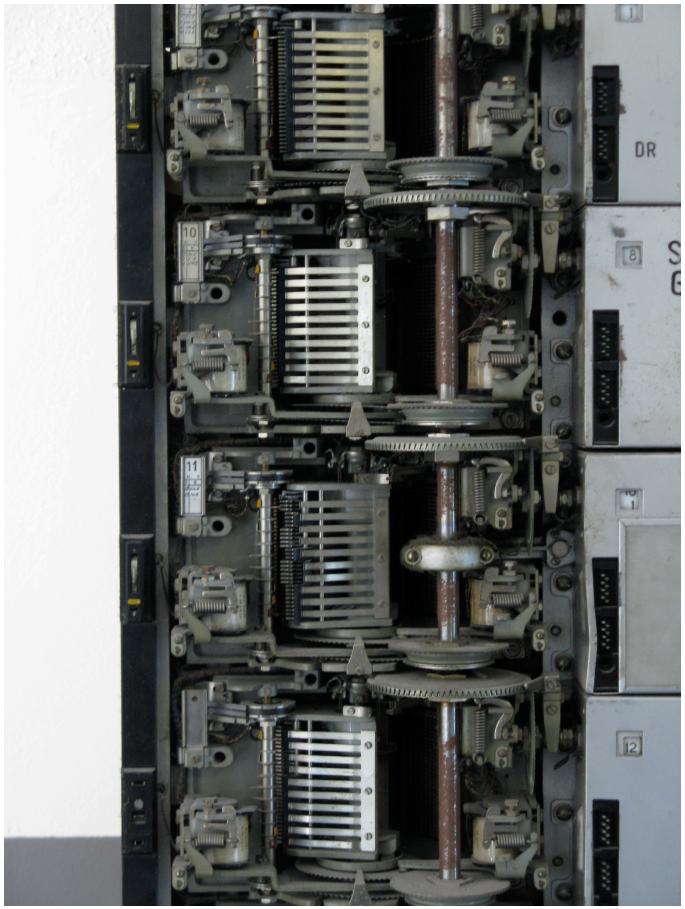
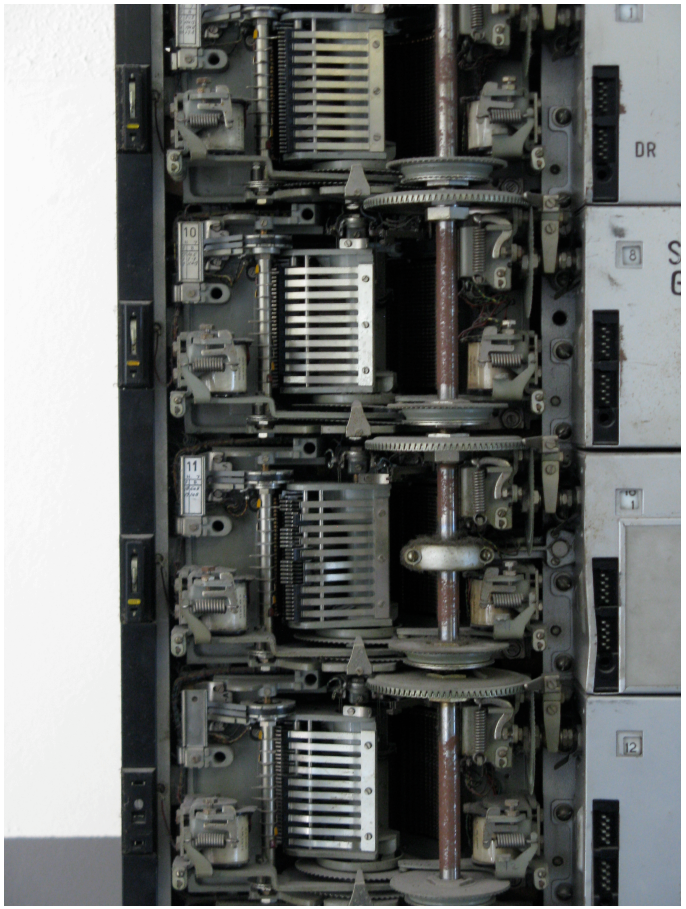
Observation-Hypothesis

ESNOG/GORE BILBAO



ESNOG/GORE BILBAO



ESNOG/GORE MADRID

New GORE/ESNOG RULE

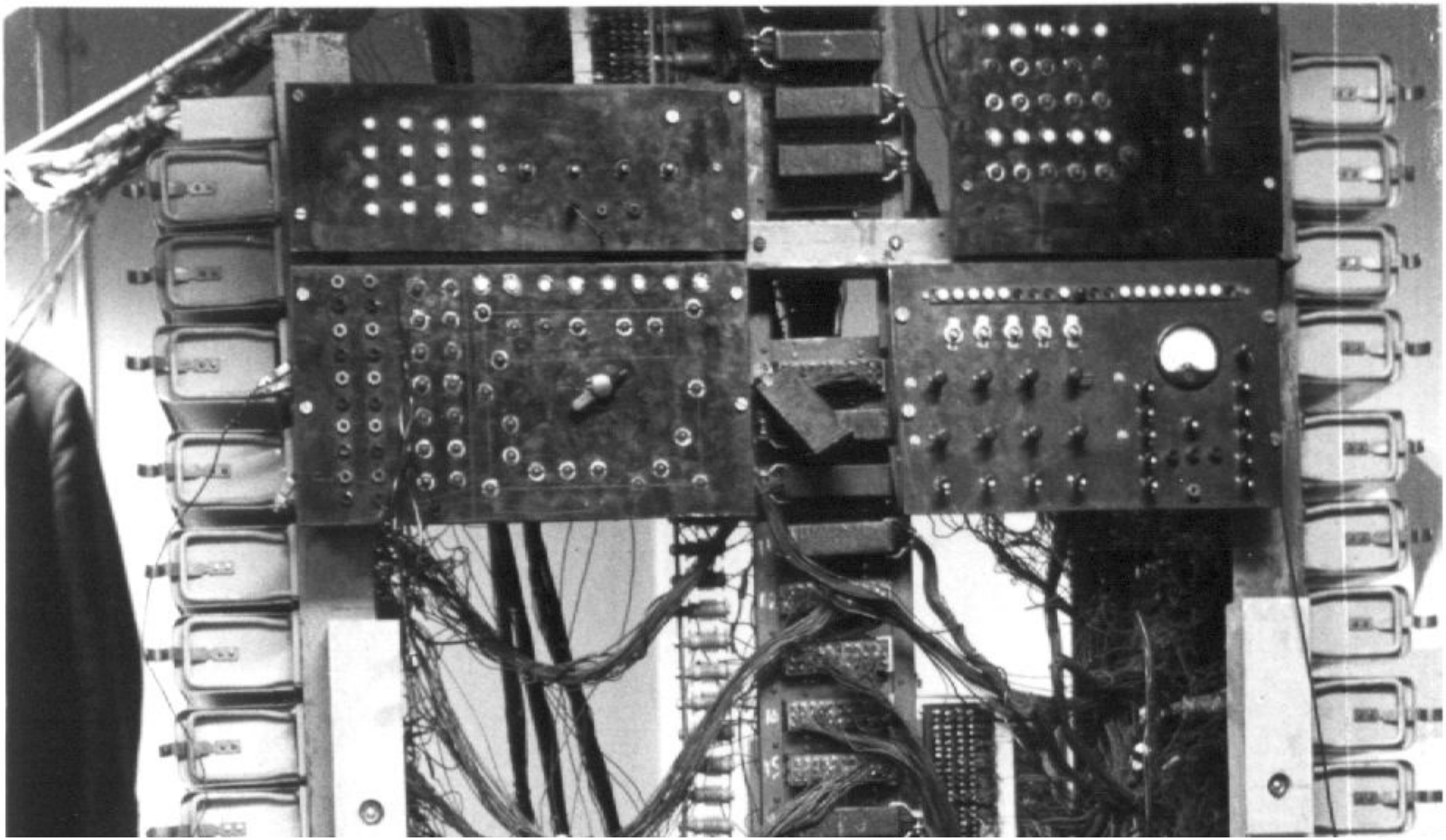
Only held in venues with
“Strowger”
Mechanical Telephone Exchange

Family connection…

Father’s first computer…

Made from telephone relays!

“ICCE ii” Computer 1950s
Imperial College, London



Counting MAC in IPv6

George Michaelson
APNIC R&D
ggm@apnic.net

EUI-64 derived addresses

- EUI-64:
  - ‘extended unique identifier’ ™ –an IEEE ™ TM ™
    - Encompasses the EUI-48 space we all know and love
    - Registry of 24 bit unique vendor prefixes, no substructure implied: they’re just unique labels
    - Also known as OUI
    - YOUR ACTUAL “MAC” ADDRESS
      - Remember ARP? Remember DECnet?

- For all unicast addresses, except those that start with the binary value 000, Interface IDs are required to be 64 bits long and to be constructed in Modified EUI-64 format. (RFC 4291).

EUI-64 into IPv6

1. Take MAC address eg: 39:A7:94:07:CB:D0
2. Divide in half

   39:A7:94 07:CB:D0
3. Insert the magic 0xff:fe into the address

   39:A7:94 FF:FE 07:CB:D0
4. Set bit 7 to 1: 39 (00111001) -> 3B (00111011)

   3B:A7:94:FF:FE:07:CB:D0
5. Low order 64 bits of IPv6 address now set
6. 3FFE:DEAD:BEEF:CAFE:3BA7:94FF:FE07:CBD0

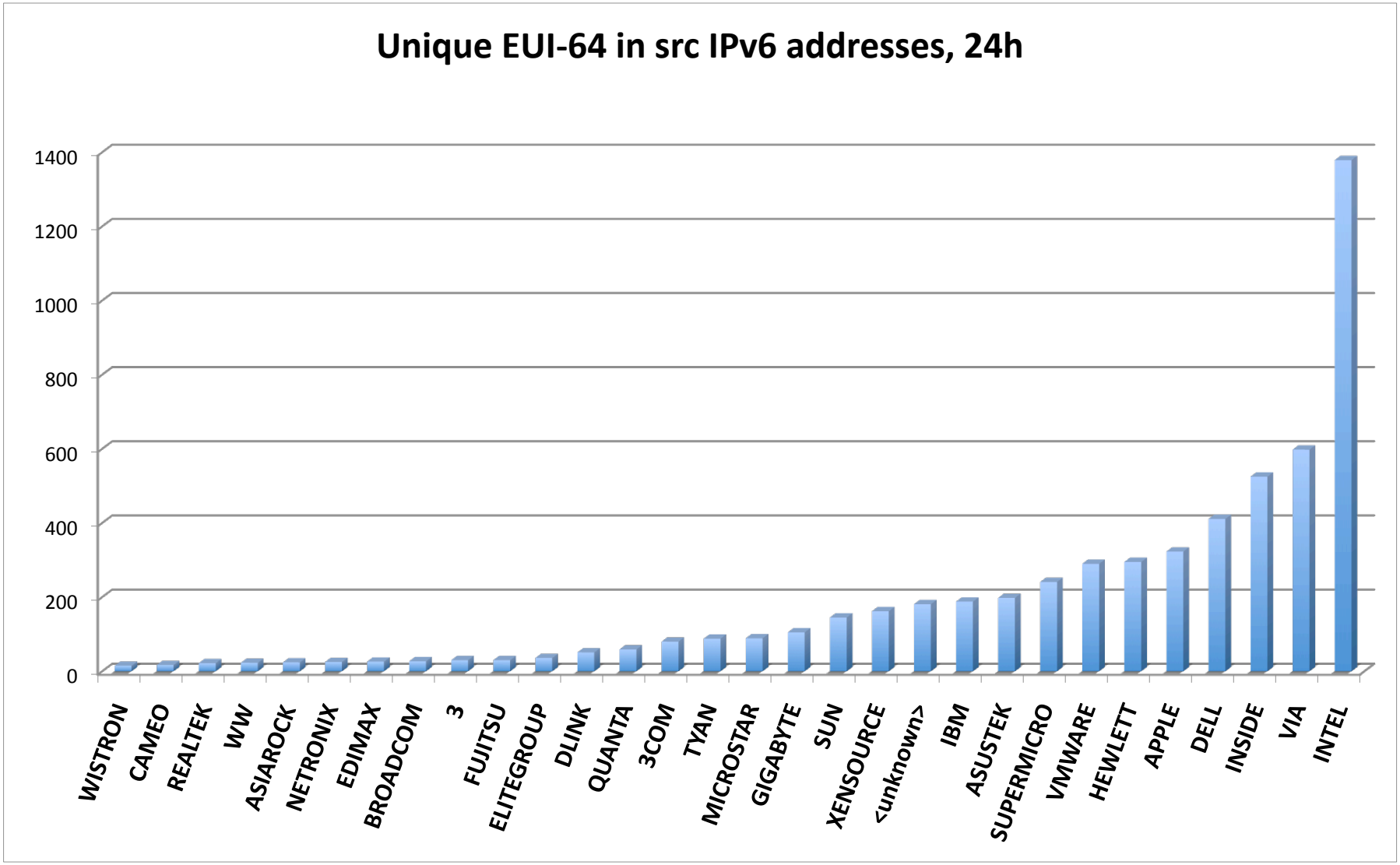
We can reverse this..

- Take an IPv6 Address with FF:FE in it
- Unset bit 7 of the low /64
- Re-derive the EUI-64/MAC address
- Look it up in the IEEE™ registry of Vendors
- Count instances
- What do we find?
- Collect 24h DNS queries on servers for ip6.arpa ranges… and look at the data

The IPv6 Vendor Beauty Pageant

- Two sub-classes
- What Vendors are used to source DNS queries?
  - What Vendors MAC addresses appear in ff:fe structured IPv6 address plans, as the IPv6 src of a DNS query.
- What vendors are targets of PTR queries?
  - What vendors MAC addresses appear in ff:fe structured IPv6 address plans, as the value of a PTR query against ip6.arpa.

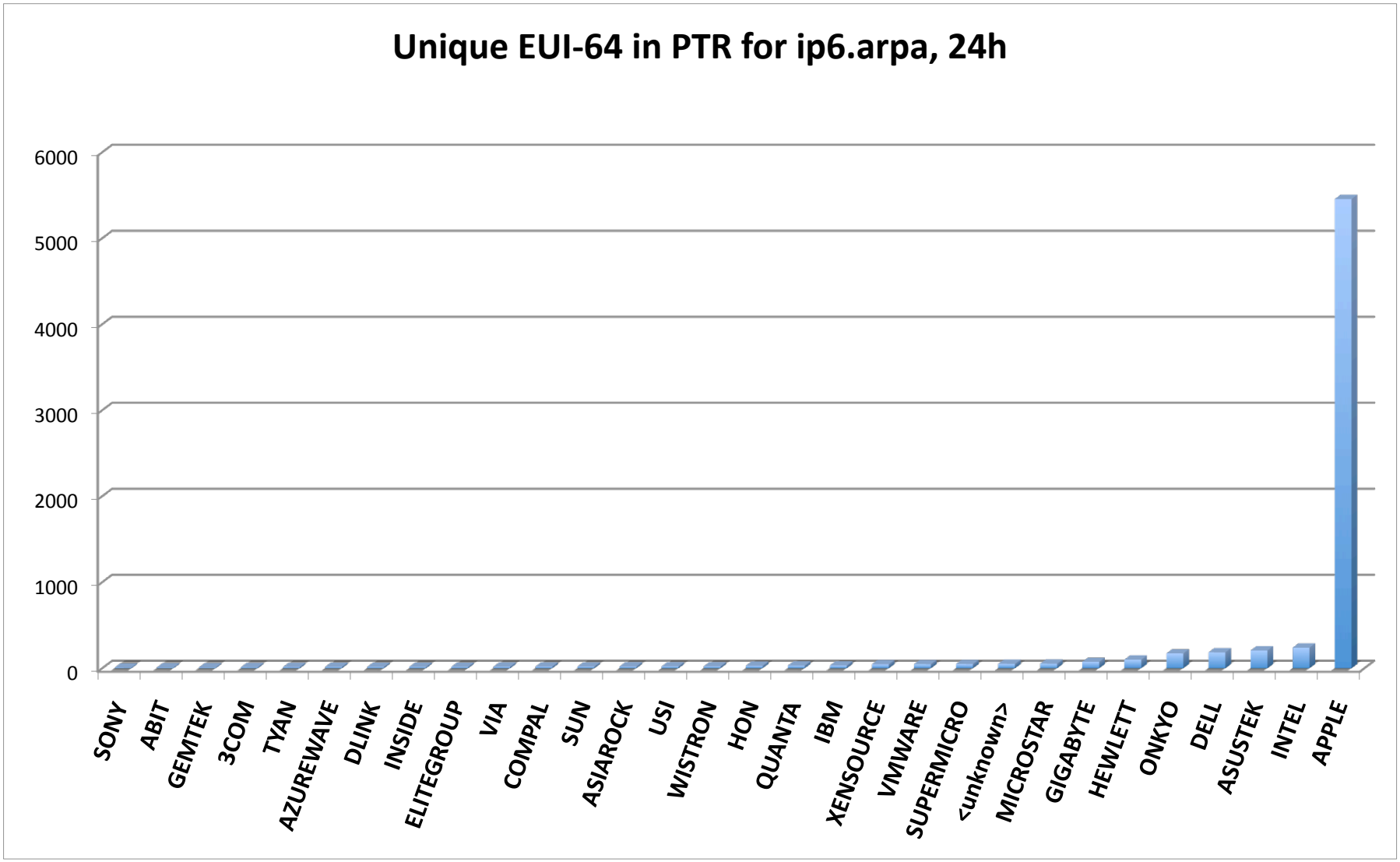
Query sources.



No Surprises

- Lots of infrastructure still runs Sun, IBM
  - But more runs HP, Dell or virtualized.
- Dell, HP own-brand their equipment
  - Intel spans the vendor-set, greybox to rackables
  - Less Cisco/Linksys than I expected
    - 10 seen, all Linksys
  - Cisco have 445 prefixes in the IEEE registry
- Is Xensource and VMWare on blade chassis?

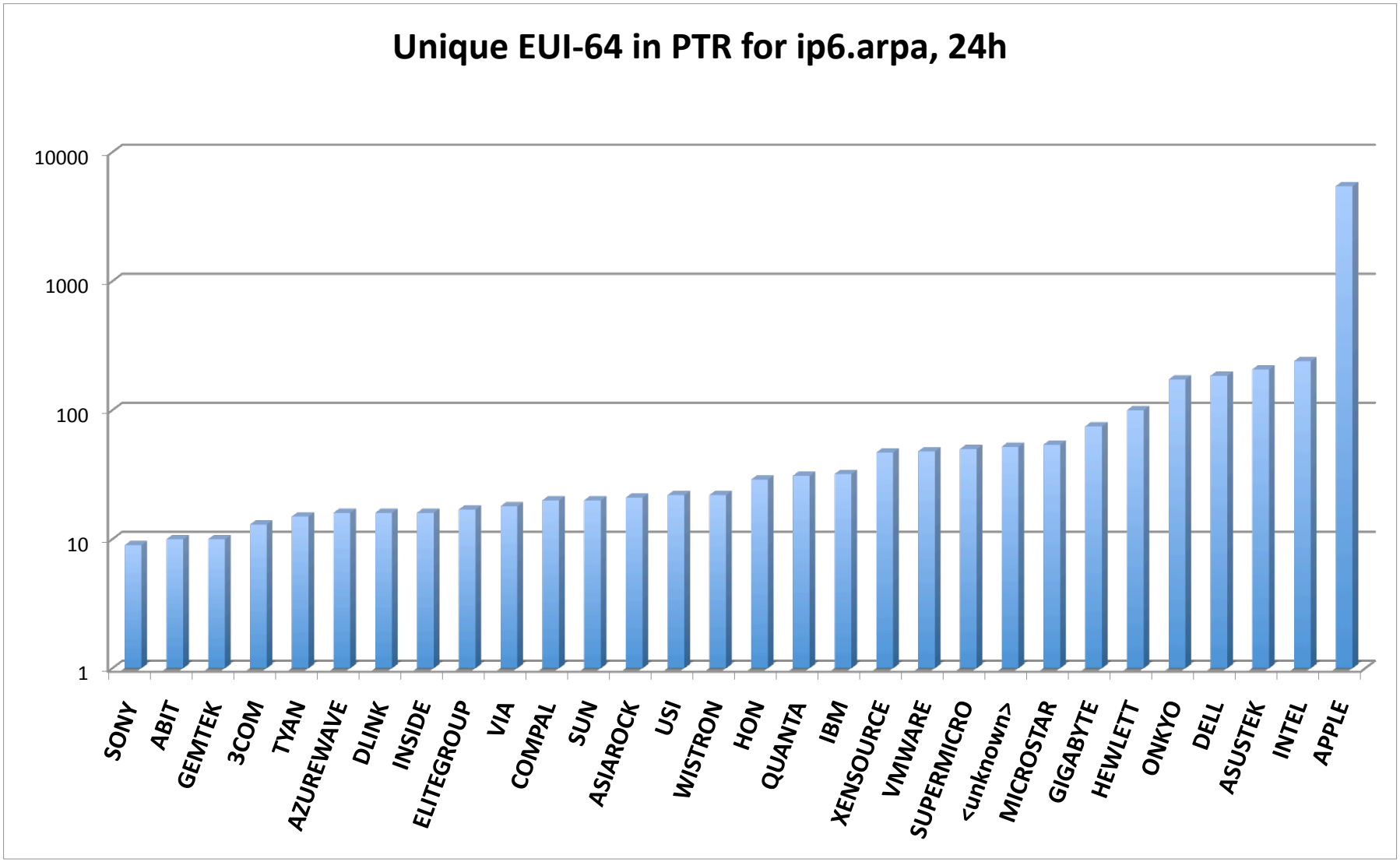
PTR ip6.arpa targets



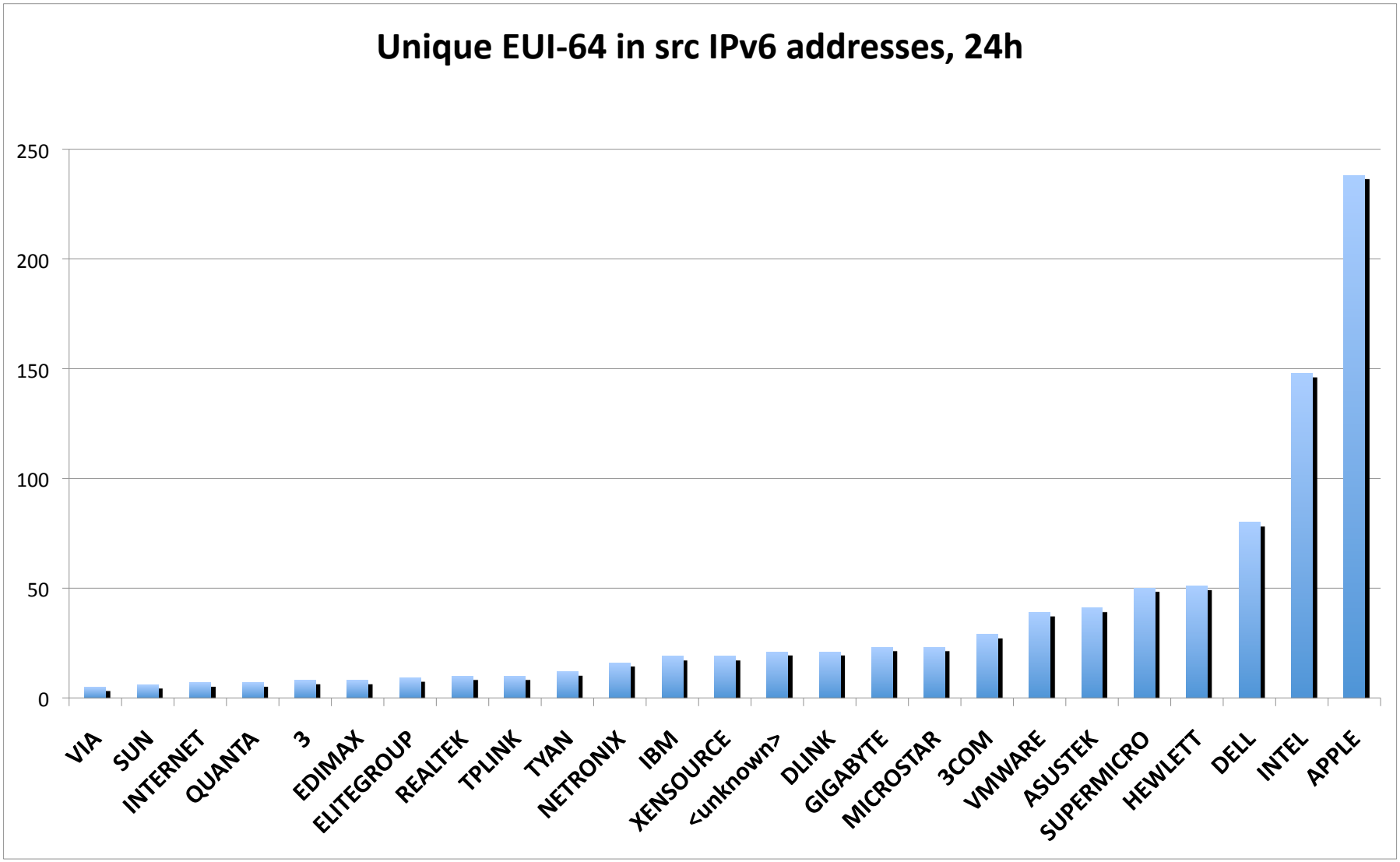
No.. Wait a minute.

- Yes. Its APPLE.
  - Its apple all the way.
  - Maybe this is an artifact of somebody abusing the structured IPv6 number space in some way
  - Or, maybe Apple are just really popular with people who wind up running IPv6?
  - Hint: Apple have 47 entries in the IEEE registry. And, they use their core Apple numbering for Appliances like the time machine and airport express

Once more in slomo (log scale)



2002 (6to4) sources..



conclusions

- Don’t draw any conclusions from this, it’s a beauty pageant.
- Its not who you buy your MAC address from, its how easy it is to use it in IPv6 which counts
- The numbers went further into the white box vendor space
  - 196 vendor codes seen.
- But I’m going to keep monitoring it.

Update: privacy addresses..

- I am informed that Windows 7 has enabled privacy mode addressing by default.
  - **`netsh interface ipv6 set global \ randomizeidentifiers=disabled`**

- OTOH.. This does permit us to identify W7
  - As long as nobody else does!

Want some IPv6/ES info?

I see your IPv6!

Seeing ES IPv6 in DITL

- Look in DITL data, collected in AU/JP
  - Collecting src, dst pairs of DNS queries
  - Collecting target (PTR) of dns lookup
- Count unique ES IPv6 source IPv6 addresses
- A brief example: this is from 10minutes of capture, 2010/04/21 22:50GMT

IPv6 assignments to ES seen

- netname: ARIDO-NET
- netname: CICA-IPV6
- netname: ES-ABRARED
- netname: ES-BTTEL
- netname: ES-COMVIVE
- netname: ES-REDIRIS
- netname: UC3M-IPV6
- netname: UV-IPV6
- netname: VOZTELECOM
- netname: ES-CESCA