Network Monitoring and Measurements: Techniques and Experience

Supratik Bhattacharyya
Sue Moon
Tutorial Outline

• Introduction
  – Internet architecture
  – The Sprint IP Backbone
  – Monitoring: requirements and challenges

• Current techniques
  – taxonomy, tools and techniques

• The IPMON project

• The future of monitoring
Tutorial Outline

• Introduction
  – Internet architecture
  – The Sprint IP Backbone
  – Monitoring: requirements and challenges
• Current techniques
  – taxonomy, tools and techniques
• The IPMON project
• The future of monitoring
The Internet Design Philosophy

• Packet switching
• Continued communication around failures
• Support for diverse services and protocols
• Distributed management of resources
• No access control
• Simplicity at the core, complexity at the edge
The Internet Hourglass (Deering@IETF)
What is the Internet today?
Today’s Tier-1 Backbones

• Technologies
  – IP over SONET (POS)
  – IP over ATM
  – IP over MPLS

• Topology - points-of-presence (POPs) connected by long-haul fiber
  – numerous small POPs (e.g., UUNet)
  – relatively few large POP (e.g., Sprint)
Tutorial Outline

• Introduction
  – Internet architecture
  – The Sprint IP Backbone
  – Monitoring: requirements and challenges

• Current techniques
  – taxonomy, tools and techniques

• The IPMON project

• The future of monitoring
Sprint IP Backbone
A Backbone POP

- **Peer**
- **Core Router**
- **Other POPs**
Common Engineering Practices

• “Over-subscription” at edge

• Protection
  – large scale outages happen regularly
  – “over-provisioned” core
  – MPLS/TE does not help

• Service Level Agreements:
  – delay (e.g., 55 msec round-trip in USA)
  – loss (e.g., 0.3%)
  – port availability (e.g., 99.99%)
Over-subscription and Over-Provisioning

Over-subscription

Rest of Backbone

Over-provisioning
**Intradomain Routing : IS-IS**

- Link weights
  - inter-POP links >> intra-POP links
- Updating weights:
  - set by hand
  - modified infrequently, usually for large-scale failures
- One-way latency across backbone governs weight selection (hence routes)
IS-IS Load Balancing and Protection

- Multiple parallel links between POP pairs
- Per-prefix splitting over equal cost paths
Interdomain Routing: E-BGP & I-BGP

R1

AS1

R2

AS2

R3

I-BGP

IS-IS

R4

AS3

R5

announced B
Multi-homing and Hot Potato Routing

Peers need to be “consistent” in their route announcements.
Transit vs. Non-transit AS

• Transit AS
  – carries traffic between two other ASes
  – propagates routes learnt from other ASes
Sprint practices

• Multi-homing with large peers and customers
• Hot Potato Routing
• Non-transit for peers
• Transit for customers
Sprint Service-Level Agreements

• Peers : no money exchanged
  – at a network exchange points (NAP)
  – point-to-point links(OC-3/12/48)

• Customers :
  – flat fee by link bandwidth

• Performance Guarantees :
  – 55 msec latency across USA
  – 0.3% loss
  – 99.9% availability
**Tutorial Outline**

- **Introduction**
  - Internet architecture
  - The Sprint IP Backbone
  - Monitoring: requirements and challenges
- **Current techniques**
  - taxonomy, tools and techniques
- **The IPMON project**
- **The future of monitoring**
Monitoring Implications of Network Design

• Network elements do not collect data
• Protocols do not provide feedback
• Network adapts to failures/congestion
• No centralized collectors
• Distributed administration:
  – operator has no control beyond own network
Monitoring Requirements

• Planning and design
• Traffic engineering
• Troubleshooting and fault diagnosis
• Customer feedback
• Research
Planning and design

- Capacity Planning
  - where to put additional capacity, when?
- Controlled evolution
  - new link/router/customer
  - new applications/protocols
- New technologies
  - MPLS, QOS, etc.
- Router Design
  - buffer dimensioning, AQM, etc.
Traffic Engineering

- Selecting primary and backup routes
- Accommodating changes
  - topology, customer usage pattern, new applications
- Routing protocols
  - configuring BGP policies, ...
Troubleshooting and Fault Diagnosis

• Some examples:
  – a link is suddenly overloaded
  – a route suddenly disappears from BGP table
  – DOS attack on a customer
  – router shows high CPU utilization
  – is a peer using me for transit?
Operations and Management

• Need
  – up-to-date traffic and routing info
  – tools to correlate them

• But…
  – do no harm
  – simplicity above all!
  – minimal changes to network
  – cannot change router configuration
Customer Requirements

- Adherence to SLA
  - difficult to verify/prove
- Protection for attacks
  - block, trace back to attackers
- Traffic Engineering:
  - how are packets being routed?
  - what are the delay/loss statistics on these routes?
  - protocol/application/AS number breakup
  - multi-homed customers
Research

• Monitoring is key to evolution of the Internet:
  – understanding its global complexity
  – designing new algorithms/protocols
  – paradigm shifts (e.g., peer-to-peer)
  – changes in design philosophy

Challenge:
  collecting and analyzing massive volumes of data!
Limitations

• Technical
  – poor support in routers
  – must not interfere with network operations
  – need storage and analysis infrastructure

• Non-technical
  – Proprietary
  – Legal
  – Privacy
  – Cost
Tutorial Outline

• Introduction:
  – current Internet architecture
  – benefits and challenges of monitoring

• Current Techniques:
  – taxonomy, tools and techniques

• The IPMon Project

• The future of monitoring
**Taxonomy: Information Types**

**Data Plane**

- **Packet-level**
  - port #, src and dst addr, type, length
- **Flow-level**
  - duration, total # of packets and bytes, application
- **Network element-specific:**
  - link utilization, dropped packet count
- **Network-level**
  - Can be derived from packet/flow-level
  - ingress vs. egress traffic
Taxonomy: Information Types

Control Plane

– Routing information
  • static - snapshots of routing tables
  • dynamic - update messages, policies

– Topology
  • Databased in facility management system
  • Physical/L2/L3 layer

– Configuration
  • relatively static, but not widely available.
Taxonomy: Observation Points

• Edge vs. core:
  – Access is often limited
  – Link-level statistics not accessible from edge
  – Important to combine observations from different points
Metrics Derived from Measurements

Loss
  – Drops per interface
  – end-to-end loss
  – per-AS loss rate

Delay & Jitter
  – One-way vs. RTT
  – Single vs. multi-hop
  – Avg vs. max
Metrics Derived from Measurements

Utilization levels
  – Derived from byte counts

Routing reachability
  – Duration and frequency of unreachability
  – # of ASs and prefixes affected

Failure
  – Frequency
  – Duration
Issues

Amount of data
  – Storage
  – Processing and transfer overhead

Level of aggregation
  – Temporal aggregation
    • Sub-second, minutes, daily, and weekly
  – Research vs. operation
    • Packet-level vs. flow/link/network-level
Network Matrices

• Network-wide representations of various metrics
  – traffic volume (Traffic Matrices)
  – delay, loss, utilization, …

• Many statistics
  – average, peak, variance, etc.

• Many aggregation levels
  – POP-to-POP, router-to-router, AS-to-AS, …
Example: AT&T Latency Matrix

Current Average: 35 msec

Latency in milliseconds

Copyright Sprint Advanced Technology Laboratories
Which Network Matrices to Build?

• What do applications need?
  – network design, TE, customer reports, operations, ...
  – may only need some components

• What is scalable?
  – e.g. router-to-router is far bigger than POP-to-POP
**Active Measurement**

Probes are injected into the network

- Can overload the network
  - careful calibration needed
  - Poisson-generated traffic often used

- Measure from the edges
  - Does not need access to inside of network
  - Can only infer network-internal performance
Active Measurement Tool: Ping

ICMP-based tool for host reachability

- Algorithm
  - Sends an ICMP echo request with:
    - Identifier for unique ping process
    - Sequence number per echo request
  - Receiving host returns an ICMP echo reply
  - Prints out RTT, TTL, and seq. #.

- Issues
  - different processing path from other packets
Active Measurement Tool: Traceroute

Used to find out the forward path to a host

• Algorithm
  – Send an IP datagram with TTL=1
  – First router sends back ICMP time exceeded
  – Then send a datagram with TTL=2
  – Continue till destination is reached/TTL expired

• Issues
  – not suited for performance measurements
Packet-Pair Based Bandwidth Estimation

RTT

rate estimate

Source  Router  Bottleneck  Sink

Time

bottleneck rate
**Pathchar**

Vary $L$, fit line to $\min[\text{RTT}(n) - \text{RTT}(n-1)]$

Slope of line gives $\frac{1}{c}$

$$2p = \text{RTT}(n) - \text{RTT}(n-1) - [2L/c + e]$$

Based on TTL expiration (like traceroute)
Active Measurement Projects

National Internet Measurement Infrastructure (NIMI)
  – Provides infrastructure for active measurements
  – BSD-based hosts, scalable, dynamic

NLANR AMP

RIPE NCC
Commercialized Monitoring Services

Matrix
  – Ping-based monitoring of customers

KeyNote
  – Subscription-based service of application-specific monitoring

Shortcomings:
  – Techniques often depend on starting points, not on the network
**Passive Measurement**

No traffic injected for measurement purpose

- Not invasive
  - Only data collection increases traffic
- Access limited
  - Measurement about total traffic
  - Privacy/Security - serious concern
**Tcpdump**

Puts a network interface to promiscuous mode

- captures only frames matching filters
- shows
  - network interface info, time, src and dst, etc.
  - or entire payload

**Issues**

- security: sees all frames on the Ethernet
- host performance penalty
- timestamps not always dependable
Passive Measurement Examples

Packet monitors
- Tcpdump for Unix-based hosts
- Dedicated measurement systems
  - OC3MON, IPMON

Router/switch traffic statistics
- Network internal behavior
- SNMP MIBs
- Flow-level information
SNMP

Managed entity

Managed device

Agent

data

Agent

data

Simple Network Management Protocol
Packet-level measurements

• Pros:
  – very fine granularity

• Challenges:
  – link speeds are increasing!
  – Large volumes of data
  – system design issues:
    • disk/PCI bus speeds
    • installation cost
Flow-level measurements

• Many granularities
  – five-tuple, BGP prefixes, IP header fields, etc.
• Pros
  – aggregated information
• Challenges
  – packet-to-flow mapping
  – terminating expired flows
  – CPU/memory requirements on routers
Flow-level Monitoring: Cisco Netflow

NetFlow: mechanism to gather flow statistics
– caches flow statistics per router interface and sends records by UDP
– Route-based aggregation possible
  • By AS, protocol port, src prefix, dst prefix, prefix
– Data flows from NetFlow-enabled device to FlowCollector
  • No MIB or SNMP
  • More aggregation possible at FlowCollector
Netflow Pros and Cons

Pros
– provide statistics on every flow
– detailed prefix-to-prefix traffic matrix

Cons
– High memory requirement for short flows
– feasible at access routers, not backbone routers
– route changes flushes flow cache, may cause CPU overload
– Flow statistics in UDP: losses during peak usage
Commercial Passive Measurement Tools

HP’s OpenView
- Integrated network management tool based on SNMP statistics
- Combined with configuration, visualization, reporting mechanisms

Agilent NetMatrix:
- Passive monitoring gear for LAN and up to OC-12 ATM

Niksun’s NetVCR solutions
- Packet monitor based management system
Research Project: CAIDA

Cooperative Association for Internet Data Analysis (http://www.caida.org)

– Measurement tools:
  • OCxMON, cflowd, CoralReef, NeTraMet: passive
  • Skitter: global coverage by traceroute

– Visualization tools:
  • Walrus, Otter, Plankton: graph visualization
  • Gtrace: traceroute visualization
  • MapNet: major ISP maps
Some Other Research Projects

• AT&T Labs Network Measurement Tools
  – active/passive, flow-level data, routing updates

• Surveyor:
  – one-way loss and delay as defined by IPPM

NLANR’s PMA and AMP
  – Passive and active measurement sites
  – Packet traces from passive measurement made public
Routing Research Projects

Routeviews

- 50+ peering at route-views.oregon-ix.net
- MRT format RIBs and BGP updates, “show ip bgp” dumps, route dampening data
- only E-BGP

RIPE (Réseaux IP Européens)

- routing updates from 9 mostly European IXs
- “Looking Glass” services for BGP
- Routing information service (RIS)
IETF/IRTF Activity

- IETF Working Groups
  - IPPM
  - IPFIX
  - BMWG
  - PSAMP
- IRTF
  - IMRG
Tutorial Outline

• Introduction
• Current techniques
• The IPMON project
  – infrastructure and data
  – selected results
• The future of monitoring
Tutorial Outline

- Introduction
- Current techniques
- The IPMON project
  - infrastructure and data
  - selected results
- The future of monitoring
**IPMON Goals**

- Identify open problems for an operational network, influence its evolution
- Feedback to network design and engineering
- Tools for operations and management
Data

- Packet traces
- SNMP statistics
- IS-IS/BGP Listeners
- Active Measurement Probes
Collecting packet traces

- Insert optical splitter on links in multiple POPs (OC-3/12/48)
- Collect and timestamp TCP/IP headers (44 bytes) - 2us clock accuracy
- Collect routing information (IS-IS, BGP)
- Transfer data to lab for off-line analysis (SAN based analysis platform)
Monitoring System Architecture

Analysis platform (located @ Sprint ATL)
Monitoring System Architecture

Diagram:
- OC-3/12/48 link
- Optical splitter
- GPS clock
- DAG Card
- SONET
- Main memory buffer
- Disk array
- IPMON system
- Linux PC with multiple PCI buses

90% and 10% labels on the diagram.
Current Status

• Three POPs:
  – one west coast, two east coast
  – 50+ IPMON systems
  – OC-3 to OC-48 capabilities
Practical Constraints

• Difficult to monitor operational network:
  – complex and expensive procedure
  – network evolves too fast

• Technology constraints:
  – line speeds are increasing...
  – PCI bus, disk speeds need to keep up!
  – need sophisticated storage systems
Python Routeing Toolkit (PyRT)

Listener software to collect IS-IS/BGP updates:

– **IS-IS listener:**
  - collects updates on link failures, weight changes, etc.

– **BGP listener:**
  - implements minimal subset of BGP state machine

– Publicly available

– Data format compatible with other projects (Routeviews, etc.)
IPMON Data Management System

- **Motivation**
  - management of 10+ terabytes
  - keep track of “metadata”
  - information sharing

- **Entities to manage**
  - packet traces, routing updates
    - location, date of collection, link speed, etc.
  - analysis results
Tutorial Outline

• Introduction
• Current techniques
• The IPMON project
  – infrastructure and data
  – selected results
• The future of monitoring
IPMON : Selected Results

- Part I: Traffic mix and patterns
- Part II: Packet delay and reordering
- Part III: SNMP analysis
- Part IV: Routing analysis
IPMON: Selected Results

• Part I: Traffic mix and patterns
  – volume
  – application breakup
  – packet sizes
  – detecting DOS attacks

• Packet delay and ordering

• SNMP analysis

• Routing analysis
Volume on an OC-12 Link
Application Breakup on OC-12 Links

Tier-2 access

CDN access
Packet size distribution on OC-48 Link

Trace: 1 hour, 676 million packets
Detecting DOS Attacks

TCP SYN bursts
Lessons Learnt - Part I

- Links differ in characteristics
- Web traffic dominates, but p2p is making inroads
- Monitoring reveals changes in traffic mix and characteristics
IPMON: Selected Results

- Traffic mix and patterns
- Packet delay and reordering
- SNMP analysis
- Routing analysis
Delay through a router - OC-12

[Papagiannaki et al 02]

Copyright © Sprint Advanced Technology Laboratories
Delay across the USA

- min: 27051
- avg: 27063
- 90%: 27080
- 99%: 27119
- max: 27129
Out of Sequence packets

• Challenge
  – how much of packet reordering?
  – where do they occur?
  – what are the causes?

• Our approach: analyze TCP flows in the mid-point of its path
# OOS Classification [Agarwal et al. 02]

All numbers in p.c.

<table>
<thead>
<tr>
<th></th>
<th>CDN</th>
<th>Tier-1 ISP</th>
<th>Tier-2 ISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-sequence</td>
<td>2</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Retransmissions</td>
<td>88</td>
<td>72</td>
<td>77</td>
</tr>
<tr>
<td>Unneeded Retransmission</td>
<td>7</td>
<td>11</td>
<td>19</td>
</tr>
<tr>
<td>Network Duplicate</td>
<td>0.01</td>
<td>0.04</td>
<td>0.07</td>
</tr>
<tr>
<td>Reordering</td>
<td>1</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>Unknown</td>
<td>3</td>
<td>5</td>
<td>1.53</td>
</tr>
</tbody>
</table>
Lessons Learnt - Part IIb

• Delays
  – speed of light
  – no jitter

• Out-of-Sequence
  – about 5% of packets
  – mostly due to loss
  – little duplication due to loops, etc.
IPMON: Selected Results

- Traffic mix and patterns
- Packet delay and ordering
- SNMP analysis
- Routing analysis
Maximum Link Load on Sprint Backbone
Effect of Failures
Lessons Learnt - Part III

• At all times, there are some overloaded links:
  – difficult to distribute traffic evenly
  – Link failures happen often
  – difficult to plan for link failures

• Average utilization conveys incomplete picture

• Essential to dampen peaks before increasing average utilization
IPMON: Selected Results

- Traffic mix and patterns
- Packet delay and ordering
- SNMP analysis
- Routing analysis
Information Sources

- BGP table snapshots
- ISIS/BGP listener logs
- Router logs
- Controlled bi-directional active probes
- SNMP data
Duration of Link Failures at IS-IS Level

Many short failures, usually one at a time
Some long outages, usually several links
BGP Activity: Temporal Trends

- Background noise:
  - 50-250 BGP updates/min
  - $O(1000)$ prefixes
  - $\sim 1\%$ routing table

- Peaks at late night/early morning
- 20-40% of routing table

 Exceptions
Active BGP Prefixes

No. of entries in BGP table ~120K !
Elephant and Mice Prefixes

Most elephant prefixes are /16 to /26
Other BGP findings

• About 5-6% of BGP updates affect prefixes carrying 80% of traffic
  – little effect on packet loss/reordering
  – but what about shifts in traffic patterns?
• Elephant flows are not stable
  – hard to use for load balancing
Lessons Learnt - Part IV

• Need to understand and control effect of “failures”
• Routing is poorly understood
  – interaction of BGP/IS-IS
  – how to set BGP policies
  – how to configure IS-IS (timers, etc.)
• Beneficial to correlate different data sets
Tutorial Outline

• Introduction
• Current techniques
• The IPMON project
  – infrastructure and data
  – selected results
• The future of monitoring
The Future of Monitoring: Topics

• Obtaining traffic matrices
  – inference techniques
  – direct measurements

• Router support for path tracing
  – IP traceback
  – Trajectory sampling

• Sampling
  – approaches and challenges
The Future of Monitoring: Topics

- Obtaining traffic matrices
  - inference techniques
  - direct measurements
- Router support for path tracing
  - IP traceback
  - Trajectory sampling
- Sampling
  - approaches and challenges
An under-specified problem:

\( n \) links, \( O(n^2) \) O-D pairs

Need statistical techniques to make “smart” guess

Assume routing is known

POP-to-POP Topology

Estimating TMs from SNMP Link Counts
Formal Problem Statement

\( X_j \): Traffic demand for POP pair \( j \)

\( n \): number of POPs

\( r \): number of links

\( c \): Number of POP pairs

\(-\ c = n \times (n - 1)\)

\( A \): \( r \) by \( c \) 1-0 routing matrix

\( Y_i \): Link count on link \( i \)

\[ A_{r \times c} X_c = Y_r \]
Proposed Statistical Techniques

- Linear Programming [Goldschmit 00]
- Network Tomography [Vardi JASA 96]
- Bayesian Estimation [Tebaldi & West 98]
- Maximum Likelihood Estimation [Cao et al 98]
Comparison [Medina et al. 2002]

- SNMP data is not enough
  - large errors
    - Bayesian: 20%-60%
    - EM: 11% - 40%
    - LP is larger
  - statistical assumptions not valid
  - marginal gain from partial information
- All methods sensitive to prior
- No good model for O-D traffic flows
Estimating POP Fan-out [Medina et al 02]

- Why does POP i choose POP j
  - user behavior
  - network design and configuration
- Use choice models
  - criterion: maximize utility

\[ U_{ij} = V_{ij} + e_{ij} \]

\[ V_{ij} = m_1 \cdot W_{ij}(1) + m_2 \cdot W_{ij}(2) + \ldots + g_j \]
Estimating POP Fan-out (contd.)

• Demand between i and j: \( X_{ij} = O_i \alpha_{ij} \)

  \( O_i = \text{total traffic sourced by POP i} \)

  \( \alpha_{ij} = \text{fan-out factor} \)

• Model for fanout

  \[
  X_{ij} = O_i \frac{\exp(V_{ij})}{\sum_{k \in S} \exp(V_{ik})}
  \]

• Initial Model: estimate \( m_1 \), \( m_2 \) and \( g_i \) using

  – \( W_j(1) \): outgoing bytes at POP i

  – \( W_i(2) \): incoming bytes at POP j
Measured fanouts
Initial Validation: Fitting Observed Data

- Parameters estimated using MLE with
  - SNMP link counts
  - fanout for three POPs

Validates exponential form for fan-out
Direct Measurement at Ingress

Measuring at egress : hard to disambiguate ingress
Challenges of Direct Measurements

• Scalability
  – monitor every ingress interface
  – how much data, what granularity
  – router overhead

• Possible directions
  – build components of TM for specific purposes
    • customer request, problem peers, etc.
  – can we monitor periodically?
The Future of Monitoring: Topics

• Obtaining traffic matrices
  – inference techniques
  – direct measurements

• Router support for path tracing
  – IP traceback
  – Trajectory sampling

• Sampling
  – approaches and challenges
**IP Traceback: Basic Idea**

Goal: *Trace sink tree from victim to source of attack, even with address spoofing*

- **Victim**
  - probability of receiving mark from d hops = \( p(1-p)^{d-1} \)
  - reconstruct path based on counting marks from each router

- router marks its address in a packet with probability \( p \)

---

*a* → *a* → *b* → *c* → **Victim**
IP Traceback : Edge Sampling

• Issues
  • slow process : \( p = 0.51, d = 15 \), need 42K packets
  • not robust to multiple attackers

\[ a \xrightarrow{\text{a XOR b}} b \xrightarrow{\text{b XOR c}} c \]

Victim

• Need additional (short) field to mark distance
• Further compression possible...
Trajectory Sampling [Duffield et al 00]

• Key Idea:
  – Track the “trajectory” of a packet by consistent sampling everywhere

• No statistics or inference techniques

• Uses:
  – how is a customer’s packet routed?
  – is routing working as expected?
  – diagnosing source address spoofing
Trajectory Sampling

Sample same pkt everywhere or nowhere

\( g(x) \) is deterministic

\[
\begin{array}{|c|c|c|c|}
\hline
\text{label} & \text{src} & \text{dest} & \text{length} \\ 
\hline
\text{g(x1)} & \text{a.b.c.d} & \text{w.x.y.z} & \text{500} \\ 
\hline
\end{array}
\]
The Future of Monitoring: Topics

- Obtaining traffic matrices
  - inference techniques
  - direct measurements
- Router support for path tracing
  - IP traceback
  - Trajectory sampling
- Sampling/Filtering
  - approaches and challenges
Why Sampling/Filtering?

Problems with large volumes of data

– feasibility of collection at high-speeds
  • memory/bus/processor requirements
– storage limitations
– complexity of analysis
State-of-Art

• Cisco
  – sampled netflow
    • capture 1 in N
    • aggregate by five-tuple

• Juniper
  – filter on any combination of header fields
  – sample 1 in N
    • recommends 1 in 1000 or less
Comparison of Approaches [Claffy et al 93]

- Traffic Characteristics
  - packet size distribution
  - inter-arrival times

- Key Results
  - Packet-triggered techniques better than time-triggered
  - difference within each class is small
Flow-Level Sampling [Duffield et al 01]

• Motivation
  – charge for measured usage
    • fixed charge below threshold
    • usage-based charged above threshold
  – sample a subset of flows with common property, e.g., source/destination address

• Key Idea :
  – flow size distribution is heavy-tailed
  – need lower estimation error for larger flows
Flow-level Sampling [Duffield et al 01]

• Approach
  – Each flow $i$ has size $x_i$ and color $c_i$
  – Goal is to estimate total usage $X(c) = \sum_{i: c_i = c} x_i$
  – Sample flow $i$ with probability $\min \{1, \frac{x_i}{Z}\}$

• Important results
  – yields unbiased estimate
  – variance decreases as $x_i$ increases
  – much smaller errors than 1 in N sampling
Towards a Two-Tier Monitoring System

Goal: make monitoring an integral part of backbone engineering and operations

• Tier 1
  – network-wide continuous monitoring
  – coarse-grained, long time-scales

• Tier 2
  – on-demand monitoring at specific points
  – fine-grained, short time-scales
Challenges

Collecting fine-grained packet data is hard!

• Sampling techniques
  – should be requirement-driven
  – need complete traces for evaluation

• (Re)Design hardware to support monitoring
  – custom-built equipment
  – router architecture...
Monitoring on Routers

- **Pros**
  - no additional infrastructure
  - up-to-date routing tables

- **Cons**
  - space and storage constraints
  - switched backplane

Modern Router Architecture
**Monitoring on Routers: Open Issues**

- **Feasibility**
  - how much memory?
  - what operations can be performed?
  - What part of the packet to capture?
  - What to export, how often?
Tutorial Summary

• Monitoring IP networks
  – difficult… but essential

• Some tools/techniques exist
  – but a lot more remains to be done

• Need integrated infrastructure
  – router support
  – wider data collection and sharing
  – storage/analysis capabilities
  – sampling and scalable export
How To Contact Us

• Email
  – sbmoon@sprintlabs.com
  – supratik@sprintlabs.com

• Visit us on-line
  – www.sprintlabs.com
  – under development: ipmon.sprintlabs.com