AS Core: Visualizing the Internet

CAIDA
SDSC/UCSD

CSE 91
4 March 2011
• overview
• data sources
• data processing
• visualization breakdown
• IPv4 vs IPv6
• summary
Provide a visual representation of the AS level Internet.
Autonomous System (AS)
an entity in the routing system
that announces and provides connectivity to
networks through a global routing protocol.
Each AS is roughly a company or network operator. UCSD has several. Some companies use multiple ASes (M&As), so not one-to-one.

On the graph: A single node is a single AS, although nodes with the same coordinate values will overlap.
what we need to draw a node

- AS’s name
- AS’s longitude
- AS’s neighbors
- AS’s degree (# neighbors)
how we get the data

Internet

CAIDA

ark

ark traces

ARK Collector

BGP Activity

AS Info process

Prefix -> AS

Regional Internet Registries

whois server

whois dumps

RIPE NCC Routeviews

BGP Collectors

BGP dumps

Prefix -> AS process

Netacuity server

Digital Envoy

AS Core process

AS Info Names Geo Location

Regional Internet Registries

whois server

whois dumps

Symbol key

Data collectors

Data processes

Data files
• **Archipelago (ark)**
  - platform that continually collects traceroute (topology) measurements

• **BGP collectors**
  - collects inter-domain (Border Gateway Protocol) routing tables and updates

• **Netacuity**
  - database of IP address geographic locations

• **WHOIS**
  - database(S) of registered users or assignees of Internet resources
Archipelago (ark)

- CAIDA’s active measurement infrastructure
- 43 monitors - growing 1 or 2 per month
- 11 w/IPv6 connectivity
- Team-probing collecting IPv4 and IPv6 topology
- http://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml

traceroute/topology data (not what is collected, but similar)

<table>
<thead>
<tr>
<th>hop</th>
<th>hostname</th>
<th>IP address</th>
<th>Round Trip Time (RTT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>pinot-g1-0-0 (192.172.226.1)</td>
<td>0.856 ms 0.334 ms 0.374 ms</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>dolphin.sdsc.edu (198.17.46.17)</td>
<td>0.888 ms 0.461 ms 0.452 ms</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>dc-sdg-agg1--sdsc-1.cenic.net (137.164.23.129)</td>
<td>0.495 ms 0.486 ms 0.463 ms</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>dc-riv-core1--sdg-agg1-10ge.cenic.net (137.164.47.111)</td>
<td>3.462 ms 3.364 ms 3.215 ms</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>dc-lax-core1--riv-core1-10ge-2.cenic.net (137.164.46.57)</td>
<td>4.774 ms 4.815 ms 5.515 ms</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>dc-lax-peer1--lax-core1-ge.cenic.net (137.164.46.116)</td>
<td>12.970 ms 4.619 ms 4.560 ms</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>gi1-1--46.tr01-lsanca01.transitrail.net (137.164.131.245)</td>
<td>4.664 ms 4.655 ms 4.849 ms</td>
<td></td>
</tr>
</tbody>
</table>
An ark monitor sends packets toward a destination IP address with small Time To Live (TTL) values. Each router decrements the TTL. When it reaches zero it discards the packet and sends a notification back to the source monitor. Chaining these responses together suggests a likely forward path.

<table>
<thead>
<tr>
<th>Trace</th>
<th>Hop 1</th>
<th>Hop 2</th>
<th>Hop 3</th>
<th>Hop 4</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace 1</td>
<td>13.5.1.8</td>
<td>5.5.1.28</td>
<td></td>
<td></td>
<td>5.5.1.28</td>
</tr>
<tr>
<td>Trace 2</td>
<td>13.5.1.8</td>
<td>10.0.1.5</td>
<td>10.0.2.3</td>
<td></td>
<td>10.0.2.3</td>
</tr>
<tr>
<td>Trace 3</td>
<td>13.5.1.8</td>
<td>10.0.1.5</td>
<td>10.0.1.1</td>
<td>9.0.1.1</td>
<td>9.0.1.1</td>
</tr>
</tbody>
</table>
Collecting and sharing global routing [Border Gateway Protocol (BGP)] data:

- University of Oregon
  - 6 collectors
  - http://www.routeviews.org

- RIPE NCC (Regional Internet Registry for Europe/Middle East)
  - 13 collectors

- used to map IP addresses to ASes

### BGP dump

<table>
<thead>
<tr>
<th>source IP</th>
<th>source AS</th>
<th>prefix</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE_DUMP2</td>
<td>127 1 649600</td>
<td>B</td>
<td>157.130.10.233</td>
</tr>
<tr>
<td>TABLE_DUMP2</td>
<td>127 1 649600</td>
<td>B</td>
<td>203.62.252.186</td>
</tr>
<tr>
<td>TABLE_DUMP2</td>
<td>127 1 649600</td>
<td>B</td>
<td>12.0.1.63</td>
</tr>
</tbody>
</table>
Routes are announced by routers and forwarded toward the collector. So the last AS, the “origin” AS, is the AS that “owns” (first announces) the prefix.
- Digital Envoy’s commercial geolocation server

- Geolocation
  - identification of real-world geographic location of Internet identifiers

- MaxMind GeoLite is a free service
  - http://www.maxmind.com/app/geoip_country

**Netacuity geographic dump**

<table>
<thead>
<tr>
<th>IP first</th>
<th>IP last</th>
<th>country</th>
<th>state</th>
<th>city</th>
<th>latitude</th>
<th>longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.172.226.0</td>
<td>192.127.226.255</td>
<td>usa</td>
<td>ca</td>
<td>la jolla</td>
<td>32.855</td>
<td>-117.249</td>
</tr>
<tr>
<td>137.164.23.0</td>
<td>137.164.23.255</td>
<td>usa</td>
<td>ca</td>
<td>tustin</td>
<td>33.736</td>
<td>-117.823</td>
</tr>
<tr>
<td>137.164.46.0</td>
<td>137.164.46.255</td>
<td>usa</td>
<td>ca</td>
<td>los angeles</td>
<td>33.973</td>
<td>-118.248</td>
</tr>
<tr>
<td>74.125.49.0</td>
<td>74.125.49.255</td>
<td>usa</td>
<td>il</td>
<td>chicago</td>
<td>41.886</td>
<td>-87.623</td>
</tr>
</tbody>
</table>
Regional Internet Registries (RIRs) assign Internet resources and maintain the WHOIS databases.

WHOIS databases store information about Internet registered users or assignees.

Whois dump

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASNumber</td>
<td>1909</td>
</tr>
<tr>
<td>OrgId</td>
<td>SDSC</td>
</tr>
<tr>
<td>OrgId</td>
<td>SDSC</td>
</tr>
<tr>
<td>OrgName</td>
<td>San Diego Supercomputer Center</td>
</tr>
<tr>
<td>Address</td>
<td>9500 Gilman Drive</td>
</tr>
</tbody>
</table>
whois

- **whois** command tools
  - whois is a command line client used to access the RIR servers
    ```
    whois -h whois.<RIR>.net <resource>
    <RIR> - afrinic, apnic, arin, lacnic, ripe,
    <resource> 129.10.1.1, AS12
    ```
  - start with ARIN, unless you know which region the allocation is in.

```
> whois -h whois.arin.net AS43

  ASNumber:     43
  ASName:       BNL-AS
  ASHandle:     AS43
  RegDate:      1985-04-11
  Updated:      2003-07-24
  Ref:          http://whois.arin.net/rest/asn/AS43

  OrgName:      Brookhaven National Laboratory
  OrgId:        BNL
  Address:      61 Brookhaven Ave
  Address:      Bldg. 515
  City:         Upton
  StateProv:    NY
  PostalCode:   11973
  Country:      US
  RegDate:      1984-09-13
  Updated:      2007-02-01
  Comment:      Brookhaven National Laboratory
  Ref:          http://whois.arin.net/rest/org/BNL

  OrgTechHandle: JB3159-ARIN
  OrgTechName:   Bigrow, John
```
We take the IP-level topology generated by ark and convert it to a AS-level topology.

We first map the IP address to the AS announcing the address space that contains it.
Map the IP address to the longest matching prefix and the those prefixes to their origin AS.
Fill in neighbors

Graph

paths

<table>
<thead>
<tr>
<th>AS</th>
<th>AS’s name</th>
<th>AS’s longitude</th>
<th>AS’s neighbors</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>5, 43</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>43</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td></td>
<td></td>
<td>1, 12</td>
<td>2</td>
</tr>
</tbody>
</table>
We take the organization name directly from the WHOIS dumps.

Geographic location will be harder, since our geolocation database does not provide locations for ASes, only IP addresses.
We assign an AS’s longitude to be equal to the weighted average of the Netacuity address blocks it announces.

\[
\frac{\sum_{i} \text{block}_i \cdot \text{longitude}_i \cdot \text{block}_i \cdot \text{size}_i}{\sum_{i} \text{block}_i \cdot \text{size}_i}
\]

<table>
<thead>
<tr>
<th>origin AS</th>
<th>prefix</th>
<th>IP block</th>
<th>longitude</th>
<th>weighted average longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>5.5.1.0/24</td>
<td>5.5.1.0 - 5.5.1.255</td>
<td>-103</td>
<td>-103</td>
</tr>
<tr>
<td>1</td>
<td>10.0.0.0/16</td>
<td>10.0.0.0-10.0.127.255</td>
<td>25</td>
<td>37.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.0.128.0-10.0.255.255</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>13.5.1.0/24</td>
<td>13.5.1.0-13.5.1.255</td>
<td>-23</td>
<td>-23</td>
</tr>
<tr>
<td>5</td>
<td>9.0.1.0/24</td>
<td>9.0.1.0-9.0.1.255</td>
<td>45</td>
<td>45</td>
</tr>
</tbody>
</table>
We now have everything we need to build the graph.

<table>
<thead>
<tr>
<th>AS</th>
<th>AS’s name</th>
<th>AS’s longitude</th>
<th>AS’s neighbors</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Level 3</td>
<td>37.5</td>
<td>5, 43</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Symbolics, Inc.</td>
<td>45</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>New York University</td>
<td>-103</td>
<td>43</td>
<td>1</td>
</tr>
<tr>
<td>43</td>
<td>Brookhaven Laboratory</td>
<td>-23</td>
<td>1, 12</td>
<td>2</td>
</tr>
</tbody>
</table>
Each node is a single AS, although ASes with nearby/same degree and longitude will overlap.

<table>
<thead>
<tr>
<th>node’s color/radius</th>
<th>$1 - \log\left(\frac{\text{degree (AS)} + 1}{\text{maximum degree} + 1}\right)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>node’s size</td>
<td>$\frac{\text{degree (AS)} + 1}{\text{maximum degree} + 1}$</td>
</tr>
<tr>
<td>node’s angle</td>
<td>longitude of the AS’s BGP prefixes</td>
</tr>
<tr>
<td>link color</td>
<td>node’s color with smallest degree</td>
</tr>
</tbody>
</table>
geographic regions

visualization breakdown
geographic regions

visualization breakdown

Asia

Europe

North American

South American

Africa

Oceana
why IPv6?

Internet Assigned Number Authority (IANA) allocated its last /8 to the RIR on 31 January 2011.

The RIRs are expected to run out of IPv4 address by no later then July 2015.

Future IANA allocations must come from IPv6 address space.

http://www.potaroo.net/ispcol/2010-10/when.html
IPv4 vs IPv6 graphs

IPv4

IPv6
IPv4 vs IPv6 graphs

IPv6 highest area of density in Europe
IPv4 vs IPv6 graphs

IPv4 high density in Asia, America, and Europe

IPv6 highest area of density in Europe
IPv4 vs IPv6 cores

IPv4 core primarily in North America

IPv6 core spread between America and Europe
American ISPs have been slower than European ISPs to take up IPv6.

With IPv4 exhaustion finally here, will this change?
- **Archipelago**

- **BGP collectors**
  - [http://www.routeviews.org](http://www.routeviews.org)

- **MaxMind GeoLite**
  - [http://www.maxmind.com/app/geoip_country](http://www.maxmind.com/app/geoip_country)

- **IPv4 RIR exhaustion**
  - [http://www.potaroo.net/ispcol/2010-10/when.html](http://www.potaroo.net/ispcol/2010-10/when.html)
Questions?

Internships:

http://www.caida.org/home/jobs/