Fantastic network tools and where to find them

Ben Cartwright-Cox (bgp.tools) @ EPF 2023

Who/What/Where?

- There is a lot of data out there to help you figure out
  - Who networks are
  - Where they may be physically present for interconnection
  - What they are hosting
  - Who they are already peering with
  - Getting traceroutes
  - Real time looking glasses

- However these resources are poorly documented

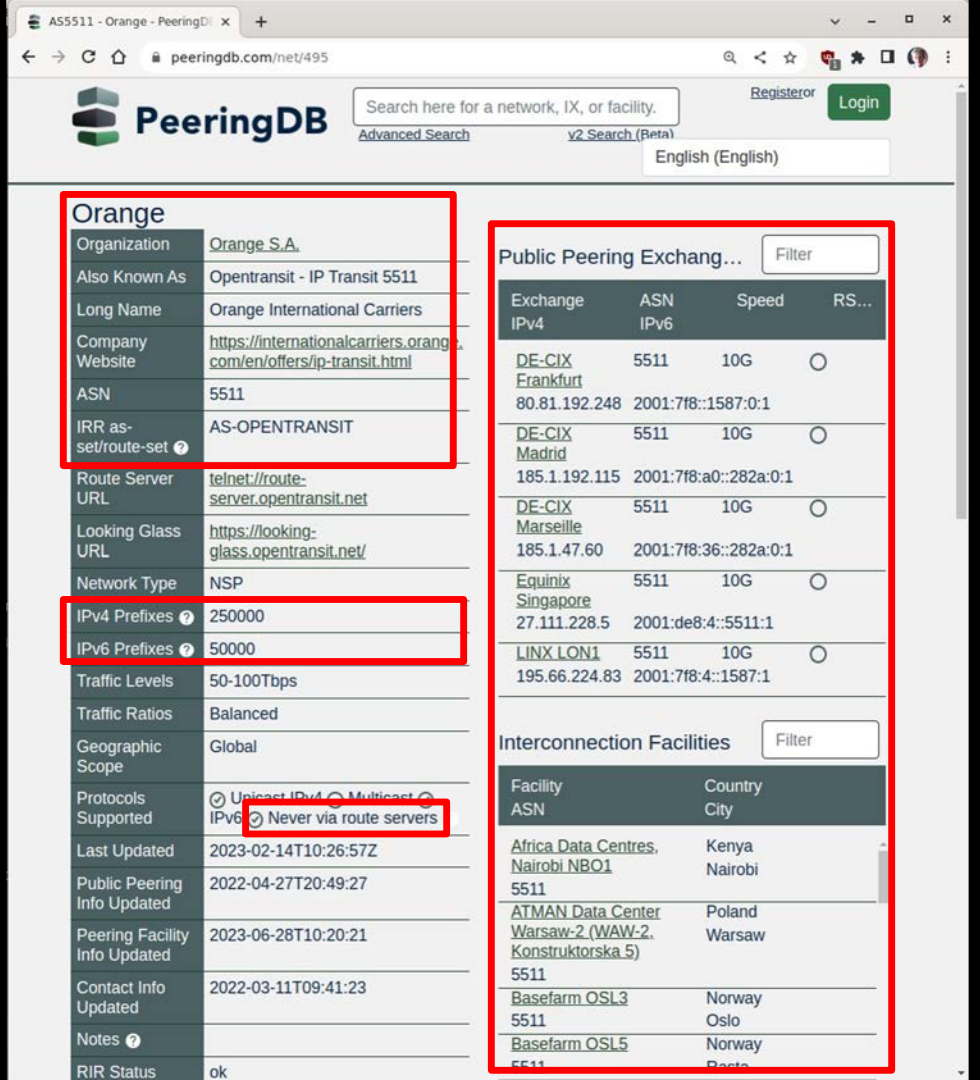
Quick intro/Full disclosure

- I run bgp.tools
  - The bgp.tools guy will at some point tell you to use bgp.tools
  - I am also more than happy to mention what might be considered competitors
  - Most of these non-bgp.tools utilities I still use anyway to cross check my own data, or just fill in gaps in my own product

- Still, the bgp.tools guy will tell you to use bgp.tools, there is a minor conflict of interest here.

Core data sources

- PeeringDB might be the most fundamental data sources around BGP networking, providing easy access to
  - Name (That may be better than the AS Name)
  - Max Prefixes number / AS-SET
  - IXPs that **they list** as being members of
  - Listing of physical locations to interconnect
  - Contact data for peering/NOC departments
- Lots of sites use PeeringDB data in their own operations
  - Easy to obtain API keys can be used for automation or local copies of the database:
  - https://www.peeringdb.com/apidocs/



Core data sources

- RIPE NCC has run for a very long time a set of route collectors on mostly IXPs to collect BGP data. As part of the "Routing Information Service" (RIS)
- This data can be very useful to look back historically, But there are **no point and click tools** to decode MRT files
- RIS also provides a real time "RIS Live" offering, that provides streaming JSON data of BGP updates
- RIS also comes with a JSON API that will return current machine routes for a prefix
- RIS forms the backbone is stat.ripe.net

Core data sources

- RIPE NCC has run for a very long time a set of route collectors on mostly IXPs to collect BGP data. As part of the "Routing Information Service" (RIS)
- This data can be very useful to look back historically, But there are **no point and click tools** to decode MRT files
- RIS also provides a real time "RIS Live" offering, that provides streaming JSON data of BGP updates
- RIS also comes with a JSON API that will return current machine routes for a prefix
- RIS forms the backbone is stat.ripe.net


```
{
  "messages": [],
  "see_also": [],
  "version": "2.1",
  "data_call_name": "looking-glass",
  "data_call_status": "supported",
  "cached": false,
  "data": {
    "rrcs": [
      {
        "rrc": "RRC00",
        "location": "Amsterdam, Netherlands",
        "peers": [
          {
            "asn_origin": "13335",
            "as_path": "34854 1299 13335",
            "community": "1299:30000 34854:3001",
            "last_updated": "2023-08-01T01:55:29",
            "prefix": "1.1.1.0/24",
            "peer": "2.56.11.1",
            "origin": "IGP",
            "next_hop": "2.56.11.1",
            "latest_time": "2023-08-14T13:11:39"
          },
```

Core data sources

- Route Views is a similar project to RIS run by the University of Oregon
- Exporting similar data to MRT files
  - Their archives go back to early 2000's
- Bonus of Route Views is that they have telnet servers that still *(mostly)* work as looking glasses

- RIS and Routeviews combined make up the majority of the data backing up academic literature on BGP

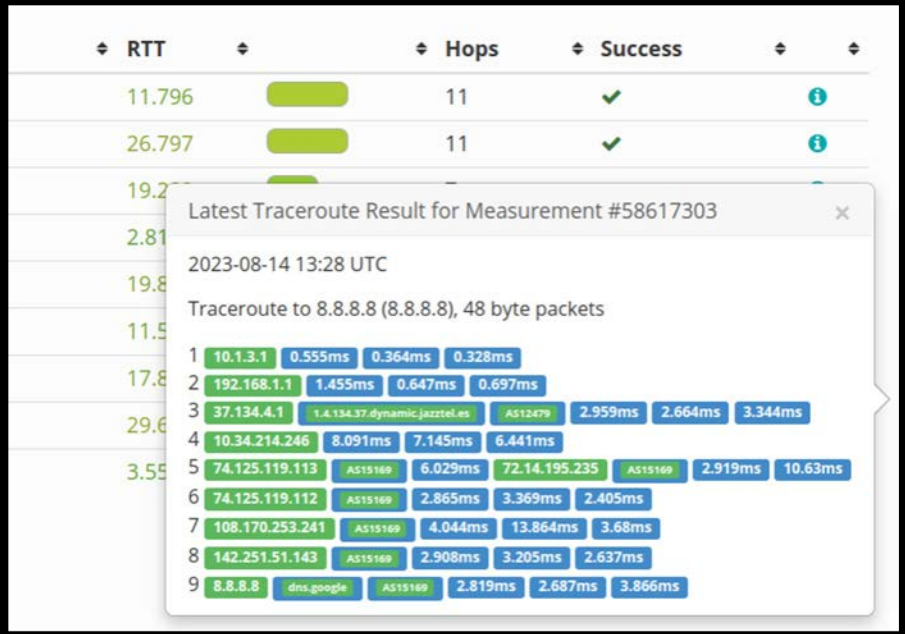
```
$ telnet route-views.chicago.routeviews.org
Trying 64.136.227.34...
Connected to route-views.chicago.routeviews.org.
Escape character is '^]'.

Hello, this is FRRouting (version 8.4.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

route-views.chicago.routeviews.org> show ip bgp 1.1.1.0/24
BGP routing table entry for 1.1.1.0/24, version 217828253
Paths: (17 available, best #7, table default)
  Not advertised to any peer
  32709 19754 13335, (aggregated by 13335 141.101.74.12)
    208.115.136.134 from 208.115.136.134 (63.134.128.248)
      Origin IGP, valid, external, rpki validation-state: valid
      Community: 19754:200
      Last update: Tue Jul 11 18:33:03 2023
  53828 13335, (aggregated by 13335 141.101.73.17)
    208.115.136.180 from 208.115.136.220 (207.200.192.81)
      Origin IGP, valid, external, rpki validation-state: valid
      Community: 13335:10014 13335:19000 13335:20050 13335:20500
13335:20530 53828:11 53828:1001
      Last update: Fri Jun 30 05:58:44 2023
  199524 13335, (aggregated by 13335 141.101.73.17)
    208.115.136.42 from 208.115.136.42 (10.255.18.65)
      Origin IGP, valid, external, rpki validation-state: valid
      Last update: Thu Jun 29 14:29:17 2023
  13335, (aggregated by 13335 141.101.73.17)
```

Traceroute debugging

RIPE Atlas

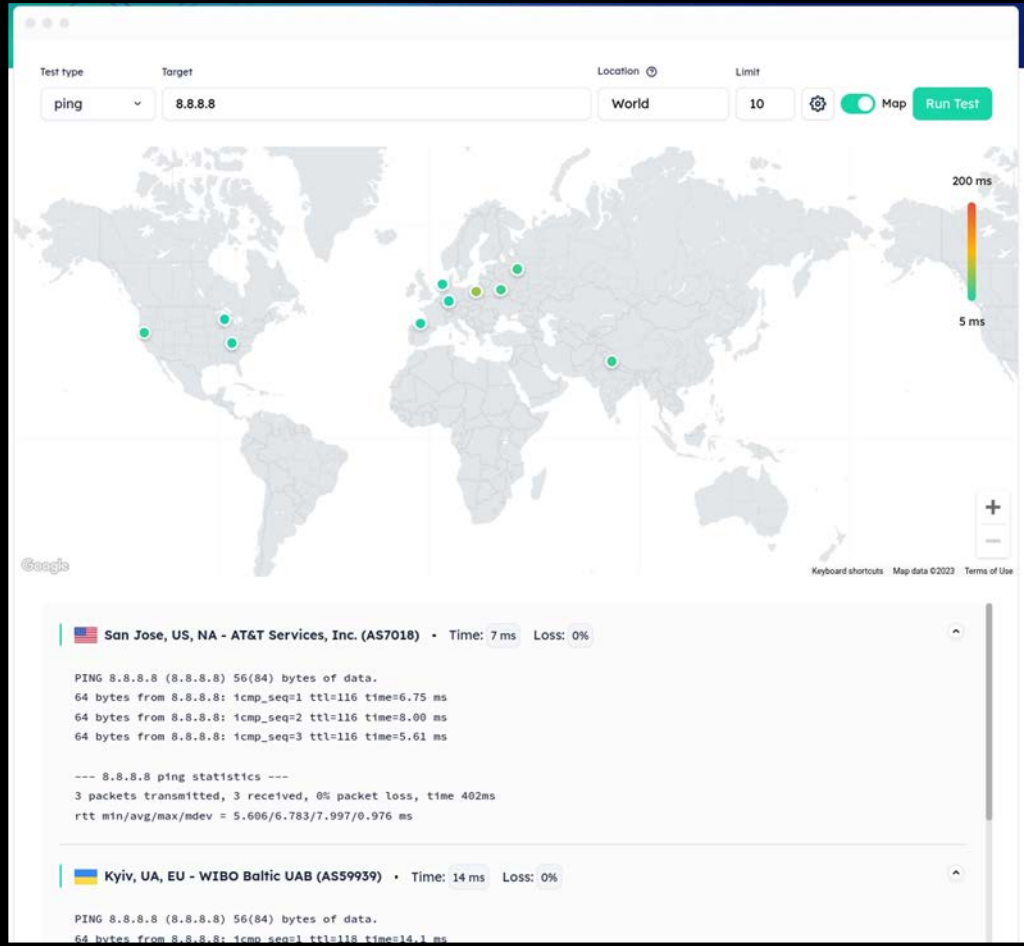
- Likely in the past when debugging problems you might have wished for a traceroute from the problematic network
- Getting traceroutes from normal people is hard (or sometimes even their NOC)
- There are tools out there with small to large networks that can do these traceroutes for you

- RIPE Atlas is by far the biggest, has a huge % of "eyeball" networks, and works on credits gained by either being a RIPE LIR or running at Atlas probe yourself.
- (You can also ask someone who has credits to give you some)



Traceroute debugging

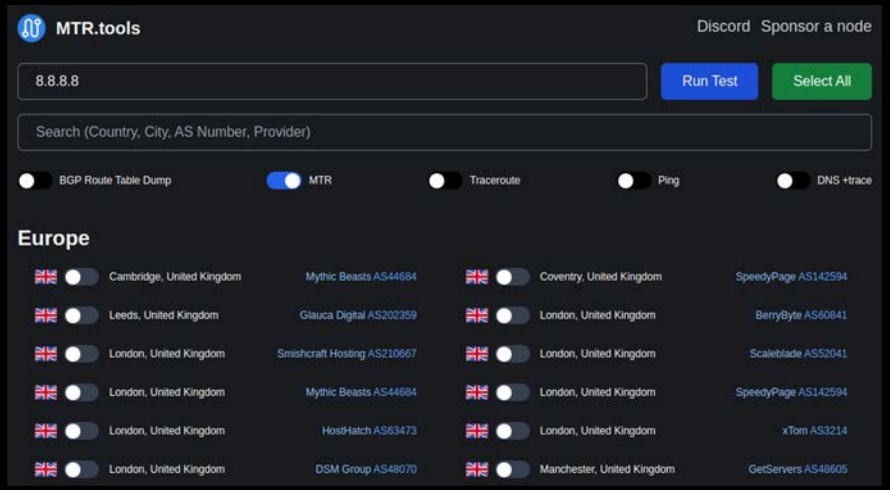
- GlobalPing is like RIPE Atlas, but with fewer "probes" (500~ vs 12,000+)
  - Most probes are on content networks in my experience
- However has a much more functional front end!
- Functional API available too, with (currently) free API keys, unclear future
- Very useful tool for a 2nd opinion or if RIPE Atlas is down/you have no Atlas credits.
- You can join their probe network by pulling a docker container

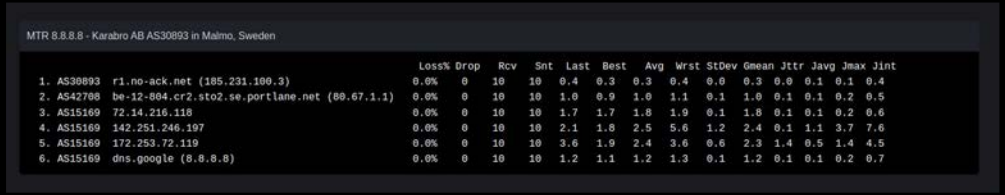


Traceroute debugging

- https://mtr.tools
  - Not affiliated with me, despite the similar name
- Hobbyist run, 150 nodes, all testing points are content providers
- Website offers traceroutes, pings, BGP route lookups, and DNS lookups

- Site is responsive and has worked every time I tried.



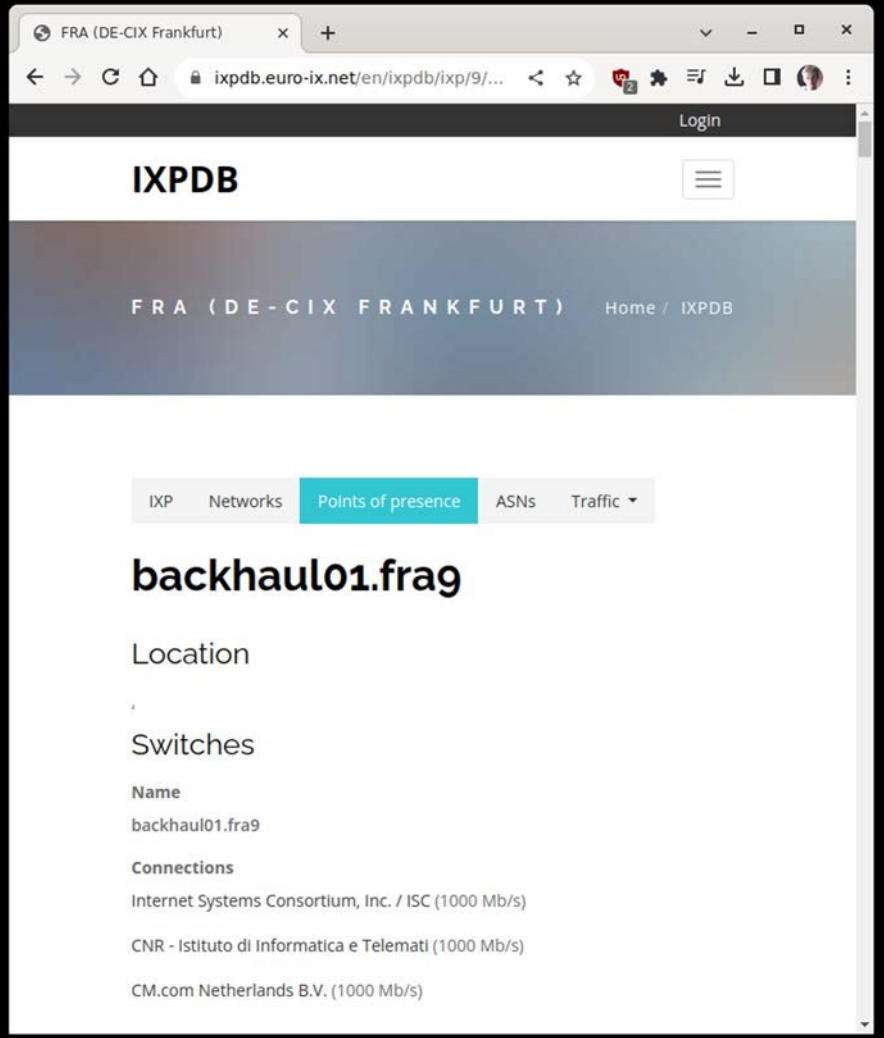


IXP Data debugging

- IXPDB by Euro IX
  - https://ixpdb.euro-ix.net
- A useful site within a niche, All data is from IX-F feeds provided by IXPs

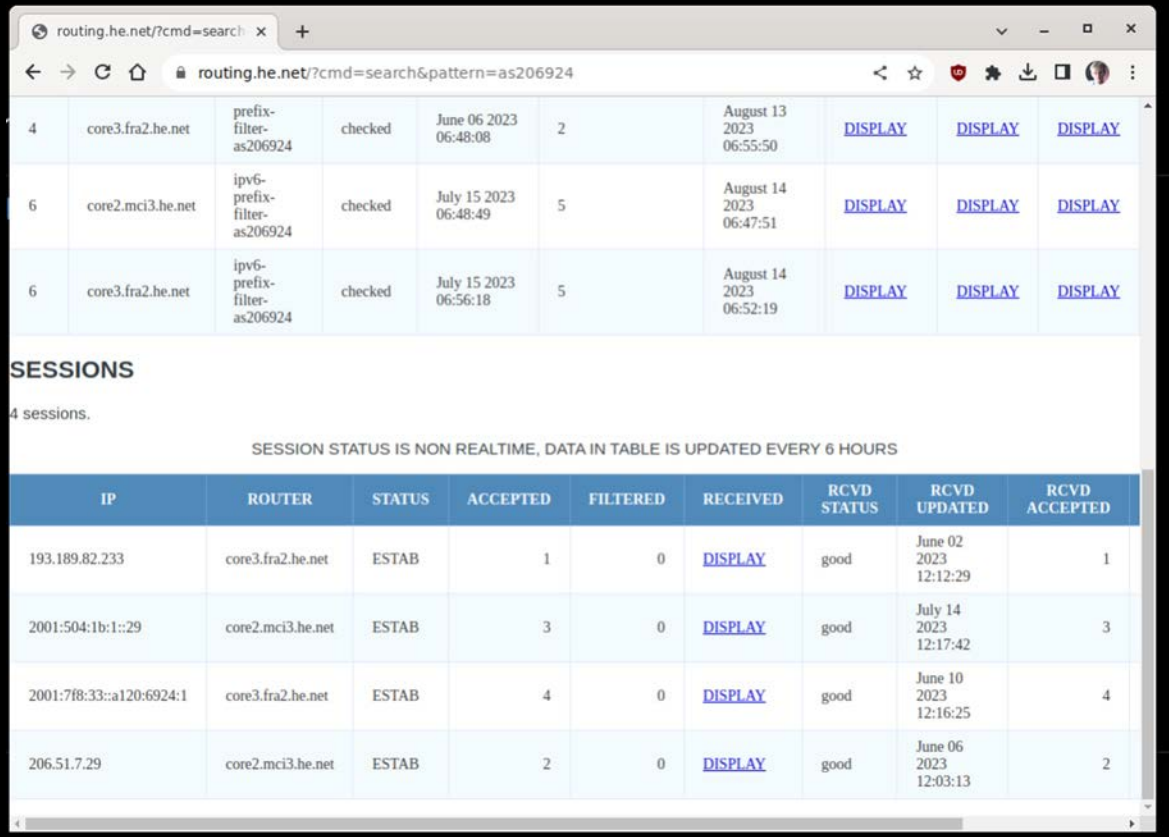
- Not a PeeringDB competitor, but useful if you want to easily see IXP switch info, or for networks who don't list themselves on PeeringDB

- If you are IXP, Please add your IX-F feed to IXPDB so other tools can pick it up too!



Useful carrier tools

- AS6939 routing.he.net provides very useful (non realtime) debugging info for peering matters with HE.
- You can lookup any ASN
- You can see what prefixes they are seeing, what sessions there are configured, and what filters they have generated for you.
- You can also see why they have rejected some prefixes from their filters



4	core3.fra2.he.net	prefix-filter-as206924	checked	June 06 2023 06:48:08	2	August 13 2023 06:55:50	DISPLAY	DISPLAY	DISPLAY
6	core2.mci3.he.net	ipv6-prefix-filter-as206924	checked	July 15 2023 06:48:49	5	August 14 2023 06:47:51	DISPLAY	DISPLAY	DISPLAY
6	core3.fra2.he.net	ipv6-prefix-filter-as206924	checked	July 15 2023 06:56:18	5	August 14 2023 06:52:19	DISPLAY	DISPLAY	DISPLAY

SESSIONS

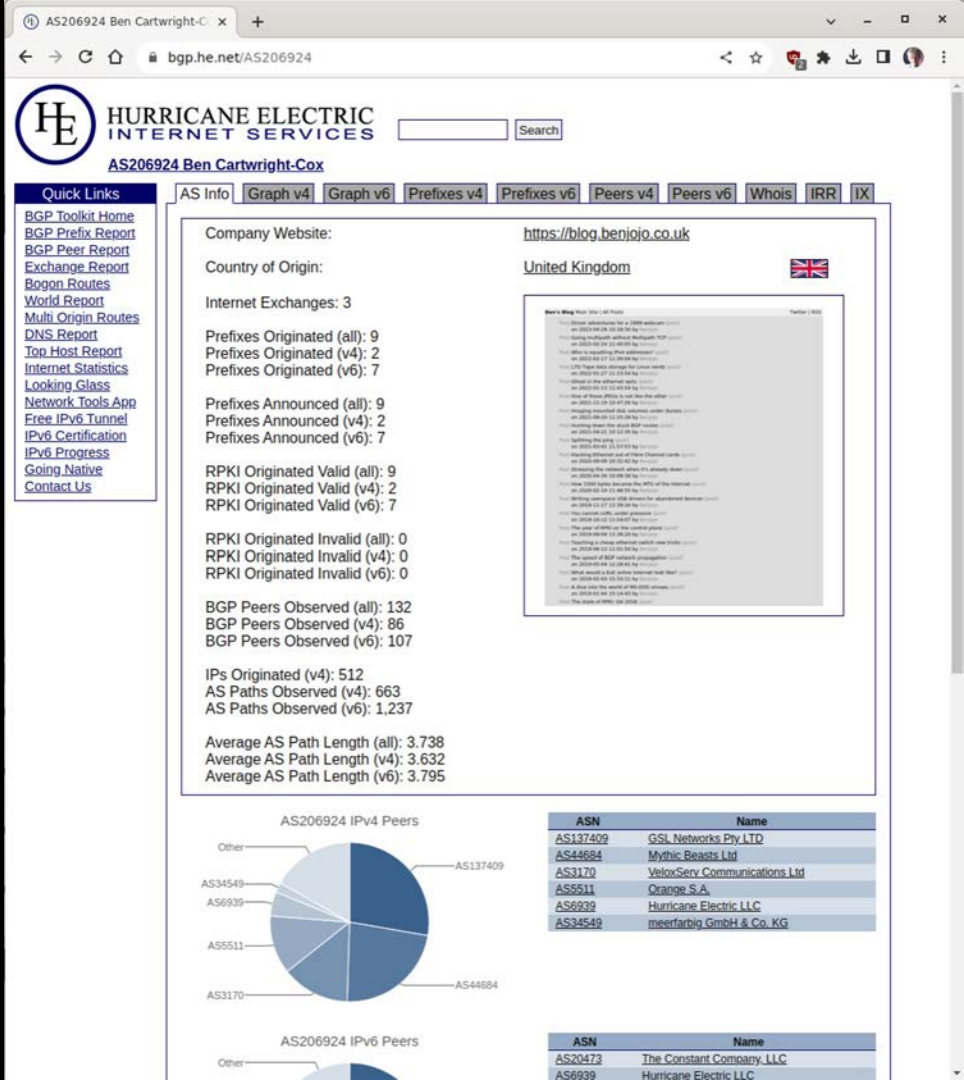
4 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS UPDATED EVERY 6 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED
193.189.82.233	core3.fra2.he.net	ESTAB	1	0	DISPLAY	good	June 02 2023 12:12:29	1
2001:504:1b:1::29	core2.mci3.he.net	ESTAB	3	0	DISPLAY	good	July 14 2023 12:17:42	3
2001:7f8:33::a120:6924:1	core3.fra2.he.net	ESTAB	4	0	DISPLAY	good	June 10 2023 12:16:25	4
206.51.7.29	core2.mci3.he.net	ESTAB	2	0	DISPLAY	good	June 06 2023 12:03:13	2

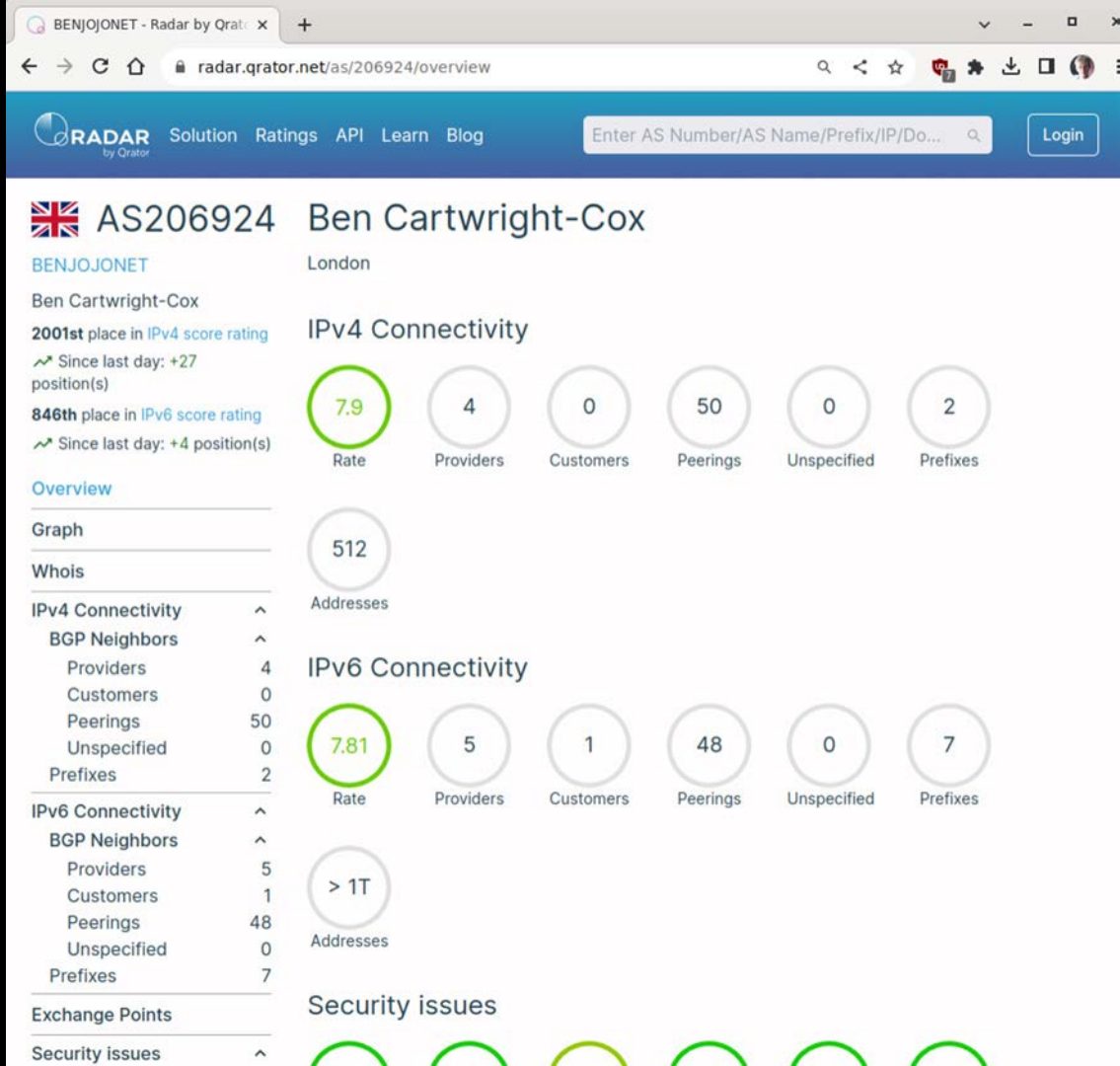
Useful aggregator tools

- AS6939 bgp.he.net provides very useful (non realtime) internet information
- Lots of features including:
  - Peering status (based on RIS/RV/HE data)
  - Prefix + Whois info
  - ccTLD + gTLD name server data
  - The "Exchange report" on the top N IXP participants
  - Far too many smaller features to list, the site has a huge depth to it
- Data is refreshed every ~24 hours



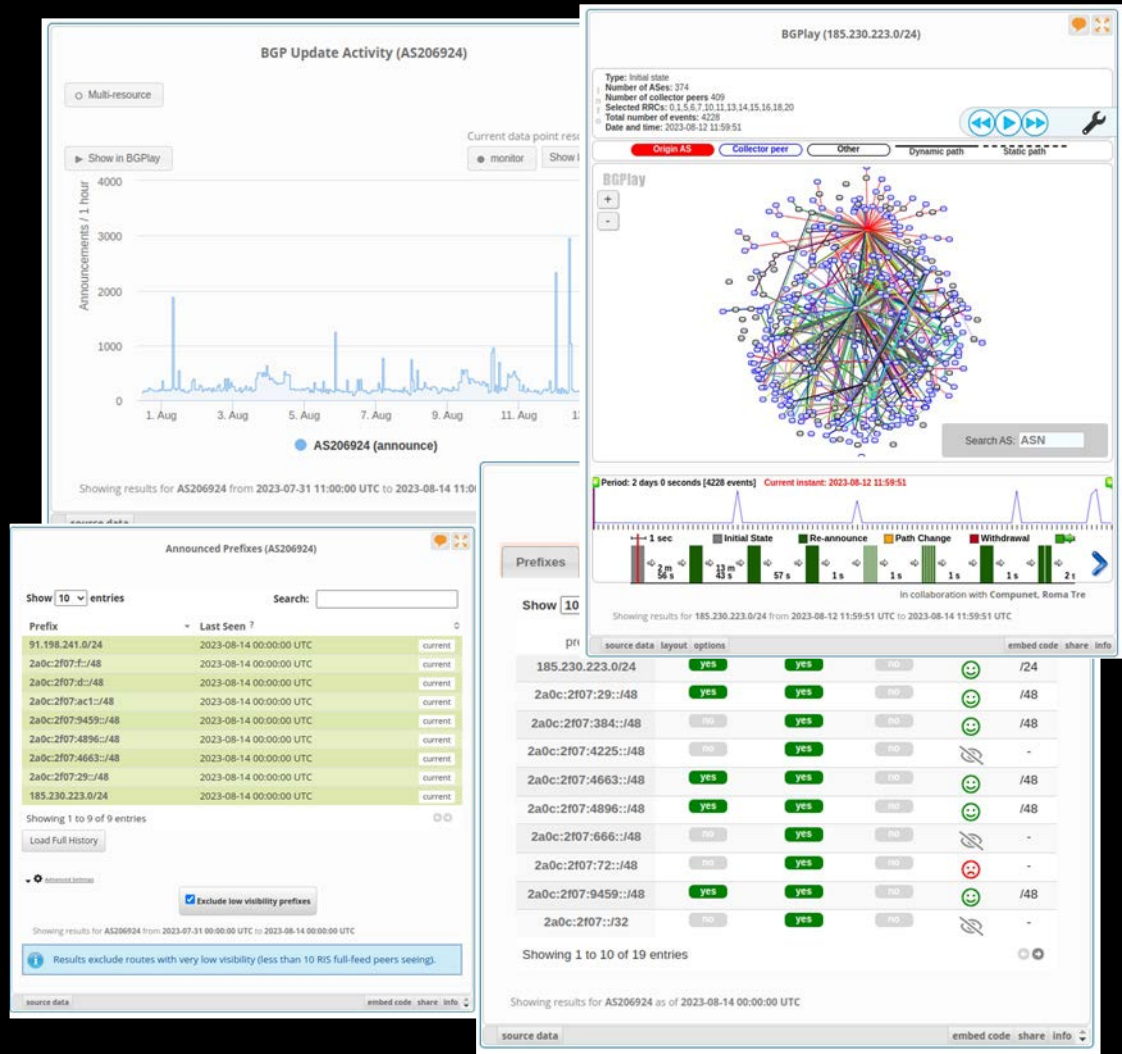
Useful aggregator tools

- https://radar.qrator.net
- Run by Qrator (A DDoS mitigation/BGP Monitoring company)
- Realtime-ish(?) data
- Strong focus on "Security Issues"
  - Listing endpoints in your network that are exploitable to amplification attacks
  - Listing suspected route leaks
- Global rankings for connectivity



Useful aggregator tools

- https://stat.ripe.net/ui2013/
- Run by RIPE NCC
- The entire kitchen sink (some useful, some weird) of data tools
- I find the new UI unusable, but the old UI is still available
- Lots of information, some is realtime-ish, some are dubious
- Standout features:
  - Geolocation debugging
  - BGPPlay
  - RIS activity graphs
  - IP Space transfer history



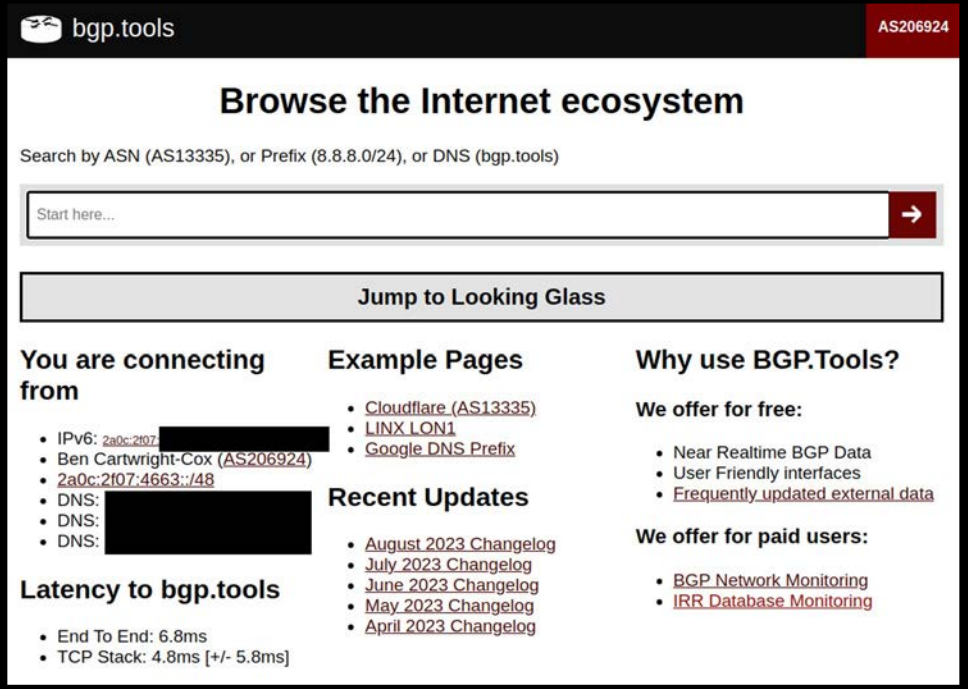
Aggregator tools honorable mentions

- https://radar.cloudflare.com/
  - Has some RIPE Stat like BGP data, but the interesting/unique data is derived from Cloudflare's own traffic data (You can use this to see countrywide internet blackouts)
- https://bgpview.io/
  - Seemingly unmaintained now, was a very useful tool from around 2015-2019 but parts of the site is now broken, was a good bgp.he.net style site
- https://asrank.caida.org/
  - Ranks website based on a ranking algorithm, quite popular with the sales people of the higher ranking networks on the site! Developed by the University of San Diego (CAIDA)

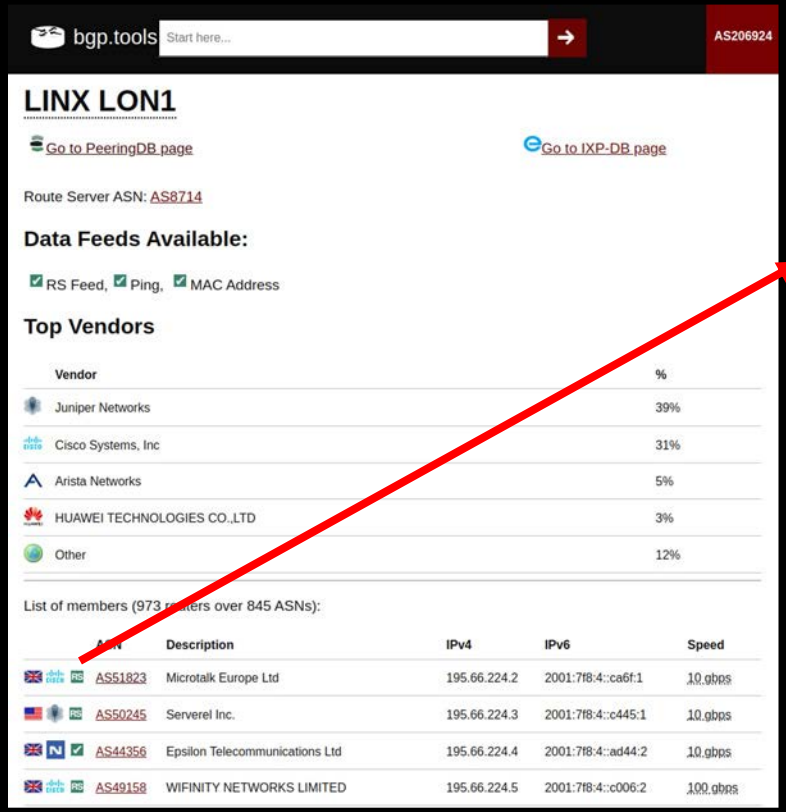
Bgp.tools (The speakers aggregator tool)

- Setup in 2018 due to frustrations with the existing aggregator sites
- Performs many of the same functions as the rest of the offerings with a focus on:
  - Fast page response times
  - Realtime as much as possible data
  - Creative data extraction from things
- The site now sustains its own operating costs by selling BGP/IRR monitoring/Managed Looking Glass (and other products still in the works)

- The site uses its own BGP collector as it's bgp data source



Bgp.tools (The speakers aggregator tool) [IXP Data]



Where bgp.tools has BGP collectors, you can see who is sending what to the route servers!

For many IXPs you can also see the vendor (based on mac address) a peer is using!

Bgp.tools (The speakers aggregator tool) [AS Info]

View Prefixes / Peers/Upstreams/ Downstreams / IXP Ports etc

Submit Corrections

Query their BGP sessions with bgp.tools, or use their RIPE Atlas probes from the site

See a listing of their known BGP Communities

Look at their downstream networks

Bgp.tools (The speakers aggregator tool) [Prefix Info]

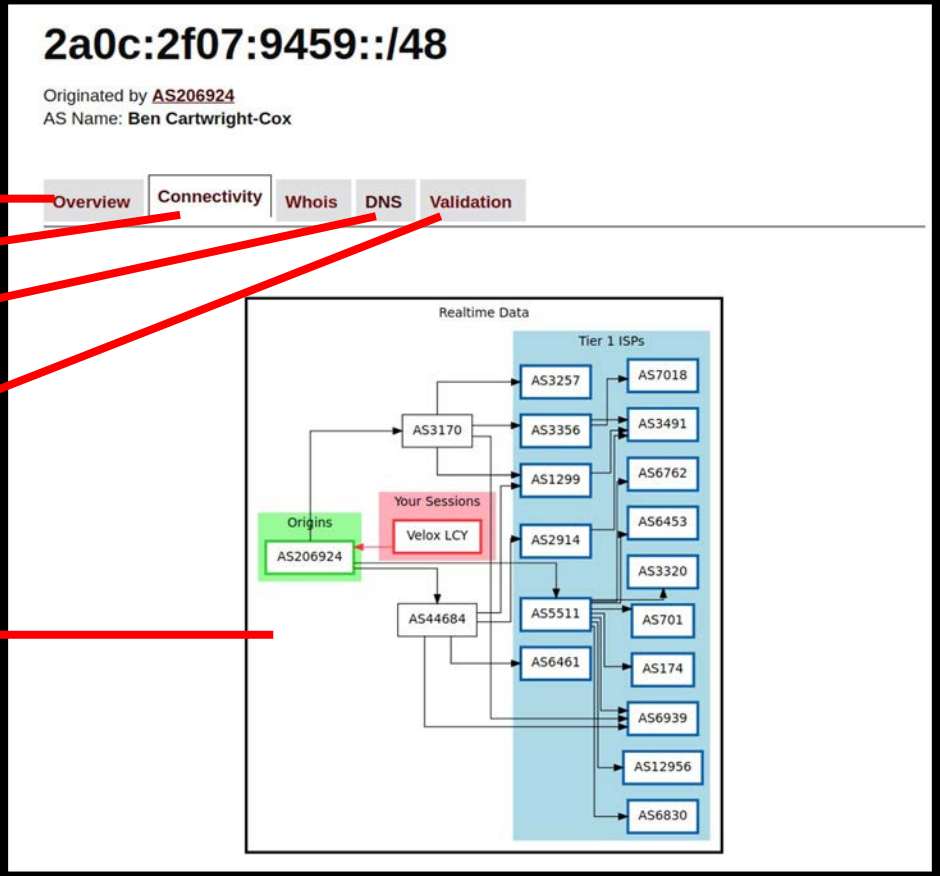
General prefix registration info

Peers/Upstreams for the prefix

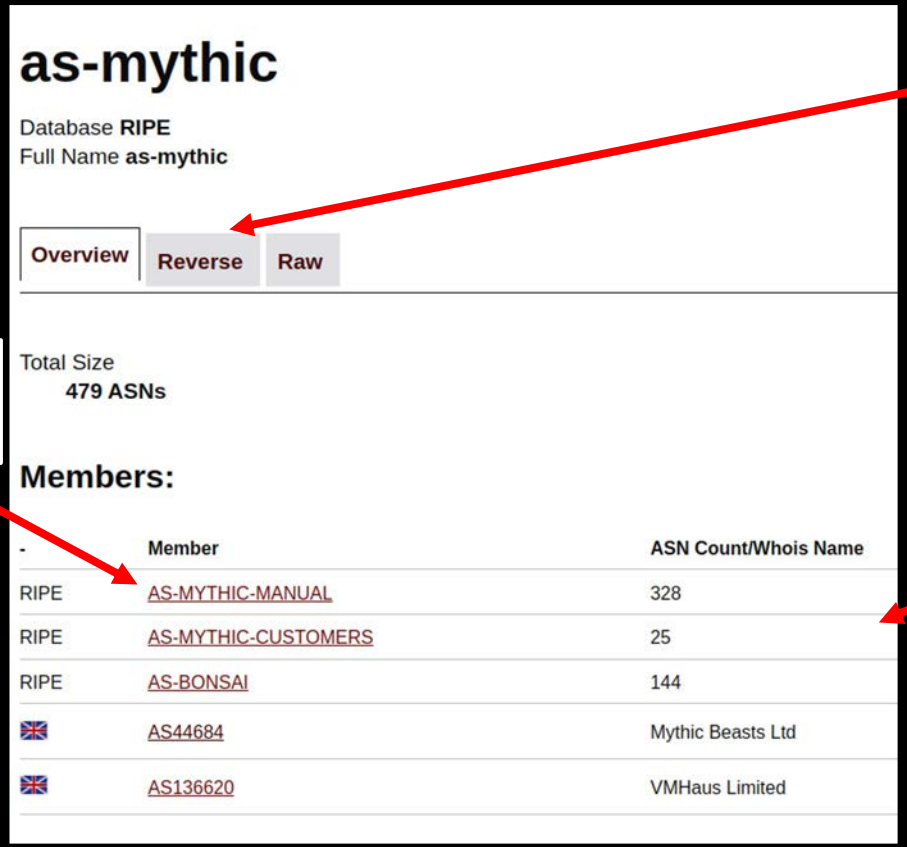
Reverse DNS + DNS records that point to IPs inside the prefix

IRR debug data, "Raw" RPKI Certificate debugging information

Auto updating "map" of how the prefix propagates



Bgp.tools (The speakers aggregator tool) [AS-SET]



See who includes this AS-SET in their AS-SET!

Handles AS-SET naming conflicts

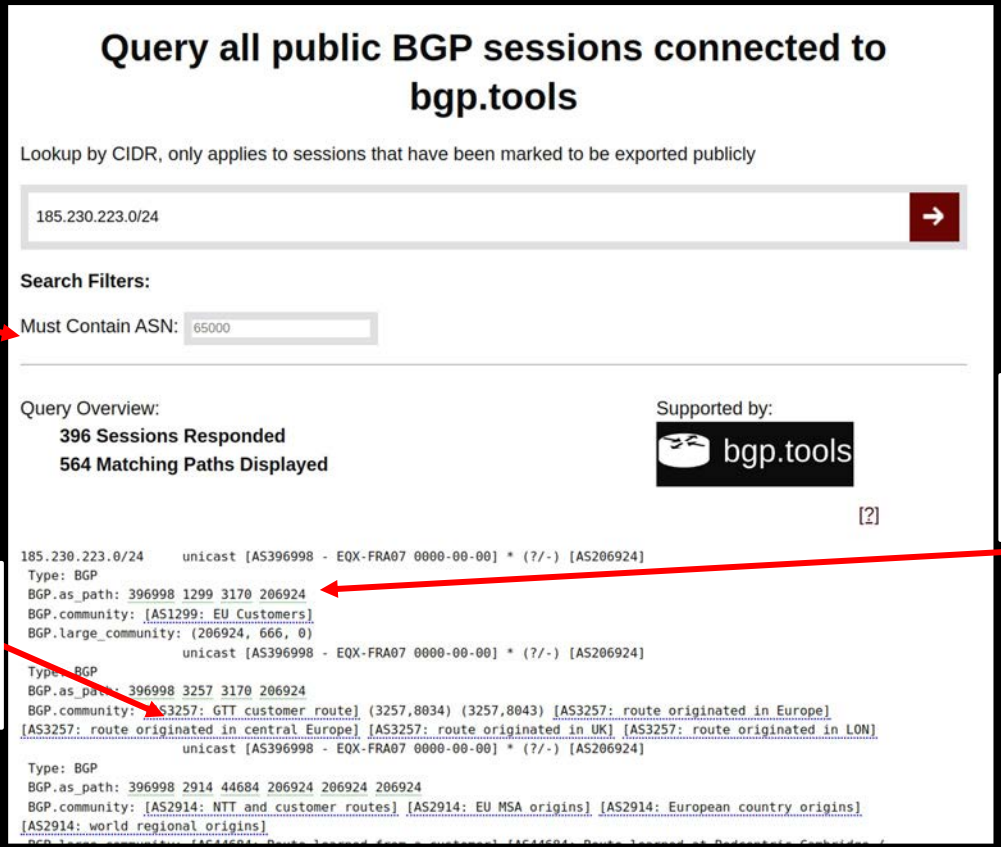
Member AS-SET's are recursively resolved to calculate true size

Bgp.tools (The speakers aggregator tool) [Looking Glass]

Ability to look for a ASN of interest in the path

BGP Communities are automatically decoded into readable sentences

You can hover over ASN numbers for their names to appear



Bgp.toc ss]

Ben Cartwright-Cox

AS Number **206924**

BGP | Ping/Traceroute | RIPE Atlas

Select BGP Session to query:

All Sessions

Input Prefix:

2600::

-

Query

```
2600::/48           unicast [Velox LCY 0000-00-00] * (?/-) [AS1239]
 Type: BGP
 BGP.as_path: 206924 60945 3257 1239
 BGP.community: (3257,8048) (3257,30176) [AS3257: route originated in Europe] [AS3257:
route originated in UK] [AS3257: route originated in LON] (60945,0) (60945,3257)
[AS206924: Learned from Transit]
                    unicast [Mythic CBG 0000-00-00] * (?/-) [AS1239]
 Type: BGP
 BGP.as_path: 206924 44684 1299 1239
 BGP.community: [AS1299: North American Peers] [AS206924: Learned from Transit]
 BGP.large_community: [AS44684: Route learned from transit] [AS44684: Route learned at
```

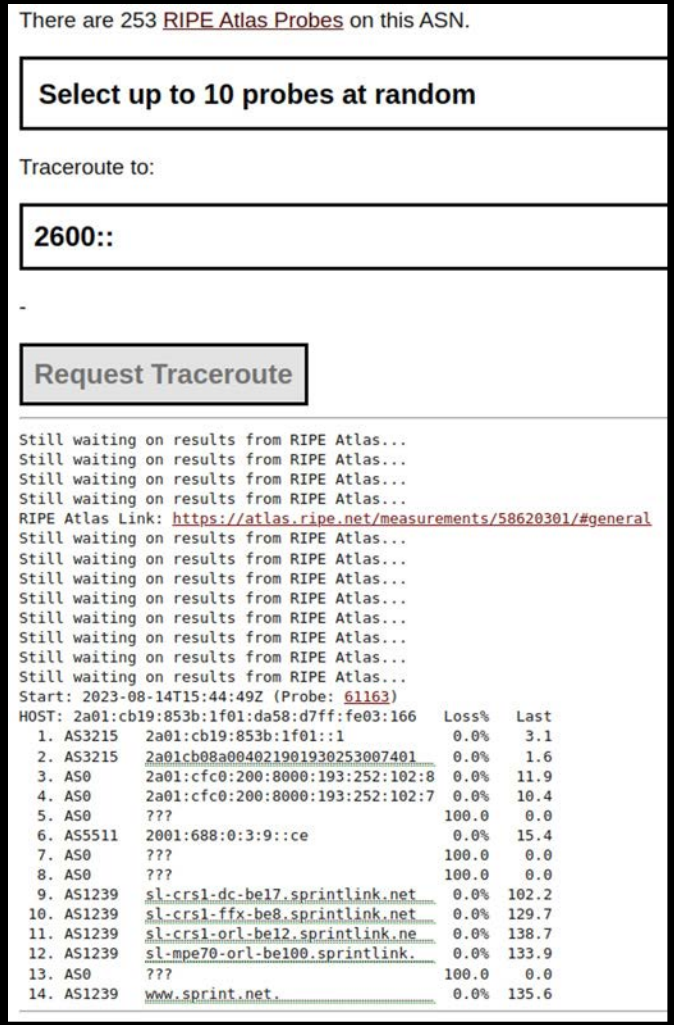
Ability to look for
of interest in the

BGP Communiti
automatically de
into readable se

over over ASN
for their names

bgp.tools RIPE Atlas Front End

- If you are logged in, and pair a RIPE Atlas API key with your account, you can use bgp.tools as a front end for RIPE Atlas!
- Providing you single click "MTR" style traceroutes from any ASN with probes on it
- It also automatically updates, handles RIPE Atlas unreliability, and provides faster results (to the user, since you don't have to keep reloading for results) than using the RIPE atlas interface itself



</promo>

(Sorry)

How you (yes, you) can help the internet

- A lot of the BGP route collectors are still underserved in many regions.
- You can help by feeding them wherever possible.
- Here are the links to setup sessions:

Service	Instant Signup	URL
RIPE	No (IXP+Multihop)	https://www.ris.ripe.net/cgi-bin/peerreg.cgi
RouteViews	No (IXP+Multihop)	https://www.routeviews.org/routeviews/index.php/peering-request-form/
bgp.tools	Yes (IXP+Multihop)	https://bgp.tools/kb/setup-sessions
Radar	Yes (Multihop)	https://radar.qrator.net/ (Login to account, in settings)

IXP Route Collection

IXP	RIS	RouteViews	bgp.tools
DE-CIX	JNB	FRA	All
LINX LON1 / LONAP	Yes	Yes	Yes
AMS-IX	Yes	Yes	No
France-IX	Yes	Yes	No
Equinix	Singapore/Miami/ Palo Alto	Singapore, US, Sydney	No
MIX-IT	Yes	Yes	No
IX.BR	Yes	Yes	Soon?
ASN:	12654	6447	212232

Questions?

Obvious things that I left out?

Email for out of band comments: epf@benjojo.co.uk