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|
The 3 flavors of Cyclops

**Web interface:** quick way of getting list of neighbors and changes for a specific network
The 3 flavors of Cyclops

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

- **Fault detection**: BGP misconfigurations, false link attacks, route leakages

- Provide AS **topology snapshot** and changes-only view

- Detection of **anomalous** (de)peering events

- **Event correlation** and root-cause inference
Cyclops architecture

Pre-processing
- BGP data

Topology & weight files

Cyclops DB
- AS relationship inference & AS classification

Visualizer
- Web Interface
- Raw data

Post-processing @ ISP side
- Alarm generation
  - weight
  - lifetime
  - PV-GT
  ...

Updating Cyclops DB

- Currently done in a **daily basis**; creates some delay in detection and reaction time

- Plan to move it to **real time** using BGPmon tool from CSU:
  http://bgpmon.netsec.colostate.edu/
Cyclops raw data

• Available at 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

• 2153@CSUNET-NE - California State University Network@Large ISP@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

The AS-level Connectivity Observatory

Cyclops: The AS-level Connectivity Observatory

Showing 24 links of AS 174 (from 2008-05-21 to 2008-05-28)

<table>
<thead>
<tr>
<th>ASN</th>
<th>AS Name</th>
<th>Type</th>
<th>Reltn.</th>
<th>Deg.</th>
<th>First App.</th>
<th>Disapp. Date</th>
<th>Age</th>
<th>Weight (From)</th>
<th>Weight (To)</th>
<th>Last BGP Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>6677</td>
<td>ICNET-AS1 ICNET Autonomous system</td>
<td>small ISP(13) Peer</td>
<td>103</td>
<td>2007-04-05</td>
<td>2008-05-27 (1)</td>
<td>418</td>
<td>0.31</td>
<td>0.31</td>
<td>91.203.35.0/24</td>
<td></td>
</tr>
<tr>
<td>5557</td>
<td>BUSINESSERVE Business Serve plc</td>
<td>small ISP(11) Provider</td>
<td>53</td>
<td>2004-03-05</td>
<td>2008-05-22 (3)</td>
<td>1500</td>
<td>0.99</td>
<td>0.99</td>
<td>217.77.176.0/20</td>
<td></td>
</tr>
<tr>
<td>24937</td>
<td>MNET mnet Internet Limited</td>
<td>small ISP(41) Provider</td>
<td>31</td>
<td>2005-10-21</td>
<td>2008-05-25 (3)</td>
<td>947</td>
<td>0.98</td>
<td>0.98</td>
<td>212.113.27.0/24</td>
<td></td>
</tr>
<tr>
<td>32523</td>
<td>INFOSTREET - infoStreet, Inc.</td>
<td>Provider</td>
<td>16</td>
<td>2005-03-29</td>
<td>2008-05-23 (5)</td>
<td>1151</td>
<td>0.67</td>
<td>0.67</td>
<td>205.62.140.0/22</td>
<td></td>
</tr>
<tr>
<td>21547</td>
<td>REVNETS - Revolution Networks</td>
<td>small ISP(50) Unknown</td>
<td>14</td>
<td>2008-05-22</td>
<td>2008-05-22 (6)</td>
<td>0</td>
<td>8.13</td>
<td>-1.24</td>
<td>205.245.0.0/24</td>
<td></td>
</tr>
<tr>
<td>16085</td>
<td>AS16085 Easynet AS</td>
<td>Sub(2) Provider</td>
<td>11</td>
<td>2007-11-15</td>
<td>2008-05-22 (6)</td>
<td>180</td>
<td>217.77.32.0/20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24933</td>
<td>MINXS-AS MINXS</td>
<td>Sub(0) Peer</td>
<td>8</td>
<td>2005-07-04</td>
<td>2008-05-27 (1)</td>
<td>1058</td>
<td>0.06</td>
<td>0.06</td>
<td>193.110.153.0/24</td>
<td></td>
</tr>
<tr>
<td>12826</td>
<td>AS12826 C-SI Autonomous System</td>
<td>Sub(0) Unknown</td>
<td>6</td>
<td>2008-05-22</td>
<td>2008-05-27 (1)</td>
<td>3.52</td>
<td>0.11</td>
<td>212.234.178.0/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19557</td>
<td>CHANGEIP-01 - CHANGEIP COM</td>
<td>Sub(0) Provider</td>
<td>4</td>
<td>2005-10-23</td>
<td>2008-05-27 (1)</td>
<td>947</td>
<td>3.18</td>
<td>3.18</td>
<td>204.16.198.0/22</td>
<td></td>
</tr>
<tr>
<td>23073</td>
<td>BigZoo-001 - Big Zoo.com</td>
<td>Sub(1) Provider</td>
<td>3</td>
<td>2007-03-10</td>
<td>2008-05-23 (5)</td>
<td>431</td>
<td>3.5</td>
<td>3.5</td>
<td>208.73.232.0/21</td>
<td></td>
</tr>
<tr>
<td>25187</td>
<td>FCV FRANCE CITEVISION</td>
<td>Sub(0) Provider</td>
<td>3</td>
<td>2004-05-17</td>
<td>2008-05-27 (1)</td>
<td>1471</td>
<td>0.45</td>
<td>0.45</td>
<td>213.151.180.0/19</td>
<td></td>
</tr>
<tr>
<td>27491</td>
<td>NATIONAL FINANCIAL PARTNERS-CORP</td>
<td>Sub(0) Provider</td>
<td>3</td>
<td>2008-09-09</td>
<td>2008-05-26 (1)</td>
<td>825</td>
<td>0.63</td>
<td>0.63</td>
<td>38.68.87.0/24</td>
<td></td>
</tr>
</tbody>
</table>
Detecting anomalies

<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>1668</td>
<td>AOL-ATDN - AOL Transit Data Network</td>
<td>Transit-Tier1</td>
<td>Unknown</td>
<td>108</td>
<td>2008-01-29 (0)</td>
<td>2008-01-29 (43)</td>
<td>0</td>
<td>64.236.38.0/24</td>
<td></td>
</tr>
<tr>
<td>35456</td>
<td>FUBRA-AS Fubra Limited</td>
<td>Stub-Unknown</td>
<td>Unknown</td>
<td>37</td>
<td>2008-03-11 (0)</td>
<td>2008-03-11 (1)</td>
<td>0</td>
<td>87.124.0.0/17</td>
<td></td>
</tr>
<tr>
<td>3595</td>
<td>GNAXNET-AS - Global Net Access, LLC</td>
<td>Transit-Unknown</td>
<td>Unknown</td>
<td>19</td>
<td>2008-01-29 (0)</td>
<td>2008-01-29 (43)</td>
<td>0</td>
<td>63.247.71.0/24</td>
<td></td>
</tr>
<tr>
<td>10994</td>
<td>TAMPA2-TWC-5 - Road Runner HotCo LLC</td>
<td>Transit-Unknown</td>
<td>Unknown</td>
<td>10</td>
<td>2008-03-05 (0)</td>
<td>2008-03-05 (7)</td>
<td>0</td>
<td>71.40.126.0/18</td>
<td></td>
</tr>
<tr>
<td>3360</td>
<td>CSC-ASN - Computer Sciences Corporation</td>
<td>Transit-Unknown</td>
<td>Unknown</td>
<td>5</td>
<td>2008-01-29 (0)</td>
<td>2008-01-29 (43)</td>
<td>0</td>
<td>62.248.116.0/24</td>
<td></td>
</tr>
<tr>
<td>23664</td>
<td>WIPT-TECH-AS-AP Wipro Technologies</td>
<td>Stub-Unknown</td>
<td>Unknown</td>
<td>2</td>
<td>2008-01-10 (0)</td>
<td>2008-01-10 (62)</td>
<td>0</td>
<td>203.91.192.0/22</td>
<td></td>
</tr>
<tr>
<td>39122</td>
<td>BLACKNIGHT-AS Blacknight Internet Solutions Ltd</td>
<td>Stub-Unknown</td>
<td>Unknown</td>
<td>10</td>
<td>2008-02-25 (1)</td>
<td>2008-02-28 (15)</td>
<td>1</td>
<td>78.153.192.0/19</td>
<td></td>
</tr>
<tr>
<td>41695</td>
<td>VOSTRON-AS Vostron Ltd</td>
<td>Stub-Unknown</td>
<td>Unknown</td>
<td>3</td>
<td>2008-03-10 (1)</td>
<td>2008-03-11 (1)</td>
<td>1</td>
<td>89.21.224.0/19</td>
<td></td>
</tr>
<tr>
<td>43889</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>1</td>
<td>2008-03-04 (1)</td>
<td>2008-03-05 (7)</td>
<td>1</td>
<td>79.170.216.0/21</td>
<td></td>
</tr>
<tr>
<td>11160</td>
<td>COSTAR-SANDEGO - COSTAR GROUP</td>
<td>Stub-Unknown</td>
<td>Unknown</td>
<td>3</td>
<td>2008-03-09 (2)</td>
<td>2008-03-11 (1)</td>
<td>2</td>
<td>204.253.48.0/24</td>
<td></td>
</tr>
<tr>
<td>40695</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>1</td>
<td>2008-03-07 (4)</td>
<td>2008-03-11 (1)</td>
<td>4</td>
<td>38.103.1.0/24</td>
<td></td>
</tr>
<tr>
<td>19332</td>
<td>Marcatel</td>
<td>Transit-Unknown</td>
<td>Unknown</td>
<td>10</td>
<td>2008-03-06 (5)</td>
<td>2008-03-11 (1)</td>
<td>5</td>
<td>148.243.52.0/24</td>
<td></td>
</tr>
</tbody>
</table>

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
Cyclops Visualizer

- Dead AS
- Peerings lost (depeering)
- New peerings
- New AS
- Time slider
- Activity Plot
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

No. of changes

![Chart showing activity changes with green and red bars representing new peerings and depeerings respectively. The vertical scale is adjustable by a grey slider.](image)
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
Case #2: Yahoo’s outage

AS 9318’s route leakage caused Yahoo’s outage

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!