Master Kurs
Rechnernetze
Computer Networks
IN2097

Prof. Dr.-Ing. Georg Carle
Dr. Thomas Fuhrmann

Institut für Informatik
Technische Universität München
http://www.net.in.tum.de

Network Monitoring

- Introduction
- Architecture & Mechanisms
- Protocols
  - IPFIX (Netflow Accounting)
  - PSAMP (Packet Sampling)
- Scenarios

Network Measurements

- Active measurements
  - “intrusive”
  - Measurement traffic is generated and fed into the operational network
  - Advantages
    - Straightforward
    - Does not depend on existing traffic by active applications
    - Allows measurement of specific parts of the network
  - Disadvantages
    - Additional load
    - Network traffic is affected by the measurement
    - Measurements are influenced by (possibly varying) network load

Network Measurements II

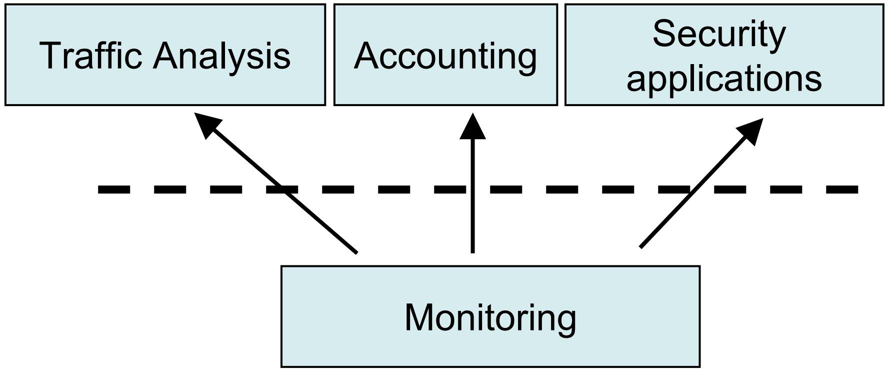
- Passive measurements (or **Network Monitoring**)
  - “non-intrusive”
  - Monitoring of existing traffic
  - Establishing of packet traces at different locations
  - Identification of packets, e.g. using hash values
  - Advantages
    - Does not affect applications
    - Does not modify the network behavior
  - Disadvantages
    - Requires active network traffic
    - Limited to analysis of existing / current network behavior, situations of high load, etc. cannot be simulated/enforced
    - Does not allow the transport of additional information (time stamps, etc.) within measured traffic

Network Measurements III

- Hybrid measurements
  - Modification of packet flows
    - Piggybacking
    - Header modification
  - Advantages
    - Same as for “passive”
    - additional information can be included (time-stamps, etc.)
  - Disadvantages
    - Modifying of data packets may cause problems if not used carefully

Network Monitoring

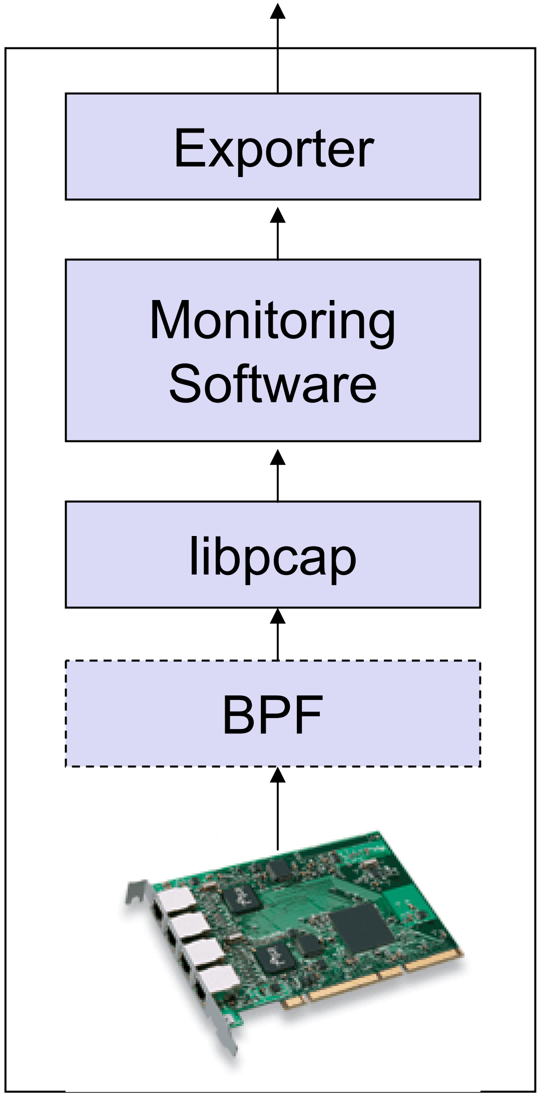
- Applications of network monitoring
  - Traffic analysis
    - Traffic engineering
    - Anomaly detection
  - Accounting
    - Resource utilization
    - Accounting and charging
  - Security
    - Intrusion detection
    - Detection of prohibited data transfers (e.g., P2P applications)



- Open issues
  - Protection of measurement data against illegitimate use (encryption, …)
  - Applicable law (“lawful interception”)

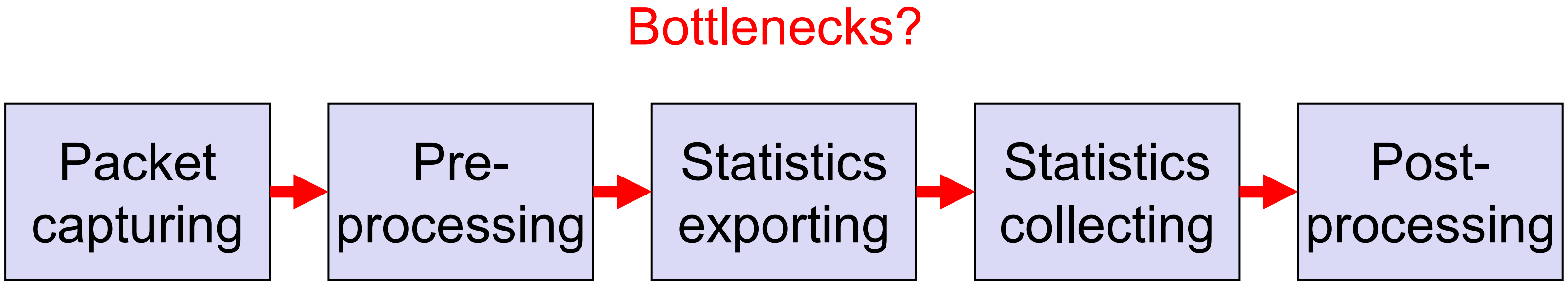
Monitoring Probe

- ❑ Standardized data export
- ❑ Monitoring Software
- ❑ HW adaptation, [filtering]
- ❑ OS dependent interface (BSD)
- ❑ Network interface



High-Speed Network Monitoring

- Requirements
  - Multi-Gigabit/s Links
  - Cheap hardware and software → standard PC
  - Simple deployment
- Problems
  - Several possible bottlenecks in the path from capturing to final analysis



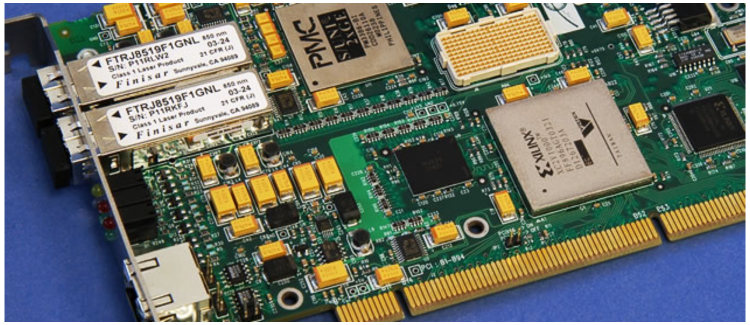
High-Speed Network Monitoring II

- Approaches
  - High-end (intelligent) network adapters
  - Sophisticated algorithms for
    - Maintaining packet queues
    - Elimination of packet copy operations
    - Managing hash tables describing packet flows
  - Sampling
  - Filtering
  - Aggregation

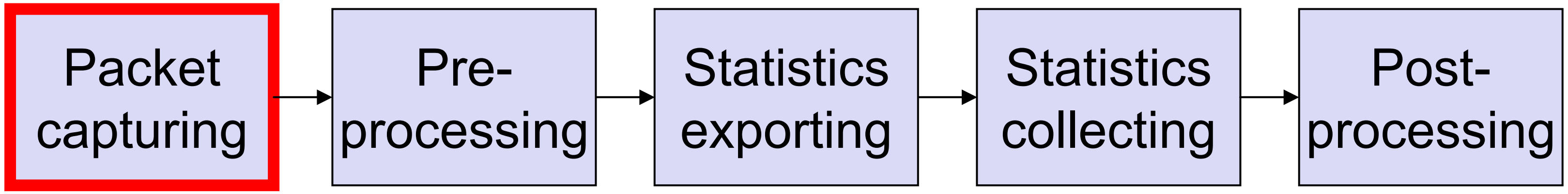
Special Network Adapters

- ❑ Server NICs (Network Interface Cards)
  - ▪ Direct access to main memory (without CPU assistance)
  - ▪ Processing of multiple packets in a single block (reduction of copy operations)

    → Reduced interrupt rates



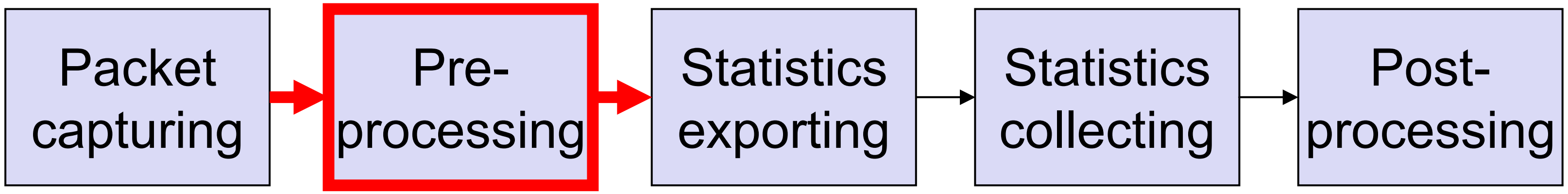
- ❑ Monitoring interface cards
  - ▪ Dedicated monitoring hardware
  - ▪ Programmable, i.e. first preprocessing steps can be done at the network interface



Packet capturing → Pre-processing → Statistics exporting → Statistics collecting → Post-processing

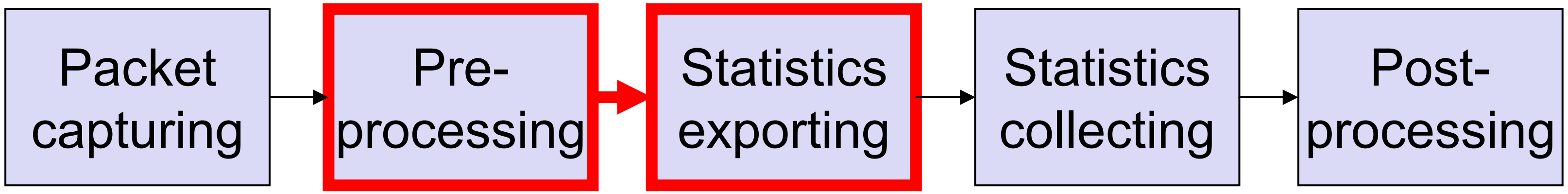
Memory Management

- Hash-tables
  - Allow fast access to previously stored information
  - Depending on the requirements, different parameters can be chosen as hash values
- Reduction of copy operations
  - Copy operations can be reduced by only transferring references pointing to memory positions holding the packet
  - Management of the memory is complex, garbage collection required
- Aggregation
  - If aggregated results are sufficient, only counters have to be maintained



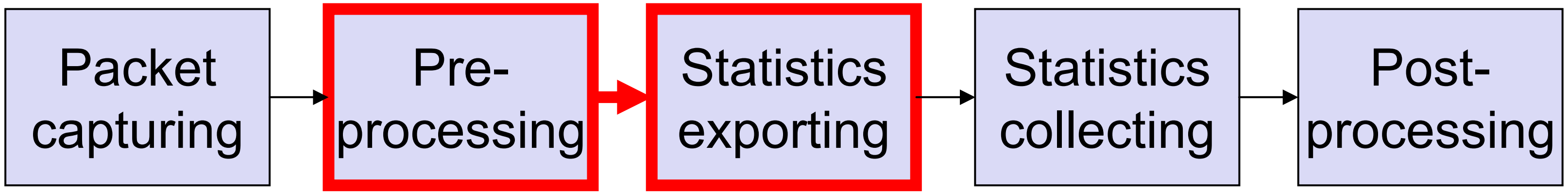
Packet Sampling

- Goals
  - Reduction of the number of packets to analyze
  - Statistically dropping packets
- Sampling algorithms
  - Systematic sampling
    - Periodic selection of every n-th element of a trace
    - Selection of all packets that arrive at pre-defined points in time
  - Random sampling
    - n-out-of-N
    - Probabilistic



Packet Filtering

- Goals
  - Reduction of the number of packets to analyze
  - Possibility to look for particular packet flows in more detail, or to completely ignore other packet flows
- Filter algorithms (explained subsequently)
  - Mask/match filtering
  - Router state filtering
  - Hash-based selection



Packet capturing

Pre-processing

Statistics exporting

Statistics collecting

Post-processing

Packet Filtering – Algorithms

- Mask/match filtering
  - Based on a given mask and value
  - In the simplest case, the selection range can be a single value in the packet header
  - In general, it can be a sequence of non-overlapping intervals of the packet
- Router state filtering
  - Selection based on one or multiple of the following conditions
    - Ingress/egress interface is of a specific value
    - Packet violated ACL on the router
    - Failed RPF (Reverse Path Forwarding)
    - Failed RSVP
    - No route found for the packet
    - Origin/destination AS equals a specific value or lies within a given range

Packet Filtering – Algorithms II

- Hash-based filtering
  - Hash function h maps the packet content c, or some portion of it, to a range R
  - The packet is selected if h(c) is an element of S, which is a subset of R called the selection range
  - Required statistical properties of the hash function h
    - h must have good mixing properties
      - Small changes in the input cause large changes in the output
      - Any local clump of values of c is spread widely over R by h
      - Distribution of h(c) is fairly uniform even if the distribution of c is not

Packet Filtering – Algorithms III

- Hash-based filtering (cont.)
  - Usage
    - Random sampling emulation
      - Hash function (normalized) is a pseudorandom variable in the interval [0,1]
    - Consistent packet selection and its application
      - Also known as trajectory sampling
      - If packets are selected quasi-randomly using identical hash function and identical selection range at different points in the network, and are exported to a collector, the latter can reconstruct the trajectories of the selected packets
      - Applications: network path matrix, detection of routing loops, passive performance measurement, network attack tracing

IPFIX: IP Flow Information Export

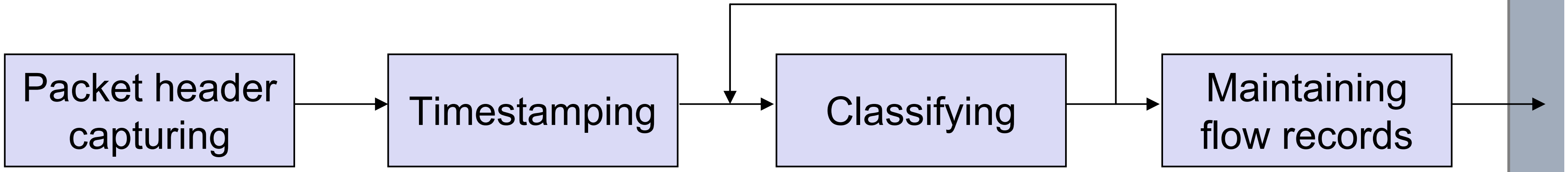
- IPFIX (IP Flow Information eXport) IETF Working Group
  - Standard track protocol based on Cisco Netflow v5…v9
- Goals
  - Collect usage information of individual data flows
  - Accumulate packet and byte counter to reduce the size of the monitored data
- Approach
  - Each flow is represented by its IP 5-tupel (prot, src-IP, dst-IP, src-Port, dst-Port)
  - For each arriving packet, the statistic counters of the appropriate flow are modified
  - If a flow is terminated (TCP-FIN, timeout), the record is exported
  - Sampling algorithms can be activated to reduce the # of flows or data to be analyzed
- Benefits
  - Allows high-speed operation (standard PC: up to 1Gbps)
  - Flow information can simply be used for accounting purposes as well as to detect attack signatures (increasing # of flows / time)

IPFIX - IP Flow Information Export Protocol

- RFCs
  - Requirements for IP Flow Information Export (RFC 3917)
  - Evaluation of Candidate Protocols for IP Flow Information Export (RFC3955)
  - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information (RFC 5101)
  - Information Model for IP Flow Information Export (RFC 5102)
  - Bidirectional Flow Export using IP Flow Information Export (IPFIX) (RFC 5103)
  - IPFIX Implementation Guidelines (RFC 5153)
- Information records
  - **Template Record** defines structure of fields in **Flow Data Record**
  - Flow Data Record is a data record that contains values of the Flow Parameters
- Transport protocol: transport of information records
  - SCTP must be implemented, TCP and UDP may be implemented
  - SCTP should be used
  - TCP may be used
  - UDP may be used (with restrictions – congestion control!)

IPFIX – Terminology

- IP Traffic Flow
  - A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties.
- Observation Point
  - The observation point is a location in the network where IP packets can be observed. One observation point can be a superset of several other observation points.
- Metering Process
  - The metering process generates flow records. It consists of a set of functions that includes packet header capturing, timestamping, sampling, classifying, and maintaining flow records.


Packet header capturing

Timestamping

Classifying

Maintaining flow records

IPFIX – Terminology II

- Flow Record
  - A flow record contains information about a specific flow that was metered at an observation point. A flow record contains measured properties of the flow (e.g. the total number of bytes of all packets of the flow) and usually also characteristic properties of the flow (e.g. the source IP address).
- Exporting Process
  - The exporting process sends flow records to one or more collecting processes. The flow records are generated by one or more metering processes.
- Collecting Process
  - The collecting process receives flow records from one or more exporting processes for further processing.

IPFIX – Devices

```
            +---+     +-----+     +---------+       +---------+
            | E-+->   |  E--+->   |    E----+->   <-+--E   E--+->
            | | |     |  |  |     |   / \   |       |  |   |  |
            | M |     |  M  |     |  M   M  |       |  M   M  |
            | | |     | /|\ |     | /|\ /|\ |       | /|\ /|\ |
            | O |     | OOO |     | OOO OOO |       | OOO OOO |
            +---+     +-----+     +---------+       +---------+
            Probe      Basic       Complex          Multiple
                       Router       Router           Exporting
                                                     Processes
          +---+     +---+     +---+
          | E-+->   | E-+->   | E-+------------->---+
          | | |     | | |     | | | +---+         +-+-----+
          +-+-+     | M |     | M | | E-+------->-+-C-M-E-+->
            |       | | |     | | | | | | +---+   +-+-----+
          +-+-+     +-+-+     | O | | M | | E-+->---+
          | | |       |       +---+ | | | | | |
          | M |     +-+-+           | O | | M |
          | | |     | | |           +---+ | | |           +-----+
          | O |     | O |                 | O |        ->-+-C-E-+->
          +---+     +---+                 +---+           +-----+

         Protocol   Remote             Concentrator        Proxy
         Converter  Observation

O ... Observation point
M ... Metering process
E ... Exporting process
```

IPFIX – Work Principles

- Identification of individual traffic flows
  - 5-tupel: Protocol, Source-IP, Destination-IP, Source-Port, Destination-Port
  - Example: TCP, 134.2.11.157, 134.2.11.159, 2711, 22

- Collection of statistics for each traffic flow
  - # bytes
  - # packets

- Periodical statistic export for further analysis

Flow	Packets	Bytes
TCP, 134.2.11.157,134.2.11.159, 4711, 22	10	5888
TCP, 134.2.11.157,134.2.11.159, 4712, 25	7899	520.202

IPFIX – Applications

- Usage based accounting
  - For non-flat-rate services
  - Accounting as input for billing
  - Time or volume based tariffs
  - For future services, accounting per class of service, per time of day, etc.
- Traffic profiling
  - Process of characterizing IP flows by using a model that represents key parameters such as flow duration, volume, time, and burstiness
  - Prerequisite for network planning, network dimensioning, etc.
  - Requires high flexibility of the measurement infrastructure
- Traffic engineering
  - Comprises methods for measurement, modeling, characterization, and control of a network
  - The goal is the optimization of network resource utilization

IPFIX – Applications II

- Attack/intrusion detection
  - Capturing flow information plays an important role for network security
  - Detection of security violation
    1) detection of unusual situations or suspicious flows
    2) flow analysis in order to get information about the attacking flows
- QoS monitoring
  - Useful for passive measurement of quality parameters for IP flows
  - Validation of QoS parameters negotiated in a service level specification
  - Often, correlation of data from multiple observation points is required
  - This required clock synchronization of the involved monitoring probes

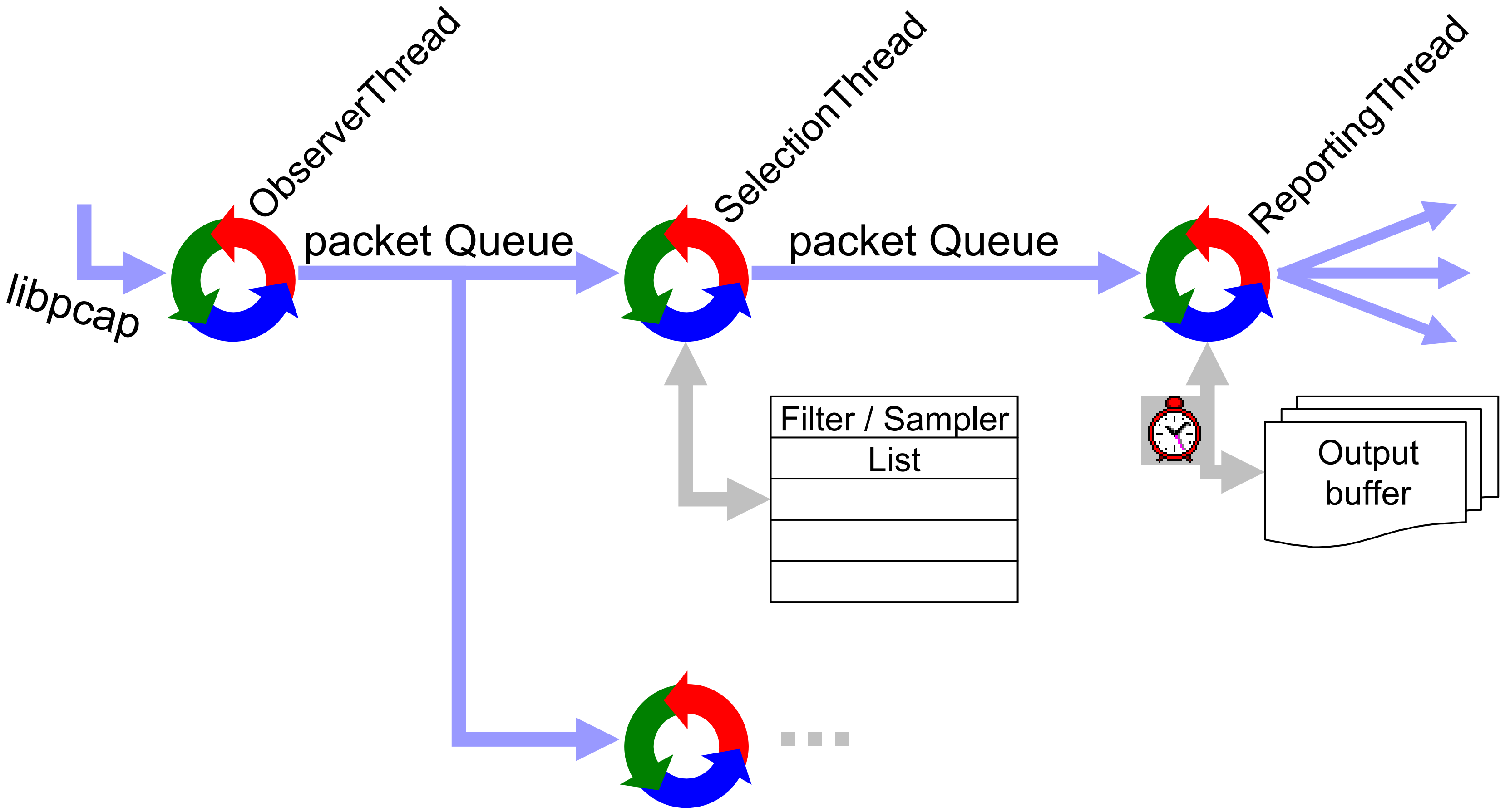
Packet Sampling

- PSAMP (Packet SAMPling) WG (IETF)

- Goals
  - Network monitoring of ultra-high-speed networks
  - Sampling of single packets including the header and parts of the payload for post-analysis of the data packets
  - Allowing various sampling and filtering algorithms
    - Algorithms can be combined in any order
    - Dramatically reducing the packet rate

- Benefits
  - Allows very high-speed operation depending on the sampling algorithm and the sampling rate
  - Post-analysis for statistical accounting and intrusion detection mechanisms

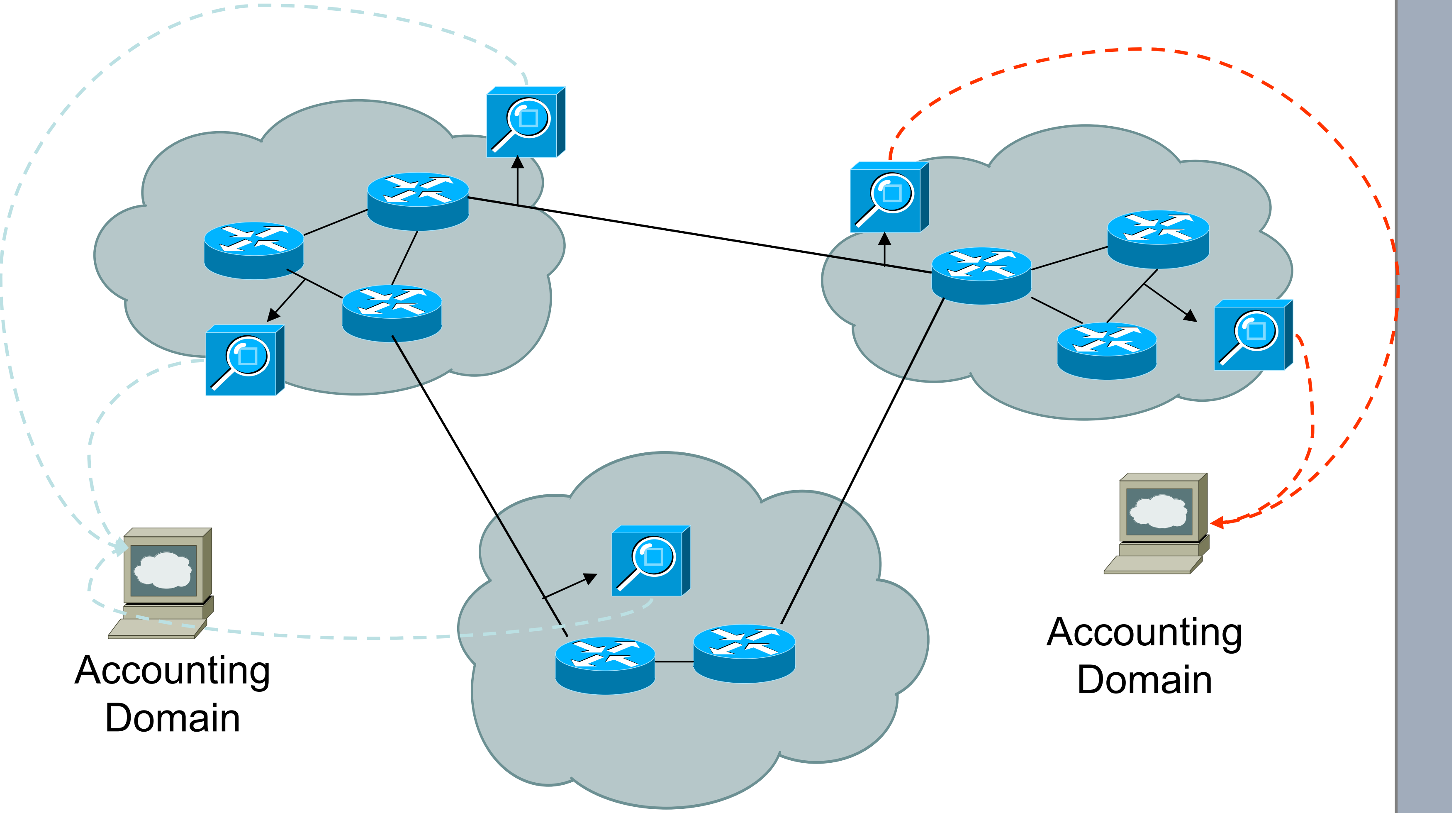
Implementation of PSAMP / IPFIX



Application Scenarios

- Accounting and Charging
  - Accounting for statistical reasons
  - Accounting for further charging
- Traffic engineering
  - Identification of primary traffic paths
  - Optimization of network parameters (e.g. routing parameters) for better network utilization
- Network Security
  - Detection of denial-of-service attacks
  - Forensic methods for post-intrusion analysis

Accounting and Charging



Network Security

- ❑ Intrusion detection with automated firewall configuration