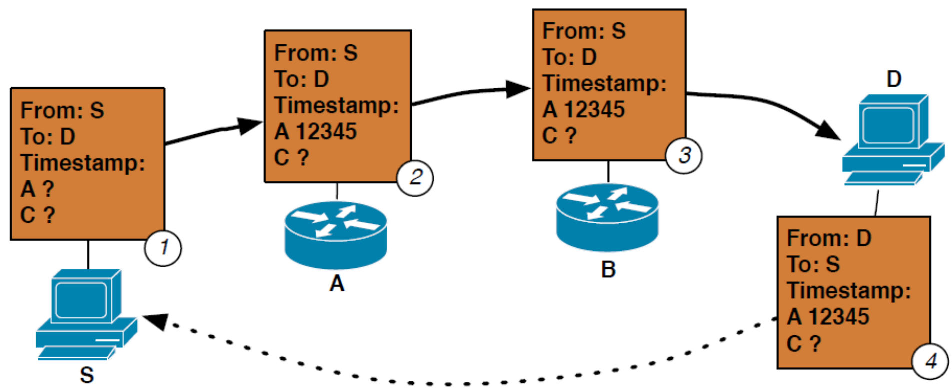
Internet Measurements with Prespecified Timestamps

Justine Sherry*, Mary Pimenova*, Ethan Katz-Bassett*,
Harsha V. Madhyastha†, Arvind Krishnamurthy*, Thomas Anderson*
*University of Washington, Seattle | †University of California, San Diego

Prespecified Timestamps are a well-supported but little-used IP option. We find that many routers respond to timestamp requests and we apply timestamp measurements to two challenges: resolving IP aliases and measuring link latencies. We find timestamps to be a valuable addition to our measurement toolkit.



Timestamps allow for a source to list up to four IP addresses in order. If a router recognizes its own IP address as the first unstamped address, it will provide a timestamp before forwarding.

Are routers responsive to timestamp requests?

- **56%** of 'pingable' addresses respond with timestamp values
- **17%** forward the packet without timestamps
- **27%** do not respond, possibly due to filters

Practical Timestamp Applications

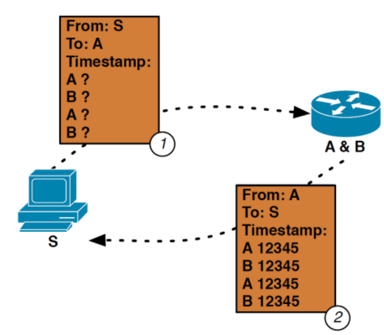
IP Alias Resolution

How do we identify when two IP addresses belong to the same router?

Why? IP aliases are necessary for route diagnosis and for generating accurate maps of Internet topologies.

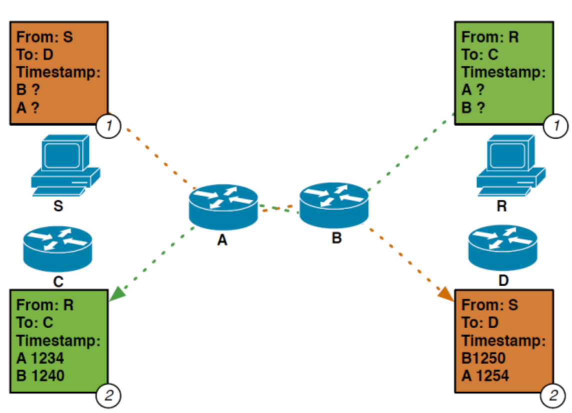
Solution: Combine timestamp requests for both addresses of a suspected alias pair (A,B) in a single probe.

Infer alias pairs from:
- Identical timestamp values (a shared clock)
- Implied looped forwarding between A and B



Link Latency

How long will it take a packet to traverse a single backbone link one way?



Why? Many applications, such as IP geolocation, depend on fine-grained latency values.

Solution: Send probes forward and reverse across the same link. Calculate delta by subtracting first timestamp from the second.

Δ_{BA} = link latency − skew(A,B)
Δ_{AB} = link latency + skew(A,B)
link latency = $(\Delta_{AB} + \Delta_{BA}) \div 2$