Implementing a “bogon” filter detection service

Steve Uhlig
Delft University of Technology

Randy Bush
Internet Initiative Japan (IIJ)

Olaf Maennel
University of Adelaide

James Hiebert
University of Oregon

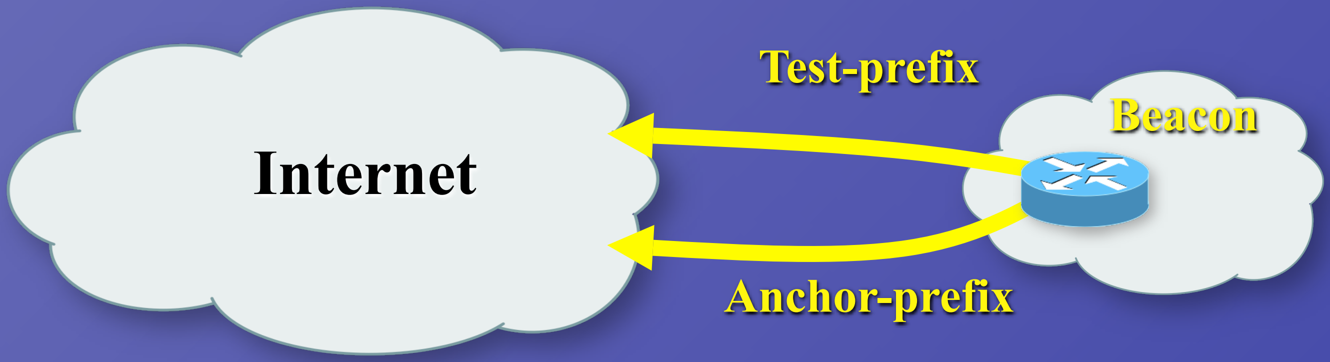
Matthew Roughan
University of Adelaide

Bogon Filters

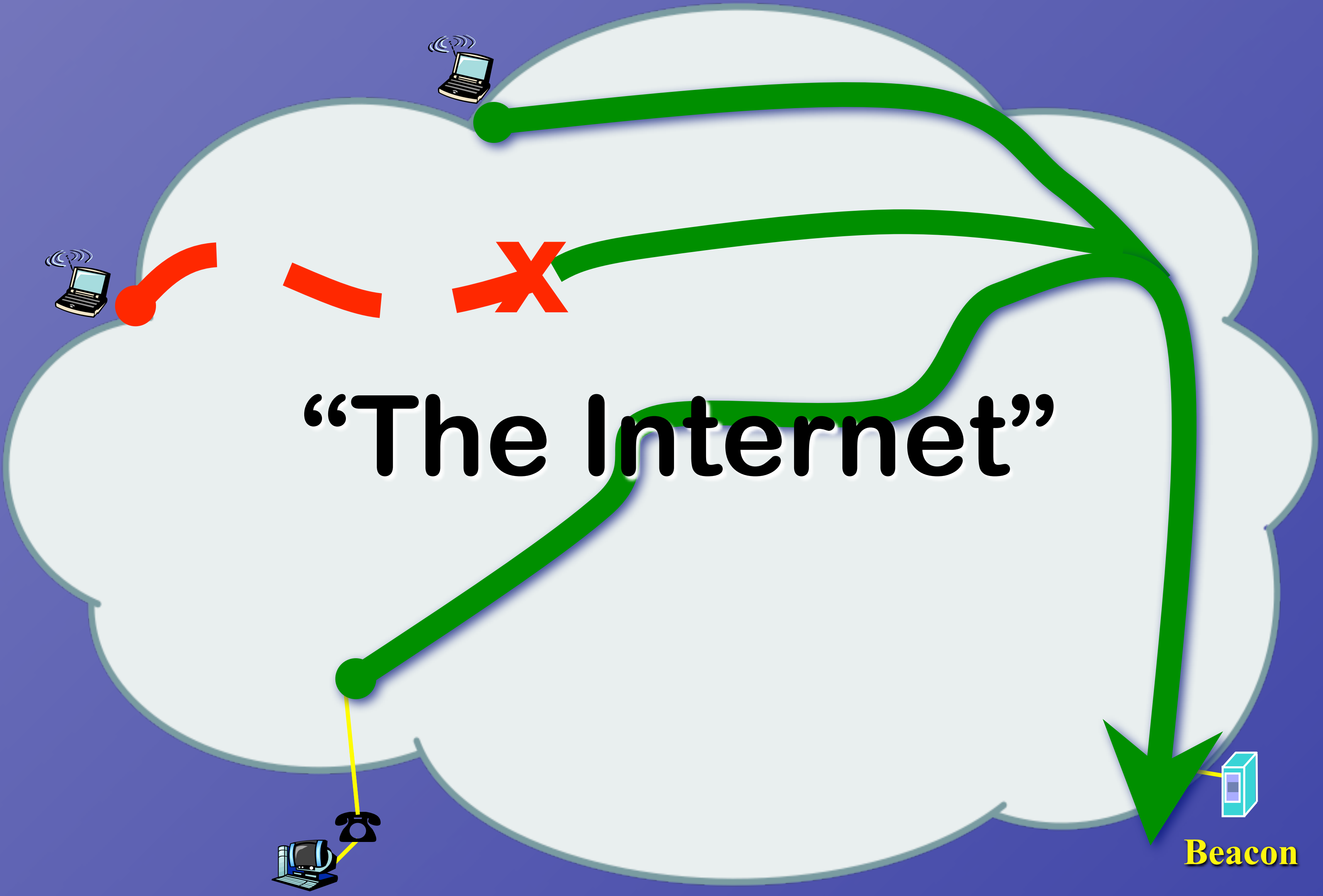
- ISPs often filter unallocated address space to protect themselves from malicious attacks
- However, over time unallocated address space becomes allocated and legitimately announced address space...
- Problem: Filters need to be updated timely, but seem often not to be
- Goal: Develop a tool that is capable of detecting and locating bogon filters, filters that are blocking newly allocated address space

Experiment

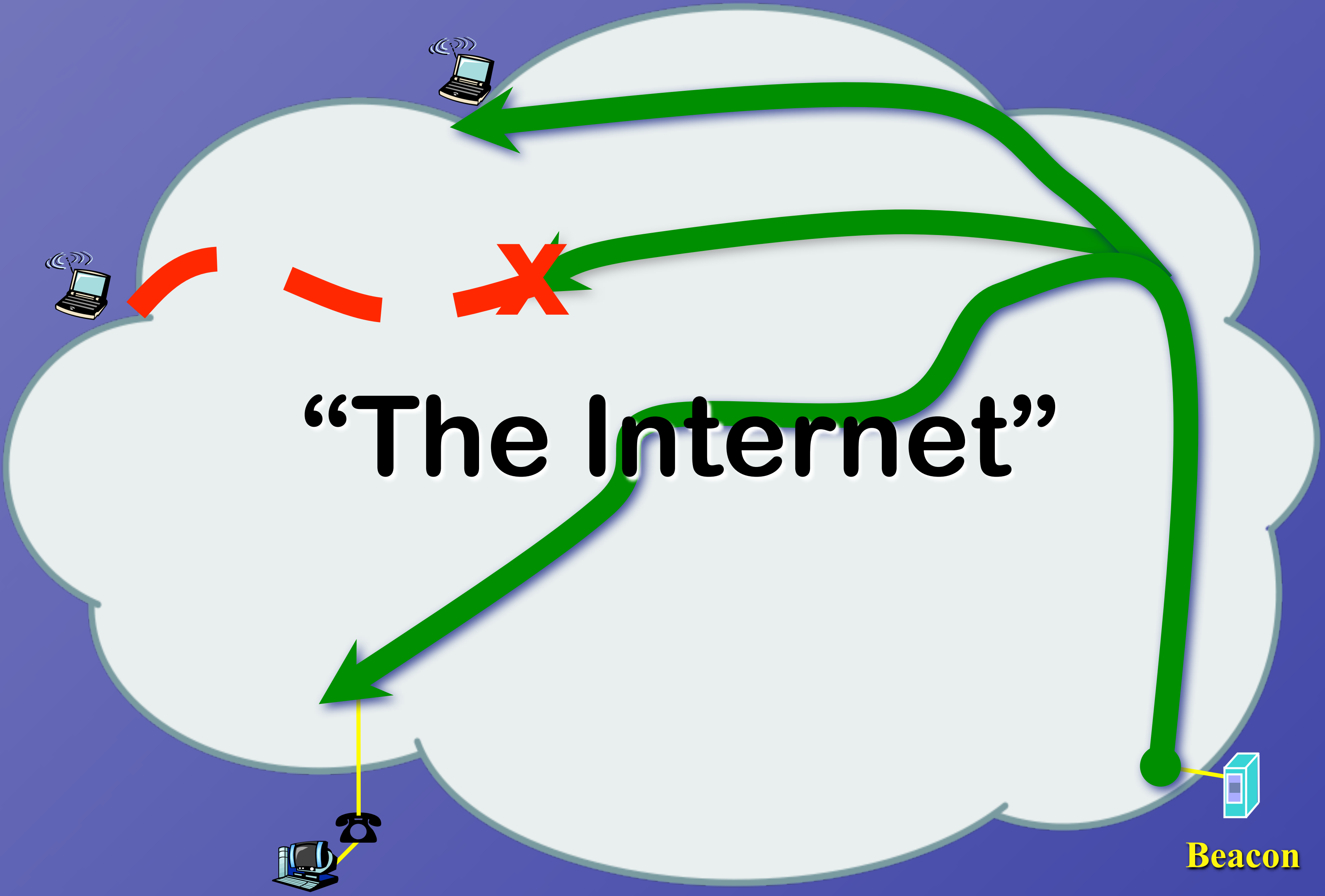
- Advertise test and anchor prefixes from 4 probe-sites: Seattle (USA), Munich (DE), Wellington (NZ), Tokyo (JPN)
- Probe as much as possible of the Internet
- Analyze reachability status of test prefix



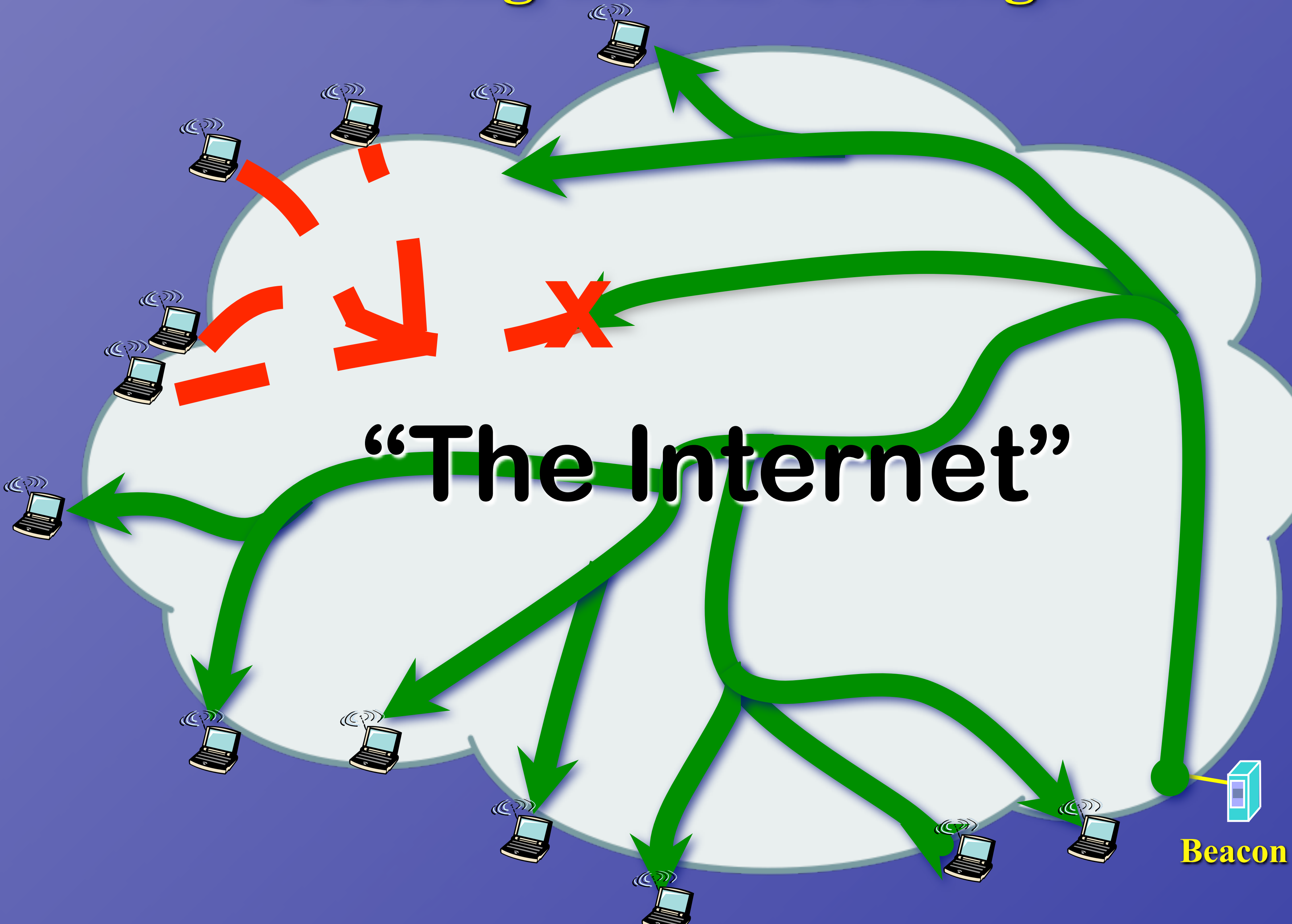
Reachability



Probing and AS Coverage

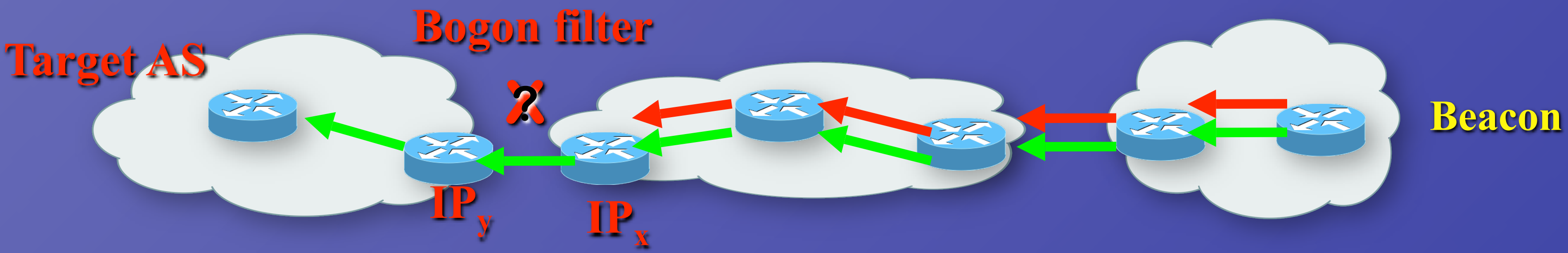


Probing and AS Coverage



Out-probes

- **Out-probe** : probes performed FROM test-IP and anchor-IP TOWARDS external IP addresses
- If probes comes back
  => reachability exits
- If probes do not come back
  => reachability does NOT exist :-(
  cross-correlate to locate bogon filter



Out-Probes: measurements

- Sent probes from beacons (test-IP and anchor-IP) towards a large set of pingable-IP addresses (46,569) in 18,574 different ASs
- If probe comes back => reachability exists
  - ~85% of all probes
- If probe does not come back => find out ASs that contain bogon filter
  - ~10% of all probes
  - ~5% not pingable anymore (e.g. dial-up)

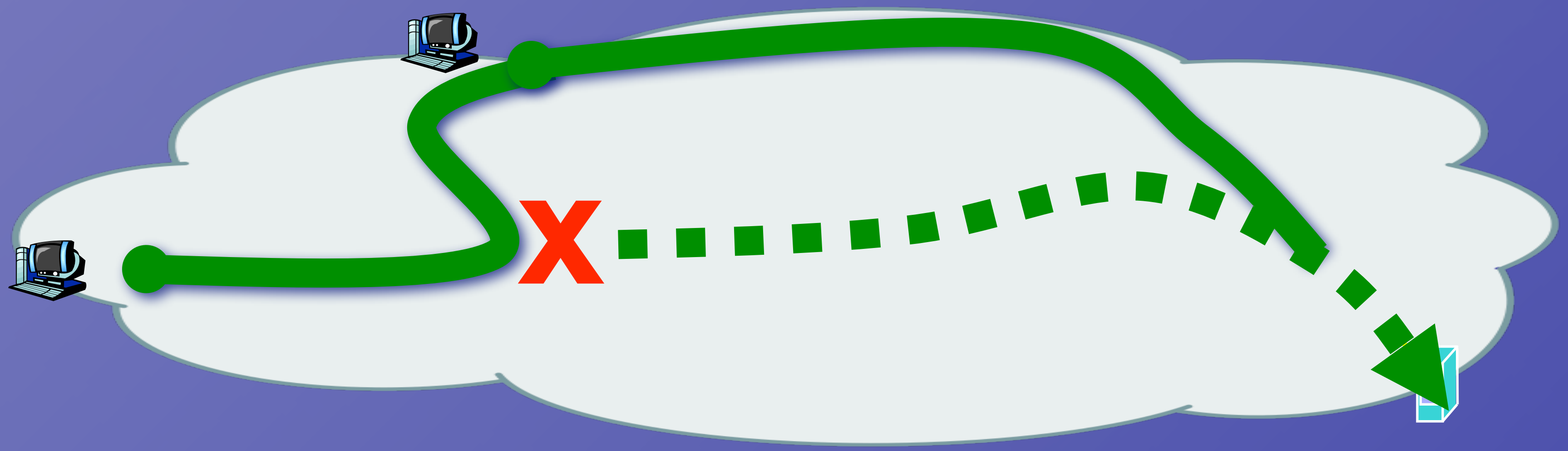
Out-Probes: Initial validation

- Derived 443 candidate ASs that are likely to filter
- Found 15 traceroute servers within those 443 candidate ASs:
  - 7 filter
  - 5 do not filter themselves, but had no usable connectivity [upstream filtered].

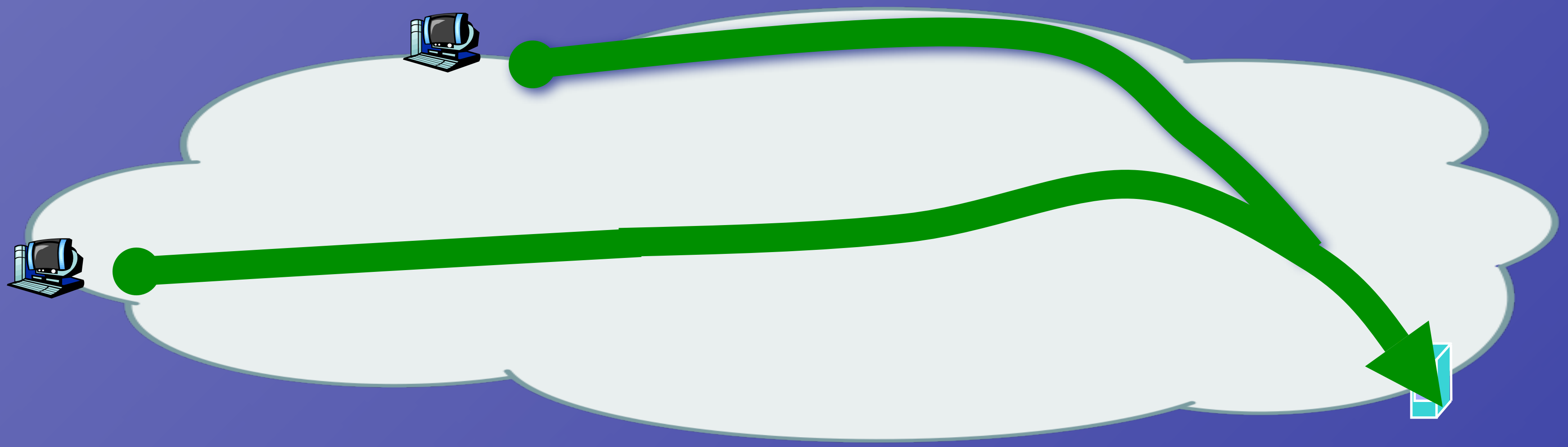
=> 12 out of 15 (80%) correctly identified

- 3 failed, but validation was done a month later. ASs might have updated filters in the meantime

Traceroutes filtered/non-filtered



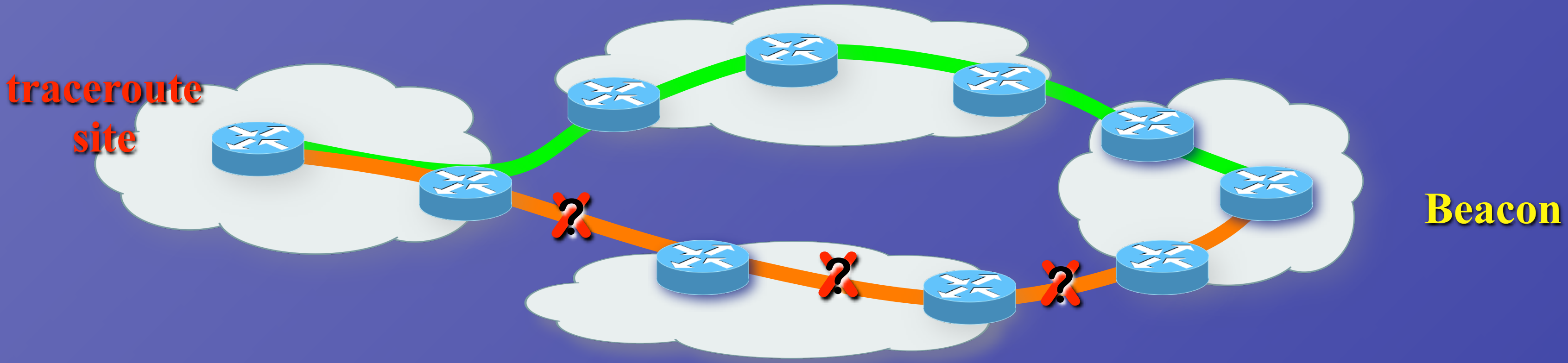
Bogon filter blocks path; BGP routes traffic around.



Well-established prefix, no filter. Compare path differences.

In-probes: Principles

- **In-probe** : traceroute performed from external IP addresses towards the test and anchor prefixes
- If traceroute towards test-prefix address diverges at some point, some bogon filter might be responsible



In-Probes: results

- Raw results:
  - 66.9% good (anchor and test take exactly same path)
  - 20.6% diverging (anchor/test use different paths)
  - 8.6% test stops, but anchor ok (bogon filter)
  - 3.9% failure (either anchor or anchor and test failed)

- Derive candidate links, eliminate unlikely candidates, then based on remaining candidate links:
  - ~ 34 ASs that may contain incorrectly configured filters

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

Conclusion

- We can identify regions in the Internet that do not have reachability
- It is possible to achieve a reasonable coverage of the Internet
- It does not only check reachability, it also detect places where there is "non-optimal" connectivity

Thanks To

- ARIN for IP space and commissioning research
- CityLink – NZ, a test site
- IIJ - JP, a test site
- SpaceNet - DE, a test site
- PSGnet – US, a test site
- Universities of Adelaide & Delft
- NSF award ANI-0221435
- Australian Research Council grant DP0557066