ISP Location in DNS Queries
draft-pan-dnsop-edns-isp-location-04

Abstract

Nowadays, many Authoritative Nameservers support GeoIP feature, they guess the user’s geolocation by the client subnet of EDNS Client Subnet (ECS) or by the source IP address of DNS query, return tailor DNS response based on the user’s geolocation. However, ECS raises some privacy concerns because it leaks client subnet information on the resolution path to the Authoritative Nameserver.

This document is inspired by EDNS Client Subnet (ECS), describes an improved solution for GeoIP-enabled Authoritative Nameservers, defines an EDNS ISP Location (EIL) extension to address the privacy problem of ECS, tries to find the right balance between privacy improvement and user experience optimization.

EIL is defined to convey isp location < COUNTRY, AREA, ISP > information that is relevant to the DNS message. It will directly provide the same sufficient information for the GeoIP-enabled Authoritative Nameserver as ECS, to decide the response without guessing geolocation of the IP address.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 28, 2018.
1. Introduction .................................................. 3
   1.1. Path Calculation and Tailored DNS Response .......... 4
2. Requirements Language ........................................ 5
3. Terminology ..................................................... 5
4. Problem of ECS .................................................. 6
   4.1. Client ...................................................... 6
   4.2. Recursive Resolver ........................................ 6
   4.3. GeoIP-enabled Authoritative Nameserver ............... 7
5. Overview ........................................................ 7
   5.1. The EIL EDNS0 option ..................................... 7
6. Protocol Description ............................................ 9
   6.1. Originating the Option .................................... 9
   6.1.1. P-Model: Public recursive resolver ................. 9
   6.1.2. I-Model: ISP recursive resolver ..................... 9
   6.1.3. L-Model: local forwarding resolver ................. 10
   6.2. Generating a Response ..................................... 10
   6.2.1. Whitelist ............................................... 10
   6.2.2. Authoritative Nameserver ............................. 10
   6.2.3. Intermediate Nameserver ............................... 11
   6.3. Handling EIL Responses and Caching .................... 11
   6.3.1. Answering from Cache ................................ 11
   6.3.2. Delegations and Negative Answers ................... 12
6.4. Deploy ....................................................... 12
   6.4.1. Transitivity ........................................... 12
   6.4.2. Compatibility with non-EDNS and ECS ............... 12
   6.4.3. Support ECS and EIL at the same time ............. 13
6.5. Why not use AS number to build EIL ....................... 14
7. Benefit and Cost ................................................ 15
   7.1. Client ..................................................... 15
   7.2. Recursive Resolver ....................................... 15
   7.3. GeoIP-enabled Authoritative Nameserver ............... 16
8. Security Considerations .............................. 16
  8.1. DNSSEC ......................................... 16
  8.2. Privacy ....................................... 16
  8.3. Target Censorship ............................. 17
  8.4. DDoS .......................................... 17
9. IANA Considerations .................................. 17
10. Acknowledgements .................................... 17
11. Appendix A. GeoIP-enabled Authoritative Nameservers Example . 17
   11.1. BIND-GeoIP .................................. 18
   11.2. PowerDNS-GeoIP ............................... 18
   11.3. Amazon-Geolocation-Routing .................. 19
   11.4. DYN-Traffic-Director-ECS .................... 20
   11.5. gdnsd-GeoIP ................................ 20
   11.6. Windows-Server-GeoLocation .................. 20
12. Appendix B. EIL Example ............................. 20
   12.1. P-Model ..................................... 20
   12.2. I-Model ..................................... 21
   12.3. L-Model ..................................... 21
13. Appendix C. Frequent GeoIP-enabled Authoritative Nameserver’s
    Response Accuracy Problem .......................... 21
   13.1. Public Recursive Resolver with non-ECS Authoritative
        Nameserver .................................. 21
   13.2. IP2Geo Database Quality ...................... 22
   13.3. Unstable ISP Network Topology ................ 22
14. References .......................................... 22
   14.1. Normative References ........................ 22
   14.2. Informative References ....................... 23
Authors’ Addresses ....................................... 24

1. Introduction

Nowadays, many authoritative nameservers support GeoIP feature, such as
[BIND-GeoIP], [PowerDNS-GeoIP], [Amazon-Geolocation-Routing],
[DYN-Traffic-Director-ECS], [gdnsd-GeoIP],
[Windows-Server-GeoLocation] (More details are given in Appendix A).
These geographically aware authoritative nameservers guess the user’s
geolocation by the client subnet of ECS or by the source IP address
of DNS query, return tailor DNS response based on the user’s
geolocation.

ECS is an EDNS0 [RFC6891] option, described in [RFC7871], carries
client subnet information in DNS queries for authoritative
nameserver. Compared to source IP address of DNS query, ECS will
help authoritative nameserver to guess the client’s location more
precisely because of the DNS forwarding query structure.

GeoIP-enabled authoritative nameservers use ECS for user geolocation
detecting. However, ECS raises some privacy concerns because it
leaks client subnet information on the resolution path to the authoritative nameserver.

This document describes an improved solution for GeoIP-enabled authoritative nameserver, defines an EDNS ISP Location (EIL) extension to address the privacy problem of ECS, tries to find the right balance between privacy improvement and user experience optimization.

EIL is defined to convey isp location < COUNTRY, AREA, ISP > information that is relevant to the DNS message. It will directly provide the same sufficient information for the GeoIP-enabled authoritative nameserver as ECS, to decide the response without guessing geolocation of the IP address.

EIL is intended for those local forwarding resolvers, recursive resolvers and authoritative nameservers that would benefit from the extension and not for general purpose deployment. It could be applied for tailor DNS response like ECS scenario. EIL can safely be ignored by servers that choose not to implement or enable it.

1.1. Path Calculation and Tailored DNS Response

Separate the consideration of path calculation (data provider) and tailored DNS response (authoritative nameserver).

Data providers make path calculations to optimize content delivery on the Internet based on the network topology, considering many factors such as IP, RIPs, FIBs, AS Path hops, system load, content availability, path latency, etc. Note that, data providers have the full details of the clients, they can make any complex path calculations without ECS and EIL.

Authoritative nameservers configure tailored DNS response based on the result of path calculations, allocate IP addresses to different datacenters, each IP address serves many client subnets. Usually, users from the same < COUNTRY, AREA, ISP > isp location are allocated to the same datacenter, the same best "network topologically close" datacenter. For example, client IP addresses from < China, Beijing, Telecom > are allocated to DataCenter-1, client IP addresses from < China, Beijing, Unicom > are allocated to DataCenter-2, etc. Above is the GeoIP-based Tailored DNS Response.

Therefore, if the GeoIP-enabled authoritative nameservers support ECS, they can use the client subnet information of ECS instead of resolver’s address for geolocation detecting. Alternative, the GeoIP-enabled authoritative nameservers can directly use the <
COUNTRY, AREA, ISP > information of EIL without geolocation detecting.

Again, we emphasize that tailored DNS response does not affect path calculation. Data Providers can make path calculations based on network topology, decide network topological close datacenter for each IP address. Authoritative nameservers allocate tailored DNS response to each IP address based on the "network topological close" result of path calculations. EIL tell authoritative nameserver like that, "I want to know what is best IP address for clients from <China, Beijing, Telecom> at network topology path calculations result", but not "I want to know what is the nearest IP address for clients from <China, Beijing, Telecom> at physical topology path calculations result".

EIL is satisfied if authoritative nameservers aggregate the IP addresses from the same <COUNTRY, AREA, ISP> isp location to visit the same datacenters, we call that GeoIP-based tailored DNS responses, and these tailored responses have the best "network topological close" distance to the users which are generated from network topology path calculations result.

ECS is satisfied if authoritative nameservers make tailored DNS response down to subnet precise level. For example, (subnet-1, ..., subnet-100) are from the same <COUNTRY, AREA, ISP> isp location, Data Provider applies (subnet-1, ..., subnet-50) visit DataCenter-1, (subnet-51, ..., subnet-100) visit DataCenter-2.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] when they appear in ALL CAPS. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual English meanings, and are not to be interpreted as [RFC2119] keywords.

3. Terminology

Basic terms used in this specification are defined in the documents [RFC1034], [RFC1035], [RFC7719] and [RFC7871].

EIL: EDNS ISP Location.

ECS: EDNS Client Subnet, described in [RFC7871].
Local Forwarding Resolver: forwarding resolver is described in [RFC7871]. It is the first forwarding resolver which receives DNS queries from stub resolver, usually deployed nearby the first-hop router such as public Wi-Fi hotspot routers and home routers.

Recursive Resolver: described in [RFC7871]. It is the last-hop before authoritative nameserver in the DNS query path.

Intermediate Nameserver: described in [RFC7871]. Any nameserver in between the stub resolver and the authoritative nameserver, such as a recursive resolver or a Forwarding Resolver.

Intermediate Forwarding Resolver: Any Forwarding Resolver in between the local forwarding resolver and recursive resolver.

authoritative nameserver: described in [RFC7719] and [RFC2182]. It is a server that knows the content of a DNS zone from local knowledge, and thus can answer queries about that zone without needing to query other servers.

4. Problem of ECS

As mentioned in [RFC7871]’s abstract section, since ECS has some known operational and privacy shortcomings, a revision will be worked through the IETF for improvement.

4.1. Client

Common users have little power to defend passive monitoring, especially in the plain-text traffic.

ECS’s client subnet leakage has rise some user privacy concerns.

4.2. Recursive Resolver

Recursive Resolver must deal with ECS’s cache problem, such as low cache hitrate, rise response time, redundant cache size, etc.

Mukund Sivaraman described some scenarios in [CLIENT-SUBNET-BIS].

ECS is precise because it is based on client subnet. But IPv6 addresses will boom, we can foresee it to increase more burden on global recursive resolvers.
4.3. GeoIP-enabled Authoritative Nameserver

Resolver’s IP can on behalf of many client subnets if they are topological close. But this scenario has been varied by public recursive resolver. ECS push client subnets to authoritative nameserver, wants to solve the "public recursive resolver’s IP is topological far from client subnet" problem.

However, ECS rises GeoIP-enabled authoritative nameserver’s dependence on IP2Geo database quality.

Many GeoIP-enabled authoritative nameserver, most of the time, use < COUNTRY, AREA, ISP > information to decide the tailored response. Every GeoIP-enabled authoritative nameserver must operate IP2Geo database carefully and catch up with topology change. The work is inevitable, but ECS aggravate this, because the number of client subnets is far greater than the number of recursive resolvers.

GeoIP-enabled authoritative nameserver needs a more precise IP2Geo database, updates it more frequent than before, to catch up with the huge client subnet network topology, but not the dns resolver’s IP network topology. Every GeoIP-enabled authoritative nameserver should cost more on IP2Geo database.

5. Overview

EIL is an EDNS0 option to allow local forwarding resolvers and recursive resolvers, if they are willing, to forward details about the isp location of client when talking to other nameservers. EIL can be added in queries sent by local forwarding resolvers or recursive resolvers in a way that is transparent to Stub Resolvers and end users.

Like ECS, authoritative nameservers could provide a better answer by using precise isp location in EIL. Intermediate Nameservers could send EIL query and cache the EIL response. This document also provides a mechanism to signal Intermediate Nameservers that they do not want EIL treatment for specific queries.

EIL is only defined for the Internet (IN) DNS class.

5.1. The EIL EDNS0 option

The EIL is an EDNS0 option to include the isp location of client in DNS messages.

It is 16 octets which is structured as follows:
OPTION-CODE, 2 octets, defined in [RFC6891]. EDNS option code should be assigned by the IANA.

OPTION-LENGTH, 2 octets, defined in [RFC6891], contains the length of the payload (everything after OPTION-LENGTH) in octets.

COUNTRY, 2 octets, uppercase, defined in [ISO3166], indicates the country information of the client’s IP. For example, China’s COUNTRY is CN.

AREA, 6 octets, uppercase, defined in [ISO3166] country subdivision code, indicates the area information of the client’s IP. For example, The AREA of Fujian Province in China is 35.

ISP, 4 octets, uppercase, indicates the ISP information of the client’s IP, using shortcut names. ISP shortcut names are unique within the context of the COUNTRY. For example, the shortcut name of China Telecommunications Corporation is TEL, the shortcut name of China United Network Communications is UNI, the shortcut name of China Mobile is MOB, etc.

All fields are in network byte order ("big-endian", per [RFC1700], Data Notation).

The aim to use short names in the fields is to limit the data size of EIL, decrease the DDoS risk.

The null value 0x20 signifies that the field is unknown. If all fields in EIL are set to null value, it means that client doesn’t want to use EIL.
authoritative nameservers can send EIL response with the * value 0x2A in AREA field or ISP field (not COUNTRY field), which signifies that the field is wildcard match. For example, < CN, *, TEL > indicates "all area in China, Telecom ISP".

Example code is at [DNS-TEST-EIL] .

6. Protocol Description

6.1. Originating the Option

The EIL can be initialized by Public recursive resolver, ISP recursive resolver, or local forwarding resolver.

Examples are given in Appendix B.

6.1.1. P-Model: Public recursive resolver

Public recursive resolvers are not close to many users because the service providers couldn’t deploy servers in every country and every ISP’s network, which will affect the response accuracy of authoritative nameservers. To encounter this problem, ECS shifts the client subnet information to authoritative nameserver, but rises user privacy concerns.

Therefore, to keep balance between precise and privacy, when a Public recursive resolver receives a DNS query, it can guess isp location of client’s IP and generate the EIL OPT data, then send EIL query to the authoritative nameserver. This will move the "guess location of client’s IP" work from authoritative nameserver back to Public recursive resolver, lighten the burden of authoritative nameserver, but increase DDoS risk on Public recursive resolver.

In order to improve the user’s privacy, if a recursive resolver receives a DNS query with ECS, it can guess the isp location of SOURCE-PREFIX from the ECS OPT data, and make a new DNS query with EIL, then send the query to authoritative nameserver which supports EIL.

P-model is the most recommended and close to the ECS.

6.1.2. I-Model: ISP recursive resolver

ISP recursive resolver only serves its customers, each of whom has a static isp location. ISP recursive resolver can add EIL transparent to end user, and then authoritative nameserver doesn’t need to "guess location of client’s IP".
EIL will be benefit if the authoritative nameserver could not find the approximate isp location of ISP recursive resolver, which is crucial to DNS response accuracy in ECS.

6.1.3. L-Model: local forwarding resolver

local forwarding resolver is usually on the first-hop router, such as public Wi-Fi hotspot routers and Cisco/Linksys/Netgear/TP-LINK home routers.

When a local forwarding resolver that implements EIL receives a DNS query from an end user, it surely can know about the isp location of client’s IP, and generate the EIL OPT data, then send the EIL query to the intermediate recursive resolver. Intermediate recursive resolver sends the EIL query to the authoritative nameserver.

In this scenario, both Public recursive resolver and authoritative nameserver don’t need to "guess location of client’s IP", because the local forwarding resolver supplies the isp location precisely. That is, EIL can reduce dependence on the IP geolocation database quality, which is crucial to DNS response accuracy in ECS.

If a local forwarding resolver had sent a query with EIL, and receives a REFUSE response, it MUST regenerate a query with no EIL.

6.2. Generating a Response

6.2.1. Whitelist

EIL contains a whitelist for COUNTRY, AREA and ISP, which can be discussed and maintained by the DNSOP working group. authoritative nameservers that supporting EIL must only response the EIL queries matched the whitelist. recursive resolver that supporting EIL must only cache the EIL responses matched the whitelist.

6.2.2. Authoritative Nameserver

Using the isp location specified in the EIL option of DNS query, an authoritative nameserver can generate a tailored response.

authoritative nameservers that have not implemented or enabled support for the EIL ought to safely ignore it within incoming queries, response the query as a normal case without EDNS0 option. Such a server MUST NOT include an EIL option within replies to indicate lack of support for it.
An authoritative nameserver that has implemented this protocol and receives an EIL option MUST include an EIL option in its response to indicate that it SHOULD be cached accordingly.

An authoritative nameserver will return a more appropriate tailored response for the query with an EIL option containing more precisely AREA.

6.2.3. Intermediate Nameserver

Like ECS, Intermediate Nameserver passes a DNS response with an EIL option to its client when the client indicates support EIL.

If an Intermediate Nameserver receives a response that has a larger area than the AREA provided in its query, it SHOULD still provide the result as the answer to the triggering client request even if the client is in a smaller area.

6.3. Handling EIL Responses and Caching

If an Intermediate Nameserver had sent a query with EIL, and receives a NOERROR response without EIL option, it SHOULD treat this answer as suitable for all clients.

Other handling considerations are similar with ECS [RFC7871], SECTION 7.3.

In the cache, all resource records in the Answer section MUST be tied to the isp location specified in the response. The Answer section is valid for all areas which the EIL option covered. For example, an EIL option < CN, 35, TEL > covers all 9 Cities in Fujian Province of China Telecommunications ISP.

Same with ECS, The Additional and Authority sections are excluded.

Enabling support for EIL in an Intermediate Nameserver will increase the size of the cache, and prevent "client subnet leak" privacy concern of ECS.

6.3.1. Answering from Cache

Cache lookups are first done as usual for a DNS query, using the query tuple of < name, type, class >. Then, the appropriate RRset MUST be chosen based on the isp location matching.

If there was an EIL option, the Intermediate Nameserver will lookup for < same COUNTRY, same ISP, same AREA > of the same query tuple in
the cache. Otherwise, try to find < same COUNTRY, same ISP, same AREA > of the same query tuple in the cache.

If no EIL option was provided, the safest choice of the Intermediate Nameserver is dealing the query as a normal case without EDNS0 option.

If no EIL option was provided, but the Intermediate Nameserver want to be more aggressive, it can guess the isp location from the source IP of the query, then respond as if there was an EIL option with the guessed information. Users can be benefit when the Intermediate Nameserver has a more precise IP location database than the authoritative nameserver, especially in global public DNS service like GoogleDNS(8.8.8.8).

If no matching is found, the Intermediate Nameserver MUST perform resolution as usual.

6.3.2. Delegations and Negative Answers

EIL’s delegation case is similar with ECS, Additional and Authority Sections SHOULD ignore EIL.

For negative answers, authoritative nameservers return traditional negative answers without EIL.

6.4. Deploy

6.4.1. Transitivity

EIL’s transitivity concerns are similar with ECS.

Name servers should only enable EIL where it is expected to benefit the end users, such as dealing with some latency-sensitive CDN domain queries in a complex network environment.

6.4.2. Compatibility with non-EDNS and ECS

For realworld compatibility, EIL is designed as an additional feature to ECS. If a nameserver supports EIL, it must support ECS first. So there are three scenarios: non-EDNS, ECS but non-EIL, ECS and EIL.

- GeoIP-enabled authoritative nameservers map ECS’s client subnet into EIL’s geolocation to get tailor response, they can simply add EIL support. Some realtime client subnet sensitive CDN domains, such as Akamai, they may not support GeoIP feature and EIL.
EIL-enabled recursive resolvers only send EIL queries to EIL-enabled authoritative nameservers. At the same time, they can also send ECS queries.

The indicator that authoritative nameservers used to generate tailored response is shown as follows:

<table>
<thead>
<tr>
<th></th>
<th>AUTH (non-EDNS)</th>
<th>AUTH (ECS but non-EIL)</th>
<th>AUTH (ECS and EIL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RECUR (non-EDNS)</td>
<td>Resolver's IP</td>
<td>Resolver's IP</td>
<td>Resolver's IP</td>
</tr>
<tr>
<td>RECUR (ECS but non-EIL)</td>
<td>Resolver's IP</td>
<td>Client Subnet</td>
<td>Client Subnet</td>
</tr>
<tr>
<td>RECUR (ECS and EIL)</td>
<td>Resolver's IP</td>
<td>Client Subnet</td>
<td>Client Subnet or EIL's &lt; COUNTRY, AREA, ISP &gt;</td>
</tr>
</tbody>
</table>

6.4.3. Support ECS and EIL at the same time

Nameservers can support ECS and EIL at the same time. ECS and EIL can’t be both initiated at the same DNS packet. It is better for user privacy if nameservers initiate the EIL query prior to the ECS query.

If authoritative nameservers support both ECS and EIL, recursive resolvers can cache both ECS response and EIL response, there are some choices for recursive resolvers when they receive DNS queries.
Receive EIL query:
  Search in EIL cache.
  If cache is matched, return EIL response.
  Otherwise, send EIL query to authoritative nameserver.

Receive ECS query:
  Search in ECS cache.
  If cache is matched, return ECS response.
  Otherwise, send ECS query to authoritative nameserver.

Receive DNS query without EDNS option:
  Search in ECS cache.
  If cache is matched, return ECS response.
  Otherwise,
    Guess the isp location information of the client’s IP,
    build EIL option for the query packet.
    Search in EIL cache.
    If cache is matched, return EIL response.
    Otherwise, send EIL query to authoritative nameserver.

Receive DNS query with not-ECS/not-EIL option:
  Search in not-EDNS cache.
  If cache is matched, return response.
  Otherwise, send the DNS query to authoritative nameserver.

Receive ECS query, improve user privacy:
  Guess the isp location information of the client’s IP,
  build EIL option for the query packet.
  Search in EIL cache.
  If cache is matched, return EIL response RR with origin ECS option.
  Otherwise, send EIL query to authoritative nameserver.

6.5. Why not use AS number to build EIL

  AS number is not an ideal object to balance between response accuracy
  and user privacy, for example:

  o AS24151 can directly guide to China Internet Network Infomation
    Center, it is not good for user privacy.

  o AS4134 contains a huge amount of IP prefixes whose geolocation
    covers from South China to North China, AS number can not afford
    the response accuracy consideration.

  o < COUNTRY-CODE, AREA-CODE, AS-NUMBER > may be a considerable
    trade-off choice on public recursive resolver, but inconvenience
    on local forwarding resolver.
7. Benefit and Cost

7.1. Client

EIL is transparent to client.

EIL is to help mitigate client subnet leakage on the resolution path, without sensitive identity information.

7.2. Recursive Resolver

ECS sends the query with client subnet, which means that recursive resolvers have to send a new query to authoritative nameservers with client_subnet_b, even it has known the response about topological close client_subnet_a. In fact, thousands of subnets visit only a few servers, there are many redundancy queries, the recursive’s cache hitrate is low.

Because of ECS’s low cache hitrate, recursive servers’s ECS tailored response latency will be longer, the average of response time will rise with the redundancy queries rate from recursive resolvers to authoritative nameservers.

Recursive’s ECS cache size grows up with the number of client subnets.

To sum it up, above problems all rise with the client subnet amount, especially when IPv6 addresses boom. Extend the subnet range in the ECS response may be mitigating, but not work for wide range client subnets. Recursive can make some guess optimization, if it has known response for client_subnet_a, then guess to return the same response for topological close client_subnet_b without send the redundancy query.

Therefore, if the ECS revision wants to make more effective client subnets aggregation for recursive resolver, then EIL can be an considerable choice. EIL wants to summary topological close client subnets into < COUNTRY, AREA, ISP > for GeoIP-enabled authoritative nameserver. With EIL response cache, recursive resolvers can directly response for many ECS client subnets queries, which will rise cache hitrate and reduce response latency. The cache size of EIL is related to the row count in the < COUNTRY, AREA, ISP > isp location whitelist. Therefore, under IPv6 environment, the cache size of EIL will be much smaller than ECS.

Note that, the EIL’s IP2Geo mapping work will make recursive resolver to cost more cpu.
7.3. GeoIP-enabled Authoritative Nameserver

Client subnet is the best factor if the company has good network topology monitor ability, often for big company. However, for many authoritative servers that only deployed GeoDNS, the accuracy limitation is commonly because of the IP2Geo database quality, and the small ISPs change to another next-hop big ISP suddenly.

For the GeoIP-enabled authoritative nameserver, the response accuracy depends on the IP geolocation database quality. If authoritative nameserver can not find approximate isp location of ECS’s client subnet, they can not return best tailored response.

Even though GeoIP-enabled authoritative nameservers know about the precise isp location of ECS’s client subnet, they may not know about the latest topological path change of the isp to update the tailored response in time. In the case of "small ISP -> big ISP (change frequency) -> ... -> website", both small ISP’s client ip/resolver ip is not good factor for GeoDNS. Big companies work hard to catch up with the client ip’s connect topology change, and adjust their authoritative nameservers’ tailored response, but smaller companies only deploy IP2Geo may not afford.

EIL wants to give downstream a chance to tell authoritative nameserver its best path quickly and proactively, help to rise the response accuracy, avoid cross-isp visit, save IP transit cost for Data Provider. EIL directly provide sufficient information for the GeoIP-enabled authoritative nameserver. Compared to ECS, EIL can reduce GeoIP-enabled authoritative nameserver’s dependence on the IP geolocation database quality.

8. Security Considerations

8.1. DNSSEC

EIL is not signed.

8.2. Privacy

The biggest privacy concern on ECS is that client subnet information is personally identifiable. The more domains publish their zones on a third-party authoritative nameserver, the more end user privacy information can be gathered by the authoritative nameserver according to the ECS queries.

EIL is to improve user privacy which is inspired by ECS, prevented leaks in the client subnet information.
Like ECS, EIL will leak the global zonefile configurations of the authoritative nameservers more easily than normal case.

8.3. Target Censorship

DNS traffic is plain text by default. It is easily to be blocked or poisoned by internet target censorship. To bypass the censorship, it is better to encrypt the DNS traffic or use some proxy tunnel.

EIL’s isp location information covers bigger area than ECS’s client subnet information. Therefore, compared to ECS in plain text condition, EIL is weaker at blocking record attack, but stronger at targeted DNS poisoning attack.

8.4. DDoS

To migrate the DDoS problem:

- If an Authority Server receives a DNS query with unknown data in EIL option, it SHOULD return the default response whose EIL option with null value.

- Nameservers OPTIONAL only implement EIL when the query is from a TCP connection.

More migration techniques described in [RFC7871], Section 11.3.

9. IANA Considerations

This document defines EIL, need request IANA to assign a new EDNS0 option code to EIL.

10. Acknowledgements

EIL is inspired by ECS, the authors especially thanks to C. Contavalli, W. van der Gaast, D. Lawrence, and W. Kumari.

Thanks comments for Barry Raveendran Greene, Paul Vixie, Petr Špaček, Brian Hartvigsen, Ask Bjoern Hansen, Dave Lawrence.

Thanks a lot to all in the DNSOP, DNSPRIV mailing list.

11. Appendix A. GeoIP-enabled Authoritative Nameservers Example
11.1. BIND-GeoIP

As described in [BIND-GeoIP], BIND 9.10 is able to use data from MaxMind GeoIP databases to achieve restrictions based on the (presumed) geographic location of that address. The ACL itself is still address-based, but the GeoIP-based specification mechanisms can easily populate an ACL with addresses in a certain geographic location.

```plaintext
acl "example" {
  geoip country US;
  geoip region CA;
  geoip city "Redwood City"; /* names, etc., must be quoted if they contain spaces */
};
```

11.2. PowerDNS-GeoIP

As described in [PowerDNS-GeoIP], PowerDNS supports many geolocation placeholders, such as %co = 3-letter country, %cn = continent, %re = region, %ci = city.
domains:
  - domain: geo.example.com
ttl: 30
records:
  geo.example.com:
    - soa: ns1.example.com hostmaster.example.com 2014090125 7200 3600 1209600 3600
    - ns:
        content: ns1.example.com
ttl: 600
    - ns: ns2.example.com
    - mx: 10 mx.example.com
fin.eu.service.geo.example.com:
  - a: 192.0.2.2
txt: hello world
  - aaaa: 2001:DB8::12:34DE:3
# this will result first record being handed out 30% of time
swe.eu.service.geo.example.com:
  - a:
        content: 192.0.2.3
        weight: 50
    - a: 192.0.2.4
services:
  # syntax 1
  service.geo.example.com: '%co.%cn.service.geo.example.com'
  # syntax 2
  service.geo.example.com: ['%co.%cn.service.geo.example.com', '%cn.service.geo.example.com']
  # alternative syntax
  services:
    service.geo.example.com:
      default: ['%co.%cn.service.geo.example.com', '%cn.service.geo.example.com']
10.0.0.0/8: 'internal.service.geo.example.com'

11.3. Amazon-Geolocation-Routing

As described in [Amazon-Geolocation-Routing], Amazon Route 53 lets you choose the resources that serve your traffic based on the geographic location of your users, meaning the location that DNS queries originate from. It allows you to route some queries for a continent to one resource and to route queries for selected countries on that continent to a different resource.

When a browser or other viewer uses a DNS resolver that does support edns-client-subnet, the DNS resolver sends Amazon Route 53 a truncated version of the user’s IP address. Amazon Route 53 determines the location of the user based on the truncated IP address rather than the source IP address of the DNS resolver; this typically provides a more accurate estimate of the user’s location.  Amazon
Route 53 then responds to geolocation queries with the DNS record for the user’s location.

11.4. DYN-Traffic-Director-ECS

As described in <DYN-Traffic-Director-Geographic-Groups> and [DYN-Traffic-Director-ECS], Dyn provides the ability to control DNS responses on a granular/customized geographical rule set. Part of the rule sets will be the identification of the global regions, countries, or states and provinces that use a specific DNS server group. DYN uses the ECS information for the geolocation lookup. Once a geolocation is found and a response is selected, it will provide a DNS response back to the source IP address.

11.5. gdnsd-GeoIP

As described in [gdnsd-GeoIP], gdnsd uses MaxMind’s GeoIP binary databases to map address and CNAME results based on geography and monitored service availability. gdnsd supports geolocation codes, such as continent, country, region/subdivision, city.

11.6. Windows-Server-GeoLocation

As described in [Windows-Server-GeoLocation], Windows server can be configured DNS Policy to respond to DNS client queries based on the geographical location of both the client and the resource to which the client is attempting to connect, providing the client with the IP address of the closest resource.

12. Appendix B. EIL Example

Authoritative nameserver of www.example.com has enabled EIL.


12.1. P-Model

Stub DNS

-> local forwarding resolver (61.48.7.2)
-> Public Forwarding Resolver (AliDNS, 223.5.5.5)
-> Public recursive resolver (AliDNS, 202.108.250.231)
-> authoritative nameserver

Public Forwarding Resolver 223.5.5.5 could enable EIL and generate the EIL OPT data < CN, 11, UNI > based on 61.48.7.2.

P-Model will not leak client subnet to authoritative nameserver.
12.2. I-Model

Stub DNS
-> local forwarding resolver
-> ISP Forwarding Resolver(202.106.196.115)
-> ISP recursive resolver(61.135.23.92)
-> authoritative nameserver

ISP recursive resolver 61.135.23.92 could enable EIL and generate the EIL OPT data < CN, 11, UNI > based on 61.135.23.92.

If authoritative nameserver doesn’t know much about 61.135.23.92, EIL will be helpful.

ISP recursive resolver generates static EIL query, simply manages response cache as transition non-ECS/non-EIL scenario.

EIL helps ISP recursive resolver to give upstream an explicit correct isp location information.

12.3. L-Model

Stub DNS
-> Local Forwarding Resolver(58.60.109.234)
-> ...
-> authoritative nameserver

Local Fowarding Resolver 58.60.109.234 could enable EIL and generate the option data is < CN, 44, TEL > based on 58.60.109.234.

L-Model can give the most precisely isp location information for DNS resolution.

13. Appendix C. Frequent GeoIP-enabled Authoritative Nameserver’s Response Accuracy Problem

13.1. Public Recursive Resolver with non-ECS Authoritative Nameserver

If authoritative nameserver doesn’t support ECS, the clients that use public recursive resolver(such as 8.8.8.8) may receive disaster latency IP.

In this scenario, we must pray that public recursive resolver’s IP is topological close to client’s IP.
13.2. IP2Geo Database Quality

If authoritative nameserver’s IP2Geo database misidentify client IP’s information, then the client may be assigned to some high latency cross-isp IP address.

With EIL, public recursive resolver and ISP recursive resolver can help to give more precise information for GeoIP-enabled authoritative nameservers.

13.3. Unstable ISP Network Topology

Some small ISPs may change their upstreams frequently. Authoritative nameservers often can not catch up the variation in time.

EIL gives downstream a chance to proactively tell authoritative nameservers the latest best topological close response itself wants now. Downstream can assure itself has got explicit tailored response with EIL.

For example, 218.247.200.100’s isp location information is < China, Beijing, PengBoShi >. In I-Model, PengBoShi’s resolver can send EIL < CN, 11, TEL > to authoritative nameservers, indicates that the best topological close response for client 218.247.200.100 is from China Beijing Telecom.

14. References

14.1. Normative References


14.2. Informative References

[Amazon-Geolocation-Routing]

[BIND-GeoIP]

[CLIENT-SUBNET-BIS]

[DNS-TEST-EIL]

[DYN-Traffic-Director-ECS]

[DYN-Traffic-Director-Geographic-Groups]

[gdnsd-GeoIP]

[ISO3166]

[PowerDNS-GeoIP]

Authors' Addresses

Lanlan Pan
Beijing
China

Email: abbypan@gmail.com
URI: https://github.com/abbypan

Yu Fu
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing
China

Email: fuyu@cnnic.cn