DNS Transport over TCP Operational Requirements

draft-kristoff-dnsop-dns-tcp-requirements-02

John Kristoff, DePaul University

Primary Objective

Encourage ops to allow DNS over TCP

Motivation

- Students and new ops often hear things like this:

  "[…] unless you needed zone transfer or long responses, [TCP] was not needed [...]"

  "[…] unless you trust the DNS admin to properly harden the service, you are better off filtering TCP/53 for inbound from the Internet"

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

- Current IETF RFC set can't dispel these positions

Outline of this current IETF I-D

- A historic textual analysis that led to this dilemma
- The proposed operational requirements changes
- Network and system considerations on TCP usage
- Risks and consequences of filtering DNS over TCP
- Summary of IETF RFCs related to DNS over TCP

Some feedback thus far

- Strong support for this doc at NANOG63 DNS BoF
- Wasn't IETF RFC 7766 (implementation) sufficient?
- Strengthen the requirements section
- Provide op guidance for robust DNS over TCP service
- Add history of early DNS over TCP implementations
- Add summary of IETF RFCs related to DNS over TCP

Questions for the dnsop wg

- Can we use MUST or MUST NOT on op practices?
- Can you help with implementation history?
- Any op experience or measurement data to share?
- Is this effort worth pursuing?