Router Siblings

NPS-SIX
January 7, 2013
Robert Beverly
rbeverly@nps.edu
Some (Bad) Ideas

• DNS-based:
  – Reliable? Probably not…

• ICMPv6 Node Information Queries (RFC4620)
  – “An implementation of this protocol MUST have a default configuration that refuses to answer queries from global-scope addresses”

• Router fingerprinting (nmap style)
  – Not enough diversity?

• ICMP4 in IPv6 (next-header 4):
  – ICMP6 parameter problem 😞

• ICMP6 hop-by-hop timestamps
  – IETF ID, not implemented....
ICMP Packet Train

• Routers typically respond to ICMP/ICMP6

• Idea:
  – Send train of (interleaved) ICMP and ICMP6 probes to candidate sibling pair
  – Analyze interpacket delay differences

• Can this possibly work?
ICMP Packet Train

• Intuition:
  – Routers distribute data-plane forwarding, centralize control-plane (e.g. proc ICMP)
  – Routers often rate-limit ICMP (serves as fingerprint?)
  – Router bandwidth from line-cards to central processor limited (still true? E.g. M40=100Mbps)
  – Router ICMP generation delay? ~0.5ms (Govindan, Paxson 2002), but with 1,2,3ms modes. (Still true today?)
  – Timing characteristics will reveal shared congestion patterns?
Contrived Example in Lab

- A4, A6 siblings. A4, A6 address single physical interface. B6 other host.
- Congest A4, A6’s physical interface
- Run interleaved v4/v6 packet trains to all
Never as clean in practice

- Known rtr siblings
- V4 processed faster than v6?
Never as clean in practise

- Known rtr siblings
- Queue on v4 path not on v6 path?
Never as clean in practise

- Known rtr siblings
- V4 and V6 paths congruent?
Rate Limit Fingerprint?

- Known rtr siblings
- V4 rate limited, but v6 not?
- Bursts indicative of congestion or processing?
Summary

• Lots more work to do...
• Questions/flames?