Avoiding insanity while trying to untangle the internet

Ben Cartwright-Cox
@ LU-CIX - Nov 16th 2022

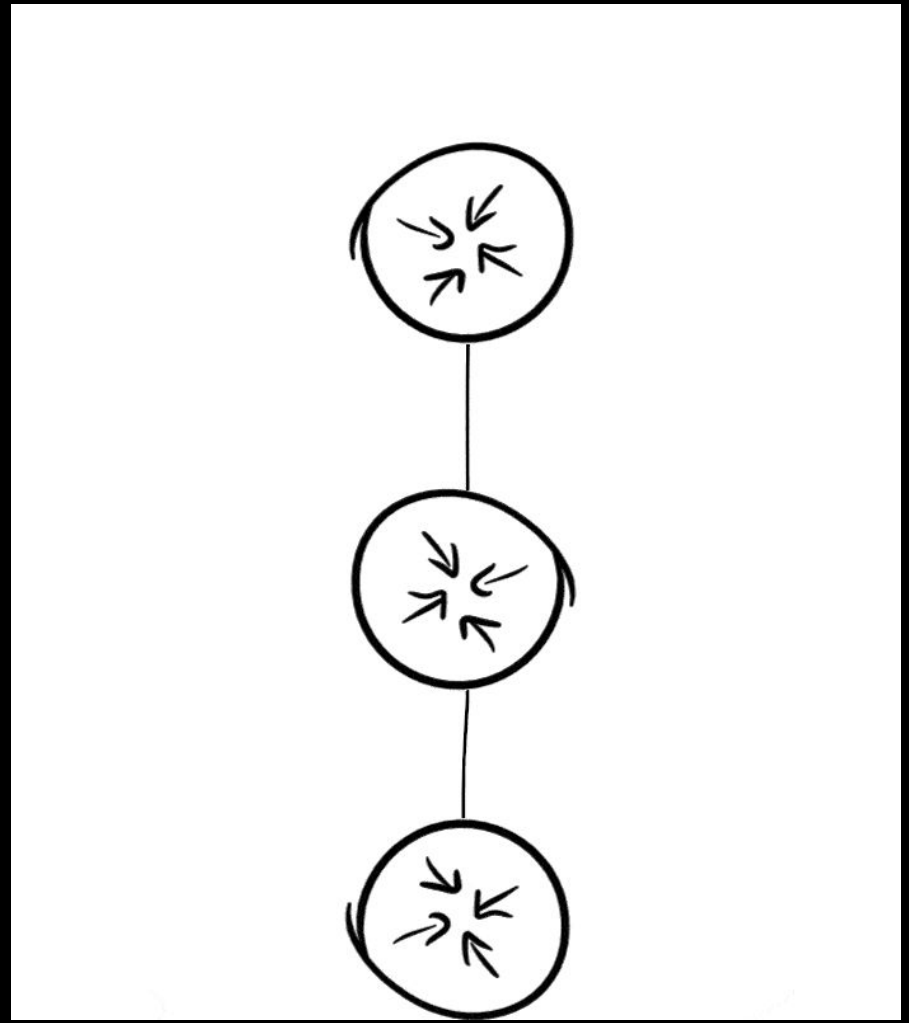
cda6ee3890045c20ade67418f5e35588

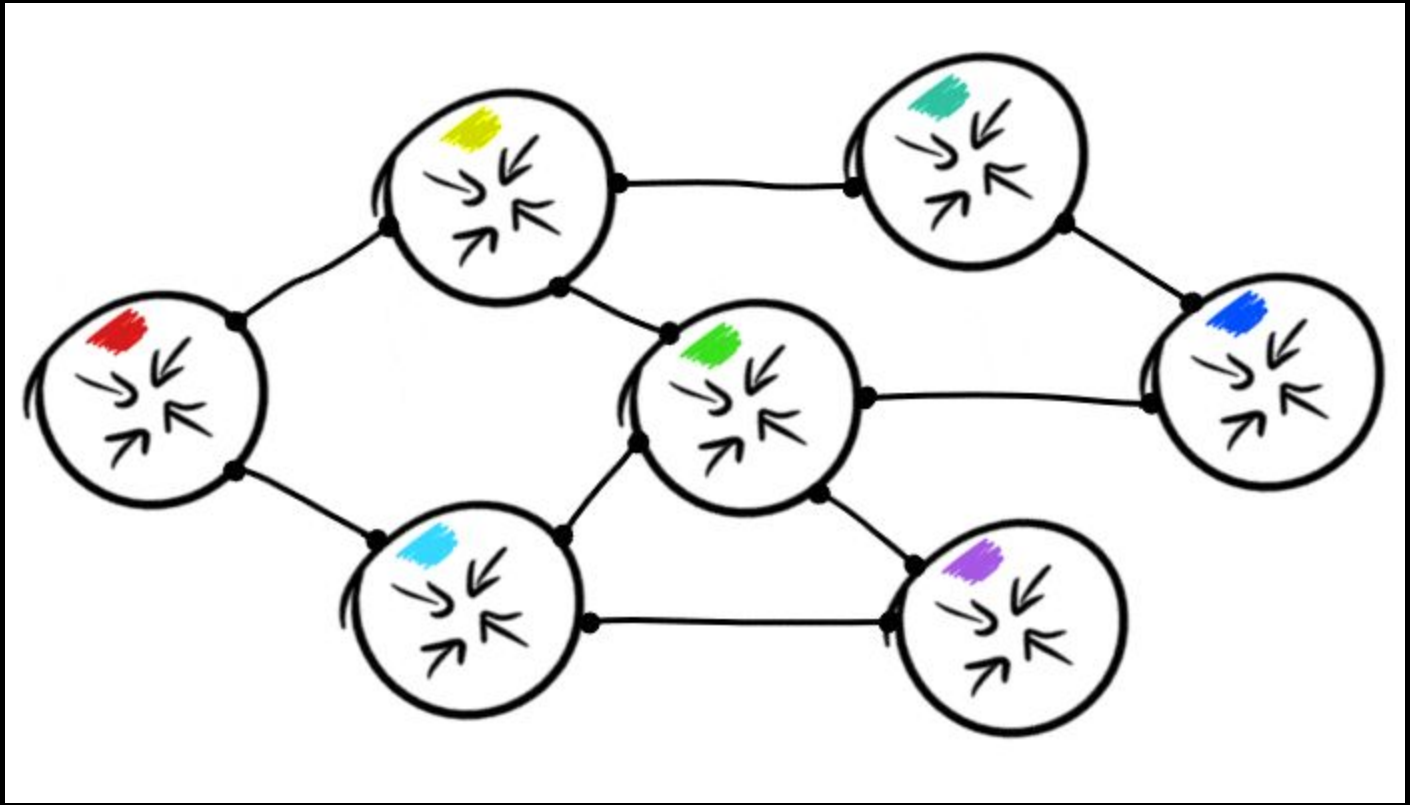
Can we take a moment to appreciate what humanity built?

cda6ee3890045c20ade67418f5e35588

Can we take a moment to appreciate what humanity built?

cda6ee3890045c20ade67418f5e35588





cda6ee3890045c20ade67418f5e35588

```
+|62.193.131.0/24|28917 13004 6700|195.208.208.147|i|||28917:4000 28917:4100 28917:4103|195.208.208.147 28917|1667136299|1
+|84.237.71.0/24|28917 9049 25549 25549 30797|195.208.208.147|i|||28917:3000|195.208.208.147 28917|1667136299|1
-|213.145.128.0/24|                          |               | |||          |195.208.210.40 6939|1667136297|1
```

	Prefix	AS Path	Next Hop	BGP Communities	Data Source / ASN		
+	62.193.131.0/24	28917 13004 6700	195.208.208.147	i | | | 28917:4000 28917:4100 28917:4103	195.208.208.147 28917	1667136299	1
+	84.237.71.0/24	28917 9049 25549 25549 30797	195.208.208.147	i | | | 28917:3000	195.208.208.147 28917	1667136299	1
-	213.145.128.0/24			| | |	195.208.210.40 6939	1667136297	1

Prefix AS Path Next Hop BGP Communities Data Source / ASN

```
route-views.amsix.routeviews.org> show bgp ipv4 185.230.223.0/24
BGP routing table entry for 185.230.223.0/24
Paths: (27 available, best #13, table default)
  Not advertised to any peer
  211398 34854 44684 206924
    185.1.167.45 from 185.1.167.45 (31.24.249.245)
      Origin IGP, valid, external
      Community: 34854:1001 65500:10000 65500:10100 65532:1000
      Large Community: 44684:0:900 44684:1:2 44684:2:206924 44684:3000:1299 211398:245:100 211398:2760245:34854
      Last update: Sun Oct 30 01:17:05 2022
  39120 3356 3170 206924
    80.249.210.28 from 80.249.210.28 (195.60.190.29)
      Origin IGP, valid, external, atomic-aggregate
      Community: 3356:2 3356:22 3356:100 3356:123 3356:500 3356:901 3356:2064 60945:0 65002:6830 65532:1000
      Last update: Sat Oct 29 08:33:29 2022
```

BGP Implicitly encodes so much extra information

- Routing around expensive providers
  - You can observe when some carriers become uncompetitive over time
- Routing around physical issues
  - Recent de-prefing of some ISPs during the recent Marseille cuts
- Routing around with politics in mind
  - North Korea brought up a 2nd upstream (Russia) after suspected tensions(?) with China
- Literally routing stuff into blackholes with *Politics* in mind

cda6ee3890045c20ade67418f5e35588

Via bgpmon

```
show router bgp routes 8.8.8.8
===============================================================================
BGP Router ID:212.156.116.127 AS:9121 Local AS:9121
===============================================================================
Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best, b - backup

===============================================================================
BGP IPv4 Routes
===============================================================================
Flag Network LocalPref MED
Nexthop Path-Id VPNLabel
As-Path
-------------------------------------------------------------------------------
u*>? 8.8.8.8/32 100 None
212.156.253.130 None -
No As-Path
*? 8.8.8.8/32 100 None
212.156.253.130 None -
No As-Path
-------------------------------------------------------------------------------
Routes : 2
===============================================================================
```

We would expect to see 8.8.8.0/24 here originated by AS 15169.
This is the proof of Turk Telekom hijacking Google DNS.

Via bgpmon

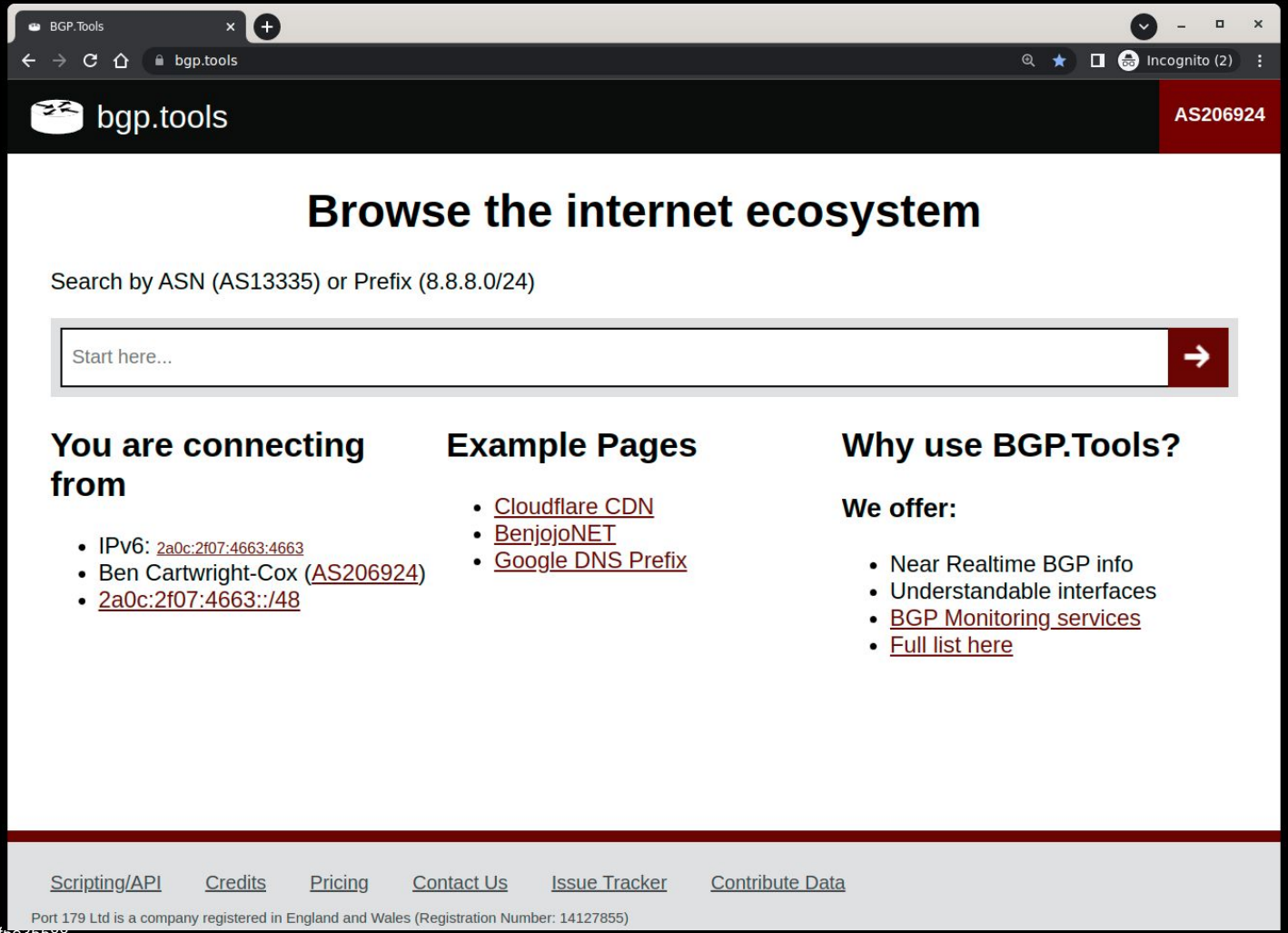
```
show router bgp routes 8.8.8.8
===============================================================================
BGP Router ID:212.156.116.127 AS:9121 Local AS:9121
===============================================================================
Legend -
Status codes : u
Origin codes : i

===============================================================================
BGP IPv4 Routes
===============================================================================
Flag Network Loc
Nexthop Path-Id
As-Path
-------------------------------------------------------------------------------
u*>? 8.8.8.8/32
212.156.253.130
No As-Path
*? 8.8.8.8/32 10
212.156.253.130
No As-Path
-------------------------------------------------------------------------------
Routes : 2
===============================================================================
```

cda6ee3890045c20ade67418f5e35588

BGP data in aggregate is far more interesting

Est Apr 2018

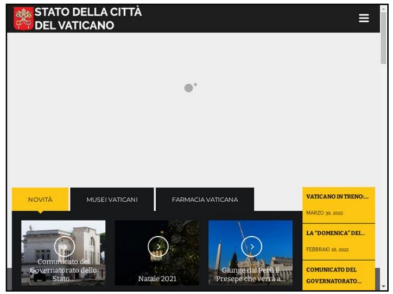


cda6ee3890045c20ade67418f5e35588

Start here...

Logged in as AS206924

View | Edit



Holy See - Vatican City State

AS Number **8978**

Website **http://www.vaticanstate.va**

Overview | Prefixes | Connectivity | Whois

Overview | Prefixes | Connectivity | Whois | IX

Registered on
9 Apr 2002 (20 years old)

Network status
Active, Allocated under RIPE

Network type
Unknown

Prefixes Announced
2 IPv4, 1 IPv6

Upstreams

- AS174 - Cogent Communications
- AS3356 - Lumen (Level 3)
- AS3257 - GTT Communications Inc.
- AS137 - Consortium GARR
- AS12874 - Fastweb SpA
- AS12637 - Seeweb s.r.l.

Locations of Operation

- Holy See (Vatican City State)
- Italy

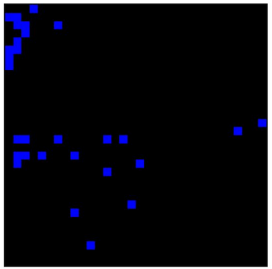
Tags:

bgp.tools/prefix/193.4

Start here...

Logged in as AS206924

View | Edit



193.43.128.0/22

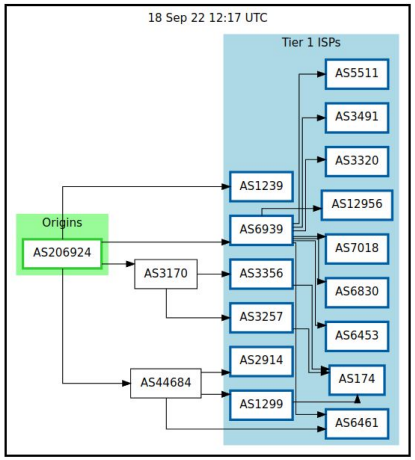
Announced by **AS8978**

Overview | Connectivity | Whois | DNS | Validation

cda6ee3890045c20ade67418f5e35588

Networks are broken up into policies

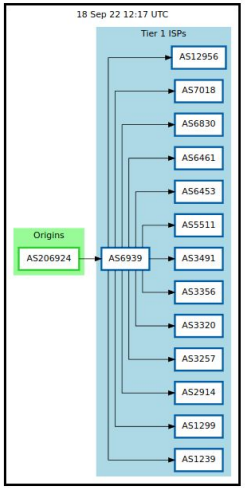
Policy blissful_hoover



Prefixes in selected policy

-	Prefix	Description
	2a0c:2f07:4896::/48	Colo in interxion LON3
	2a0c:2f07:9459::/48	Shared v6 services
	2a0c:2f07:29::/48	Colo in Cambridge business park

Policy upbeat_gould



Prefixes in selected policy

-	Prefix	Description
	2a0c:2f07:f::/48	KCIX Sitelocal
	2a0c:2f07:d::/48	KleyReX Sitelocal

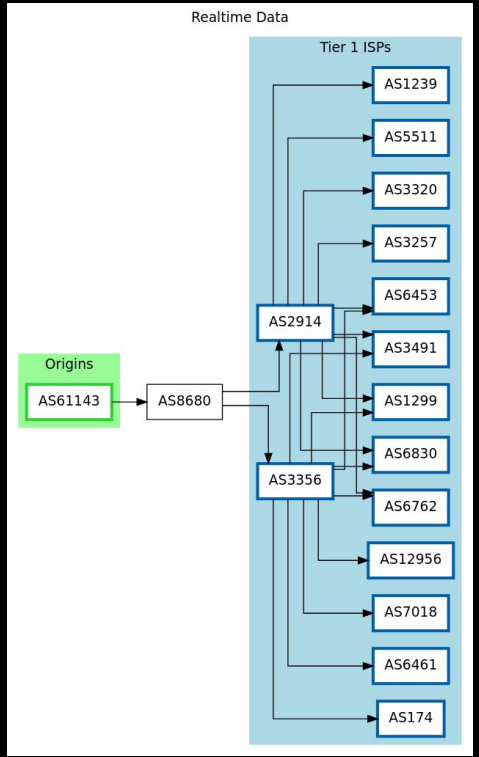
cda6ee3890045c20ade67418f5e35588

What is a upstream anyway?

cda6ee3890045c20ade67418f5e35588

What does bgp.tools count as a upstream?

- Any path that intersects a tier 1 ISP is activates logic that "sets" upstream/downstreams
- Walk up from the tier 1 ISP and set downstreams all the way,
  - Aka, a path like
  - 112 **174 2914** 8680 61143
  - Every link is set as a peer
  - Everything onwards from 2914-> is set as a downstream
  - Upstreams are inverse of downstreams
- This has *some* flaws
  - Some people peer with tier 1 providers. Causing some misleading info



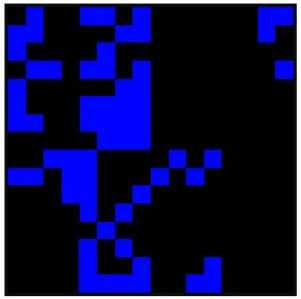
AS33891	Core-Backbone GmbH	195.66.224.238	2001:7f8:4::8463:1	400 gbps
AS61226	Flexiscale Technologies Limited	195.66.224.239	2001:7f8:4::ef2a:1	10 gbps
AS21396	NetConnex Broadband Ltd.	195.66.224.240	2001:7f8:4::5394:1	10 gbps
AS30827	Extraordinary Managed Services Ltd	195.66.224.241	2001:7f8:4::786b:1	10 gbps
AS35598	Inetcom LLC	195.66.224.242	2001:7f8:4::8b0e:1	10 gbps
AS12390	KCOM GROUP LIMITED	195.66.224.243	2001:7f8:4::3066:2	40 gbps
AS8881	1&1 Versatel Deutschland GmbH	195.66.224.245	2001:7f8:4::22b1:1	100 gbps
AS212263	Rocket Fibre Ltd	195.66.224.246	2001:7f8:4::3:3d27:1	10 gbps
AS50957	MEMSET Ltd	195.66.224.247	2001:7f8:4::c70d:1	10 gbps
AS35399	Online50 Limited	195.66.224.248		100 mbps
AS34066	Telappliant Limited	195.66.224.249		10 gbps
AS199335	Talk Straight Ltd.	195.66.224.250		10 gbps
AS2906	Netflix Streaming Services Inc.	195.66.224.251	2001:7f8:4::b5a:3	100 gbps
AS6663	Turk Telekom International	195.66.224.252	2001:7f8:4::1a07:1	10 gbps

Detected Vendor: IBM Corp

View | Edit

185.186.64.0/24

Announced by AS202562



Overview | Connectivity | Whois | DNS | Validation

Show Reverse DNS

Address	PTR
185.186.64.1	core2.ein.aperture-networks.net.
185.186.64.2	core1.ams.aperture-networks.net.
185.186.64.3	core1.ein.aperture-networks.net.
185.186.64.4	core1.fra.aperture-networks.net.
185.186.64.5	core1.ciab.aperture-networks.net.
185.186.64.6	core1.mci.aperture-networks.net.
185.186.64.8	core1.lax.aperture-networks.net.

Full ICMP /0 scan every 30 days

RDNS gets re-scanned if the DNS SOA changes

cda6ee3890045c20ade67418f5e35588

View | Edit

2a04:ad80::/47

Announced by AS44684

Overview | Connectivity | Whois | DNS

Show Reverse DNS

Address	PTR
2a04:ad80::53d0:59a0	i.v6.20hz.biz.
2a04:ad80::8613:e3c2	l02a.shelladdress.co.uk.
2a04:ad80::bec6:c021	hv302.nl1.bhost.net.
2a04:ad80::d437:8afa	ipv4.totallysucks.co.uk.
2a04:ad80::d51e:7035	nether.juzam.net.
2a04:ad80::f676:8691	hv301.nl1.bhost.net.
2a04:ad80:0:79::e74d	lists.videsfonds.lv.
2a04:ad80:0:ac::4239	ichenil.com.

RDNS scanning also works on IPv6*

* Assuming the DNS server is RFC Compliant

2a04:ad80::/47

Announced by AS44684

Overview | Connectivity | Whois | DNS

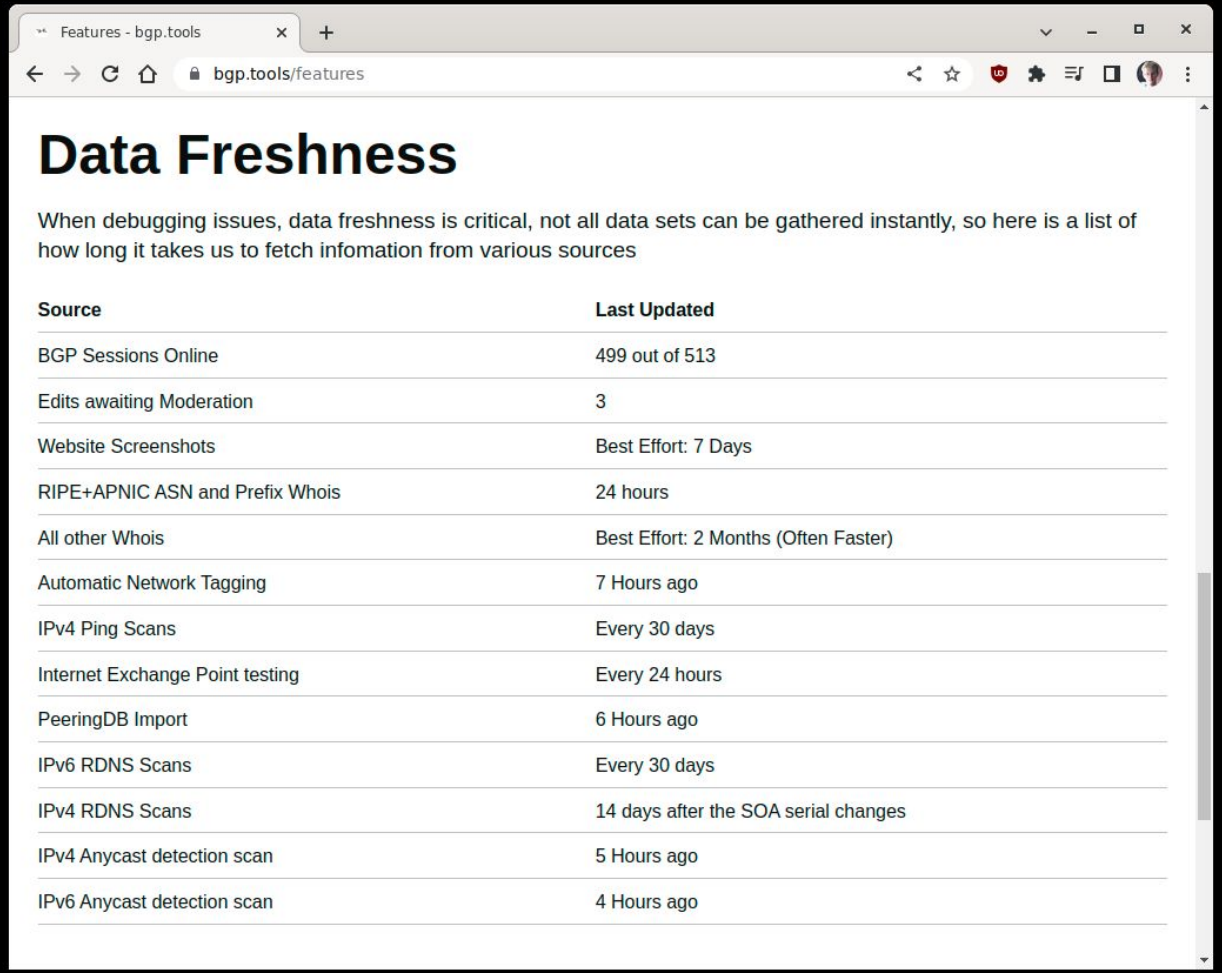
Show Forward DNS

AAAA	DNS
2a04:ad80::10b8:b5b6	isolation.thordendal.ru, thordendal.ru, 410.thordendal.ru
2a04:ad80::53d0:59a0	l02a.customhost.org.uk
2a04:ad80::8613:e3c2	l02a.shelladdress.co.uk
2a04:ad80::d51e:7035	nether.juzam.net
2a04:ad80:0:ce::7295	bh00051.vs.mythic-beasts.com
2a04:ad80:0:114::e2b7	cloudy.sh
2a04:ad80:0:182::8d3e	dungeons.sh, transylvanian.recipes
2a04:ad80:1:6e::1	mastergen.com, dev.mastergen.com, www.mastergen.com (4 more...)
2a04:ad80:1:79::d547	joseph.walton-rivers.uk, walton-rivers.uk
2a04:ad80:1:8b::1	grothendieck.bio, ecosocial.space, tsmithe.net, loby.life (6 more...)

We can also show you what DNS points *to* that prefix*

* Assuming it has issued a SSL cert

cda6ee3890045c20ade67418f5e35588



Data Freshness

When debugging issues, data freshness is critical, not all data sets can be gathered instantly, so here is a list of how long it takes us to fetch infomation from various sources

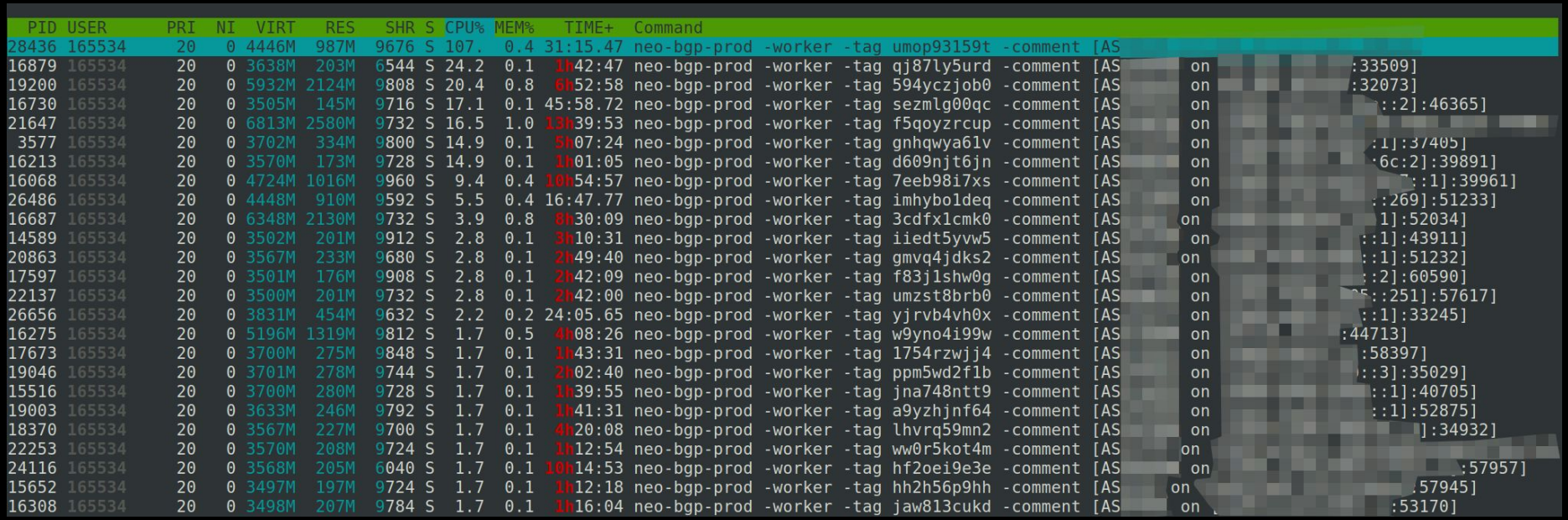
Source	Last Updated
BGP Sessions Online	499 out of 513
Edits awaiting Moderation	3
Website Screenshots	Best Effort: 7 Days
RIPE+APNIC ASN and Prefix Whois	24 hours
All other Whois	Best Effort: 2 Months (Often Faster)
Automatic Network Tagging	7 Hours ago
IPv4 Ping Scans	Every 30 days
Internet Exchange Point testing	Every 24 hours
PeeringDB Import	6 Hours ago
IPv6 RDNS Scans	Every 30 days
IPv4 RDNS Scans	14 days after the SOA serial changes
IPv4 Anycast detection scan	5 Hours ago
IPv6 Anycast detection scan	4 Hours ago

cda6ee3890045c20ade67418f5e35588

I built my own BGP collector

cda6ee3890045c20ade67418f5e35588

A New BGP daemon for a new use case



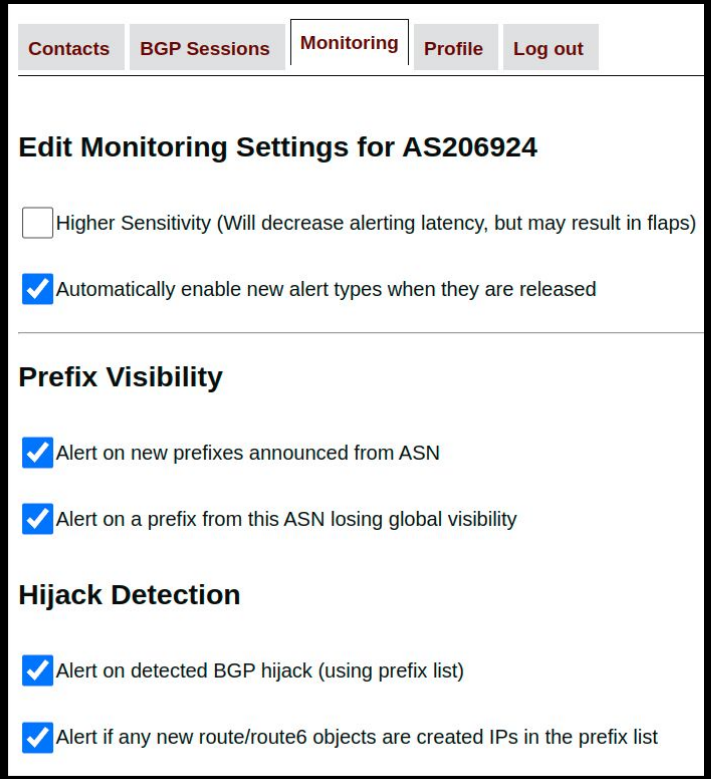
It turns out if you don't need to converge routes writing a bgp demon can be easy, runs ~500 Site QPS

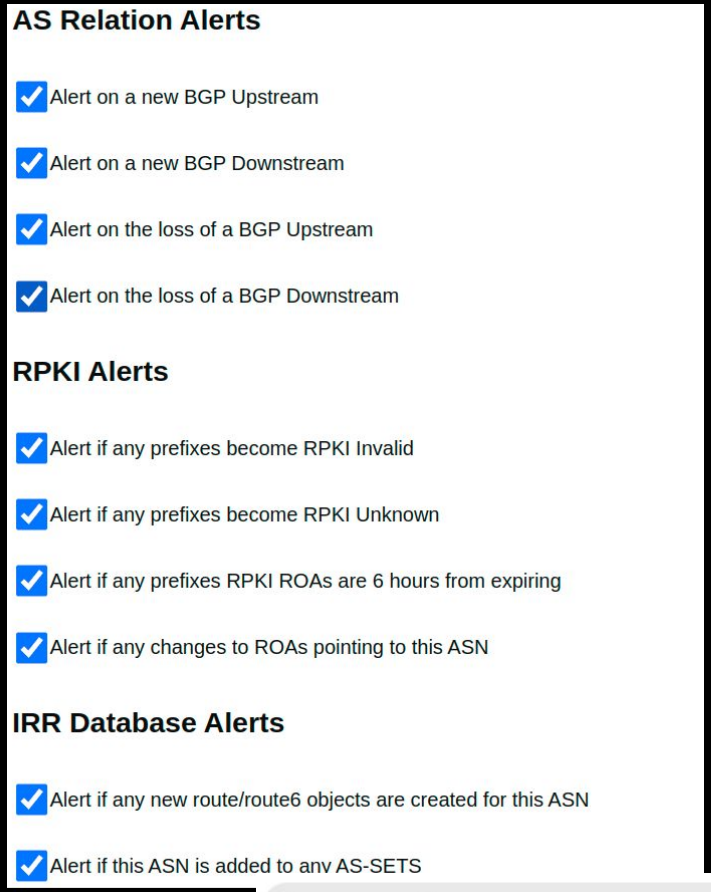
300+ Million Routes, Over 64 CPU cores. 10k/s route updates on average, Surges of 100k/s+

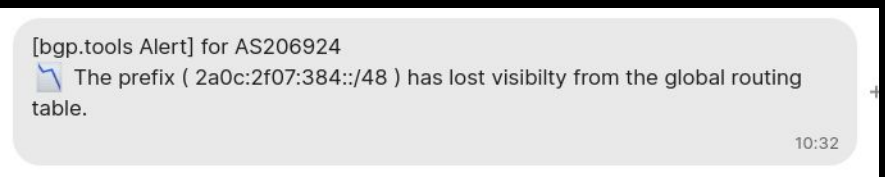
Fun things you can do if you "*simply*" write your own bgpd

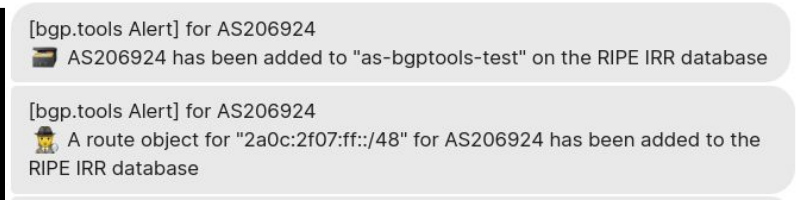
- Rather than processing paths, you can directly implement code for what the site is doing (List Prefixes Originated, Upstreams, Peers, etc)
- Direct support for "watching" changes to ASNs/Prefixes
- Point in time snapshots
- Point in time reload (go backwards in time)

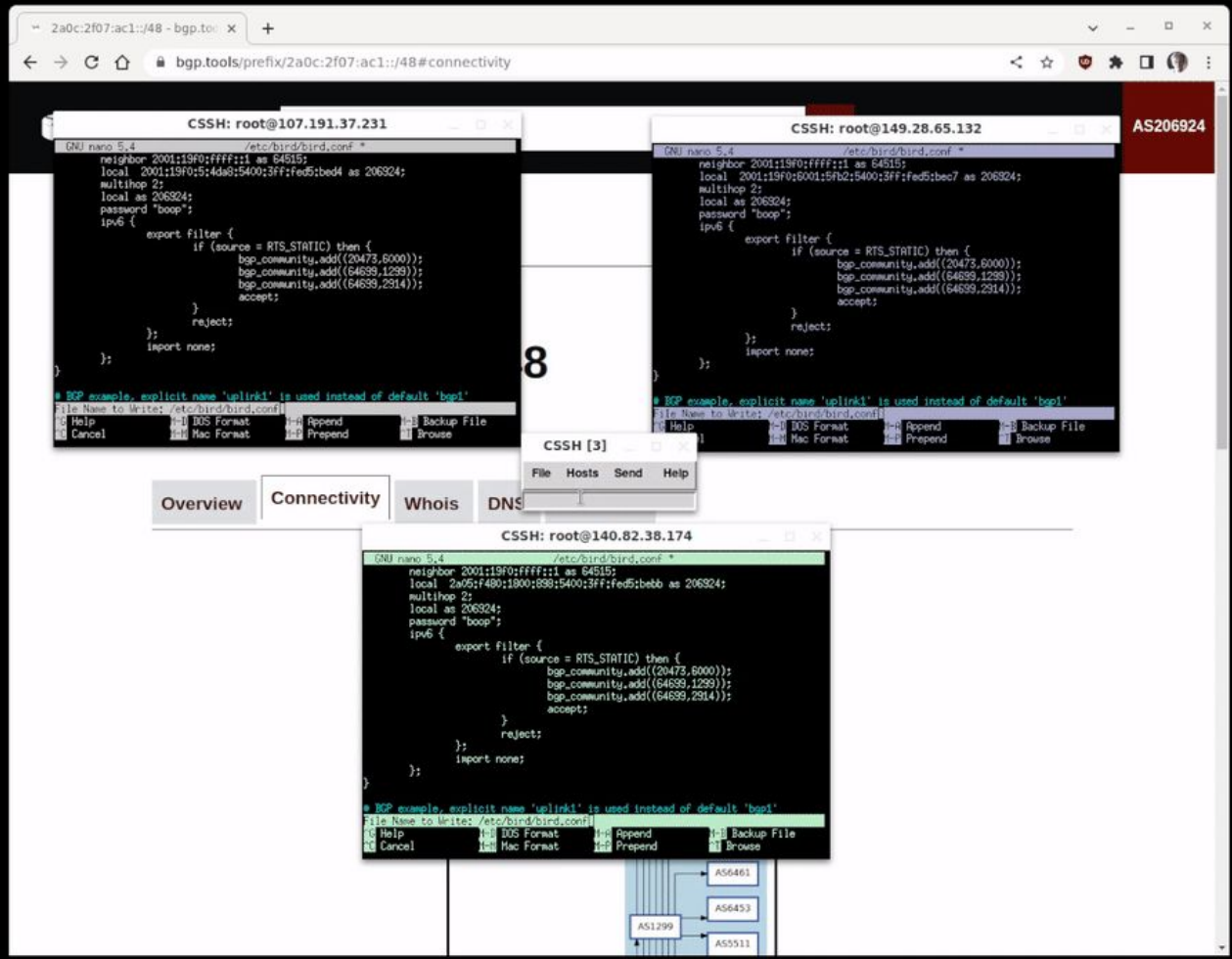
cda6ee3890045c20ade67418f5e35588


Contacts
BGP Sessions
Monitoring
Profile
Log out
Edit Monitoring Settings for AS206924
Higher Sensitivity (Will decrease alerting latency, but may result in flaps)
Automatically enable new alert types when they are released
Prefix Visibility
Alert on new prefixes announced from ASN
Alert on a prefix from this ASN losing global visibility
Hijack Detection
Alert on detected BGP hijack (using prefix list)
Alert if any new route/route6 objects are created IPs in the prefix list


AS Relation Alerts
Alert on a new BGP Upstream
Alert on a new BGP Downstream
Alert on the loss of a BGP Upstream
Alert on the loss of a BGP Downstream
RPKI Alerts
Alert if any prefixes become RPKI Invalid
Alert if any prefixes become RPKI Unknown
Alert if any prefixes RPKI ROAs are 6 hours from expiring
Alert if any changes to ROAs pointing to this ASN
IRR Database Alerts
Alert if any new route/route6 objects are created for this ASN
Alert if this ASN is added to anv AS-SETS


[bgp.tools Alert] for AS206924
The prefix (2a0c:2f07:384::/48) has lost visibilty from the global routing table.
10:32


[bgp.tools Alert] for AS206924
AS206924 has been added to "as-bgptools-test" on the RIPE IRR database
[bgp.tools Alert] for AS206924
A route object for "2a0c:2f07:ff::/48" for AS206924 has been added to the RIPE IRR database



cda6ee3890045c20ade67418f5e35588

2a00:1098::/32 - bgp.tools

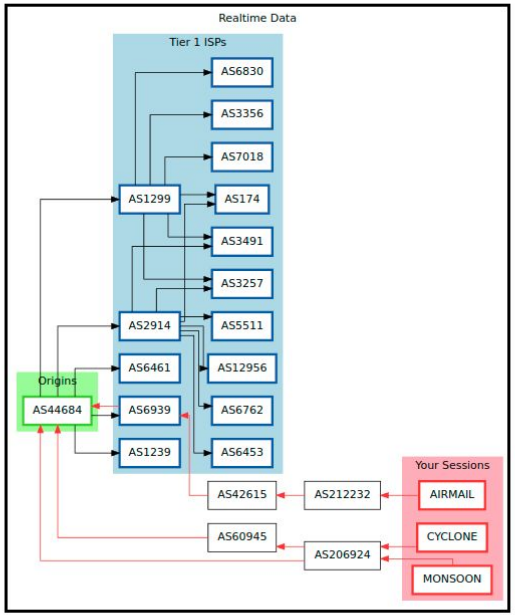
bgp.tools/prefix/2a00:1098::/32#connectivity

Incognito (2)

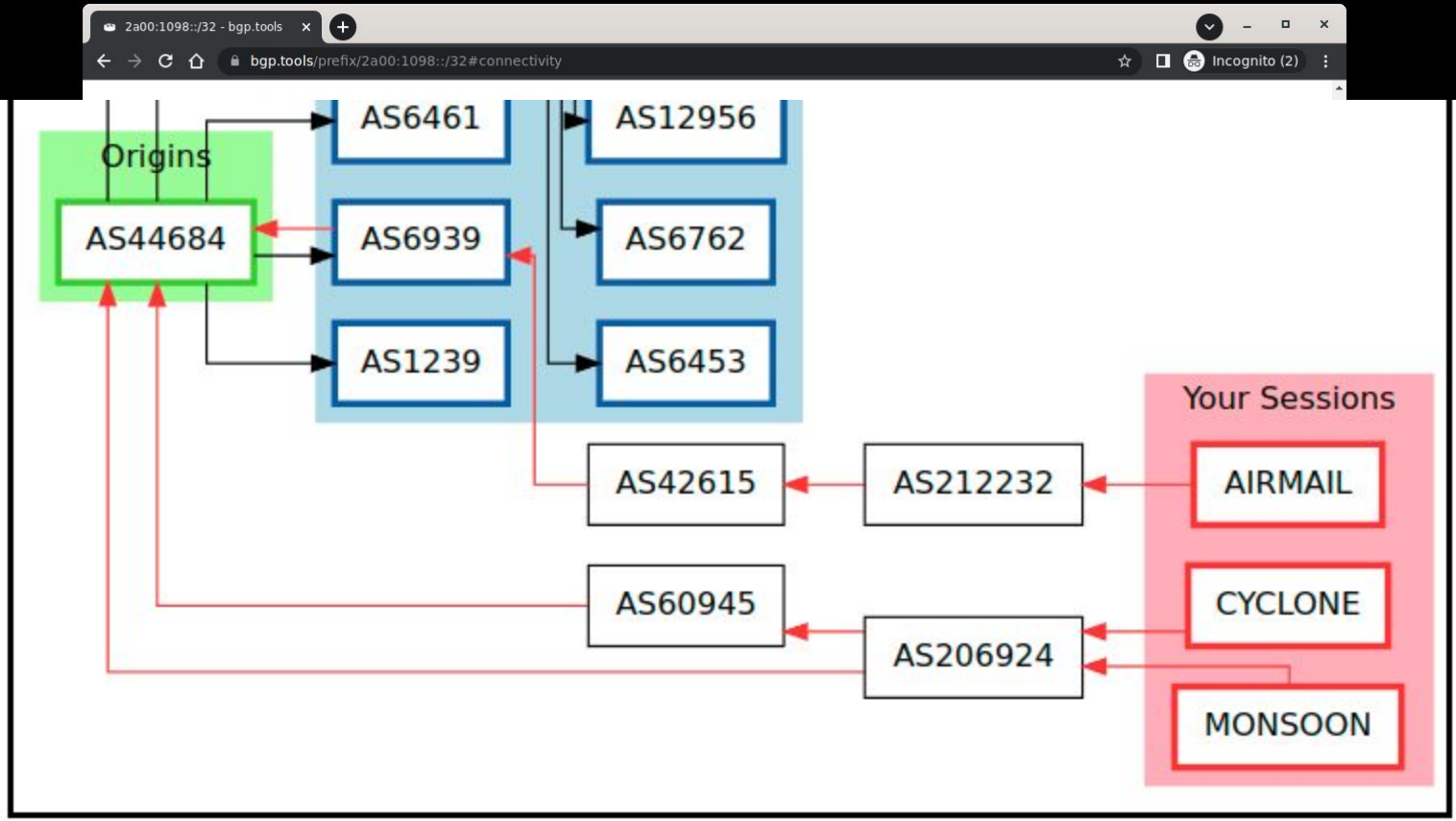
2a00:1098::/32

Announced by AS44684

Overview | Connectivity | Whois | DNS | Validation



cda6ee3890045c20ade67418f5e35588



cda6ee3890045c20ade67418f5e35588

Some interesting things about the LU market

cda6ee3890045c20ade67418f5e35588

Luxembourg Network Rankin

bgp.tools/rankings/LU?sort=cone

bgp.tools Start here... AS206924

Luxembourg Network Rankings

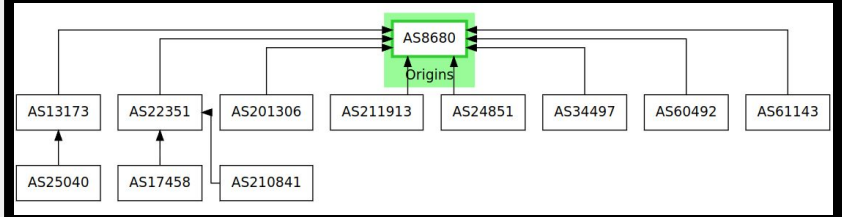
Sort by: AS Cone

Learn more about how these ranks are calculated

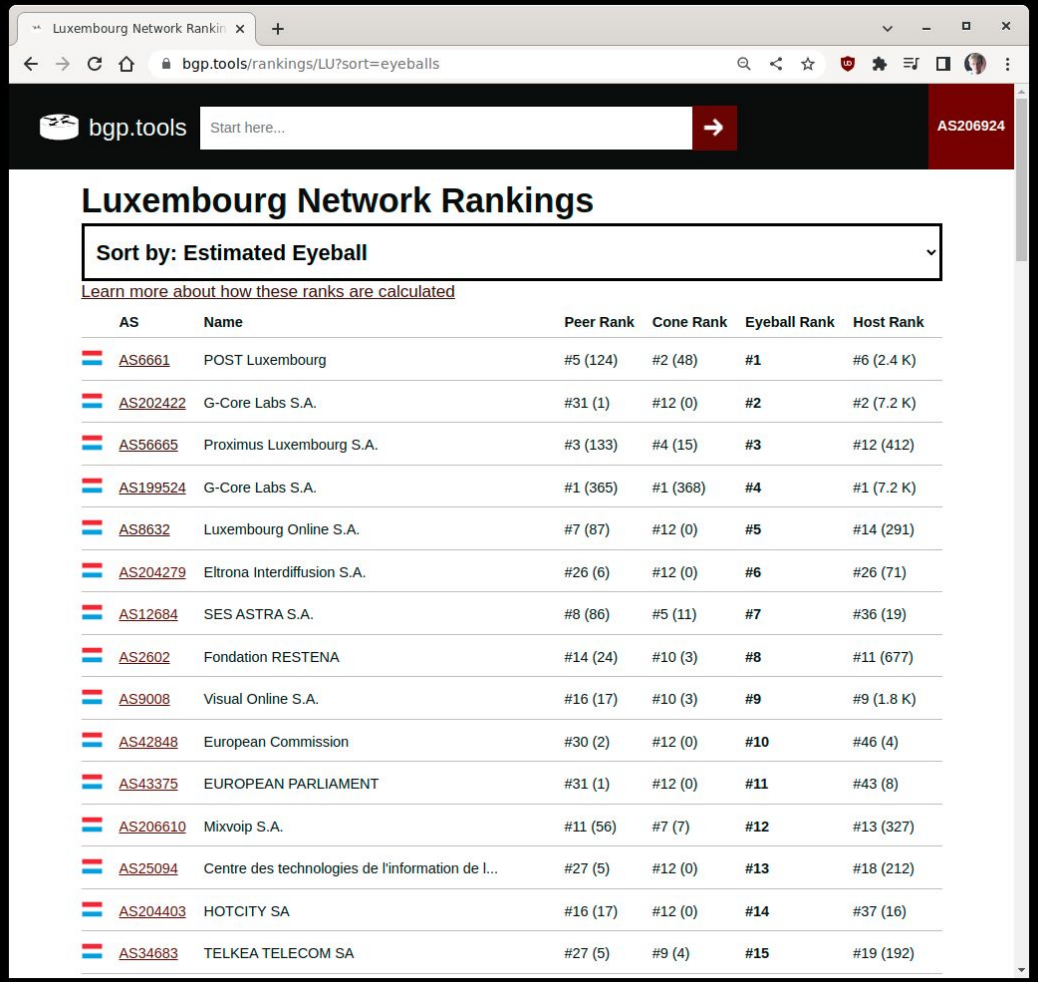
AS	Name	Peer Rank	Cone Rank	Eyeball Rank	Host Rank
AS199524	G-Core Labs S.A.	#1 (365)	**#1** (368)	#4	#1 (7.2 K)
AS6661	POST Luxembourg	#5 (124)	**#2** (48)	#1	#6 (2.4 K)
AS29467	LUXNETWORK S.A.	#6 (94)	**#3** (34)	#21	#20 (185)
AS56665	Proximus Luxembourg S.A.	#3 (133)	**#4** (15)	#3	#12 (412)
AS12684	SES ASTRA S.A.	#8 (86)	**#5** (11)	#7	#36 (19)
AS15965	CEGECOM S.A.	#9 (72)	**#6** (9)	#18	#21 (149)
AS206610	Mixvoip S.A.	#11 (56)	**#7** (7)	#12	#13 (327)
AS24611	Datacenter Luxembourg S.A.	#14 (24)	**#8** (6)	#25	#3 (5.6 K)
AS60497	Uwe Zeidler	#15 (19)	**#8** (6)	#34	#50 (0)
AS208374	LU-CIX Management GIE	#27 (5)	**#9** (4)	#44	#50 (0)
AS25273	Broadcasting Center Europe (an RTL Group Comp...	#21 (11)	**#9** (4)	#31	#22 (106)
AS210834	LU-CIX Management GIE	#23 (9)	**#9** (4)	#44	#40 (12)
AS34683	TELKEA TELECOM SA	#27 (5)	**#9** (4)	#15	#19 (192)
AS9008	Visual Online S.A.	#16 (17)	**#10** (3)	#9	#9 (1.8 K)
AS60391	Papa-Razzi Media Group A.s.b.l.	#24 (8)	**#10** (3)	#44	#50 (0)

Sum of all of the ASNs "behind" (downstreamed) another ASN.

For example, this ASN has a cone of 12 (including itself)



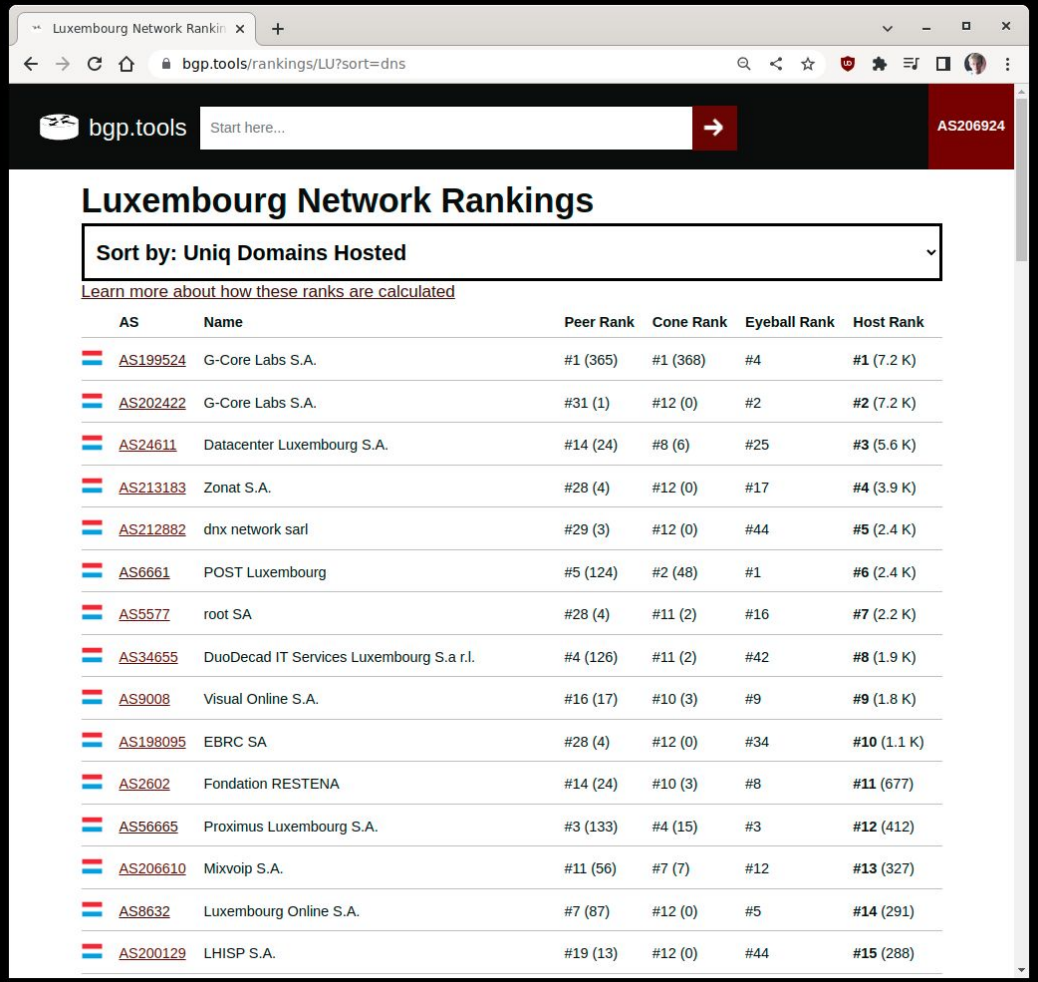
cda6ee3890045c20ade67418f5e35588



A mixer metric, using bittorrent data, ads, and other "eyeball" signals, ranked.

It also catches VPN networks. Raw numbers are hard to understand, so are hidden from view.

cda6ee3890045c20ade67418f5e35588



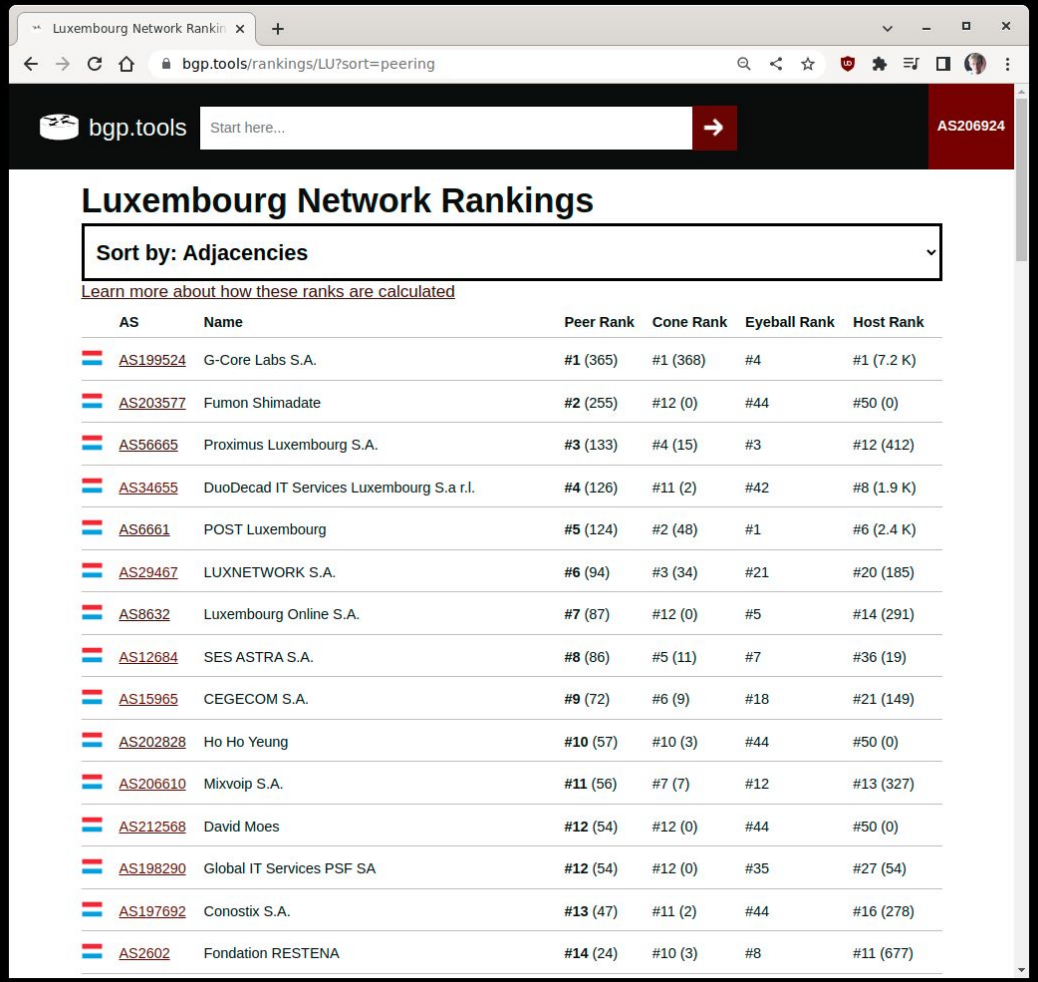
Using the forward DNS database, I count the amount of domain names (rounded up to the domain) that points to each ASN.

Example:

a.b.benjojo.co.uk -> benjojo.co.uk

One domain can occupy more than one ASN, so if you sum up the whole host rank numbers, the resulting number will be larger than the number of all domains.

cda6ee3890045c20ade67418f5e35588



Sum of all visible unique peering (A<->B) relationships.

Is easily "gameable" and is biased to what data I have.

Also (probably because of this) a well loved metrics for sales and marketing

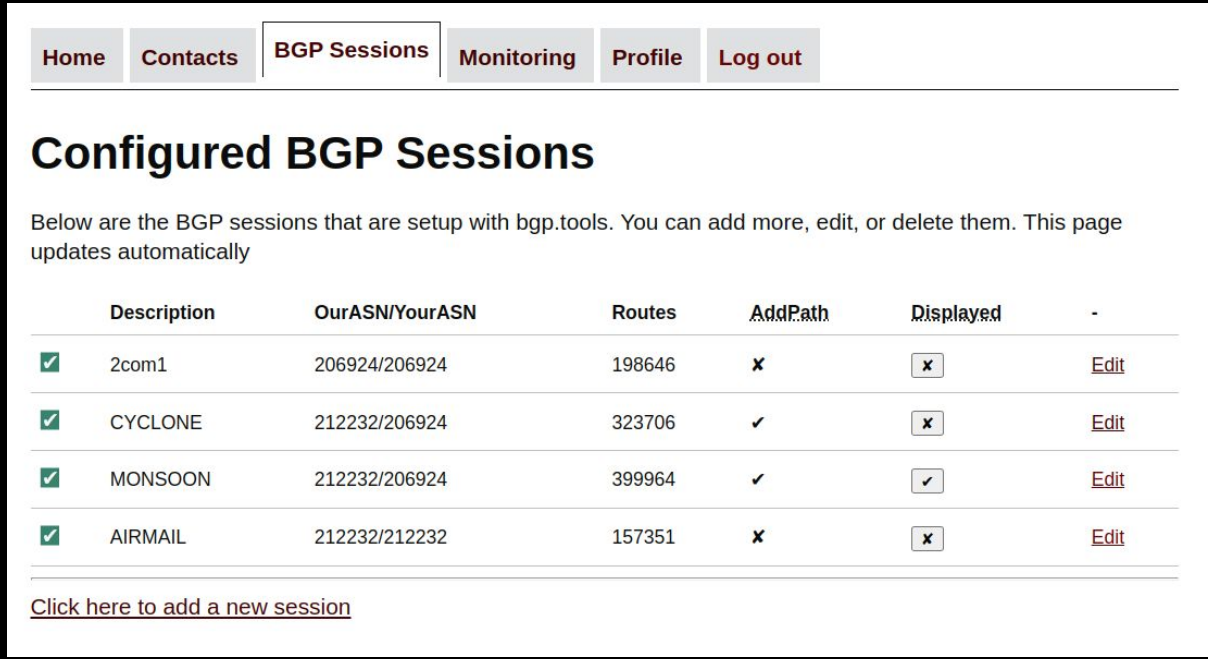
cda6ee3890045c20ade67418f5e35588

Want to improve your peering number?

cda6ee3890045c20ade67418f5e35588

Frictionless and easy

- Login via PeeringDB, or sign up for a bgp.tools account
- We setup some kind of communication method (That includes more "exotic" stuff like Discord, Slack, Telegram, Signal, Webhooks)
- You can **instantly** create a new session and the backend and UI live updates to the status



cda6ee3890045c20ade67418f5e35588

This is all you need

New BGP Session:

Description for Router/Session: (max 16 chars)

LHR01

Select the ASN you would like us to use for you. We will only accept AS212232 (bgp.tools), AS206924, and Private ASN ranges

212232

Select the ASN you are going to use with us. We will only accept AS206924 and Private ASN ranges

206924

Select the IP you will be connecting from.

192.0.0.1 / 2001:db8::

You will get the remote (bgp.tools side) IP after you create the session.

Please send **Full tables** rather than just your peering routes/customer routes. bgp.tools may automatically switch your sessions to only import your peering routes to save RAM, but allow us to figure that out for future flexibility!

We support (and encourage) BGP AddPath, and MultiProtocol/MultiFamily BGP

If you absolutely need a MD5 Password on the session, please enter the desired MD5 password

☐ Export this data into publicly available MRT files

☐ Also allow commercial products to use those MRT files

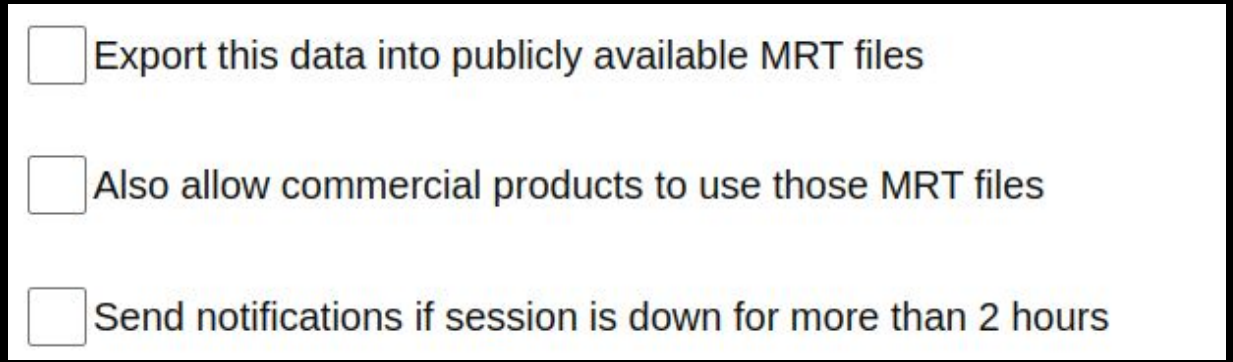
☐ Send notifications if session is down for more than 2 hours

cda6ee3890045c20ade67418f5e35588

MRT Support will be offered soon

People can opt in to having their routes exported out into a large MRT file.

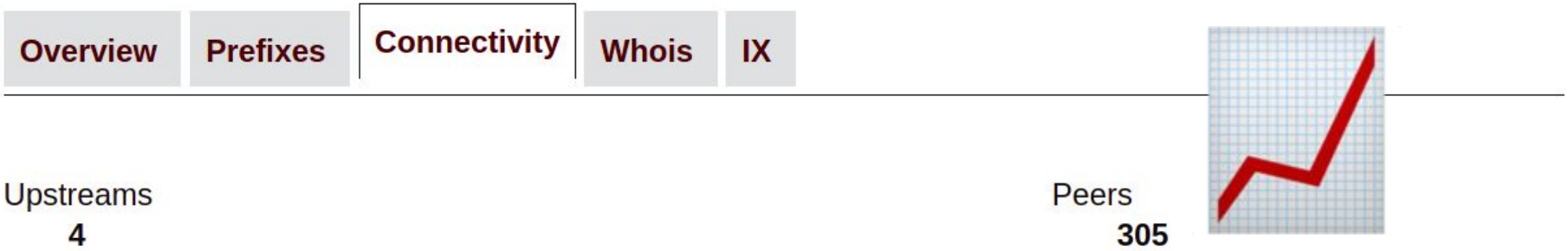
To deal with usage concerns, the files are split between profit allowed and non-profit uses.



cda6ee3890045c20ade67418f5e35588

If you like this tool, Please setup BGP Collector sessions

- I'm in particular need for Verizon (AS701(2,3)), DTAG (AS3320), Telefonica (AS12956), Sparkle (AS6762), and the **LU ecosystem**
- However if you want a better peering rank, you should feed anyway



- This also will help the academic community get access to unique AS Path data!

cda6ee3890045c20ade67418f5e35588

Questions? / Requests?

Or admin@bgp.tools / ben@benjojo.co.uk

Longer term bgp.tools goals:

- Work with poorly covered networks/regions (*Like Luxembourg*) to start sessions with us
- Continue to build better debugging systems designed for real network engineers to use, not marketing slides
- Historical data pull back
- **Talk to me in person for more plans!**

cda6ee3890045c20ade67418f5e35588

Backup slides

cda6ee3890045c20ade67418f5e35588

API… ish?

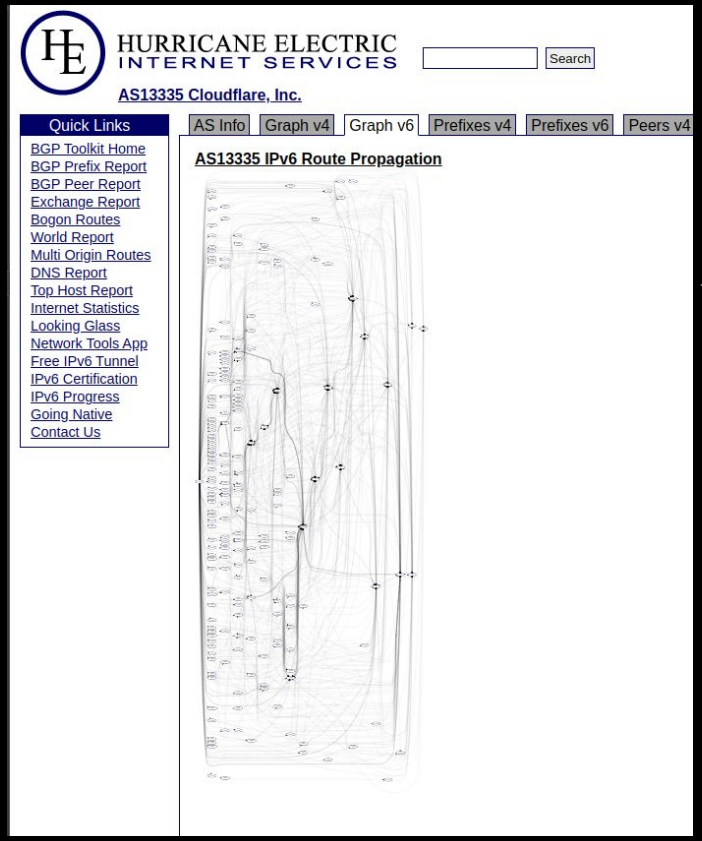
- Similar whois+bulk mode server to Team Cymru's

```
[16:56:34] ben@metropolis:~$ whois 185.230.223.69 -h bgp.tools
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
206924  | 185.230.223.69   | 185.230.223.0/24    | GB | RIPE     | 2022-06-21 | Ben Cartwright-Cox
```

- table.txt / table.jsonl for full table <-> ASN mapping
- asns.csv for **ASN -> Name mappings**
- Dumping of network tag members
- Gopher (yes, really) support if you *really* hate yourself

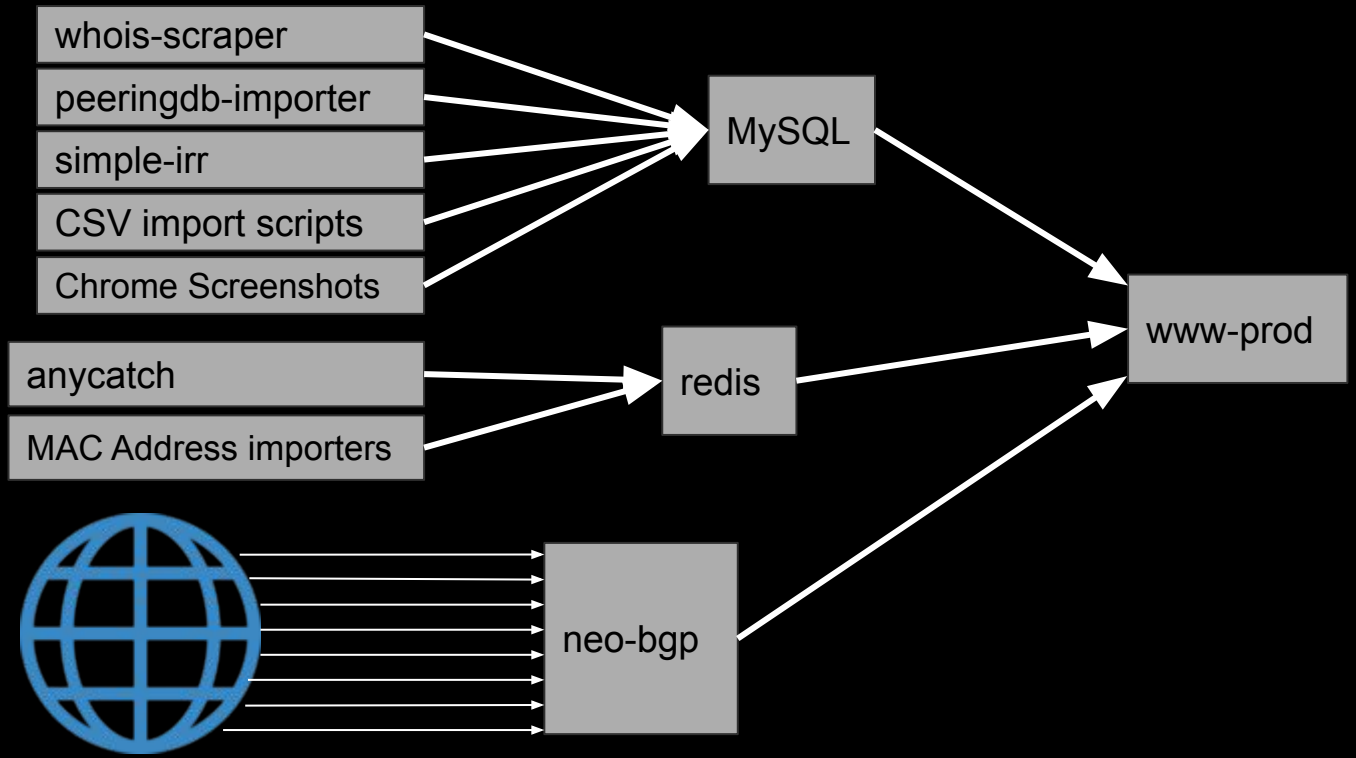
https://bgp.tools/kb/api

Avoids situations like this:



GraphViz Routing Spaghetti

General Data Flows of bgp.tools



cda6ee3890045c20ade67418f5e35588