



# A strategy to keep your geolocation up to date

**Massimo Candela**  
Senior Software Engineer  
Global IP Network  
massimo@ntt.net  
@webrobotics

# Finding and Using Geofeed Data



Draft <https://www.ietf.org/archive/id/draft-ietf-opsawg-finding-geofeeds-08.txt>

## **Randy Bush**

IJJ & Arrcus  
randy@psg.com

## **Massimo Candela (presenting)**

NTT  
massimo@ntt.net

## **Warren Kumari**

Google  
warren@kumari.net

## **Russ Housley**

Vigil Security  
housley@vigilsec.com

# What's the problem?



- For IP geolocation there is no:
  - Central repo
  - Common strategy
  - Authoritative data
- Many companies have their own dataset
- If the geolocation is wrong you have to contact many organizations
  - RIRs are often (erroneously) contacted

# What if my geolocation is wrong?



- **MaxMind**: <https://support.maxmind.com/geoip-data-correction-request/>
- **dbip**: [https://db-ip.com/report/?addr=\\_\\_YOUR\\_IP\\_\\_](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\\_](https://ipmap.ripe.net/api/v1/crowdsource/_IP_OR_PREFIX_)
- **IPdata.co**: <https://ipdata.co/corrections.html>
- **IP2Location**: [support@ip2location.com](mailto:support@ip2location.com)
- **IPhub**: <https://iphub.info/contact>
- **IPIP**: [support@iipip.net](mailto:support@iipip.net)
- **IPligence**: <https://www.ipligence.com/contact>
- **BigDataCloud**: <https://www.bigdatacloud.com/update-my-location>
- **NetAcuity**: N/A - try support

# What we propose



1. Create a CSV file with the prefixes/IPs you want to correct/geolocate
  - Each entry like: **204.141.120.0/22,US,US-VA,Ashburn**,
  - Geofeed <https://tools.ietf.org/html/rfc8805> (format supported by ~all geolocation providers)
2. Publish that CSV file somewhere (including GitHub), possibly over https
  - Examples:
    - NTT <https://raw.githubusercontent.com/nttgin/geofeeds/master/geofeeds.csv>
    - Tmobile <https://raw.githubusercontent.com/tmobile/tmus-geofeed/main/tmus-geo-ip.txt>
3. Add a remark/comment to the related inet(6)num/NetRange
  - “Geofeed <https://your/file.csv>”
  - This allows for auto-discovery and easy ownership verification
  - Multiple inet(6)num can point to the same geofeed file

# Example of Geofeed file



```
83.231.214.172/30,RO,RO-B,Bucharest,  
83.231.214.212/30,RO,RO-SB,Sibiu,  
212.119.27.192/30,IT,IT-21,Turin,  
5.158.213.8/30,IE,IE-D,Dublin,  
83.231.214.228/30,CH,CH-GE,Genève,  
83.231.214.196/30,FI,FI-18,Helsinki,  
83.231.214.112/30,IT,IT-MI,Milan,  
213.198.77.176/30,RO,RO-TM,Timisoara,  
165.254.178.240/28,US,US-NY,,  
202.68.64.0/20,AU,AU-NSW,Sydney,  
103.13.80.0/22,AU,AU-NSW,Sydney,  
153.254.80.0/22,AU,AU-NSW,Sydney,  
198.107.141.0/24,US,US-CA,,  
128.241.0.128/29,US,US-CA,,  
116.51.31.96/30,SG,,Singapore,  
209.212.229.0/24,HK,,,  
165.254.42.200/29,US,US-VA,,  
209.212.233.0/24,AU,AU-NSW,Sydney,  
209.212.228.0/24,JP,JP-13,Tokyo,  
209.212.236.0/24,KR,,Seoul,  
209.212.234.0/24,MY,,,  
209.212.232.0/24,SG,,Singapore,
```

# Geofeed 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>



Carlos M Martínez  
AIL

UY-LACN-LACNIC

Información

Recursos IP/ASN

Solicitar

Gestionar

Transferir/Devolver

Servicios

Membresía

4

Pagos

Pagos

Reportes

Organizaciones no asociadas

Bulkwhois



4



Cerrar Sesión

Inicio / Organización / IP / ASN

45.6.248.0/22 ☆

### Sistemas Autónomos

AS28000

AS28001

### IP LACNIC

45.6.248.0/22

45.6.252.0/22

168.121.184.0/22

170.247.168.0/22

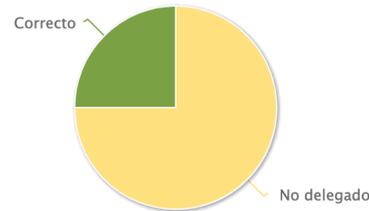
179.0.156.0/22

190.112.52.0/22

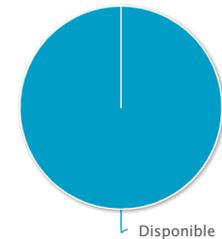
45.6.248.0 - 45.6.251.255 (AS28000)

ASSIGNED

### DNS reverso



### Subasignaciones



**Organización** LACNIC - Latin American and Caribbean IP address (UY-LACN-LACNIC)  
**Fecha Asignación** 27-abr-2017  
**Fecha Actualización** 27-abr-2017



TECNICO  
AIL



ABUSO  
AIL

Subasignar

Delegar (rDNS)

Editar Contactos

ASN de Origen

Remarks

Ayuda



Carlos M Martínez  
AIL

UY-LACN-LACNIC

Información

Recursos IP/ASN

Servicios

Membresía

Pagos

Pagos

Reportes

Organizaciones no asociadas

Bulkwhois



Cerrar Sesión

Inicio / Organización / IP / ASN / Remarks

### Bloques IP Remarks

Geofeed <https://link/to/my.csv>

Volver

Guardar

LACNIC - Latin American and Caribbean IP address

45.6.248.0/22

ASSIGNED

Ayuda

# Result



```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.ripe.net

inetnum:    83.0.0.0 - 83.255.255.255
organisation: RIPE NCC
status:     ALLOCATED

whois:      whois.ripe.net

changed:    2003-11
source:     IANA

# whois.ripe.net

inetnum:    83.231.214.0 - 83.231.214.255
netname:    VERIO-DE-INFRA
descr:      NTTEO DE frankfurt facility
country:    DE
admin-c:    NERA4-RIPE
tech-c:     NAIA1-RIPE
status:     ASSIGNED PA
remarks:    INFRA-AW
remarks:    Abuse/UCE: abuse@us.ntt.net
remarks:    Network: noc@us.ntt.net
remarks:    Security issues: security@us.ntt.net
remarks:    Geofeed https://geo.ip.gin.ntt.net/geofeeds/geofeeds.csv
mnt-by:     MAINT-VIPAR
created:    2013-12-10T17:18:59Z
last-modified: 2020-09-08T18:21:39Z
source:     RIPE # Filtered
```

Download from <https://github.com/massimocandela/geofeed-finder>

```
$ ./geofeed-finder-macos-x64 -t 81.93.181.144/28
```

```
81.93.181.144/28 https://geo.ip.gin.ntt.net/geofeeds/geofeeds.csv [cache]
```

```
81.93.181.144/28,FR,FR-IDF,Paris
```

# Geofeed is flexible



- Geolocate single IPs or entire prefixes (longest prefix match)
- Geolocate at whatever level you wish (from nothing to city)
- You don't need an inet(6)num for each prefix/IP to geolocate
  - Geofeed files can have more granularity of the inet(6)num

- We are not trying to replace geolocation providers
  - They have an important role in validating and distributing geo data
  - We are trying to ease/automate the communication with them
- Our proposal includes a way to safely consume geofeed data
  - The inet(6)num gives assurance about the ownership of the prefixes in the file
    - in the file, the prefixes outside the parent inet(6)num MUST be discarded
  - In case of weak rpsl authentication, an optional authenticator MAY be appended
    - a digest of the main body of the file signed by the private key of the relevant RPKI certificate for the covering prefix

# Consuming Geofeeds



- <https://github.com/massimocandela/geofeed-finder>
- It uses whois dumps
- The output is a big geofeed file
- Geolocation providers already supporting geofeeds can periodically run the geofeed-finder and import result.csv

# Thank you.

**Massimo Candela**

Senior Software Engineer, Network Information Systems Development

Global IP Network

massimo@ntt.net

@webrobotics

[www.gin.ntt.net](http://www.gin.ntt.net)

@GinNTTnet #globalipnetwork #AS2914