1999-12-15

BU/NSF Workshop on Internet Measurement, Instrumentation and Characterizatio

Heuristics for Internet Map Discovery

Ramesh Govindan

USC/Information Sciences Institute

Joint work with Hongsuda Tangmunarunkit

Don't Try This At Home...

Date: Mon, 08 Mar 1999 09:44:03 -0800
From: "Harry Starr" <starr@gccs.com.au>
To: <action@ISI.EDU>
Subject: {9903.309} Attempted break-in attempts from your domain

It has been noted that REPEATED attempts, from a machine in your domain;

128.9.160.210 (water.isi.edu)

at source routing to our router has occurred.

If this action is NOT stopped forthwith, **you will be reported to Australian Federal Police as computer hackers.**

Yours,

Harry Starr
- ----------

Harry N. Starr
Gold Coast Computer Services
6 Glen Osmond Road
Yatala QLD 4207
Australia

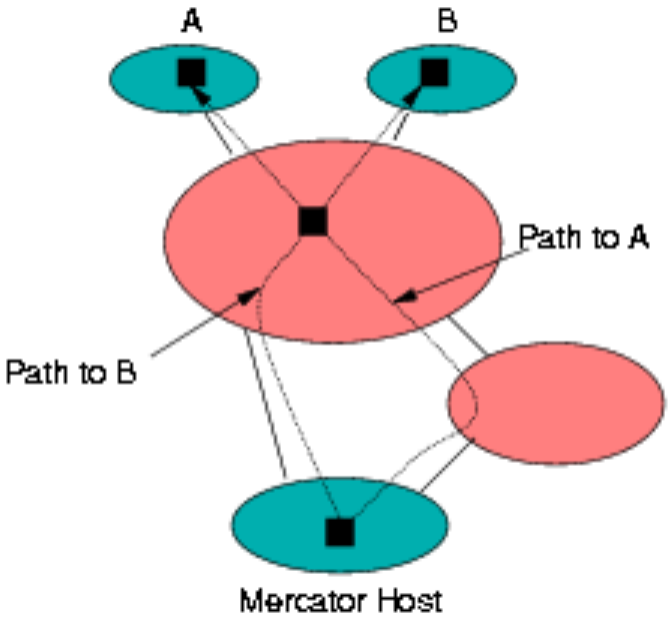
Informed Random Probing

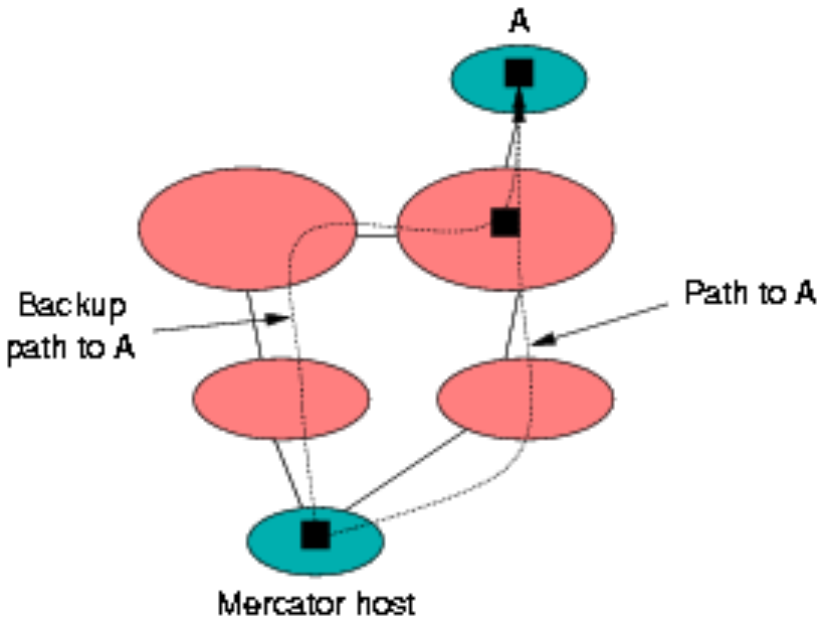
- In the absence of external databases
  - guess which portions of the space contain addressable nodes
- Guessing addressable prefixes
  - If an address A is seen in a path probe, assume that some prefix P of A contains addressable nodes
    - hence, *informed* by path probes
  - If a prefix P contains addressable nodes, then some neighboring prefix also contains addressable nodes
- What prefix lengths to use?
  - 8 for class A, 16 for class B and 19 for class C
  - mirrors registry allocation policies

Path Probing

- Easy, like traceroute, but stops when
  - a hop fails
  - or a loop is detected
- Select prefixes by lottery scheduling
  - … based on the number of successful probes to that prefix
- To limit overhead
  - … a configurable number of prefixes probed in parallel

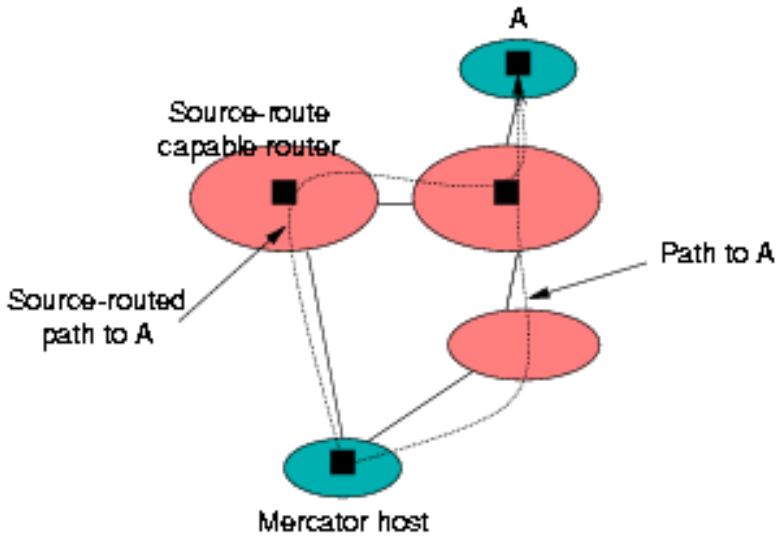
Path Probing





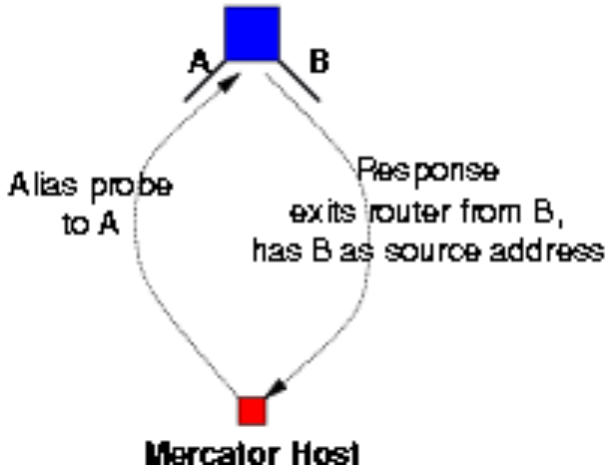
… can provide some richness in topology

Source-routed Path Probing



Alias Resolution

- For ICMP unreachables
  - most routers use as source address
  - … the address of the outgoing interface towards host
- So, a UDP packet sent to A
  - … can reveal A and B to be aliases for the same router
- Need to do this repeatedly!
  - … because routes can change
  - only a small number of such probes outstanding at any instant



Experiences: Path Probing

- Misconfiguration
  - class D address as source
  - traceroutes to net 10
- Otherwise, path probing seems to work well
  - doesn't appear that major ISPs disable traceroute
  - … or avoid decrementing TTLs across their infrastructure
- Oddity
  - router with more than 1800 neighbors!

Experiences: Source Routing

- Number of source-route capable routers surprising
- About 1 in 6 links are discovered by source routing
- Source routing not entirely bug free
  - missing hops in source-routed traceroutes
  - at least one router which ignores the source route option and processes packet
  - older versions of router code may not decrement TTLs

Experiences: Alias Resolution

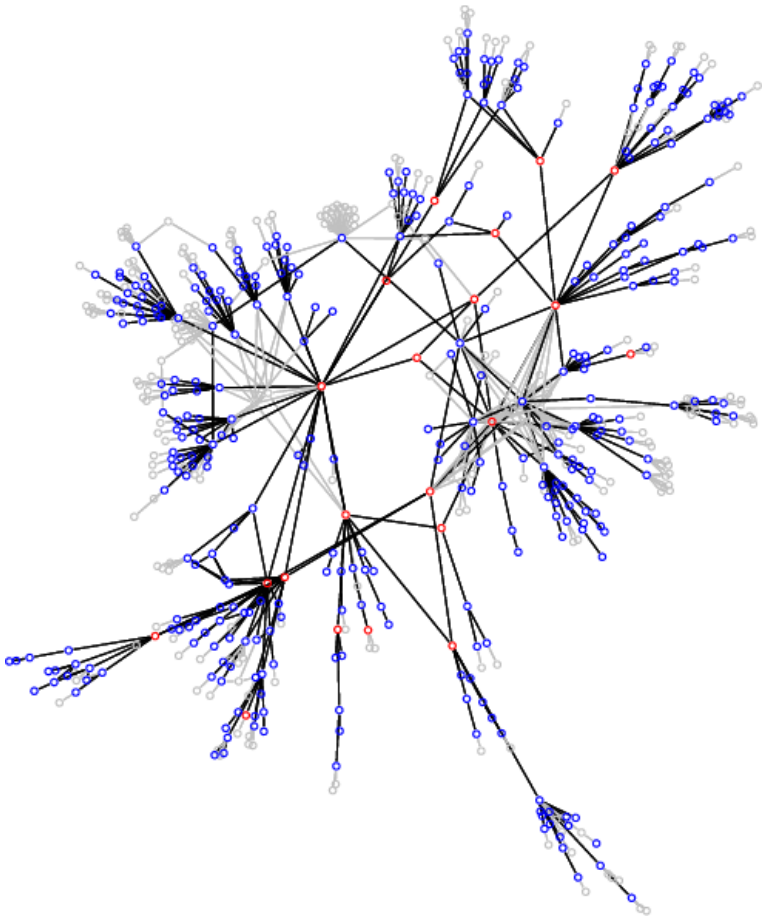
- About 15% of interfaces were not reachable
- Reasons
  - numbered out of private space
  - routes not propagated beyond ISP border
  - routes not widely propagated
    - source-routed alias resolution works, but is slow

Experiences: Social

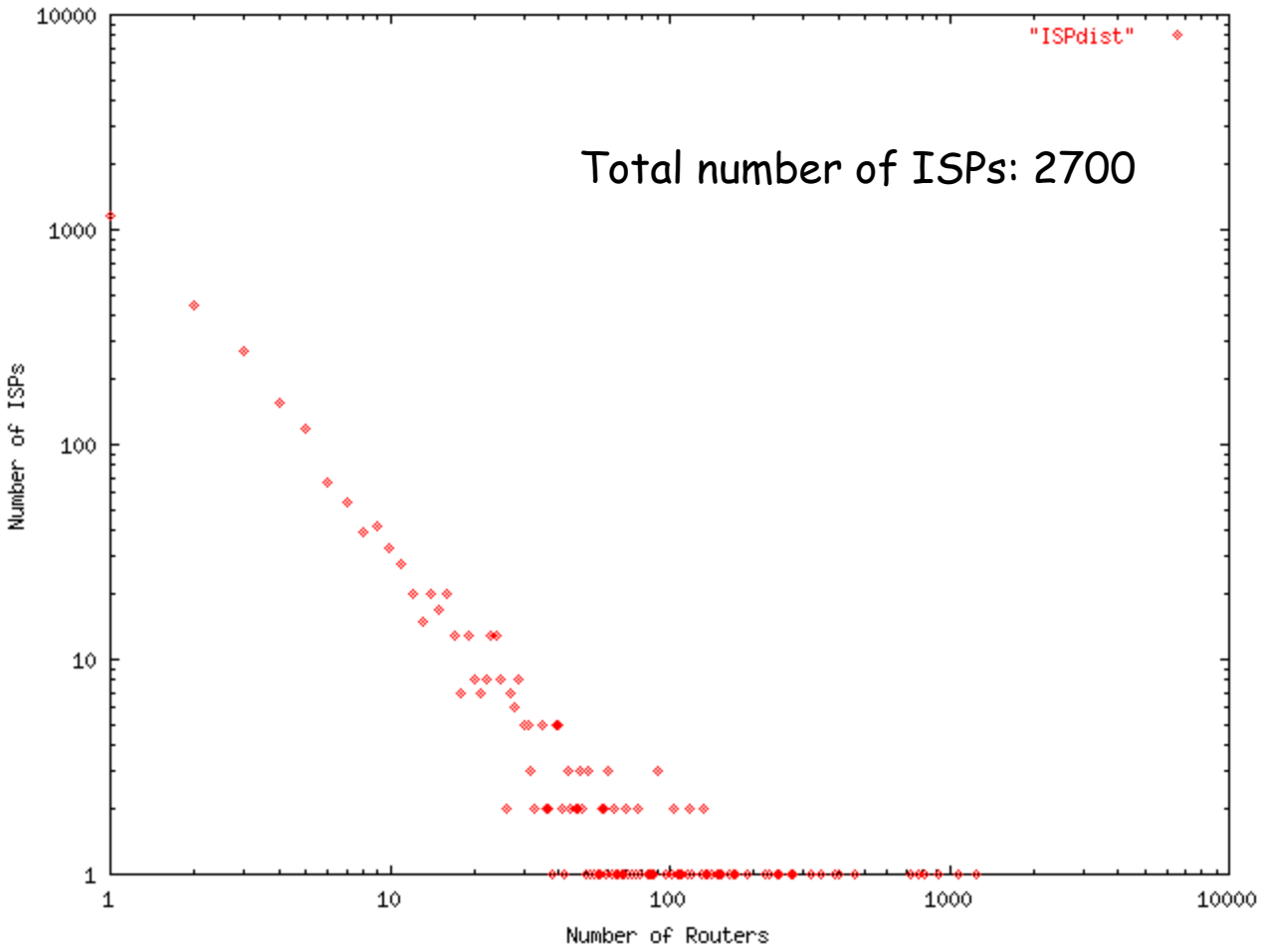
- About 100 abuse complaints over a six month period
- Mostly from firewall operators with logging enabled
  - financial institutions
  - the DoD
- International representation
  - few from Europe, one each from South Africa, Australia
- Only one major ISP
  - and only because the probes reached their corporate offices…
- Mostly supportive, for others we use exclusion lists

Validation: Extracting Subgraphs

- Can use DNS to extract ISP maps
  - map of Telstra shown
- Compare against ISP maps
  - Los Nettos: 100%
  - Verio: 90%



ISP Size Distribution



http://www.isi.edu/div7/scan