Abstract

This document describes an Extension Mechanisms for DNS (EDNS0) option that is in active use to carry information about the network that originated a DNS query and the network for which the subsequent response can be cached.

It is inspired by EDNS Client Subnet (ECS) with some privacy considerations, goals to reduce the "guess geolocation of client’s IP" work on Authoritative Nameservers.

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 14, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must
1. Introduction

As described in EDNS Client Subnet (ECS) [RFC7871], many Authoritative Servers today return different responses based on the perceived geolocation of the user. Traditionally, Authoritative Server guesses the user’s geolocation by the source IP address of dns query.
ECS is an EDNS0 [RFC6891] option to carry client subnet information in DNS queries for Authoritative Server. Compared to source IP address of DNS query, ECS will help Authoritative Server to guess the client's geolocation more precisely because of the DNS forwarding query structure. However, ECS raises some privacy concerns because it leaks client subnet information on the resolution path to the Authoritative Server.

This document is an improved solution for ECS, describes an EDNS ISP Location (EIL) extension to address the privacy problem of ECS, find the right balance between privacy improvement and user experience optimization. EIL is defined to convey ISP location information that is relevant to the DNS message. It will provide sufficient information for the Authoritative Server to decide the response without guessing geolocation of the IP address.

EIL is intended for those Local Forwarding Resolvers, Recursive Resolvers and Authoritative Servers that would benefit from the extension and not for general purpose deployment like ECS scenario. It could be applied for tailor DNS response. EIL can safely be ignored by servers that choose not to implement or enable it.

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] key words.

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 Server 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.

Authoritative Server: 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. Overview

This document provides 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.

The format of EIL option is described in Section 5. 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. EIL is only defined for the Internet (IN) DNS class.

Like ECS, Authoritative Servers 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.

The security concerns for EIL are like ECS, such as cache growth, spoof EDNS0 option and privacy, etc. Mitigation techniques are discussed in Section 6.

5. The EIL EDNS0 option

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

It is 14 octets which is structured as follows:
EIL Structure

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.

6. Protocol Description

6.1. Originating the Option

The EIL can be initialized by Public Recursive Resolver, ISP Recursive Resolver, or Local Forwarding Resolver.

6.1.1. P-Model: Public Recursive Resolver

When a public Recursive Resolver receives a DNS query, it can guess geolocation of client’s IP and generate the EIL OPT data, then send EIL query to the Authoritative Server. This will move the "guess geolocation of client’s IP" work from Authoritative Server to Public Recursive Resolver, lighten the burden of Authoritative Server, 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 Server 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 geolocation. ISP Recursive Resolver can add EIL transparent to end user, and then Authoritative Server doesn’t need to "guess geolocation of client’s IP".

EIL will be benefit if the Authoritative Server could not find the approximate geolocation 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 geolocation information 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 Server.
In this scenario, both public Recursive Resolver and Authoritative Server don’t need to “guess geolocation of client’s IP”, because the Local Forwarding Resolver supplies the geolocation 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-CODE, AREA-CODE and ISP, which can be discussed or maintained by the DNSOP working group. Authoritative Servers 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 Server

Using the isp location specified in the EIL option of dns query, an Authoritative Server can generate a tailored response.

Authoritative Servers 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 Server 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 Server will return a more appropriate tailored response for the query with an EIL option containing more precisely AREA-CODE.

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-CODE 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, SECTION 7.3.

6.3.1. Caching the Response

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 { "COUNTRY-CODE": "CN", "AREA-CODE": "35", "ISP": "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.

6.3.2. 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-CODE, same ISP, same AREA-CODE > of the same query tuple in the cache. Otherwise, try to find < same COUNTRY-CODE, same ISP, same AREA-CODE > 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 Server, 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.
6.3.3. Support ECS and EIL at the same time

Name servers 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 name servers initiate the EIL query prior to the ECS query.

If Authoritative servers 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 Server.

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

Receive DNS query without EDNS option:
   Search in ECS cache.
   If cache is matched, return ECS response.
   Otherwise,
      Guess the geolocation 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 Server.

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 Server.

Receive ECS query, improve user privacy:
   Guess the geolocation 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 Server.
6.4. Delegations and Negative Answers

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

For negative answers, Authoritative Servers return traditional negative answers without EIL.

6.5. 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.

7. Security Considerations

7.1. DNSSEC

EIL is not signed.

7.2. 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 Server, the more end user privacy information can be gathered by the Authoritative Server 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 Servers more easily than normal case.

7.3. 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 geolocation 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.
7.4. Cache Size

Like ECS, cache size will raise if a public recursive resolver supports EIL. The cache size of ECS grows up with the number of client subnets. The cache size of EIL is related to the row count in the <COUNTRY-CODE, AREA-CODE, ISP> geolocation whitelist. Therefore, under IPv6 environment, the cache size of EIL will be smaller than ECS.

7.5. 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.

8. IANA Considerations

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

9. Acknowledgements

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

Thanks a lot to all in the DNSOP and DNSEXT mailing list.

This document was produced using the xml2rfc tool [RFC2629].

10. References

10.1. Normative References


10.2. Informative References


Appendix A. Example

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


Example 1: P-Model

Resolution Path: 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 Server
Public Forwarding Resolver 223.5.5.5 could enable EIL and generate the EIL OPT data { "COUNTRY-CODE": "CN", "AREA-CODE": "11", "ISP": "UNI" } based on 61.48.7.2.

P-Model will not leak client subnet to Authoritative Server.

Example 2: I-Model

Resolution Path: Stub DNS -> Local Forwarding Resolver -> ISP Forwarding Resolver (202.106.196.115) -> ISP Recursive Resolver (61.135.23.92) -> Authoritative Server

ISP Recursive Resolver 61.135.23.92 could enable EIL and generate the EIL OPT data { "COUNTRY-CODE": "CN", "AREA-CODE": "11", "ISP": "UNI" } based on 61.135.23.92.

If Authoritative Server doesn’t know much about 61.135.23.92, EIL will be helpful.

Example 3: L-Model

Resolution Path: Stub DNS -> Local Forwarding Resolver (58.60.109.234) -> ... -> Authoritative Server

Local Forwarding Resolver 58.60.109.234 could enable EIL and generate the option data is { "COUNTRY-CODE": "CN", "AREA-CODE": "44", "ISP": "TEL" } based on 58.60.109.234.

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

Authors’ Addresses

Lanlan Pan
CNNIC
No.4 South 4th Street, Zhongguancun
Hai-Dian District, Beijing, 100190
P.R. China

Email: abbypan@gmail.com