dnsop
Internet-Draft
Updates: 1034 (if approved)
Intended status: Standards Track
Expires: January 16, 2019

O. Sury
Internet Systems Consortium

July 15, 2018

CNAME+DNAME Name Redirection
draft-sury-dnsop-cname-plus-dname-00

Abstract

This document updates RFC1034 to allow coexistence of the CNAME Resource Record with DNAME Resource Record at the same owner node, which provides redirection for a sub-tree of the domain name tree in the DNS system, in a parent zone. By allowing this cooexistence, DNS system will have a way how to create a sub-tree redirection together that includes the Resource Records owner name. This would allow parent zones to create full domain aliases.

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 https://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 January 16, 2019.

Table of Contents

1. Introduction

RFC 1034 [RFC1034] defines CNAME resource record for cases when there are multiple names for single host. A CNAME resource record identifies its owner name as an alias, and specifies the corresponding canonical name in the RDATA section of the resource record. If a CNAME resource record is present at a node, no other data MUST be present; this ensures that the data for a canonical name and its aliases cannot be different. This rule also insures that a cached CNAME can be used without checking with an authoritative server for other resource record types.

However there is already existing exceptions to this rule. RFC 4034 [RFC4034] defines exception to RRSIG and NSEC records, which MUST exist for the same name as a CNAME resource record in a signed zone.

RFC 6672 [RFC6672] defines DNAME resource record, which provides redirection for a sub-tree of the domain name tree in the DNS system. That is, all names that end with a particular suffix are redirected to another part of the DNS.

The DNAME RR and the CNAME RR RFC 1034 [RFC1034] cause a lookup to (potentially) return data corresponding to a domain name different from the queried domain name. The difference between the two resource records is that the CNAME RR directs the lookup of data at its owner to another single name, a DNAME RR directs lookups for data

at descendents of its owner's name to corresponding names under a different (single) node of the tree.

1.1. Terminology

All the basic terms used in this specification are defined in the documents RFC 1034 [RFC1034], RFC 1035 [RFC1035], and RFC 6672 [RFC6672].

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Motivation

In some languages, some characters has the variants, which look differently or very similar but are identical in the meaning. For example, Chinese character U+56FD and its variant U+570B look differently, but are identical in the meaning. If Internationalized Domain Label or "IDL" RFC 3743 [RFC3743] are composed of variant characters, we regard this kind of IDL as the IDL variant. If these IDL variants are put into the DNS for resolution, they are expected to be identical in the DNS resolution. More comprehensible example is that we expect color.example.com to be equivalent with the colour.example.com in the DNS resolution. Currently this is something we are unable to achieve without copying the data for the owner of the domain record (ie. for the color.example.com) and keeping it in sync by some external mechanism. The CNAME+DNAME record placed in the parent zone will remove this need for synchronization. Without this bundling mechanism, current mechanisms such as DNAME or CNAME are not enough capable to solve all the problems with the emergence of internationalized domain names. The internationalized domain names may have alias or equivalence of the original one.

The CNAME+DNAME is not limited to internationalized domain names. This bundling could be used by TLD registries to offer additional service for it's registrants. F.e. a hosting company could create generic record for it's service and with simple CNAME+DNAME bundle it can create all needed DNS resource records for providing this service.

There are already such uses of CNAME which violates existing DNS standards by replying with CNAME records in the apex of the zone. This proposal would allow these perpetrators to comply with the DNS standard again.

3. CNAME+DNAME Bundle

This proposal doesn't change wire formats of the existing CNAME and DNAME records. It also doesn't change handling of the CNAME and DNAME on the resolver side.

4. Query processing

Existing rules for a DNAME RR and a CNAME RR are still valid with following exception: The DNAME and CNAME resource records MAY co-exist at the same owner name in the parent zone.

4.1. Processing by Authoritative Servers

The authoritative server implementations MUST allow CNAME record when there is a DNAME record for the same name and vice versa.

TODO: Experiment with returning DNAME together with CNAME.

4.2. Processing by Recursive Servers

The recursive server implementations MUST NOT deny CNAME record when there is a DNAME record already present in the cache for the same name and vice versa.

5. Implementation Report

The author has implemented a change for BIND 9 authoritative server during the IETF Hackathon in Montreal, and the domain with CNAME+DNAME can be tested at www.cname-plus-dname.rocks.

The conducted experiment confirmed that BIND, Unbound and Google Public DNS work fine, Knot Resolver has a bug that makes the DNS answer contain the DNAME records, but with RCODE=SERVFAIL, and PowerDNS returns RCODE=SERVFAIL for any DNAME query. The other public DNS implementations follow the errors of their respective deployed software.

6. Security Considerations

The security is the same as security of the individual CNAME and DNAME records.

7. IANA Considerations

This document makes no requests of IANA.

8. References

8.1. Normative References

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

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, DOI 10.17487/RFC6672, June 2012, <https://www.rfc-editor.org/info/rfc6672>.

8.2. Informative References

[RFC3743] Konishi, K., Huang, K., Qian, H., and Y. Ko, "Joint Engineering Team (JET) Guidelines for Internationalized Domain Names (IDN) Registration and Administration for Chinese, Japanese, and Korean", RFC 3743, DOI 10.17487/RFC3743, April 2004, <https://www.rfc-editor.org/info/rfc3743>.

Author's Address

Ondrej Sury
Internet Systems Consortium
CZ

Email: ondrej@isc.org