A Comparison of Syslog and IS-IS for Network Failure Analysis

Daniel Turner
Kirill Levchenko
Stefan Savage
Alex C. Snoeren
Network Reliability

- Networks component failure at scale is inevitable
Network Reliability

- Networks component failure at scale is inevitable
- Many mechanisms in place to keep customers from noticing
  - Redundant hardware & protocols
Network Reliability

- Networks component failure at scale is inevitable
- Many mechanisms in place to keep customers from noticing
  - Redundant hardware & protocols
- Evaluating reliability mechanisms requires data
Network Reliability Data

- Syslog has been popular for this role
  - Easy to obtain and utilize (open source & commercial tools)
  - [Gill Sigcomm11], [Mahimkar Sigcomm09], [Qiu IMC10], [Potharaju Sigmetrecs13], [Turner Sigcomm10]

- The gold standard is direct IGP routing messages capture
  - Fate sharing with network
  - Less widely used because its harder to obtain
Failure Example
Failure Example
Failure Example
Failure Example

Router x:
Interface 1/1
DOWN
Failure Example
Failure Example

IS-IS
Link State Packet

ID: Router 3
Time: 2/2/11 3:00PM
Current Neighbors:
  * Router 4 : weight 27
...
Data Usage

- How accurate is syslog, as compared to IS-IS, when used to capture and characterize failure?

- Different actors have different needs from the data
  - Details about root cause
  - Frequency and duration
  - Failure impact
Question 1: Can syslog be used as a drop in replacement for IS-IS data?

Question 2: For what purposes can syslog be used as a replacement for IS-IS data?

Question 3: If you are limited to only using syslog what can be done to improve its accuracy?
Data Collection

- **CENIC Network**
  - ISP to California educational institutions
  - 225+ routers
  - 299 Links
  - Thousands of miles of fiber
  - Millions of daily users

- **13 Months of data**
  - 11 Million IS-IS LSPs
  - 47,000 Syslog Messages
What is required to be a drop in replacement?
- State of the network as seen by both data sources is the same

We are focusing on link state (Up / Down)
- Function of state transitions

Do syslog’s state transitions mirror IS-IS’s?
- Straightforward to measure and compare
Examine State Transitions

<table>
<thead>
<tr>
<th>Transitions</th>
<th>Router Syslog Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>One</td>
</tr>
<tr>
<td>DOWN</td>
<td></td>
</tr>
<tr>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>
Examine State Transition

<table>
<thead>
<tr>
<th>Transitions</th>
<th>Router Syslog Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>One</td>
</tr>
<tr>
<td>DOWN</td>
<td>4,512 (39%)</td>
</tr>
<tr>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>
Exchanging State Transitions

<table>
<thead>
<tr>
<th>Transitions</th>
<th>Router Syslog Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>None</td>
</tr>
<tr>
<td>DOWN</td>
<td>2,022 (18%)</td>
</tr>
<tr>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>
Examine State Transitions

<table>
<thead>
<tr>
<th>Transitions</th>
<th>Router Syslog Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>None</td>
</tr>
<tr>
<td>DOWN</td>
<td>2,022 (18%)</td>
</tr>
<tr>
<td></td>
<td>4,962 (43%)</td>
</tr>
<tr>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>

18% is huge
Examining State Transitions

<table>
<thead>
<tr>
<th>Transitions</th>
<th>Router Syslog Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>None</td>
</tr>
<tr>
<td>DOWN</td>
<td>2,022 (18%)</td>
</tr>
<tr>
<td>UP</td>
<td>1,696 (15%)</td>
</tr>
</tbody>
</table>

18% is huge
What are the implications

- Syslog is not a drop in replacement for IS-IS data
  - Can’t do failure for failure accounting

- Question 2: For what purposes can syslog be used as a replacement for IS-IS data?

- Some people only need statistical similarity
  - Statistics are usually about failures not state changes
## Link Failures

<table>
<thead>
<tr>
<th></th>
<th>IS-IS</th>
<th>Syslog</th>
<th>Overlap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime (Hours)</td>
<td>3,648</td>
<td>2,714</td>
<td>2,331</td>
</tr>
<tr>
<td>Failure Count</td>
<td>11,213</td>
<td>11,738</td>
<td>9,298</td>
</tr>
</tbody>
</table>
### Link Failures

<table>
<thead>
<tr>
<th></th>
<th>IS-IS</th>
<th>Syslog</th>
<th>Overlap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime (Hours)</td>
<td>3,648</td>
<td>2,714</td>
<td>2,331</td>
</tr>
<tr>
<td>Failure Count</td>
<td>11,213</td>
<td>11,738</td>
<td>9,298</td>
</tr>
</tbody>
</table>

Missing 1k hours of downtime
### Link Failures

<table>
<thead>
<tr>
<th></th>
<th>IS-IS</th>
<th>Syslog</th>
<th>Overlap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime (Hours)</td>
<td>3,648</td>
<td>2,714</td>
<td>2,331</td>
</tr>
<tr>
<td>Failure Count</td>
<td>11,213</td>
<td>11,738</td>
<td>9,298</td>
</tr>
</tbody>
</table>

- 20% of syslog failures are false positives
- Missing 1k hours of downtime
What are the implications

- Not all statistics will match
  - But some could
- Statistical similarity measured w/ Komogorov-Smirnov test

<table>
<thead>
<tr>
<th></th>
<th>Backbone Links</th>
<th>Customer Access Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annualized Downtime per Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annualized Failures per Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure Duration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What are the implications

- Not all statistics will match
  - But some could
- Statistical similarity measured w/ Komogorov-Smirnov test

<table>
<thead>
<tr>
<th></th>
<th>Backbone Links</th>
<th>Customer Access Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annualized Downtime per Link</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Annualized Failures per Link</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Failure Duration</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
What are the implications

- Not all statistics will match
  - But some could

- Statistical similarity measured w/ Komogorov-Smirnov test

<table>
<thead>
<tr>
<th></th>
<th>Backbone Links</th>
<th>Customer Access Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annualized Downtime per Link</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Annualized Failures per Link</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Failure Duration</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Due to false positives and can be fixed
Question 3: If you are limited to only using syslog what can be done to improve its accuracy?

- Eliminate false positives
  - Mostly very short failures
- Remove ambiguous state transitions
  - 8% of link time is between to ambiguous transitions

How do we know this?

- We have access to both syslog and IS-IS data
Ambiguous State Transitions

Link State

0  1  2  3  4  5

Time

Syslog
Up
Down

Down

Up
Ambiguous State Transitions

Syslog Down
Syslog UP

Link State

Time
Ambiguous State Transitions

```
<table>
<thead>
<tr>
<th>Link State</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Syslog Down</td>
</tr>
<tr>
<td></td>
<td>Syslog UP</td>
</tr>
</tbody>
</table>

Time:
0 1 2 3 4 5

Down

Up

Syslog Down

Syslog UP
```
Ambiguous State Transitions

<table>
<thead>
<tr>
<th>Time</th>
<th>State</th>
<th>Link State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>Down</td>
</tr>
</tbody>
</table>

Time
Ambiguous State Transitions
Ambiguous State Transitions

Link State

Time

Up

Down

0 1 2 3 4 5
Ambiguous State Transitions

What happened?

Time

Up

Link State

Down

0 1 2 3 4 5

Time
Ambiguous State Transitions

What happened?
Message Lost

Up
Link State
Down

0 1 2 3 4 5
Time
Ambiguous State Transitions

- Time
  - 0
  - 1
  - 2
  - 3
  - 4
  - 5

- Link State
  - Up
  - Down

- What happened?
  - Message Lost
  - Spurious Message
Ambiguous State Transitions

Exclude time between 2 & 3
Ambiguous State Transitions

Link State

Up

Down

Time

0 1 2 3 4 5
Ambiguous State Transitions

<table>
<thead>
<tr>
<th>Time</th>
<th>Link State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Up</td>
</tr>
<tr>
<td>2</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>Down</td>
</tr>
<tr>
<td>4</td>
<td>Up (event)</td>
</tr>
<tr>
<td>5</td>
<td>Time</td>
</tr>
</tbody>
</table>
Ambiguous State Transitions

- Up
- Down

Time

Link State

- Same issue with double UPs
Correcting Ambiguous Transitions

- Strategies to best improve syslog’s fidelity
  - Always down? Always up?
  - Ignore the first? Ignore the second?
Correcting Ambiguous Transitions

- Strategies to best improve syslog’s fidelity
  - Always down? Always up?
  - Ignore the first? Ignore the second?

<table>
<thead>
<tr>
<th></th>
<th>DOWN</th>
<th>UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost Message</td>
<td>42%</td>
<td>86%</td>
</tr>
<tr>
<td>Spurious retransmit</td>
<td>52%</td>
<td>14%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Strategies to best improve syslog’s fidelity
- Always down? Always up?
- Ignore the first? Ignore the second?

Almost always multiple retransmits per failure

<table>
<thead>
<tr>
<th></th>
<th>DOWN</th>
<th>UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost Message</td>
<td>42%</td>
<td>86%</td>
</tr>
<tr>
<td>Spurious retransmit</td>
<td>52%</td>
<td>14%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Correcting Ambiguous Transitions

- Strategies to best improve syslog’s fidelity
  - Always down? Always up?
  - Ignore the first? Ignore the second?

- Optimal strategy: ignore the second message

<table>
<thead>
<tr>
<th></th>
<th>DOWN</th>
<th>UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost Message</td>
<td>42%</td>
<td>86%</td>
</tr>
<tr>
<td>Spurious retransmit</td>
<td>52%</td>
<td>14%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Conclusion

- Syslog not a drop in replacement for IGP data when studying failure
- Can be used to measure aggregate failure characteristics
  - Downtime & Failure counts
- Filtering can improve syslog’s fidelity
- When possible we recommend setting up an IGP listener