Deployment of an interoperable and cost-effective monitoring infrastructure in ISP networks

draft-bhattacharyya-monitoring-deployment-00

Gianluca Iannaccone, gianluca@sprintlabs.com

ispmon BOF - July 17th, 2003

Monitoring to support operations: areas of interest

- Resource Usage
  - application: network provisioning
  - need: link/CPU/buffer utilization
- Traffic Accounting
  - application: traffic engineering
  - need: flow-based traffic information & routing info
- Fault diagnosis & troubleshooting
  - application: identify anomalies and “undesired” behaviors
  - need: packet-level traces & routing information

Different requirements for the monitoring infrastructure

Task	Granularity	Timescale	Presence
Resource Usage	Aggregate Statistics	Large (minutes)	Ubiquitous
Traffic Accounting	Flow-level	Flow lifetime	Edges of the network
Fault diagnosis	Packet-level	Packet inter-arrival	“Strategic” locations

What about monitoring performance?

- For network operators, performance monitoring is a fault diagnosis method
  - Devices in the network have survived conformance tests.
  - If a device is working around a valid operating point (see resource usage), then poor performance is a fault.
- Partial knowledge of the network forces to do some form of performance monitoring
  - black box approach
  - e.g., crossing administrative borders.

Current tools available to ISPs

- Resource Usage
  - SNMP
- Traffic Accounting
  - Netflow-like approach
  - IPFIX-protocol
- Fault diagnosis
  - none really agreed upon
  - router logs (very poor), RMON, SNMP
  - very limited *visibility* of the traffic.

Areas addressed by the IETF

- Packet sampling/filtering (PSAMP)
- Flow export (IPFIX)
- Performance metrics (IPPM)

- In general, they will benefit from knowledge of operational systems
  - in form of applicability statements and BCPs

Aspects not yet addressed by IETF

- Inter-operability of measurement systems
- Storage, analysis and aging
- Control plane functionalities

Inter-operability of measurement systems

- How to share data among ISPs?
  - useful for fault diagnosis, incident reporting
- Need agreed-upon measurement framework
  - define common set of metrics
  - define methods to measure them
  - define methods to compare them
    - metrics may depend on topology, routing or other ISP-specific characteristics

Storage, analysis and aging of collected data

- Common format to store packet traces
- Set of basic primitives to query/analyze the collected data.
- Aging for long-term planning
  - what to do with stored data over time
  - may need sampling or summarization techniques

Control plane functionalities

- Need for semantically-rich control protocol
  - dynamically control the measurement operations
  - defined automatic responses to alert messages
- Coordination among monitoring systems
  - between a collector and the monitoring systems
  - or, among the monitoring systems themselves