ISPMON and IPFIX:

Improving measurement and monitoring for ISPs

Nevil Brownlee
CAIDA, SDSC, UC San Diego *and*
The University of Auckland
nevil@caida.org

IETF 57, Vienna, July 2003

Background

- ISPs have always monitored their networks
  Today many of them provide near-real-time reports of their network performance via web pages
- Measurement is still an art (underpinned by science)
  I believe that an ISPMON Working Group could improve this situation, thereby helping ISPs ...

Define more useful *ISP metrics*

- Plenty of metrics are already defined
- Many of them, e.g. IPPM one-way and two-way delay, have well-tested implementations
- We need to collect ISP experience as to what metrics would really help to support network operations, and how they can best be measured
- Such an effort would produce a (short) list of metrics, and of tools which measure them reliably

Provide better tools for *e2e* measurements

- End-to-end application performance is important to customers, e.g. companies using VPNs linking many sites
- Determining why e2e performance is poor can be difficult because several different ISP networks may be involved
- To help with this:
  - Equipment vendors should provide standard ways to measure the *ISP metrics*
  - ISPs should work towards making those metrics accessible to other ISPs, e.g. from a set of well-placed ‘measurement boxes’ in their own network

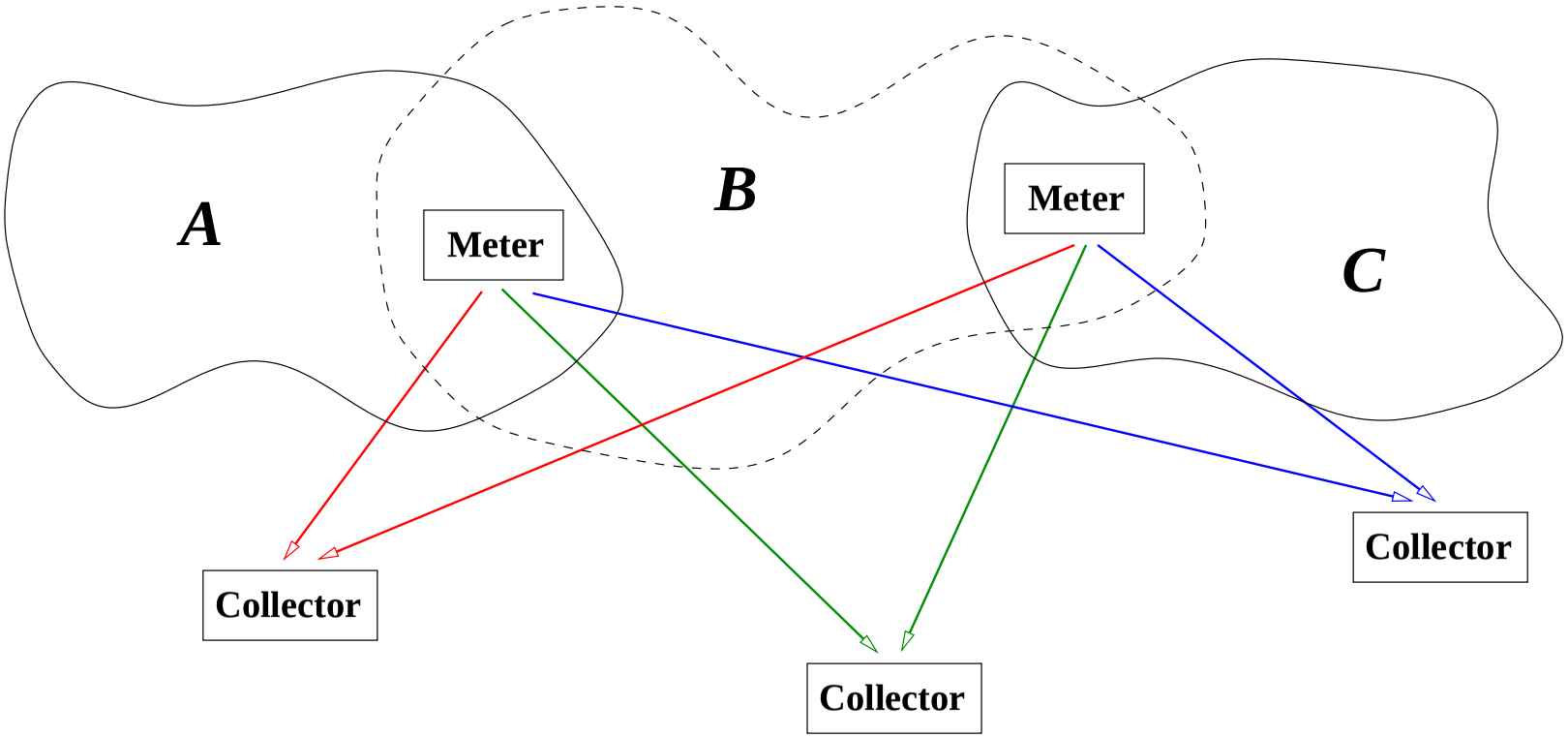
Find better ways to *use* network data

- Storing, visualising and analysing network data is *hard* to do
- Everyone uses tools like MRTG, Argus, snort, bro, etc., but can we do better?
- For example, would it be worth looking again at something like the Operational Statistics reporting scheme, RFC 1857?

IPFIX: IP Flow Information eXport

- Charter: to standardise Best Current Practice for IP Flow Export
- Overview:
  - Flow – *set of packets sharing some common properties*
  - Observation Point – *probe, router, line card, etc.*
  - Metering Process – *builds table of flows*
  - Exporting Process – *sends flows out from IPFIX Meter*
  - Collecting Process – *receives flows from Meter(s)*

ISPMON Scenario:
Multiple ISPs sharing Traffic Matrices



- Three ISPs (A, B, C), two border routers, each with an IPFIX meter
- Each meter configured to export AS-AS traffic data *relevant to each ISP*
- All providers get accurate info about their transit traffic among each others' networks