

Resolver IP ranges/Locations

Distribution mechanisms

draft-bretelle-dnsop-recursive-iprange-location

Manu Bretelle

IETF 109, 2020-11-17

Problem Statement

Why do we care about IP ranges/Geolocations

- Geolocation
 - Recursive resolver distributed around the globe
 - Authoritative may serve geo based answers
 - inet6?num's country attribute not necessarily good/up-to-date indicator
 - IP ranges can be re-assigned as owner's POP come and go
 - Existing GeoDB may not be accurate

Problem Statement

Why do we care about IP ranges/Geolocations

- IP ranges
 - Resolver use a subset of organization's global IP pool
 - Can be used when building network ACL
 - Can be used when devising DDoS mitigation
 - “From talking with DNS operators at conferences, we know that RRL works for them, but that they would like to exclude the resolvers with which they have a well established long-standing relationship.”
<https://blog.nlnetlabs.nl/journeying-into-xdp-part-1-augmenting-dns/>

Goal/Non-Goal

- Goals:
 - mechanism for resolver operators to distribute their IP ranges/geolocations
 - mechanism for auth operator to consume those programmatically to generate network policies, RRL rules, geo-targeted answers....
- Non-Goal:
 - Real-time usage by auth servers/network policy controllers.

Current Status

It's all over the place

- No consistency in location (provider F.A.Q, API documentation)
- No consistency in medium (HTTPS, DNS, email)
- No consistently in format (web page, CSV, JSON)

Proposal

- publication format
 - TXT record with list of subnet separated by a space
 - TXT record with a list of subnet,2-letter-country-code separated by a space
 - HTTPS record with a uri where to get the RFC8805 geofeed from.
- A “discovery” mechanism
 - rdns.example.com to find ranges/locations of resolvers from example.com organization

Other Ideas

- IP range holder to list the URL to a Geofeeds serve using the inetnum object:
draft-ymbk-opsawg-finding-geofeeds
- draft-google-self-published-geofeeds-04#section-7.3 made use of U-NAPTR (RFC4848)
- _rdns/TXT query on IP's {in-addr,ip6}.arpa

Open Questions

- RFC8805 has notion of region/city/postal code. IATA 3-letter code may be more meaningful
- TXT record is limited in format and prone to grow in size and be an abuse vector. But distribution stays in DNS.
 - TXT rfc8805:<https://example.com/geofeed>
- URI (RFC7553) vs SVCB (draft-ietf-dnsop-svcb-https). The latter seems more flexible.

Questions?