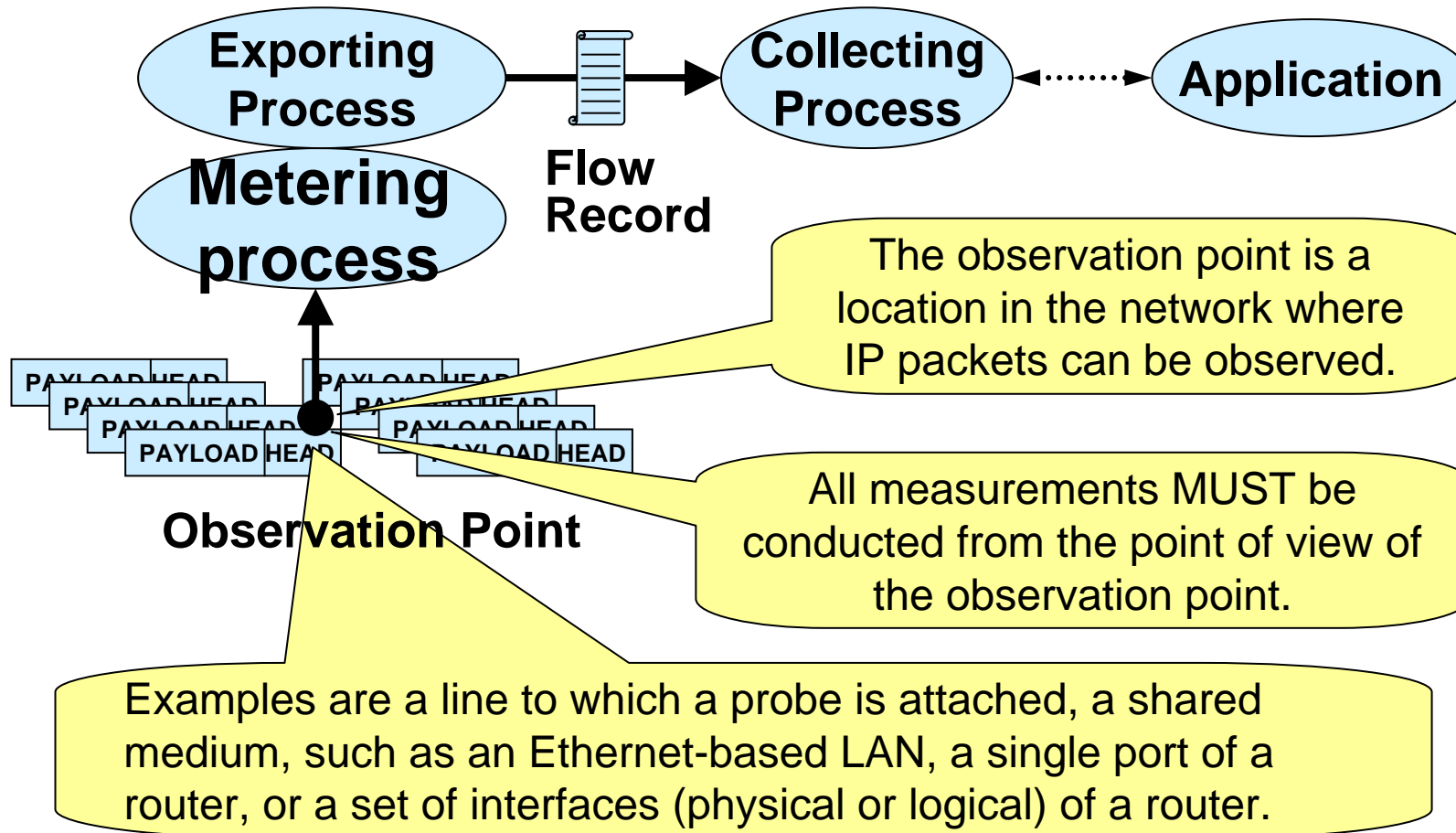
IPFIX Architecture Overview



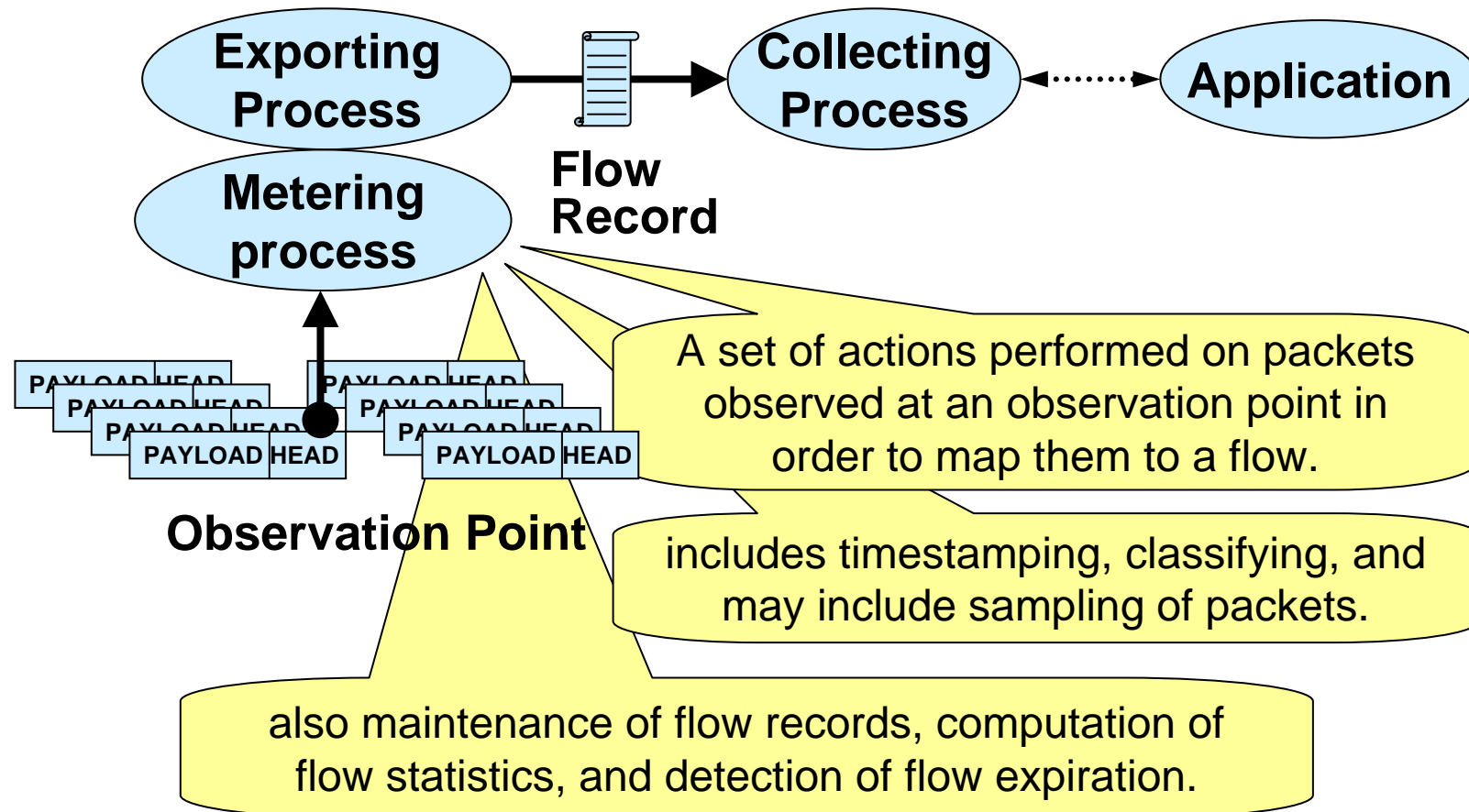
IPFIX Terminology: IP Traffic Flow



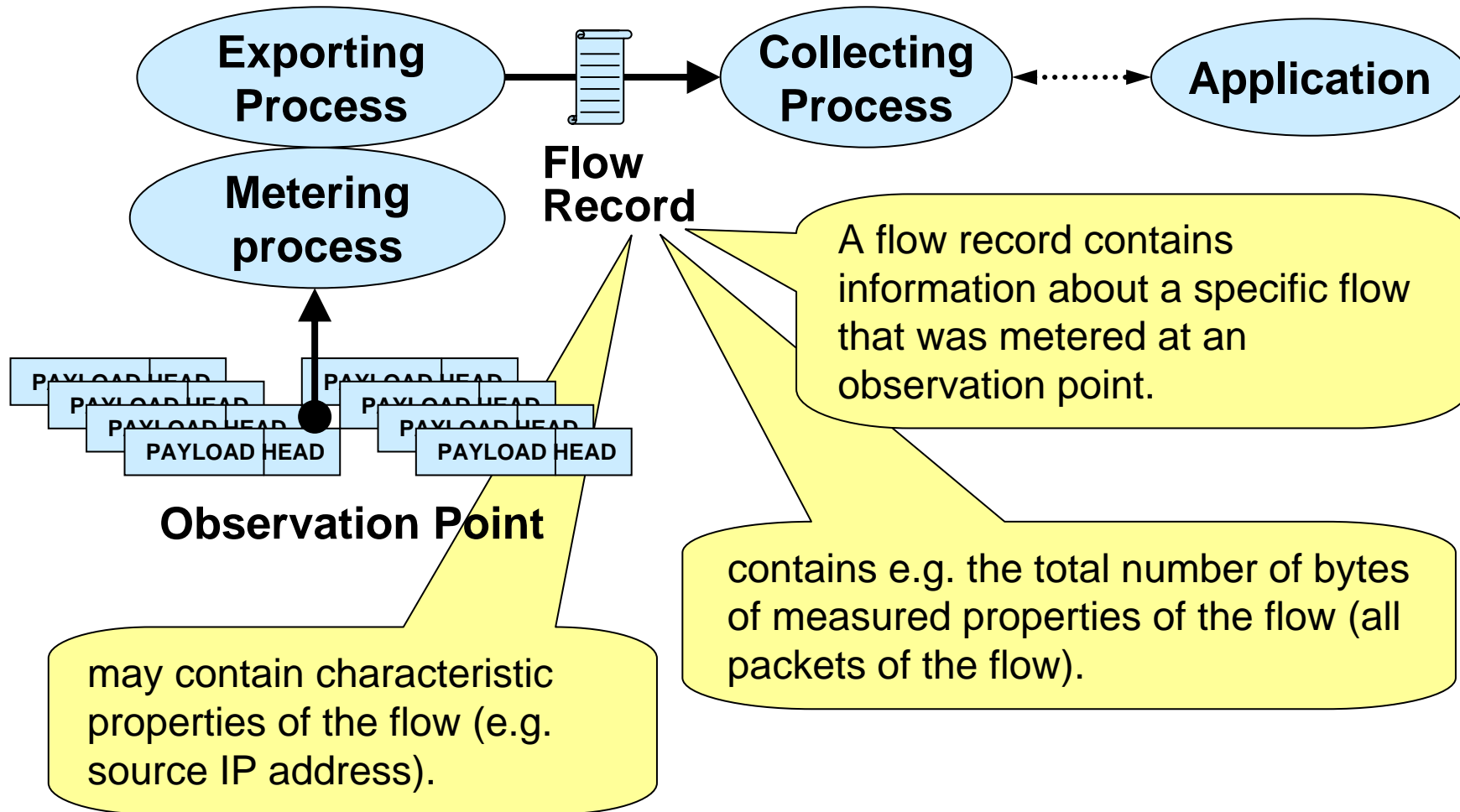
IPFIX Terminology: Observation Point



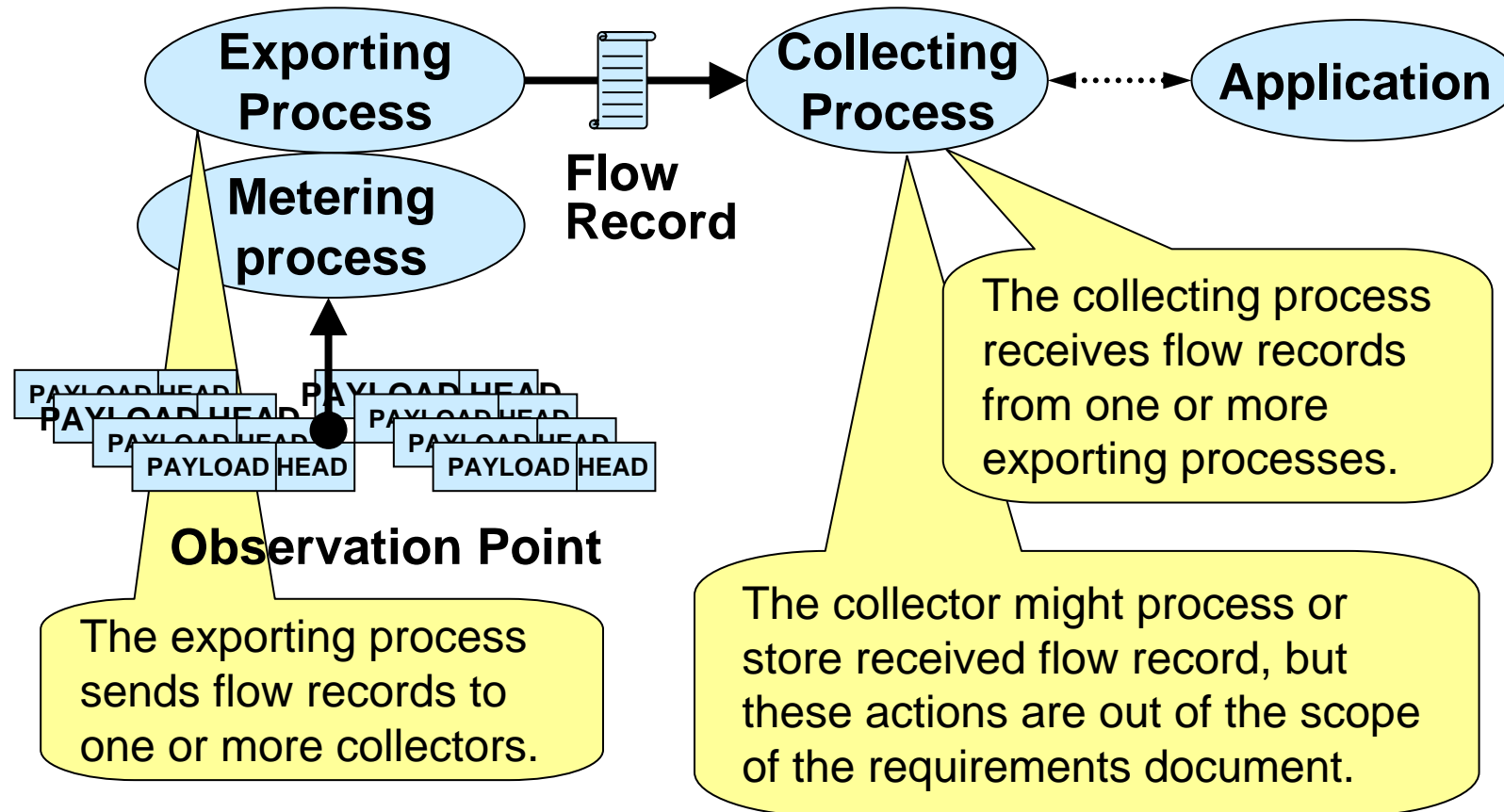
IPFIX Terminology: Metering Process



IPFIX Terminology: Flow Record



IPFIX Terminology: Exporting & Collecting Process



IPFIX – 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, Fraunhofer, ...

IPFIX – RFCs and Drafts

- Request For Comments (RFCs):
 - RFC 3917: Requirements for IP Flow Information Export
 - RFC 3955: Evaluation of Candidate Protocols for IP Flow Information Export (IPFIX)
- Current Drafts:
 - Architecture for IP Flow Information Export (IESG last call)
 - Information Model for IP Flow Information Export (IESG last call)
 - IPFIX Protocol Specification + IPFIX Applicability (IESG last call)
 - IPFIX Implementation Guidelines (new, ongoing)
 - Use of IPFIX for Export of Per-Packet Information (name change)
 - Inter-domain Data Exchange Questionnaire (new, related)
- Out of Scope:
 - Configuration of measurements will not be standardized

IPFIX – Critical Outlook

- Potential Problems Still Ahead:
 - Is IPFIX already too complicated?
 - Very flexible flow definition
 - Reliability
 - Congestion awareness
 - Flexible data format
 - Many people might not be satisfied with *not* using UDP
 - Cisco NetFlow v9 to become standard
 - Of course (as always): Security issues to be resolved

IPFIX – Recent/Upcoming

- July 2005 – Interoperability Event
 - including IPFIX Tests
 - there five implementations „attended“
 - each brought exporter and collector
 - impl. problems → impl. guidelines
- with regard to the IPFIX protocol
 - some ambiguities have been identified
 - behavior in certain cases need to be defined
 - to be discussed in the IETF IPFIX WG session

Contact

- IPFIX:
 - <http://ipfix.doit.wisc.edu>
 - <http://www.ietf.org/html.charters/ipfix-charter.html>
- Mailing Lists:
 - General Discussion: ipfix@net.doit.wisc.edu
 - To Subscribe: majordomo@net.doit.wisc.edu
(in Body: subscribe ipfix)
 - Archive: <http://ipfix.doit.wisc.edu/archive/>
- Chair(s):
 - Nevil Brownlee <n.brownlee@auckland.ac.nz>
 - Dave Plonka <plonka@doit.wisc.edu>

Thank you!

MOME

- Questions?
- Discussion