



# Including the Network View into Application Response Time Diagnostics using Netflow

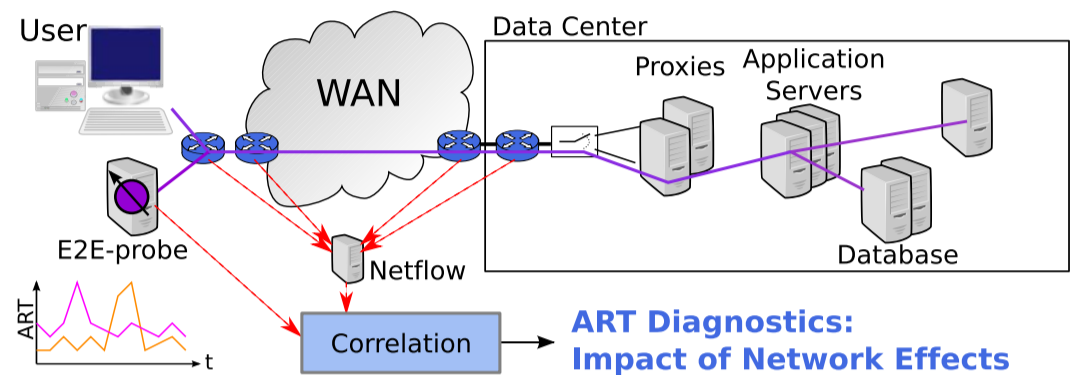
Jochen Kögel  
jochen.koegel@ikr.uni-stuttgart.de

## Scenario

- Global Enterprise Network
- Central Application Servers, accessed from distant locations
- Application Response Time (ART) measurements by E2E-Probes
- Unsampled Netflow data collected from major routers

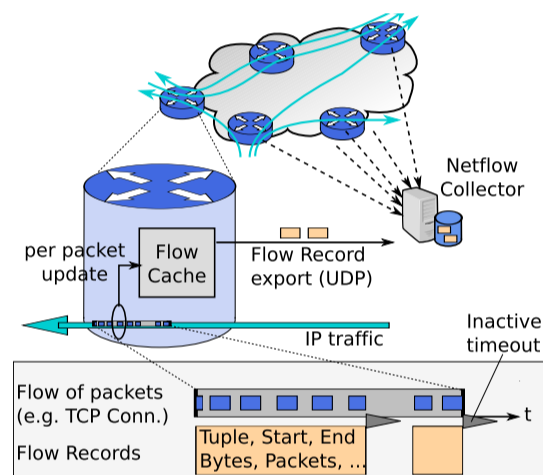
## Goals

- Diagnostics of ART in running systems
- Are network effects the cause of high ART?
- Which network effects contribute to which extent?



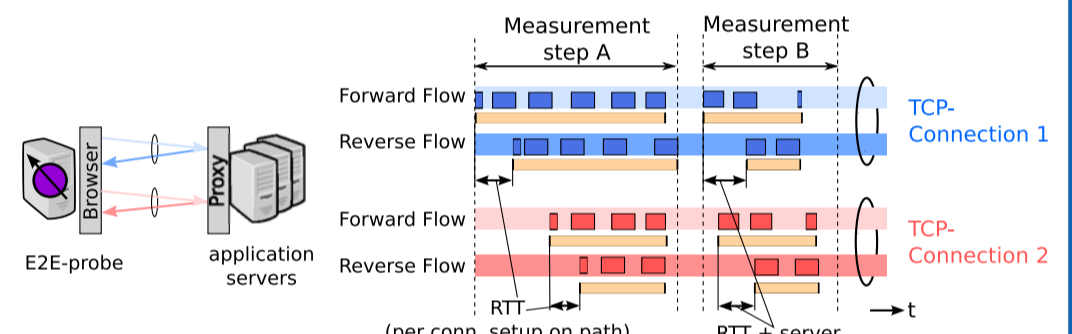
## Netflow characteristics

- Netflow: Flow-level metering
- Inherently incomplete measurement due to memory limitations and packet loss
- Mainly used for reporting, accounting, security. **However, it is much more valuable!**
  - More efficient than packet traces
  - More information than interface counters



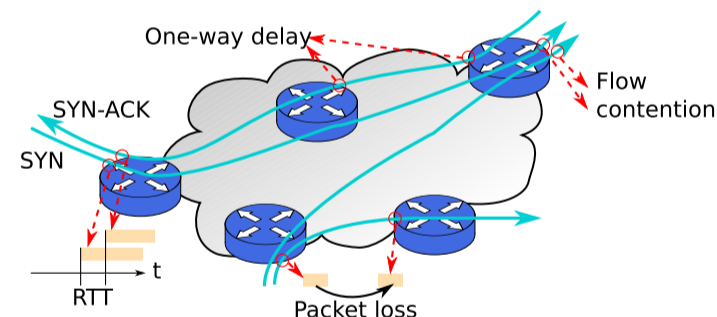
## Flow Records resulting from E2E-Probes

- Persistent TCP connections to proxy
- Deterministic measurement runs: similar flow patterns



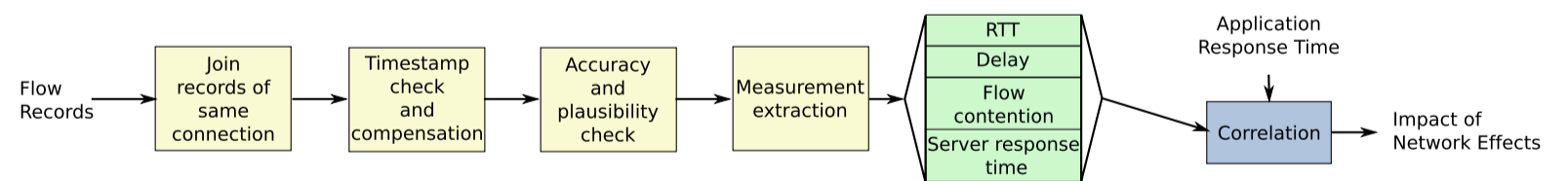
## Derivable measurements

- Network characteristics
  - RTT estimation from TCP handshake seen by one router
  - One-way delay between different routers (with synchronized clocks or time offset compensation)
  - Packet loss based on packet count differences between routers
  - Flow contention on interface-level
- Server response time from mid-flow record offset

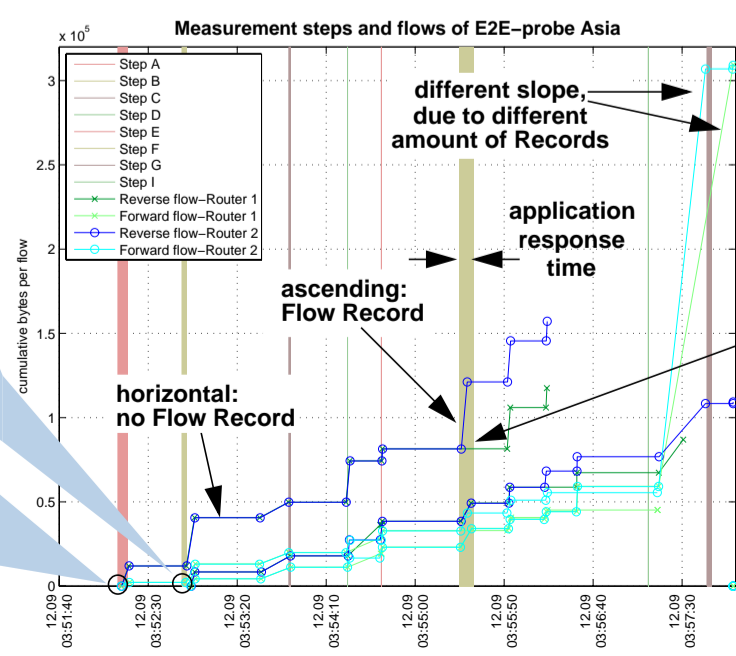
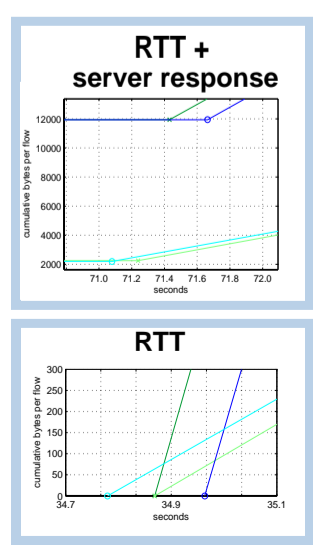


## Netflow processing for deriving measurements

- Joining Flow Records of one connection to larger records
- Incompleteness demands for sophisticated preprocessing



## Results



## Outlook

- Comprehensive evaluation
  - Impact of all derivable measurements
  - Data of complete network
  - E2E-Probes at different locations
- Development of robust compensation algorithms for incomplete flow data
- Study of measurement accuracy
- Comparison of E2E-Probe traffic and user traffic