



Let's Measure

- **Rethinking Address Reality: IPv4 Utilisation**
 - **Proxy Network Exposure in Australia**

Aftab Siddiqui

Head of Stakeholder Relations

[APNIC Foundation]



IPv4 Utilisation

Who is using Australian Resources

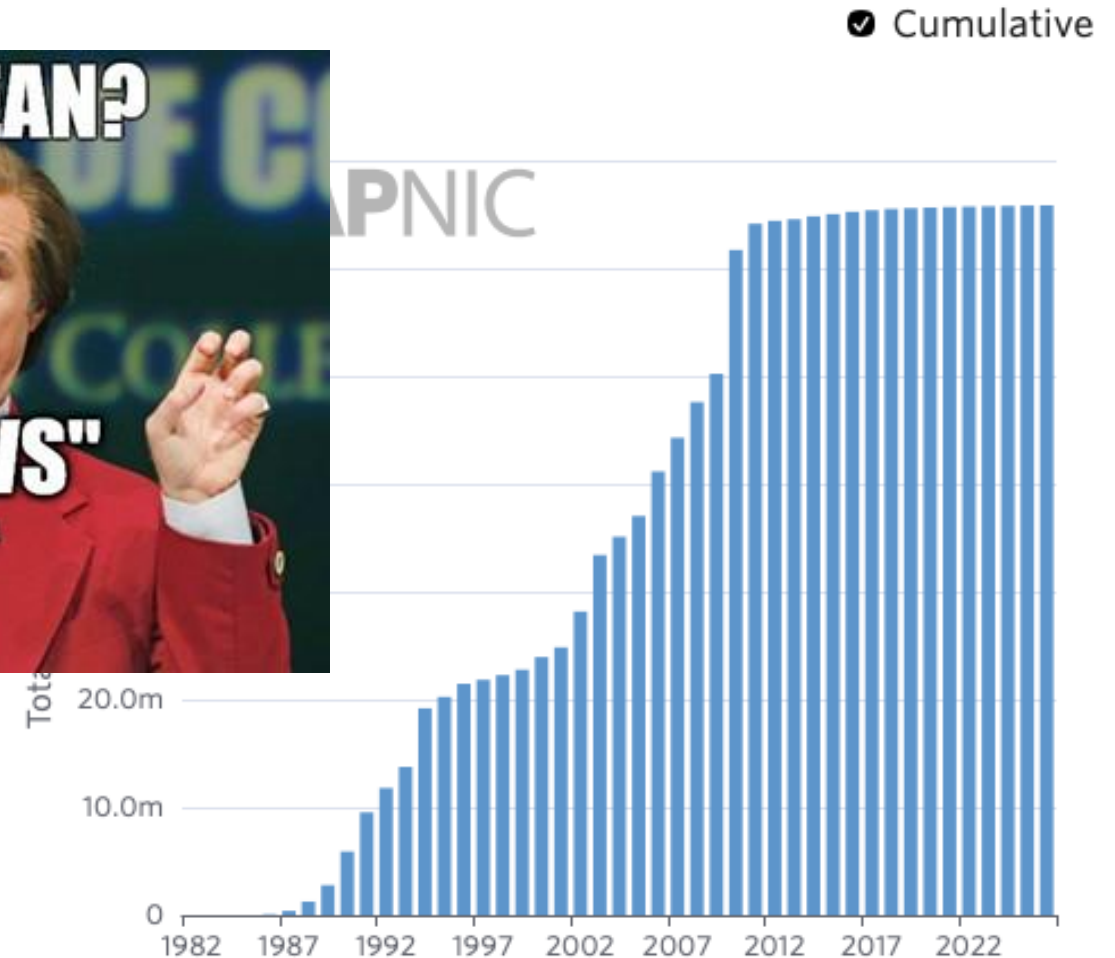


IPv4 Delegation

IP addresses	/24 prefixes	Delegations
65,830,912	257,152	16,106

As per the records published by APNIC

- Australia has more IPv4 addresses but not the capability that corresponds to 257K /24 prefixes.
- That's around 6.5% of the space APNIC has delegated in the APAC region
- There are 2760 unique entities holding those resources





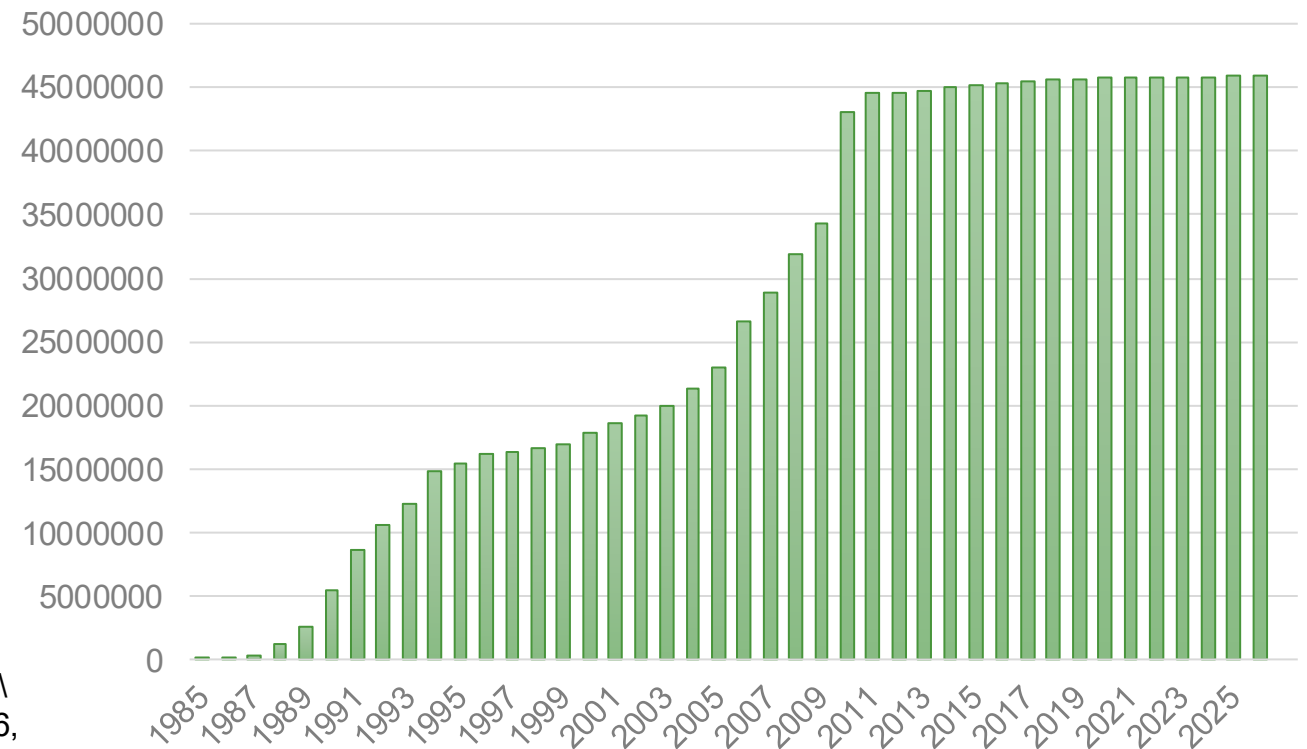
IPv4 Delegation [Real Figures]

But the real numbers are different from what is presented by APNIC REX.

- 45,886,208 addresses
- 179,243 /24s
- 9,867 delegation
- Entities (registrant handles): 2764

```
awk -F'|' \
'$1=="apnic" && $2=="AU" && $3=="ipv4" && $7!="summary" {n++; s+=$5} \
END {printf "%d delegations, %d addresses (%.1fM, %d /24s)\n", n, s, s/1e6, s/256}' nro-delegated-stats
```

Cumulative Addresses





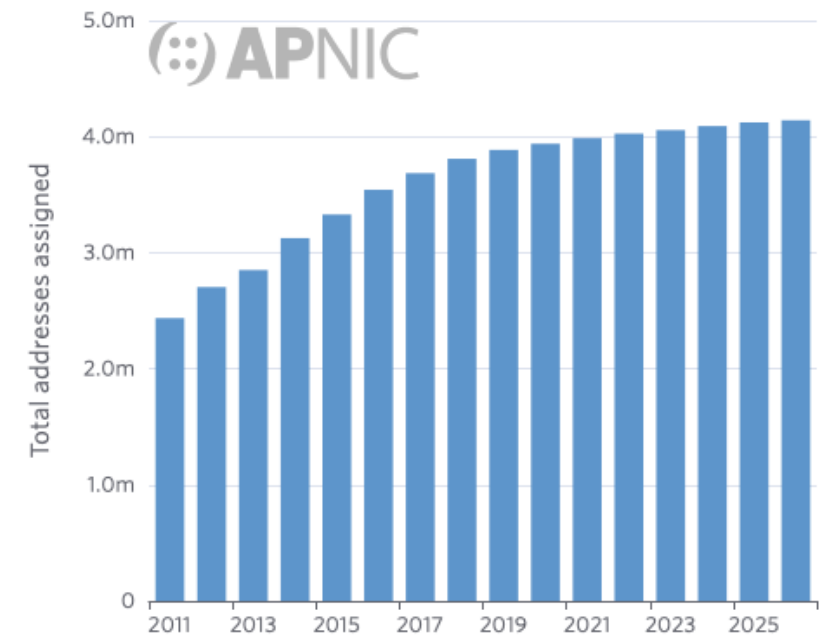
IPv4 Transfers

If the IPv4 resources are in abundance, then are we involved in transfer market?

IP addresses	/24 prefixes	Delegations
4,140,544	16,174	3,182

- Last 10 years graph suggest that we are adding more IPv4 space.
- Does that mean there are more transfers into the country?

✓ Cumulative



Don't Trust This!



IPv4 Transfers

APNIC provides transfer log of all resources. [1] – 20260810

Resource type	Total records
IPv4	16,624
ASN	3,580
IPv6	696

Direction	ASN	IPv4	IPv6
Into AU (to_economy == AU)	737	3,923	302
Out of AU (from_economy == AU)	754	4,423	309
Intra-AU (both from & to = AU)	697	3,640	295

Resource	Into AU	Out of AU	Intra-AU	Net (Into – Out)
ASN	737	754	697	-17
IPv4	3,923	4,423	3,640	-500
IPv6	302	309	295	-7

Metric	Into AU	Out of AU	Intra-AU	Net (Into – Out)
Individual IPv4 addresses	27,027,712	29,161,216	10,907,136	-2,133,504
Equivalent /24 blocks	105,577	113,911	42,606	-8,334



Geolocation

- Where is Australian IP address space actually located?
- Registry data says who holds it, not where it's deployed
- Three independent sources:
 - registry (APNIC/NRO),
 - routing (BGP),
 - geolocation (geofeed + commercial)
- RFC 8805: CSV of prefix → country, region, city, postal
- RFC 9632: how to find it — geofeed: attribute in whois (obsoletes RFC 9092)
- Published by the operator, who knows; commercial providers only infer
- Free, standardised, no infrastructure required



Geofeed adoption

Almost nobody publishes

- **520 of 9,867** AU delegations publish a geofeed - **5.3%**
 - 354 fully covered, 166 partly covered
 - 9,347 publish nothing at all i.e. **94.7%**
- At the network-object level: **1,913 of 129,371 i.e. 1.48%**
- **17.7%** of AU address space described i.e. 8.1M of 45.9M addresses
- Publishing delegations hold **15,644** addresses on average vs **4,650** overall
 - Adoption is concentrated among large operators but the long tail is silent



Geofeed Publishers – Top 10

Publisher	Addresses	/24s	Objects
geofeed.tools.telstra.net	12,845,056	50176	35
nettools.vocus.network	974,848	3808	39
geoip.aussiebroadband.com.au	304,128	1188	533
lg.superloop.com	203,520	795	54
geofeed.telstraglobal.net	91,136	356	34
cdn0.mysau.com.au	62,976	246	84
geofeed.swoop.com.au	50,176	196	11
raw.githubusercontent.com	46,336	181	47
spintel.net.au	42,240	165	6
zettagrid.com	37,632	147	19



Geofeed Publishers - Issues

- Hard to maintain, many operators not tracking of the url they published.
- `github.com/.../blob/...` returns HTML, not CSV — needs `raw.githubusercontent.com`
- URLs yield no valid data, concentrated on ~10 operators
 - 6 `https://acquirebpo.com/geofeed.csv`
 - 6 `https://www.xi.com.au/geo/RFC8805.csv`
 - 5 `https://emutel.net/geofeed.csv`
 - 4 `https://geofeed.oneqode.net/oq-geo-feed.csv`
 - 3 `https://github.com/githubapnic/geofeed/blob/main/prefixes.csv`
 - 3 `https://cdn.onaperim.com/ip/geo/geofeed_file.csv`
 - 2 `https://github.com/Viasat/geofeed/blob/main/geofeed.csv`
 - 2 `https://itsfubar.com.au/geofeed`
 - 2 `https://r2.sltry.au/geofeeds.csv`
 - 1 `https://amuri.net/geofeed/geofeed.csv`



Where Australian IP space actually is

Conflicts

NZ->AU: 4
AU->SG: 1
VN->SG: 1
SG->GB: 1
GB->US: 1
AU->US: 1

Geofeed data		
Economy	/24s	%
AU	31366	98.92
IN	91	0.29%
JP	55	0.17%
SG	46	0.15%
US	28	0.09%
NZ	21	0.07%
HK	13	0.04%
GB	10	0.03%
KR	8	0.03%
TW	7	0.02%
ZA	6	0.02%
DE	6	0.02%

Ipinfo.io		
Economy	/24s	%
AU	153026	98.89
US	441	0.28%
NZ	362	0.23%
JP	176	0.11%
SG	163	0.11%
IN	156	0.10%
HK	81	0.05%
MY	58	0.04%
GB	48	0.03%
DE	24	0.02%
ZA	21	0.01%
NL	20	0.01%



Where Australian IP space actually is

- **98.9% in Australia** (confirmed by geofeeds and ipinfo)
 - IPinfo 98.89% · geofeeds 98.92%
 - NSW 41.7% · VIC 26.7% · QLD 13.1% · WA 8.2% · SA 6.9%
 - Sydney 38.8% · Melbourne 25.6% · Brisbane 10.0%
- Only 1.1% deployed offshore
- **Caveat: 13.7% of AU space is unrouted and unmeasurable**
- **The two sources agree on country. They don't agree on city.**
- Country: **99.97%** agreement (9 mismatches in 31,710)
- City: **80.5%** i.e. 6,139 prefixes disagree
- Commercial data pulls toward capitals; operators name the actual town



Proxy Network Exposure

We are providers of large residential proxy network



What is a residential proxy?

- A service that routes your traffic through someone else's home internet connection
- The target website sees a residential ISP address, not a datacentre
- Sold by the gigabyte (data volume), priced by country and city
- Australian exits carry a premium i.e. high-value geo for streaming, betting, retail

	Datacentre proxy	Residential proxy
IP registered to	Hosting provider	Consumer ISP
Blocked by	Easily, by ASN	Hard, blocking hits real customers
Cost	Cents/GB	Dollars/GB
Supply	Bought	Sourced from end users

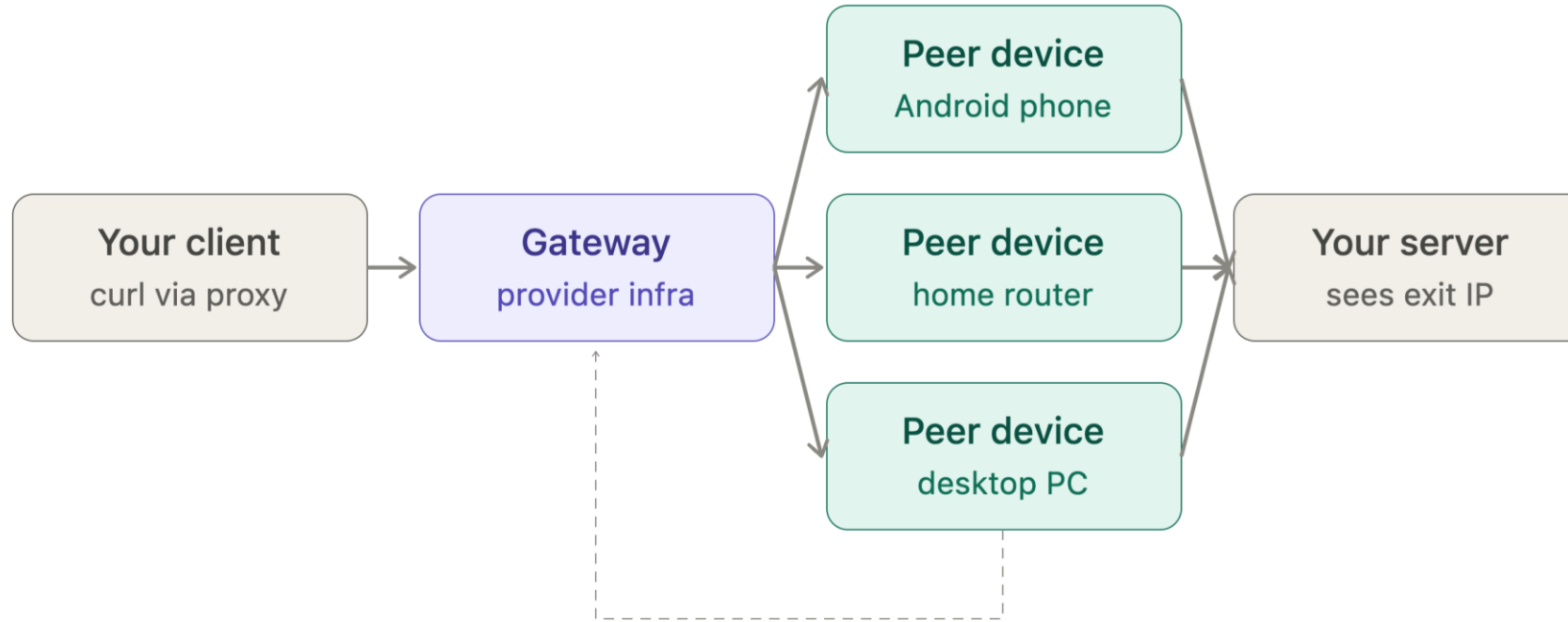


Where the IPs come from

- Three sourcing models, very different consent stories:
 - SDK monetization: a free app embeds a proxy SDK; the user "agreed" in a ToS nobody read. The app developer is paid per device.
 - Explicit opt-in: user installs software and is paid or gets a service in return. Rare.
 - Malware / unauthorized: device compromised, owner unaware.
- The line between (1) and (3) is thinner than the industry admits. A consent buried on page 14 of a EULA, on a device owned by someone who never read it, is functionally close to unauthorised use of their connection and bandwidth.

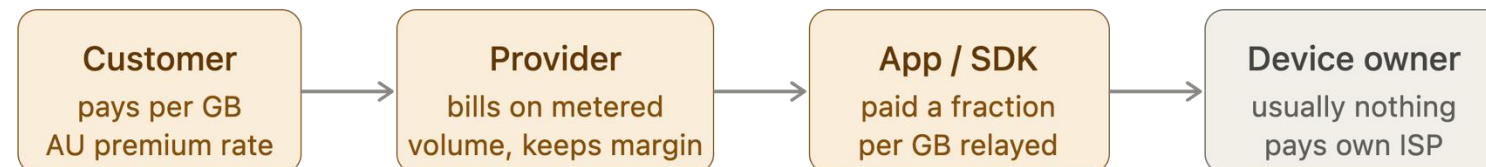


How a request actually flows



tunnel opened earlier by the peer, outbound through NAT

Money





Why should anyone care?

- Geolocation is a control surface. These decisions are made from an IP address:
 - Content scrubbing
 - Social Media clicks
 - LLM training?
- Residential proxies exist to make that control surface unreliable and they work because the address genuinely belongs to an Australian household.
- The householder's IP accrues the reputation damage from someone else's scraping, credential stuffing, or fraud
- Blocking the abuse means blocking a real residential customer



Market scale - external figures

Provider	Australia	Japan	South Korea	Canada
Shifter	2,358,149 (~2.36M)	3,139,296 (~3.14M)	2,892,793 (~2.89M)	4,284,786 (~4.28M)
Oxylabs	~1,980,646	~2,633,211	~1.3M+	~3,568,500
Bright Data	543,966	557,566	291,188	404,950
IPRoyal	584,915	487,067	66,728	373,796
FloppyData	Not Available	24,395	Not Available	25,360

Numbers taken from the service provider website (claims not verified)



Lets try to fingerprint these devices

Layer 2: Proxy measurement

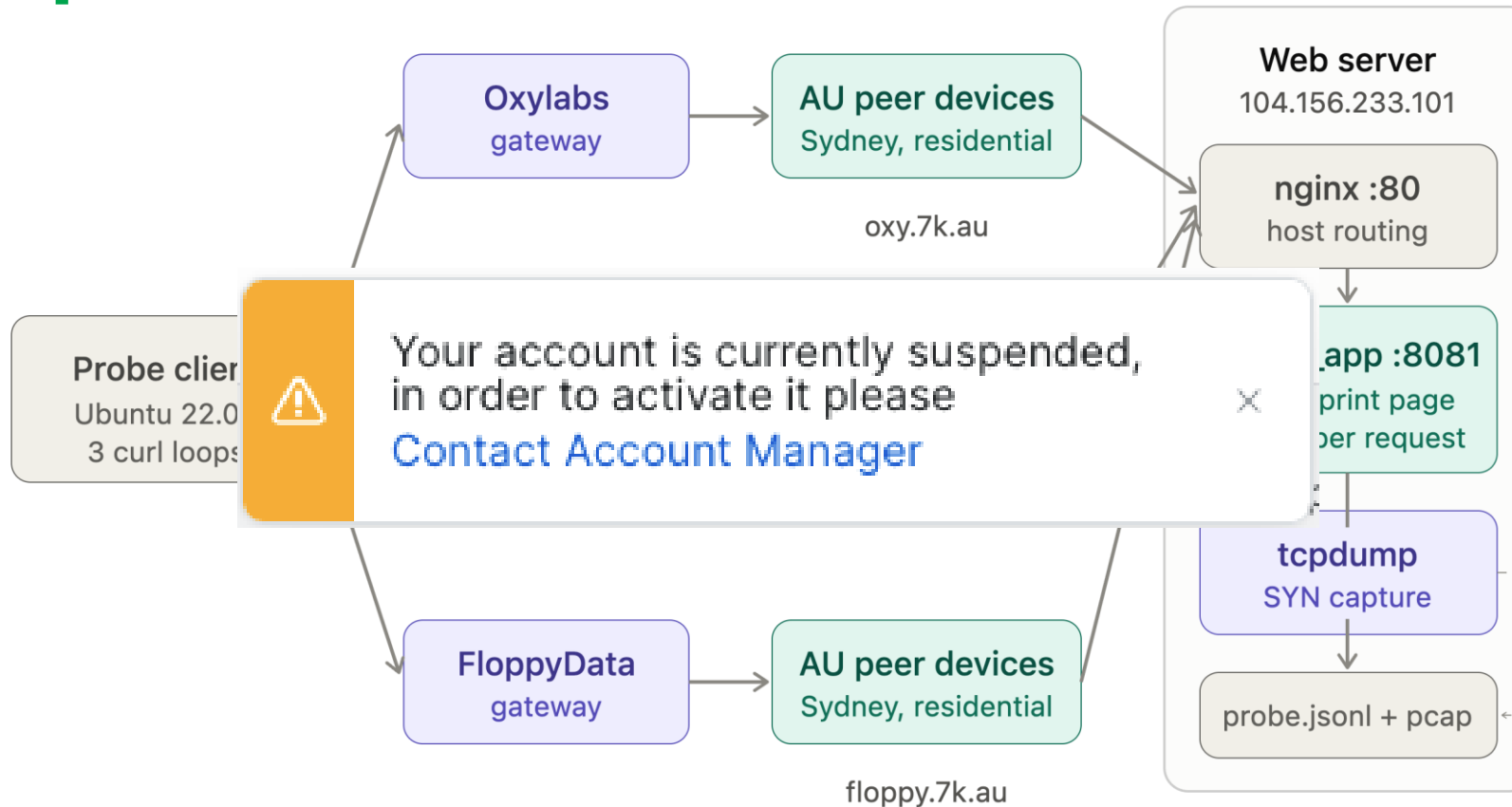
- Five providers: Oxylabs, IPRoyal, FloppyData, Shifter, BrightData
- All requests targeted **Sydney (2wks), Melbourne (1wk), Brisbane (1wk)**
- Per-provider hostname (oxy. / royal. / floppy./bright./shifter.7k.au) → provider tagged at the transport layer
- Per-request token → server-side and client-side logs join exactly
- Instrumented endpoint logs headers, header order, client IP, timing

Layer 3: Device characterisation

- tcpdump on SYN packets → TTL, MSS, TCP options, timestamp tick rate
- Browser fingerprinting page (canvas, WebGL, fonts, WebRTC)



The Setup



Each provider gets its own hostname, so the Host header tags the request without a query string.
nginx forwards the exit IP via X-Real-IP; tcpdump captures the same handshakes independently.
A per-request token joins the HTTP log, the fingerprint payload and the packet capture.



The Setup

5 Proxy
Providers

3 Cities
SYD, MEL, BNE

~500,000
Request

28,217
Unique IPs

25,272
IPv4

2,945
IPv6

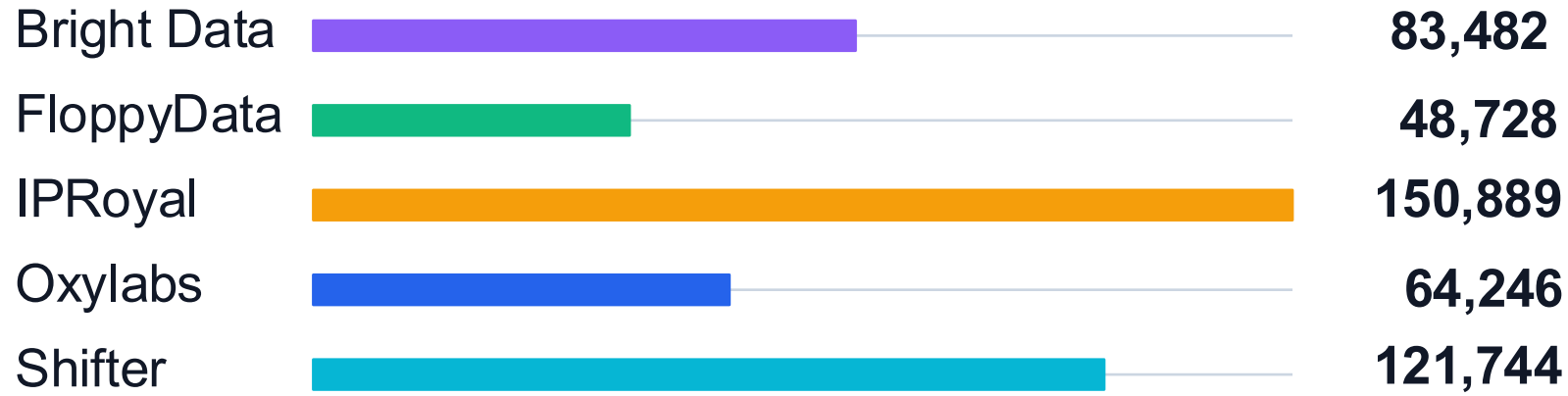
Address family by observation count

IPv4 ~90%

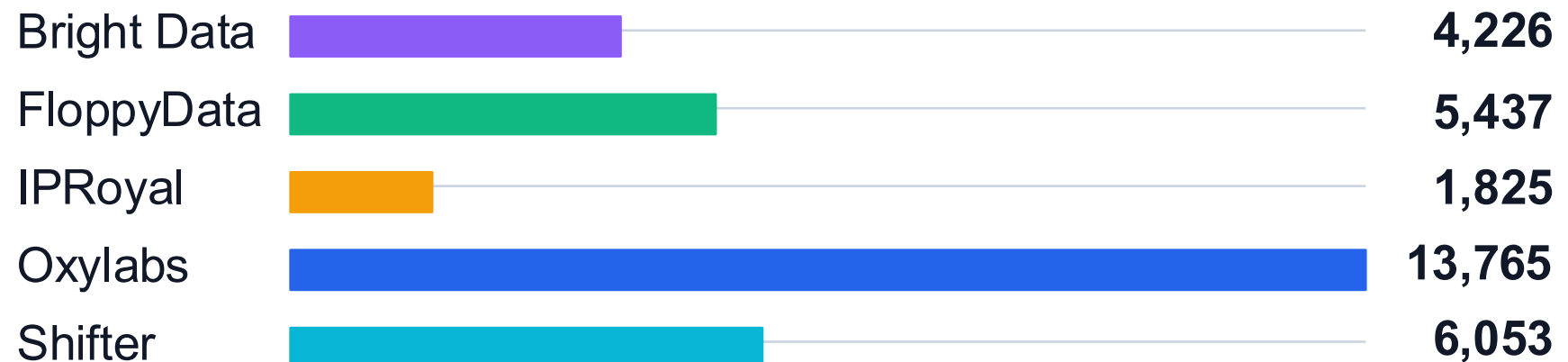
IPv6
~10%



The Setup



Unique public exits





The Setup

City	Obsv	Uniq	%	Obsv IPv4	Uniq IPv4	Obsv IPv6	Uniq IPv6
Brisbane	107,712	4,978	21.638	97,229	3941	10,483	1,037
Melbourne	86,125	8,999	9.571	77,452	7515	8,673	1,484
Sydney	275,252	14,335	19.201	273,027	13908	2,225	427

Overlaps

City_A	City_B	Uniq_A	Uniq_B	Shared
Brisbane	Melbourne	4978	8999	49
Brisbane	Sydney	4978	14335	19
Melbourne	Sydney	8999	14335	31



The Setup – Proxy Overlaps

2,747

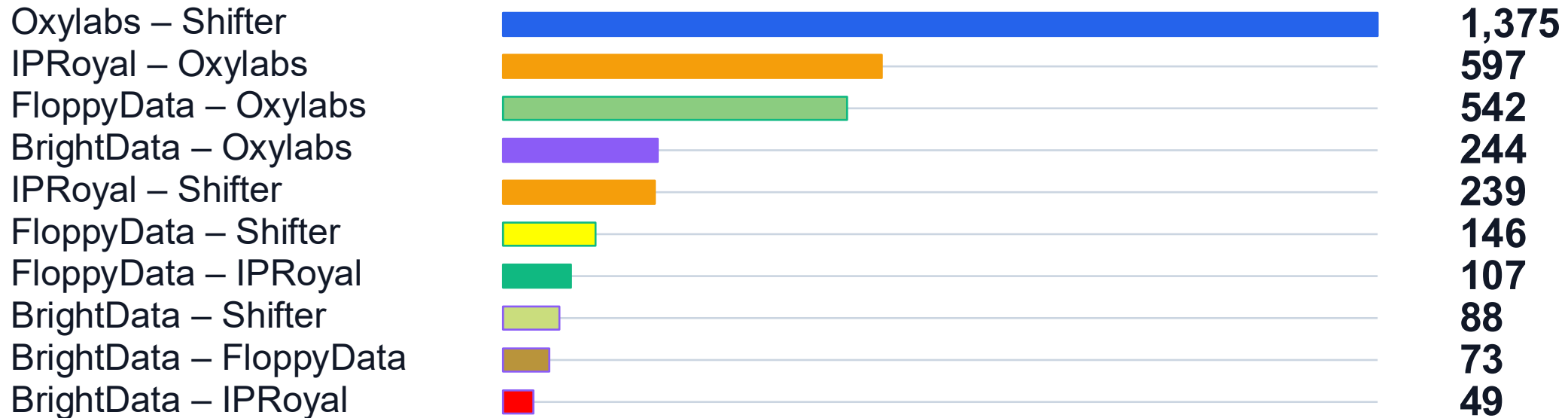
seen in ≥ 2 providers

314

seen in ≥ 3 providers

27

seen in ≥ 3 providers



Top provider-pair overlaps

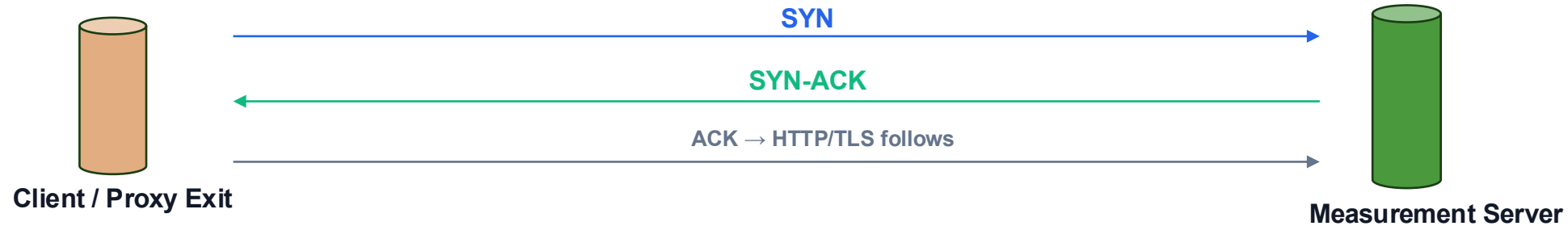


Top Proxy Hosting ASNs

ASN	AS Name	Uniq IPs
1221	ASN-TELSTRA - Telstra	6668
7545	TPG-INTERNET-AP - TPG Telecom Limited	4776
4804	MPX-AS - Microplex PTY LTD (Optus)	3099
4764	WIDEBAND-AS-AP - Aussie Broadband	2571
14593	SPACEX-STARLINK - Space Exploration Technologies Corporation	1925
38195	SUPERLOOP-AS-AP - Superloop	1831
9443	VOCUS-RETAIL-AU - Vocus Retail	1572
133612	VODAFONE-AS-AP - Vodafone Australia Pty Ltd	943
14618	AMAZON-AES - Amazon.com	618
135887	TELSTRA-BELONG-AP - Belong (Telstra Limited)	613
13335	CLOUDFLARENET - Cloudflare	266
18390	SPINTEL-AS-AP - Spintel Pty Ltd	261
36183	AKAMAI-AS - Akamai Technologies	214
136994	SOUTHERNPHONE-AS-AP - Southern Phone Company Ltd	195
134090	LEAP-AS-AP - Leaptel	173



The Setup – Sample Data



--- probe.jsonl (what the application saw) -----

```
time          2026-08-17T00:31:48Z
provider      iproyal   (from Host: royal.7k.au)
token         7740192fe55a4ee3
exit IP       125.209.156.251
path          /?seq=744&session=ed390aa986a94ea7
behind nginx  True     (peer_ip 127.0.0.1)
header order  X-Real-IP | X-Forwarded-For | Host | X-Forwarded-Proto | Connection | User-Agent | Accept
X-Real-IP:    125.209.156.251
X-Forwarded-For: 125.209.156.251
Host:         royal.7k.au
X-Forwarded-Proto: http
Connection:   close
User-Agent:   curl/7.81.0
Accept:       */*
```



The Setup – Sample Data

--- pcap (what the peer's TCP stack revealed) ----

source port 35308 -> 80

TTL observed 53 (initial 64, so ~11 hops away)

TCP window 64240

MSS 1440

option order MSS-SAckOK-Timestamp-NOP-WScale

TSval at SYN 1739354674

packets seen 15 in the window



The clocking mechanism

TCP timestamps give us a counter generated by the TCP endpoint. Extract the TSval from every timestamp-bearing packet and pair it with the packet's capture time. Within each individual TCP connection, plot TSval against elapsed real time and fit a straight line. The slope of that line gives us timestamp ticks per second e.g:

A TSval increase of roughly 1,000 ticks per second corresponds to a ~1000 Hz timestamp rate. We only accepted measurements with at least three samples over 250 milliseconds. What emerged were four clear recurring rate families around 100, 250, 300 and 1000 Hz.

Measured rate
~1000 Hz
~300 Hz
~250 Hz
~100 Hz
Absent

Why it survives a proxy: the SDK relays HTTP, but the peer's own kernel builds the TCP segments. Nothing at the application layer can change this.



The clocking mechanism - Device class results

Rate family	Classified exits	Share
~1000 Hz	7,983	70.80%
~300 Hz	1,394	12.36%
~100 Hz	975	8.65%
~250 Hz	778	6.90%
Other	146	1.29%
Total	11,276	100%

We did not start by assuming that 100, 250, 300 and 1000 Hz represented particular operating systems. We measured timestamp rates independently inside TCP connections and found that the observed population repeatedly clustered around those four rates.



The clocking mechanism - Device class results

TCP timestamp-rate families across proxy providers

Provider	Classified exits	~1000 Hz	~300 Hz	~250 Hz	~100 Hz	Other
Bright Data	1,885	67.32%	0.16%	5.78%	24.77%	1.96%
FloppyData	2,254	85.85%	0.93%	8.83%	3.42%	0.98%
IPRoyal	1,368	67.47%	15.86%	9.28%	6.29%	1.10%
Oxylabs	4,785	68.32%	19.46%	6.54%	4.08%	1.61%
Shifter	2,417	61.69%	25.11%	4.63%	8.40%	0.17%

Provider numbers are non-exclusive. Of 11,276 strongly classified endpoints, 1,336 (11.9%) appeared through multiple providers, producing 12,709 provider memberships.



TTL, MSS, Window and Timestamp

Field	Observed example	What it tells us
TTL	53; likely initial 64	If initial TTL=64, approximately 11 hops . Useful as a coarse path/topology signal; initial TTL is inferred, not observed.
MSS	1440	Advertised maximum TCP payload. Can reflect MTU, encapsulation or MSS clamping; path-influenced, not device-specific .
Window	64240	TCP implementation/configuration signal. Useful with WS/SACK/options, but not enough to assign an OS by itself.
Option order	MSS-SACK-TS-NOP-WS	The order and padding of SYN options are usually set by the originating TCP stack, making them less path-dependent than TTL or MSS.
Timestamp rate	~100/~250/~300/~1000 Hz	Independently measured TCP timing family; adds discrimination to the static SYN fingerprint.



TTL, MSS, Window and Timestamp

Coverage	Stack Families	% covered	Core behaviour
Top 1	1	31.94%	WIN 64240, WS7, TS, MSS-SACK-TS-NOP-WS
Top 3	3	56.87%	WIN 65535, WS8, no TS, MSS-NOP-WS-NOP-NOP-SACK
Top 5	5	73.72%	WIN 65535, WS8, TS, MSS-SACK-TS-NOP-WS
Top 10	10	91.88%	WIN 65535, WS6, TS, MSS-SACK-TS-NOP-WS
Top 20	20	98.06%	WIN 64240, WS8, no TS, MSS-NOP-WS-NOP-NOP-SACK
All observed	112	100%	

WIN 64240
WS 7
SACK yes
TS yes
MSS-SACK-TS-NOP-WS
DF yes
likely initial TTL 64

Linux-family TCP stack signature



Limitations - These exits do not render anything

- Across the full run, the probe page was served with five 1×1 tracking pixels. **Zero were ever fetched.** 😞
- The exit retrieves the response body and stops
- No HTML parsing, no sub-resources, no JavaScript
- One customer request = exactly one connection from one exit
- Device matching by clock skew didn't work.



What can be done

For ISPs/Network operators

- Detect the tunnels. Proxy SDKs hold persistent outbound connections from consumer CPE to a small set of gateway endpoints. Long-lived flows to the same handful of destinations, from thousands of unrelated subscriber lines, are visible in NetFlow without any packet inspection.
- Check your own ranges. I found proxy exits concentrated in specific consumer /24s. I will share all the data with who ever is interested.

For End Users

- Visit <https://lookup.7k.au>
- Enter your IP address, if you see this banner then contact me

PROXY EXIT OBSERVED

This public IP address was observed as an exit during controlled residential-proxy measurements.



Thankyou

aftab.siddiqui@apnic.foundation