Abstract

This document describes a new DNS resource record (RR) type, called the Edge Exchanger (EDX) RR, that is used to find services and location of the server(s) for any specific domain (the word domain is used here in the strict RFC1034 sense).

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 https://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."

Copyright Notice

Copyright (c) 2019 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 include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

This document proposes a new Resource Record (RR) named Edge Exchanger (EDX) for the Domain Name System (DNS) [RFC1034] and its application usage. This document specifies how this DNS resource record helps client in finding lowest latency servers and also facilitate service discovery given the correct domain name.

Currently, the service discovery can be done using SRV resource record type where the client requests for a specific service and protocol for a domain name and receives the target host and port where the service instance can be reached. To connect to the target host client needs to perform DNS resolution to fetch the IP address. Hence, we propose DNS EDX RR which provides a platform for clients to discover the services available for a domain name with list of primary IP address, running services and port information.

At present, there is no way to find all the services available in a server using one DNS query. The new RR EDX allow servers to advertise its services to all users as well as it enables client to find the low latency edge servers for a service using the service and location information.

Querying the EDX Resource Record does not mean replacement of SRV.
Internet Draft                                          October 23, 2019

[RFC2782] and LOC [RFC1876] Resource record. Instead, EDX RR provides a complimentary mechanism to find the list of services as well as location, port and IP address of the primary servers present for the corresponding services for a domain, using just one query.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Applicability Statement

In general, it is expected that EDX records will be used by clients for applications to find the hosted services and locations for a specific hostname. Clients pass a hostname with EDX Service Field and get back the services, protocol and target names of all available servers. One example is when an organization provides more than one services running on multiple primary and backup servers but the clients are unaware of these services. Clients can discover these set of services using EDX RR type queries.

3. EDX Resource Record Format

The master file format of EDX RR type is defined below.

owner TTL Class EDX (Edge Port Lat Long Priority Version Address _Service._Proto.Target-host)

( The parentheses are used for multi-line data as specified in [RFC 1035] section 5.1. )

Owner       : The domain-name for which these RR refers to.
TTL         : Standard DNS meaning [RFC1035].
Class       : Standard DNS meaning [RFC1035]. EDX records occur in the IN Class.
Edge        : A flag to set the target host as edge or remote server.
Service     : The symbolic name of the services supported by the owner. An underscore (_) is prepend to the service identifier to avoid collisions with DNS labels that occur in nature. Valid service parameters are those registered by IANA in the "Service Name and Transport Protocol Port Number Registry" as mentioned in [RFC6335]. The Service is case insensitive.
Proto : The symbolic name of the protocol supported by target host, with an underscore (_) prepend to prevent collisions with DNS labels that occur in nature. Valid protocol parameters are those registered by IANA in the "Service Name and Transport Protocol Port Number Registry" as mentioned in [RFC2782]. _TCP and _UDP are at present the most useful values for this field, though any name defined by Assigned Numbers or locally may be used (as for Service). The Proto is case insensitive.

Target-host : The domain name of the target host. There MUST be one or more address records for this name, the name MUST NOT be an alias (in the sense of [RFC1034]).

Port : The port on this target host of this service. The range is 0-65535. This is a 16 bit unsigned integer in network byte order. This is often as specified in Assigned Numbers but need not be.

Lat : The latitude of the center of the sphere described by the SIZE field, expressed as a 32-bit integer, most significant octet first (network standard byte order), in thousandth of a second of arc. 2^31 represents the equator; numbers above that are north latitude.

Long : The longitude of the center of the sphere described by the SIZE field, expressed as a 32-bit integer, most significant octet first (network standard byte order), in thousandths of a second of arc, rounded away from the prime meridian. 2^31 represents the prime meridian; numbers above that are east longitude.

Priority : The priority of this target host. A client MUST attempt to contact the target host with the lowest-numbered priority it can reach; target hosts with the same priority SHOULD be tried in an order defined by the weight field. The range is 0-65535. This is a 16 bit unsigned integer in network byte order.


Address : A 128 bit Internet address. The IP addresses may belong to A [RFC1035] or AAAA [RFC3596] Resource Record Sets. The IP address will range from 32 bit to 128 bit.

3.1. Example Data
3.2. EDX RDATA Wire Format

The RDATA of EDX RR consist fixed length as well as variable length parameters.

<table>
<thead>
<tr>
<th>MSB</th>
<th>LSB</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>28</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+-------------------------------+</td>
</tr>
<tr>
<td>28+x</td>
<td></td>
</tr>
</tbody>
</table>

Edge flag and Port are unsigned 16 bit integer. Edge Flag is 0 or 1
for remote server or edge server respectively, whereas the value of port ranges from 0-65535. It is expressed in network byte order.

Latitude and Longitude are signed integers expressed in network byte order.

Priority and IP Version are unsigned integers in network byte order.

IP Address can vary from 32 to 128 bit unsigned integer based on IP Address Type "A" or "AAAA".

Finally, the RDATA consists of a variable length Target field which consist of service, protocol and target name. The length of the Target Field MUST be greater than zero.

4. Usage Rules

A EDX-cognizant client SHOULD use this procedure to discover the list of services and the location of these servers:

Do a lookup for QNAME=domain-name, QTYPE=EDX.

5. Usage Scenarios

In this section, a number of scenarios showing the usage and practical applications of EDX RR are explained briefly.

5.1. Query without knowing the service name

Client need not know the service name for querying the domain for any service related information. The EDX resource record can be viewed as a broader extension of SRV RR. Unlike SRV RR, where SHOULD know the domain name, the service name and the protocol name, EDX RR can be used without knowing the service name. Just the correct domain name is enough to fetch the available services and its related information.

5.2. A new way to explore available services

Client can now explore a domain for its available services. An organization having specific domain name providing many services like FTP archive, http and https services can be browsed by any client knowing the domain name. For example, the organization with domain name sribsamsung.example.com. can have these entries in DNS master file.

$ORIGIN sribsamsung.example.com.
These services provided by sribsamsung.example.com can be fetched using just one DNS EDX RR query using the domain name and without knowing all the services and protocols. With the EDX RR responses the clients can use these available services.

The number of answers and its sequence in EDX RR MUST be based on server Resource Record configuration and the maximum limit of response data. This document does not specify any priority criteria, based on service name or location information.

5.3. Discover the edge servers

Clients can use the edge flag and the location information of EDX response to locate the low latency servers among all for any services.

5.4. A platform to advertise the available services

This new EDX RR provides servers a platform to advertise their services to clients by updating their running services and target host information as EDX resource record.

6. IANA considerations

This RFC defines the format of a new Resource Record (RR) for the Domain Name System (DNS), and reserves a corresponding DNS type mnemonic (EDX) and numerical code (234) if accepted by IANA. IANA is requested to assign a DNS RR data type value of 234 and DNS type mnemonic EDX for this new DNS EDX RR. No other IANA services are required by this document.

7. Security Considerations

This section contains a description of the known threats involved with the usage of the DNS EDX RR.

7.1. Attacker Tampering with an Insecure EDX RR

With EDX, DNS spoofers can supply false port numbers, locations as well as target names and addresses. Because this vulnerability exists
already, with names and addresses, this is not a new vulnerability, merely a slightly extended one, with little practical effect.

To avoid the same, an EDX client SHOULD obtain EDX RRs from a trusted party through a secure channel ensuring data integrity and authenticity of the RRs. DNSSEC [RFC4033] [RFC4034] [RFC4035] provides such a secure channel. However, it should be emphasized that DNSSEC only offers data integrity and authenticity guarantees to the channel between the DNS server publishing a zone and the HIP node. DNSSEC does not ensure that the entity publishing the zone is trusted.

7.2. Response Data

In the absence of secure channel, the Authoritative DNS servers MAY validate the client IP Address. An Authoritative DNS server MAY prevent returning EDX records over UDP unless the source IP address has been confirmed with DNS Cookies. If a query is received via UDP without source IP address verification, the server MUST NOT return REFUSED but answer the query with an empty answer section and the truncation flag set ("TC=1").

7.3. Error Handling

It is also possible that the EDX in the resource record type has errors in it. Applications using the EDX resource record type for resolution SHOULD behave similarly as if the user typed the correct domain name without any resource records. At least it must be clear to the user that the error is not due to any error from his side.

8. References

8.1. Normative References


8.2. Informative References


Author’s Addresses

Sweta Jaiswal
Samsung R&D Institute India – Bangalore

Expires April 25, 2020
Karnataka - 560037
India.
Email: sweta.j@samsung.com

Karthikeyan Arunachalam
Samsung R&D Institute India - Bangalore
Karnataka - 560037
India.
Email: karthikeya.a@samsung.com

Jamsheed Manja Ppallan
Samsung R&D Institute India - Bangalore
Karnataka - 560037
India.
Email: jamsheed.mp@samsung.com

Dronamraju Siva Sabareesh
Samsung R&D Institute India - Bangalore
Karnataka - 560037
India.
Email: s.sabareesh@samsung.com

Madhan Raj Kanagarathinam
Samsung R&D Institute India - Bangalore
Karnataka - 560037
India.
Email: madhan.raj@samsung.com