Reverse traceroute

Ethan Katz-Bassett, Harsha V. Madhyastha, Vijay Kumar Adhikari, Colin Scott, Justine Sherry, Peter van Wesep, Thomas Anderson, Arvind Krishnamurthy
UW-Seattle, UC-San Diego, University of Minnesota

Presenter: Andrew Weiner
1/28/2016

The one thing you should take away?
Motivation (Why we need reverse traceroute)

• Debugging path inflation ⭐
• Topology discovery
• Measuring one-way link latency ⭐
Motivation: Debugging path inflation
Motivation: One-way link latency

Assuming path symmetry, what is the one-way latency between hop 2 and hop 3?

<table>
<thead>
<tr>
<th>Traceroute</th>
<th>Time (ms)</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>123.0.0.1</td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>456.0.0.1</td>
</tr>
<tr>
<td>3</td>
<td>40</td>
<td>789.0.0.1</td>
</tr>
</tbody>
</table>

But if the return path is different, then this method gives a false result.

\[40 \text{ ms} - 20 \text{ ms}/2 = 10 \text{ ms}\]
How they do it

Suppose I am sitting at the source $S$ and I want to know the path from destination $D$ back to me.

I can also use PlanetLab sites to help (“Vantage Points”)
How they do it

(a) Vantage points traceroute to $S$, creating an atlas of known paths.

1) Run traceroutes from PlanetLab sites
How they do it

1) Run traceroutes from PlanetLab sites
2) Send ping from source S with record-route option (IP option type = 7). (Who knows the limitation?)

(b) Vantage points measure path from D until it intersects a path in the atlas.
How they do it

1) Run traceroutes from PlanetLab sites
2) Send ping from source S with Record Route option (IP option type = x07). (Who knows the limitation?)
3) Send pings from source S with Timestamp option (IP option type = x44). Ask for timestamp at D followed by guess $R_k$. 

(b) Vantage points measure path from D until it intersects a path in the atlas.
How they do it

1) Run traceroutes from PlanetLab sites
2) Send ping from source S with Record Route option (IP option type = x07). (Who knows the limitation?)
3) Send pings from source S with Timestamp option (IP option type = x44). Ask for timestamp at D followed by guess $R_k$.
4) Send Record Route ping from some V spoofing as S.

(b) Vantage points measure path from $D$ until it intersects a path in the atlas.
How they do it

1) Run traceroutes from PlanetLab sites
2) Send ping from source S with Record Route option (IP option type = x07). (Who knows the limitation?)
3) Send pings from source S with Timestamp option (IP option type = x44). Ask for timestamp at D followed by guess $R_k$.
4) Send Record Route ping from some V spoofing as S.
5) When all else fails, assume path symmetry.
Fig. 8 Testing against traceroutes from PlanetLab. Median sees 87% of hops.
How well it works

Fig. 9 Testing against traceroutes from traceroute servers. Median sees 75% of hops. 28% false positive.
How well it works

Sources of mismatch:
• Symmetry assumption (median 5% of hops)
• Router aliasing—many addresses for one router
• Exceptional handling of Record Route and Timestamp option packets
• Problems with traceroute!
The one thing you should take away?

Reverse traceroute exists, but it isn’t perfect.
http://revtr.cs.washington.edu/