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?

CLOUDFLARE

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

CLOUDFLARE

1985: Address is a Host

Every computer has one static address
All systems are on the Internet

Address == Identity

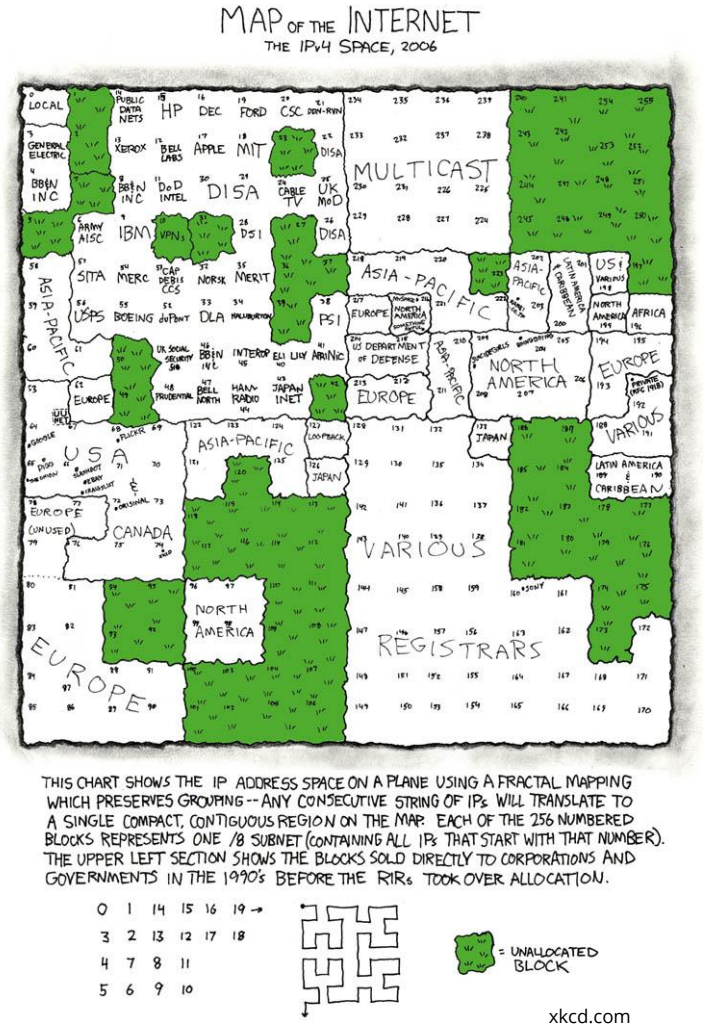
1990's Address crisis

A block is too big

- Average use 2%

B block is frequently too big

C mostly too small



xkcd.com

CLOUDFLARE

Timeline of factors affecting addresses

1980

- Routers
- 802-11
- Email
- Protocols
- Servers
- OSI battles

1990

- Firewalls
- CIDR's
- NAT
- Proxies
- Work stations
- PC's
- Load Balancers
- Dynamic addresses
- WWW
- Attacks
- Fraud
- Commerce

2000

- Anycast
- WIFI
- Smart phones
- Tablets
- Grid Computing
- IPv6
- SPAM
- Advertising
- Nigerian scams

2010

- IoT
- Cloud compute
- CGN == Carrier Grade NAT
- Happy Eyeballs
- Address trading and stealing
- Mass Surveillance
- Great Firewalls

CLOUDFLARE

Where does this leave us ?

Understanding of addresses is fragmented

What one learned in school

Your workplace guru

What your environment exposes

What one reads online

What did the teacher know?

When did they learn it ?

Is it state of the art?

Are  more enlightened?

CLOUDFLARE

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

CLOUDFLARE

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
- .....

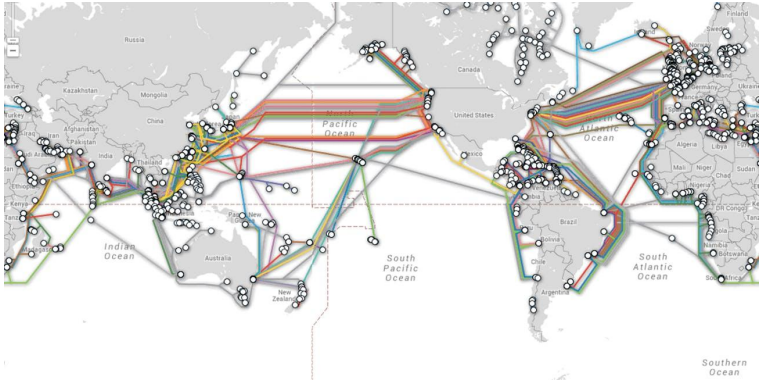
CLOUDFLARE

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
….



CLOUDFLARE

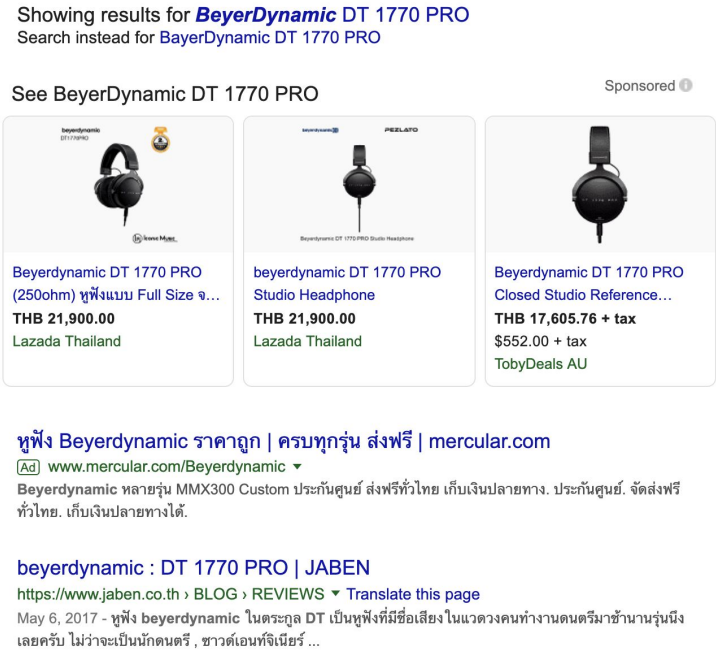
Location

“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.



CLOUDFLARE

Location

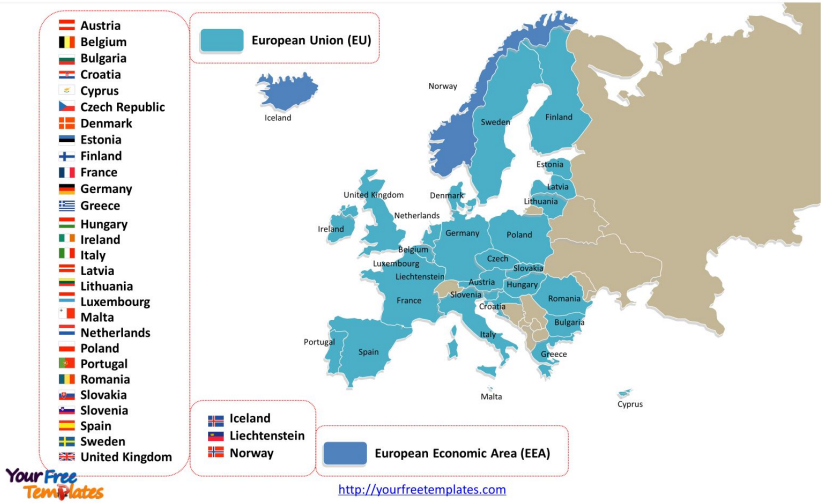
Privacy/GDPR/Sovereignty

Those issues affect what can be logged

May affect how the addresses are treated and served

Personal Data from

28 EU and as well as 3 EEA member states

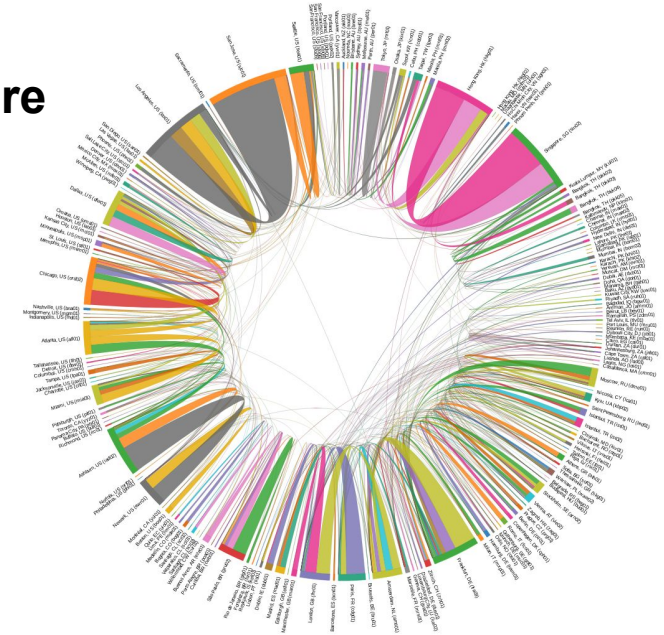


CLOUDFLARE

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?**



CLOUDFLARE

Properties
Address Reputation

Has this address done *"bad"* things ?

Is this address crawling, scanning, probing?

Services sell lists but questions about

- **accuracy**
- **temporal relevance**

CLOUDFLARE

Address ! = Device implications

- NAT maks 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

CLOUDFLARE

Address information from external services

GeoIP2 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

CLOUDFLARE

Address “ownership”

Trading of addresses:

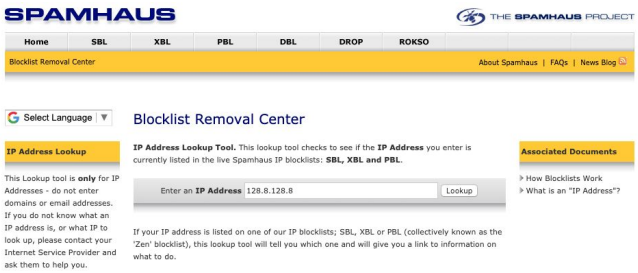
- IPv4 shortage of addresses ==> big market in addresses
  - current price is around $20+/address for /8
    - more for smaller blocks
- Insane # IPv6 so no market

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

By CircleID Reporter

Borrowing of addresses:

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



CLOUDFLARE

What does Cloudflare care about ?

That depends on context:

Resolver: Does query address have privacy implications?

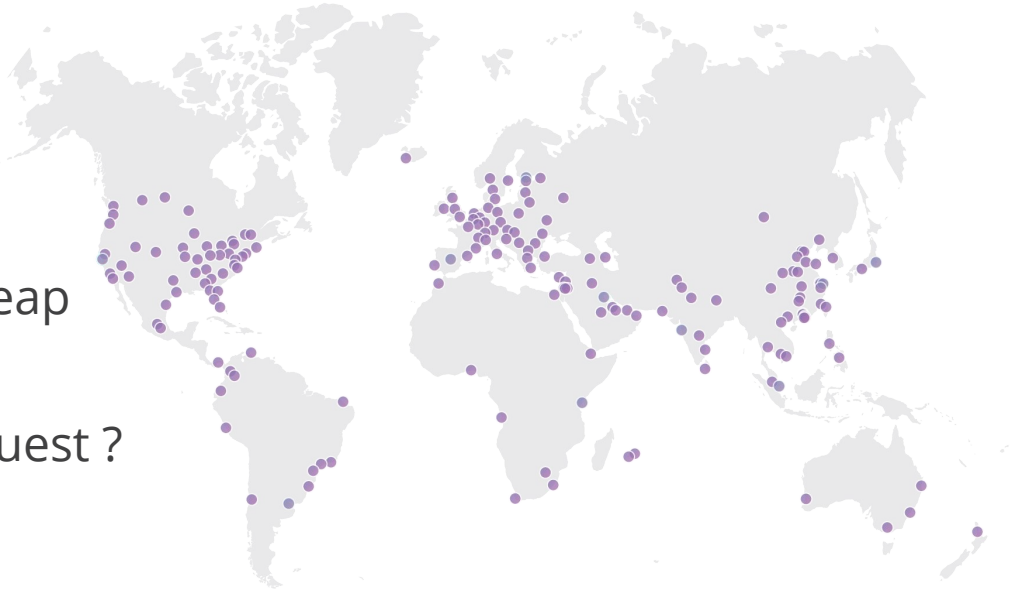
⇒ Affects logging etc.

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



CLOUDFLARE

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
...

CLOUDFLARE

Q/A