IP Alias Resolution with Prespecified Timestamps

Justine Sherry, Ethan Katz-Bassett, Mary Pimenova,
Harsha V. Madhyastha, Thomas Anderson, Arvind Krishnamurthy

Internet Measurement Conference 2010 | Melbourne, Australia

We Need Accurate Internet Toplogies

IP Geolocation

Performance comparisons of ISPs

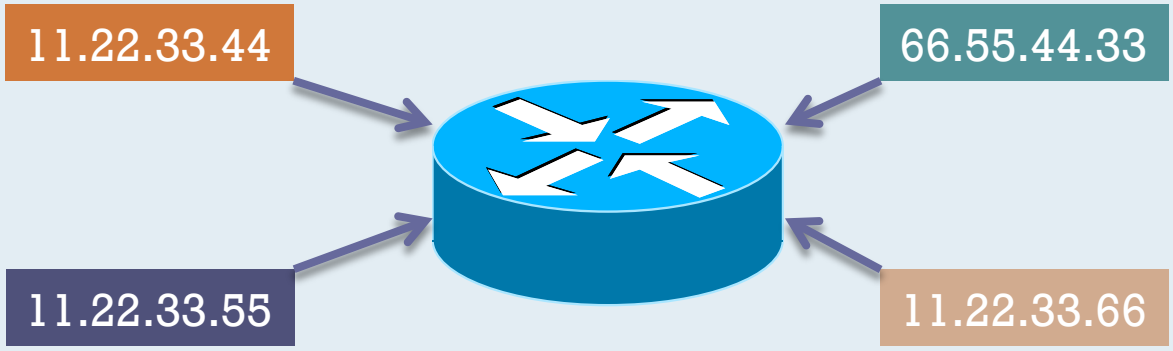
Pinpoint outages and failures

Latency estimates

Study structure and evolution of the Internet

IP Aliasing Problem

- We use IP addresses as identifiers for routers
- Routers may have dozens of IP addresses
- Multiple measurements of the same router may discover different IP addresses



Related Work

- Commonly used techniques:
  - RadarGun [Bender '08]/Ally [Spring '02]

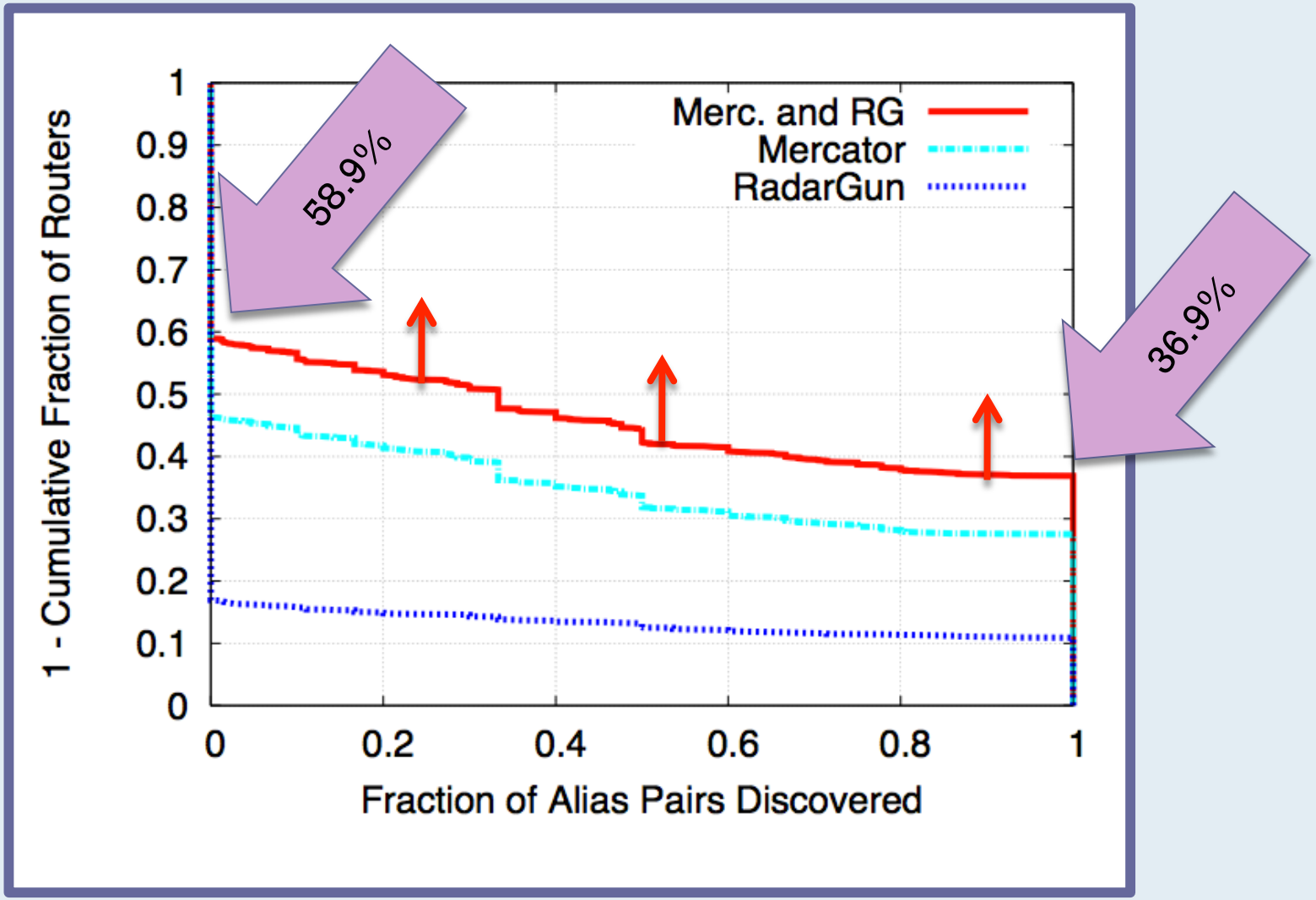
    Routers source packets from a single IPID counter; correlate IPID values from potential alias pairs.

  - Mercator [Govindan '00]

    Routers sometimes reply to UDP pings from a different address than the packet was sent to.

- Even in combination, techniques provide limited coverage.

Related Work



Our Alias Resolution Technique

We use the IP prespecified timestamp option to identify when multiple addresses belong to the same router.

Evaluation:

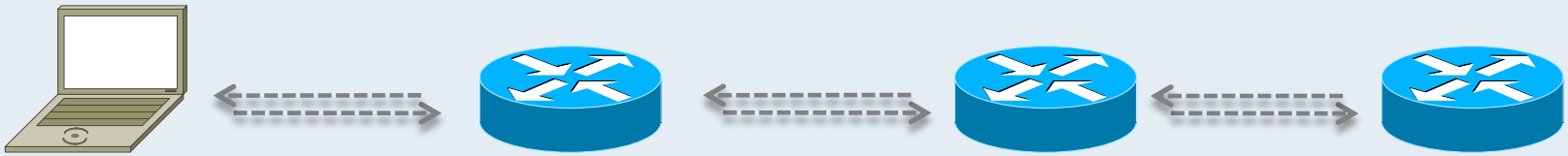
- Accurate: only 5.3% of aliases we discovered were false positives
- Complements existing techniques: 76.7% of aliases discovered were not discovered by other techniques

IP Prespecified Timestamps

- Sender lists up to four IP addresses in packet header
- Each router along the way checks if one of its own IP addresses is the first unstamped IP address
- If so, it inserts a timestamp into the header before forwarding the packet

Example

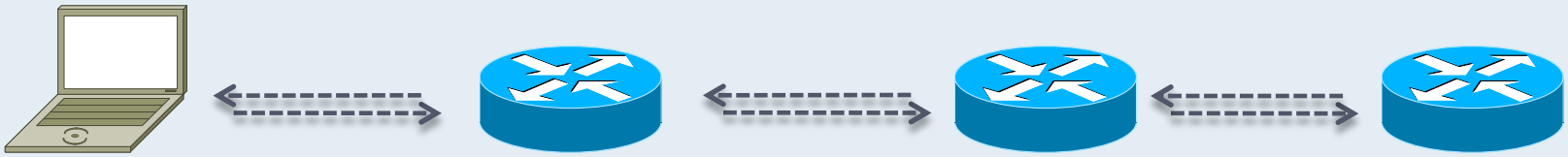
To: 11.22.33.44
From: Justine
Timestamps?
99.88.77.66 ?
11.22.33.44 ?
66.55.44.33 ?



Justine's Laptop | 99.88.77.66 | 66.55.44.33 | 11.22.33.44

Example

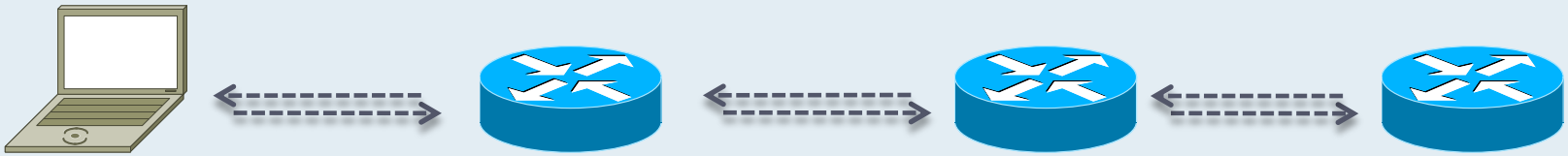
To: 11.22.33.44
From: Justine
Timestamps?
99.88.77.66 55
11.22.33.44 ?
66.55.44.33 ?



Justine's Laptop | 99.88.77.66 | 66.55.44.33 | 11.22.33.44

Example

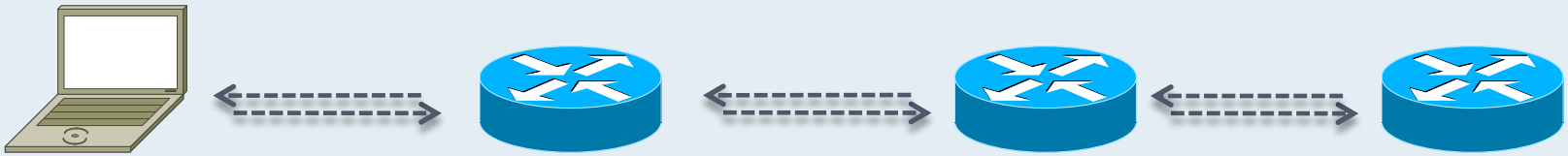
To: 11.22.33.44
From: Justine
Timestamps?
99.88.77.66 55
11.22.33.44 ?
66.55.44.33 ?



Justine's Laptop | 99.88.77.66 | 66.55.44.33 | 11.22.33.44

Example

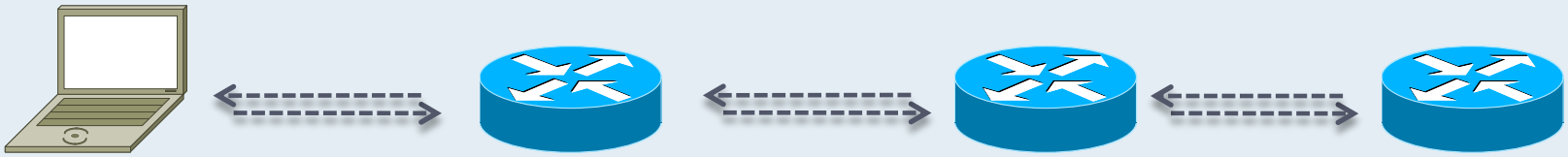
To: Justine
From: 11.22.33.44
Timestamps?
99.88.77.66 55
11.22.33.44 60
66.55.44.33 ?



Justine's Laptop | 99.88.77.66 | 66.55.44.33 | 11.22.33.44

Example

To: Justine
From: 11.22.33.44
Timestamps?
99.88.77.66 55
11.22.33.44 60
66.55.44.33 65



Justine's Laptop | 99.88.77.66 | 66.55.44.33 | 11.22.33.44

Insight: Request Multiple Timestamps from Same Router

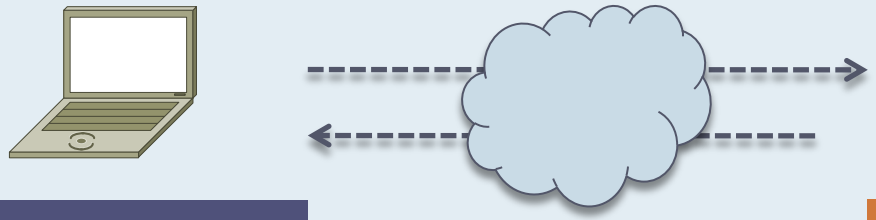
To: 11.22.33.44
From: Justine
Timestamps?
11.22.33.44 ?
44.33.22.11 ?
11.22.33.44 ?
44.33.22.11 ?

Justine's Laptop

11.22.33.44
44.33.22.11

Insight: Request Multiple Timestamps from Same Router

To: Justine
From: 11.22.33.44
Timestamps?
11.22.33.44 500
44.33.22.11 500
11.22.33.44 500
44.33.22.11 500

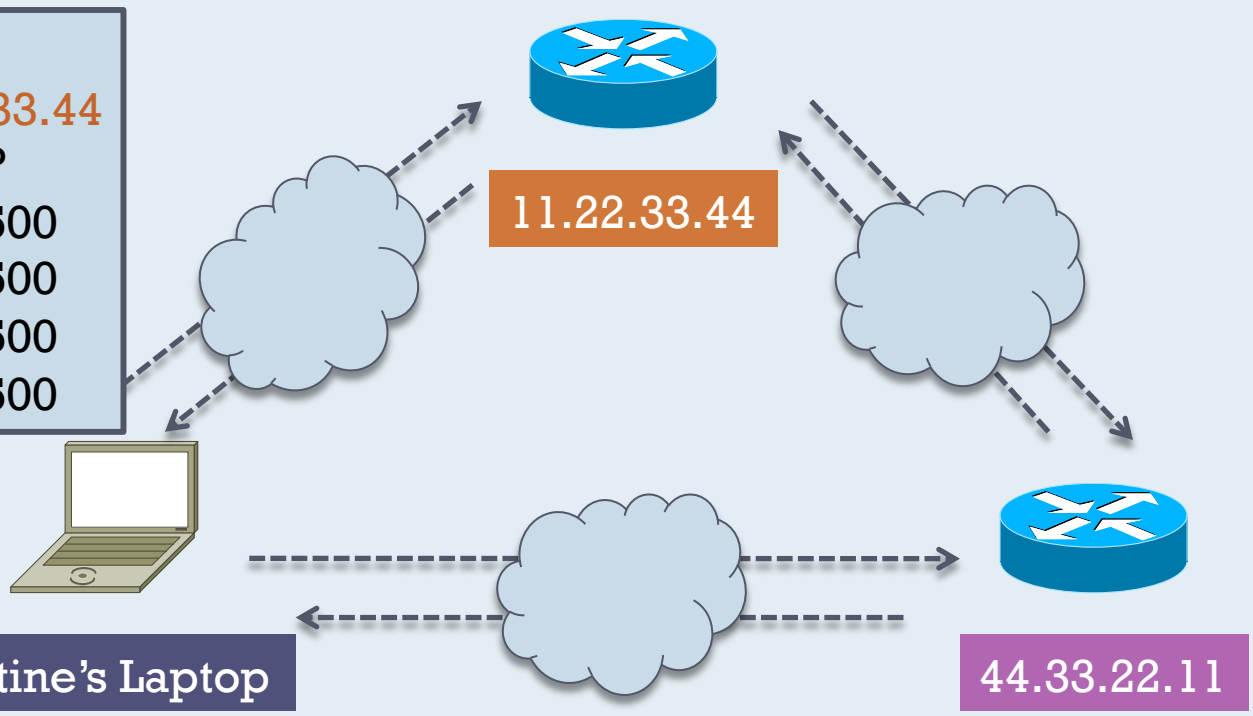


Justine's Laptop

11.22.33.44
44.33.22.11

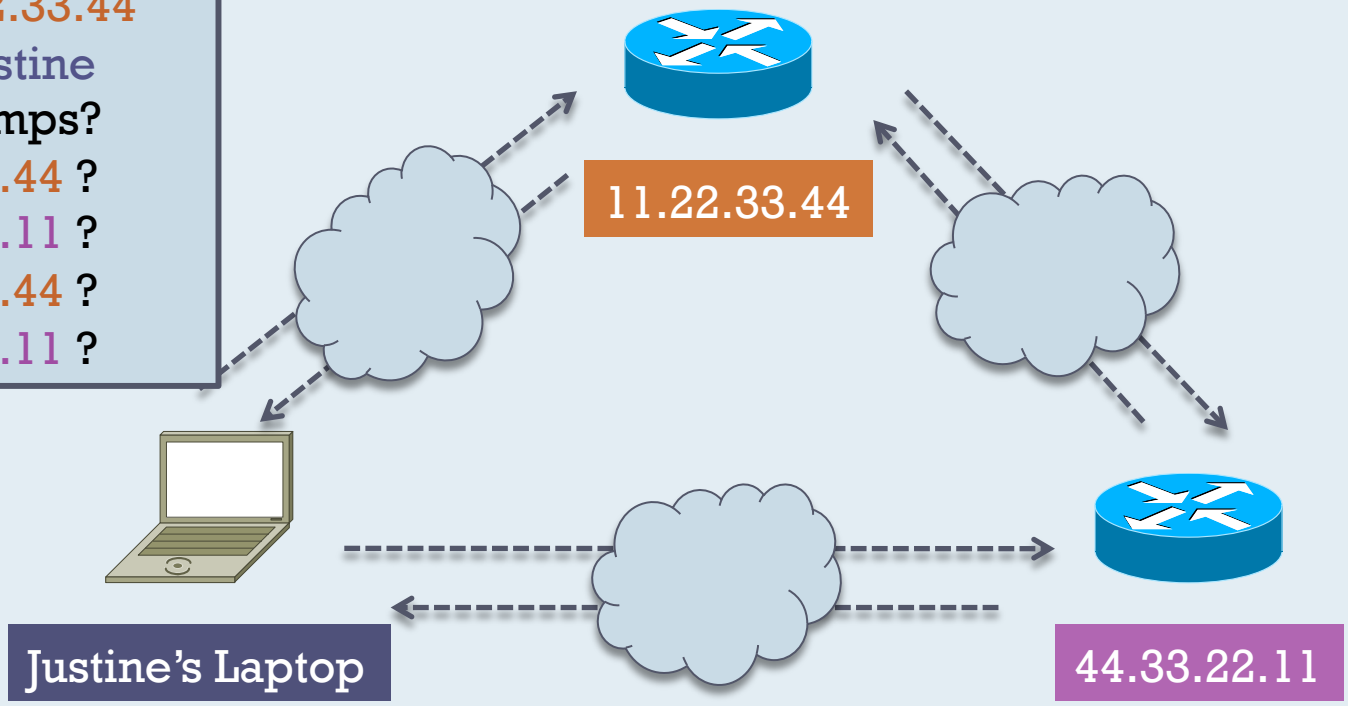
What if the response was generated by different routers?

To: Justine
From: 11.22.33.44
Timestamps?
11.22.33.44 500
44.33.22.11 500
11.22.33.44 500
44.33.22.11 500

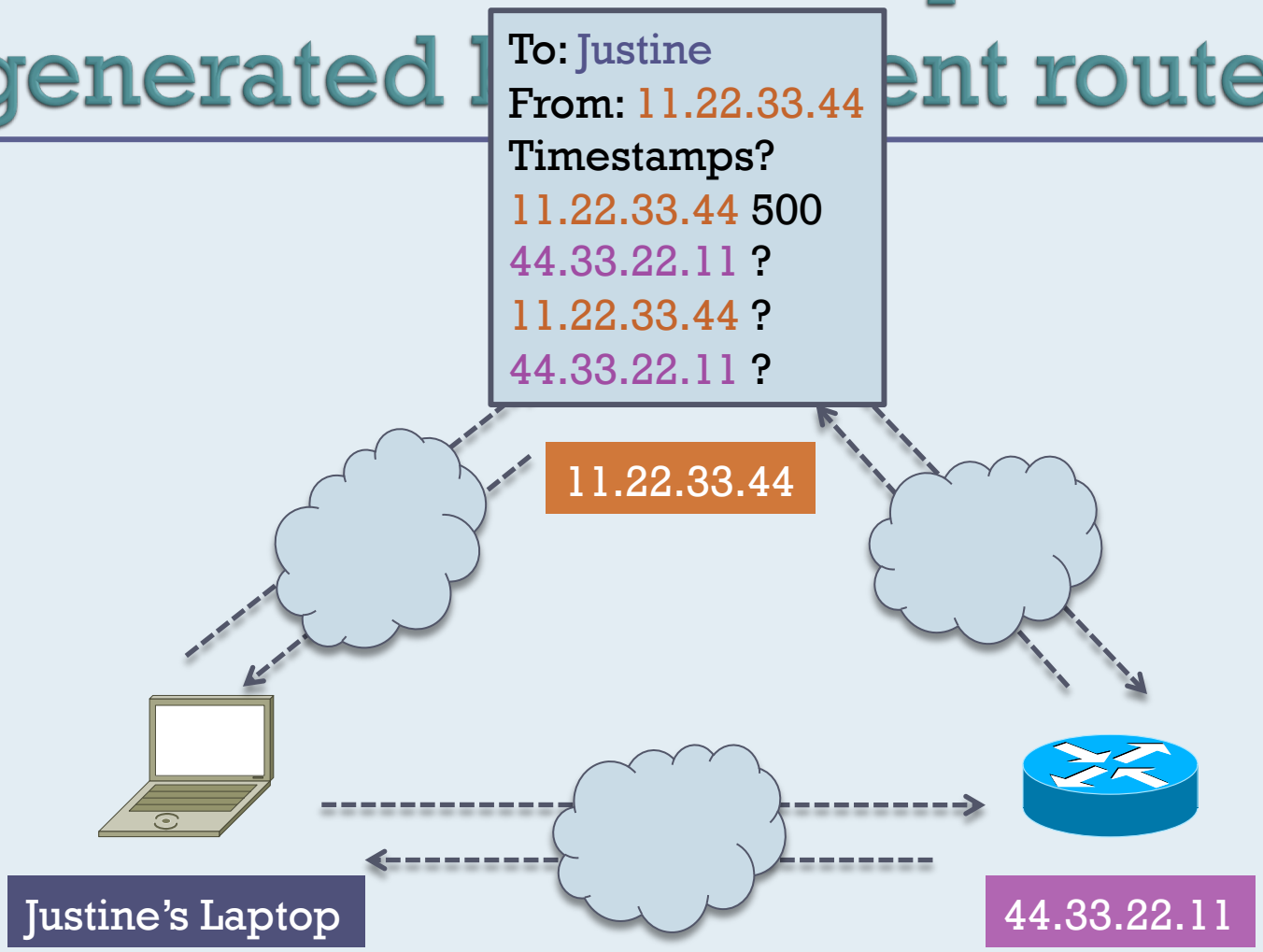


What if the response was generated by different routers?

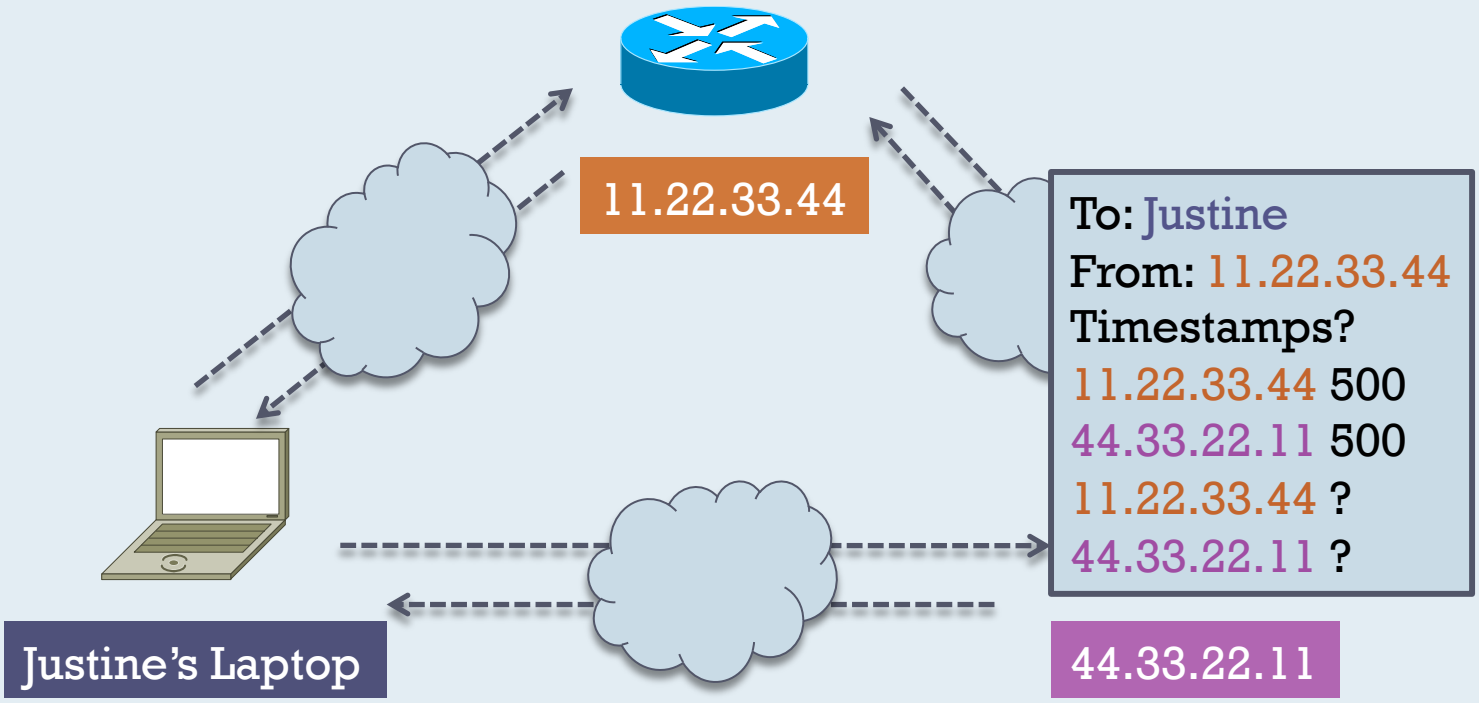
To: 11.22.33.44
From: Justine
Timestamps?
11.22.33.44 ?
44.33.22.11 ?
11.22.33.44 ?
44.33.22.11 ?



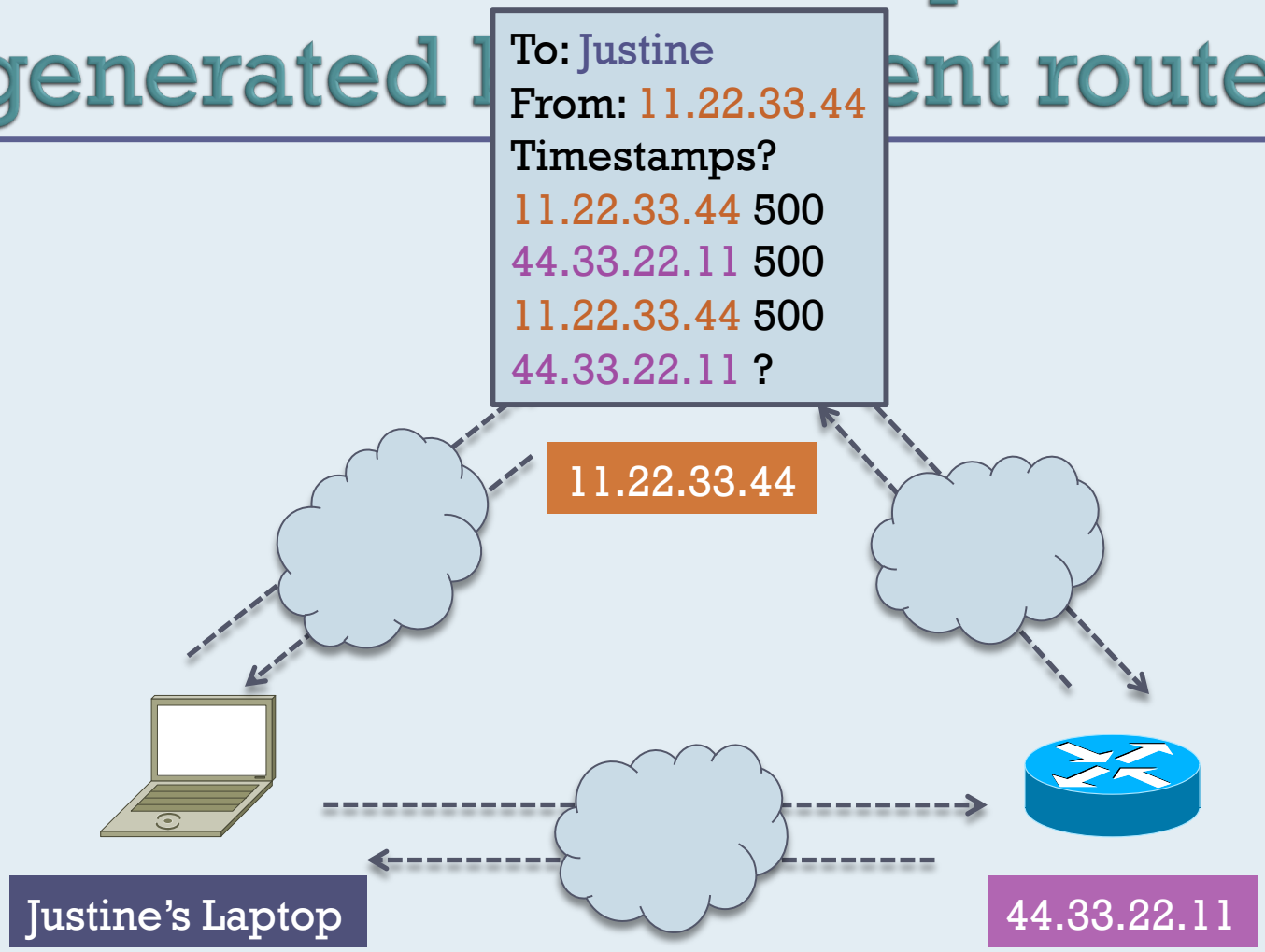
What if the response was generated by different routers?



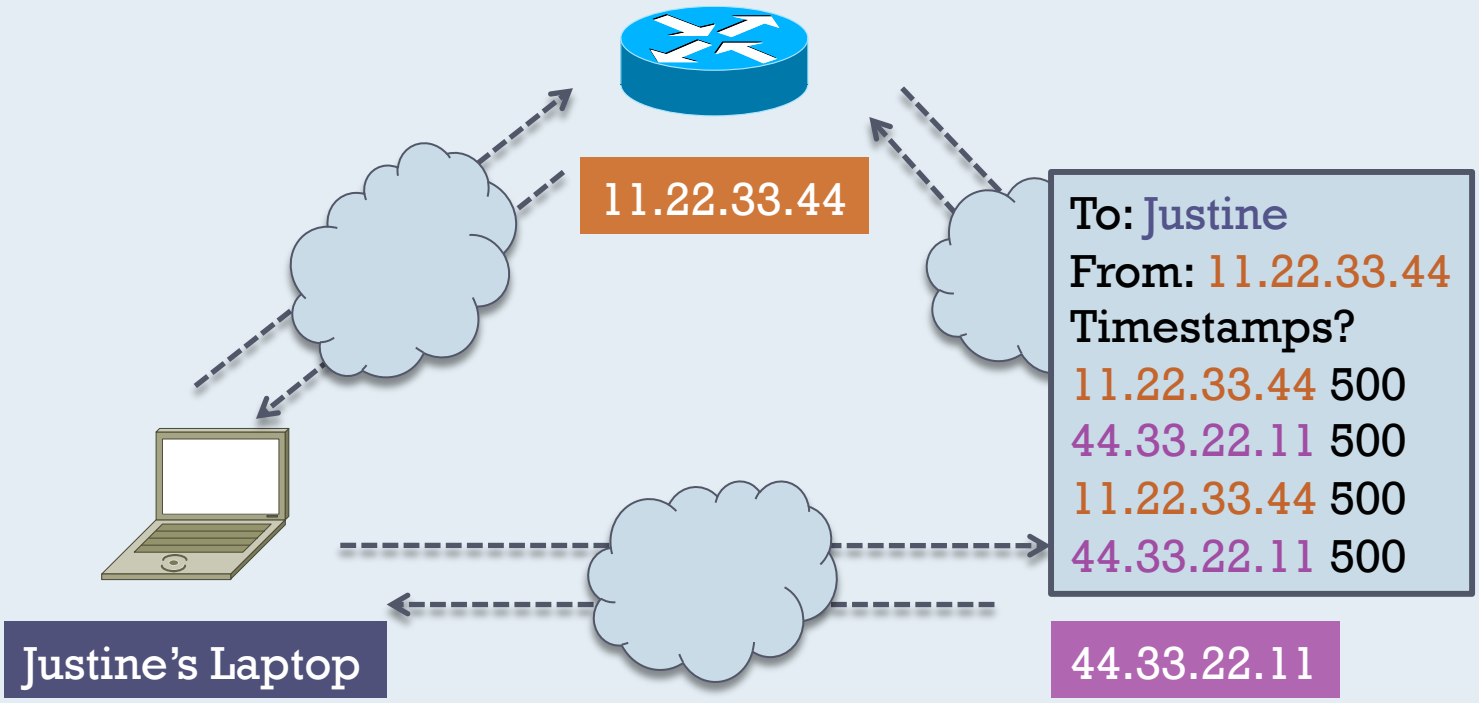
What if the response was generated by different routers?



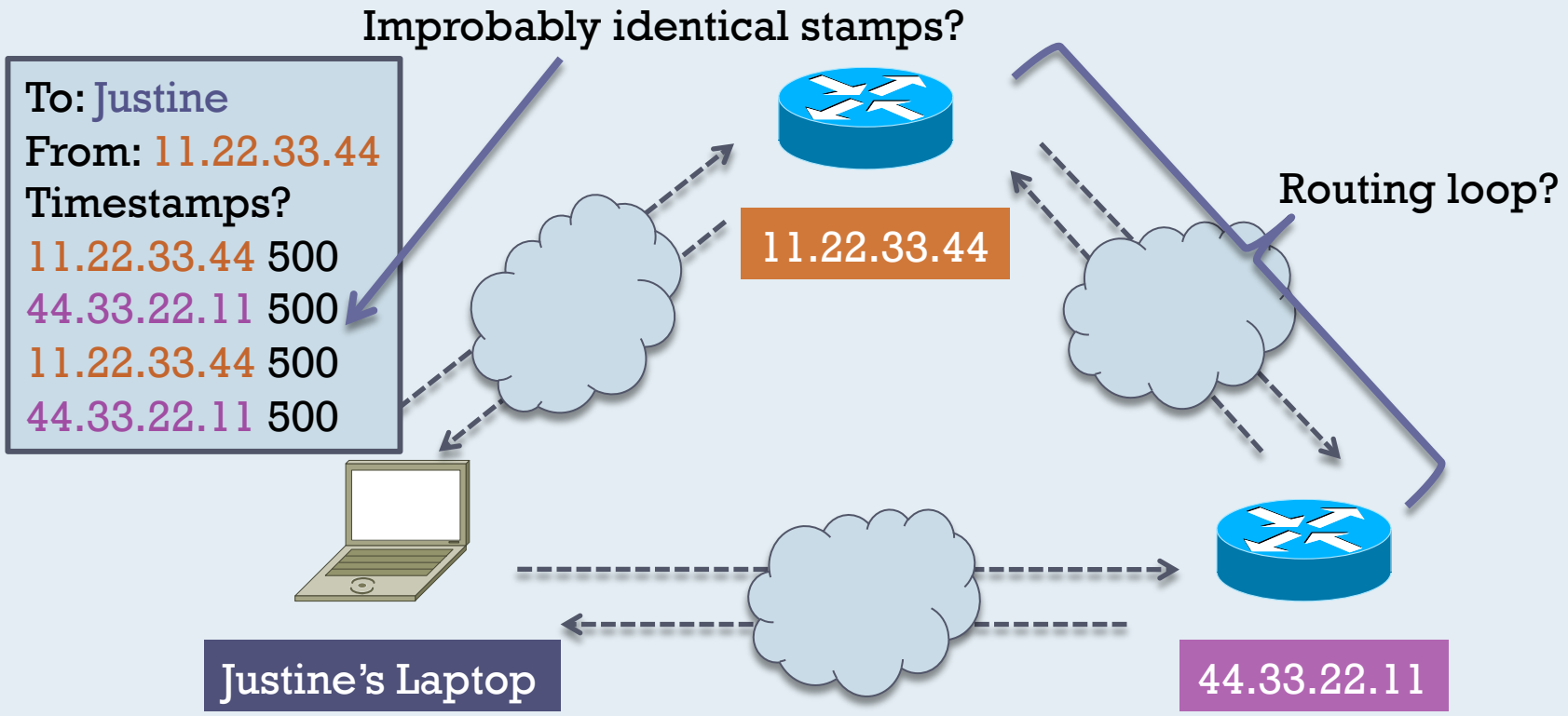
What if the response was generated by different routers?



What if the response was generated by different routers?



What if the response was generated by different routers?



Identifying IP Aliases

- 1: Generate candidate pairs
- 2: Craft packets which contain requests for both addresses of the candidate pair
- 3: Categorize results. Look for:
  - Multiple timestamps in the reply
  - All timestamps should match

To: Justine
From: 11.22.33.44
Timestamps?
11.22.33.44 500
44.33.22.11 500
11.22.33.44 500
44.33.22.11 500

Identifying IP Aliases

- Some machines provide unsolicited stamps.

  We can identify these routers and remove them.

- 10% of ping-responsive routers respond with four stamps, but a further 20% stamp with two.

  By performing multiple measurements and studying TTL values, we can also identify alias pairs for these.

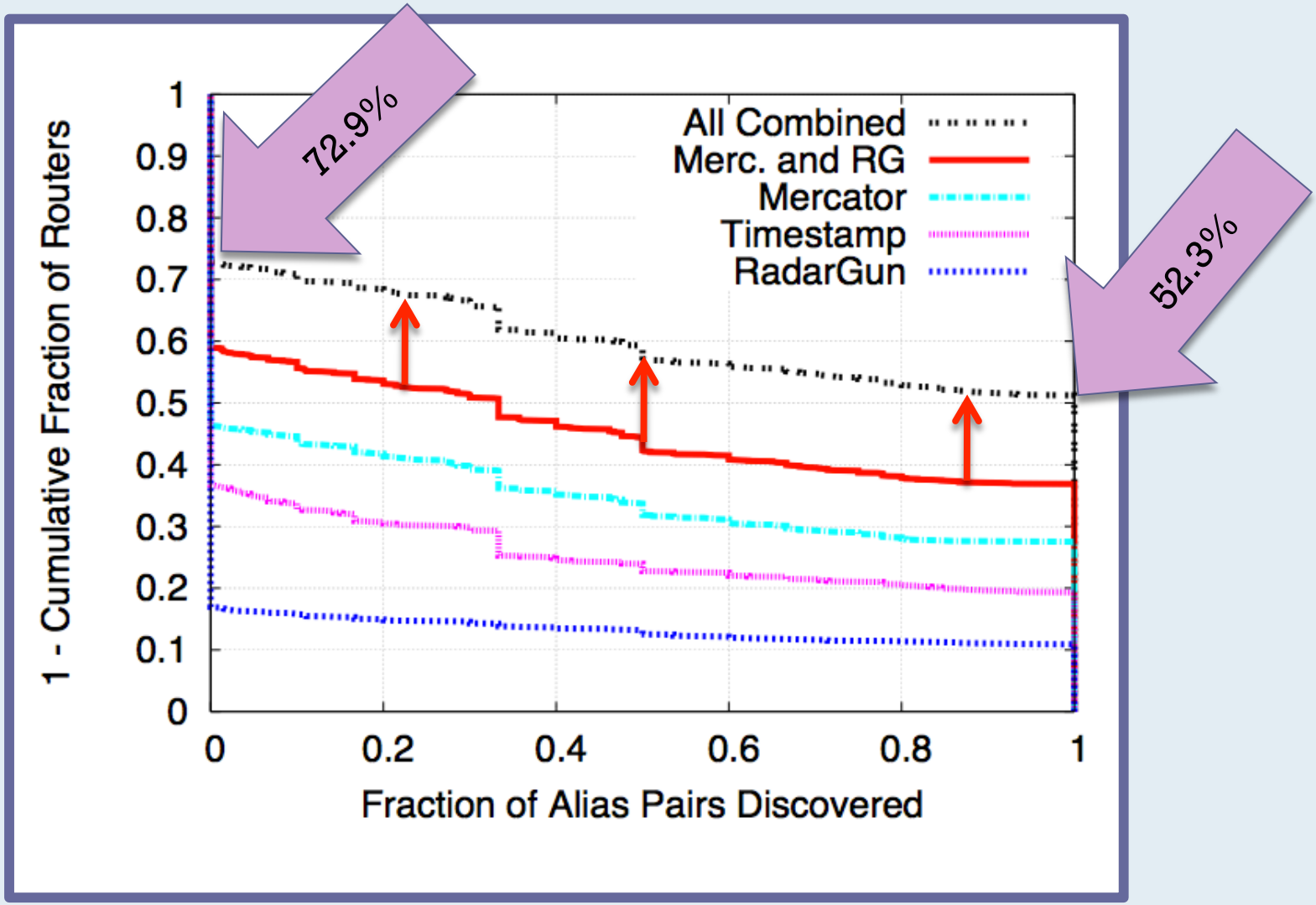
Evaluation: Experimental Setup

- Set of alias pairs discovered by mrinfo [Mérindol '09]
  - 9,130 addresses and 1,635 routers
- Provides complete list of aliases for each router
- Good approximation of ground truth
- We performed timestamp, Mercator, and Radargun techniques over all addresses

Evaluation: Results

- Accuracy: only 5.3% of the aliases we identified were false positives
- Coverage: 76.7% of the aliases we discovered using timestamp measurements were unidentified by other techniques

Evaluation: Coverage



Thank you!

We use the IP prespecified timestamp option to identify when multiple addresses belong to the same router.

- Accurate: few false positives
- Complements existing techniques: majority of timestamp-discovered aliases undiscovered by other techniques