Cyclops: The AS-level Connectivity Observatory

Ricardo Oliveira, Ying-Ju Chi, Mohit Lad, Lixia Zhang
University of California, Los Angeles

Speaker: Ricardo Oliveira
rveloso@cs.ucla.edu
“Did AS9318 leak routes from Yahoo?”
@Nanog mailing list, July 8th 2007

“Did Cogent depeer Limelight, WV Fiber and nLayer?”
@Nanog mailing list, Sept 28th 2007

“Can anyone confirm a partition between Telia 1299 and Cogent 174?”
@Nanog mailing list, March 14th 2008
Need #1: AS connectivity

- Even though AS connectivity can be inferred from BGP updates collected from hundreds of vantage points - the public view (PV) …

- … there’s no tool to gather this info to infer the AS connectivity and changes
Need #2: fault detection

- Each ISP knows who its neighbors are: the ground truth

- Public view captures part of the ground truth and more...

**False link prefix hijack and misconfigurations**

- Y starts announcing a false link to Z w/ X’s prefix P

- In this case the link X-Y will appear in the PV
Cyclops concept

• Show 1-hop connectivity of specific AS at a time: eye of the cyclops
The 3 flavors of Cyclops

**Raw data:** raw connectivity data to be processed at ISP side

- 2153@CSUNET-NE - California State University Network@Transit-Unknown@Provider@42@2003-12-31@2008-03-13@1532@TABLE_DUMP|1205284560|B|134.55.200.1|293|128.97.0.0/16|293 2153 52|IGP

**Web interface:** quick way of getting list of neighbors and changes for a specific network

**Visualizer:** enables visual correlation of changes
Cyclops in a nutshell

• Comparison between PV and ground truth; contrast the observed connectivity with the intended connectivity

• Display changes-only view + snapshot view

• Search for anomalous (de)peering events

• Event correlation and root-cause inference
Cyclops architecture

- BGP data
- Topology & weight files
- Pre-processing
- AS relationship inference & AS classification
- Visualizer
- Web Interface
- Raw data
- Post-processing @ ISP side
- Alarm generation
  - weight
  - lifetime
  - PV-GT
  - ...
Cyclops raw data

• Available at [http://cyclops.cs.ucla.edu/rawdata](http://cyclops.cs.ucla.edu/rawdata)

• Last digit of ASN is the directory to look at, e.g. UCLA AS-52 is at [http://cyclops.cs.ucla.edu/rawdata/2/52.20080313](http://cyclops.cs.ucla.edu/rawdata/2/52.20080313)

• 2153@CSUNET-NE - California State University Network@Transit- Unknow@Provider@42@2003-12-31@2008-03-13@1532@TABLE_DUMP|1205284560|B|134.55.200.1|293|128.97.0.0/16|29 3 2153 52|IGP| |

• Known valid UCLA neighbors: AS2153 an AS2152
  – Everything else that appears connected to UCLA should trigger an alarm

• Easy to setup a script to periodically download these files and process them using filters to produce an alarm list
Web interface

• Allow users to have a quick view of the snapshot+connectivity

• Two modes:
  – “Change only”
  – “Connectivity”

• Allow filtering and sorting by relevant parameters
Web Interface

Cyclops: The AS-level Connectivity Observatory

Showing 3 links of AS 52 (on 2008-03-03)

<table>
<thead>
<tr>
<th>ASN</th>
<th>AS Name</th>
<th>Type</th>
<th>Relationship</th>
<th>Degree</th>
<th>Appearance Date</th>
<th>Disappearance Date</th>
<th>Lifetime</th>
<th>Weight</th>
<th>Last BGP Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11164</td>
<td>TRANSITRAIL - National LambdaRail, LLC</td>
<td>Transit-Unknown</td>
<td>Peer</td>
<td>126</td>
<td>2007-08-01 (104)</td>
<td>2007-12-14 (80)</td>
<td>104</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2152</td>
<td>CSUNET-NW - California State University Network</td>
<td>Transit-Unknown</td>
<td>Provider</td>
<td>111</td>
<td>2003-12-31 (1518)</td>
<td>2008-02-26 (6)</td>
<td>1518</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2153</td>
<td>CSUNET-NE - California State University Network</td>
<td>Transit-Unknown</td>
<td>Provider</td>
<td>42</td>
<td>2003-12-31 (1518)</td>
<td>2008-02-26 (6)</td>
<td>1518</td>
<td></td>
<td>192.154.2.0/24</td>
</tr>
</tbody>
</table>
Detecting anomalies

Suspicious ephemeral routes, most likely misconfigurations or malicious attacks
Detecting anomalies

Cyclops also keep tracking of number of routes in each link; possible to sort links by weight variation.
Visualizer Components

- **Main layout**

- Disappeared link/node
- New link/node
- Existing link/node

- Cyclops’ eye
- Expanded node

- stub
- transit
- tier-1

- Link thickness represents link weight (#prefixes, age)
- Transparency represents change confidence
Cyclops Visualizer

• **Event correlation:** enables visual correlation of events happening in different ASes

• **Activity plot:** help identify periods of "anomalous" number of AS connectivity changes

• **Time slider:** finer control over time window
Visualizer components

- **Activity graph**: makes it easier to spot abnormal events, e.g. massive depeerings
  - each bar represents changes aggregated over 1 week
  - top green bars represent new peerings; bottom red bars represent depeerings
  - Vertical scale can be set by the user
  - Grey slider allows to focus on period of interest
Visualizer Components

- **Time slider**: fine gain control of the observation time we’re interested; allows to move to next/previous change
Visualizer components

• **Visualization modes:**
  - “Only changes” display only the changes in the relevant time period; changes can be filtered by confidence [sigcomm'07]
  - “Connectivity” displays the topology snapshot at a given time

• **Other options:**
  - filters by type of AS and degree
  - configure link labels and thickness, e.g. #routes, age
Case study #1: Google’s route leakage

Activity plot helps spot anomalous changes

July 19, 2006
Case #2: Yahoo’s outage

After studying Yahoo’s connectivity, we noticed a transient peering with AS9318

July 6, 2007
Case #2: Yahoo’s outage

AS 9318’s route leakage caused Yahoo’s outage

July 6, 2007

http://isc.sans.org/diary.html?storyid=3112
Case#3 Cogent depeerings (9/15 – 29)

“Did Cogent depeer Limelight, WV FIBER, and nLayer?”
@Nanog mailing list, Sept 28th 2007
Case#3 Cogent depeerings (9/15 – 29)

Apparently nLayer not depeered…
Future work: Cyclops’ alarms

- Idea is to allow ISPs to register for alarms; examples of alarms are:
  - Large shifts in number of routes/link
  - Links with very short lifetime
  - Differences between PV-GT (ground truth)

- Feature under development, would like to hear ISP ideas about this; who would like to sign up for these alarms?
Req Feedback

- We encourage everybody to try it out (the server can be down if all try at same time;))

  http://cyclops.cs.ucla.edu

- What would you like to change in Cyclops?
- What new functionality you would like to see?
- Did it help diagnosing some problem in your network? Let us know!
- And please report any data inconsistency
More resources

• AS-level connectivity raw data
  http://cyclops.cs.ucla.edu/rawdata

• Cyclops mailing list:
  http://www.cs.ucla.edu/mailman/listinfo/cyclops

• IRL topology page
  http://irl.cs.ucla.edu/topology
Send all questions and comments to
cyclops@lists.cs.ucla.edu
Thanks!