DELEG Working Group
Internet-Draft
Intended status: Informational
Expires: 8 October 2025

D. Lawrence
Salesforce
E. Lewis

J. Reid

T. Wicinski
Cox Communications
6 April 2025

Problem Statement and Requirements for an Improved DNS Delegation Mechanism abbrev: DNS DELEG Requirements draft-ietf-deleg-requirements-03

Abstract

Authoritative control of parts of the Domain Name System namespace are indicated with a special record type, the NS record, that can only indicate the name of the server which a client resolver should contact for more information. Any other features of that server must then be discovered through other mechanisms. This draft considers the limitations of the current system, benefits that could be gained by changing it, and what requirements constrain an updated design.

Table of Contents

1. Introduction

In the Domain Name System [STD13], subtrees within the domain name hierarchy are indicated by delegations to servers which are authoritative for their portion of the namespace. The DNS records that do this, called NS records, can only represent the name of a nameserver. In practice, clients can expect nothing out of this delegated server other than that it will answer DNS requests on UDP port 53.

As the DNS has evolved over the past four decades, this has proven to be a barrier for the efficient introduction of new DNS technology, particularly for interacting with servers other than via UDP or TCP on port 53. Many features that have been conceived come with additional overhead as they are limited by this least common denominator of nameserver functionality.

Various mechanisms have been proposed for communicating additional information about authoritative nameservers. This document investigates problems that could be addressed with a new delegation mechanism and the factors that need to be considered in the design of a solution.

2. Terminology

This document assumes familiarity with DNS terms as defined in [BCP219]. Additionally, the following new terms are introduced:

DELEG: A new method of DNS delegation, matching the requirements in this document but not presuming any particular mechanism, including previous specific proposals that used this name

zone operator: The person or organization responsible for the nameserver which serves the zone

3. Requirements Framework

The requirements constraining any proposed changes to DNS delegations fall broadly into two categories.

"Hard requirements" are those that must be followed by a successful protocol [RFC5218], because violating them would present too much of an obstacle for broad adoption. These will primarily be related to the way the existing Domain Name System functions at all levels.

"Soft requirements" are those that are desirable, but the absence of which does not intrinsically eliminate a design. These will largely be descriptive of the problems that are trying to be addressed with a new method, or features that would ease adoption.

The context used here will be for the Domain Name System as it exists under the IANA root and the Registry/Registrar/Registrant model [BCP219], and some conditions will only be relevant there. While it is expected that any design which satisfies the requirements of put forth here would be broadly applicable for any uses of the DNS outside of this environment, such uses are not in scope.

3.1. Hard Requirements

The following strictures are necessary in a new delegation design.

* H1. DELEG must not disrupt the existing registration model of domains.

* H2. DELEG must be backwards compatible with the existing ecosystem. Legacy zone data must function identically with both DELEG-aware and DELEG-unaware software. Nameserver (NS) records will continue to define the delegation of authority between a parent zone and a child zone exactly as they have.

* H3. DELEG must not negatively impact most DNS software. This is intentionally a bit vague with regard to "most", because it can't be absolutely guaranteed for all possible DNS software on the network. However, the DNS community should strive to test any proposed mechanism against a wide range of legacy software and come to a consensus as to what constitutes adherence to this requirement.

* H4. DELEG must be able to secure delegations with DNSSEC.

* H5. DELEG must support updates to delegation information with the same relative ease as currently exists with NS records. Changes should take the same amount of time (eg, controlled by a DNS TTL) and allow a smooth transition between different operational platforms.

* H6. DELEG must be incrementally deployable and not require any sort of flag day of universal change.

* H7. DELEG must allow multiple independent operators to simultaneously serve a zone.

3.2. Soft Requirements

The following items are the aspirational goals for this work, describing the features that are desired beyond what current NS-based delegations provide.

* S1. DELEG should facilitate the use of new DNS transport mechanisms, including those already defined by DNS-over-TLS (DoT [RFC7858]), DNS-over-HTTPS (DoH [RFC8484]), and DNS-over-QUIC (DoQ [RFC9520]). It should easily allow the adoption of new transport mechanisms.

* S2. DELEG should make clear all of the necessary details for contacting a service -- its protocol, port, and any other data that would be required to initiate a DNS query.

* S3. DELEG should minimize transaction cost in its usage. This includes, but is not limited to, packet count, packet volume, and the amount of time it takes to resolve a query.

* S4. DELEG should simplify management of a zone's DNS service.

* S5. DELEG should allow for backward compatibility to the conventional NS-based delegation mechanism. That is, a zone operator who wants to maintain a single source of truth of delegation information using DELEG should be able to easily have Do53 delegations derived from it.

* S6. DELEG should be extensible and allow for the easy incremental addition of new delegation features after initial deployment.

* S7. DELEG should be able to convey a security model for delegations stronger than currently exists with DNSSEC.

3.3. Non-Requirements

Several potential areas of requirement have been raised that are being explicitly acknowledged here as not being in the scope of this higher level document.

* Whether NS records must continue to be the primary means by which resolutions happen.

* Whether information for a new delegation mechanism is stored in at the zone name or elsewhere in the domain name hierarchy.

* If a new delegation protocol is based on a DNS resource record, that record must not appear in both the parent and child with the same name and type. The protocol should clearly describe how to handle an occurrence of that record appearing in the child.

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

Updating the means by which DNS delegation information is communicated has tremendous implications for the security of the Internet. There will security considerations that accompany proposed solutions. This section will be made more robust in future drafts. Contributions welcome.

6. Informative References

[STD13] Internet Standard 13,
<https://www.rfc-editor.org/info/std13>.
At the time of writing, this STD comprises the following:

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

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

[BCP219] Best Current Practice 219, <https://www.rfc-editor.org/info/bcp219>. At the time of writing, this BCP comprises the following:

Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

[RFC5218] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <https://www.rfc-editor.org/rfc/rfc5218>.

[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/rfc/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/rfc/rfc8484>.

[RFC9520] Wessels, D., Carroll, W., and M. Thomas, "Negative Caching of DNS Resolution Failures", RFC 9520, DOI 10.17487/RFC9520, December 2023, <https://www.rfc-editor.org/rfc/rfc9520>.

Acknowledgements

Authors' Addresses

David Lawrence
Salesforce
Email: tale@dd.org

Ed Lewis
Email: eppdnsprotocols@gmail.com

Jim Reid

Email: jim@rfc1035.com

Tim Wicinski
Cox Communications
Email: tjw.ietf@gmail.com