



What do we know about an IP address?

Ólafur Guðmundsson

Outline

1 Evolution of address use

2 How address information is used

3 Is address == Device?

Ancient history

- **January 1, 1983**, when the ARPANET changed from NCP to the TCP/IP protocol suite.
- In 1985, with the **creation** of the Supercomputer Centers program, NSF **created NSFNET**, a network that connected the five supercomputer centers and provided a network for research and education. Based on the ARPANET protocols, the **NSFNET created** a national backbone service.
- 1987 ISP start showing up
- IANA (Jon Postel @ ISI) gives out address blocks to anyone that asks

IP address classes (pre 1993 mindset)

Class A	1.0.0.1 to 126.255.255.254	16M hosts 127 networks
Class B	128.1.0.1 to 191.255.255.254	64K hosts 16K networks
Class C	192.0.1.1 to 223.255.254.254	254 hosts 2M networks
Class D	224.0.0.0 to 239.255.255.255	Multicast
Class E	240.0.0.0 to 254.255.255.254	R&D == wasted

1985: Address is a Host

Every computer has one static address

All systems are on the Internet

Address == Identity

1990's Address crisis

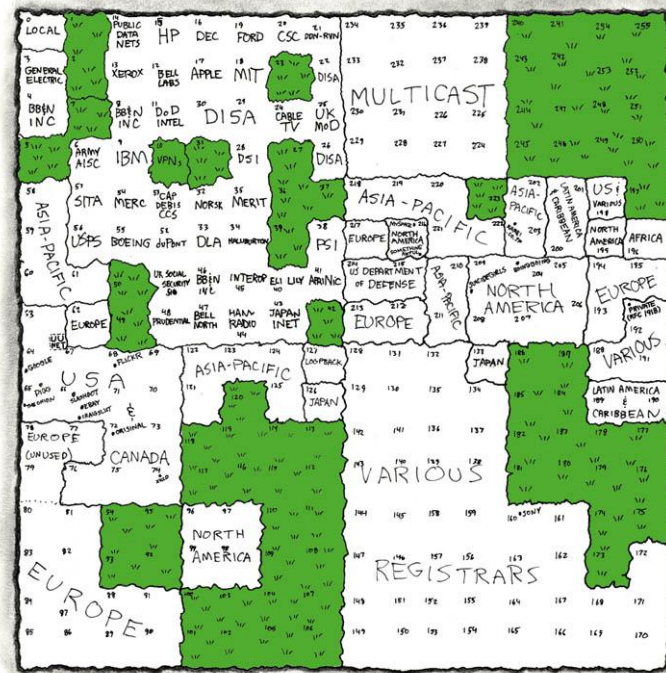
A block is too big

- Average use 2%

B block is frequently too big

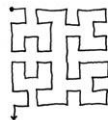
C mostly too small

MAP OF THE INTERNET
THE IPV4 SPACE, 2006



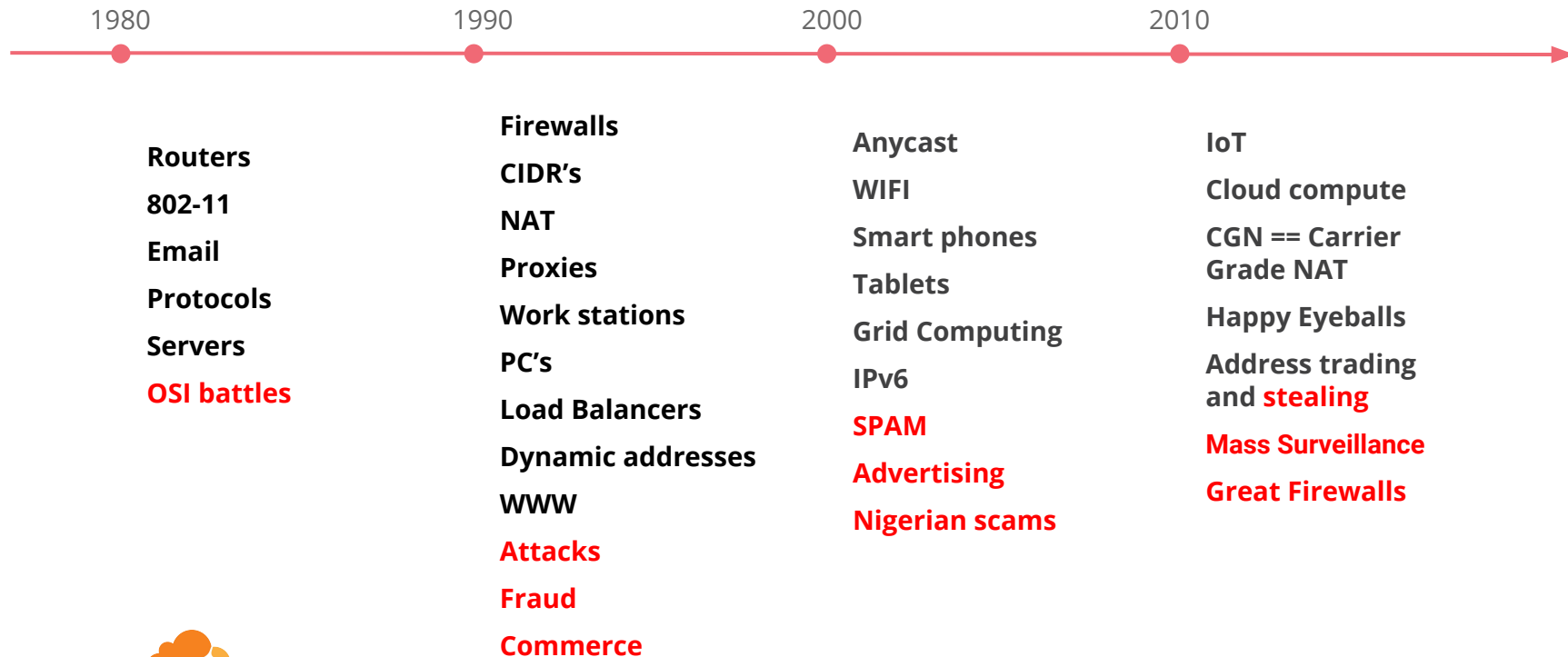
THIS CHART SHOWS THE IPV4 ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING--ANY CONSECUTIVE STRING OF IP_s WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IP_s THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.

0 1 14 15 16 19 →
3 2 13 12 17 18
4 7 8 11
5 6 9 10



 = UNALLOCATED BLOCK

Timeline of factors affecting addresses



Where does this leave us ?

Understanding of addresses is fragmented

What one learned in school

What did the teacher know?

Your workplace guru

When did they learn it ?

What your environment exposes

Is it state of the art?

What one reads online

Are  more enlightened?

What does one want to know about address?

Depends on perspective, “needs”, and context!!

Location, type, kindness, potential \$€£,

Moral: Address is an identifier on how to get somewhere

Address attributes

- RIR
- Registrant postal address
- Network/Location
- Routing: Unicast vs Anycast
- Services: email, DNS, HTTP, none
- History
- Abuse

Network types:

- University
- Office
- Hosting
- Residential
- "Hotel"
- Cloud
- Unknown
- CGN
- Unused
- Government
-

Location

Where in the world is the address?

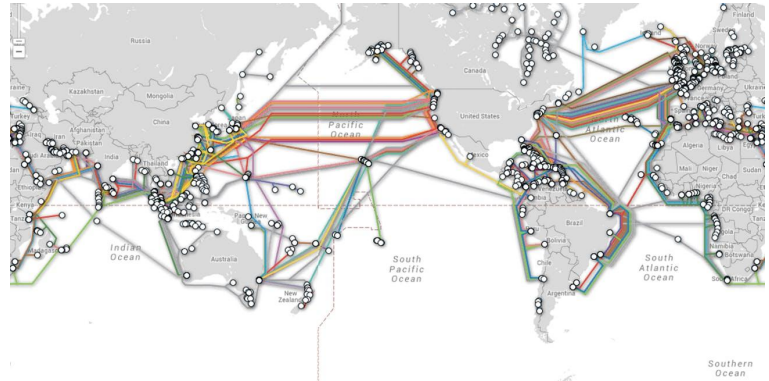
Two dimensional: Geographical and “AS”
Possible third dimension: Sub-AS or “cabling”

⇒ why is this important

Content “crap-timization”

Access to unicast resources that are close

....



Location

“Crap-timization”

- Advertise local services
- Pages in local language

Cloudflare SF office used get Yahoo
Hong Kong Chinese content ⇒ *even if
browser did not have Chinese as a language
preference*




Why: IPv6 address was “registered” from APNIC.



Showing results for **BeyerDynamic DT 1770 PRO**
Search instead for **BayerDynamic DT 1770 PRO**

See BeyerDynamic DT 1770 PRO

Sponsored ⓘ

 Beyerdynamic DT 1770 PRO (250ohm) หูฟังแบบ Full Size จ... THB 21,900.00 Lazada Thailand	 beyerdynamic DT 1770 PRO Studio Headphone THB 21,900.00 Lazada Thailand	 Beyerdynamic DT 1770 PRO Closed Studio Reference... THB 17,605.76 + tax \$552.00 + tax TobyDeals AU
---	---	--

หูฟัง Beyerdynamic ราคาถูก | ครบทุกรุ่น ส่งฟรี | mercular.com

[Ad] www.mercular.com/Beyerdynamic

Beyerdynamic หลายรุ่น MMX300 Custom ประกันศูนย์ ส่งฟรีทั่วประเทศ เก็บเงินปลายทาง. ประกันศูนย์. จัดส่งฟรี
ทั่วประเทศ. เก็บเงินปลายทางได้.

beyerdynamic : DT 1770 PRO | JABEN

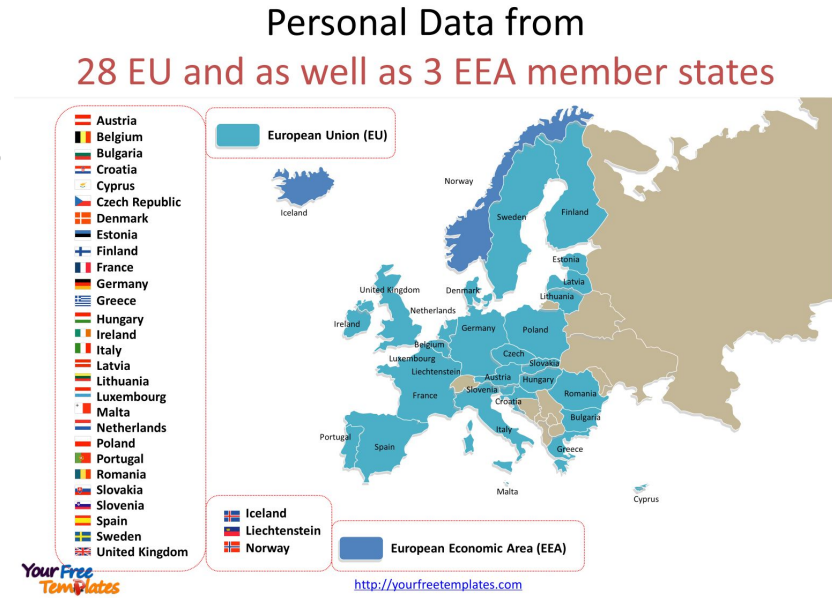
<https://www.jaben.co.th> > BLOG > REVIEWS > Translate this page

May 6, 2017 - หูฟัง beyerdynamic ในตระกูล DT เป็นหูฟังที่มีชื่อเสียงในแวดวงคนทำงานดนตรีมาช้านานรุ่นนี้
เลยครับ ไม่ว่าจะเป็นนักดนตรี , ชาวต่อนท์จ๊อเนียร์ ...

Location Privacy/GDPR/Sovereignty

**Those issues affect what can
be logged**

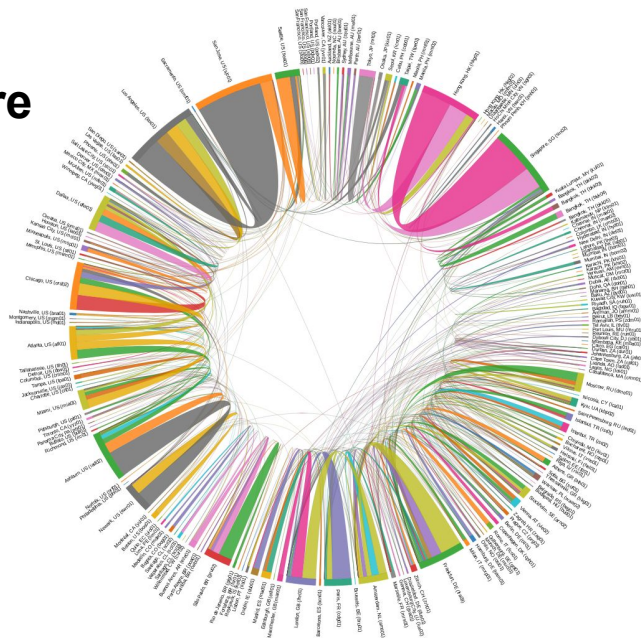
**May affect how the addresses
are treated and served**



Location

Cloudflare network perspective

- Where does the address land at our PoP's
- Where will it move to if preferred PoP is “down”?
- What if the top two/three/four are down?
- What if the “transit” provider goes down where will the alternate one take the address?



Properties

Address Reputation

Has this address done “*bad*” things ?

Is this address crawling, scanning, probing?

Services sell lists but questions about

- accuracy
- temporal relevance



Address != Device implications

- NAT masks individual devices
- CIDR uses address space better
- Dynamic address are used by different “user” at different times
- Roaming devices change address when changing networks
- IPv4 and IPv6 used concurrently

Address persistence

Static addresses:

same address all the time

Dynamic address:

new address every so often

Shared address:

multiple devices using the same address NAT, CGN

Roaming addresses:

example conference networks



Address information from external services

GeolIP2 City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
1.1.1.1	AU	Australia, Oceania		-33.494, 143.2104	1000	Cloudflare	Cloudflare		

Geolocation: MaxMind, etc

Threat information: spam, malware, etc

Block/Allow lists: many, including what is blocked in different countries

Address “ownership”

Trading of addresses:

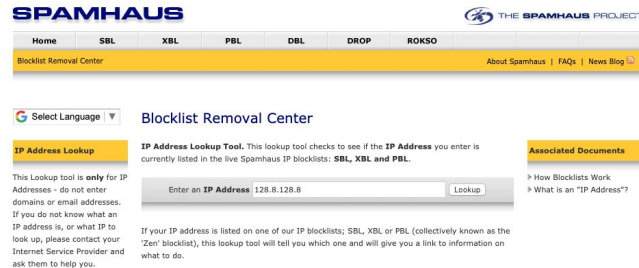
- IPv4 shortage of addresses ==> big market in addresses
 - current price is around \$20+/-address for /8
 - more for smaller blocks
- Insane # IPv6 so no market

Borrowing of addresses:

- Just say no. Ill-repute entities try to work around “blocking” by changing addresses frequently
 - **Restoring good reputation is hard**

Close to 735K Fraudulently Obtained IP Addresses Have Been Uncovered and Revoked, ARIN Reveals

By CircleID Reporter



The screenshot shows the Spamhaus website's Blocklist Removal Center. The header includes the Spamhaus logo and navigation links for Home, SBL, XBL, PBL, DBL, DROP, and ROKSO. Below the header, there's a section titled "Blocklist Removal Center" with a "Select Language" dropdown. The main content area features the "IP Address Lookup Tool" which explains its purpose: to check if an IP address is listed in the live Spamhaus IP blocklists (SBL, XBL, and PBL). It includes a text input field for an IP address (with the example "128.8.128.8") and a "Lookup" button. To the right, there are links for "Associated Documents" such as "How Blocklists Work" and "What is an 'IP Address?'". A footer note states that if an IP is listed on any of the blocklists, the tool will identify which one and provide a link to information on what to do.

What does Cloudflare care about ?

That depends on context:

Resolver: Does query address have privacy implications?

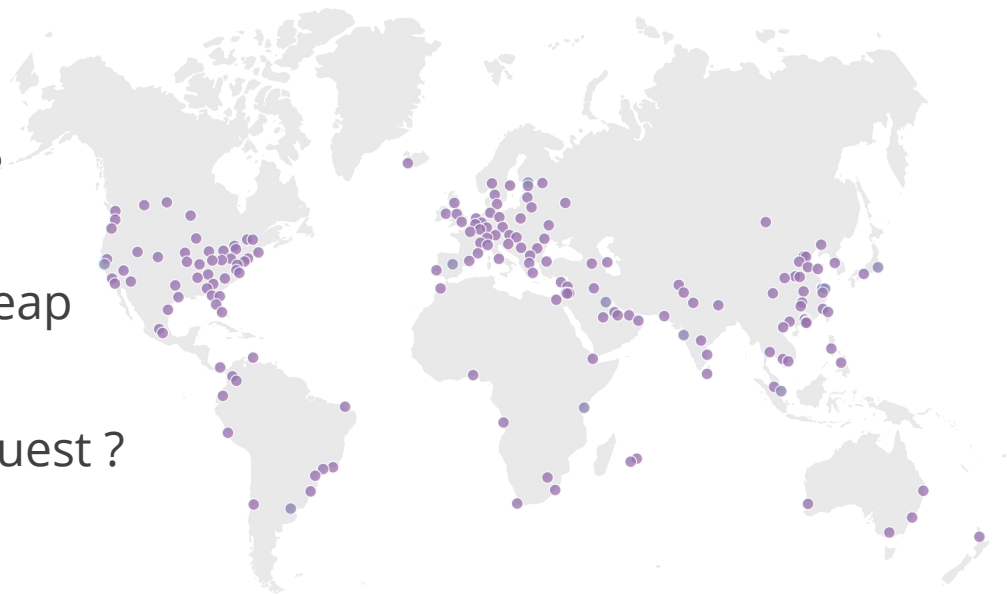
⇒ Affects logging etc.

DoS: Is this a forged packet? Bot?
Expected location?

⇒ Dropping bad packets is cheap
close to edge

CDN: Should we answer this request ?

⇒ Connections are not free



Rough classification of addresses

Types

Eyeball addresses

- Home ISP
- Cellular
- Hotel/Cafe Hotspot

Server addresses

- On-site
- Server

Office addresses

- Corporate locations
- Coworking spaces

VPN exit nodes

Properties

NAT

- 2-50 devices
- home/small office

CGNAT

- Carrier grade
- 20-500 devices

Static vs Dynamic

Transit Specific

...

Bad behavior

- Spam
- DoS
- Bots
- Evil Content
- ...

Value of serving

- \$£¥
- Message
- ...

Disagreeable

- Politics
- Visual Stimulation
- Violence
- ...

Q/A