Geo-Network Operations

IAB Workshop on IP Address Geolocation (ip-geo)
December 2025

Joe Abley
Director of Engineering
Cloudflare

Cloudflare

Why does Cloudflare care about IP geolocation?

- Cloudflare runs proxies that allow customers to apply rules that control how individual requests are handled
  - this includes rules of the form "if client is located in this place, process the request in this particular way"
  - **mapping a client address to a location is important**
- Cloudflare provides connectivity to end-users and to enterprises, e.g. Cloudflare WARP, Magic Transit
  - Cloudflare is an access provider
  - **mapping the address assigned to a user's device to a location is important for that user**

What does Cloudflare do?

- Cloudflare consumes commercial geolocation datasets from an external vendor
  - these mappings are used, for example, in the inbound request handling mentioned earlier
- Cloudflare publishes geolocation mappings for its own addresses in the format specified in RFC 8805:
  - https://api.cloudflare.com/local-ip-ranges.csv
  - This URL is known to be polled by significant geolocation data brokers
- Cloudflare does not currently publish that URL through RIR-published datasets (e.g. RPSL inetnum objects) as specified in RFC 9632.

Some minimal context about Cloudflare's infrastructure

- Pretty much anything Cloudflare does involves Anycast
  - Anycast destination addresses for inbound connections
  - Anycast source addresses for outbound connections
    - if this makes you twitch, it should, but we do it and we can explain
- Cloudflare operates in 330 cities in 125 countries
- The location of any service that is accessible through Cloudflare will usually not reveal itself using ping or traceroute
- Outbound connections from Cloudflare might well appear to originate locally, even if they are from far away

Correspondence

My network is not where Cloudflare thinks it is and this is hurting my users

> I hope you are well.
>
> We are contacting you regarding incorrect geolocation data for several IP prefixes we operate under ASxxxxx and ASxxxxx. While MaxMind, IPinfo and other major geolocation providers are showing the correct location, Cloudflare continues to display outdated or incorrect geolocation information for the following prefixes:
>
> [...]
>
> These prefixes belong to Xxxxxxxx Xxxxxx and the correct geolocation for all of them is Xxxxxxxxx. We have published an official RFC 8805 geofeed file for our IP resources here: https://xxxxxxxxxxx
>
> Because some websites behind Cloudflare use Cloudflare's IP geolocation to enforce regional access policies, the incorrect location is causing service accessibility issues.

Our earlier guesses turned out to be wrong so we are making new guesses

> Thanks for getting back.
>
> Here's what I see internally: we have the entire XXX.XXX.XXX.XXX/24 in XX, but this smaller XXX.XXX.XXX.XXX/26 range moved from XX to XX on Xxx XX XXXX, due to RTT evidence (which I no longer see, by the way)
>
> Given the lack of other hints to support XX, I'm adding a manual correction to get these two ranges to point to XX for now:
>
> XXX.XXX.XXX.XXX/24, XX
>
> XXX.XXX.XXX.XXX/24, XX
>
> But please let me know if you'd like these reviewed further. By the way, do you know if the customers who own these ranges and need them showing a specific location?

We are making reasonable requests but you are not doing what we are asking fast enough

> Dear Colleagues
>
> We wrote you about this problem 9 days ago, but we haven't received any news from your side:
>
> The problem is urgent for us, I will repeat.
>
> We have an issue with IP geolocation,
>
> This IP XXX.XXX.XXX.XXX is from Xxxxxx, but Cloudflare recognizes it as from Xxxxx.
>
> Please correct the geolocation because we have restriction rules for Xxxxx.

Gaps

Some gaps that we see (gaps that, if filled, would reduce customer frustration)

- **Authentication, Provenance and Integrity Protection**
  - Consumers don't know how to trust the mappings we publish; we don't know how to trust the mappings we consume
  - There is no way to tell whether or how a published mapping has been modified before being consumed
  - There is no way to tell whether a mapping we have published has been accepted by anybody else
- **Data Quality**
  - There is no way to ensure data quality, and no obvious way to measure it

The idea that a single user on the Internet is represented by a single IP address is not a useful one

- Almost everything described up until now is based on someone making an assumption that an IP address maps to an end user
- There is a related assumption that all addresses within the same prefix map to individual users in the same location
  - These are not good assumptions
  - These are proxies (*sic*) for other missing signals
- For HTTP, there are other channels through which assertions about location can be made
  - The Internet is not the Web, but the Web is where much of the demand for these signals appears to be

Opportunities

It would be great if we could say more about an address than simply handwaving about a city

- It would be helpful if the expected use of an address was better known
  - This address relates to set of residential users in one location
  - This address relates to residential users in one region
  - This address is a consumer VPN exit interface, and we cannot usefully say where the users whose traffic originates here are located
  - This address is some other kind of VPN exit interface and we can say with confidence that all the users associated with it are in this region
  - This address is not usually used to originate outbound connections
- These kinds of heuristics would have other applications, e.g. in the active management of unwanted traffic

This data is important, but there are many gaps in data governance

- Processes and understanding of the data itself varies widely between different originators, processors and consumers
- It would be much easier to support customers who are struggling because of address mismapping if we knew who to talk to
  - Tag corrections or modifications
  - Understand the provenance of particular mappings
  - Provide some cryptographic assurance that assertions and corrections are made by parties whose opinions are plausible
    - note that *plausible* should be expected to vary

Questions!