Connection Close Signalling for DNS
draft-bellis-dnsop-connection-close-00

Abstract

   This document updates [RFC6891] by specifying a new single-bit flag
   in a DNS response that when seen in a packet carried over a
   connection-orientated transport protocol indicates to the client that
   it should close the current connection.

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 April 27, 2015.

Table of Contents

## 1.  Introduction

   The DNS protocol [RFC1035] supports use of persistent TCP
   connections, although guidance as to when a connection should be
   terminated (and by which party) is limited [RFC5966].

   This document updates the Extension Mechanisms for DNS (EDNS(0))
   [RFC6891] by specifying a new single-bit flag in a DNS response that
   when seen in a packet carried over a connection-orientated transport
   protocol indicates to the client that it should close the current
   connection.

   Having the client close the connection reduces the amount of TCP
   state information that must be stored by the server compared to that
   resulting from the server initiating a unilateral close itself.

   TODO: does it make sense to specify a request side meaning for this
   flag, indicating that the server may half-close its "read" side of
   the connection?  This would make the semantics even closer to those
   of the HTTP/1.1 "Connection: close" header (see Section 14.10 of
   [RFC2616])

## 2.  Terminology

   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 [RFC2119].

## [3](). Specification

The "Connection Close" (CC) bit is held in the third-most signifiant bit of the third byte of the "extended RCODE and flags" portion of an EDNS(0) OPT meta-RR:

```
                +0 (MSB)                +1 (LSB)
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
   0: |    EXTENDED-RCODE    |        VERSION        |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
   2: |DO| Z|CC|                  Z                  |
      +--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Note to RFC editor: replace the first 'Z' in the figure above with 'TO' if draft-hzhwm-dprive-start-tls-for-dns is published as an RFC before this specification.

## [4](). Connection Handling

## [4.1](). Servers

Servers MAY set this flag to indicate that further queries received over the current connection should not be sent.

An incompatible client will not understand this flag and may continue sending requests and therefore the server MUST NOT refuse to service subsequent requests.  The server MAY unilaterally close idle connections regardless, per [RFC5966] and Section 4.2.2 of [RFC1035]

Since this flag requires EDNS(0) support, note that this flag cannot be set unless the client has indicated support for EDNS(0) by sending an OPT meta-RR itself, per Section 7 of [RFC6891]

TODO: note - the constraint in RFC 6891 appears unnecessarily strict - it appears to mandate that the EDNS(0) support indication is on a per-request basis, but it would be reasonable on a connection-orientated transport to assume that ANY preceding request on that connection with an OPT RR is sufficient to indicate that the client supports EDNS(0).

TODO: if a request-side semantic is defined for this flag, what are the TCP state-maintenance implications if the server performs a 'shutdown(fd, SHUT_RD)'?

## 4.2.  Clients

Clients receiving a packet with this flag set MUST NOT send any
further queries over the current connection and MUST initiate closure
of that connection.

TODO: what are the TCP state-maintenance implications if the client
performs a 'shutdown(fd, SHUT_WR)'?

## 5.  Security Considerations

None identified (yet).

## 6.  IANA Considerations

IANA are requested to update the EDNS Header Flag Registry according
to Section 3.

Note to IANA and RFC Editor: The actual bit assigned will depend on
whether any other document specifies a used for the above-specified
bit in advance of publication of this document as an RFC.

## 7.  References

### 7.1.  Normative References

[RFC1035]   Mockapetris, P., "Domain names - implementation and
            specification", STD 13, RFC 1035, November 1987.

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5966]   Bellis, R., "DNS Transport over TCP - Implementation
            Requirements", RFC 5966, August 2010.

[RFC6891]   Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms
            for DNS (EDNS(0))", STD 75, RFC 6891, April 2013.

### 7.2.  Informative References

[RFC2616]   Fielding, R., Gettys, J., Mogul, J., Frystyk, H.,
            Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext
            Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

**Appendix A**.  **Change Log**

   Note to RFC editor: remove this section before publication.

   draft-bellis-dnsop-connection-close-00

      Initial draft

Author's Address

   Ray Bellis
   Nominet UK
   Minerva House
   Edmund Halley Road
   Oxford Science Park
   Oxford  OX4 4DQ
   United Kingdom

   Phone: +44 1865 332211
   Email: ray.bellis@nominet.org.uk
   URI:   http://www.nominet.org.uk/