RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Internet Data Analysis with RIPE RIS

Advanced Topics

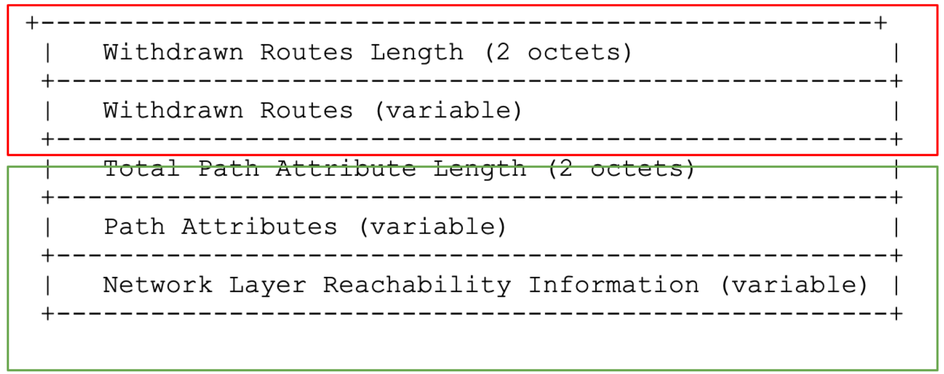
Emile Aben | 2022 | TMA PhD School

BGP Packet Formats

- BGP Open. Initial session setup. Parameter negotiation
  - MRT data contains STATE messages (state 6 = ESTABLISHED)
- BGP Update

'You can not reach these through me anymore'

'Got traffic for $NLRI? I can route that for you via $AS_PATH'



BGP Info Normalisation

- 1 BGP packet format contains many “state changes”
- For analysis: Process one “state change” at a time

./bgpdump <file>

```
TIME: 02/23/08 12:50:00
TYPE: BGP4MP/MESSAGE/Update
FROM: 213.179.39.65 AS16186
TO: 193.0.4.28 AS12654
WITHDRAW
  192.23.187.0/24
  213.42.0.0/17
  195.229.128.0/17
  195.229.0.0/17
```

vs.

./bgpdump -m <file>

```
BGP4MP|1203771000|W|213.179.39.65|16186|192.23.187.0/24
BGP4MP|1203771000|W|213.179.39.65|16186|213.42.0.0/17
BGP4MP|1203771000|W|213.179.39.65|16186|195.229.128.0/17
BGP4MP|1203771000|W|213.179.39.65|16186|195.229.0.0/17
```

- “No flags” format will tell you about uncommon attributes

AS Path Surprises

- Sequence of same ASN: Traffic Engineering/“prepending”

```
91.205.158.0/24 2497 174 62206 56399 207313 207313
91.205.158.0/24 25152 6939 56399 207313 207313
91.205.158.0/24 4777 2516 174 62206 56399 207313 207313
```

```
4777 6939 23947 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004
25152 6939 23947 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004 18004
```

- AS Path poisoning: Paths ends with: ASx ASy (..) ASx

```
25152 6939 1273 15924 44327 16010 44327
4777 2516 1273 15924 44327 16010 44327
```

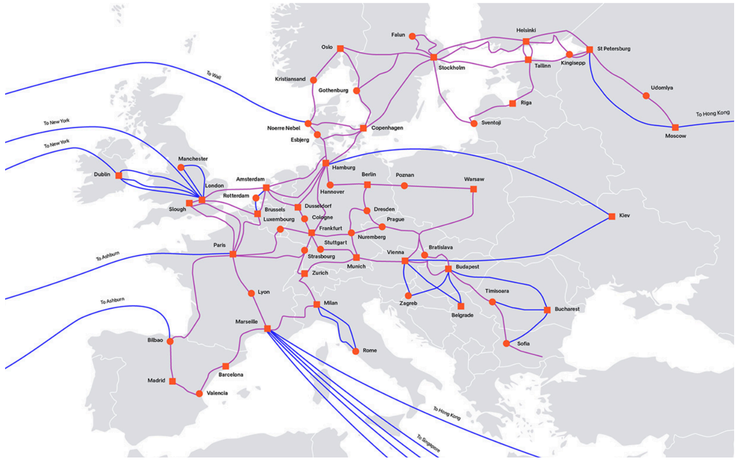
- Config typo: Prepend config differs on different platforms

```
45.82.88.0/22 2497 3356 8400 25144
45.82.88.0/22 25152 2914 3356 8400 25144
45.82.88.0/22 4777 6939 5391 25144 2
```

- Deliberate attempts to misguide (hijacks)

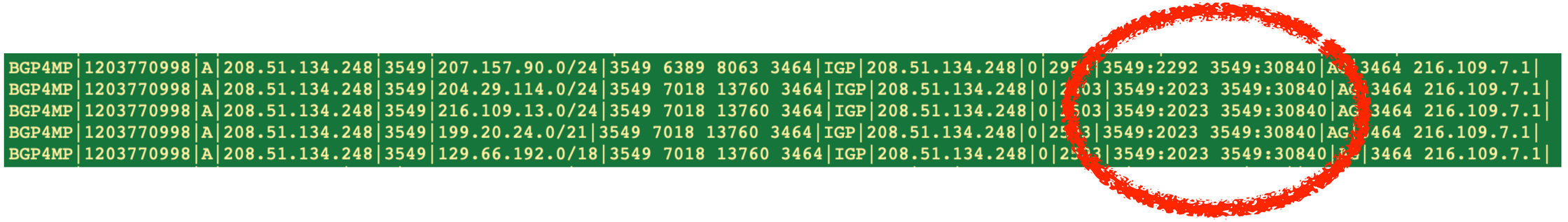
BGP And Geography

- It’s complex!
  - Don’t assume: a prefix is in a single location, IP geolocation is correct, ASNs are in a single country, even when there are datasets for these mappings!
  - ASNs are often mapped to single countries (via RIR stats). Can be misleading
    - 1299 = SE ? 1299 is (was?) headquartered in Sweden, network is worldwide



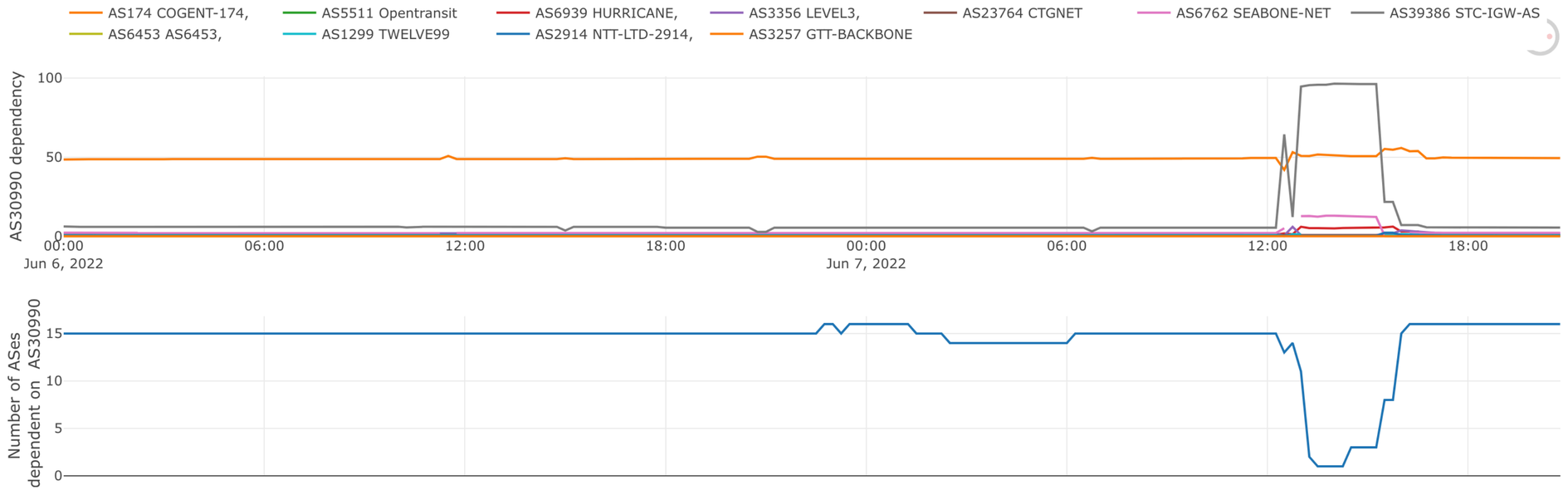
BGP Communities

- It is possible to tag a route
  - Informational: “I announce/receive this route from location X”
  - Action: “prefer/depref/change this route”
- Each BGP route has 0+ communities, encoded as 32 bit values.
- Typically
  - The first 16 bits encode an ASN
  - The last 16 bits is informational/action



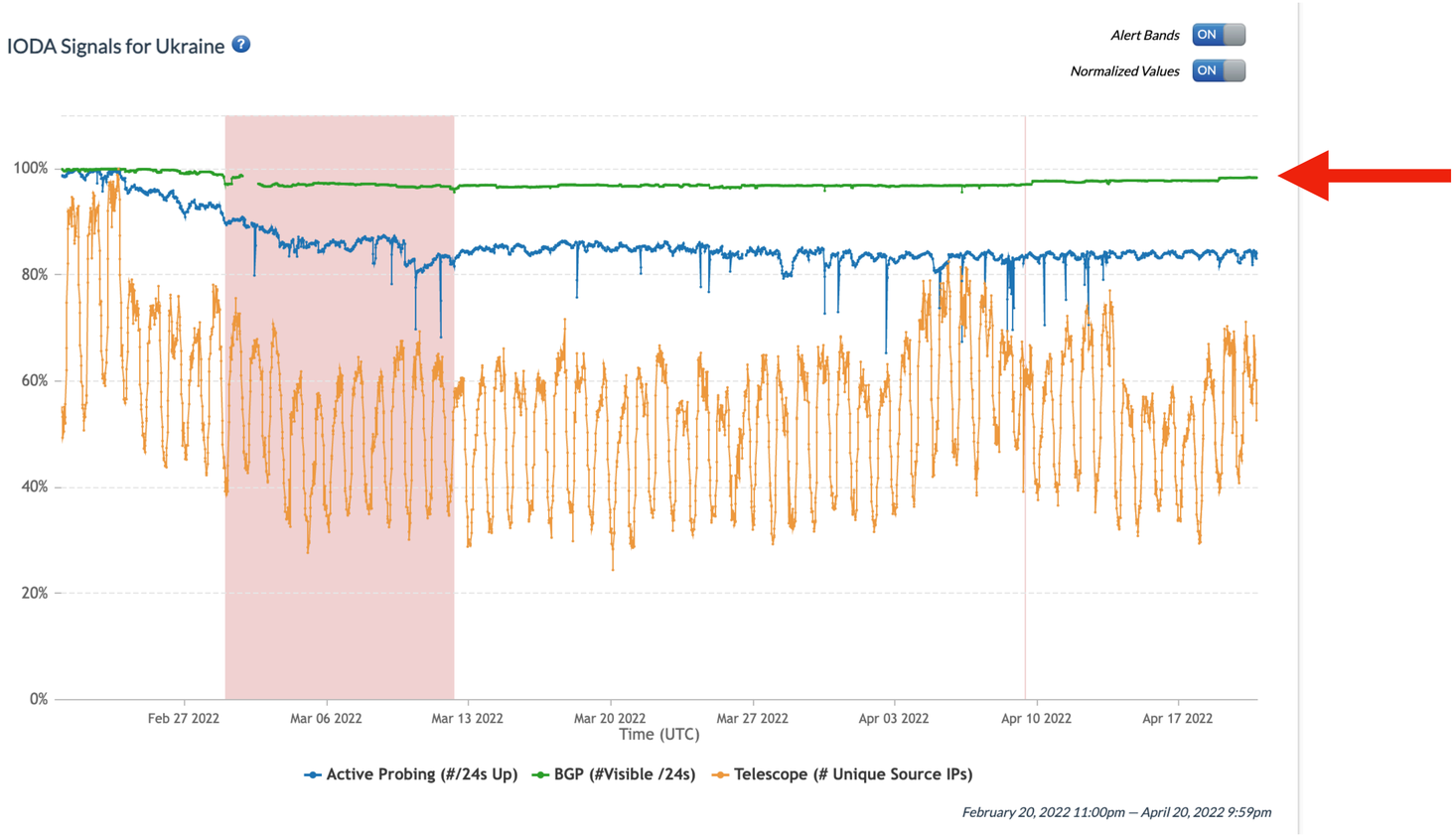
Derived Data: Internet Health Report

- https://ihr.iijlab.net/
- AS-Hegemony: How much does a network depend on another?



Derived Data: IODA

- https://ioda.inetintel.cc.gatech.edu/



Other Useful Sites For BGP

- bgp.he.net (uses RIS data)
- bgp.tools
- peeringdb.com