DNSext Working Group
Internet-Draft
Updates: 1034 (if approved)
Intended status: Standards Track
Expires: February 19, 2011

O. Sury
CZ.NIC

August 18, 2010

CNAME at the zone apex
draft-sury-dnsext-cname-at-apex-00

Abstract

This document proposes a modification to CNAME record to coexist with SOA and NS records at the zone apex. This proposal will improve aliasing in the DNS system. The users are often forced to manually add duplicate A, AAAA and MX records by copying data from the target zone to the aliased zone. This forces zone owner to keep track of target domain name since the mismatch in the data could cause failures. This administrative burden will be eliminated by allowing CNAME to coexist with NS and SOA resource records.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on February 19, 2011.

Copyright Notice

Table of Contents

1. Introduction

RFC 1033 [RFC1033] 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 are 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 1034 [RFC1034] defines the data that defines the top node of the zone. They are logically part of the authoritative data, the RRs that describe the top node of the zone are especially important to the zone's management. These RRs are of two types: name server RRs that list, one per RR, all of the servers for the zone, and a single SOA RR that describes zone management parameters.

The Start Of Authority (SOA) record designates the start of a zone. It must be present in the zone apex.

The NS (Name Server) record lists the name of a machine the provides domain service for a particular zone. The NS record is placed both in the parent and the child zone and should be same. The NS record(s) are also mandatory in the zone.

1.1. Terminology

All the basic terms used in this specification are defined in the documents RFC 1033 [RFC1033], RFC 1034 [RFC1034].

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

The aliasing in the DNS system is usually done by placing CNAME for each individual record which needs to be aliased. There is one notable exception - the zone apex which has to include the SOA and NS

RRs. Because of that the zone owner is unable to place CNAME record there and this can lead to several failure conditions. Either the data in the apex is copied by hand and new administrative burden is created to keep the data in the sync, or there is no alias in the apex at all.

The aliases zone is prone to several types of errors when the copy method is used. The target domain can change the data and while subdomains (like www.example.net) still works the zone apex A record (example.net) doesn't work. This could go overlooked for some time if the zone owner doesn't do regular checks. Same condition can happen with MX records causing failure to deliver email or it could even lead to malicious use if the bad guys happen to own previous manually copied MX records. Also there could be a semi-failures, f.e. if the target zone adds AAAA record for IPv6, it will not be copied to aliased zone automatically causing IPv6 resolution failures.

3. CNAME at the apex

This proposal defines new rules for the CNAME record. RFC 1033 [RFC1034] defines that:

There must not be any other RRs associated with a nickname of the same class.

This rule is changed with full compliance with DNSSEC RFCs to:

There must not be any other RRs with the same owner as the CNAME RR with the exception of NS, SOA, DNSKEY, RRSIG and NSEC RRs.

4. Query processing

Because of the change of the existing behaviour in the CNAME processing there is a need to add a signaling bit for the queries issued by resolvers understanding CNAME at the zone apex.

4.1. Processing by Authoritative Servers

The authoritative server implementations MUST allow CNAME resource record in the zone apex to coexist with NS, SOA, DNSKEY, RRSIG and NSEC resource records. They MUST NOT allow any other resource record types in the zone apex when the CNAME resource record is placed in the zone apex.

The authoritative server will return an answer containing specific

resource record type when asked for SOA, NS, DNSKEY, RRSIG or NSEC RR type. The authoritative server will return an answer containing the CNAME if any other RR type is requested in the query. If the query contains the CNAME-at-apex signaling bit then the authoritative server will use correct TTL in the zone for the requests in the zone apex. If the query doesn't contain the CNAME-at-apex signaling bit then the authoritative server will override TTL in the zone and will return answer with 0 TTL for all resource requests in the zone. This should prevent the resolvers to store the result in the cache and thus breaking the internal rules for the CNAME.

4.2. Processing by Recursive Servers

The resolver compliant with this proposal will issue a query which has the CNAME-at-apex signaling bit. Such resolver MUST NOT deny CNAME if it already has other resource record in the cache with the same owner with the SOA, NS, DNSKEY, RRSIG or NSEC resource record type. It MUST NOT deny SOA, NS, DNSKEY, RRSIG or NSEC resource records if it already has a CNAME resource record in the cache. The compliant resolver SHOULD NOT deny CNAME in the case it has any other RR type in the cache and it SHOULD NOT deny any other RR types if it already has CNAME records in the cache.

The rules for the authoritative server is same for the compliant resolver acting as an upstream cache.

5. Security Considerations

The author is not aware of any security consideration, but he is aware that this proposal could create problems for the name servers not following the Robustness principle - Be conservative in what you send; be liberal in what you accept.

6. Normative References

[RFC1033] Lottor, M., "Domain administrators operations guide", RFC 1033, November 1987.

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions",

RFC 4034, March 2005.

Author's Address

Ondrej Sury
CZ.NIC
Americka 23
120 00 Praha 2
CZ

Phone: +420 222 745 110
Email: ondrej.sury@nic.cz