DNS Resolver Information

Abstract

This document specifies a method for DNS resolvers to publish
information about themselves. DNS clients can use the resolver
information to identify the capabilities of DNS resolvers.

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."

This Internet-Draft will expire on 4 March 2023.

Copyright Notice

Table of Contents

1. Introduction

Historically, DNS stub resolvers communicated with recursive
resolvers without needing to know anything about the features
supported by these recursive resolvers. As more and more recursive
resolvers expose different features that may impact the delivered
DNS service, means to help stub resolvers to identify the
capabilities of the resolver are valuable. Typically, stub resolvers
can discover and authenticate encrypted DNS servers provided by a
local network, for example, using the techniques specified in [I-
D.ietf-add-dnr] and [I-D.ietf-add-ddr]. However, these stub
resolvers need a means to retrieve information from the discovered
recursive resolvers about their capabilities.

This document fills that void by specifying a method for stub
resolvers to retrieve such information. To that aim, a new RR type
is defined for stub resolvers to query the recursive resolvers. The
information that a resolver might want to give is defined in Section
5.

Retrieved information can be used to feed the server selection
procedure.

2. Terminology

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
BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all
capitals, as shown here.

This document makes use of the terms defined in [RFC8499].

'Encrypted DNS' refers to a DNS protocol that provides an encrypted
channel between a DNS client and server (e.g., DoT, DoH, or DoQ).

3. Retrieving Resolver Information

A stub resolver that wants to retrieve the resolver information may
use the RR type "RESINFO" defined in this document (see Section
7.1).

The content of the RDATA in a response to RR type query is defined
in Section 5. If the resolver understands the RESINFO RR type, the
RRSet in the Answer section MUST have exactly one record.

A DNS client can retrieve the resolver information using the RESINFO
RR type and QNAME of the domain name that is used to authenticate
the DNS server (referred to as ADN in [I-D.ietf-add-dnr]).

If the special use domain name "resolver.arpa" defined in [I-D.ietf-
add-ddr] is used to discover the Encrypted DNS server, the client
can retrieve the resolver information using the RESINFO RR type and
QNAME of the designated resolver.

4. Format of the Resolver Information

The resolver information uses the same format as DNS TXT records.
The intention of using the same format as TXT records is to convey a
small amount of useful information about a DNS resolver. As a
reminder, the format rules for TXT records are defined in Section
3.3.14 of the DNS specification [RFC1035] and further elaborated in
Section 6.1 of the DNS-based Service Discovery (DNS-SD) [RFC6763].
The recommendations to limit the TXT record size are discussed in
Section 6.2 of [RFC6763].

Similar to DNS-SD, the RESINFO RR type uses "key/value" pairs to
convey the resolver information. Each "key/value" pair is encoded
using the format rules defined in Section 6.3 of [RFC6763]. Using
standardized "key/value" syntax within the RESINFO RR type makes it
easier for future keys to be defined. If a DNS client sees unknown
keys in a RESINFO RR type, it MUST silently ignore them. The same
rules for the keys as those defined in Section 6.4 of [RFC6763] MUST
be followed for RESINFO.

Keys MUST either be defined in the IANA registry Section 7.2 or
begin with the substring "temp-" for names defined for local use
only.

5. Resolver Information Keys/Values

The following resolver information keys are defined:

qnamemin:
        If the DNS resolver supports QNAME minimisation [RFC9156]
   to improve DNS privacy, the key is present. Note that, as per the
   rules for the keys defined in Section 6.4 of [RFC6763], if there
   is no '=' in a key, then it is a boolean attribute, simply
   identified as being present, with no value.

   This is a mandatory attribute.

exterr: If the DNS resolver supports extended DNS errors (EDE)
   [RFC8914] to return additional information about the cause of DNS
   errors, the value of this key lists the possible extended DNS
   error codes that can be returned by this DNS resolver. When
   multiple values are present, these values MUST be comma-
   separated.

   This is an optional attribute.

infourl: An URL that points to the generic unstructured resolver
   information (e.g., DoH APIs supported, possible HTTP status codes
   returned by the DoH server, how to report a problem) for
   troubleshooting purpose.

   The server MUST support the content-type 'text/html'. The DNS
   client MUST reject the URL if the scheme is not "https". The
   client MUST validate that both the encrypted DNS server and the
   resolver information server are owned and managed by the same
   entity by establishing a TLS connection to the domain name in the
   URL and checking if the subjectAltName entry in the server
   certificate includes the name of the encrypted DNS server. If
   this match fails, the client MUST ignore the resolver
   information. The URL should be treated only as diagnostic
   information for IT staff.

   This is a mandatory attribute.

New keys can be defined as per the procedure defined in Section 7.2.

Figure 1 shows an example of published resolver information record:


```
resolver.example.net. 7200 IN RESINFO qnamemin exterr=15,16,17
                   resinfourl=https://resolver.example.com/guide
```

            Figure 1: An Example of Resolver Information Record

6. Security Considerations

Unless a DNS request to retrieve the resolver information is
encrypted (e.g., sent over DNS-over-TLS (DoT) [RFC7858] or DNS-over-

HTTPS (DoH)) [RFC8484]), the response is susceptible to forgery. The DNS resolver information can be retrieved after the encrypted connection is established to the DNS server or retrieved before the encrypted connection is established to the DNS server by using local DNSSEC validation.

7. IANA Considerations

Note to the RFC Editor: Please update [RFCXXXX] with the RFC number to be assigned to this document.

7.1. RESINFO RR Type

This document requests IANA to register a new value from the "Resource Record (RR) TYPEs" subregistry of the "Domain Name System (DNS) Parameters" registry available at [RRTYPE]:

Type: RESINFO
Value: TBD
Meaning: Resolver Information as Key/Value Pairs
Reference: [RFCXXXX]

7.2. DNS Resolver Information Key Registration

This document requests IANA to create a new registry entitled "DNS Resolver Information Keys". This registry contains definitions of the keys that can be used to provide the resolver information.

The registration procedure is Specification Required (Section 4.6 of [RFC8126]).

The structure of the registry is as follows:

Name: The key name. The name MUST conform to the definition in Section 4. The IANA registry MUST NOT register names that begin with "temp-", so these names can be used freely by any implementer.

Value Type: The type of the value to be used in the key.

Description: A description of the registered key.

Specification: The reference specification for the registered element.

The initial content of this registry is provided in Table 1.

Name	Value Type	Specification	Specification
qnamemin	boolean	Indicates whether qnameminimization is enabled or not	[RFCXXXX]
exterr	number	Lists the set of extended DNS errors	[RFCXXXX]
infourl	string	Provides an unstructured resolver information that is used for troubleshooting	[RFCXXXX]

Table 1: Initial RESINFO Registry

8. Acknowledgments

This specification leverages the work that has been documented in [I-D.pp-add-resinfo].

Thanks to Tommy Jensen, Vittorio Bertola, Vinny Parla, Chris Box, Ben Schwartz, Tony Finch, Daniel Kahn Gillmor, Eric Rescorla, and Shashank Jain for the discussion and comments. Thanks to Mark Andrews, Joe Abley, Paul Wouters, Tim Wicinski, and Steffen Nurpmeso for the discussion on the RR formatting rules.

9. References

9.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/ RFC2119, March 1997, <https://www.rfc-editor.org/info/ rfc2119>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26,

RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/info/rfc9156>.

9.2. Informative References

[I-D.ietf-add-ddr] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-10, 5 August 2022, <https://www.ietf.org/archive/id/draft-ietf-add-ddr-10.txt>.

[I-D.ietf-add-dnr] Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-13, 13 August 2022, <https://datatracker.ietf.org/api/v1/doc/document/draft-ietf-add-dnr/>.

[I-D.pp-add-resinfo] Sood, P. and P. Hoffman, "DNS Resolver Information Self-publication", Work in Progress, Internet-Draft, draft-pp-add-resinfo-02, 30 June 2020, <https://www.ietf.org/archive/id/draft-pp-add-resinfo-02.txt>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RRTYPE]
                IANA, "Resource Record (RR) TYPEs", <http://www.iana.org/
                assignments/dns-parameters/dns-parameters.xhtml#dns-
                parameters-4>.

Authors' Addresses

   Tirumaleswar Reddy
   Nokia
   India

   Email: kondtir@gmail.com

   Mohamed Boucadair
   Orange
   35000 Rennes
   France

   Email: mohamed.boucadair@orange.com