traceroute(8)

ECE-9609B-001-GW19

Joe Abley <jabley@uwo.ca>

traceroute(8)

- A way to map a path from one point to another over an IP network
    - First implemented by Van Jacobson in 1987/8, based on an idea by Steve Deering
    - Concept preserved in IPv6
- Applications in network operations, customer support, and remote mapping of networks from the outside for whatever reason

this is a stupidly brief

12-minute overview

Mechanism

- Makes use of the TTL field in the IP datagram header
  - intended for loop detection/prevention
    - routers decrease the TTL as they process a packet; if the TTL drops to zero the packet is dropped and a control message is sent back to the source
- Traceroute sends probe packets with increasing TTL and collects and processes the control messages

Variations

- Probe Protocol (e.g. UDP, TCP, ICMP echo request)
- Multiple probe packets per hop
- Asynchronous origination of probe packets
- Combination with other diagnostic tools, like ping
- DNS resolution of intermediate router addresses; identification of originating Autonomous System numbers

Round-Trip Latency

- Traceroute records round-trip latency but only identifies an outbound path
- Latency includes
  - queuing and serialisation delay (measure of congestion)
  - propagation delay (measure of signal distance)
  - processing delay (due to rate-limiting and processing constraints in routers)
  - errors (transient phenomena that are not reliable indicators of anything much)

Asymmetric Paths

- In general, all Internet routing is asymmetric
  - the path back from any intermediate router to the source may not be the simple reverse of the outbound path, and the return path latency might not match the outbound
- prevalent at autonomous system borders
  - routing policy divergence
  - multi-homing

Equal-Cost Multi-Path

- Link aggregation at the IP layer
  - rely upon equal-cost routes to share traffic across multiple candidate paths
  - flow-hashing defeated e.g. by transport-layer destination port variation in successive probes
  - different-length equal-cost paths can produce confusing output

MPLS

- Internet (or accessible) routing domain implemented as an overlay network above a label-switched core
    - core network still runs on IP, still decrements TTL
        - core network doesn't have the routing scope to be able to send ICMP messages to the traceroute source
- Tunnel the ICMP messages to the end of the label switch path
    - all hops across the core demonstrate identical latency

Everybody Hates the DNS

- Reverse DNS -- mapping of address to name (hence "reverse"; the original and prevalent motivation is the other way round)
- Nothing breaks, in general, if you neglect your Reverse DNS
    - as a consequence, everybody neglects it unless they automate it
    - most people don't automate it
    - it sucks

let's play