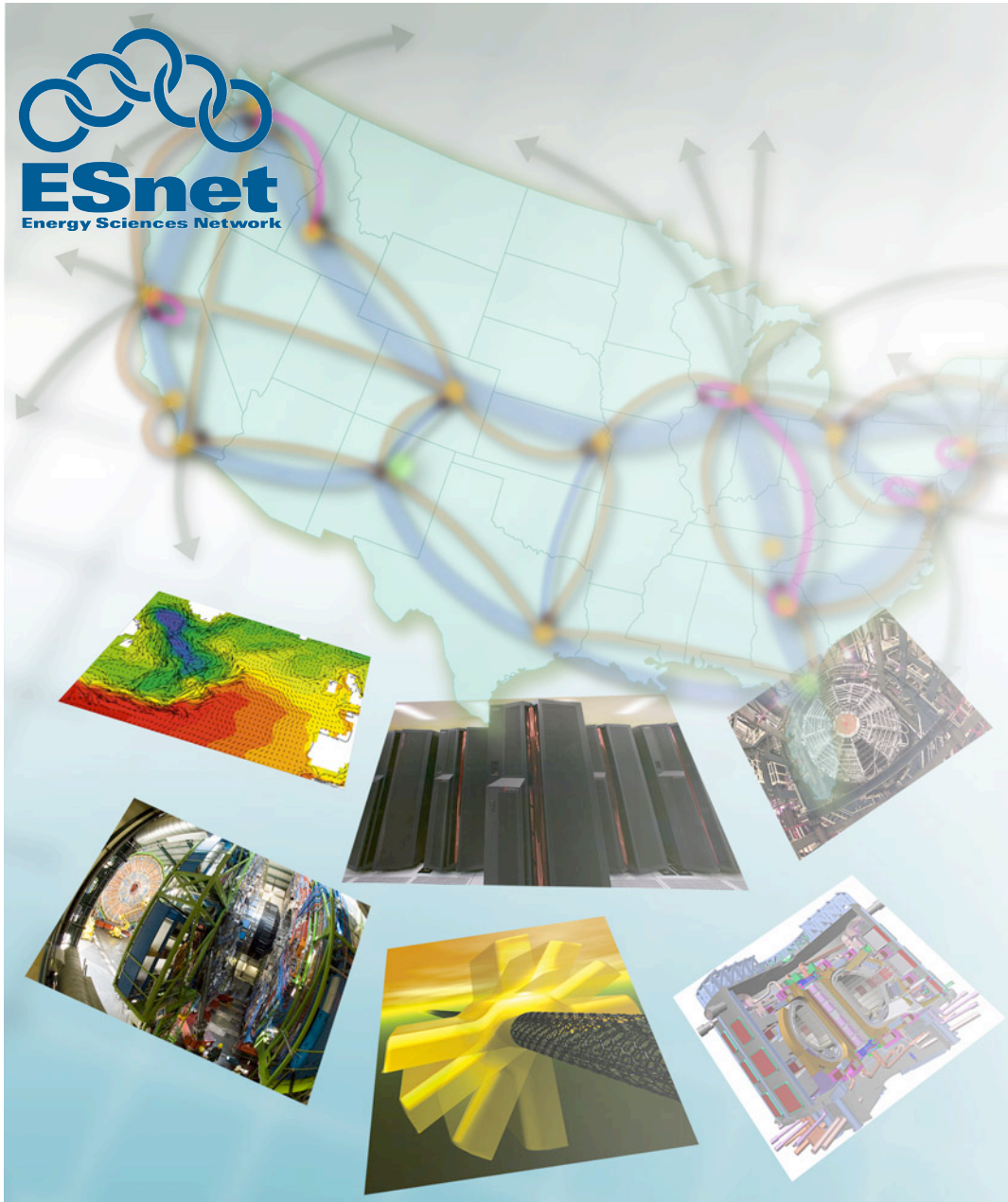


Overview of Network Measurement Tools

Jon M. Dugan
<jdugan@es.net>

Energy Sciences Network
Lawrence Berkeley National Laboratory

NANOG 43, Brooklyn, NY
June 1, 2008

Networking for the Future of Science

What we hope to give you today

- An idea of what kinds of thing can be measured
- An introduction to supporting terms and concepts
- An overview of what tools are available
- A first level introduction to a few tools
- Resources to enable you to learn more later

Ask questions! Disagree*! Interact!

* But only if you *do* disagree…

Active and Passive Measurements

- **Active Measurements send traffic through the network and observe the effect**
  - Generally easy to interpret
  - Affect the network under test
- **Passive measurements simply observe existing network traffic**
  - Often harder to interpret
  - Do not affect the network

Taxonomy of Measurements

- **Latency**
  - Round trip time (RTT)
  - One Way
- **Path**
- **Bandwidth**
  - Achievable Bandwidth
  - Bandwidth Estimation
- **Loss**
- **Frameworks**
- **Host instrumentation**
- **Traffic monitoring**

Things to be aware of

- **Interpreting results is often more difficult than expected**
  - The internet is a complex system
  - Problems can mask other problems
  - Many measurements are performed with heuristic approaches

- **Some examples**
  - Path Asymmetry
  - MTU mismatch blackholes
  - ICMP response blocking/limiting
  - Tunnels
  - Rate limiting, QoS

- **Closing doors seems to open new doors**
  - Or “people are creative…”

Latency

- **RTT vs One Way**
  - Round trip measures how long it takes to get from A to Z and back to A again.
  - One way is simply A to Z
  - So One Way = RTT/2, right?
  - …Wrong.
- **Jitter is the change in delay**
  - Can often expose congestion
- **RTT tools**
  - ping
  - thrulay
- **One way delay tools**
  - OWAMP

Latency, Congestion, Loss

- **Latency is determined by two factors**
  - Physical length of path (limited by the speed of light)
  - Queuing delays along the path

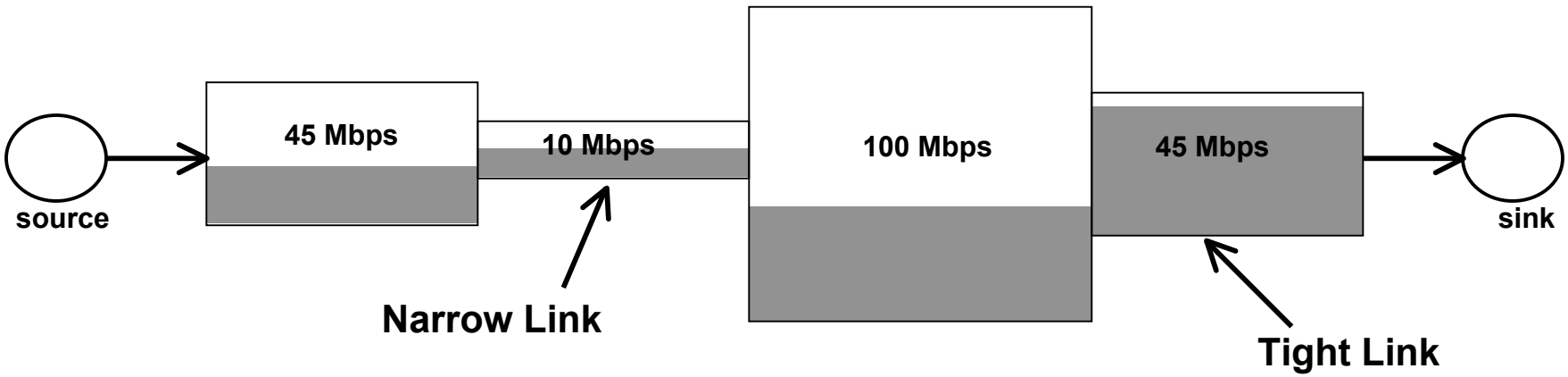
- **Loss can be thought of as infinite latency**

Path

- **traceroute**
  - Very useful
  - Must be mindful of asymmetry
    - traceroute servers can help, http://www.traceroute.org/
- **IP record route**
  - Often an option for ping
- **Handy hybrid tool: mtr**
  - http://www.bitwizard.nl/mtr/
  - traceroute+ping Finds path and pings each hop

What is bandwidth?

- **The term "Throughput" is vague**
  - Capacity: link speed
    - Narrow Link: link with the lowest capacity along a path
    - Capacity of the end-to-end path = capacity of the narrow link
  - Utilized bandwidth: current traffic load
  - Available bandwidth: capacity – utilized bandwidth
    - Tight Link: link with the least available bandwidth in a path
  - Achievable bandwidth: includes protocol and host issues



Achievable Bandwidth

- **Active measurement**
- **Put some traffic out on the wire and see how fast it goes**
- **The devil is in the details**
- **Common examples**
  - nttcp http://freeware.sgi.com/source/nttcp/nttcp-1.47.tar.gz
  - Iperf http://iperf.sourceforge.net/
  - nuttcp http://www.lcp.nrl.navy.mil/nuttcp/
- **Many/most of these tools can do UDP and TCP tests**
- **Some can do things like multicast, etc**
- **Hybrid approach: thrulay**
  - Measures throughput and RTT
  - http://e2epi.internet2.edu/thrulay/

Bandwidth estimation tools

- **Idea: send a train of packets and observe how they disperse along the path**
- **Gives insight into queuing behavior**
- **Clock resolution is limiting factor**
- **Examples**
  - pathload, measures available bandwidth
  - http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/pathload.html
  - pathchar, ftp://ftp.ee.lbl.gov/pathchar/
  - pchar, http://www.kitchenlab.org/www/bmah/Software/pchar/

Frameworks

- perfSONAR, http://www.perfsonar.net/
- BWCTL, http://e2epi.internet2.edu/bwctl/
- NetLogger, http://acs.lbl.gov/NetLoggerWiki/index.php/Main_Page

perfSONAR

- **A collaboration**

  Production network operators focused on designing and building tools that they will deploy and use on their networks to provide monitoring and diagnostic capabilities to themselves and their user communities.

- **An architecture & a set of protocols**
  - Web Services Architecture
  - Protocols based on the Open Grid Forum Network Measurement Working Group Schemata
  - Several interoperable software implementations
    - Java, Perl, Python…
  - Tools are designed to work in a cross provider fashion
- **A deployed measurement infrastructure**
  - primarily in the R&E space
- **http://www.perfsonar.net/**

Traffic Monitoring

- **Packet capture & analysis tools**
  - tcpdump, http://www.tcpdump.org/
  - Wireshark, http://www.wireshark.org/
  - ntop, http://www.ntop.org/
  - tcptrace, http://www.tcptrace.org/
  - bro, http://www.bro-ids.org/
    - Designed for security research
    - Very nice language to tracking network state
    - Might be a good base for other kinds of analysis
- **Flow analysis**
  - Netflow
  - Sflow
- **SNMP**
  - Coarse granularity

Host Instrumentation

- **Web100, http://www.web100.org/**
  - Best place to observe TCP issues is inside the TCP implementation
  - Defines a MIB for inspecting the state of a TCP session
  - Current implementation is for Linux (Windows possibly)
  - There is a lot you infer from this data, see NDT

- **Other host instrumentation**
  - Interface counters
  - Log messages

Resources

- **CAIDA's Taxonomy of Tools: http://www.caida.org/tools/taxonomy/**
- **http://www.cs.columbia.edu/~hgs/internet/tools.html**