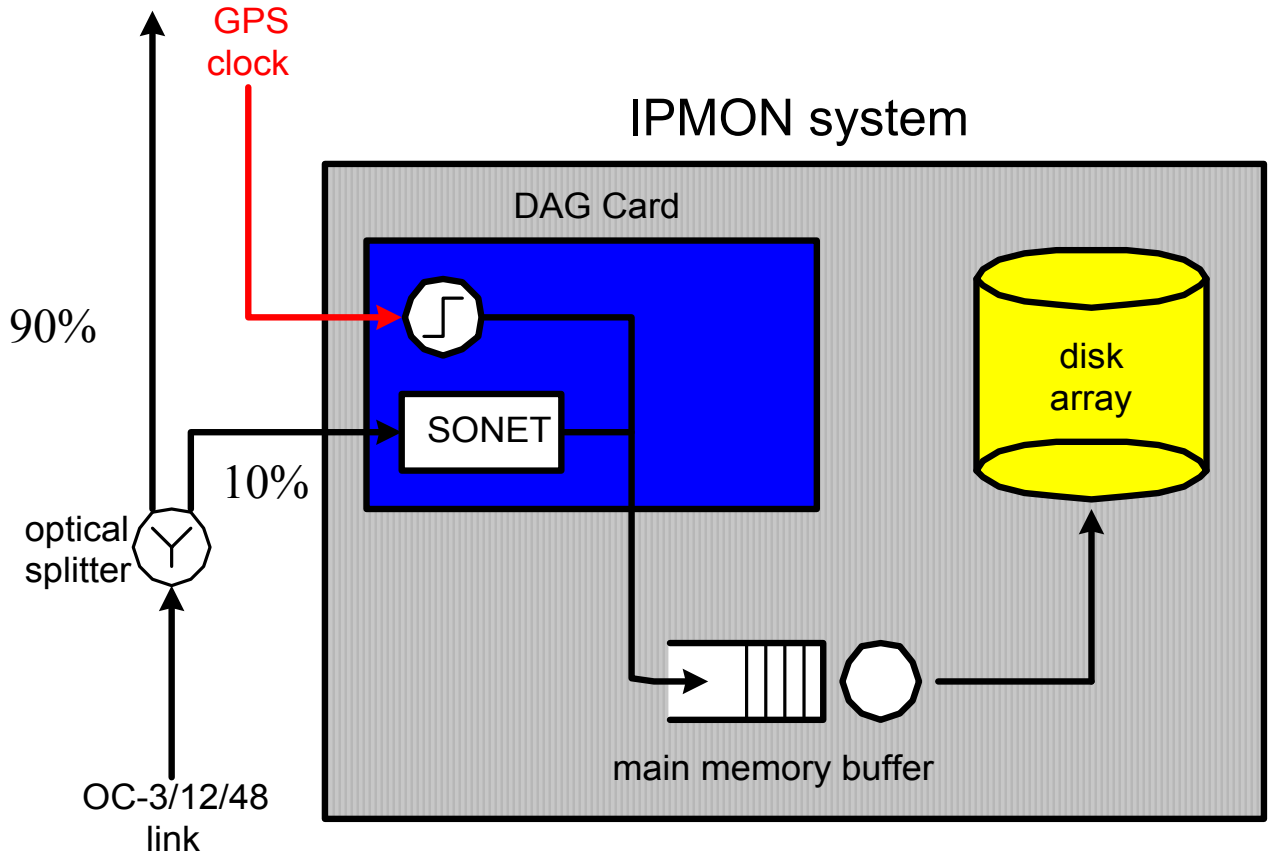
Monitoring: from research to operations

Christophe Diot and the IP group @ Sprintlabs

[cdiot|ipgroup]@sprintlabs.com
ipmon.sprintlabs.com

Sprint

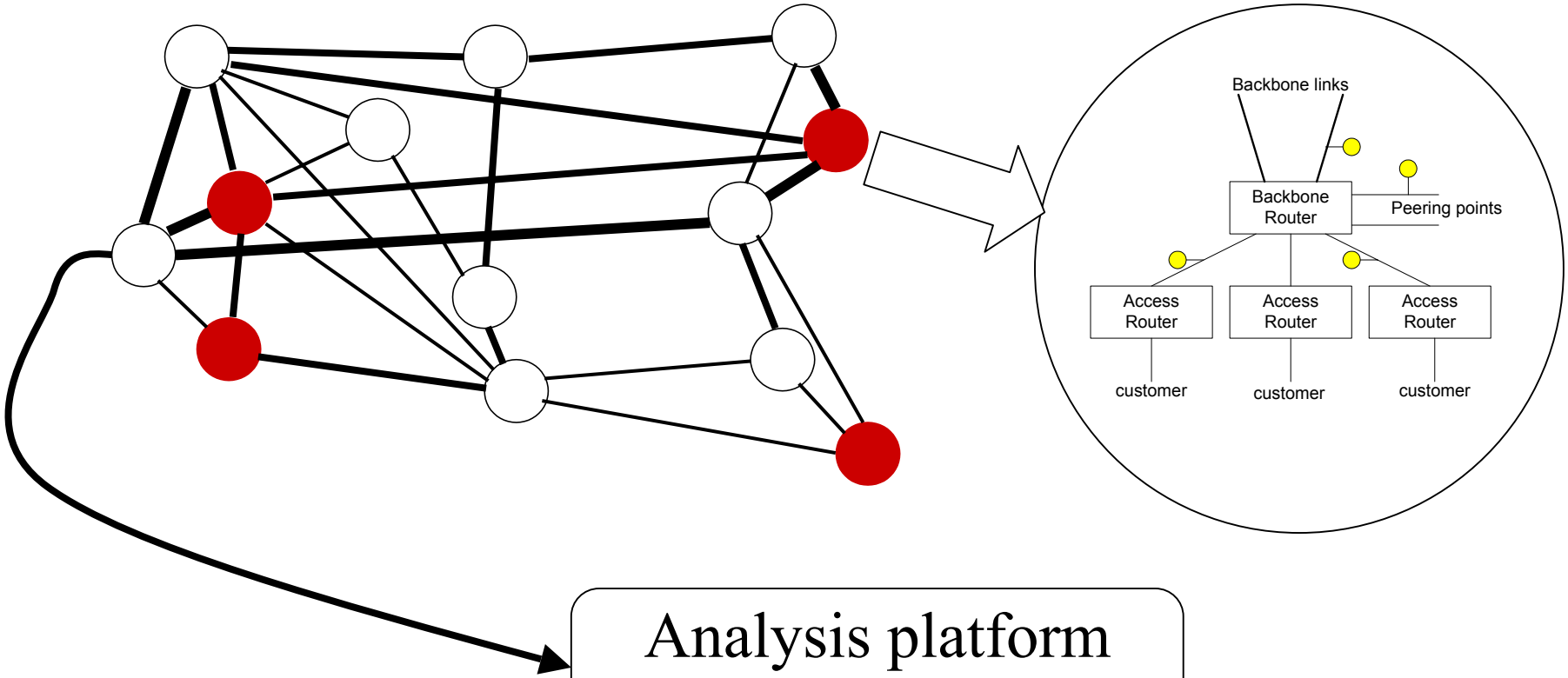
Monitoring System Architecture



Linux PC with multiple PCI buses

Sprint

IPMON architecture



Analysis platform
(located @ sprintlabs)

Sprint

Needs for Monitoring

- Management
  - configuration, traffic engineering
  - forecasting, provisioning, dimensioning
  - traffic matrices
- Diagnosis
  - detect and report problems
- Value-added services
  - feedback to customers

Sprint

What information is needed

- Time-stamped IP headers
- IS-IS and BGP information
- Lower level alarms (if any)
- SNMP
- Router logs

Sprint

Systematic approach

- Continuously monitor each link
  - Compute and export a small set of statistics (volume, peak, flows, out-of-sequence)
  - Store packet traces for a limited amount of time
- Query when more is needed
  - SQL type queries
  - Match routing information to packet trace

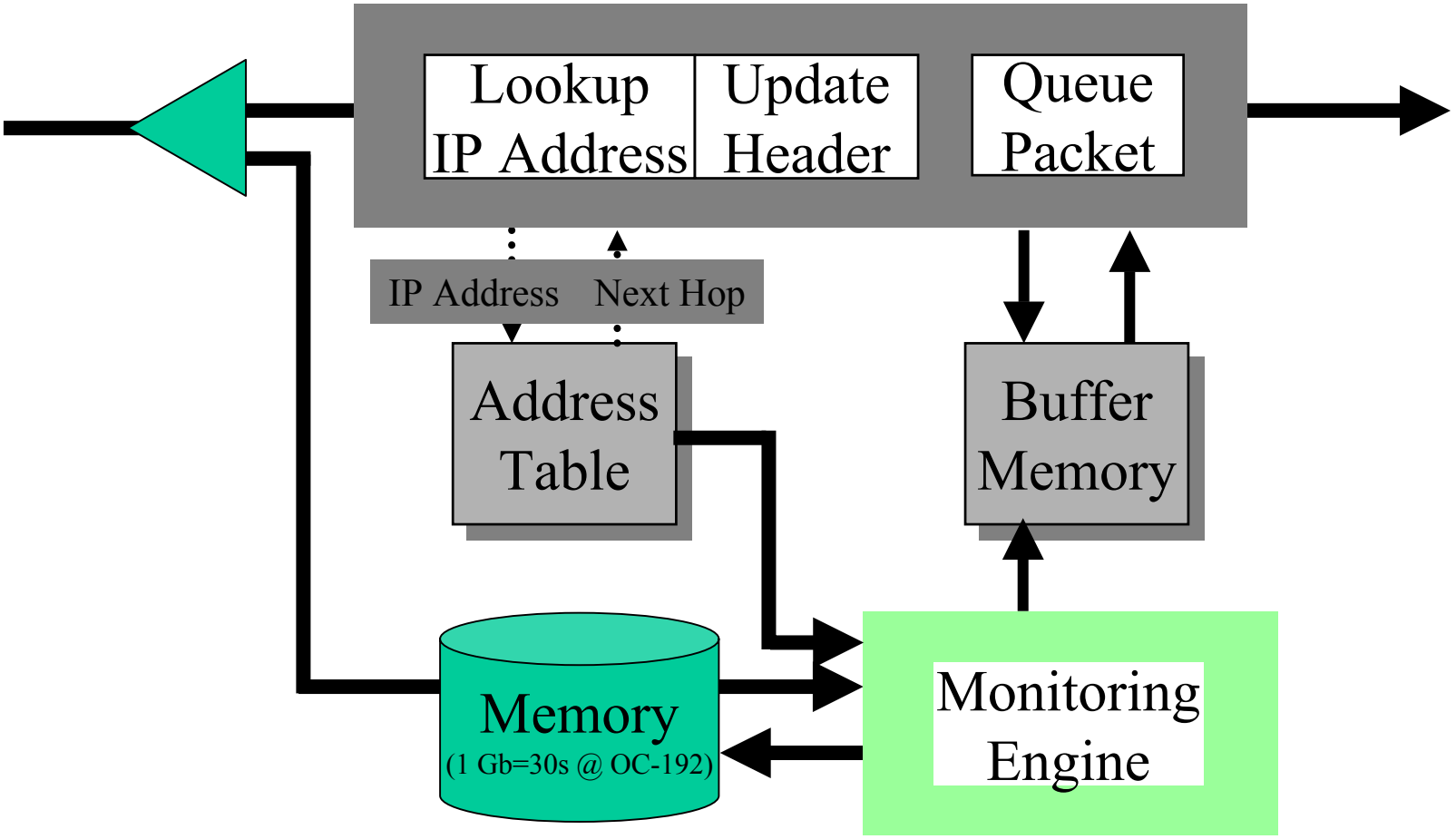
Sprint

How to implement

- Active monitoring does not solve all problems
- OC-x MON approach is quite expensive and increases network complexity
- Line cards would be optimal
  - packet traces and routing information available
  - must not affect forwarding performance

Sprint

Implementation



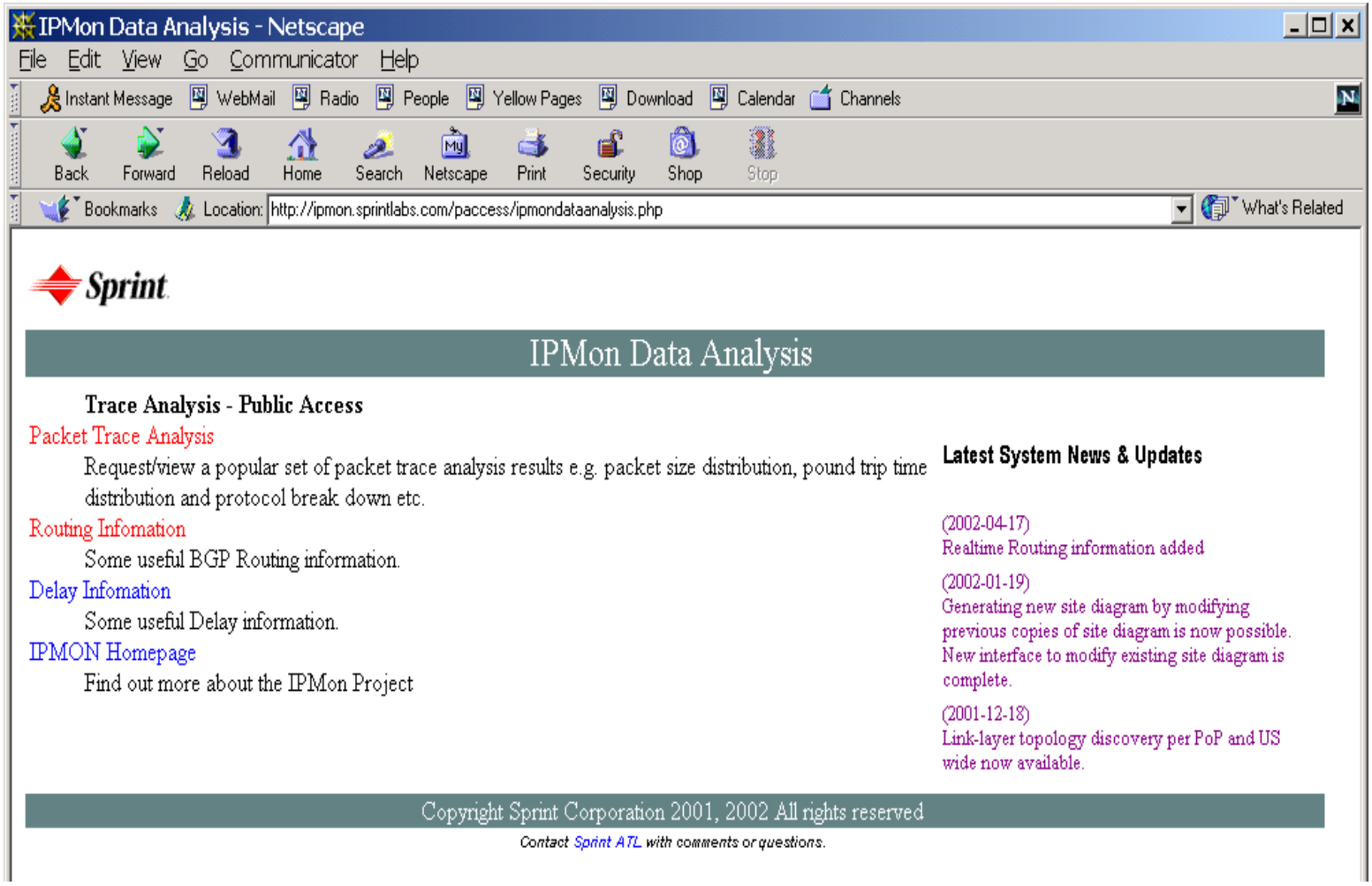
Sprint

Potential problems

- 5 clock cycles at OC-192 between two 40 bytes packets
- Query/Export might be heavy
- Complexity for line cards
- Memory
- Centralized management

Sprint

ipmon.sprintlabs.com (under construction)



Sprint

To know more

- ipmon.sprintlabs.com
- Internet draft:

  draft-bhattacharyya-monitoring-sprint-00.txt
- cdiot@sprintlabs.com

Sprint