Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: June 1, 2015

P. Hoffman
VPN Consortium
A. Sullivan
Dyn
K. Fujiwara
JPRS

November 28, 2014

DNS Terminology
draft-hoffman-dns-terminology-00

Abstract

The DNS is defined in literally dozens of different RFCs. The terminology used in by implementers and developers of DNS protocols, and by operators of DNS systems, has sometimes changed in the decades since the DNS was first defined. This document gives current definitions for many of the terms used in the DNS in a single document.

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 June 1, 2015.

Copyright Notice

Table of Contents

1. Introduction

The DNS is a simple query-response protocol whose messages in both directions have the same format. The protocol and message format are defined in [RFC1034] and [RFC1035]. These RFCs defined some terms, but later documents defined others. Some of the terms from RFCs 1034 and 1035 now have somewhat different meanings than they did in 1987.

This document collects a wide variety of DNS-related terms. Some of them have been precisely defined in earlier RFCs, some have been loosely defined in earlier RFCs, and some are not defined in any earlier RFC at all.

The definitions here are believed to be the consensus definition of the DNS community, both protocol developers and operators. Some of the definitions differ from earlier RFCs, and those differences are noted. The terms are organized loosely by topic. Some definitions are for new terms for things that are commonly talked about in the DNS community but that never had terms defined for them.

In this document, where the consensus definition is the same as the one in an RFC, that RFC is quoted. Where the consensus definition has changed somewhat, the RFC is mentioned but the new stand-alone definition is given.

Note that capitalization in DNS terms is often inconsistent between RFCs and between DNS practitioners. The capitalization used in this

document is a best guess at current practices, and is not meant to indicate that other capitalization styles are wrong or archaic.

(Note: the formatting of this early draft is a bit funky. It will improve in later drafts. Bikeshedding the format, as compared to the content, of this draft is probably premature.)

2. DNS Message Format

Header -- The first 12 octets of a DNS message. Many of the fields and flags in the header diagram in section 4.1.1 of RFC 1035 are referred to by their names in that diagram. For example, the response codes are called "RCODEs", and the authoritative answer bit is often called "the AA flag" or "the AA bit".

Some of response codes that are defined in RFC 1035 have gotten their own shorthand names. Some common ones are:

FORMERR -- A response message whose header has an RCODE of 1

SERVFAIL -- A response message whose header has an RCODE of 2

NXDOMAIN -- A response message whose header has an RCODE of 3. NXDOMAIN is defined as an official synonym for Name Error in RFC 2308, section 1.

TTL -- The "time to live" of a resource record. A TTL value is an unsigned number, with a minimum value of 0, and a maximum value of 2147483647. That is, a maximum of 2^31 - 1. When transmitted, the TTL is encoded in the less significant 31 bits of the 32 bit TTL field, with the most significant, or sign, bit set to zero. (Quoted from [RFC2181], section 8) (Note that RFC 1035 erroneously stated that this is a signed integer; it is fixed in an erratum.)

The TTL "specifies the time interval that the resource record may be cached before the source of the information should again be consulted". (Quoted from RFC 1035, section 3.2.1) Also: "the time interval (in seconds) that the resource record may be cached before it should be discarded". (Quoted from RFC 1035, section 4.1.3). Despite being defined for a resource record, the TTL of every resource record in an RRset is required to be the same (RFC2181, section 5.2).

Glue records -- Resource records which are not part of the authoritative data, and are address resource records for the servers listed in the message. They contain data that allows access to name servers for subzones. (Definition from RFC 1034, section 4.2.1)

Referrals -- Data from the authority section of a non-authoritative answer. RFC 1035 section 2.1 defines "authoritative" data. However, referrals at zone cuts are not authoritative. Referrals may be a zone cut NS resource records and their glue. NS records on the parent side of a zone cut are an authoritative delegation, but are not treated as authoritative data by the client. [[A more complete and precise definition will be needed here.]]

3. Resource Records

RR -- A short form for resource record. (RFC 1034, section 3.6.)

RRset -- A set of resource records with the same label, class and type, but with different data. (Definition from RFC 2181). Also spelled RRSet in some documents.

OPT -- A pseudo-RR (sometimes called a meta-RR) that is used only to contain control information pertaining to the question-and-answer sequence of a specific transaction. contains control information pertaining to the question-and-answer sequence of a specific transaction. (Definition from [RFC6891], section 6.1.1)

Owner -- The domain name where a RR is found (RFC 1034, section 3.6). Often appears in the term "owner name".

4. DNS Servers

This section defines the terms used for the systems that act as DNS clients, DNS servers, or both. Some terms about servers describe servers that do and do not use DNSSEC; see Section 6 for those definitions.

Resolver -- Programs that interface user programs to domain name servers. (Quoted from RFC 1034, section 5.1) A resolver performs queries for a name, type, and class, and receives answers. The logical function is called "resolution". In practice, the term is usually referring to some specific type of resolver (some of which are defined below), and understanding the use of the term depends on understanding the context.

Stub resolver -- A resolver that cannot perform all resolution itself. Stub resolvers generally depend on a recursive resolver to undertake the actual resolution function. Stub resolvers are discussed but never fully defined in RFC 1034, section 5.3.1.

Iterative resolver -- A system that receives DNS queries and responds with a referral to another server. RFC 1034 (section 2.3) describes

this as, "The server refers the client to another server and lets the client pursue the query."

Recursive resolver -- A system that receives DNS queries and either responds to those queries from a local cache or sends queries to authoritative servers in order to get the final answers to the original queries. RFC 1034 (section 2.3) describes this as, "The first server pursues the query for the client at another server." Recursive resolvers may be thought of as having a name server side (which is what answers the query) and a resolver side (which performs the resolution function). A recursive resolver is responsible for resolving domain names for clients by following the domain's delegation chain, starting at the DNS root. These systems are also commonly called "recursive servers".

Authoritative server -- A system that responds to DNS queries with information about zones for which it has been configured to answer with the AA flag in the response header set to 1. It is a server that has authority over one or more DNS zones. Note that it is possible for an authoritative server to respond to a query without the parent zone delegating authority to that server.

DNS forwarder -- A system receives a DNS query, possibly changes the query, sends the resulting query to a recursive resolver, receives the response from a resolver, possibly changes the response, and sends the resulting response to the stub resolver. Section 1 of [RFC2308] describes a forwarder as "a nameserver used to resolve queries instead of directly using the authoritative nameserver chain". [RFC5625] does not give a specific definition for DNS forwarder, but describes in detail what features they need to support. The protocol interfaces for DNS forwarders are exactly the same as those for recursive resolvers (for interactions with DNS stubs) and as those for stub resolvers (for interactions with recursive resolvers).

Full resolver -- This term is used in RFC 1035, but it is not defined there. RFC 1123 defines a "full-service resolver" that may or may not be what was intended by "full resolver" in RFC 1035. In the vernacular, a full-service resolver is usually one that would be suitable for use by a stub resolver.

Consensual policy-implementing resolver -- A resolver that changes some answers it returns based on policy criteria, such as to prevent access to malware sites. These policy criteria are agreed to by systems that query this resolver through some out of band mechanism (such as finding out about the resolver from a web site and reading the policy).

Non-consensual policy-implementing resolver -- A resolver that is not a consensual policy-implementing resolver that changes the answers it returns. The difference between this and a consensual policy-implementing resolver is that users of this resolver are not expected to know that there is a policy to change the answers it returns.

5. Zones

This section defines terms that are used when discussing zones that are being served or retrieved.

Zone -- A unit of organization of authoritative data. Zones can be automatically distributed to the name servers which provide redundant service for the data in a zone. (Quoted from RFC 1034, section 2.4).

Child -- The entity on record that has the delegation of the domain from the Parent. (Quoted from [RFC7344], section 1.1)

Parent -- The domain in which the Child is registered. (Quoted from RFC 7344, section 1.1)

Zone cut -- The delimitation point between two zones where the origin of one of the zones is the child of the other zone. (Section 6 of RFC 2181 uses this term extensively, although never actually defines it.)

In-bailiwick response -- A response in which the name server answering is authoritative for an ancestor of the owner name in the response. The term normally is used when discussing the relevancy of glue records. For example, the parent zone example.com might reply with glue records for ns.child.example.com. Because the child.example.com zone is a descendant of the example.com zone, the glue is in-bailiwick.

Out-of-bailiwick response -- A response in which the name server answering is not authoritative for an ancestor of the owner name in the response.

Origin -- 1. The domain name within which a given relative domain name appears. Generally seen in the context of "$ORIGIN", which is a control entry defined in RFC 1035, section 5.1, as part of the master file format. For example, if the $ORIGIN is set to "example.org.", then a master file line for "www" is in fact an entry for "www.example.org.". 2. The domain name that appears at the top of a zone, that is, the owner name of the apex records.

Authoritative data -- RRsets in a DNS response that has the AA bit in the response header set to 1.

Delegation -- The process by which a separate zone is created in the name space beneath a given domain. Delegation happens when an NS RRset is added in the parent zone for the child origin, and a corresponding zone apex is created at the child origin.

Apex -- The SOA and NS RRsets at the origin of a zone. This is also called the "zone apex".

Root zone -- The zone whose origin is the zero-length label. Also sometimes called "the DNS root".

6. DNSSEC

This section will mostly be populated with direct quotes from RFC 4033. For some terms, there will be additional commentary.

[[The four types of validation states]]

[[The many types of DNSSEC-aware and -unaware resolvers and validators]]

NSEC -- [[Definition goes here]]

NSEC3 -- [[Definition goes here]]

7. IANA Considerations

This document has no effect on IANA registries.

8. Security Considerations

These definitions do not change any security considerations for the DNS.

9. Acknowledgements

The authors gratefully acknowledge all of the authors of DNS-related RFCs that proceed this one. [[More acks will go here as people point out new terms to add and changes to the ones we have listed here.]]

10. References

10.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

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

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

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

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating DNSSEC Delegation Trust Maintenance", RFC 7344, September 2014.

10.2. Informative References

[RFC5625] Bellis, R., "DNS Proxy Implementation Guidelines", BCP 152, RFC 5625, August 2009.

Authors' Addresses

Paul Hoffman
VPN Consortium
127 Segre Place
Santa Cruz, CA 95060
USA

Email: paul.hoffman@vpnc.org

Andrew Sullivan
Dyn
150 Dow St, Tower 2
Manchester, NH 1604
USA

Email: asullivan@dyn.com

Kazunori Fujiwara
Japan Registry Services Co., Ltd.
Chiyoda First Bldg. East 13F, 3-8-1 Nishi-Kanda
Chiyoda-ku, Tokyo 101-0065
Japan

Phone: +81 3 5215 8451
Email: fujiwara@jprs.co.jp