

The unending misery of



bgp.tools

Ben Cartwright-Cox
@ RIPE84 - May 19 2022

The screenshot shows a web browser window with the address bar displaying "bgp.tools". The page header features the BGP.Tools logo and the text "bgp.tools". The main heading is "Browse the internet ecosystem". Below this is a search prompt: "Search by ASN (AS13335) or Prefix (8.8.8.0/24)". A search input field contains the text "Start here... (New search engine as of 10th Oct 2021)" and a red arrow button. The page is divided into three columns: "You are connecting from", "Example Pages", and "Why use BGP.Tools?". The "You are connecting from" column lists various IP addresses and DNS records. The "Example Pages" column lists links to Cloudflare CDN, BenjojoNET, and Google DNS Prefix. The "Why use BGP.Tools?" column lists features like fast updates and enhanced data. The footer contains links for "Scripting/API", "Credits", "Contact Email", "Issue Tracker", and "Twitter".

Browse the internet ecosystem

Search by ASN (AS13335) or Prefix (8.8.8.0/24)

Start here... (New search engine as of 10th Oct 2021)

You are connecting from

- IPv6: [2a0c:2f07:4663::](#)
- Ben Cartwright-Cox ([AS206924](#))
- [2a0c:2f07:4663::/48](#)
- [\[redacted\]](#)
- [\[redacted\]](#)
- [\[redacted\]](#)
- [\[redacted\]](#)
- DNS: [185.230.223.109](#)
- DNS: [185.230.223.87](#)
- DNS: [2a0c:2f07:29:666::5353](#)
- DNS: [2a0c:2f07:4896:666:216:3eff:feff:861f](#)

Example Pages

- [Cloudflare CDN](#)
- [BenjojoNET](#)
- [Google DNS Prefix](#)

Why use BGP.Tools?

We offer:

- Fast updates to data
- Enhanced Data on networks
- Understandable interfaces
- [Full list here](#)

[Scripting/API](#) [Credits](#) [Contact Email](#) [Issue Tracker](#) [Twitter](#)

```
[01:05:21] ben@metropolis:~$ routeviews
```

```
Trying 195.66.241.146...
```

```
Connected to route-views.linx.routeviews.org.
```

```
Escape character is '^']'.
```

```
Hello, this is FRRouting (version 7.3-rv).
```

```
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

```
route-views.linx.routeviews.org> show bgp ipv4 185.230.223.0/24
```

```
BGP routing table entry for 185.230.223.0/24
```

```
Paths: (37 available, best #33, table default)
```

```
Not advertised to any peer
```

```
61955 44684 206924
```

```
195.66.224.13 from 195.66.224.13 (62.168.193.234)
```

```
Origin IGP, valid, external
```

```
Large Community: 44684:0:900 44684:1:2 44684:2:206924 44684:3000:1299
```

```
Last update: Tue Mar 8 21:14:15 2022
```

```
58511 44684 206924
```

```
195.66.238.214 from 195.66.238.214 (103.247.3.120)
```

```
Origin IGP, valid, external
```

```
Community: 58511:200 58511:9007
```

```
Last update: Tue Mar 8 15:59:08 2022
```

```
398465 44684 206924
```

```
195.66.227.122 from 195.66.227.122 (216.176.32.97)
```

```
Origin IGP, valid, external
```

[01:05:21] ben@metro
Trying 195.66.241.14
Connected to route-v
Escape character is

Hello, this is FRRou
Copyright 1996-2005

route-views.linx.rou
BGP routing table en
Paths: (37 available
Not advertised to
61955 44684 206924
195.66.224.13 fr
Origin IGP, va
Large Communit
Last update: T
58511 44684 206924
195.66.238.214 f
Origin IGP, va
Community: 585
Last update: T
398465 44684 20692
195.66.227.122 f
Origin IGP, va



Search

AS206924 Ben Cartwright-Cox

Quick Links

- [BGP Toolkit Home](#)
- [BGP Prefix Report](#)
- [BGP Peer Report](#)
- [Exchange Report](#)
- [Bogon Routes](#)
- [World Report](#)
- [Multi Origin Routes](#)
- [DNS Report](#)
- [Top Host Report](#)
- [Internet Statistics](#)
- [Looking Glass](#)
- [Network Tools App](#)
- [Free IPv6 Tunnel](#)
- [IPv6 Certification](#)
- [IPv6 Progress](#)
- [Going Native](#)
- [Contact Us](#)

- AS Info
- Graph v4
- Graph v6
- Prefixes v4
- Prefixes v6
- Peers v4
- Peers v6
- Whois
- IRR
- IX

Company Website: <https://blog.benjojo.co.uk>

Country of Origin: [United Kingdom](#) 

Internet Exchanges: 2

Prefixes Originated (all): 9
Prefixes Originated (v4): 1
Prefixes Originated (v6): 8

Prefixes Announced (all): 11
Prefixes Announced (v4): 3
Prefixes Announced (v6): 8

RPKI Originated Valid (all): 8
RPKI Originated Valid (v4): 1
RPKI Originated Valid (v6): 7

RPKI Originated Invalid (all): 0
RPKI Originated Invalid (v4): 0
RPKI Originated Invalid (v6): 0

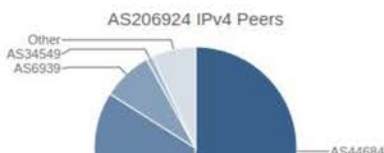
BGP Peers Observed (all): 39
BGP Peers Observed (v4): 30
BGP Peers Observed (v6): 33

IPs Originated (v4): 256
AS Paths Observed (v4): 477
AS Paths Observed (v6): 1,538

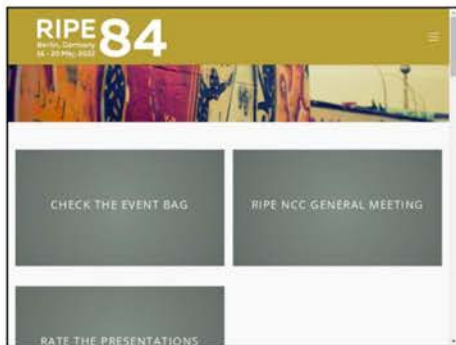
Average AS Path Length (all): 4.042
Average AS Path Length (v4): 3.658
Average AS Path Length (v6): 4.161

Ben's Blog Home Site | 81 Posts Twitter | RSS

- 470 Top-Info Storage for Linux users on 2020-02-27 11:23:04 by [unreadable]
- 1000 in the ethernet netw on 2020-01-17 21:43:54 by [unreadable]
- One of those things is not like the other on 2020-03-18 07:28:59 by [unreadable]
- Imaging mounted disk subvolumes under storage on 2020-09-20 13:29:26 by [unreadable]
- Working down the stack: BGP routes on 2020-04-22 09:12:36 by [unreadable]
- Splitting the ping on 2020-09-05 13:09:43 by [unreadable]
- Working Ethernet out of Band Channel Levels on 2020-08-08 10:52:02 by [unreadable]
- Showing the network when it's already down on 2020-04-20 10:09:34 by [unreadable]
- How I can't figure out how the RPKI of the Internet on 2020-03-18 13:49:53 by [unreadable]
- Writing computer code drivers for abandoned devices on 2019-11-17 12:08:38 by [unreadable]
- The correct call, under pressure on 2020-08-12 13:04:02 by [unreadable]
- The year of RPKI on the control plane on 2020-08-08 12:08:04 by [unreadable]
- Teaching a cheap ethernet switch new tricks on 2020-08-13 13:03:03 by [unreadable]
- The speed of BGP network propagation on 2020-05-04 13:29:01 by [unreadable]
- What would a 6rd network element look like? on 2020-02-03 10:33:51 by [unreadable]
- A shot into the world of IPv6-6rd on 2020-05-04 13:14:42 by [unreadable]
- The spiky of RPKI on 2019 on 2020-07-28 13:07:59 by [unreadable]
- Prox-IPsec in reverse shell on 2020-09-20 14:29:05 by [unreadable]
- How BGP security features working on 2020-09-20 14:29:05 by [unreadable]
- Working telemetry for the 6rd Telemetry on 2020-09-20 14:29:05 by [unreadable]



ASN	Name
AS44684	Mythic Beasts Ltd
AS3170	Etheroute Ltd
AS6939	Hurricane Electric LLC
AS34549	meerfarbig GmbH & Co. KG


[View](#)
[Edit](#)


RIPE Meeting Network

AS Number 2121

Website <https://ripe84.ripe.net/>

[Overview](#)
[Prefixes](#)
[Connectivity](#)
[Whois](#)
[Overview](#)
[Prefixes](#)
[Connectivity](#)
[Whois](#)

Registered on

20 Sep 2002 (19 years old)

Network status

Active, Allocated under RIPE

Network type

Eyeball

Prefixes Announced

1 IPv4, 1 IPv6

Upstreams

- [AS3320](#) - Deutsche Telekom AG

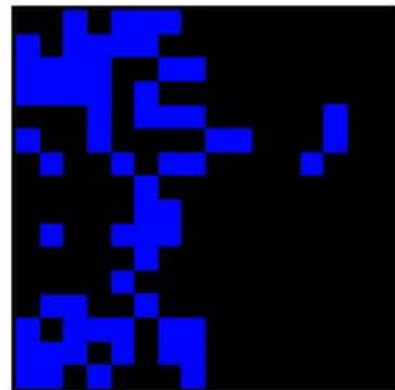
Locations of Operation

- Netherlands

Tags:

[Event](#)



[View](#)
[Edit](#)


185.230.223.0/24

Announced by [AS206924](#)

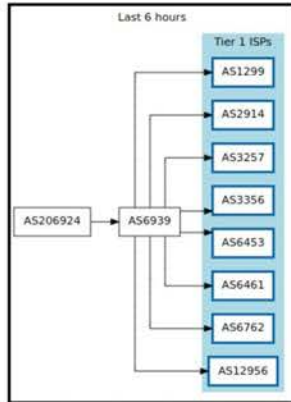
[Overview](#)
[Connectivity](#)
[Whois](#)
[DNS](#)
[Validation](#)

2a0c:2f07:f::/48

Announced by [AS206924](#)

Overview Connectivity **Whois** DNS Validation

This prefix is not reachable from Cogent on IPv6 ([What does that mean?](#))



[How are upstreams and downstreams calculated?](#)

Upstreams i

ASN	Description
AS6939	Hurricane Electric LLC

Peers i

ASN	Description
AS34927	iFog GmbH
AS1828	Unitas Global LLC
AS6939	Hurricane Electric LLC

This prefix is not reachable from Cogent on IPv6 ([What does that mean?](#))

[How are upstreams and downstreams calculated?](#)

Upstreams i

ASN	Description
AS6939	Hurricane Electric LLC

Peers i

ASN	Description
AS34927	iFog GmbH
AS1828	Unitas Global LLC
AS6939	Hurricane Electric LLC

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 information from various sources

Source	Last Updated
BGP Sessions Online	82 out of 82
Edits awaiting Moderation	0
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	Every 24 hours
IPv4 Ping Scans	Every 30 days
Internet Exchange Point testing	Every 24 hours
PeeringDB Import	23 Hours ago
IPv6 RDNS Scans	Every 30 days
IPv4 RDNS Scans	Every 60 days
IPv4 Anycast detection scan	3 Hours ago
IPv6 Anycast detection scan	1 Hours ago

API... ish?

- Similar whois+bulk mode server to Team Cymru's
 - table.txt / table.jsonl for full table <-> ASN mapping
 - Dumping network tag members
 - Gopher support if you *really* hate yourself
-
- More API calls to come when i'm less scared about operating a stable API interface
 - (there is a secret API for those who don't care)

Slightly more adventurous for data sources

			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

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

Vendor Detection (the logos) Enabled by:

Friends pingng IX ranges and sending me their arp tables

Scraping fe80:: addresses out of BGP MRTs

Creative use of IX looking glasses to get the fe80 addresses

Detected Vendor: IBM Corp

		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
		AS212263	Rocket Fibre Ltd	195.66.224.246	2001:7f8:4::3:3d27:1	10 gbps
		AS55555	NETNET LTD	195.66.224.245	2001:7f8:4::6000:1	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

Online-ness (the green tick) comes from:

IX Looking glasses (Are you announcing routes to the RR?)

Abuse of larger networks who don't ACL access to IXP ranges

Their lack of prioritization is a huge bonus for bgp.tools

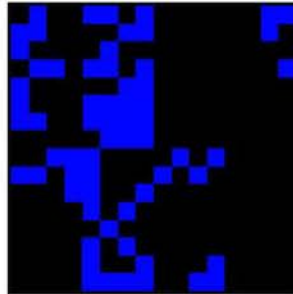
View

Edit



185.186.64.0/24

Announced by [AS202562](#)



Full ICMP /0 scan every 30 days

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.



RDNS gets re-scanned if the DNS SOA changes

View

Edit



2a04:ad80::/47

Announced by [AS44684](#)

Overview

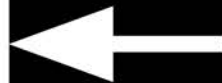
Connectivity

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...)

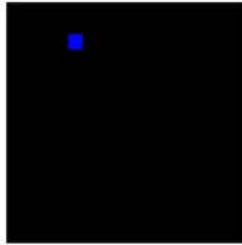
We can also show you what DNS points *to* that prefix*

* Assuming it has issued a SSL cert

Handles annoying edge cases

209.112.123.0/24

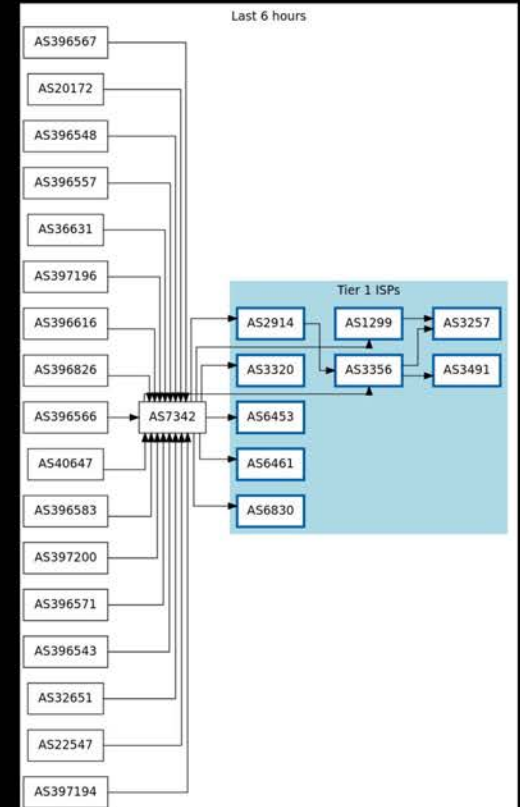
Announced by [AS396566](#), and [21 others](#)



[Overview](#) [Connectivity](#) [Whois](#) [DNS](#) [Validation](#)

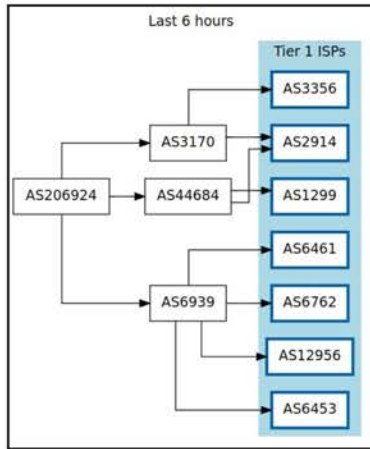
Originators i

ASN	Description
 AS396566	VeriSign Global Registry Services
 AS32651	VeriSign Global Registry Services
 AS396576	VeriSign Global Registry Services
 AS396616	VeriSign Global Registry Services
 AS397194	VeriSign Global Registry Services
 AS396548	VeriSign Global Registry Services
 AS397196	VeriSign Global Registry Services
 AS397196	VeriSign Global Registry Services



Networks are broken up into policies

Policy inspiring_ardinghelli

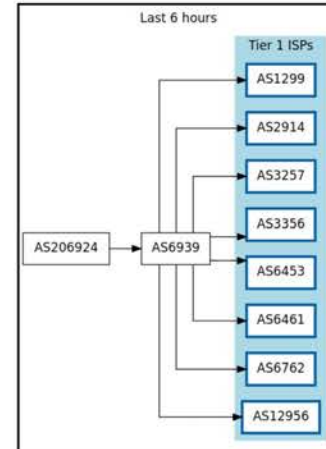


[Click here to learn more about what this graph means and what makes up a network policy](#)

Prefixes in selected policy

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

Policy gracious_buck

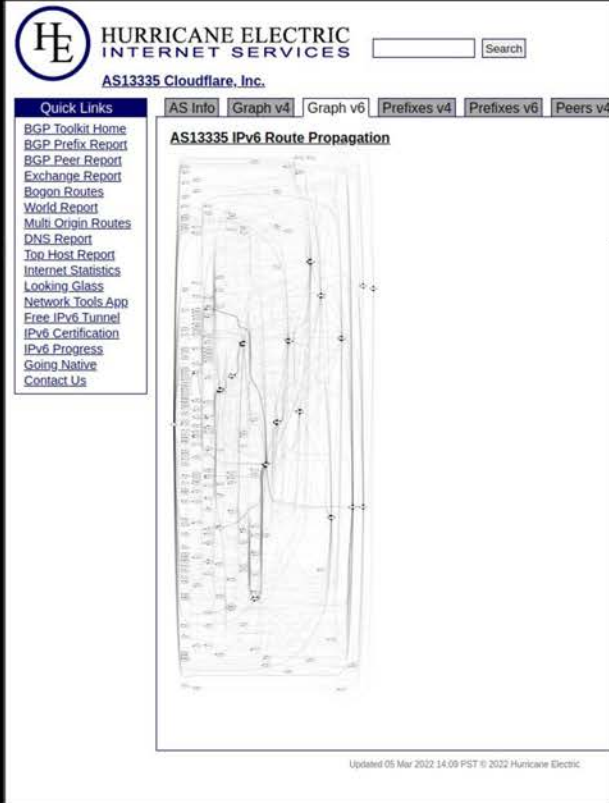


[Click here to learn more about what this graph means and what makes up a network policy](#)

Prefixes in selected policy

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

Avoids situations like this:



The screenshot shows the Hurricane Electric website interface. At the top left is the Hurricane Electric logo (HE) and the text "HURRICANE ELECTRIC INTERNET SERVICES". Below this is "AS13335 Cloudflare, Inc." and a search bar. A navigation bar contains tabs for "AS Info", "Graph v4", "Graph v6", "Prefixes v4", "Prefixes v6", and "Peers v4". On the left is a "Quick Links" menu with various tools like "BGP Toolkit Home", "BGP Prefix Report", etc. The main content area displays "AS13335 IPv6 Route Propagation" with a complex network graph. A large white arrow points from the text "GraphViz Routing Spaghetti" to the graph.

HURRICANE ELECTRIC
INTERNET SERVICES

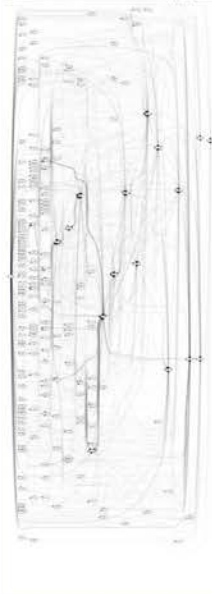
AS13335 Cloudflare, Inc.

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi-Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

AS Info Graph v4 Graph v6 Prefixes v4 Prefixes v6 Peers v4

AS13335 IPv6 Route Propagation

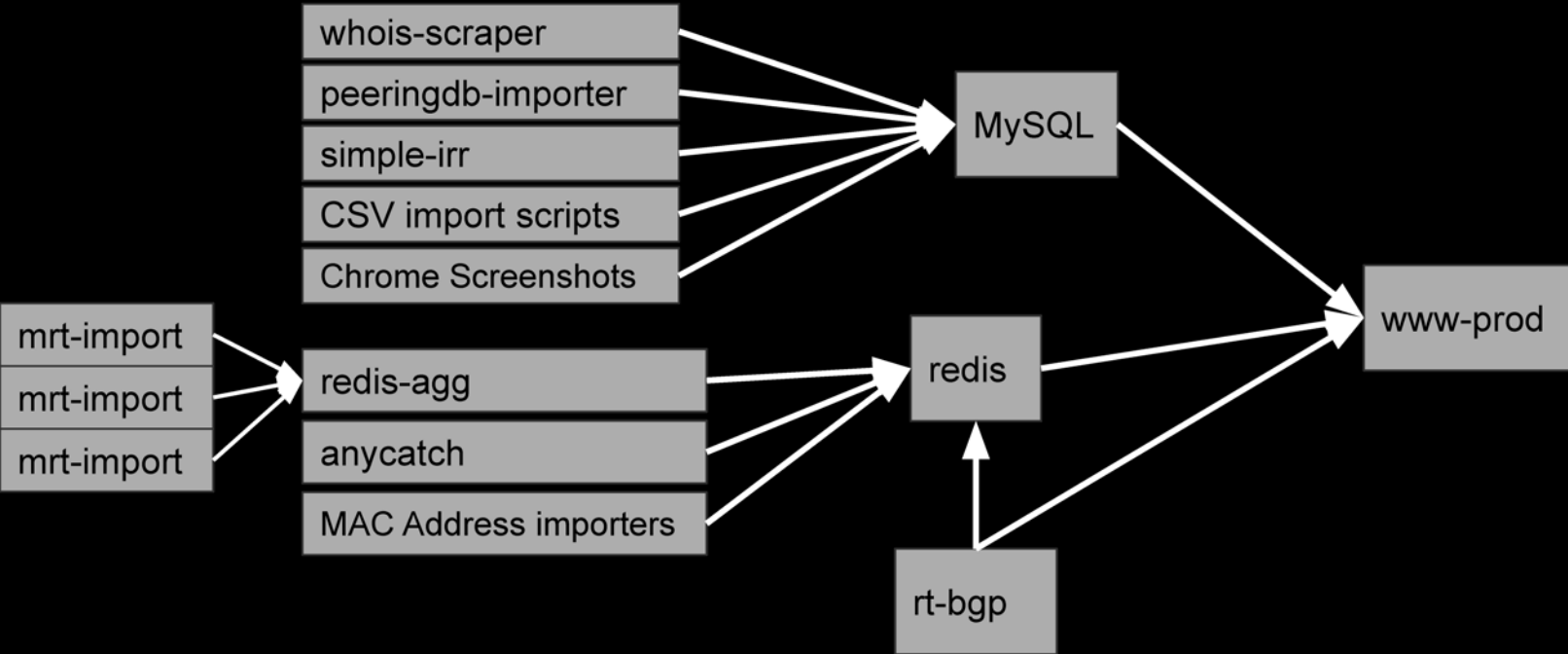


Updated 05 Mar 2022 14:09 PST © 2022 Hurricane Electric.

GraphViz Routing Spaghetti

How hard can it be?

General Data Flows of bgp.tools (last week's basic overview)



This way, it's remarkably cheap to run

- MySQL runs at ~13G of storage
- Redis sits at 4G of RAM (post all imports)
- The hilbert map data is 4GB since 2^{32} bytes = IP addresses
- The rDNS data lands in at 8GB of gzipped files (Custom DNS database format for speed and ease of update)
- The fDNS data lands in at 26GB (uncompressed)

Overall less than 64G of storage really needed, except the data has heavy churn so SSD writes can get a little spicy!

p99 page build and render is 200ms, p50 is 5ms

The hardest feature of bgp.tools

AS32787 Akamai Technolog | x +

bgp.tools/as/32787

bgp.tools Start here... →

View Edit

Akamai Technologies, Inc.

Website <https://www.akamai.com/us/en/cloud-security.jsp>

Access Denied

You don't have permission to access "http://www.akamai.com/us/en/cloud-security.jsp" on this server.
Reference #161-408803-168889708-4702048

Overview Prefixes Connectivity Whois IX

Registered on
23 Jul 2004 (17 years old)

Network status
Active, Allocated under ARIN

Network type
Content

Prefixes Announced
320 IPv4, 61 IPv6

Upstreams

Locations of Operation

aut-num: AS206924
as-name: BENJOJONET
org: ORG-BC129-RIPE
remarks: I'm not sure you can sue for emotional damages directly due to IP packet loss
...
mnt-by: BENJOJO
created: 2017-04-11T09:47:42Z
last-modified: 2020-12-29T17:28:18Z
source: RIPE
sponsoring-org: ORG-JS121-RIPE
...

organisation: ORG-BC129-RIPE
org-name: Ben Cartwright-Cox
org-type: OTHER
address: Dummy address for ORG-BC129-RIPE
e-mail: unread@ripe.net
abuse-c: ACRO5162-RIPE
mnt-ref: BENJOJO
mnt-by: BENJOJO
created: 2017-03-12T18:51:12Z
last-modified: 2019-05-11T14:25:32Z
source: RIPE
remarks: *****
remarks: * THIS OBJECT IS MODIFIED



View

Edit



Ben Cartwright-Cox

AS Number **206924**

Website <https://blog.benjojo.co.uk>



Overview

Prefixes

Connectivity

Whois

IX

aut-num: AS138211
as-name: MOEQING-AS-AP
descr: MoeQing Network Service
country: CN
org: ORG-VL5-AP
admin-c: YH2770-AP
tech-c: YH2770-AP
abuse-c: AM2427-AP
mnt-lower: MAINT-VMHAUSLIMITED-AP
mnt-routes: MAINT-VMHAUSLIMITED-AP
mnt-by: APNIC-HM
mnt-irt: IRT-MoeQing
last-modified: 2020-05-28T14:00:30Z
source: APNIC

organisation: ORG-VL5-AP
org-name: VMHaus Limited
country: GB
address: PO BOX 1363 45 Argyle Street
address: Cambridge
phone: +447378301289
e-mail: *****
mnt-ref: APNIC-HM
mnt-by: APNIC-HM
last-modified: 2019-08-27T12:56:33Z
source: APNIC



View

Edit



MoeQing Network Service

AS Number **138211**

Website <https://as138211.bgp.world/>



Overview

Prefixes

Connectivity

Whois

IX

```
[ JPNIC database provides information regarding IP address and ASN. Its use ]  
[ is restricted to network administration purposes. For further information, ]  
[ use 'whois -h whois.nic.ad.jp help'. To only display English output, ]  
[ add '/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'. ]
```

Network Information:

```
[Network Number]          210.235.64.0/18  
[Network Name]  
[Organization]           KDDI CORPORATION  
[Administrative Contact]  JP00000181  
[Technical Contact]      JP00000181  
[Abuse]                  abuse@dion.ne.jp  
[Allocated Date]        2003/02/05  
[Last Update]           2009/09/07 11:32:34 (JST)
```

Less Specific Info.

```
-----  
No match!!
```

More Specific Info.

```
-----  
No match!!
```


[16:52:

% Copyr
% The
% full
% bein
% repr
% any
% 2022

aut-num
owner:
ownerid
respons
country
owner-c
routing
abuse-c
created
changed
inetnum
inetnum
as-in:
as-in:
as-in:

```
% Copyright (c) Nic.br
% The use of the data below is only permitted as described in
% full by the terms of use at https://registro.br/termo/en.html ,
% being prohibited its distribution, commercialization or
% reproduction, in particular, to use it for advertising or
% any similar purpose.
% 2022-03-10T09:06:02-03:00 - IP: 2a0c:2f07:29:666:0:0:0:247
```

```
aut-num:      AS267263
owner:        VIVA TELECOM
ownerid:      14.216.538/0001-42
responsible:  Dione Conceição Lima
country:      BR
owner-c:      VITLT49
routing-c:    VITLT49
abuse-c:      VITLT49
created:      20180308
changed:      20210910
inetnum:      160.238.24.0/22
inetnum:      2804:4ac8::/32
as-in:        from AS52551 100 accept ANY
as-in:        from AS263047 100 accept ANY
as-out:       to AS52551 announce AS267263
as-out:       to AS263047 announce AS267263
```

Falsehoods programmers believe about Whois

- There is a single name a prefix / aut-num can have
 - There is any name at all a prefix / aut-num could have
 - That the whois server has a single language (KRNIC)
 - That the whois is transmitted in something UTF-8 ish
 - That the data given back to you by a RIR's whois server is UTF-8 compliant (LACNIC)
 - That the whois server is constantly online
 - That the whois server will respond correctly when it is online
-
- That there is whois at all
 - That RRDP is any different

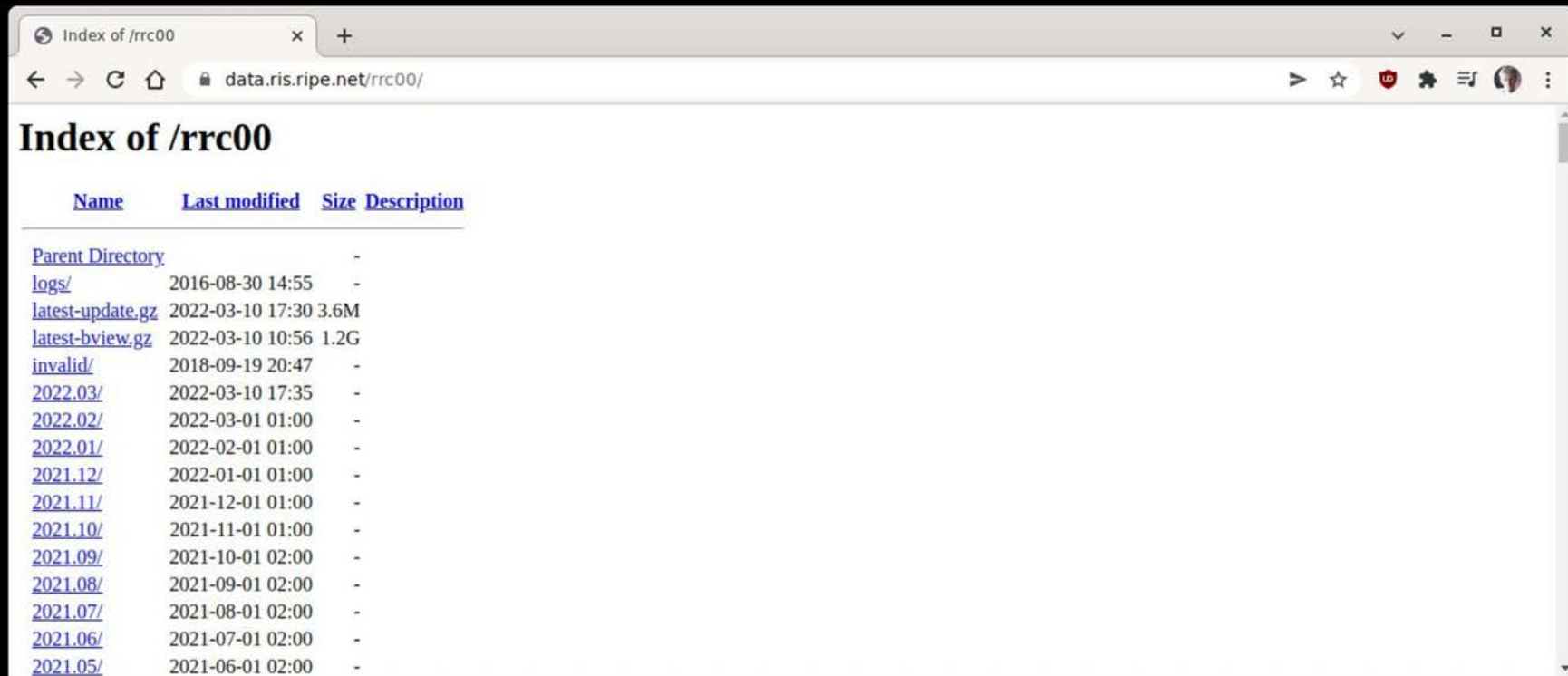
Falsehoods programmers believe about BGP

- Prefixes match against their whois records
- Prefixes match against their route/route6 objects
- Prefixes have any kind of functioning database entries at all
- Prefixes are only originated by one ASN
- That prefixes are necessarily globally visible
 - Looking at you Comcast/Bell mostly
- Peers fall into a easy Upstream/Downstream/Peer classification
- Upstreams are easy to detect at all
- That there is only one AS_PATH per route
- That private ASNs don't plague the table from some sources (thanks Vultr)

Standard Data Sources for these kinds of sites



Standard Data Sources for these kinds of sites



The screenshot shows a web browser window with the address bar displaying "data.ris.ripe.net/rrc00/". The page title is "Index of /rrc00". Below the title is a table listing directory entries with columns for Name, Last modified, Size, and Description.

Name	Last modified	Size	Description
Parent Directory		-	
logs/	2016-08-30 14:55	-	
latest-update.gz	2022-03-10 17:30	3.6M	
latest-bview.gz	2022-03-10 10:56	1.2G	
invalid/	2018-09-19 20:47	-	
2022.03/	2022-03-10 17:35	-	
2022.02/	2022-03-01 01:00	-	
2022.01/	2022-02-01 01:00	-	
2021.12/	2022-01-01 01:00	-	
2021.11/	2021-12-01 01:00	-	
2021.10/	2021-11-01 01:00	-	
2021.09/	2021-10-01 02:00	-	
2021.08/	2021-09-01 02:00	-	
2021.07/	2021-08-01 02:00	-	
2021.06/	2021-07-01 02:00	-	
2021.05/	2021-06-01 02:00	-	

Falsehoods programmers believe about MRTs

- MRTs are a single format... ish?
- The file extension is actually the compression encoding used
- That the file was published recently
- That the file will exist consistently on schedule
- That the peers in the MRT are still connected to the route collector
- That the peers on the route collector are not outright lying
- That there is upstream diversity in a single MRT file

Looking down the graph

- Everybody's gangster until a multi billion node graph turns up

Looking down the graph

- Everybody's gangster until a multi billion node graph turns up
- So bgp.tools cheats a little with hard coded T1 networks
- Upstreams are derived based on reachability to T1's

Looking down the graph

- Everybody's gangster until a multi billion node graph turns up
- So bgp.tools cheats a little with hard coded T1 networks
- Upstreams are derived based on reachability to T1's

```
PREFIX_AS_PATH: 185.230.223.0/24 [[4777 2516 1299 3170 206924]]
```

```
PREFIX_AS_PATH: 185.230.223.0/24 [[198290 2914 44684 206924]]
```

```
PREFIX_AS_PATH: 185.230.223.0/24 [[41157 3257 1299 3170 206924]]
```

```
PREFIX_AS_PATH: 185.230.223.0/24 [[20080 2914 3170 206924]]
```

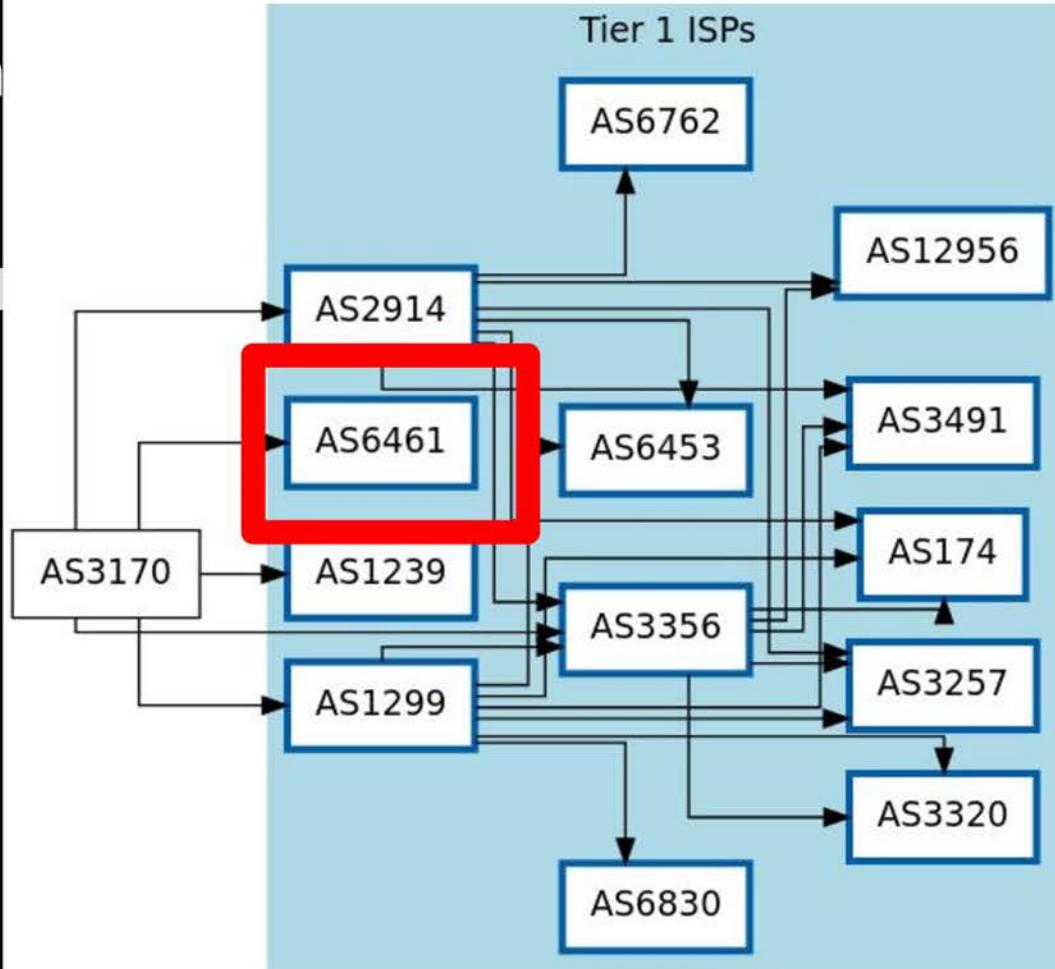
God dammit

- This was fine until Sprint and Zayo start accepting routes from route collectors in IXs
- Now people on IX's look like they have Sprint/Zayo transit!

Last 6 hours

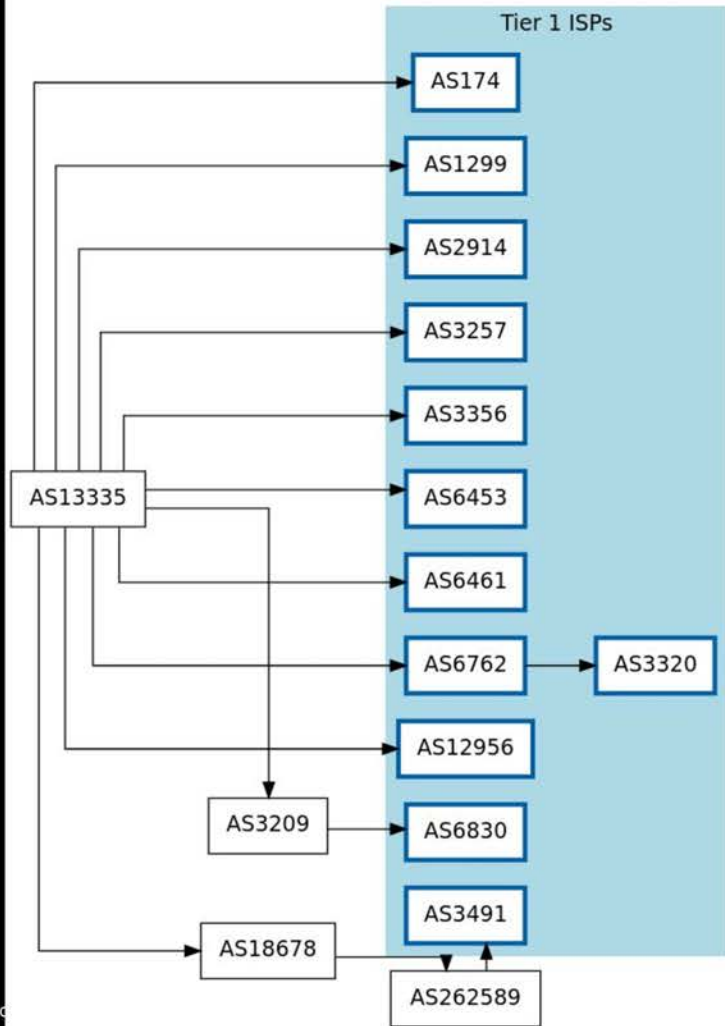
God damm

- This was route coll
- Now peo



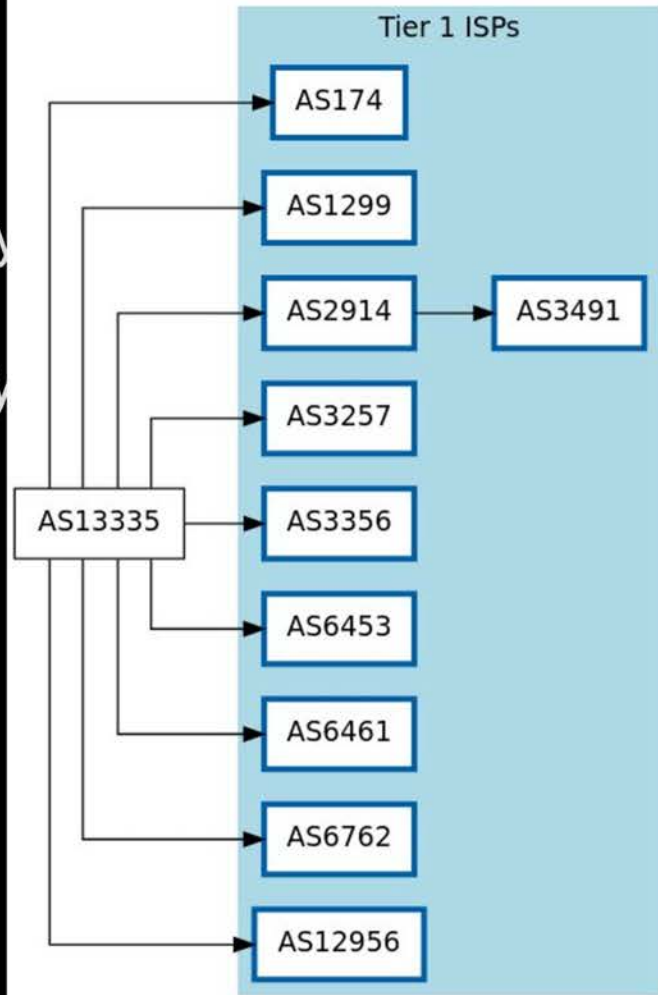
outes from
transit!

Last 6 hours



and Zay
like they

Last 6 hours



om

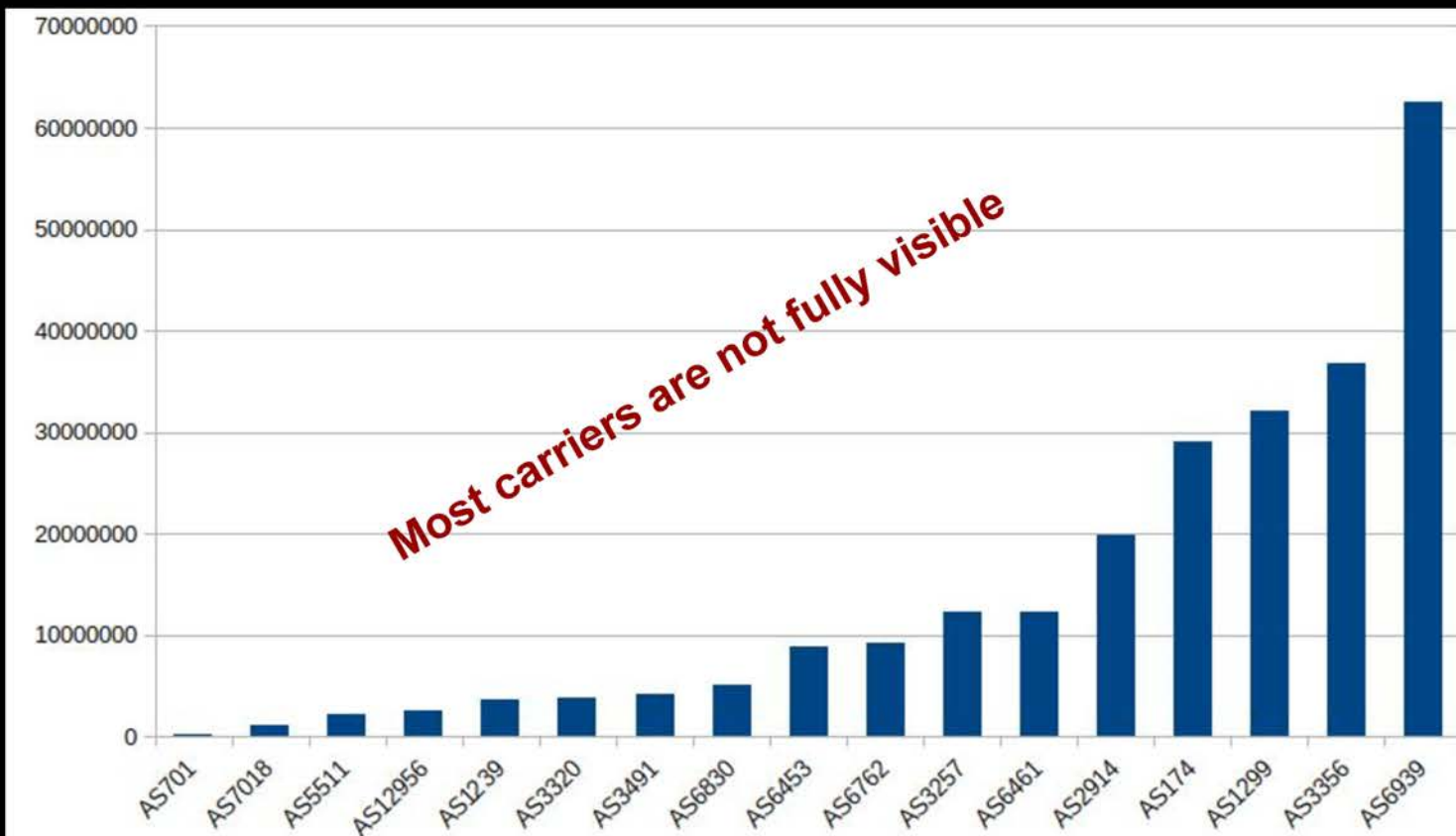
The awkward truth

These sites are only as good as the data they are provided

- Most MRT files seem to be heavily biased
- A lot of them have stuck routes
- De-biasing the data is really hard work
- Detecting stuck routes vs. Partially Visible is REALLY hard work
- Writing this kind of tool that 90% works is easy, the 99.9% is mind breaking
- Prepare to send a lot of polite "**wtf**" emails/IRC DMs to people/networks
 - I've sent over 120~ different messages in the last 4 years

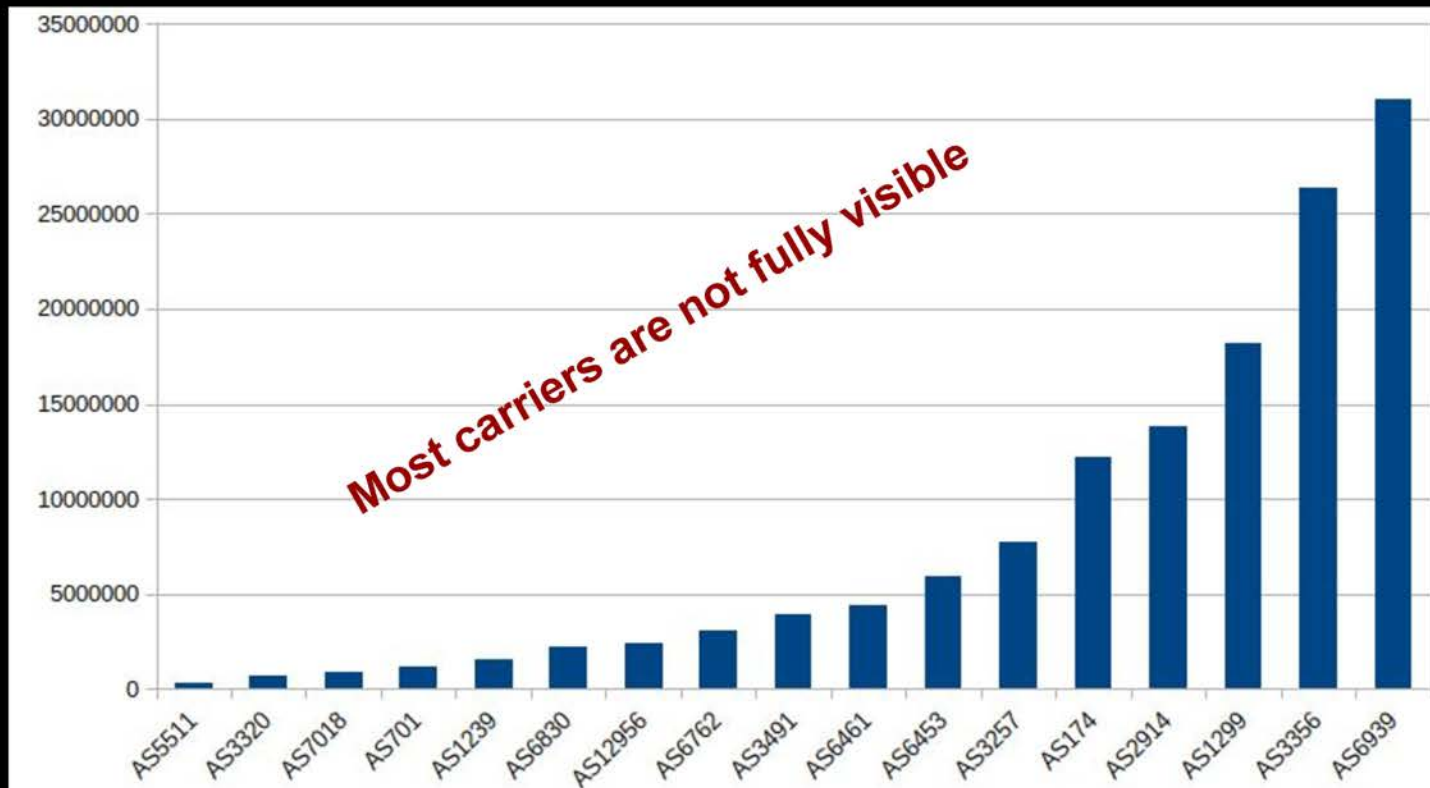
MRT files are not immune to bad data

- RIS:



MRT files are not immune to bad data

- RouteViews:



So what is bgp.tools doing about it?

We have built our own collector

Frictionless and easy

- Login via PeeringDB
- 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

[Contacts](#) **BGP Sessions** [Profile](#)

Configured BGP Sessions

Below are your ASN's (206924) BGP sessions setup with bgp.tools. You can add more, restart them, or delete them. This page updates automatically

	Description	OurASN/YourASN	Routes	AddPath	-
<input checked="" type="checkbox"/>	CYCLONE	212232/206924	154365	✓	Edit
<input checked="" type="checkbox"/>	OLD	65000/65000	0	✗	Edit
<input checked="" type="checkbox"/>	MONSOON	212232/206924	155923	✓	Edit

Recent connection failures that might have been you

Source IP	Dest IP	Their ASN	Reason
185.230.223.8	185.230.223.39	206924	ASN Looked Close, AS/SrcIP not right or configured

[Click here to add a new session](#)

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

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.

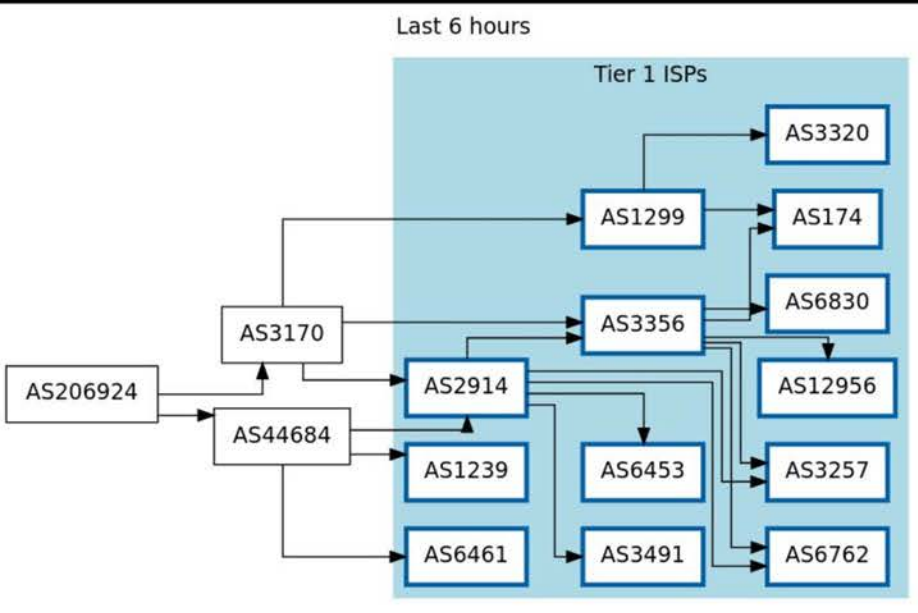
- Export this data into publicly available MRT files
- Also allow commercial products to use those MRT files
- Send notifications if session is down for more than 2 hours

A New BGP daemon for a new use case

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1	root	20	0	161M	9188	7780	S	0.0	0.0	0:01.14	/sbin/init
61	root	20	0	197M	116M	111M	S	0.0	0.3	0:44.77	- /lib/systemd/systemd-journald
128	messagebu	20	0	8196	3920	3692	S	0.0	0.0	0:00.02	- /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-
130	root	20	0	13344	5152	5044	S	0.0	0.0	0:00.32	- /lib/systemd/systemd-logind
184	root	20	0	2498M	30064	6872	S	0.7	0.1	37:04.04	- /usr/bin/neo-bgp-prod -apiserver -republish.target [REDACTED]
186	redis	20	0	76880	22380	8752	S	0.0	0.0	8:17.55	- /usr/bin/redis-server 127.0.0.1:6379
192	root	20	0	5416	2052	2040	S	0.0	0.0	0:00.00	- /sbin/agetty -o -p -- \u --noclear --keep-baud console 115200,38400,9600 linux
193	root	20	0	5416	2012	2004	S	0.0	0.0	0:00.00	- /sbin/agetty -o -p -- \u --noclear --keep-baud pts/0 115200,38400,9600 vt220
194	root	20	0	5416	1884	1868	S	0.0	0.0	0:00.00	- /sbin/agetty -o -p -- \u --noclear --keep-baud pts/1 115200,38400,9600 vt220
195	root	20	0	5416	1976	1960	S	0.0	0.0	0:00.00	- /sbin/agetty -o -p -- \u --noclear --keep-baud pts/2 115200,38400,9600 vt220
196	root	20	0	5416	2004	2004	S	0.0	0.0	0:00.00	- /sbin/agetty -o -p -- \u --noclear --keep-baud pts/3 115200,38400,9600 vt220
223	nobody	20	0	3422M	180M	6568	S	0.0	0.4	13:31.77	- /usr/bin/neo-bgp-prod -worker -tag yn0mbq712q -comment [AS206924 on [REDACTED] 41663]
251	nobody	20	0	4094M	806M	6492	S	0.0	1.8	48:39.24	- /usr/bin/neo-bgp-prod -worker -tag sfd2piagyx -comment [AS211562 on [REDACTED] :50239]
271	nobody	20	0	4101M	809M	6512	S	0.0	1.8	50:24.99	- /usr/bin/neo-bgp-prod -worker -tag j7filuxhvy -comment [AS205479 on [REDACTED] 033]
306	nobody	20	0	4101M	795M	6508	S	0.0	1.7	44:25.31	- /usr/bin/neo-bgp-prod -worker -tag 4jwvyniy7z -comment [AS212934 on [REDACTED] :60290]
362	nobody	20	0	4100M	813M	6492	S	0.0	1.8	49:17.11	- /usr/bin/neo-bgp-prod -worker -tag 5wagoqulvn -comment [AS207616 on [REDACTED] 51130]
397	nobody	20	0	4377M	976M	6612	S	0.0	2.1	1:01:45	- /usr/bin/neo-bgp-prod -worker -tag lfc6q2xd95 -comment [AS4294967290 on [REDACTED] 61561]
431	nobody	20	0	1920M	24104	6568	S	0.0	0.1	1:44.29	- /usr/bin/neo-bgp-prod -worker -tag wl8q2psgn6 -comment [AS44570 on [REDACTED] :57434]
472	nobody	20	0	3355M	171M	6444	S	0.7	0.4	12:31.19	- /usr/bin/neo-bgp-prod -worker -tag 3lqqf71m2z -comment [AS211562 on [REDACTED] :6879]
530	nobody	20	0	3354M	170M	6528	S	0.0	0.4	12:54.07	- /usr/bin/neo-bgp-prod -worker -tag wk771bp0x2 -comment [AS65530 on [REDACTED] :2]:43893]
609	nobody	20	0	3426M	166M	6560	S	0.0	0.4	10:13.71	- /usr/bin/neo-bgp-prod -worker -tag cm0dfyiii5 -comment [AS212934 on [REDACTED] :44849]
644	nobody	20	0	3354M	165M	6504	S	0.0	0.4	12:08.07	- /usr/bin/neo-bgp-prod -worker -tag 4z7kdw24d -comment [AS211562 on [REDACTED] :48223]
678	nobody	20	0	3354M	175M	6500	S	0.7	0.4	10:47.48	- /usr/bin/neo-bgp-prod -worker -tag 2lvvgywzui -comment [AS44570 on [REDACTED] :33396]
841	nobody	20	0	3496M	206M	6500	S	1.3	0.5	23:06.85	- /usr/bin/neo-bgp-prod -worker -tag bkt888awxg -comment [AS204345 on [REDACTED] :1]:56104]
2084	nobody	20	0	4647M	936M	6512	S	0.0	2.0	49:42.21	- /usr/bin/neo-bgp-prod -worker -tag poh5lglhoa -comment [AS207616 on [REDACTED] :9]
6791	nobody	20	0	5322M	1821M	6504	S	2.0	4.0	1:03:12	- /usr/bin/neo-bgp-prod -worker -tag 22axlgy13y -comment [AS208563 on [REDACTED] :3]
10187	nobody	20	0	3356M	168M	6512	S	0.0	0.4	1:33.55	- /usr/bin/neo-bgp-prod -worker -tag epe3xnk4la -comment [AS213021 on [REDACTED] :48813]
10372	nobody	20	0	3355M	150M	6404	S	0.0	0.3	1:45.45	- /usr/bin/neo-bgp-prod -worker -tag 3ksk81r5zk -comment [AS205479 on [REDACTED] :58]:48985]
11174	root	20	0	1919M	15748	6488	S	0.0	0.0	0:05.64	- /usr/bin/neo-bgp-prod -primary

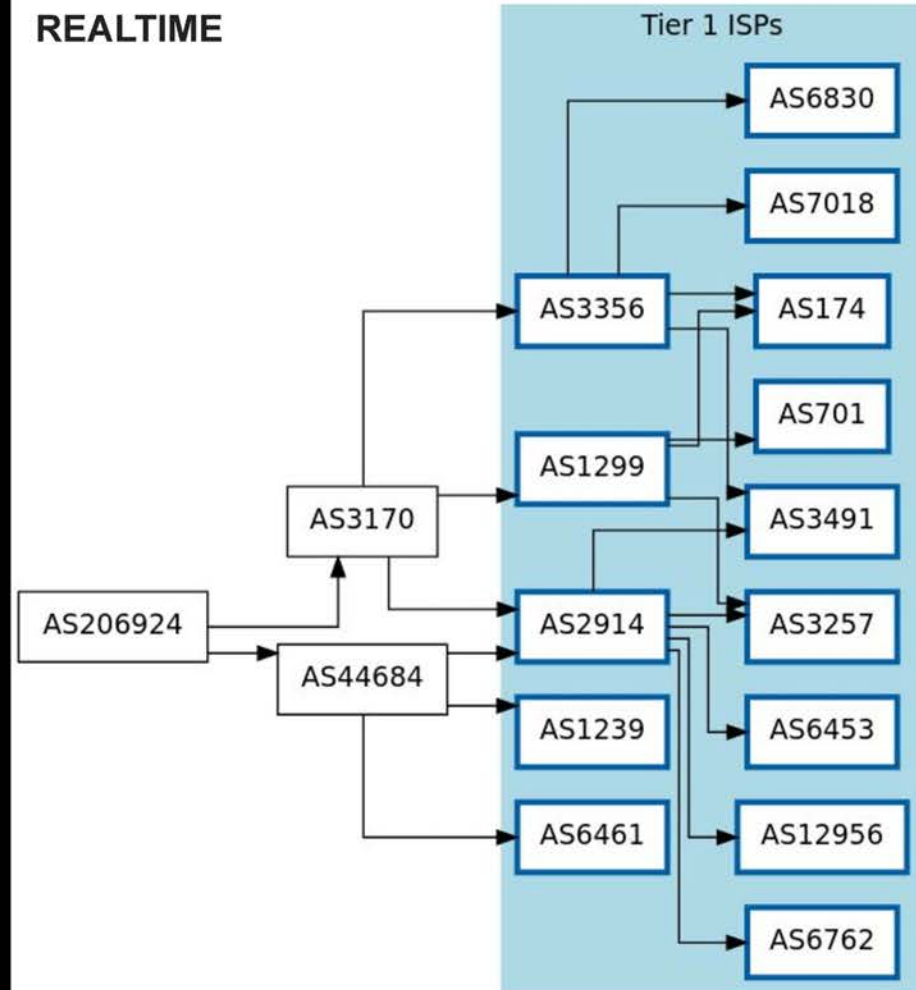
Est: March, It turns out if you don't need to insert routes writing a bgp daemon is easy, runs ~500 QPS reliability

MRT



Realtime Data

REALTIME



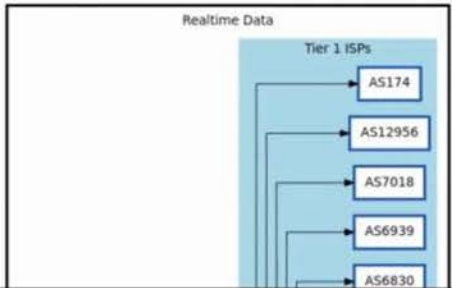


View Edit

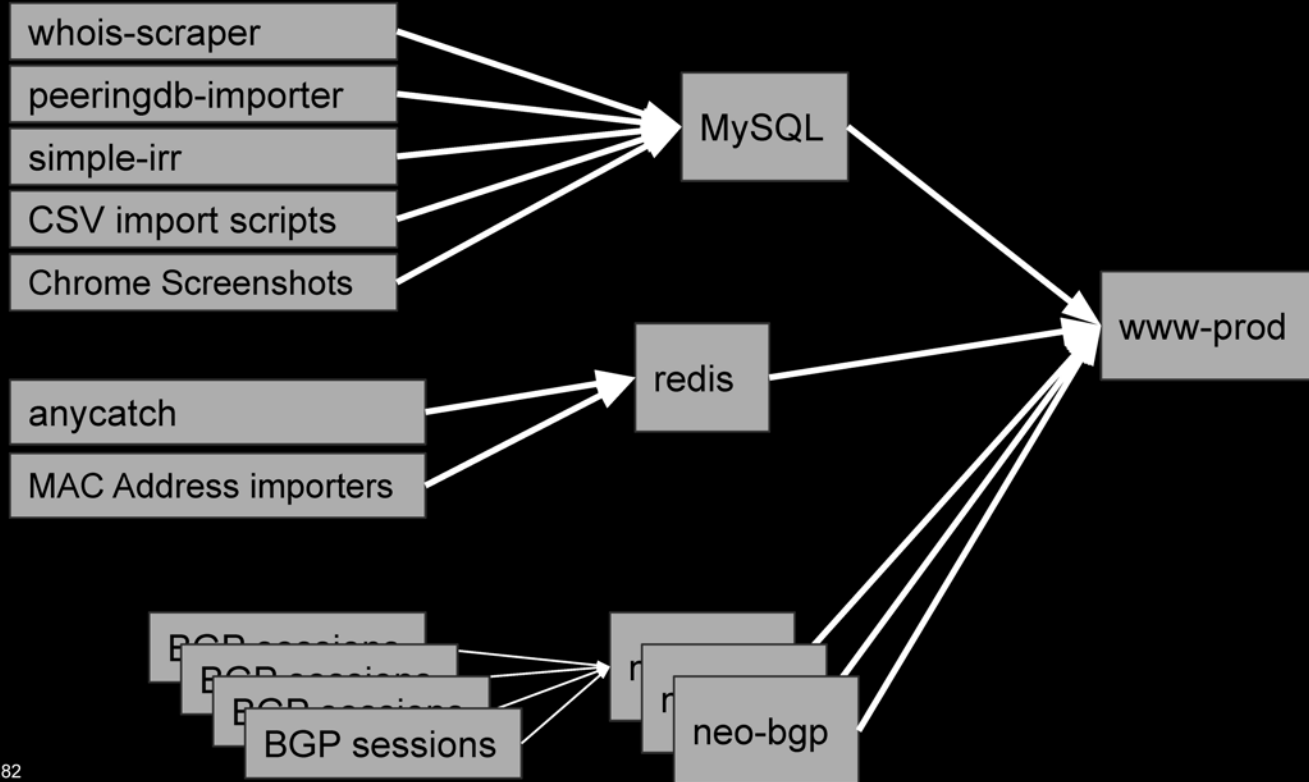
2a0c:2f07:ac1::/48

Taskbar with icons for: 2a0c2f07..., OBS 27.2..., CSSH [3], Terminal, CGP - Mon..., CSSH root..., CSSH root..., CSSH root..., redis-look..., New Tab..., benops - D..., Terminal, Terminal, Terminal, Terminal, DBeaver 2..., Terminal

Whois DNS Validation



New Sources of bgp.tools (basic overview)

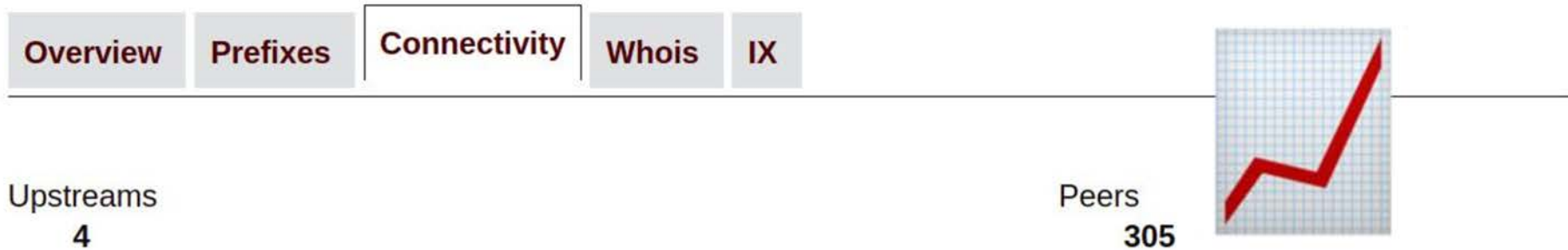


If you like this tool, Please setup BGP Collector sessions

- I'm in particular need for Orange (AS5511), Verizon (701) and AT&T Full table customers

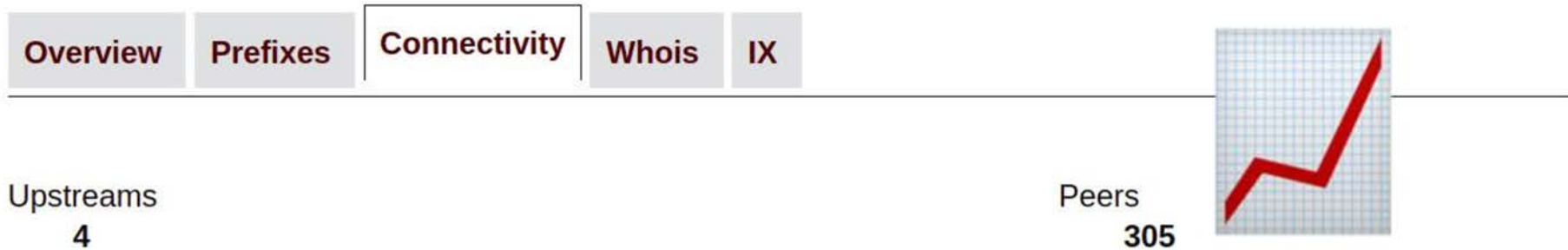
If you like this tool, Please setup BGP Collector sessions

- I'm in particular need for Orange (AS5511), Verizon (701) and AT&T Full table customers
- However if you want better peering numbers, you should feed anyway



If you like this tool, Please setup BGP Collector sessions

- I'm in particular need for Orange (AS5511), Verizon (701) and AT&T Full table customers
- However if you want better peering numbers, you should feed anyway



- Also help the academic community get access to unique AS Path data!

Questions? / Requests?

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

Longer term bgp.tools goals:

- Avoid being bought by that-one-company-that-buys-these-things ;)
- Work with poorly covered networks/regions to start sessions with 'tools
- Continue to build better debugging systems designed for real network engines to use, not marketing slides
- Historical data pull back
- **Talk to me in person for more info, I'm here until Friday**