Presentation Structure:

1. Overview of Paper
2. Description of System
3. Discussion of Data Analysis Challenges
4. Discussion of Alternative Passive Monitoring Systems
Paper Overview:

- Describes a passive monitoring system that captures packet-level traces on a high speed backbone link.

2 Main Points:
1. Simultaneous data collection on multiple, geographically remote hardware.
2. All collected data is normalized to a common timestamp.

Network Monitoring Challenges:

1. Heterogeneous network links
2. Monitoring system impact on network
   - must limit
3. Distributed system
   – how to obtain a synchronized global view?
   ----------------------------------------------
4. Data Management
   - how to handle the volume of data collected
Sprint IP Backbone Description:

Nodes = Point-of-Presence (POPS)
Links = OC48 (2.5 Gbps)
       OC192 (10Gbps)
NAP= Public Network Access Point

Packet-Level Traffic Measurements from the Sprint IP Backbone Presentation, CS670, March 4, 2004

Sprint IP Backbone Description, more detail:
• Inside the POP
  • Access router (gateway)
  • Backbone router (core)
  • Monitoring Entity

Packet-Level Traffic Measurements from the Sprint IP Backbone Presentation, CS670, March 4, 2004
Data Recording and Data Analysis – 3 pieces:

1. Passive Monitoring Hardware
   • Special machine with lots of memory
   • Special N/W interface card (DAG) w/embedded clock synched to external GPS signal (max error: 5 microseconds)
   • Packet Trace (collection of packet headers)
   • Packet Header (40 bytes)
     • IP header
     • UDP/TCP header
     • Timestamp

2. Data Repository
   • Single Trace Analysis
   • Multi-Trace Analysis

3. Off-Line Analysis Tools
   • Single Trace Extraction based on timestamp & header info.
   • CoralReef public suite, protocol/application specific filtering
   • Multi-Trace analysis through some type of custom approach

Trace Sanitization (Typical ETL):

Check for:
• Hardware issues
  • Monitoring Entity
  • Network Card
  • Tape Drive
  • Tapes
• Software issues
  • Data Validity (header contents)
  • Time Synch
Other Passive Monitoring Systems:

1. SNMP (Simple Network Mgmt Protocol) –
   - tracks interface rate, drop rate in terms of #packets, #bytes
   - tracks link transmission error rate
2. NetFlow
   - Cisco router built-in monitoring system
   - collects more detailed info than SNMP
   - requires external system for data recording
3. Juniper router
   - built-in monitoring system similar to NetFlow
4. CoralReef (CAIDA, based on OC3MON)
   - like IPMON but without GPS global timestamp
5. NetDetector (Niksun), ATM Probe (NetScout)
   - limited to OC3 and lower speed lines

Works Cited