On The Correlation between Route Dynamics and Routing Loops

Ashwin Sridharan and Sue. B. Moon
and Christophe Diot
Problem Statement

• Identify possible causes of routing loops within the Sprint backbone.
  – Methodology to correlate loops detected in traffic traces with routing events.
  – Any dominant cause(s) ?
  – Analyze impact of routing events on loop characteristics.
Talk Layout

• Routing Loops
  – Classification, causal sources.

• Methodology
  – Collection of data
  – Detection of loops and correlation with events.

• Analysis of data
  – Contribution of various protocols to loop creation.
  – Effectiveness of detection technique.
  – Effect of updates on path length distribution.

• Conclusions
Routing Loops

• Finite speed of propagation causes loops.
  – Routers change state in reaction to event.
  – After update, they broadcast new state.
  – Routing protocols have non-zero convergence time
  – BGP and ISIS routing protocols within Sprint.
• Can be classified based on cause/duration.
  – Transient: occur in normal state of operation.
  – Persistent: typically associable to anomalies.
An ISIS Loop
A BGP Loop

Customer changes preference to AS Y

Initially AS X preferred path
Methodology

- Collection of data.
  - Packet Traces.
  - Routing traces.
- Detection of packet loops in traces.
  - [Hengartner et al.]
- Correlation of packet loops with routing events.
  - Correlation with BGP events.
  - Correlation with ISIS events.
Collection of Data

- Collected OC-48 traces from 6 backbone links using Sprint IPMON equipment.
  - Dumps first 44 bytes from each packet.
  - Timestamps packet using GPS.
- BGP updates collected via Zebra BGP daemon peering with a BGP router.
- Pyrt ISIS routing daemon creates adjacency with an ISIS router and collects LSPs.
Detecting Packet Loops

Packet Stream →

Hash Buckets →

Differ only in TTL and Checksum

Packet Loops
Correlating packet loops and BGP Events

• Feed BGP updates to a Zebra router emulating the BGP decision process.
• For each BGP update
  – Determine changes in next-hop or AS Path for any loop.
  – If change in vicinity of loop origin, assume event responsible for loop.
Correlating packet loops and ISIS Events

- After each LSP is received, compute shortest path from observation node to all destinations.
- For each packet loop
  - Determine any change in forwarding path.
  - Determine if it overlaps with previous path.
  - If event in vicinity of loop, assume event was causal in the creation of the loop.
Analysis of Data

- Do both protocols cause routing loops?
  - All loops in traces associable only with BGP updates.
- Link state protocols have fast convergence time.
- Extensive use of multiple equal cost paths prevents overlap of ISIS forwarding path.
  - Monitored links were inter-POP links.
Analysis of Data – (2)

• How effective is the detection technique?
  – Affected by “distance” of source from observation point.
  – Updates related to events in other Ases may get filtered out.
# Matching Efficiency

<table>
<thead>
<tr>
<th>Trace</th>
<th>% Transient &amp; BGP Updates</th>
<th>% Persistent &amp; BGP Updates</th>
<th>% Persistent &amp; no Updates</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>NYC-20</td>
<td>40.1</td>
<td>0</td>
<td>50.8</td>
<td>90.8</td>
</tr>
<tr>
<td>NYC-21</td>
<td>80.2</td>
<td>0</td>
<td>7.5</td>
<td>87.9</td>
</tr>
<tr>
<td>NYC-22</td>
<td>18.8</td>
<td>0</td>
<td>80.6</td>
<td>99.4</td>
</tr>
<tr>
<td>NYC-23</td>
<td>3.3</td>
<td>0</td>
<td>0</td>
<td>3.3</td>
</tr>
<tr>
<td>NYC-24</td>
<td>70.0</td>
<td>0</td>
<td>0</td>
<td>70.0</td>
</tr>
<tr>
<td>NYC-25</td>
<td>43.7</td>
<td>15.5</td>
<td>0</td>
<td>59.2</td>
</tr>
</tbody>
</table>
# Average AS Path Length

<table>
<thead>
<tr>
<th>Trace</th>
<th>Avg. AS Path Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>NYC-20</td>
<td>1.34</td>
</tr>
<tr>
<td>NYC-21</td>
<td>1.04</td>
</tr>
<tr>
<td>NYC-22</td>
<td>0.51</td>
</tr>
<tr>
<td><strong>NYC-23</strong></td>
<td><strong>1.74</strong></td>
</tr>
<tr>
<td>NYC-24</td>
<td>1.61</td>
</tr>
<tr>
<td>NYC-25</td>
<td>1.63</td>
</tr>
</tbody>
</table>
Impact of BGP updates on loop length

- Path Length defined as the number of hops in a loop.
- Relationship between path length distribution and BGP updates.
  - If updates impacts large set of destinations, more likely that path length distribution has a higher variance.
Conclusions

- Methodology to correlate routing events with packet loops.
- BGP updates were almost exclusively responsible for routing loops.
- No loop creation event directly associable with ISIS.
  - Attributable to equal cost multiple paths.
- Correlation between BGP updates and path length distribution.