Sprint's Continuous Monitoring

Gianluca Iannaccone, gianluca@sprintlabs.com

ispmon BOF - July 17th, 2003

Motivation

- Sprint's IPMON project (http://ipmon.sprint.com)
  - It demonstrated the need for fine-grained traffic monitoring systems
  - Main limit: trace collection needs to be scheduled well in advance
- Sprint's Operations requires a system available 24/7
  - Timely identification of network problems
  - Ability to trace back causes

Operational Requirements

- Passive system that does not interfere with operational network
- Compute (and export) statistics on several metrics
  - real-time, fine granularity
  - goal: IPFIX-compliant
- Store past 24 hours of packet-level traces
  - 24 hours on OC48, a few days for OC12.
  - system accepts queries on collected packet trace

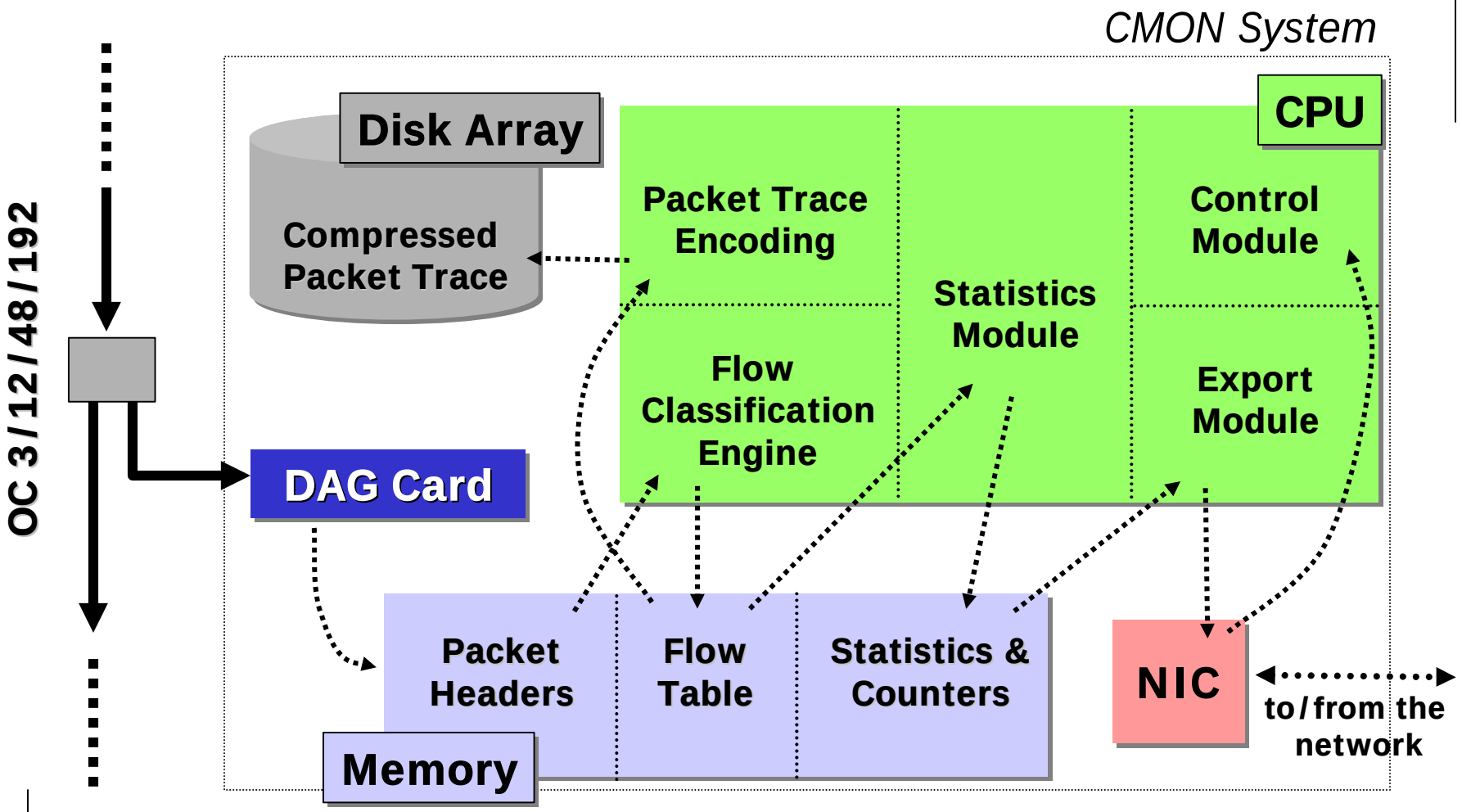
Goals

- Proof-of-concept for always-on packet-level monitoring:
  - what is doable/needed, what is not
- Define Sprint position on monitoring to router vendors and industry

Why not directly inside the routers?

- Not as simple as it sounds
  - Switched backplanes make it impossible to find single point of observation
  - Integrated approach may be harmful (e.g., worms, DOS)
  - Storage/Export issues (impossible to have packet traces)
- Not to mention the development costs
  - It is yet not clear what metrics are needed
  - Avoid to replicate the multicast example

CMON Design


CMON System
OC 3/12/48/192
Disk Array
Compressed Packet Trace
CPU
Packet Trace Encoding
Control Module
Statistics Module
Flow Classification Engine
Export Module
DAG Card
Packet Headers
Flow Table
Statistics & Counters
Memory
NIC
to/from the network

Open Issues

- Performance
  - “how to quickly get the data in and out of the boxes”
- Placement
  - “where to place the boxes to have a good view of the network”
- Coordination
  - “how to answer network-wide-related questions with multiple boxes”
- Data Summarization
  - “how to answer traffic questions using minimum resources”