Routing transparency

Is the Internet routing system transparent?

- Yes, to a certain extent. Public route collectors (RIS, RouteViews, PCH) make a lot of data available
  - Some portions of the Internet and some of the relationships are not visible as they are not being exposed to these route collectors

- But making sense of these data is a heavy lift, available to few
  - BGP data is very noisy
  - Analysis requires assumptions about relationships between operators and other heuristics

Why do we need more transparency?

- The Bitcanal case:
  - "*As should be blatantly self-evident to pretty much everyone who has ever looked at any of the Internet's innumeriable prior incidents of very deliberately engineered IP space hijackings, all of the routes currently being announced by AS3266 (Bitcanal, Portugal) except for the ones in 213/8 are bloody obvious hijacks*." Ronald F. Guilmette, NANOG ML, June 2017.
- Ability to see (and analyse) **unusual events/anomalies** that are happening in the Internet routing with many eyes will **more clearly** expose systematic abuse or gross negligence, allow to remedy anomalies **quicker**, and **better** inform research and discussions related to routing security with stable references.

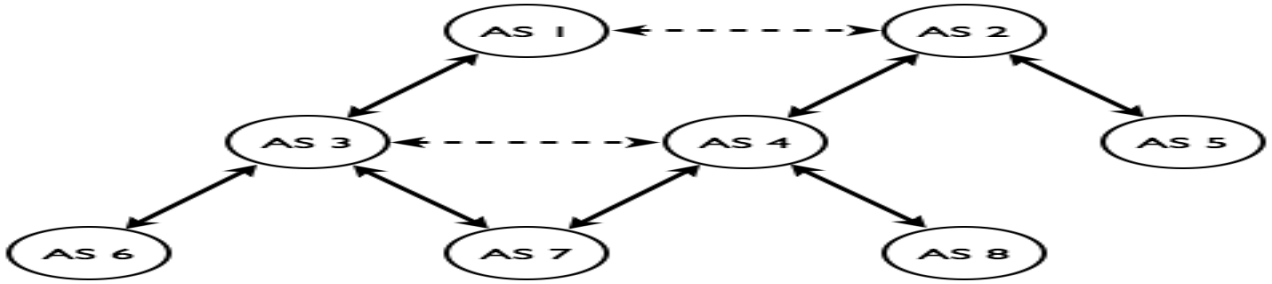
What tools do we have?

- Network based views –
  - https://stat.ripe.net, https://bgp.he.net, https://radar.qrator.net
  - Commercial integrated products Kentik, Crosswork
  - good when you know what/who to look at

- Global routing system based views - https://bgpstream.com/ - a great service, but
  - not transparent - heuristics is largely a black box
  - EOL

“Raw BGP”

```
BGP4MP|1445306400|W|2001:504:1::a502:4482:1|24482|2a03:5080::/32
BGP4MP|1445306400|A|193.232.245.109|24482|208.74.216.0/21|24482 7029 40377|IGP|193.232.245.109|0|8000|7029:1002 24482:2|NAG||
BGP4MP|1445306400|A|198.32.176.20|6939|212.22.66.0/24|6939 12389 41938 8359 50618 35189 201432|IGP|198.32.176.20|0|0||NAG||
…
```

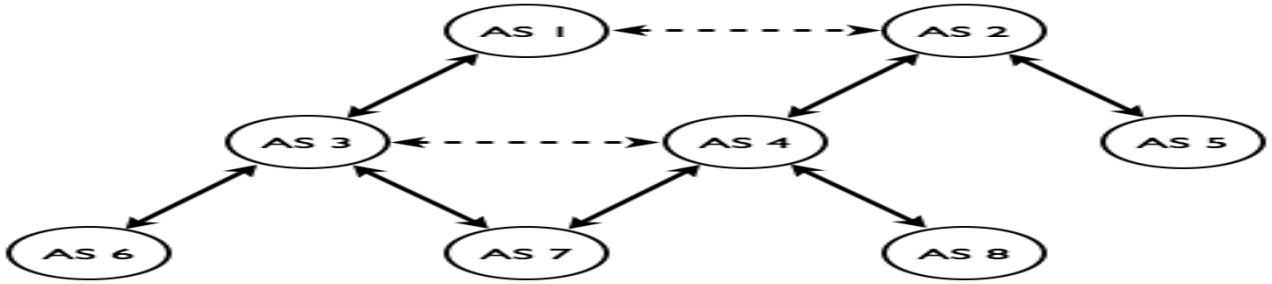


“Transparency layer”


```
”unusual_event":{
    "id": 809606602873, "start_time": "2018-01-07T07:00:00", "end_time": "2018-01-08T11:00:00", "as-path": [24482, 7029, 40377], "nlri":
    "195.64.224.0/24”, "expected":{ "origin_asn": 8695, "nlri": "195.64.224.0/24”, "path_segment": null,    …}
}
```

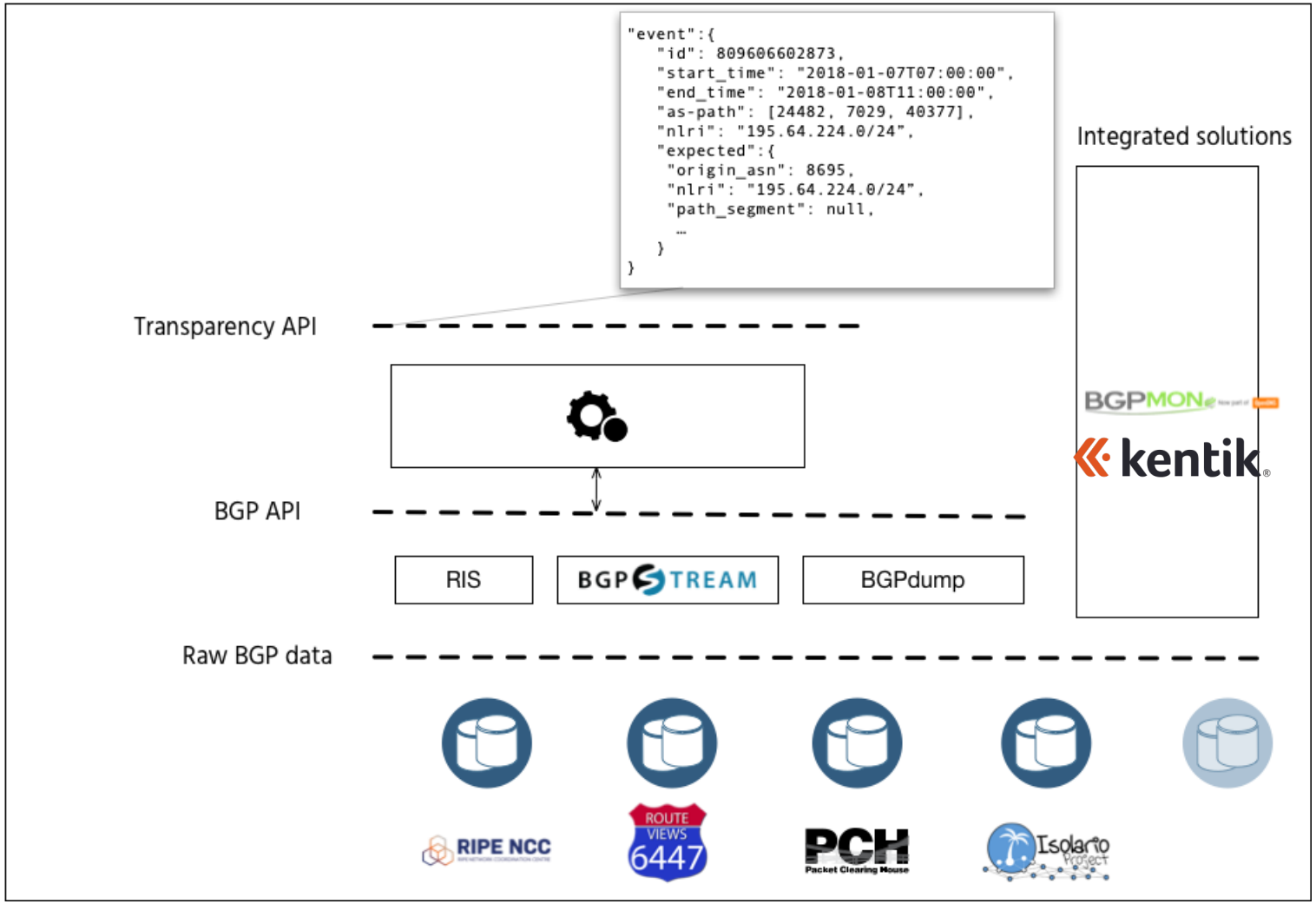


```
BGP4MP|1445306400|W|2001:504:1::a502:4482:1|24482|2a03:5080::/32
BGP4MP|1445306400|A|193.232.245.109|24482|208.74.216.0/21|24482 7029 40377|IGP|193.232.245.109|0|8000|7029:1002 24482:2|NAG||
BGP4MP|1445306400|A|198.32.176.20|6939|212.22.66.0/24|6939 12389 41938 8359 50618 35189 201432|IGP|198.32.176.20|0|0||NAG||
…
```

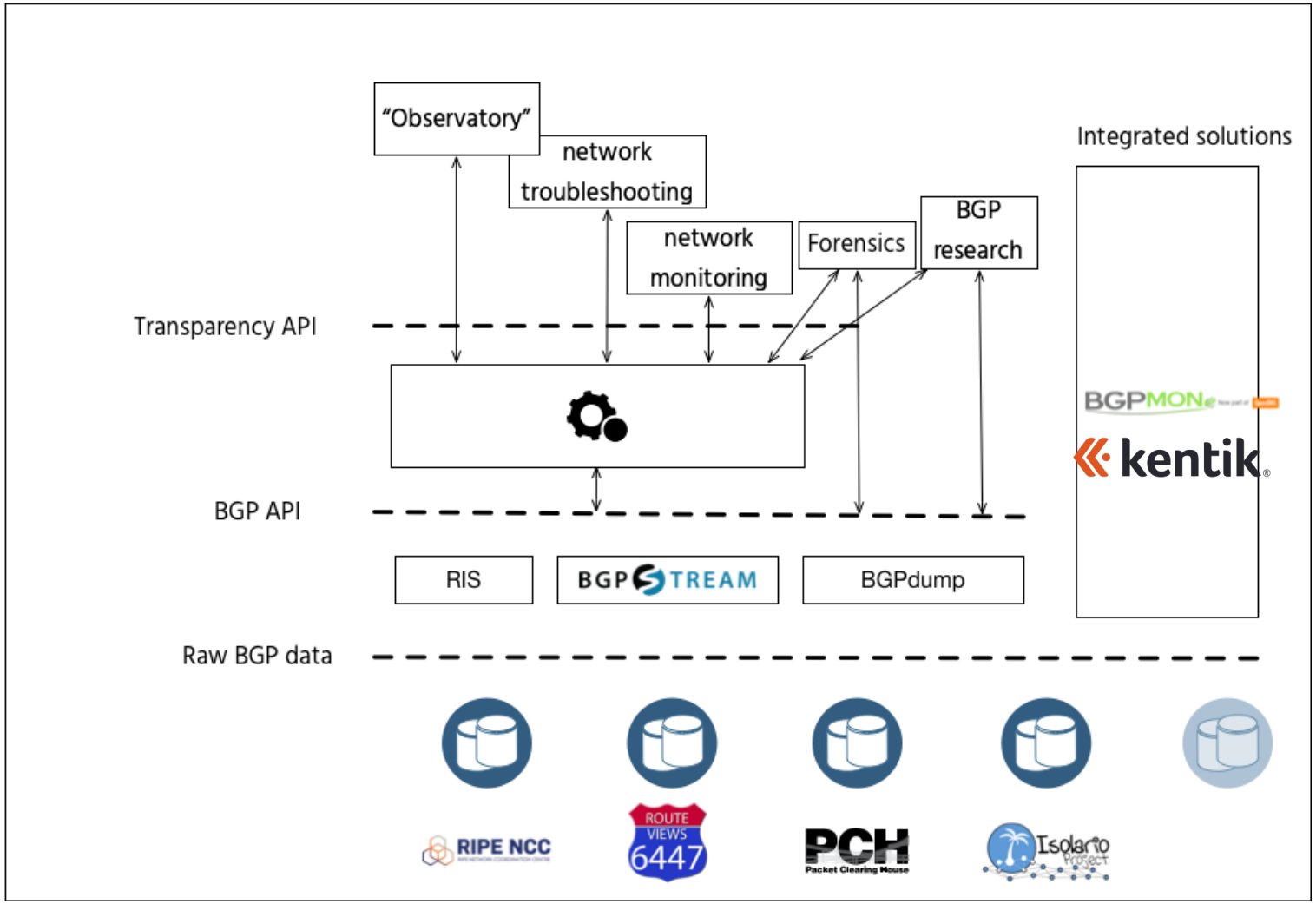
Conceptual view

Transparency layer



Conceptual view

Transparency layer



What answers the service like this could offer?

- Were there any unusual events related to a specific prefix over last year/month/week?
- Were there any unusual events potentially affecting a specific network?
- What were the unusual events (if any) related to a specific networks?
- With what certainty can we assume that the unusual event is a routing attack, rather than a legitimate change?
- The unusual event related to my network is a false positive, how can I report and fix this?
- …. ?

What are the requirements?

- Open. Should be provided as a free service to the community
- Transparent. Heuristics and methodology should be open and subject to modifications
- Community driven. Impartial and responsive to community needs. Also regarding methodology improvements

Where from here?

- Get community feedback and develop a more concrete proposal (or throw it in the trash bin)
- Get interested parties together
  - Routing researchers
  - Network operators
  - Software developers
  - Anyone interested in contributing
- Set up a proof-of-concept prototype
- Present at RIPE 79

Questions?

robachevsky@isoc.org