DNSOP Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 5, 2019

R. Bellis
A. Clegg
ISC

March 04, 2019

DNS EDNS Tags
draft-bellis-dnsop-edns-tags-00

Abstract

This document describes EDNS Tags, a mechanism by which DNS clients and servers can transmit an opaque data field which has no defined semantic meaning other than as previously agreed between the client and server.

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 September 5, 2019.

Copyright Notice

Table of Contents

1. Introduction

This document describes EDNS Tags, a mechanism by which DNS clients and servers [RFC1034] can transmit an opaque data field which has no defined semantic meaning other than as previously agreed between the client and server operators.

The tag is a single 16 bit field stored within the RDATA of an EDNS(0) OPT RR as described in [RFC6891].

Two EDNS options are defined to allow for the detection of servers that incorrectly echo responses verbatim. The EDNS-Client-Tag option may only appear in client requests, and the EDNS-Server-Tag may only appear in responses from servers.

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.

3. Description

The values of the individual bits within a tag are not defined to have any semantic meaning in this specification. Their interpretation is defined entirely by bi-lateral agreement between client and server operators. The definitions for EDNS-Client-Tag and EDNS-Server-Tag values MAY be different.

Operators are free to partition the bits within that field as they see fit; for example it could be used to transmit up to 16 separate boolean flags, or perhaps to transmit a 10 bit numeric value combined a 2 bit value and four boolean flags.

Possible use cases for EDNS-Client-Tags include:

- client-controlled selection of a DNS-based security filter
- marking a packet passing through a proxy with transport-related information

Use cases for EDNS-Server-Tags are still to be determined. The option is specified here for symmetry and in anticipation of new use cases being discovered.

3.1. Packet Validation Rules

The OPT RR in a DNS request packet (QR = 0) MUST NOT contain an EDNS-Server-Tag option. A request packet MUST NOT contain more than one EDNS-Client-Tag option.

The OPT RR in a DNS response packet (QR = 1) MUST NOT contain an EDNS-Client-Tag option. A response packet MUST NOT contain more than one EDNS-Server-Tag option.

An EDNS-Server-Tag option MUST NOT be sent unless the corresponding client query contained an EDNS-Client-Tag option.

3.2. Error Handling

Clients MUST discard any response packet that breaches any applicable packet validation rule.

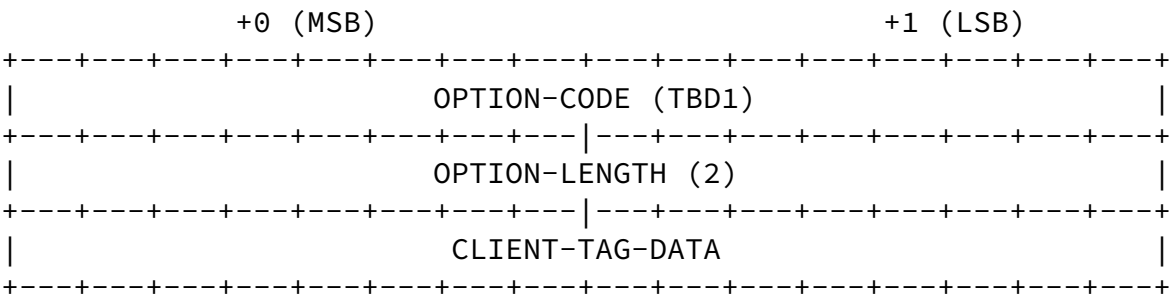
Servers MUST respond with a FORMERR in accordance with Section 7 of [RFC6891] on receipt of a request that breaches any applicable packet

validation rule.

3.3. Wire Format

The format of the EDNS options are as follows, to be stored within the RDATA of an OPT RR as specified in [RFC6891]:

3.3.1. EDNS-Client-Tag

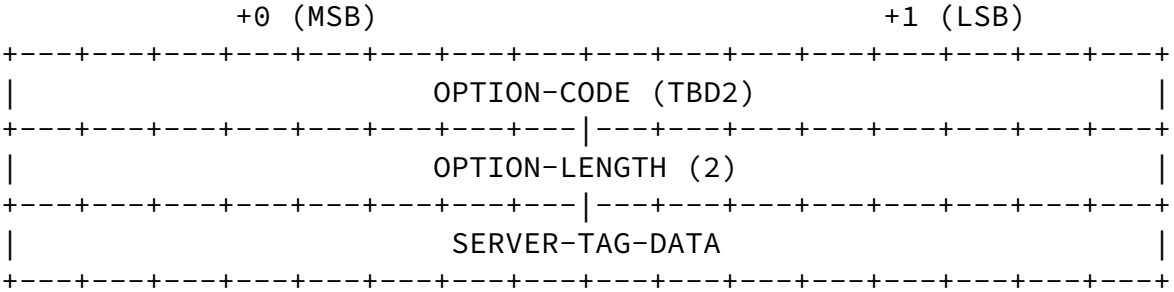


OPTION-CODE: The option code identifier (TBD1).

OPTION-LENGTH: Size (in octets) of OPTION-DATA. MUST be 2.

CLIENT-TAG-DATA: The tag field sent from client to server.

3.3.2. EDNS-Server-Tag



OPTION-CODE: The option code identifier (TBD2).

OPTION-LENGTH: Size (in octets) of OPTION-DATA. MUST be 2.

SERVER-TAG-DATA: The tag field sent from server to client.

4. Security Considerations

Client tags are under the control of the client software and as such (and in the absence of any other mechanism to authenticate the client's identity) this mechanism is not appropriate for applications where the DNS server operator wishes to contractually differentiate service based on the presence (or absence) of any particular tag.

5. Implementation status

TBC.

6. Privacy Considerations

Tags are opaque fields that encode only a limited amount of information. The size of the data field in this specification is chosen to offer a compromise between offering sufficient content to be technically useful while also limiting the scope for it to be used to transmit Personally Identifiable Information.

7. IANA Considerations

IANA has assigned the following EDNS(0) Option Codes:

Value	Name	Status	Reference
TBD1	EDNS-Client-Tag	Standard	RFCXXXX
TBD2	EDNS-Server-Tag	Standard	RFCXXXX

<< Note to IANA - please assign an even value to TBD1, and the next consecutive odd value to TBD2. This allows the least-significant bit of the option value to be compared against the packet's QR bit >>

8. Acknowledgements

The authors wish to particularly thank Brian Conry, Peter van Dijk and Matthijs Mekking for early review and feedback on this document.

9. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[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>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[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>.

Authors' Addresses

Ray Bellis
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City CA 94063
USA

Phone: +1 650 423 1200
Email: ray@isc.org

Alan Clegg
Internet Systems Consortium, Inc.
950 Charter Street

Redwood City CA 94063
USA

Phone: +1 650 423 1200
Email: aclegg@isc.org