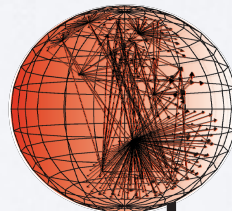


# *BGPStream: a framework for historical analysis and real-time monitoring of BGP data*

Chiara Orsini, Alistair King, Alberto Dainotti  
*alberto@caida.org*



caida

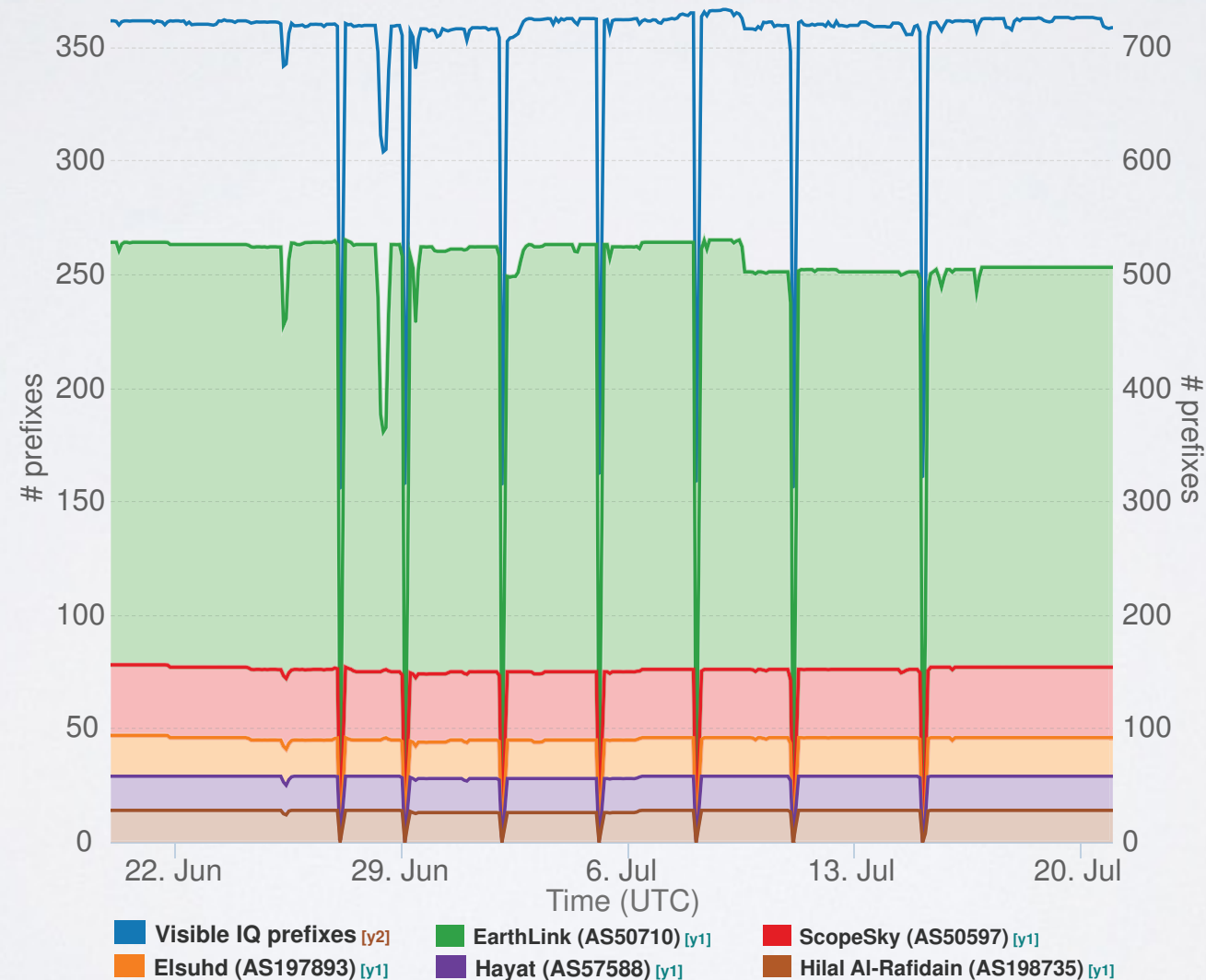
www.caida.org

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

# BGP EVENTS & DYNAMICS

## *IODA: Detection and Analysis of Internet Outages*

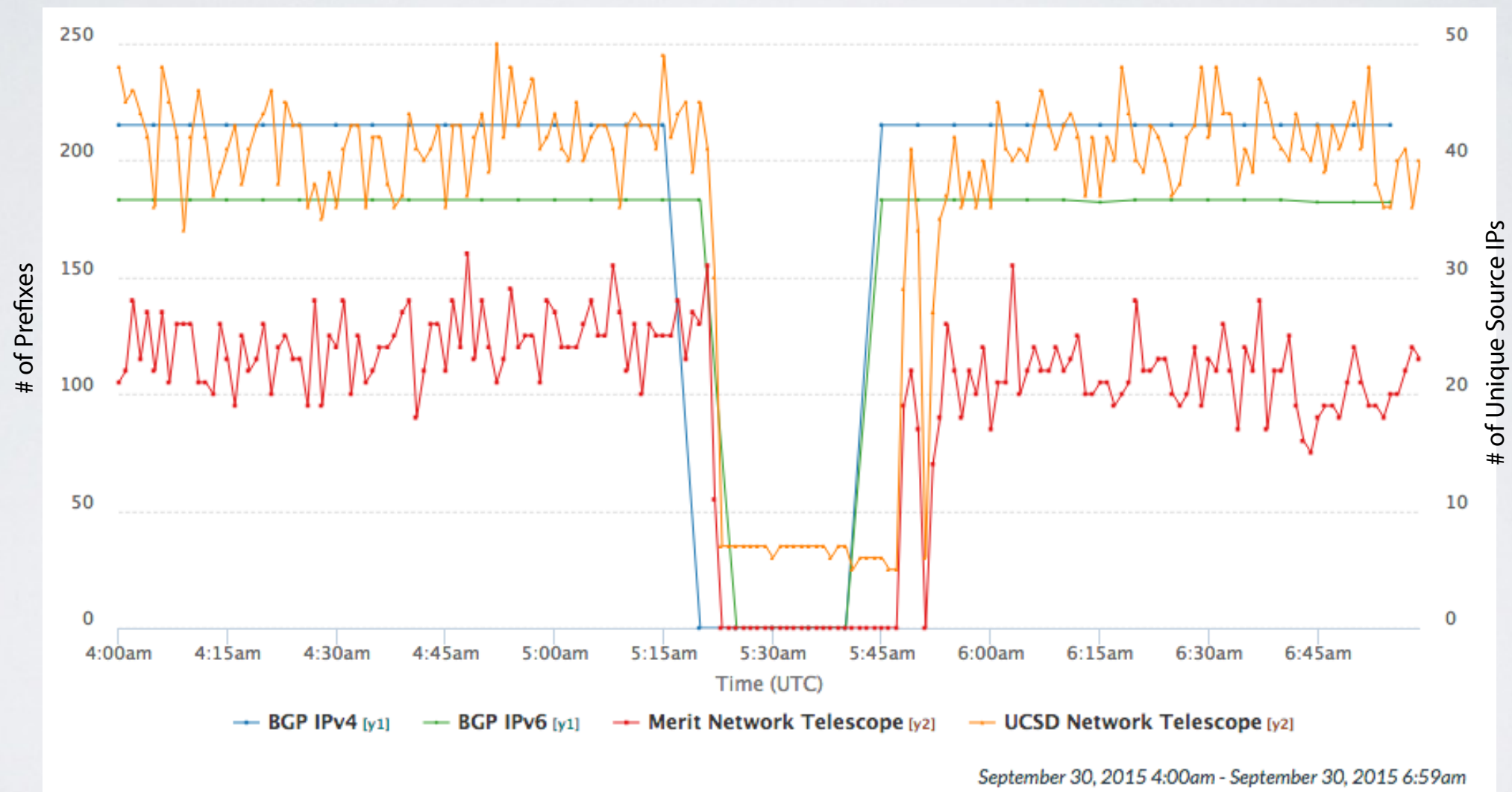
Country-wide Internet outages in Iraq that the government ordered in conjunction with the ministerial preparatory exams - Jul 2015



# BGP EVENTS & DYNAMICS

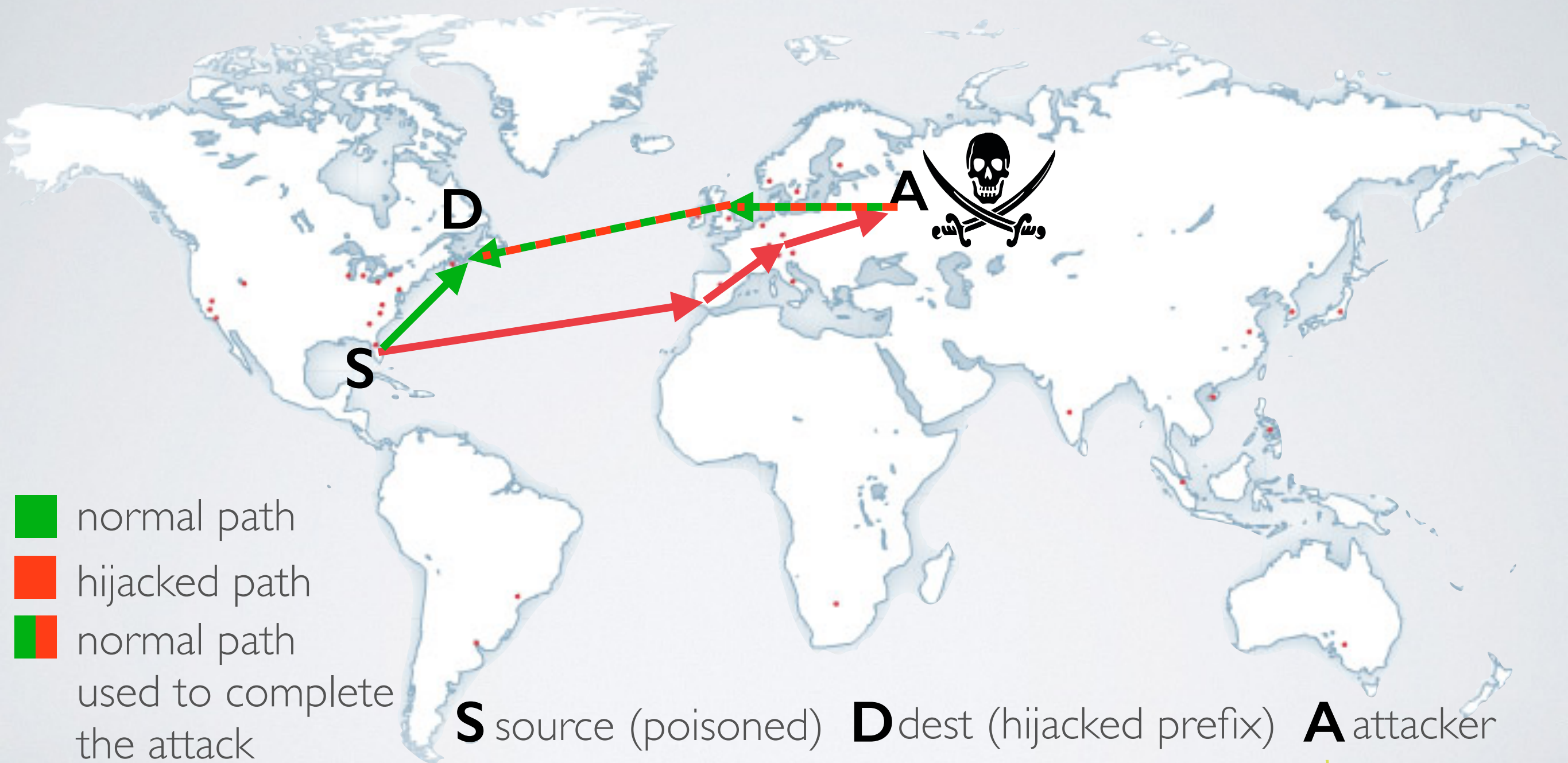
## *IODA: Detection and Analysis of Internet Outages*

Outage of AS11351 (Time Warner Cable LLC)  
September 30, 2015



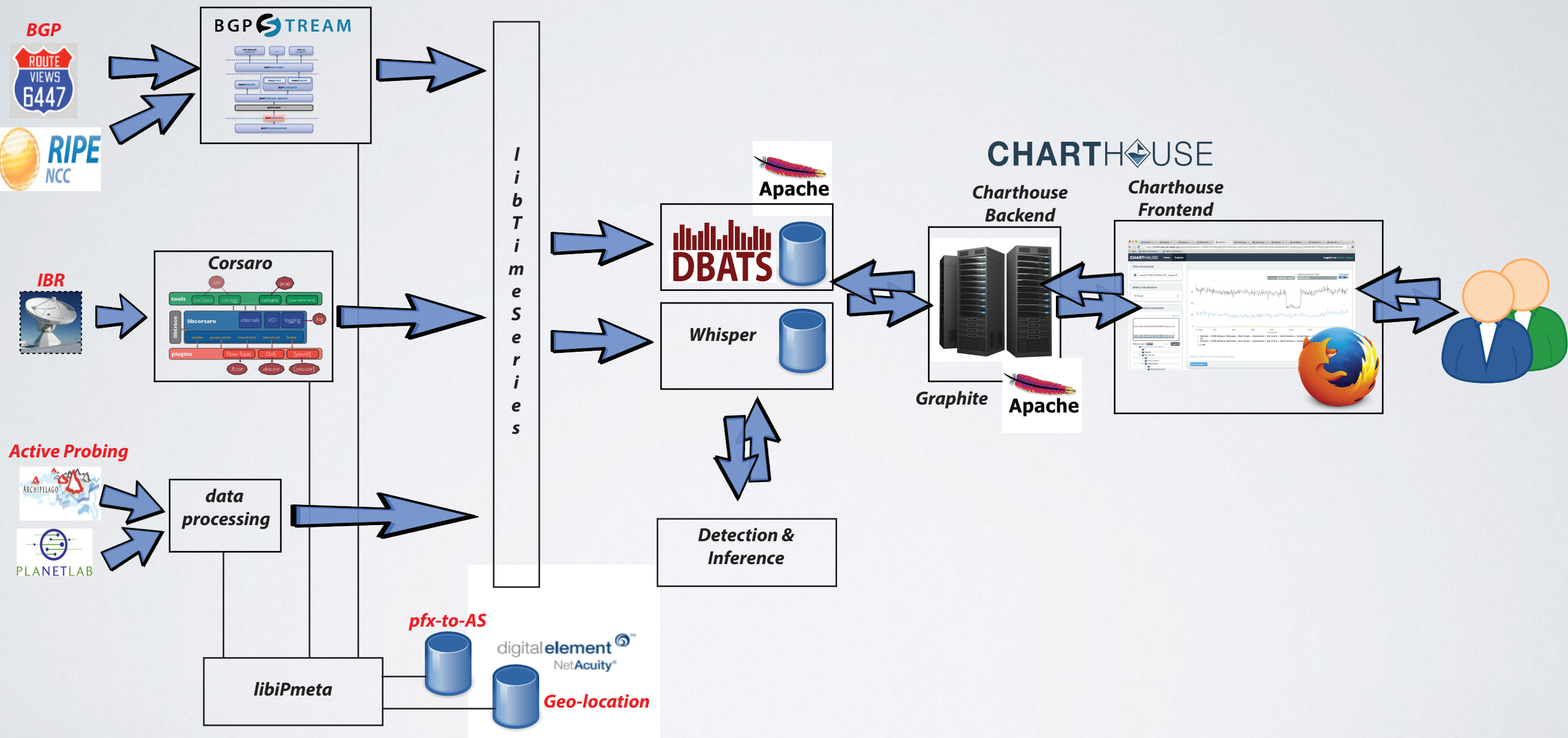
# BGP EVENTS & DYNAMICS

*Hijacks: detection of MITM BGP attacks*



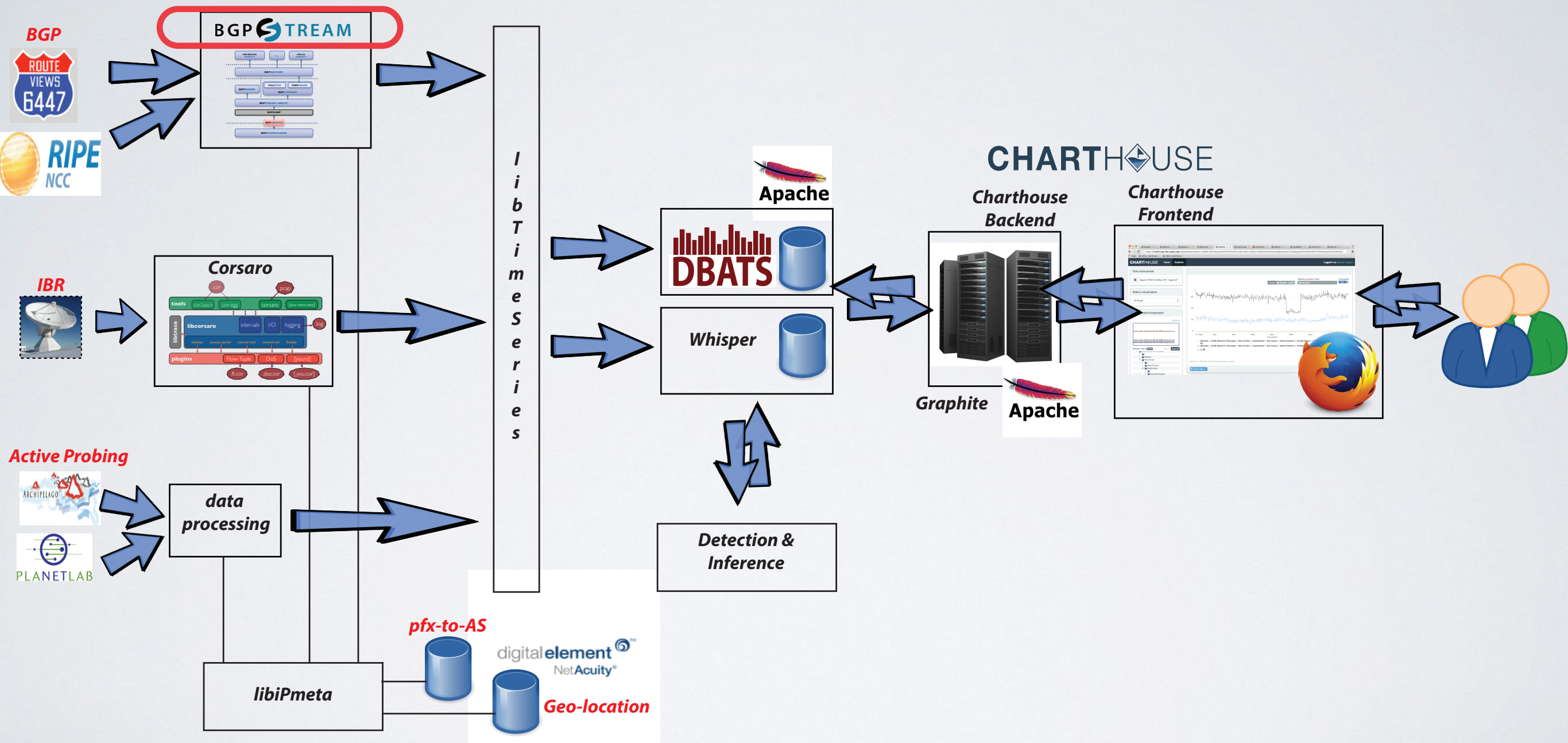
# IODA SYSTEM DIAGRAM

(toy diagram)



# IODA SYSTEM DIAGRAM

(toy diagram)



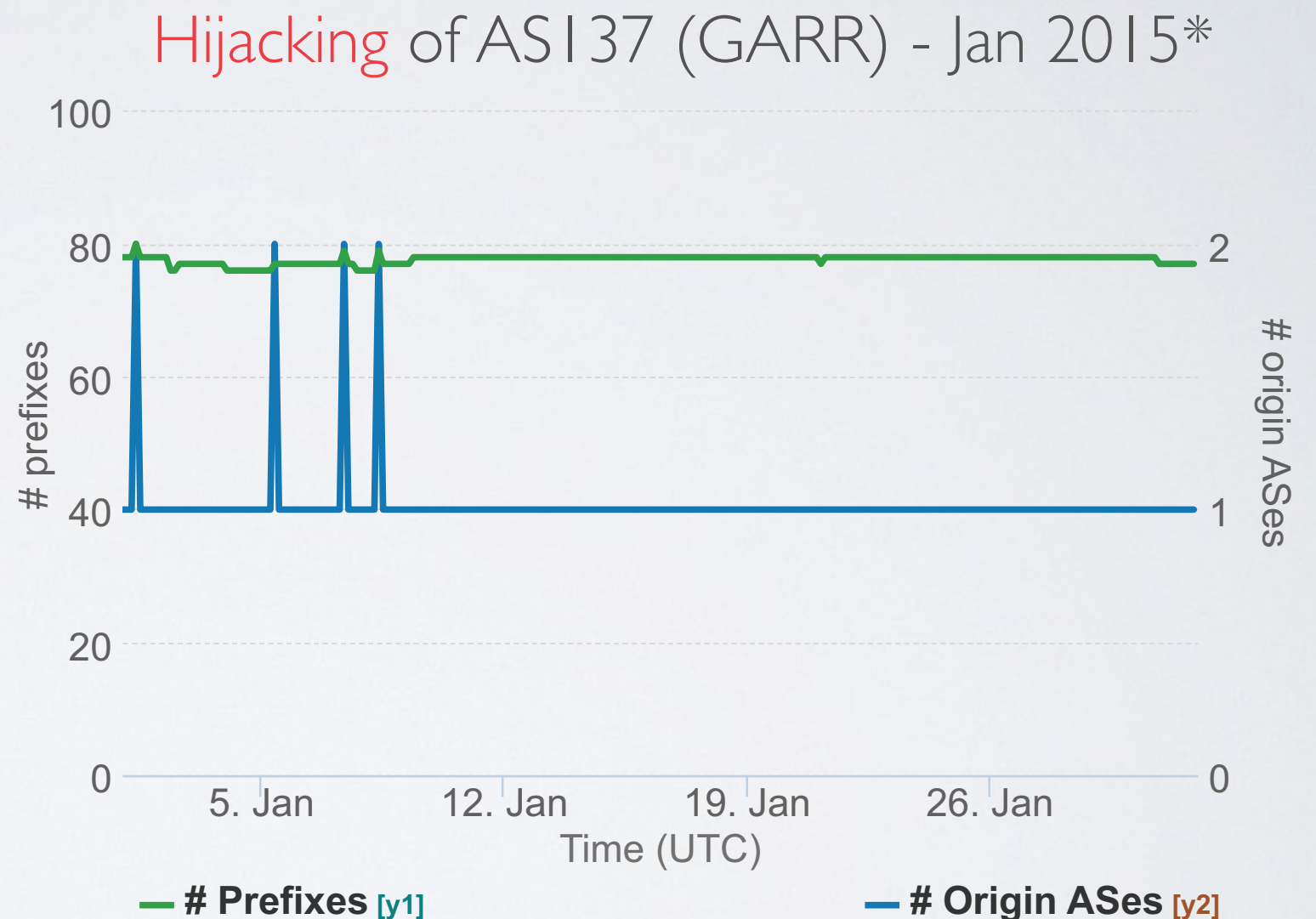


*[bgpstream.caida.org](http://bgpstream.caida.org)*

## Example: monitor your own address space on BGP

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



\*Originally discovered by Dyn:

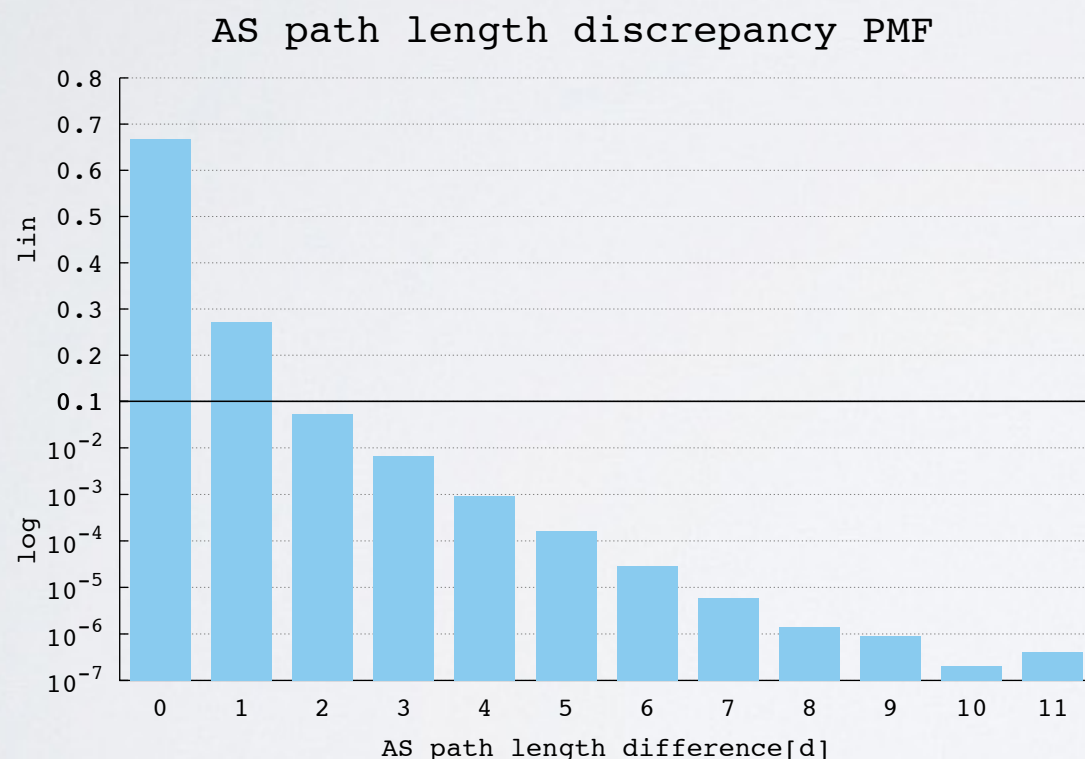
<http://research.dyn.com/2015/01/vast-world-of-fraudulent-routing/>

# PYBGPSTREAM



## 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*)



```
1 from _pybgpstream import BGPStream, BGPREcord, BGPElem
2 from collections import defaultdict
3 from itertools import groupby
4 import networkx as nx
5
6 stream = BGPStream()
7 as_graph = nx.Graph()
8 rec = BGPREcord()
9 bgp_lens = defaultdict(lambda: defaultdict(lambda: None))
10 stream.add_filter('record-type', 'ribs')
11 stream.add_interval_filter(1438415400, 1438416600)
12 stream.start()
13
14 while(stream.get_next_record(rec)):
15     elem = rec.get_next_elem()
16     while elem:
17         monitor = str(elem.peer_asn)
18         hops = [k for k, g in groupby(elem.fields['as-path'].split(" "))]
19         if len(hops) > 1 and hops[0] == monitor:
20             origin = hops[-1]
21             for i in range(0, len(hops)-1):
22                 as_graph.add_edge(hops[i], hops[i+1])
23                 bgp_lens[monitor][origin] = \
24                     min(filter(bool, [bgp_lens[monitor][origin], len(hops)]))
25             elem = rec.get_next_elem()
26 for monitor in bgp_lens:
27     for origin in bgp_lens[monitor]:
28         nxlen = len(nx.shortest_path(as_graph, monitor, origin))
29         print monitor, origin, bgp_lens[monitor][origin], nxlen
```

**30 LINES OF PYTHON CODE**

# BGPREADER



*command-line tool for ASCII output w/ filters*

```
$ bgpreader -w 1445306400,1445306402 -c route-views.sfmix
RIB|1445306400|routeviews|route-views.sfmix|
RIR|1445306400|routeviews|route-views.sfmix|32354|206.197.187.5|1.0.0.0/24|206.197.187.5|32354 15169|15169||
...
RIR|1445306401|routeviews|route-views.sfmix|14061|2001:504:30::ba01:4061:1|2c0f:ffd8::/32|
2001:504:30::ba01:4061:1|14061 1299 33762|33762|1299:30000||
RIR|1445306401|routeviews|route-views.sfmix|32354|2001:504:30::ba03:2354:1|2c0f:ffd8::/32|
2001:504:30::ba00:6939:1|32354 6939 37105 33762|33762||
RIR|1445306401|routeviews|route-views.sfmix|14061|2001:504:30::ba01:4061:1|3803:b600::/32|
2001:504:30::ba01:4061:1|14061 2914 3549 27751|27751|2914:420 2914:1008 2914:2000 2914:3000||
RIE|1445306401|routeviews|route-views.sfmix|
UIA|1445306401|routeviews|route-views.sfmix|32354|2001:504:30::ba03:2354:1|2402:ef35::/32|
2001:504:30::ba03:2354:1|32354 6939 6453 4755 7633|7633||
UIA|1445306401|routeviews|route-views.sfmix|14061|2001:504:30::ba01:4061:1|2a02:158:200::/39|
2001:504:30::ba01:4061:1|14061 2914 44946|44946|2914:410 2914:1201 2914:2202 2914:3200||
...
```

# BGPSTREAM

[bgpstream.caida.org](http://bgpstream.caida.org)

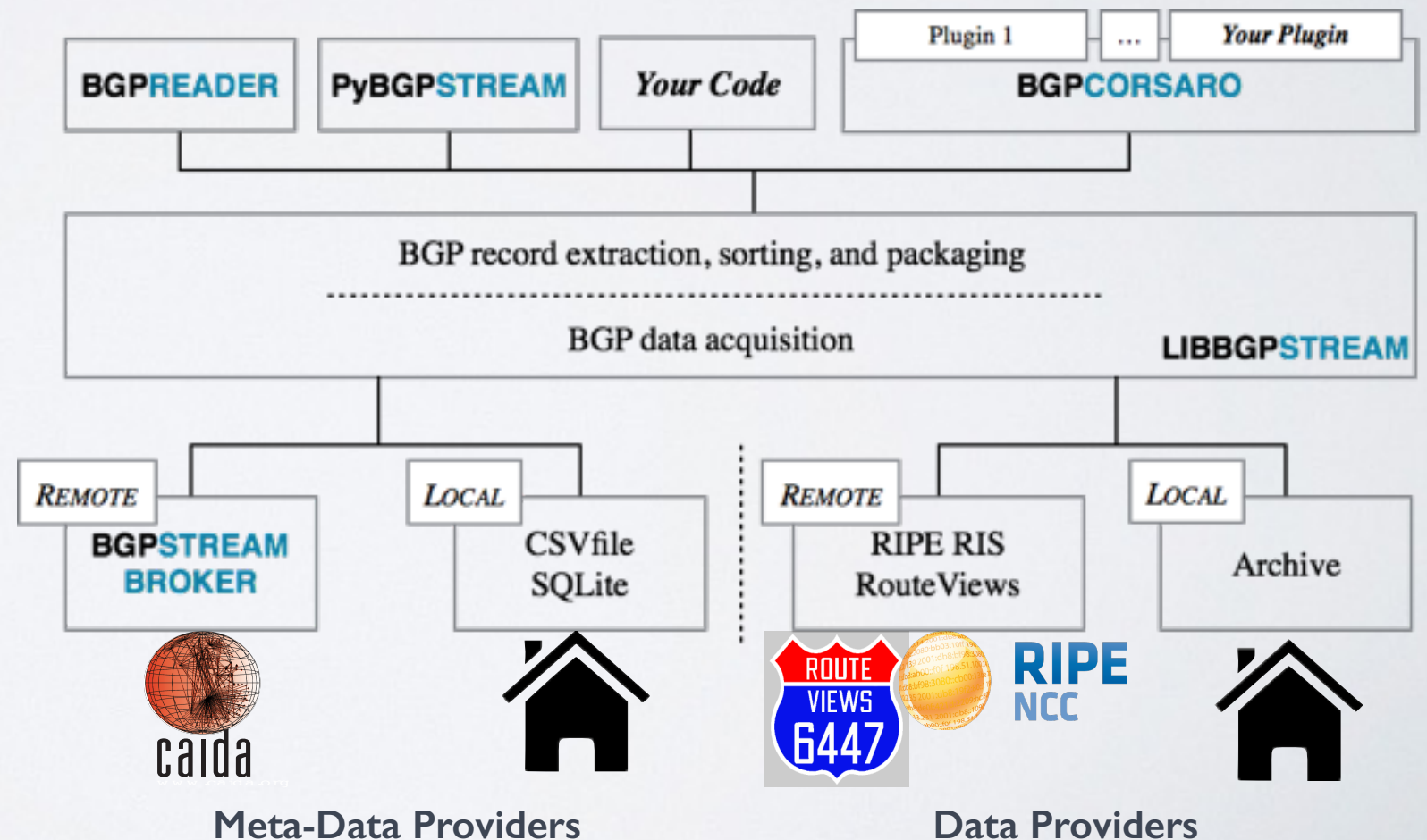
1. A web service (“BGPStream Broker”)

- enables SIMPLE **access** to LOTS of heterogeneous BGP sources

2. LibBGPStream:

- Acquires the data and provides to upper layers a realtime stream of BGP data
- makes it SIMPLE to **process** data from LOTS of heterogeneous BGP sources

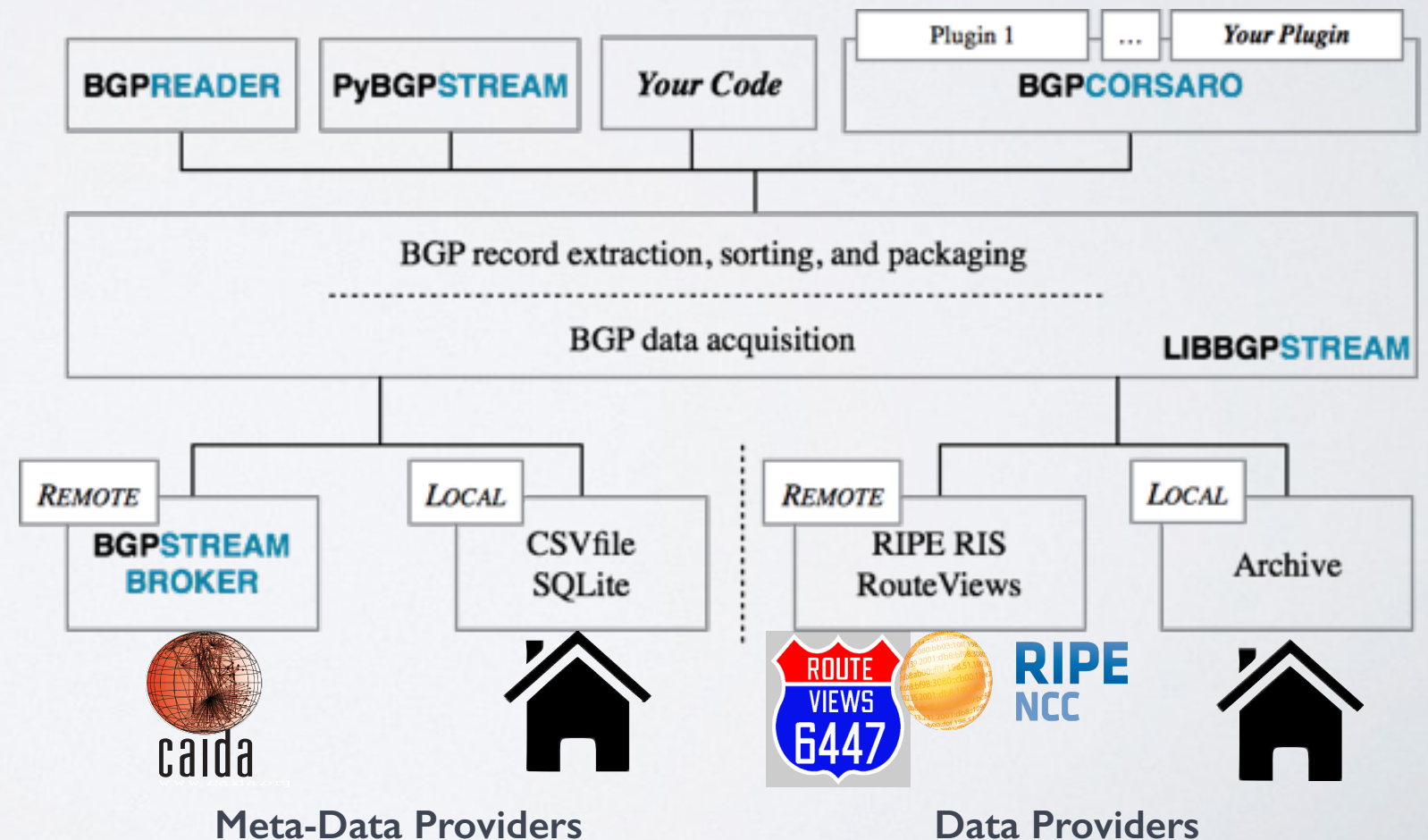
3. Command-line tools and APIs in C and Python



# BGP STREAM

[bgpstream.caida.org](http://bgpstream.caida.org)

- Design goals:
  - Efficiently deal with large amounts of distributed BGP data
  - Offer a time-orderd data stream of data from heterogeneous sources
  - Support near-realtime data processing
  - Target a broad range of applications and users
  - Scalable
  - Easily extensible



# NO MANUAL DOWNLOADS

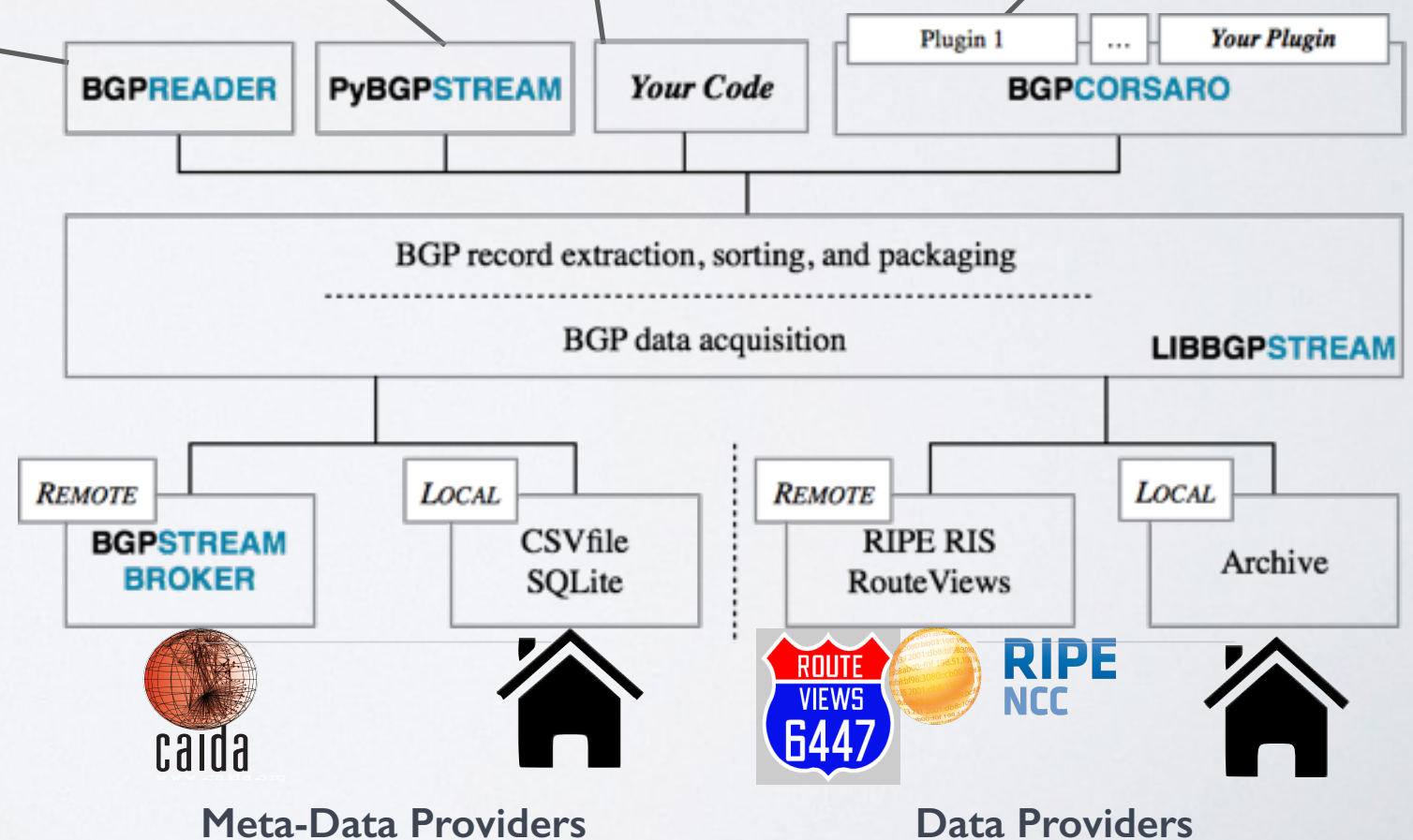
*libBGPStream talks to the broker and gets the data*

```
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_COLLECTOR, "rrc06");  
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_COLLECTOR, "route-views.jinx");  
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_RECORD_TYPE, "updates");  
bgpstream_add_interval_filter(bs, 1286705410, 1286709071);
```

```
stream.add_filter('record-type', 'ribs')  
stream.add_filter('collector', 'route-views.sfmix')  
stream.add_interval_filter(1445306400, 1445306402)
```

```
$ bgpreader -w 1445306400,1445306402 -c route-views.sfmix -t updates
```

```
$ bgpcorsaro -w 1445306400,1445306402 -p ris
```



# GET A LIVE STREAM

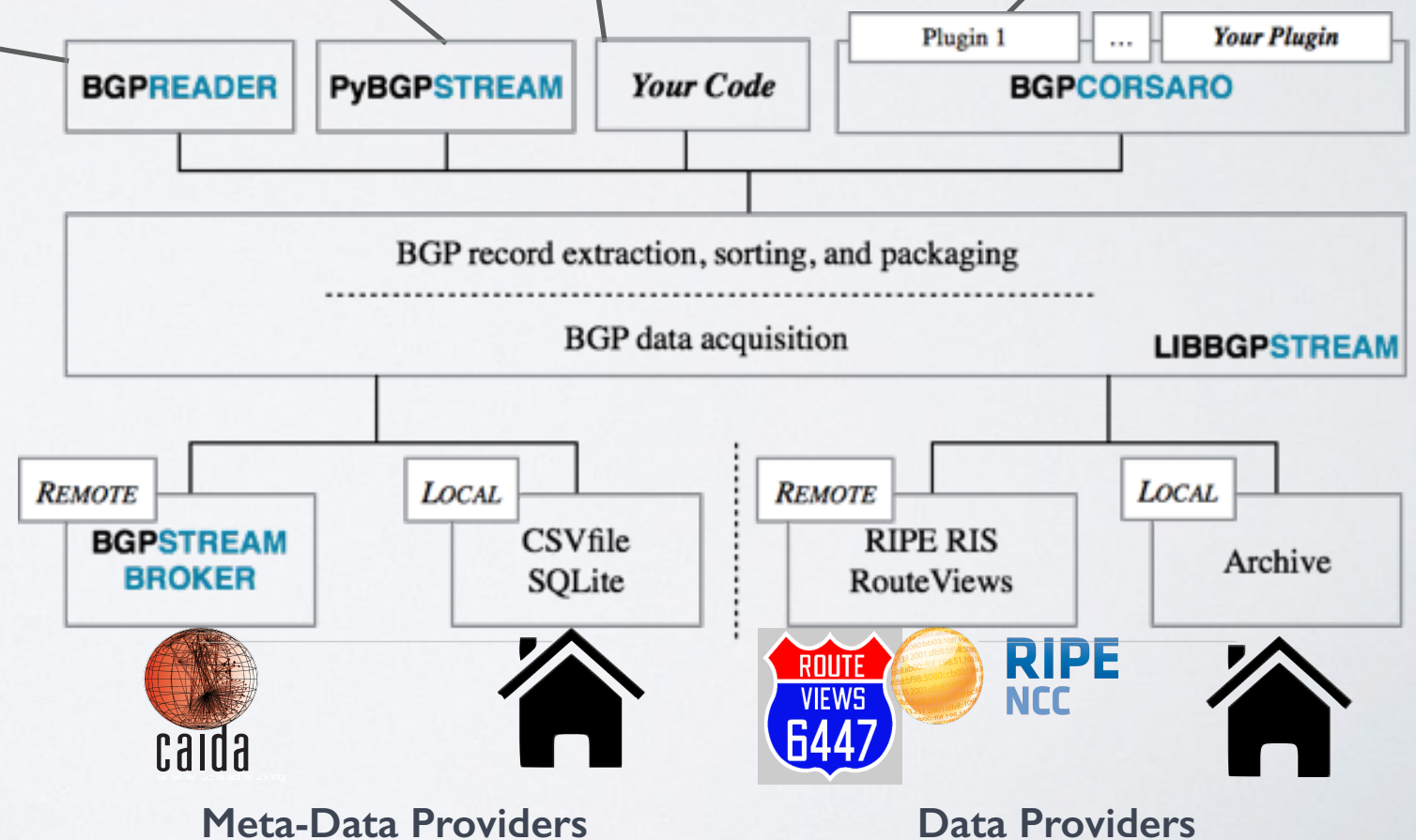
*libBGPStream keeps retrieving data as it becomes available*

```
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_COLLECTOR, "rrc06");  
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_COLLECTOR, "route-views.jinx");  
bgpstream_add_filter(bs, BGPSTREAM_FILTER_TYPE_RECORD_TYPE, "updates");  
bgpstream_add_interval_filter(bs, 1286705410, BGPSTREAM_FOREVER);
```

```
stream.add_filter('record-type', 'ribs')  
stream.add_filter('collector', 'route-views.sfmix')  
stream.add_interval_filter(1445306400, -1)
```

```
$ bgpreader -c route-views.sfmix -t updates
```

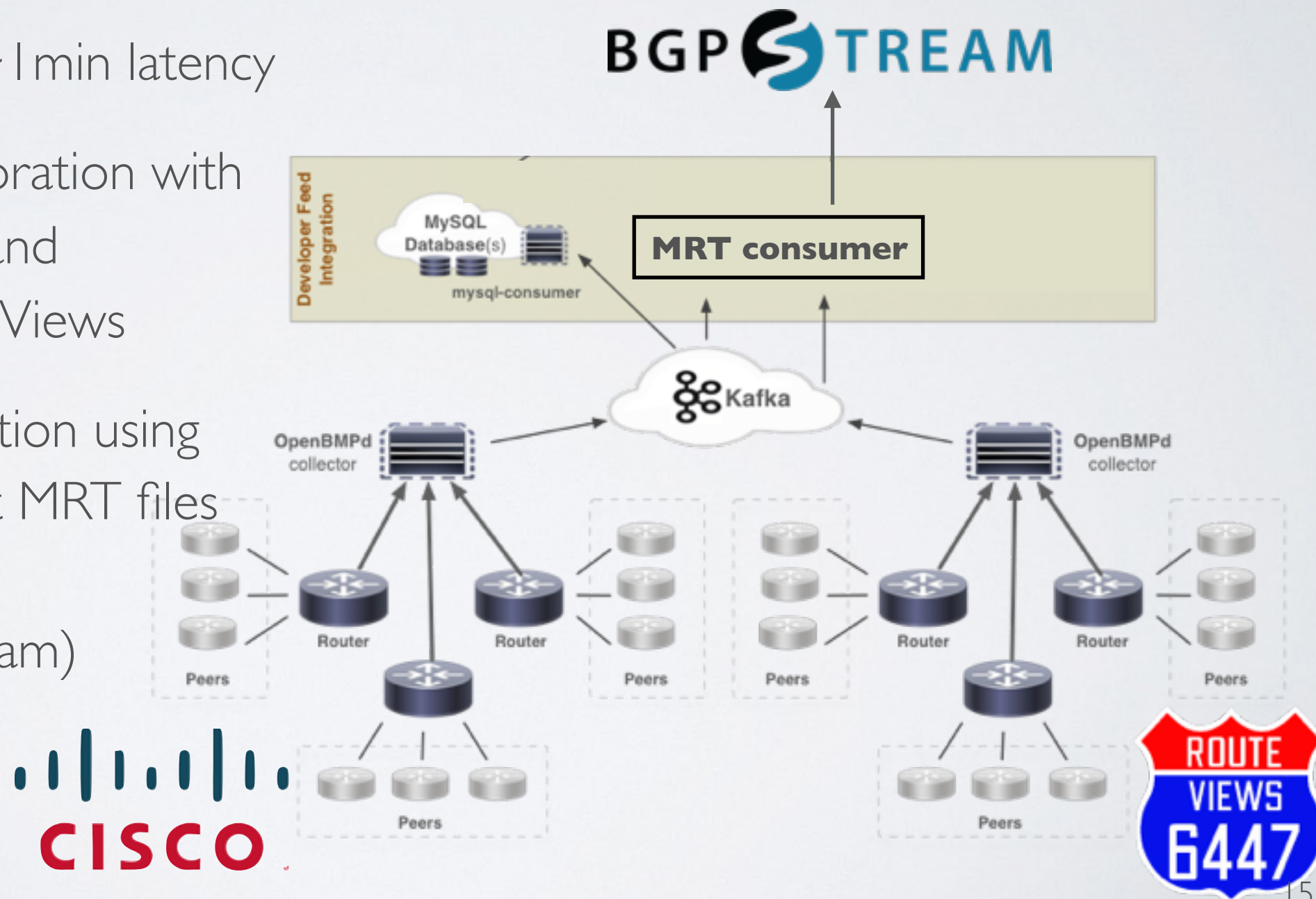
```
$ bgpcorsaro -p ris
```



# BMP DATA SOURCES

*(experimental)*

- Access BMP-generated data from BGPStream
- Data available with  $\sim 1$  min latency
- Developed in collaboration with Tim Evens @ Cisco and John Kemp @ Route Views
- Experimental integration using OpenBMP to export MRT files (native BMP support planned for BGPStream)



# BMP DATA SOURCES

## *Data Providers*

- Current BMP feeds provided courtesy of **Route Views**, **Cisco**, and **Randy Bush**

| CAIDA OpenBMP (experimental) <span>caida-bmp</span>                                                                                                                                                               |                                  |                |                               |                                   |  |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------|-------------------------------|-----------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| The CAIDA OpenBMP provider is a collaboration with Route Views and Cisco to provide access to a low-latency (~1min) stream of BGP measurement data using the OpenBMP stack. Data is served to BGPStream by CAIDA. |                                  |                |                               |                                   |                                                                                     |                                                                                     |
| Collector                                                                                                                                                                                                         | Dump Type                        | Dump Frequency | First Dump                    | Latest Dump                       |                                                                                     |                                                                                     |
| router-route-views.routeviews.org.peer-IPV4_route-spews.cbttier3.att.net                                                                                                                                          | RIBs ( <span>ribs</span> )       | an hour        | 2016/01/29 16:12 (7 days ago) | 2016/02/05 21:00 (42 minutes ago) |                                                                                     |                                                                                     |
|                                                                                                                                                                                                                   | Updates ( <span>updates</span> ) | a minute       | 2016/01/28 22:18 (8 days ago) | 2016/02/05 21:40 (2 minutes ago)  |                                                                                     |                                                                                     |
| router-route-views.routeviews.org.peer-IPV4_lo-22.car2.Seattle1.Level3.net                                                                                                                                        | RIBs ( <span>ribs</span> )       | an hour        | 2016/01/29 16:12 (7 days ago) | 2016/02/05 21:00 (42 minutes ago) |                                                                                     |                                                                                     |
|                                                                                                                                                                                                                   | Updates ( <span>updates</span> ) | a minute       | 2016/01/28 22:18 (8 days ago) | 2016/02/05 21:40 (2 minutes ago)  |                                                                                     |                                                                                     |
| router-route-views.routeviews.org.peer-IPV6_core1.sjc2.he.net                                                                                                                                                     | RIBs ( <span>ribs</span> )       | an hour        | 2016/01/29 16:12 (7 days ago) | 2016/02/05 21:00 (42 minutes ago) |                                                                                     |                                                                                     |
|                                                                                                                                                                                                                   | Updates ( <span>updates</span> ) | a minute       | 2016/01/28 22:18 (8 days ago) | 2016/02/05 21:40 (2 minutes ago)  |                                                                                     |                                                                                     |
| router-route-views.routeviews.org.peer-IPV6_2001:1890:111d:1::63                                                                                                                                                  | RIBs ( <span>ribs</span> )       | an hour        | 2016/01/29 16:12 (7 days ago) | 2016/02/05 21:00 (42 minutes ago) |                                                                                     |                                                                                     |
|                                                                                                                                                                                                                   | Updates ( <span>updates</span> ) | a minute       | 2016/01/28 22:18 (8 days ago) | 2016/02/05 21:40 (2 minutes ago)  |                                                                                     |                                                                                     |
| router-192.133.197.1.peer-IPV4_192.133.159.1                                                                                                                                                                      | RIBs ( <span>ribs</span> )       | an hour        | 2016/01/29 16:12 (7 days ago) | 2016/02/05 21:00 (42 minutes ago) |                                                                                     |                                                                                     |
|                                                                                                                                                                                                                   | Updates ( <span>updates</span> ) | a minute       | 2016/01/28 22:18 (8 days ago) | 2016/02/05 21:40 (2 minutes ago)  |                                                                                     |                                                                                     |
| router-r1.sea.rg.net.peer-IPV4_sl-gw20-sea-0-3-2-1.sprintlink.net                                                                                                                                                 | RIBs ( <span>ribs</span> )       | an hour        | 2016/01/30 22:15 (6 days ago) | 2016/02/05 21:00 (42 minutes ago) |                                                                                     |                                                                                     |
|                                                                                                                                                                                                                   | Updates ( <span>updates</span> ) | a minute       | 2016/01/30 22:15 (6 days ago) | 2016/02/05 21:40 (2 minutes ago)  |                                                                                     |                                                                                     |

# BMP DATA SOURCES

*don't need to download a new BGPStream version*

- Available **to all** existing BGPStream installs
  - Use filter to select data from provider “caida-bmp”
  - E.g. bgpreader -p caida-bmp -w 1453912260
- send us a bmp feed!
  - contact [bgpstream-info@caida.org](mailto:bgpstream-info@caida.org)

```
alistair@gibi:~$ bgpreader -p caida-bmp -w 1453912260 2>/dev/null | head -10
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV6_core1.sjc2.he.net|6939|2001:470:0:1a
::1|2a06:9380::/29|2001:470:0:1a::1|6939 12732|12732||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV6_2001:1890:111d:1::63|7018|2001:1890:
111d:1::63|2804:14d::/40|2001:1890:111d:1::63|7018 174 4230 28573|28573|7018:5000 7018:38000||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV4_route-spews.cbbtier3.att.net|7018|12
.0.1.63|206.208.95.0/24|12.0.1.63|7018 3356 4323 3728 19837 19837 19837 19837|19837|7018:5000 7018:39220|
|
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV6_core1.sjc2.he.net|6939|2001:470:0:1a
::1|2804:14d::/40|2001:470:0:1a::1|6939 4230 28573|28573||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV6_2001:1890:111d:1::63|7018|2001:1890:
111d:1::63|2804:14d::/40|2001:1890:111d:1::63|7018 6453 4230 28573|28573|7018:5000 7018:37232||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV4_route-spews.cbbtier3.att.net|7018|12
.0.1.63|94.236.200.0/24|12.0.1.63|7018 3356 57344 60168|60168|7018:5000 7018:37232||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV4_route-spews.cbbtier3.att.net|7018|12
.0.1.63|79.124.4.0/24|12.0.1.63|7018 3356 57344 60168|60168|7018:5000 7018:37232||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV4_route-spews.cbbtier3.att.net|7018|12
.0.1.63|177.136.84.0/23|12.0.1.63|7018 3356 3549 18881 263164 262485 264162 263132|263132|7018:5000 7018:
37232||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV4_route-spews.cbbtier3.att.net|7018|12
.0.1.63|177.136.86.0/24|12.0.1.63|7018 3356 3549 18881 263164 262485 264162 263132|263132|7018:5000 7018:
37232||
UIA11454019502|caida-bmp|router-route-views.routeviews.org.peer-IPV4_route-spews.cbbtier3.att.net|7018|12
.0.1.63|206.208.95.0/24|12.0.1.63|7018 3356 4323 3728 19837 19837 19837 19837|19837|7018:5000 7018:37232|
```

# THANKS

*[bgpstream.caida.org](http://bgpstream.caida.org)*