Measuring and Monitoring BGP

Alberto Dainotti,
alberto@caida.org

Center for Applied Internet Data Analysis
University of California, San Diego
MEASURING BGP

Why?

BGP is the central nervous system of the Internet

BGP’s design is known to contribute to issues in:

• Availability

• Performance

• Security

Need to engineer protocol evolution!

Center for Applied Internet Data Analysis
University of California San Diego
MEASURING BGP

Why?

Defining problems and make protocol engineering decisions through realistic evaluations is difficult also because we know little about the structure and dynamics of the BGP ecosystem!

- AS-level topology
- AS relationships
- AS interactions: driven by relationships, policies, network conditions, operator updates
MEASURING BGP

two issues - somehow related

1. Literature shows that **we need more/better data**
   - more info from the protocol/routers

Attempts to generate more info *(not much traction in the past)*:
- RFC 4384 BGP Communities for Data Collection
- draft-ymbk-grow-bgp-collector-communities
MEASURING BGP

two issues - somehow related

1. Literature shows that **we need more/better data**
   - more info from the protocol/routers, more collectors,

Attempts to generate more info
*(not much traction in the past):*
- RFC 4384 BGP Communities for Data Collection
- draft-ymbk-grow-bgp-collector-communities
MEASURING BGP

two issues - somehow related

1. Literature shows that **we need more/better data**
   • more info from the protocol/routers, more collectors, more experimental testbeds, ...

Attempts to generate more info
(not much traction in the past):
• RFC 4384 BGP Communities for Data Collection
• draft-ymbk-grow-bgp-collector-communities

Inject/Receive Routes & Traffic.
PEERING - http://peering.usc.edu
MEASURING BGP

two issues - somehow related

1. Literature shows that we need more/better data
   • more info from the protocol/routers, more collectors, more experimental testbeds, …

2. But we also need better tools to learn from the data
   • to make data analysis: easier, faster, able to cope with BIG and heterogeneous data
   • to monitor BGP in near-realtime
   • tightening data collection, processing, visualization, …

libBGPDump
https://bitbucket.org/ripencc/bgpdump
BGP EVENTS & DYNAMICS

IODA: Detection and Analysis of Internet Outages

• Country-level Internet Blackouts during the Arab Spring

  Dainotti et al. “Analysis of Country-wide Internet Outages Caused by Censorship” IMC 2011

• Natural disasters affecting the infrastructure

  Dainotti et al. “Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet” SIGCOMM CCR 2012
Country-wide Internet outages in Iraq that the government ordered in conjunction with the ministerial preparatory exams - Jul 2015
Outage of AS11351 (Time Warner Cable LLC)
September 30, 2015

BGP EVENTS & DYNAMICS
IODA: Detection and Analysis of Internet Outages
BEFORE IODA

post-event manual analysis

Egypt, Jan 2011
Government orders to shut down the Internet

4 months of work

Dainotti et al. “Analysis of Country-wide Internet Outages Caused by Censorship” IMC 2011
Last Christmas we made it possible for anybody to follow the North Korean disconnection almost live.

https://charthouse.caida.org/public/kp-outage
MEASURING BGP

two issues - somehow related

1. Literature shows that **we need more/better data**
   - more info from the protocol/routers, more collectors, more experimental testbeds, …

2. But we also **need better tools to learn from the data**
   - to make data analysis: easier, faster, able to cope with BIG and heterogeneous data
   - to monitor BGP in near-realtime
   - tightening data collection, processing, visualization, …
A software framework for **historical** and **live** BGP data analysis

- Efficiently deal with large amounts of distributed BGP data
- Offer a time-ordered data stream of data from heterogeneous sources
- Support near-realtime data processing
- Target a broad range of applications and users
- Scalable
- Easily extensible
Example: studying AS path inflation

How many AS paths are longer than the shortest path between two ASes due to routing policies? (directly correlates to the increase in BGP convergence time)

![AS path length discrepancy PMF](Image)

```
$ python

from pybgpstream import BGPStream, BGPRecord, BGPElements
from collections import defaultdict
from itertools import zip_longest

# Define a function to calculate AS path length differences

stream = BGPStream()
as_graph = nx.Graph()
rec = BGPRecord()
bgp_lens = defaultdict(list)

for rec in stream:  # loop through all records
    if rec.type == 'BGP':  # only process BGP records
        origin = rec['origin']
        # Add the AS path length to the graph
        as_paths = [str(int(as_num)) for as_num in origin.split(',')]
        as_graph.add_node(origin, as_paths=as_paths)
        for i in range(len(as_paths) - 1):
            hop = int(as_paths[i + 1])
            bgp_lens[monitor][origin] +=
                min(filter(bool, bgp_lens[monitor][origin]), len(hops[i + 1]))

# Analyze AS path length differences

print('AS path length difference [d]

<table>
<thead>
<tr>
<th>d</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.8</td>
</tr>
<tr>
<td>1</td>
<td>0.6</td>
</tr>
<tr>
<td>2</td>
<td>0.4</td>
</tr>
<tr>
<td>3</td>
<td>0.2</td>
</tr>
<tr>
<td>4</td>
<td>0.1</td>
</tr>
<tr>
<td>5</td>
<td>0.08</td>
</tr>
<tr>
<td>6</td>
<td>0.06</td>
</tr>
<tr>
<td>7</td>
<td>0.04</td>
</tr>
<tr>
<td>8</td>
<td>0.02</td>
</tr>
<tr>
<td>9</td>
<td>0.01</td>
</tr>
<tr>
<td>10</td>
<td>0.005</td>
</tr>
<tr>
<td>11</td>
<td>0.002</td>
</tr>
</tbody>
</table>

# Example code snippet

# Function to add interval filters

for monitor in bgp_lens[monitor]:
    nlen = len(nx.shortest_path(as_graph, monitor, origin))
    print(monitor, origin, bgp_lens[monitor][origin], nlen)
```

30 LINES OF PYTHON CODE
The “prefix-monitor” plugin (distributed with source) monitors a set of IP ranges as they are seen from BGP monitors distributed worldwide:
- how many prefixes reachable
- how many origin ASes
- generates detailed logs

Hijacking of AS137 (GARR) - Jan 2015*

Hijacks: detection of MITM BGP attacks

normal path

hijacked path

normal path

used to complete the attack

S source (poisoned)  D dest (hijacked prefix)  A attacker

www.caida.org/funding/hijacks/
Hijacks: detection of MITM BGP attacks

Research informed by (and tested with) **data in the wild**

Live BGP measurements trigger on-demand dataplane measurements (e.g., traceroutes) **during** a suspicious event.
BGP HACKATHON - FEB 2016

theme: “live BGP measurements & monitoring”

Improve/Integrate tools to study the BGP eco-system. Target practical problems: topology, hijacks, outages, RPKI deployment, path inflation, circuitous paths, policies, relationships, visualize dynamics, …
We will provide a rich toolbox and “live” data access:

RIPE Atlas  CAIDA Ark  Looking Glasses

Data-plane active measurements

Generation  Collection  Injection  Processing & Analysis

PEERING

CAIDA AS Rank

VIZ tools
BGP HACKATHON
http://github.com/CAIDA/bgp-hackathon/wiki

• 6-7 February 2016  (weekend before NANOG 66)
• San Diego  Supercomputer Center, UC San Diego
• Theme: live BGP measurements and monitoring
• Toolbox: BGPMon, RIPE RIS, PEERING, BGPStream, RIPE Atlas, CAIDA Archipelago, Route Views, looking glasses, AS relationships, AS Rank, Visualization tools, …

• How to contribute:
  • join us and come over to hack!
  • help teams as a domain expert
  • propose projects that hacking teams may pick
  • offer to join the jury that will assign awards

>>> bgp-hackathon-info@caida.org <<<
THANKS

bgpstream.caida.org
github.com/CAIDA/bgp-hackathon/wiki