DNS over TCP
A Rudimentary Textual Analysis

John Kristoff
jtk@cymru.com

DNS over TCP queries...

a) SHOULD (or MUST) NOT be filtered

b) MAY (or MUST) be filtered

IETF RFC 1033 (November 1987)
DOMAIN ADMINISTRATORS OPERATIONS GUIDE

No applicable mention of transport protocol requirements.

IETF RFC 1034 (November 1987)
DOMAIN NAMES – CONCEPTS AND FACILITIES

3.7 Queries

"In the Internet, queries **are** carried in UDP datagrams or over TCP connections."

IETF RFC 1035 (November 1987)

DOMAIN NAMES – IMPLEMENTATION AND SPECIFICATION

4.2 Transport

"While virtual circuits **can be** used for any DNS activity, datagrams are preferred for queries due to their lower overhead and better performance."

IETF RFC 1123 (October 1989)

Requirements for Internet Hosts -- Application and Support

6.1.3.2 Transport Protocols

"DNS resolvers and recursive servers MUST support UDP, and **SHOULD** support TCP, for sending (non-zone-transfer) queries. […] A name server MAY limit the resources it devotes to TCP queries, but it **SHOULD NOT** refuse to service a TCP query just because it would have succeeded with UDP."

IETF RFC 1536 (October 1993)

note: category = informational

Common DNS Implementation Errors and Suggested Fixes

1. Fast Retransmissions

"DNS implements the classic request-response scheme of client-server interaction. **UDP is**, therefore, the chosen protocol for communication though TCP is used for zone transfers."

IETF RFC 2136 (April 1997)

Dynamic Updates in the Domain Name System (DNS UPDATE)

2.1 – Transport Issues

"An update transaction **may be** carried in a UDP datagram, if the request fits, or in a TCP connection (at the discretion of the requestor)."

7.8

"It is possible for a UDP response to be lost in transit and for a request to be retried due to a timeout condition. […] For this reason,requestors who require an accurate response code **must** use TCP."

IETF RFC 2181 (July 1997)
Clarifications to the DNS Specification

9. The TC (truncated) header bit

"When a DNS client receives a reply with TC set, it **should** ignore that response, and query again, using a mechanism, such as a TCP connection, that will permit larger replies."

IETF RFC 2541 (March 1999)
DNS Security Operational Considerations

4. Public/Private Key Size Considerations

"[...] larger keys increase the size of the KEY and SIG RRs. This increases the chance of DNS UDP packet overflow and the **possible necessity** for using higher overhead TCP in responses."

note: ultimately obsoleted by two later RFCs, neither of which mention TCP

IETF RFC 2671 (August 1999)
Extension Mechanisms for DNS (EDNS0)

4.5.4

Somewhat out of context, but note the underlying capability provided that suggests larger UDP messages using EDNS0

“[...] is considered **preferrable** to the outright use of TCP for oversized requests, if there is any reason to suspect that the responder implements EDNS, and if a request will not fit in the default 512 payload size limit.)”

IETF RFC 2870 (June 2000)
Root Name Server Operational Requirements

No applicable mention of transport protocol requirements.

IETF RFC 4033 (March 2005)
DNS Security Introduction and Requirements

9. Name Server Considerations

“Because inclusion of these DNSSEC RRs could easily cause UDP message truncation and fallback to TCP, a security-aware name server **must also** support the EDNS "sender's UDP payload" mechanism.”

IETF RFC 4697 (October 2006)
Observed DNS Resolution Misbehavior

No applicable mention of transport protocol requirements.

IETF RFC 5358 (October 2008)

Preventing Use of Recursive Nameservers in Reflector Attacks

No applicable mention of transport protocol requirements.

IETF RFC 5966 (August 2010)
DNS Transport over TCP – Implementation Requirements

1. Introduction

"Whilst **this document makes no specific recommendations to operators** of DNS servers, it should be noted that failure to support TCP (or the blocking of DNS over TCP at the network layer) may result in resolution failure and/or application-level timeouts"

IETF I-D (in RFC Editor queue)

Child to Parent Synchronization in DNS

3.1. Processing Procedure

"To ensure a single host is being addressed, DNS over TCP **SHOULD** be used to avoid conversing with multiple nodes at an anycast address."

Work in Progress

- draft-ietf-dnsop-edns-tcp-keepalive
- draft-ietf-dnsop-edns-tcp-chain-query
- draft-ietf-dnsop-dnssec-roadblock-avoidance
- T-DNS: TCP and TLS for DNS

Are Operators in Agreement with DNS over TCP?

- ISC KB #AA-01219 seems to conflate implementation with operational requirements

  "DNS queries using TCP (best current practice for many years, and now clarified and asserted in RFC 5966 [...]"

- In Geoff Huston's "A Question of DNS Protocols"

  "This data appears to point to a level of failure to followup from a truncated UDP response to a TCP connection of some 2.6% of clients."

- "[...] if someone said that DNS absolutely required TCP/53 for simple client resolutions that I disagreed with it."

- "I want to get rid of all my UDP"

Is there any DNS over TCP?

- Some, but proportionally it is a very small amount
- When is it used?
  - Larger answers due to TC=1 switchover
  - Sometimes TC=1 switchover for DDoS mitigation
  - Very rarely initiated by the client

Is there a DNS over TCP danger?

- TCP-based resource consumption attacks
  - May be a preferable challenge than UDP DDoS
- Zone transfer threat probably blown out of proportion
- There is also a danger if you don't allow it
  - Some names just won't resolve
  - Stuck TCP state on resolvers trying filtered authoritative servers (reverse resource exhaustion) – see NANOG 32 talk “DNS Anomalies and Their Impacts on DNS Cache Servers”

A DNS over TCP Operational Requirements document...

a) SHOULD (or MUST) be written

b) SHOULD (or MUST) NOT be written

Thank you

- John Kristoff
- <jtk@cymru.com> - https://www.cymru.com/jtk/