Network Working Group E. Hunt
Internet-Draft ISC
Intended status: Standards Track P. van Dijk
Expires: November 25, 2017 PowerDNS
A. Eden
DNSimple
May 24, 2017

Address-specific DNS Name Redirection (ANAME)
draft-ietf-dnsop-aname-00

Abstract

This document defines the "ANAME" DNS RR type, to provide similar functionality to CNAME, but only redirects type A and AAAA queries. Unlike CNAME, an ANAME can coexist with other record types. The ANAME RR allows zone owners to redirect queries for apex domain names in a standards compliant manner.

Status of This Memo

This Internet-Draft will expire on November 25, 2017.

Copyright Notice

Table of Contents

1. Introduction

Websites hosted by content distribution networks are often served by multiple IP addresses handling different geographic areas. In many cases, an initial query for a domain name returns a CNAME record whose <target> is a name served by the CDN, and which ultimately resolves to a different final answer depending on the client's IP address or subnet, geographic location, or other considerations.

It is common practice for websites to publish content at their registered domain name (sometimes referred to as a "bare domain" or "zone apex": for example, "example.com" rather than "www.example.com"). However, [RFC1033] forbids the use of CNAME records at the same node as any other record type. Zone apex nodes always contain SOA and NS RRsets, and frequently contain other types such as DNSKEY, MX, TXT/SPF, etc. Consequently, a CNAME record is not permitted at zone apex nodes.

It should be noted that [RFC4034] relaxed this restriction by allowing coexistence of CNAME with RRSIG and NSEC records, but such exceptions are not applicable to other resource records. RRSIG and NSEC exist to prove the integrity of the CNAME record; they are not intended to associate arbitrary data with the domain name.

DNAME [RFC6672] is also not a solution, as its function is to redirect all names in the namespace below the DNAME <owner>, not the DNAME <owner> itself.

Redirecting website lookups to an alternate domain name via SRV or URI resource records would be an effective solution, but to date this approach has not been accepted by browser implementations. In addition, it is not possible to use SRV records with wildcard names.

As a result of the above, the only widely supported and standards-compliant way to publish content at a zone apex is to to place A and/or AAAA records at that node. The flexibility afforded by CNAME is not available.

This document specifies a new RR type "ANAME", which provides similar functionality to CNAME, but only for address queries (i.e., for type A or AAAA). The ANAME record can be present at any DNS node, and can coexist with most other RR types, enabling it to be present at a zone apex. Authoritative servers configured with ANAME records will answer address queries for the ANAME owner with addresses found at the ANAME's target, and also with the ANAME itself. Recursive resolvers which understand ANAME can re-query for the ANAME target, just as if they had received a CNAME response. Recursive resolvers which do not understand ANAME will ignore the ANAME and consume the provided A/AAAA records directly.

Similar authoritative functionality has been implemented and deployed by a number of DNS software vendors and service providers, using names such as ALIAS, ANAME, apex CNAME, CNAME flattening, and top level redirection. These approaches have all been standards-noncompliant in one way or another, and none have provided a mechanism for a recursive resolver to follow the redirection chain itself.

1.1. Terminology

"Address type" refers to a DNS RR type that encodes a network address. Currently the set of address types consists of A and AAAA.

"Address query" refers to a DNS query for any address type.

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 [RFC2119].

2. The ANAME Resource Record

This document defines the "ANAME" DNS resource record type, with RR TYPE value [TBD].

The ANAME presentation format is identical to that of CNAME [RFC1033]:

```
    owner ttl class ANAME target
```

The wire format is also identical to CNAME, except that name compression is not permitted in ANAME RDATA, per [RFC3597].

No more than one ANAME resource record SHALL be present at any DNS node.

3. Authoritative Server Behavior

When an ANAME record is present at a DNS node and a query is received by an authoritative server for type A or AAAA, the authoritative server returns the ANAME RR in the answer section.

Because not all querying resolvers understand ANAME, the authoritative server MUST also return address records, as described below. This is conceptually similar to the synthesized CNAME record included with DNAME responses [RFC6672].

Authoritative servers implementing ANAME MUST be equipped to resolve the ANAME <target> on the querying resolver's behalf, either by sending queries to an external recursive resolver or by implementing recursive resolution logic internally, so that address records can be expanded when the ANAME <target> is in a separate zone from <owner>.

If a query for the ANAME <target> returns a chaining response (i.e., CNAME, DNAME, or another ANAME), then the authoritative server (or the resolver tasked with resolving the ANAME <target> on its behalf) MUST attempt to follow the chain until it is able to resolve a final address response, or until resolution fails. Intermediate ANAMEs, CNAMEs, and DNAMEs MUST be omitted from the response.

3.1. Address records returned with ANAME

If the original query is for type A, and an RRset of type A exists at the final ANAME <target>, then that A RRset (with <owner> changed to match that of the ANAME RR), MUST be appended to the answer section after the ANAME RRset. If an AAAA RRset is also known to exist at the ANAME <target>, then the AAAA RRset MAY be appended to the

additional section (again, with <owner> changed to match that of the ANAME RR).

Similarly, if the original query was for type AAAA, and an AAAA RRset exists at the final ANAME <target>, then it is appended to the answer section (with <owner> changed), and if an A RRset also exists at the final ANAME <target> then it MAY be appended to the additional section.

If the original query is for type ANAME, A and AAAA records MAY be returned in the additional section.

If the original query is for type ANY and access to ANY query processing is not restricted, then the answer section MUST contain both the ANAME and the A and AAAA RRsets, if present and successfully resolved at the ANAME <target>.

How and when an authoritative server resolves the A and AAAA responses from the ANAME <target> (when it is not itself authoritative for <target>) is unspecified. If the authoritative server is capable of performing recursive resolution, then it MAY resolve the query itself, or it MAY send address queries to an external resolver. It MAY send address queries to the ANAME <target> when loading the zone and cache the responses locally, or it MAY delay resolution of the address records until a query is received for the ANAME <owner>. In either case, for performance reasons, it is RECOMMENDED that address records be cached locally by the authoritative server.

Address records cached locally MUST have a limited TTL. The initial TTL for locally-cached address records MUST be set to the lesser of the ANAME TTL and the TTL of the address records retrieved from the ANAME <target>. The local TTL MUST count down, just as it would in a conventional resolver cache. Records with an expired TTL MUST NOT be used to answer address queries until refreshed with a new query to the ANAME <target>.

If configured to do so, then the authoritative server MAY, when sending queries to the ANAME <target>, include an EDNS CLIENT-SUBNET (ECS) option [RFC7871], either forwarding an ECS option that was sent to it by the querying resolver, or generating a new ECS option from the querying resolver's address. If a response from the ANAME <target> includes an ECS option with a SCOPE PREFIX-LENGTH greater than zero, the response SHOULD be cached with the ECS data and should only be used in response to queries from the same client subnet.

3.2. Coexistence with other types

If the zone is configured with an A or AAAA RRset at the same DNS node as ANAME, then the ANAME is considered to have been pre-expanded for zone transfer purposes. When a zone is being transferred to a secondary server, if any address record already exists at the same node as an ANAME RR, then the ANAME RR MUST NOT be further expanded by the authoritative server.

ANAME MUST NOT coexist with CNAME or any other RR type that restricts the types with which it can itself coexist.

Like other types, ANAME MUST NOT exist below a DNAME, but it can coexist at the same node; in fact, the two can be used cooperatively to redirect both the owner name (via ANAME) and everything under it (via DNAME).

ANAME can freely coexist at the same owner name with any other RR type.

3.3. DNSSEC signing

If the zone in which the ANAME resides is DNSSEC-signed, and if the server has access to its private zone-signing key, then the A and AAAA RRsets MUST be signed, either in advance when populating the A/AAAA answers for the ANAME records, or "on the fly" when responding to a query.

If the server does not have access to the private zone-signing key then it MAY return unsigned address records, but this is NOT RECOMMENDED unless every resolver with access to the zone is known to support ANAME (as might be the case in a split-horizon deployment where ANAME records are only served to an internal network with its own resolvers).

Validating resolvers which do not yet implement ANAME will not be able to validate the A and AAAA responses included with an ANAME response unless those responses are validly signed by a DNSKEY at the apex of the zone in which the ANAME resides. Passing along the RRSIGs associated with the original A and AAAA RRsets from the ANAME <target> will not be sufficient for DNSSEC validation.

Implementers MAY allow address records associated with the ANAME to be populated and signed by the primary server, then sent along with their RRSIGs to secondaries via zone transfer. In this case, the master server MUST respect the TTLs of the address records, MUST refresh the address records by re-resolving the ANAME <target> when their TTLs expire, SHOULD respond to address queries with TTLs that

count down as they would when answering from a normal DNS cache, and MUST inform secondary servers via DNS NOTIFY they need to refresh the zone when address records have been updated. A secondary server SHOULD store address records and associated RRSIGs supplied via zone transfer in such a way that their TTLs will count down, as they would in a normal DNS cache, and ultimately trigger a zone refresh query upon reaching zero. When a secondary server is responding to an address query, it SHOULD answer with the reduced TTL, but when responding to a zone transfer request, it MUST answer with the original TTL received from the primary.

If this address record expansion and signing during zone transfer is not supported, then every authoritative server providing ANAME responses in a signed zone SHOULD have access to the private zone-signing key for that zone. Deployment of ANAME in signed zones where address records cannot be signed due to lack of access to the private zone-signing key is NOT RECOMMENDED.

When ANAME is present in a signed DNS node and address records exist at the ANAME <target>, the type bit map in the NSEC [RFC4034] or NSEC3 [RFC5155] record for that node MUST include bits for A and/or AAAA as well as ANAME. This is for the benefit of validating resolvers not implementing ANAME which may use a signed proof of nonexistence for type A and AAAA to prevent address queries from being resolved. The type bit map SHOULD only include address types which are known to exist at the <target>.

4. Recursive Server Behavior

When a recursive resolver sends a query of type A or AAAA and receives a response with an ANAME RRset in the answer section, it MUST re-query for the ANAME <target>. This is necessary because, in some cases, the address received will be dependent on network topology and other considerations, and the resolver may find a different answer than the authoritative server did. (This requirement MAY be relaxed if both the ANAME <owner> and <target> are validly signed and provably in the same zone.)

If resolution fails -- for example, due to the local resolver being nonfunctional or the ANAME <target> zone being unreachable -- then the resolver MAY use the address records that were included in the authoritative response as a fallback. Otherwise, these records MUST NOT be cached or returned.

If configured to do so, the resolver MAY include an EDNS CLIENT-SUBNET option [RFC7871] both when sending the initial query to the ANAME <owner> and when re-querying for the ANAME <target>. If the response includes a SCOPE PREFIX-LENGTH greater than zero, the

response SHOULD be cached with the ECS data and should only be used in response to queries from the same client subnet.

5. Operational Considerations

When a zone containing ANAME records is transferred to a secondary server, the ANAME records are transferred, but the A or AAAA records retrieved from the ANAME <target> may not be. If the primary server implements ANAME but the secondary server does not, then the two will return different answers for address queries. It is therefore RECOMMENDED that ANAME not be deployed in a zone unless all of the authoritative servers for that zone implement ANAME, or the primary is able to expand the ANAME with the related address RRsets during the zone transfer.

6. Implementation Status

PowerDNS <https://powerdns.com> currently implements a similar authoritative-only feature using "ALIAS" records, which are expanded by the primary server and transfered as address records to secondaries.

[TODO: Add discussion of DNSimple, DNS Made Easy, EasyDNS, Cloudflare, and Akamai.]

7. Security Considerations

An authoritative server which implements ANAME resolves address queries on behalf of its clients, either internally or by querying an external resolver. This resolution must be allowed to take place regardless of whether the client would ordinarily have been permitted by local policy to send recursive queries.

When a resolver that does not understand ANAME receives a response containing A or AAAA records with <owner> rewritten to match that of the ANAME RR, this may bypass security mechanisms based on local policy limiting access to the original ANAME <target>.

A validating resolver that does not understand ANAME will not be able to validate A and AAAA records unless they are signed.

Both authoritative servers and resolvers that implement ANAME should carefully check for loops and treat them as an error condition.

8. IANA Considerations

IANA is requested to assign a DNS RR data type value for the ANAME RR type under the "Resource Record (RR) TYPEs" subregistry under the "Domain Name System (DNS) Parameters" registry.

9. Acknowledgments

Thanks to Mukund Sivaraman, Stephen Morris, Ray Bellis, Mark Andrews, Richard Salts, Job Snijders, and Hakan Lindqvist for discussion and feedback.

10. References

10.1. Normative References

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

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record (RR) Types", RFC 3597, September 2003.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

10.2. Informative References

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

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

[RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", RFC 6672, June 2012.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <http://www.rfc-editor.org/info/rfc7871>.

Authors' Addresses

Evan Hunt
ISC
950 Charter St
Redwood City, CA 94063
USA

Email: each@isc.org

Peter van Dijk
PowerDNS.COM B.V.
Den Haag
The Netherlands

Email: peter.van.dijk@powerdns.com

Anthony Eden
DNSimple
Boston, MA
USA

Email: anthony.eden@dnsimple.com
URI: https://dnsimple.com/