Public Annotations of DNS RFCs

Paul Hoffman

DNS-OARC 40

February 2023

Motivation for the RFC Annotations project

- DNS developers, protocol developers, and security researchers read the DNS RFCs for many reasons
- When you read about a protocol in an RFC, you want to know about that protocol in the real world
  - Has it been updated?
  - Were there errors?
  - What design decisions were weighed?
  - Have there been academic papers about this?

Design of the project

- List every DNS-related RFC we could think of
  - This is *not* an official list
- Show the RFCs **as-is** with annotations **to the side** in the appropriate places
- Start with annotations like “updated by” that shows which part of an RFC was updated
- Let others in the DNS technical community contribute annotations
- Make it easily extensible

Project home

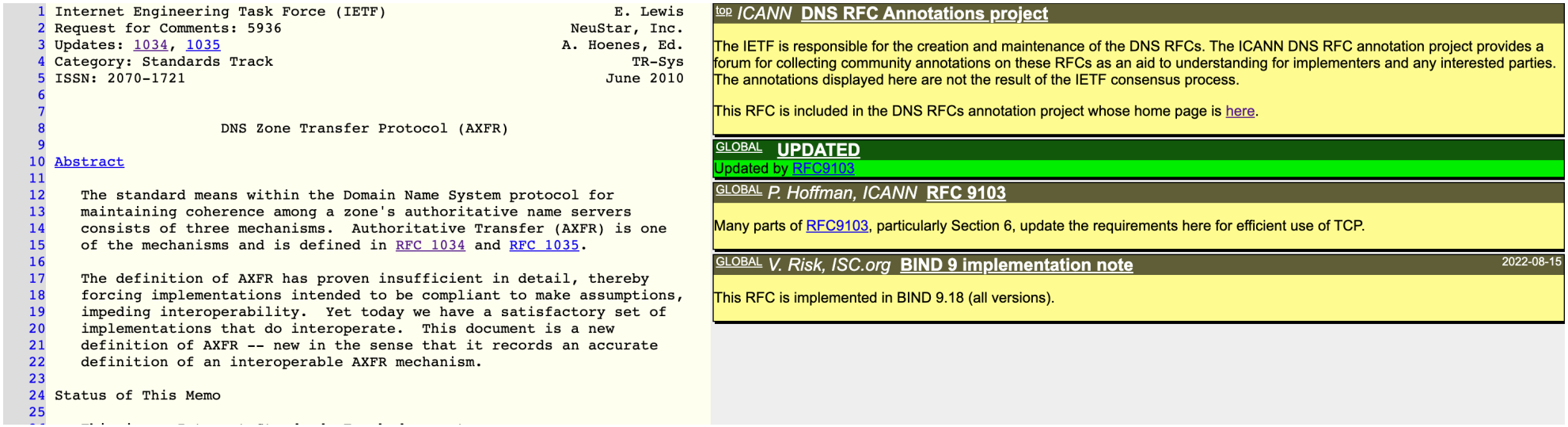
- https://rfc-annotations.research.icann.org/

Basic DNS RFCs

RFC	Title
1034	Domain names - concepts and facilities
1035	Domain names - implementation and specification
1123	Requirements for Internet Hosts - Application and Support
1536	Common DNS Implementation Errors and Suggested Fixes
1912	Common DNS Operational and Configuration Errors
1982	Serial Number Arithmetic
1995	Incremental Zone Transfer in DNS

Annotated RFCs

- RFC 5936



```
Internet Engineering Task Force (IETF)                          E. Lewis
Request for Comments: 5936                                   NeuStar, Inc.
Updates: 1034, 1035                                        A. Hoenes, Ed.
Category: Standards Track                                          TR-Sys
ISSN: 2070-1721                                                June 2010


                    DNS Zone Transfer Protocol (AXFR)

Abstract

   The standard means within the Domain Name System protocol for
   maintaining coherence among a zone's authoritative name servers
   consists of three mechanisms.  Authoritative Transfer (AXFR) is one
   of the mechanisms and is defined in RFC 1034 and RFC 1035.

   The definition of AXFR has proven insufficient in detail, thereby
   forcing implementations intended to be compliant to make assumptions,
   impeding interoperability.  Yet today we have a satisfactory set of
   implementations that do interoperate.  This document is a new
   definition of AXFR -- new in the sense that it records an accurate
   definition of an interoperable AXFR mechanism.

Status of This Memo
```

top *ICANN* **DNS RFC Annotations project**

The IETF is responsible for the creation and maintenance of the DNS RFCs. The ICANN DNS RFC annotation project provides a forum for collecting community annotations on these RFCs as an aid to understanding for implementers and any interested parties. The annotations displayed here are not the result of the IETF consensus process.

This RFC is included in the DNS RFCs annotation project whose home page is here.

GLOBAL **UPDATED**

Updated by RFC9103

GLOBAL *P. Hoffman, ICANN* **RFC 9103**

Many parts of RFC9103, particularly Section 6, update the requirements here for efficient use of TCP.

GLOBAL *V. Risk, ISC.org* **BIND 9 implementation note** 2022-08-15

This RFC is implemented in BIND 9.18 (all versions).

Annotations at the top of an RFC

- RFC 4035

GLOBAL **UPDATED**

Updated by RFC4470, RFC6014, RFC6840, RFC8198, RFC9077

GLOBAL **HAS ERRATA**

Has errata: #3044, #5226

GLOBAL *P. Hoffman, ICANN* **RFC 6014 doesn't seem to update RFC 4035**

RFC6014 says that it updates RFC 4035, and talks about RFC 4035 in a few places, but doesn't seem to update any of the material in RFC 4035.

GLOBAL *P. Hoffman, ICANN* **Updates from RFC 6840**

RFC6840, "Clarifications and Implementation Notes for DNSSEC", updates RFC 4035 in many places throughout the document.

GLOBAL *V. Risk, ISC.org* **BIND 9 implementation note** 2022-08-15

This RFC is implemented in BIND 9.18 (all versions).

Annotations appear in-line

- In the middle of RFC 4035

970
971 3.2.3. The AD Bit
972
973   The name server side of a security-aware recursive name server MUST
974   NOT set the AD bit in a response unless the name server considers all
975   RRsets in the Answer and Authority sections of the response to be
976   authentic. The name server side SHOULD set the AD bit if and only if
977   the resolver side considers all RRsets in the Answer section and any
978   relevant negative response RRs in the Authority section to be
979   authentic. The resolver side MUST follow the procedure described in
980   Section 5 to determine whether the RRs in question are authentic.
981   However, for backward compatibility, a recursive name server MAY set
982   the AD bit when a response includes unsigned CNAME RRs if those CNAME

section-3.2.3 *P. Hoffman, ICANN* **RFC 6840 defines the semantics of the AD bit**

Section 5.8 of RFC6840 says:

Section 3.2.3 of [RFC4035] describes under which conditions a validating resolver should set or clear the AD bit in a response. In order to interoperate with legacy stub resolvers and middleboxes that neither understand nor ignore the AD bit, validating resolvers SHOULD only set the AD bit when a response both meets the conditions listed in Section 3.2.3 of [RFC4035], and the request contained either a set DO bit or a set AD bit.

Additional useful annotations

- Pointers to academic papers
- Implementation notes (“we realized the text here was fuzzy, but the example below cleared it up”)
- Design choices that were made
- Who has implemented optional parts of a protocol
- ...and probably a lot of other things

Questions

- Volunteers to annotate
- Please look!
  - https://rfc-annotations.research.icann.org/
- And comment!
  - https://github.com/icann/rfc-annotations