CNAME at apex - a website publisher perspective
draft-york-dnsop-cname-at-apex-publisher-view-01

Abstract

There has been a large amount of discussion about the "CNAME at apex" issue within the DNSOP Working Group. This draft provides the perspective of one publisher of multiple websites about why CNAME-like functionality is desirable at the apex of a domain zone.

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 May 10, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Table of Contents

1. Introduction ................................................. 2
2. The Challenge ................................................ 3
   2.1. Note ................................................... 4
3. CNAME works for subdomains ................................. 4
4. CNAME at apex does not work ............................... 4
5. Proprietary solutions ....................................... 4
   5.1. Proprietary lockin ..................................... 4
   5.2. Restriction on using multiple CDNs ..................... 5
6. Existing and proposed solutions ............................ 5
7. Author opinion ................................................ 5
8. Past discussion ............................................... 5
9. Conventions and Definitions ................................. 6
10. Security Considerations .................................... 6
11. IANA Considerations ....................................... 6
12. References .................................................. 6
   12.1. Normative References ................................ 6
   12.2. Informative References ............................... 6
Acknowledgments ................................................... 7
Author’s Address .................................................. 7

1. Introduction

From the early days of the Web, publishers of websites generally operated their main public website using the "www" subdomain, as in "www.example.com".

In recent years many organizations have moved to dropping the "www" and referring to their main website by simply the domain name, as in "example.com". There are numerous reasons for this change, including the simplicity of saying or writing the name and also smaller address bars on mobile browsers. If you are designing a large advertisement to display in, say, an airport hallway, you can make the domain name address larger and more visible if you simply use "example.com" and drop the "www". Additionally, some web browsers are no longer showing the full URL (or even any of the URL) and so the "www" is no longer visible.

Regardless of the reasons, the fact is that many website publishers and marketing/communications teams are moving to using only the domain name without the "www" or other subdomains to reference their public website.

The expectations from the marketing / communications teams are that:

1. users will be able to simply enter "example.com" into their browser; and
2. users will only see "example.com" in their address bar (if URLs are even displayed).

2. The Challenge

If the organization’s website is a simple web server with specific A and AAAA records, this change can be easily implemented by adding the appropriate A and AAAA records at the zone apex.

However, most larger site publishers (and many smaller publishers) now use content distribution networks (CDNs), global load balancers, or some other form of a caching / load balancing network in front of their website. The result is that there is no single "A" or "AAAA" record for the organization’s website.

Publishers use CDNs for a variety of reasons, including:

- **Performance** - connecting users to an edge server with the lowest latency
- **Geo-location** - connecting users to edge servers appropriate for their geography
- **DDoS / security** - using various security mechanisms provided by CDNs
- **IPv6** - using a CDN to offer IPv6 access when the origin server is only on IPv4
- **TLS** - using a CDN to offer higher levels of TLS usage than possible with origin server

While there may be many non-CDN mechanisms to address those reasons, website publishers in 2018 are increasingly using CDNs as a simple business solution.

The DNS issue is that the website publisher is told to simply redirect all traffic to some address within the CDN along the lines of one of these:

- a123qkt5y7xxb3df8.example-cdn.net
- (companyname).example-cdn.net
- (companyname).(location).example-cdn.net
- some-random-string.example-cdn.net
The CDN then performs its service of providing the requesting client with the A or AAAA record most appropriate for the client’s network/geographic location.

2.1. Note

Some CDNs require that they manage the DNS services for the target domain name. The publisher must designate the CDN’s DNS servers as the authoritative name servers (NS records) for the domain. At that point the CDN handles all of the name resolution directly and dynamically returns the A and AAAA records back to the client web browser. The browser has no idea that a CDN is in usage.

However, this document is discussing CDNs where the publisher retains control of serving out DNS records for the domain.

3. CNAME works for subdomains

For websites using a subdomain such as "www", this is simply done in DNS using CNAME and pointing to a target URL provided by the CDN:

```text
www.example.com 300 IN CNAME a123qkt5y7xxb3df8.example-cdn.net
```

Now all web traffic to www.example.com is redirected to the CDN address. The CDN returns the appropriate A and AAAA records. This all works and the browser connects to the site hosted on one of the CDN edge servers.

4. CNAME at apex does not work

For reasons outlined in Appendix C of [I-D.ietf-dnsop-aname] CNAME does not work at the apex of a domain. A primary reason is section 3.6.2 of [RFC1034].

5. Proprietary solutions

To respond to this business demand, various DNS operators (including CDN providers who also act as DNS operators) have developed proprietary solutions (also referred to as "stupid DNS tricks" within the DNSOP community). Under various names such as "URL flattening" or "CNAME flattening", these techniques do work and allow the sites to be accessible on the CDN via the simple domain name.

5.1. Proprietary lockin

However, because of the proprietary nature, they then lock the website publisher into using that DNS operator / CDN. The website publisher does not have an easily ability to move to a different DNS
operator / CDN unless the new DNS operator / CDN can also provide a mechanism to allow the non-www domain usage.

5.2. Restriction on using multiple CDNs

Additionally, many large web site publishers use (or want to use) multiple CDNs to achieve various business objectives, including resiliency / availability. The lack of a standard mechanism to do this "CNAME at apex" functionality limits the ability to explore multi-CDN options.

6. Existing and proposed solutions

Various email discussions have indicated that existing mechanisms can address this issue, although deployment/adoption concerns have been raised. Existing solutions include:

- SRV record - [RFC2052]
- URI record - [RFC7553]
- NAPTR-based solutions (need to understand more)

Multiple solutions have been proposed for discussion at IETF 103, including:

- [I-D.ietf-dnsop-aname]
- [I-D.bellis-dnsop-http-record]

7. Author opinion

As a website publisher, I have a business objective to meet - make the site accessible over "example.com" versus "www.example.com". As long as this can happen in a manner that can be widely deployed, I am not partial to any specific solution. I just want it to work and not lock me in to specific proprietary solutions.

8. Past discussion

There was a lengthy discussion of this topic in the DNSOP session at IETF 102 in Montreal in 2018. Slides from that session are useful for more context:

- https://datatracker.ietf.org/meeting/102/materials/slides-102-dnsop-somethingapex-02
9. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

10. Security Considerations

TODO add any security considerations.

11. IANA Considerations

This document has no IANA actions.

12. References

12.1. Normative References


12.2. Informative References


Acknowledgments

TODO acknowledge.

Author’s Address

Dan York
Internet Society

Email: york@isoc.org