Diagnosing the Location of Bogon Filters

Randy Bush
Internet Initiative Japan (IIJ)

James Hiebert
National Oceanic and Atmospheric Administration

Olaf Maennel
University of Adelaide

Matthew Roughan
University of Adelaide

Steve Uhlig
Delft University of Technology

Outline

- Advertising a new prefix
- Methodology
- In-probes
- Out-probes
- Relationship in- and out-probes
- Further work

Problem: “Bogon filters”

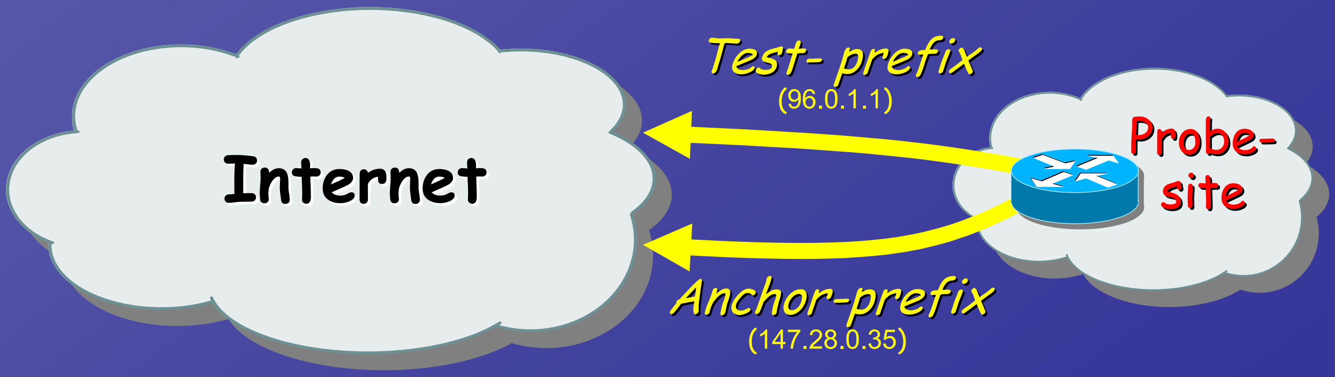
- ISPs often filter unallocated address space to protect themselves from malicious attacks and unwanted traffic
- Over time unallocated address space may become allocated and legitimately announced address space...
- Problem: Filters need to be updated but seem often not to be

Objectives

- Develop methodology that is capable of detecting filters that are blocking newly allocated address space
- Analyze reachability status of a newly allocated prefixes
- For the experiment, ARIN loaned us
  96.0.0.0/16 97.64.0.0/16
  98.128.0.0/16 99.192.0.0/16

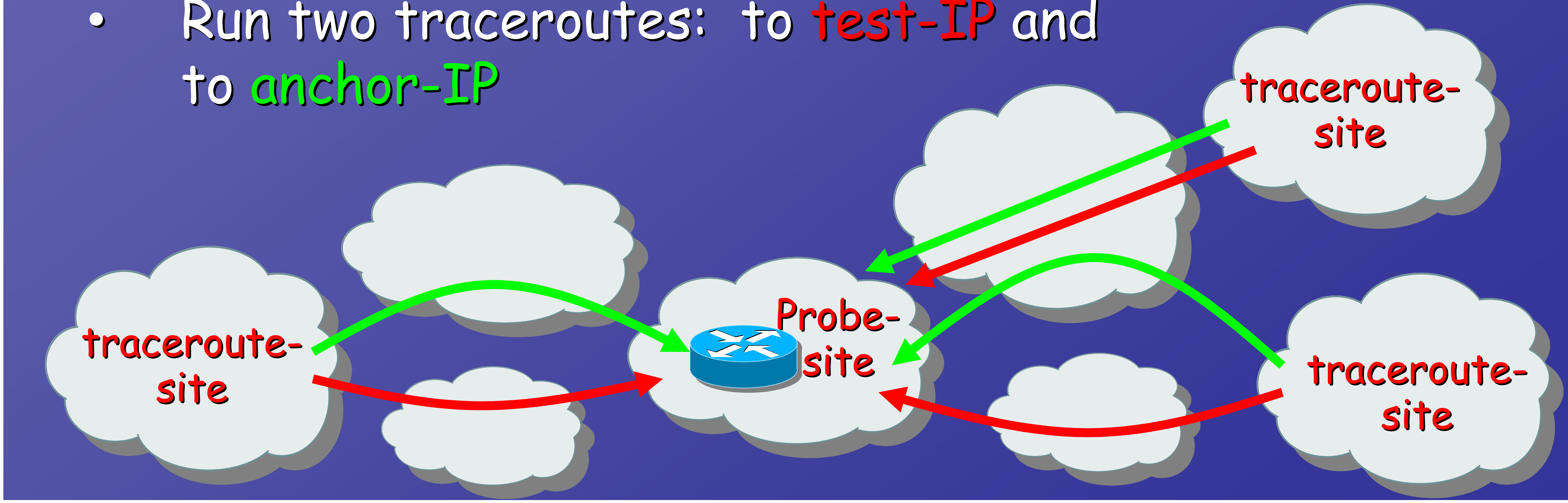
Testing reachability of a new prefix

- Terminology:
  - *Test-prefix*: newly allocated prefix to be tested
  - *Anchor-prefix*: well-established prefix whose reachability should be fine
  - *Probe-site*: router that announces *both* the test-prefix and the anchor-prefix



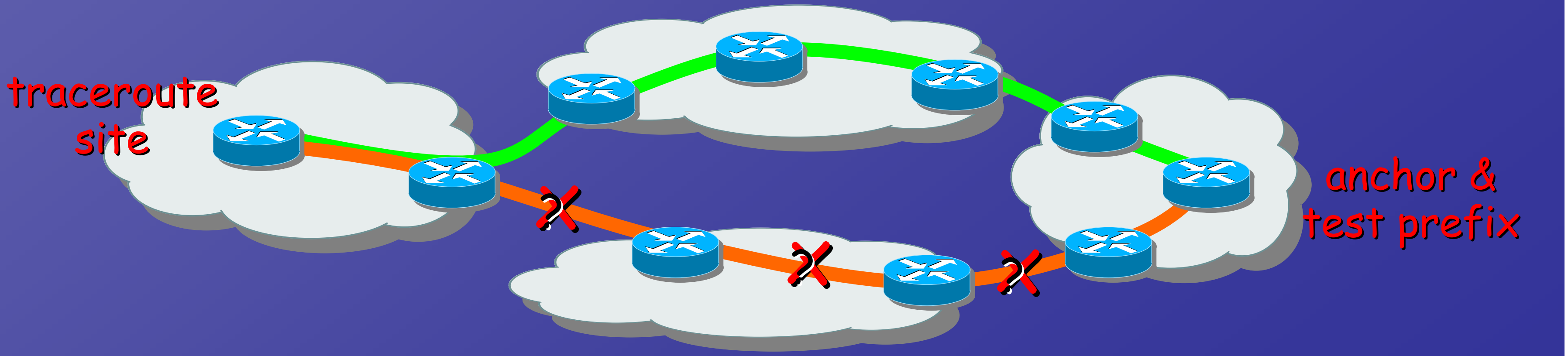
Testing reachability of a new prefix: In-Probes

- Two IPs hosted at the same location:
  - anchor IP : well established, hopefully unfiltered
  - test IP : newly allocated address
- Assume that they are propagated in the same way (as they are announced from the same location)
- Run two traceroutes: to test-IP and to anchor-IP



In-Probes: Principles

- *In-probe* : traceroute performed from external IP addresses towards the test and anchor prefixes
- In-probes give reachability information towards the test and anchor prefixes
- If traceroute from test-prefix address diverges at some point, we conjecture that some *bogon filter* is responsible



In-Probes: measurements

- Advertise test and anchor prefixes from 4 probe-sites: Seattle (USA), Munich (DE), Wellington (NZ), Tokyo (JPN)
- 2,052 traceroutes in total (test+anchor counting as one):
  - from up to 744 different locations
  - from NANOG-posting: 881 (towards two locations)
  - from Traceroute-sites: 981 (towards four locations)
  - from PlanetLab: 190 (towards four locations)

In-Probes: results

Categories:

- "good" (anchor and test take exactly same path)
  - 66.9% (1,373)
- "diverging inside" (anchor and test take different paths)
  - 20.6% (423)
- Test stops, but anchor ok
  - 8.6% (177)
- Failure (either anchor or anchor and test failed)
  - 3.9% (79)

In-Probes: results

- Derive candidate links, eliminate unlikely candidates.
- Remaining candidate links:
  - ~ 32 ASs that may contain wrongly configured filters.

- http://psg.com/filter-candidates.txt

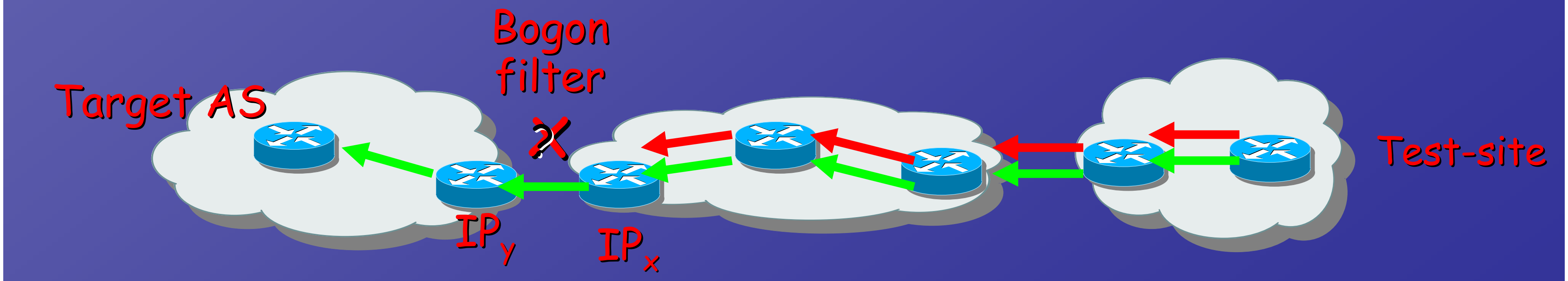
In-Probes: evaluation

- Advantages:
  - traceroutes go around bogon filters
  - known details about IP-level path
- Disadvantages:
  - traceroute site MUST be "behind" bogon filter
  - Not many traceroute sites available

- Goal: test as many ASs as possible for reachability
- Solution: "*out-probes*"

Testing for usable reachability: Out-Probes

- *Out-probe* : ping and traceroute performed from test-IP and anchor-IP towards external IP addresses
- *Target-AS* : AS towards which we perform out-probes
- If out-probe towards target AS from test-IP stops while the out-probe from anchor-IP goes on, we conjecture a *bogon filter of the form* <IP X, IP Y>:



Out-Probes: measurements

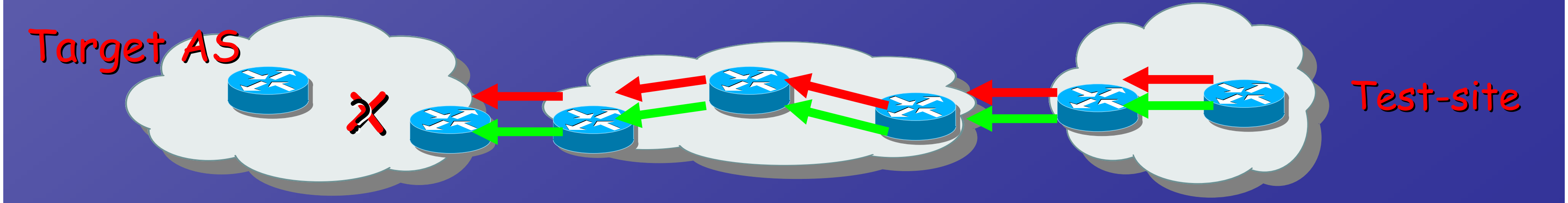
- Perform ping from *test-sites* (*test-IP* and *anchor-IP*) towards a large set of *target-IP* addresses (58,766) in 20,142 different ASs
- If ping comes back => usable reachability from *target-IP*
- If ping does not come back => run traceroutes to find out location of *bogon-filter(s)*
- Traceroute return path is interesting, but unknown: only usable reachability of the IPs on the path towards *target-IP* is obtained

Out-Probes: measurements

- Finding pingable IPs with acceptable AS coverage:
  - Probing IPs inside many prefixes to get 58,766 *target-IP* addresses that answer to ping probes
  - Among those *target-IPs*, not all may answer during the actual out-probe measurements
    (e.g., host might have been dial-up and down at the time of measurement)
- Data:
  - 197,825 traceroutes in total (test+anchor counting as one) from the 4 sites

Out-Probes: IP-level results

- Results of out-probes:
  - 65% successful pings
  - 13% test-only fails
  - 15% both pings fail
  - 6% of ping artefacts
- If ping does not reach *target-IP* but traceroute gets inside *target -AS* => ICMP artefact



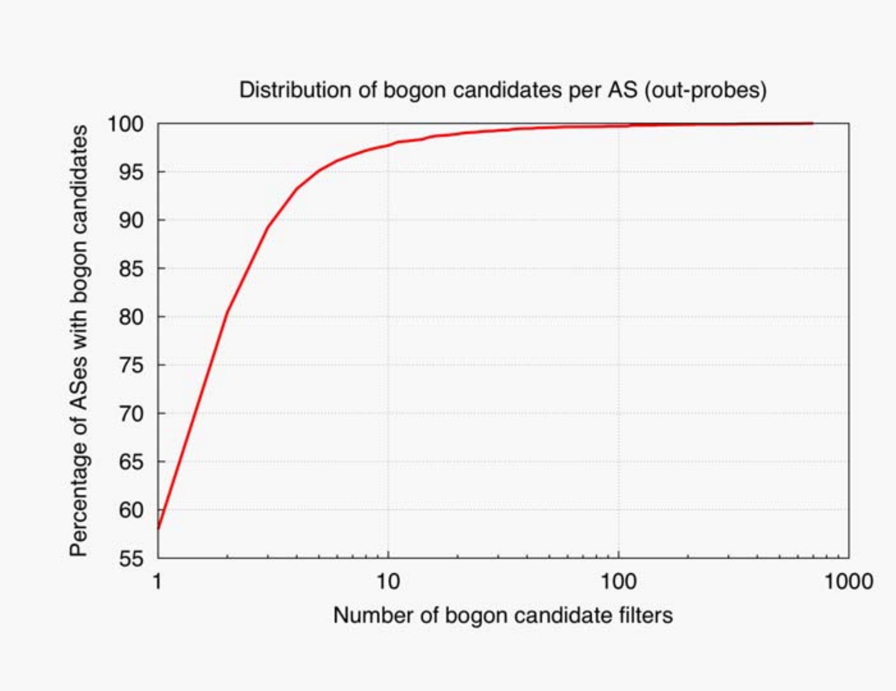
Out-Probes: AS-level results

- *Successful out-probe* : ping success for test towards all IPs within a target AS
  Unsuccessful out-probe : ping failure for test towards all IPs within a target AS
  Undefined out-probe : inconsistent results for test towards the IPs within a target AS
- Results:
  - 7,677 ASs with *successful out-probes* only
  - 2,298 ASs with *unsuccessful out-probes* only
  - 10,167 ASs with undefined out-probes
  - 50% of the 20,142 target ASs see a mix of successful and unsuccessful out-probes!

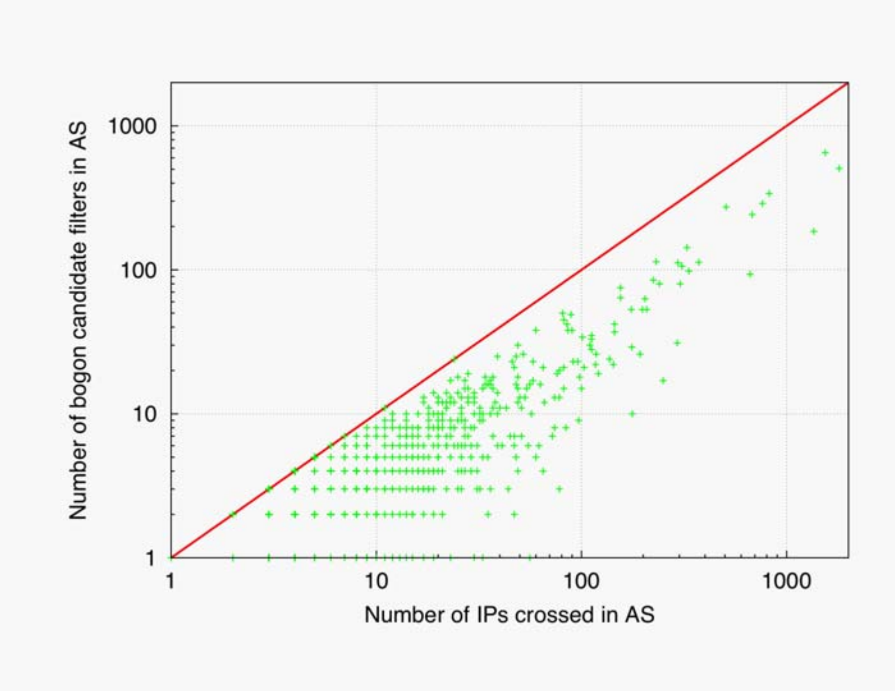
Out-Probes: *bogon filters*

- Identification of bogon filters gives 16,471 candidate links in 5,538 ASs
- Among the candidate links many are of the form <IP,?>, probably an artefact of ICMP filtering

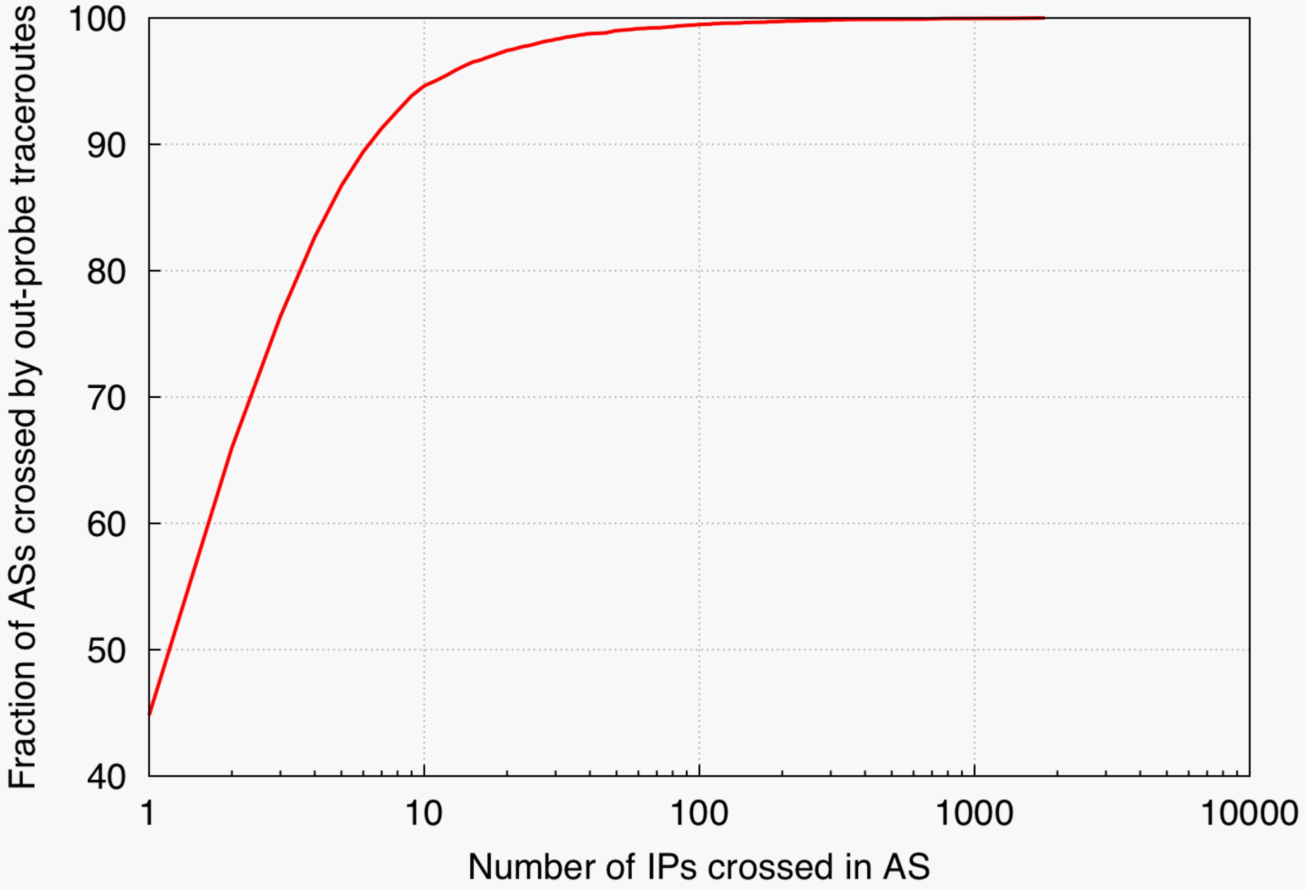
Some ASs have more candidate links than others:



Candidate links seem proportional to sampled IPs in each AS:

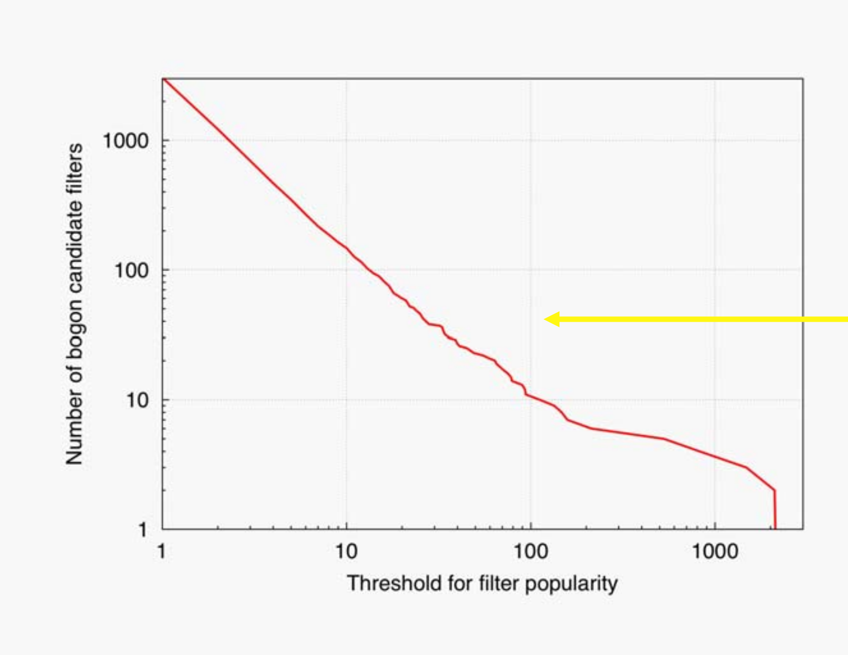


CDF of Number of Links Crossed



Out-Probes: popular *bogon filters*

- Building a list of likely bogon filters based on out-probes:
  - Remove the potential ICMP artifacts <IP,?>
  - Associate with each candidate a *popularity counter* that tells how many times a given bogon filter was identified in the traceroutes (for different sites and target IP addresses)
  - Number of candidates as a function of the threshold:



Power-law

=

no natural threshold

Relationship In- and Out-Probes

- Out-probes tell about “usable reachability”:
  - Find areas of non-reachability
  - Larger coverage (currently > 85% of Internet ASs)
  - No information about: return path and thus non-optimal paths
- In-probes tell us about filters on the path:
  - Reachability available - goal: detect intermediate filters
  - Smaller coverage
  - Many traceroute servers are needed at the “edge”

Further Work

- Sent list of candidate suspected bogon filtering links to ISPs, waiting for their feedback to validate our analysis
- Increasing number of in-probes to have more information about location of bogon filters and their number
- How accurate can we be in identifying bogon filters using measurements?
- How would we quantify that accuracy?
- How many out-probes are needed/useful

Results – Out-Probes

- We can identify unreachable places: Via out-probes we can see if an IP is not well routed.
- Aside from small issues related to ICMP, we know that if the probe doesn't come back that there is NO usable connectivity. That's simple and straight forward.
- The main contribution here is: it is possible to achieve a reasonable coverage of the Internet (~20k ASes).
- The methodology produces useable results.

Results – In-Probes

- We can go a step further and detect places where there is "non-optimal" connectivity.
- Keep in mind that with the in-probes we mainly look at traceroutes that BOTH reach the destination.
- We are talking "only" about sites that CAN reach the desired destination... so, we are looking at "interesting" routing scenarios and this is more like optimizing routing
- We are very curious to see where this will lead us.
- We would very much like more validation by the operational community

Thanks To

- ARIN
- CityLink - NZ
- IIJ - JP
- SpaceNet - DE
- Universities of Adelaide, Delft, and Oregon