RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Something's Wrong on the Internet

How Internet Measurements Help Us Detect Internet Events

Qasim Lone | 5 September 2024 |TLDCON

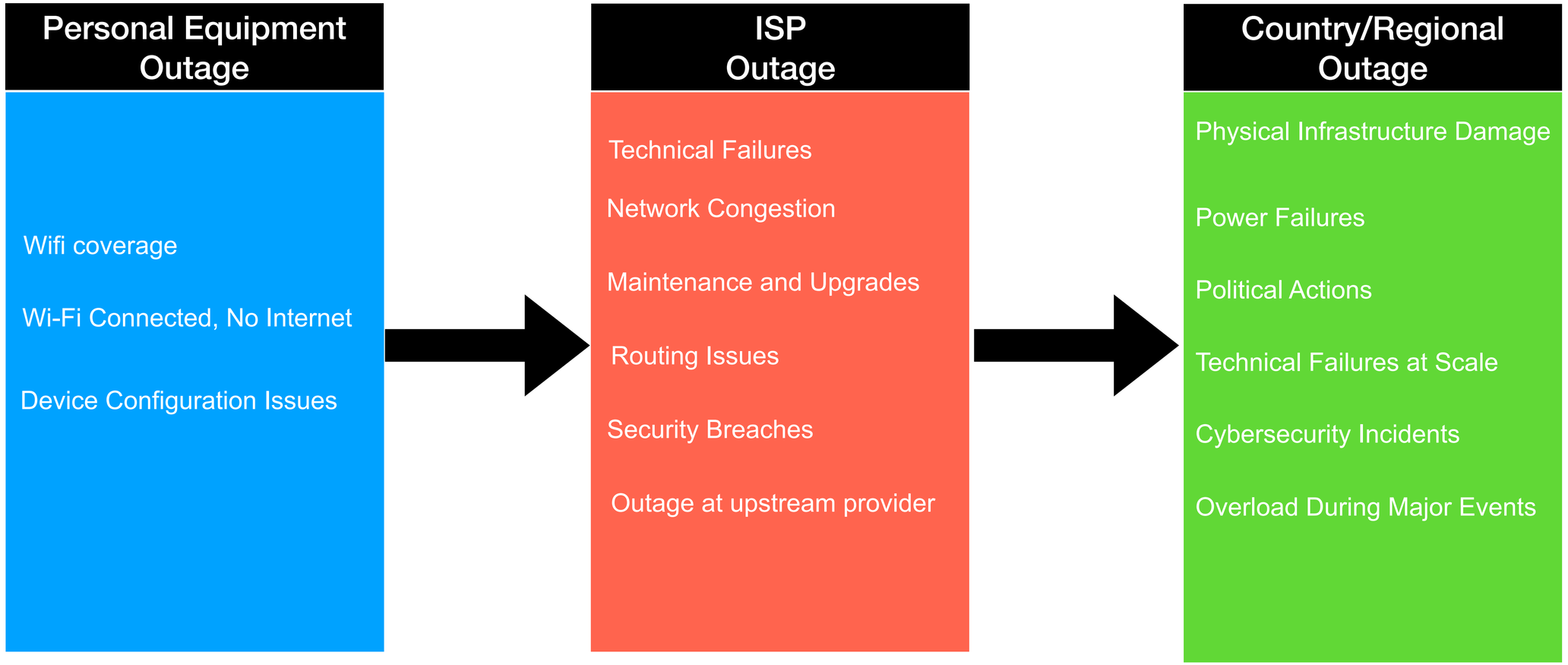
No Internet

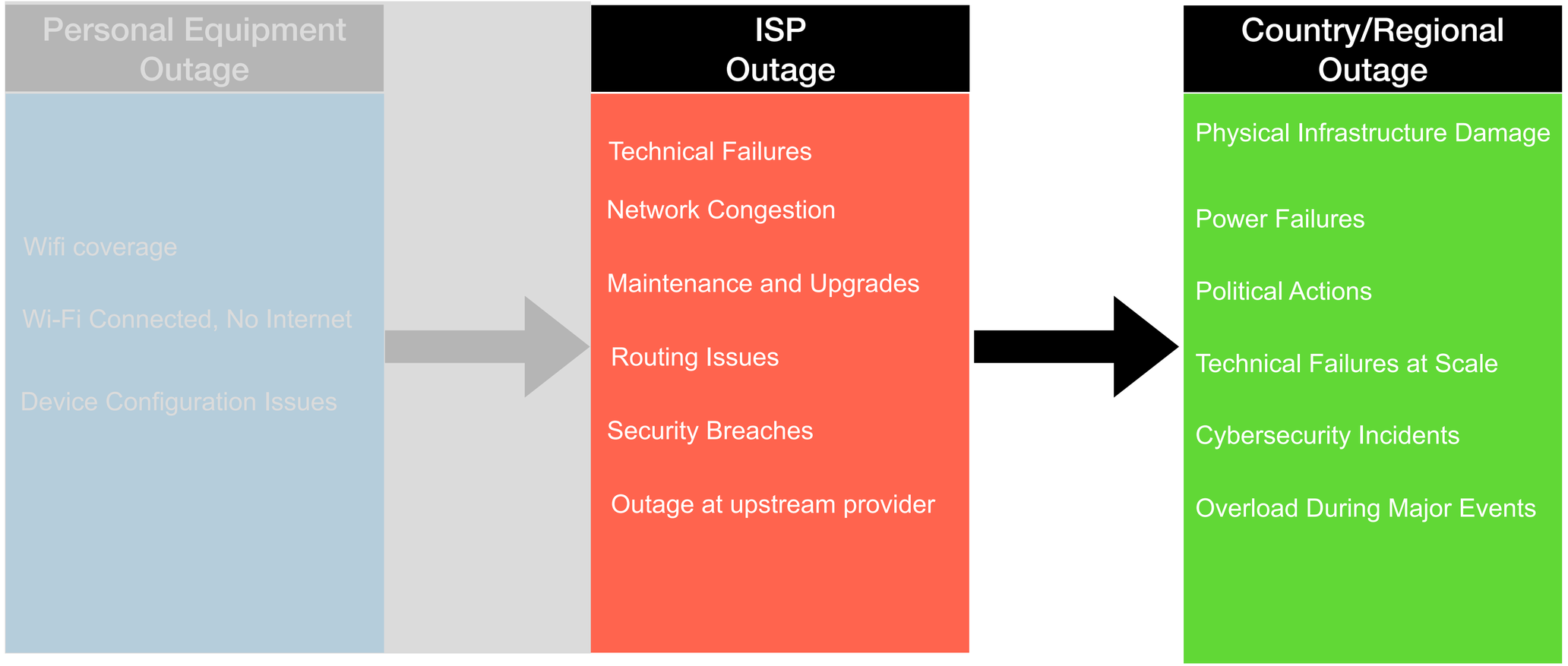
Try:

- Checking the network cables, modem and router
- Reconnecting to Wi-Fi

ERR_INTERNET_DISCONNECTED


HAVE YOU TRIED
TURNING IT OFF AND ON AGAIN?


Personal Equipment Outage
Wifi coverage
Wi-Fi Connected, No Internet
Device Configuration Issues
ISP Outage
Technical Failures
Network Congestion
Maintenance and Upgrades
Routing Issues
Security Breaches
Outage at upstream provider
Country/Regional Outage
Physical Infrastructure Damage
Power Failures
Political Actions
Technical Failures at Scale
Cybersecurity Incidents
Overload During Major Events


Personal Equipment Outage
Wifi coverage
Wi-Fi Connected, No Internet
Device Configuration Issues
ISP Outage
Technical Failures
Network Congestion
Maintenance and Upgrades
Routing Issues
Security Breaches
Outage at upstream provider
Country/Regional Outage
Physical Infrastructure Damage
Power Failures
Political Actions
Technical Failures at Scale
Cybersecurity Incidents
Overload During Major Events

Publicly Available Datasets

- Control Plane
  - Determine how data is routed across the Internet using protocols like BGP, ensuring efficient and reliable paths through constant updates to routing tables.
  - Route Collectors:
    - RIS
    - Routeviews
- Data Plane
  - Active and passive traffic flows
  - Traceroute, Ping, DNS etc
- Examples:
  - RIPE Atlas
  - Open Intel
  - Caida Datasets
    - Some are publicly available other’s can be requested

Routing Information Service (RIS)

Routing Information Service (RIS)

- RIS is a routing data collection platform, started in 1999
  - all historical data is publicly available
- Deployed at Internet Exchange Points
- Collects raw BGP data from peers
  - stores BGP messages and routing table dumps
- Real-time routing information, as opposed to information in databases and routing registries
- Is a source of data for many other services

Why collect BGP data?

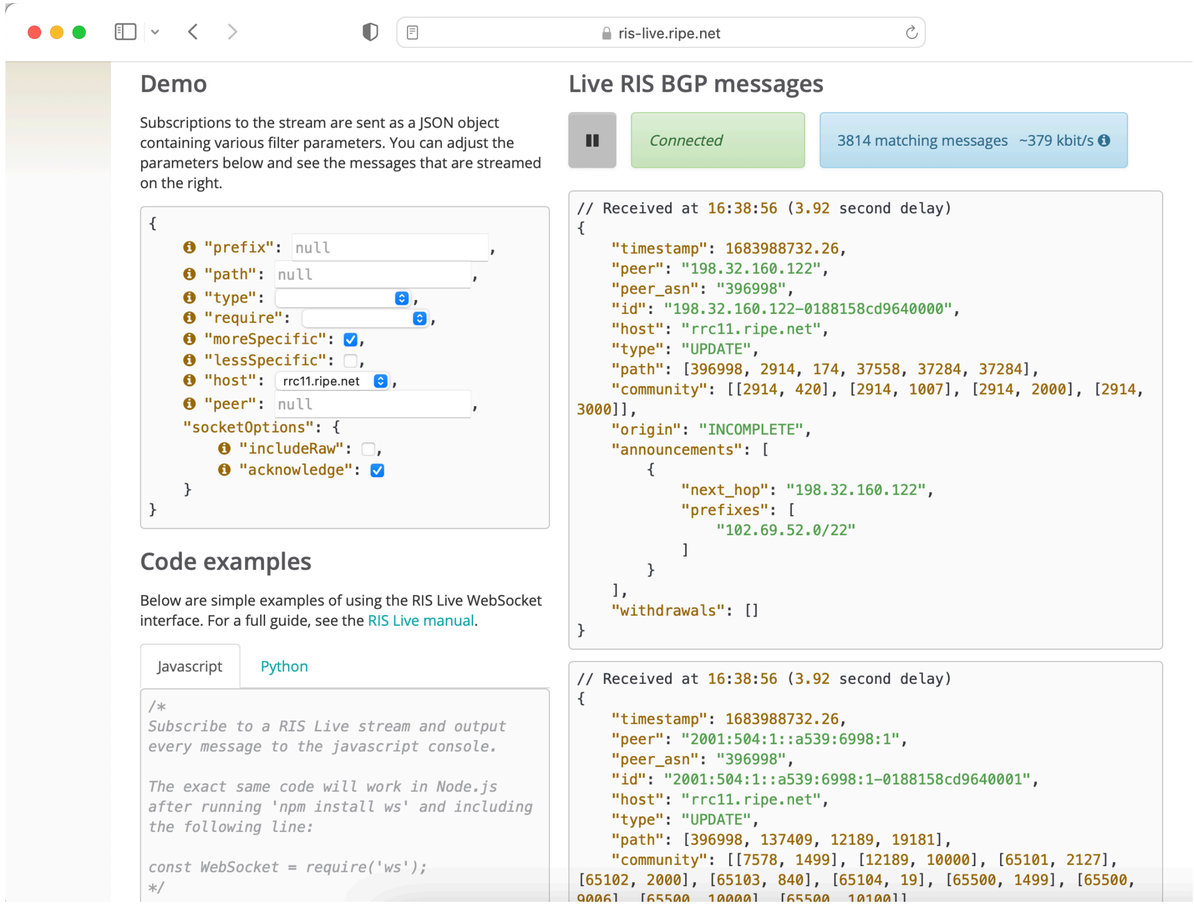
- BGP doesn’t have in-built security mechanisms and routing incidents are not rare
- Routing problems and Looking glasses are temporary
- BGP history is recorded to track what is happening and what has happened
- Better visibility → greater security → lower risk of a BGP attacks

Who is RIS for?

- Network operators, network policy makers
  - To check specific routes and routing incidents
  - To troubleshoot Internet routing
  - To develop future plans based on routing trends
- Researchers
  - To investigate notable events occurring in the Internet (i.e. network disruptions in specific countries, service outages, etc.)

How can you use RIS?

- Available as:
  - Raw data (archived MRT files)
  - Live stream – RIS Live
  - Whois query interface – RISwhois
  - Visualisations in RIPEstat



- Find more at ris.ripe.net

RIPE Atlas

RIPE Atlas

- RIPE Atlas is the RIPE NCC’s Internet measurement platform
- It is a global network of devices that actively measure Internet connectivity
- Anyone can access this data via Internet traffic maps, streaming data visualisations, and an API
- RIPE Atlas users can also perform customised measurements to gain information about their own networks

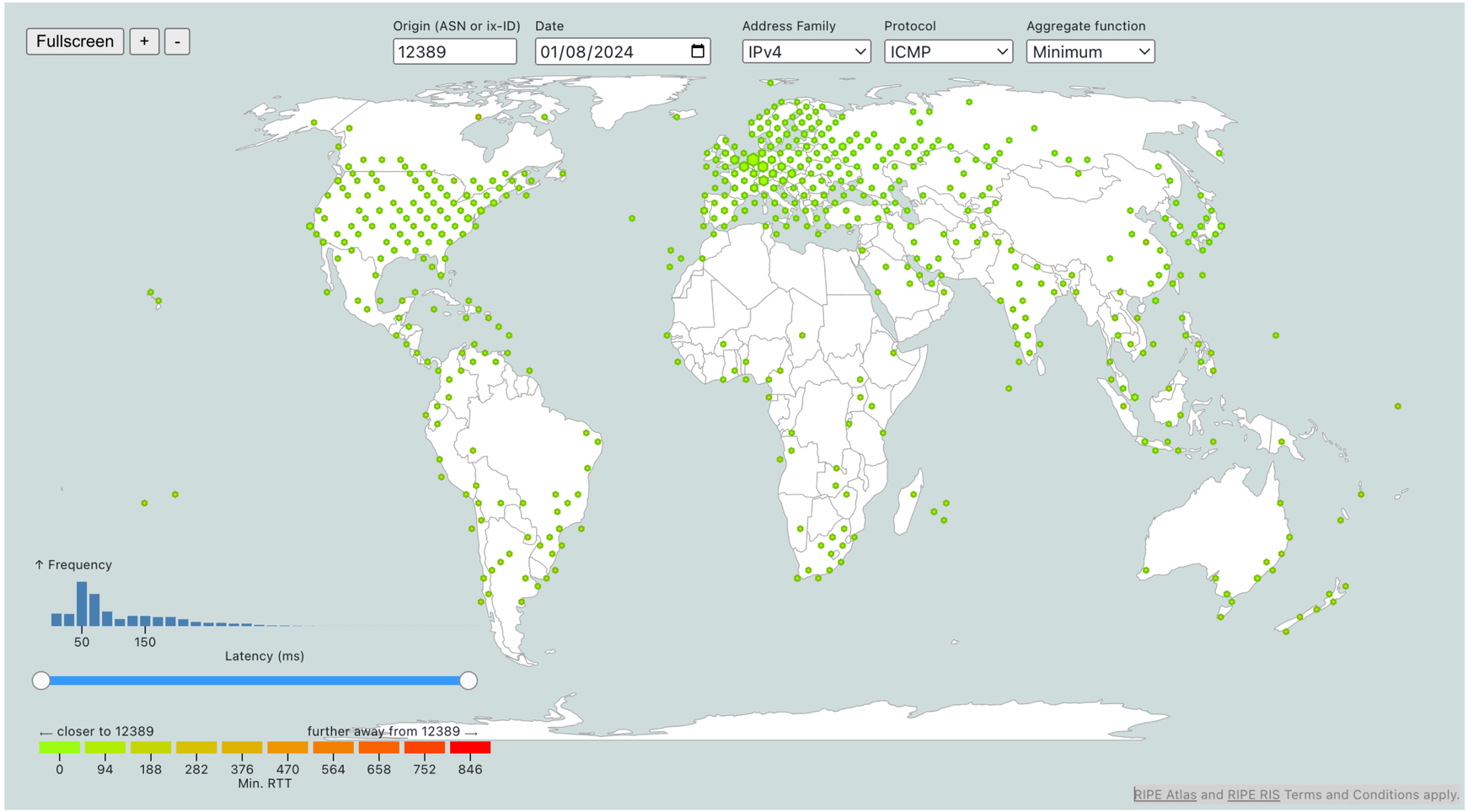
How we collect data?

- 12,000+ RIPE Atlas probes connected in 169 countries
- 787 RIPE Atlas Anchors
- 14,000+ results collected per second
- 33,000+ measurements currently running

What Can I Do With RIPE Atlas?

- RIPE Atlas customised measurements allow hosts and sponsors to conduct measurements on their own network(s) using other probes within the RIPE Atlas network:
  - Continuously monitor network reachability from thousands of vantage points around the globe
  - Investigate and troubleshoot network issues with quick, flexible connectivity checks
  - Create alarms using RIPE Atlas status checks, which work with your own monitoring tools
  - Check the responsiveness of DNS infrastructure, such as root name servers
  - Test IPv6 connectivity
- A complete collection of use cases, published research and analyses based on RIPE Atlas is published on RIPE Labs

Atlas Latency Map



https://observablehq.com/@ripencc/atlas-latency-worldmap

Case Studies

Detecting DNS Root Manipulation[1]

- **Issue:** In Nov 2021, hosts in Mexico couldn't reach whatsapp.net due to DNS query interception.
- **Cause:** Middleboxes in China, triggered by a route leak, intercepted DNS queries to a root server, sending incorrect responses.
- **Impact:** Outage lasted a week, affecting not just Mexico but also probes in the US, Europe, and Africa.Twitter SSL fetches failed across multiple networks in Turkey starting at 21:30 UTC, suggesting possible network interference.

Detecting DNS Root Manipulation

- Root servers should only provide zone referrals, not authoritative responses.
- An invalid response is identified if a root server returns an A or AAAA reply.
- Example in: shows a manipulated response (left) vs. a valid root server response (right).

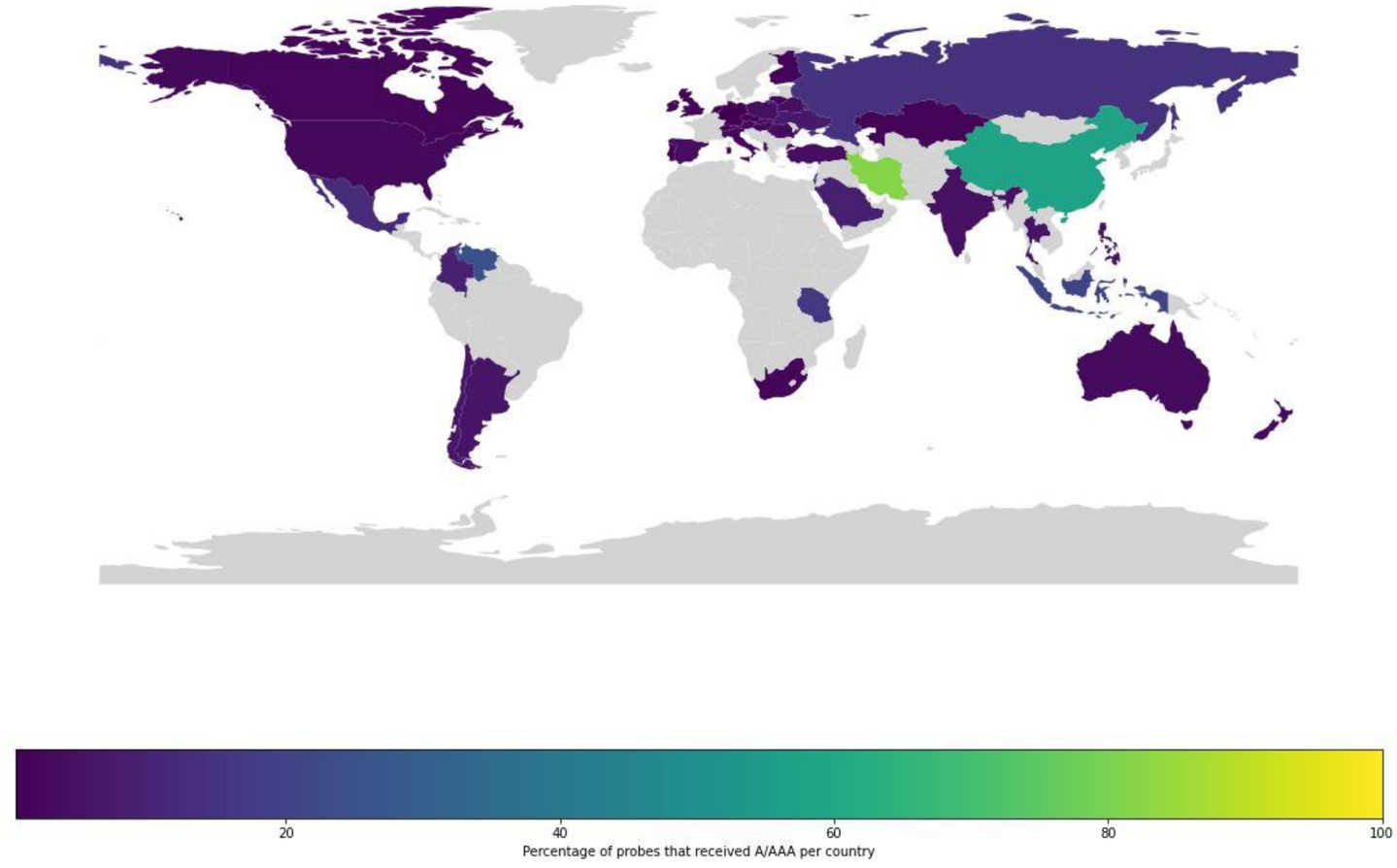
```
Probe #52013
================================================================================

- 1 -

  ; <<>> RIPE Atlas Tools <<>> facebook.com.
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52536
  ;; flags: aa qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

  ;; QUESTION SECTION:
  ;facebook.com.                  IN     A

  ;; ANSWER SECTION:
  facebook.com.           172     IN     A      67.228.235.91

  ;; Query time: 194.23 msec
  ;; SERVER: 2001:7fd::1#53(2001:7fd::1)
  ;; WHEN: Mon Apr 04 03:54:17 CEST 2022
  ;; MSG SIZE  rcvd: 46
```

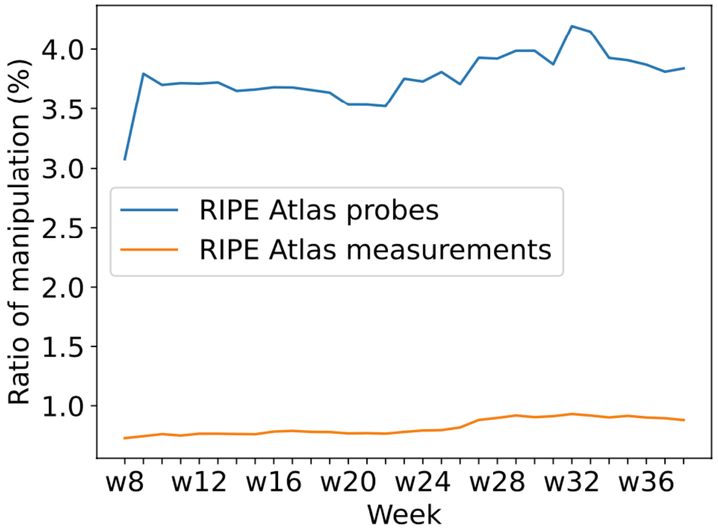
```
Probe #1000331
================================================================================

- 1 -

  ; <<>> RIPE Atlas Tools <<>> ripe.net.
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1840
  ;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 26

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 1232

  ;; QUESTION SECTION:
  ;ripe.net.                      IN     AAAA

  ;; AUTHORITY SECTION:
  net.                    172800  IN     NS     a.gtld-servers.net.
  net.                    172800  IN     NS     b.gtld-servers.net.
  net.                    172800  IN     NS     c.gtld-servers.net.
  net.                    172800  IN     NS     d.gtld-servers.net.
  net.                    172800  IN     NS     e.gtld-servers.net.
  net.                    172800  IN     NS     f.gtld-servers.net.
  net.                    172800  IN     NS     g.gtld-servers.net.
  net.                    172800  IN     NS     h.gtld-servers.net.
  net.                    172800  IN     NS     i.gtld-servers.net.
  net.                    172800  IN     NS     j.gtld-servers.net.
  net.                    172800  IN     NS     k.gtld-servers.net.
  net.                    172800  IN     NS     l.gtld-servers.net.
  net.                    172800  IN     NS     m.gtld-servers.net.

  ;; ADDITIONAL SECTION:
  a.gtld-servers.net.     172800  IN     A      192.5.6.30
  b.gtld-servers.net.     172800  IN     A      192.33.14.30
  c.gtld-servers.net.     172800  IN     A      192.26.92.30
  d.gtld-servers.net.     172800  IN     A      192.31.80.30
  e.gtld-servers.net.     172800  IN     A      192.12.94.30
  f.gtld-servers.net.     172800  IN     A      192.35.51.30
  g.gtld-servers.net.     172800  IN     A      192.42.93.30
  h.gtld-servers.net.     172800  IN     A      192.54.112.30
  i.gtld-servers.net.     172800  IN     A      192.43.172.30
  j.gtld-servers.net.     172800  IN     A      192.48.79.30
  k.gtld-servers.net.     172800  IN     A      192.52.178.30
  l.gtld-servers.net.     172800  IN     A      192.41.162.30
  m.gtld-servers.net.     172800  IN     A      192.55.83.30
  a.gtld-servers.net.     172800  IN     AAAA   2001:503:a83e:0:0:0:2:30
  b.gtld-servers.net.     172800  IN     AAAA   2001:503:231d:0:0:0:2:30
  c.gtld-servers.net.     172800  IN     AAAA   2001:503:83eb:0:0:0:0:30
  d.gtld-servers.net.     172800  IN     AAAA   2001:500:856e:0:0:0:0:30
  e.gtld-servers.net.     172800  IN     AAAA   2001:502:1ca1:0:0:0:0:30
  f.gtld-servers.net.     172800  IN     AAAA   2001:503:d414:0:0:0:0:30
  g.gtld-servers.net.     172800  IN     AAAA   2001:503:eea3:0:0:0:0:30
  h.gtld-servers.net.     172800  IN     AAAA   2001:502:8cc:0:0:0:0:30
  i.gtld-servers.net.     172800  IN     AAAA   2001:503:39c1:0:0:0:0:30
  j.gtld-servers.net.     172800  IN     AAAA   2001:502:7094:0:0:0:0:30
  k.gtld-servers.net.     172800  IN     AAAA   2001:503:d2d:0:0:0:0:30
  l.gtld-servers.net.     172800  IN     AAAA   2001:500:d937:0:0:0:0:30
```

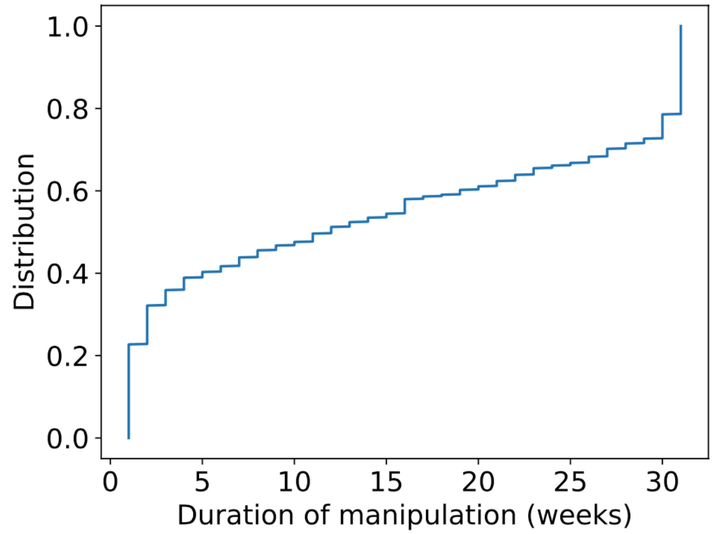
Detecting DNS Root Manipulation

- Collected data using 312 non-recursive DNS measurements, conducted twice daily from ~11,000 RIPE Atlas probes.
- Directed queries to all root server letters (a-m).
  - Alternated between IPv4 and IPv6, UDP and TCP, multiple types (e.g., A, AAAA).
  - Targeted domain names: facebook.com, google.com, and ripe.net.
- Categorized responses into two groups:
  - **Non-injected:** Empty answer section, expected referral to .com/.net TLD nameservers.
  - **Injected:** Received unexpected responses, despite root servers not being authoritative for the queried domains.

Detecting DNS Root Manipulation







DNS Censorship (DNS Lies) As Seen By RIPE Atlas[3]

- DNS is essential for connecting to services, making it a prime target for censorship.
- Censorship often targets DNS resolvers, altering responses for control or commercial reasons.
- RIPE Atlas probes are valuable for analyzing DNS behavior globally, particularly useful in detecting censorship.
- Probes can be directed at specific resolvers or use the default resolver indicated by local network settings.

```
% python resolve-name.py --country=CN --requested=30 www.facebook.com
Measurement #3048986 for www.facebook.com/A uses 8 probes
[1.2.3.4] : 1 occurrences
[59.24.3.173] : 1 occurrences
[159.106.121.75] : 5 occurrences
Test done at 2015-11-28T13:44:17Z
```

```
% python resolve-name.py --country=FR --requested=100 romecasino.com
Measurement #3049070 for romecasino.com/A uses 100 probes
[217.19.248.132] : 64 occurrences
[ERROR: SERVFAIL] : 6 occurrences
[ERROR: NXDOMAIN] : 11 occurrences
[127.0.0.1] : 15 occurrences
Test done at 2015-11-28T14:14:27Z
```

```
% python resolve-name.py --country FR t411.io
Measurement #3049724 for t411.io/A uses 500 probes
[ERROR: SERVFAIL] : 41 occurrences
[104.24.124.37 104.24.125.37] : 187 occurrences
[ERROR: NXDOMAIN] : 43 occurrences
[127.0.0.1] : 197 occurrences
[146.112.61.106] : 2 occurrences
Test done at 2015-11-29T16:04:34Z
```

Internet Access Disruption In Turkey - July 2016[2]

- User-initiated measurements for Twitter and Facebook showed anomalies.
- Twitter SSL fetches failed across multiple networks in Turkey starting at 21:30 UTC, suggesting possible network interference.
- SSL fetches timing out after five seconds could indicate either blocking or severe throttling; the exact cause remains undetermined.

Conclusions

- Network disruptions can stem from device issues, ISP failures, or network congestion, making stable connectivity challenging.
- BGP (RIS) provides essential control plane data for troubleshooting routing issues and enhancing network security.
- RIPE Atlas offers data plane measurements, giving global insight into network performance and detecting anomalies like DNS manipulation.
- Explore labs.ripe.net for case studies showcasing how BGP (RIS) and RIPE Atlas data are used to analyze and understand network disruptions.

References

- [1] https://labs.ripe.net/author/qasim-lone/detecting-dns-root-manipulation/
- [2] https://labs.ripe.net/author/stephane_bortzmeyer/dns-censorship-dns-lies-as-seen-by-ripe-atlas/
- [3] https://labs.ripe.net/author/emileaben/internet-access-disruption-in-turkey-july-2016/

Questions

qlone@ripe.net