Measuring the Measurers: How is Atlas Used?

Cristel Pelsser <pelsser@unistra.fr>
Emile Aben <emile.aben@ripe.net>
Laurent Vanbever <lvanbever@ethz.ch>
Randy Bush <randy@psg.com>
Romain Fontugne <romain@iij.ad.jp>
Thomas Holterbach <thomahol@ethz.ch>
Agenda

• What Tools are Popular?
• What Measurements are Made?
• The Major User Classes
  • Built-Ins (DNS Roots, Anchors) – One ‘Measurement’
  • System users (DNSmon etc.)
  • Privileged Users (Long Running RIPE Experiments)
  • Normal Users (Operators & Researchers)
• Ops and Researchers
• No Personal Data were Used or Published
What Tools are Popular?
Figure 1: Number of results the platform delivered between April 2015 and April 2016 with a per-day granularity and for each type of measurement.
How Many Users Used Each Tool?
Figure 2: Number of users who used each type of measurement between April 2015 and April 2016. Ping and traceroute are the most popular tools.
How Many Pings and Traceroutes?
Built-ins Dominate

(a) Ping
System Users Dominate

(b) Traceroute
Can We Tell Ops from Researchers?
Shooters & Sprayers

shooters, who predominantly source measurements from, or perform measurements to, a single AS (ops?)

sprayers, where the sources and destinations of measurements are more diverse (researchers?)
Figure 5: Characterisation of topological diversity per user using the *shoot-or-spray* metric. Users are ordered by increasing metric.
We Also Looked at Probe Diversity, Geographic and Topological
We Also Looked at Measurement Diversity, Geographic and Topological
And it is All in Our Lovely Paper (in submission to IMC so not yet distributable)

What Can We Do Using Only the Built-In & Anchor Traceroutes?
Challenge: Traffic is asymmetric

The differential RTT ≠ delay of link B-C but ...
Delays along non-common paths are independent.

(a) Round-trip to router B (blue) and C (red).

(b) Difference of the two round-trips ($\Delta_{PBC}$).
The central theorem tells us that with enough samples we have a normal distribution.

We only keep links that are observed from a significant number of ASs.
Detection of RTT changes

Example: DDoS attacks against DNS root servers
We Have a Similar Technique to Detect Forwarding Changes & Drops
Telekom Malaysia BGP route leak

(a) London-London link: delay change reported on June 12th at 09:00 and 10:00 UTC.

(b) New York-London link: delay change reported at 10:00 UTC. RTT samples for June 12th at 09:00 UTC are missing due to forwarding anomaly (packet loss).
But Why Did We Look at That?

Figure 8: Delay change magnitude for all monitored IP addresses in two Level(3) ASs.
And Forwarding Too!

**Per-AS Alarm!**

**For Forwarding**

**Figure 9:** Forwarding anomaly magnitude for all monitored IP addresses in two Level(3) ASs.
Congestion: Red nodes depict IP addresses detected by forwarding anomalies

Malaysia 10,200km this way
See! Research Can Be Operationally Useful!