

Finding and Using Geofeed Data

Massimo Candela (presenting)

NTT

massimo@ntt.net

Randy Bush

IIJ & Arrcus

randy@psg.com

Warren Kumari

Google

warren@kumari.net

Russ Housley

Vigil Security

housley@vigilsec.com



IP geolocation

- IP geolocation is needed in various occasions
 - To respect country regulations
 - To provide localized content
 - Troubleshooting
 - Research



What's the problem?

- Unfortunately there is no:
 - Central repo
 - Common strategy
 - Authoritative data
- Many companies have their own dataset
 - Or enrich datasets of geolocation providers
- If the geolocation is wrong you have to contact many organizations

What if my geolocation is wrong?

- **MaxMind:** <https://support.maxmind.com/geoip-data-correction-request/>
- **dbip:** <https://db-ip.com/report/?addr= YOUR IP>
- **IP Info:** <https://ipinfo.io/contact?s=correction>
- **RIPE IPmap:** https://ipmap.ripe.net/api/v1/crowdsource/_IP_OR_PREFIX_
- IPdata.co: support@ipdata.co
- IP2Location: support@ip2location.com
- IPhub: <https://iphub.info/contact>
- IPIP: support@iip.net
- IPLigence: <https://www.ipligence.com/contact>
- Neustar's IP GeoPoint: N/A - try generic support
- NetAcuity: N/A - try generic contact

Geofeeds

Geofeeds

- Format for self-published IP geolocation feeds
 - <https://tools.ietf.org/html/rfc8805>
- Only if/what you want to publish
- Flexible
 - Geolocate single IPs or entire prefixes (longest prefix match)
 - Geolocate at whatever level you wish (from nothing to city)
- Adopted by Google and many geolocation providers

Geofeeds format

- IP/prefix,country,region,city,
- Country expressed in 2 letter ISO 3166-1 alpha2
 - <https://www.iso.org/obp/ui/#search>
- Region expressed in ISO 3166-2
 - Go in <https://www.iso.org/obp/ui/#search>
 - Search for the country and click
 - Search for the region code
- City in free UTF-8 text format
 - I recommend the name in the GeoNames dataset
 - <https://public.opendatasoft.com/explore/dataset/geonames-all-cities-with-a-population-1000/table/?disjunctive.country>

Geofeeds examples

- 192.0.2.0/24,,,,
- 194.0.2.0/25,US,,
- 140.0.0.0/16,IT,IT-62,,
- 140.0.1.1,IT,IT-62,Frosinone,

Geofeed support

From

Subject **Geofeed support**

To Me <massimo@us.ntt.net> ★

11/09/2020, 17:27

Hi Massimo,

I watched your LACNIC webinar on geolocation two weeks ago. While I was already using geofeed with Google and [IPInfo.io](#), I contacted the geolocation providers on your list and was able to set up automatic updates with pretty much all of them.

I thought I could share my list:

- [DB-IP](#) - Geofeed supported
- [Google](#) - Geofeed supported
- [IP2Location](#) - Geofeed supported
- [IPData.io](#) - Geofeed supported
- [IPGeolocation.io](#) - Geofeed supported
- [IPHub](#) - Geofeed supported
- [IPInfo.io](#) - Geofeed supported
- Maxmind - Geofeed supported

- But no central repo

Indexing Geofeeds in RPSL

Proposed (simple) solution

- Finding and Using Geofeed Data
 - Draft: <https://tools.ietf.org/html/draft-ymbk-opsawg-finding-geofeeds-04>
 - We asked for adoption in opsawg

- We use a remark of a inet(6)num to point to a geofeed file

```
inet(6)num: 192.0.2.0/24
```

```
remarks: Geofeed https://geo.ip.gin.ntt.net/geofeed.csv
```

In ARIN inet(6)num => NetRange and remarks => Comment

- Ideally, RPSL would be augmented to define a new “geofeed:” attribute in the inet(6)num class
- Geolocation providers already access this data
- After you can focus on keeping up-to-date your CSV file

When publishing

- Geofeed data can have more granularity of the inet(6)num
- Geofeed files SHOULD be served over HTTPS
- Once linked, you don't need the RIR portal anymore
- Multiple inet(6)num can refer to the same geofeed file
 - In one file you can collect all your prefixes
 - But only if the file is not signed!
- An optional authenticator MAY be appended
 - Is the Geofeed data authorized by the 'owner'? The inetnum which points to the geofeed file provides some assurance
 - Additionally, a digest of the main body of the file signed by the private key of the relevant RPKI certificate for the covering prefix can be added

When fetching

- Prefixes outside of the referring inet(6)num MUST be discarded
- The most specific inet(6)num object *with a geofeed reference* MUST be used
 - Both customers and providers can fix a geolocation
- You can parse bulk whois data!
 - Publicly available over FTP for RIPE, LACNIC, AFRINIC, APNIC
 - Partially available for ARIN, or
 - You ask bulk access (geo providers already use such data), or
 - You get the NetRanges from bulk and Comments from whois/rdap

Tool: geofeed-finder

- Available on GitHub
 - <https://github.com/massimocandela/geofeed-finder>
- Steps
 - Run the binary `./geofeed-finder-linux-x64`
 - See the final geofeed file in `result.csv`

```
massimo:geofeed-finder massimocandela$
```



Tool: geofeed-finder

- The output is a big goofeed file
- Geolocation providers already supporting geofeeds don't have to do anything
 - Just periodically run the geofeed-finder and import result.csv

Questions?

Massimo Candela

NTT

massimo@ntt.net

Twitter: @webrobotics

Randy Bush

IIJ & Arrcus

randy@psg.com

Warren Kumari

Google

warren@kumari.net

Russ Housley

Vigil Security

housley@vigilsec.com