Update to DNAME Redirection in the DNS
draft-ietf-dnsext-rfc2672bis-dname-01

Status of This Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 July 26, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

The DNAME record 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. This is an update to the original specification in RFC 2672.
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].

Table of Contents

1. Introduction .................................................. 3

2. The DNAME Resource Record ................................. 3
   2.1. Format .................................................... 3
   2.2. The DNAME Substitution ............................... 4
   2.3. Names next-to and below a DNAME record ............. 5
   2.4. Compression of the DNAME record ..................... 5

3. Processing .................................................... 5
   3.1. Wildcards ............................................... 5
   3.2. DNAME bit in NSEC type map ........................... 6
   3.3. CNAME synthesis ....................................... 6
   3.4. Processing ............................................... 6

4. DNAME Discussions in Other Documents ................... 7

5. Issues with DNAME ............................................. 7
   5.1. DNAME Apex not Redirected itself .................... 8
   5.2. MX, NS and PTR Records Must Point to Target of DNAME .. 8
   5.3. NSEC3 and DNAME ....................................... 8
   5.4. Validators Must Understand DNAME .................... 9
      5.4.1. DNAME in Bitmap Causes Invalid Name Error .... 9
      5.4.2. Valid Name Error Response Involving DNAME in Bitmap . 9
      5.4.3. Response With Synthesized CNAME ................ 9

6. IANA Considerations ........................................... 10

7. Security Considerations .................................... 10

8. Document History ............................................. 10

9. Acknowledgments .............................................. 11

10. Normative References ....................................... 11
1. Introduction

DNAME is a DNS Resource Record type. DNAME provides redirection from a part of the DNS name tree to another part of the DNS name tree.

For example, given a query for foo.example.com and a DNAME from example.com to example.net, the query would be redirected to foo.example.net. With the same DNAME a query for foo.bar.example.com is redirected to foo.bar.example.net.

The DNAME RR is similar to the CNAME RR in that it provides redirection. But where the CNAME RR only provides redirection for exactly one name, the DNAME RR provides redirection for all names in a sub-tree of the DNS name tree.

This document is an update to the original specification of DNAME in [RFC 2672](https://tools.ietf.org/html/rfc2672), by Matt Crawford. DNAME was conceived to help with the problem of maintaining address-to-name mappings in a context of network renumbering. So that with a careful set-up a renumbering event in the network causes no change to the authoritative server that has the address-to-name mappings.

Other usage of DNAME lies in redirection of name spaces. Where a zone administrator want subtrees of the DNS to contain the same information. Examples in practice are classless reverse address space delegations and punycode alternates for domain spaces. DNAME is also used for redirection of ENUM domains to another maintaining party.

This update to DNAME does not change the wire format, or the handling of DNAME Resource Records by existing software. Discussion is added on the problems that can be encountered when using DNAME.

2. The DNAME Resource Record

2.1. Format

The DNAME RR has mnemonic DNAME and type code 39 (decimal).

The format of the DNAME record has not changed compared to [RFC 2672](https://tools.ietf.org/html/rfc2672). DNAME has the following format:

```
<owner> <ttl> <class> DNAME <target>
```

The format is not class-sensitive. All fields are required. The RDATA field target is a domain-name. The RDATA field target name MUST be sent uncompressed [RFC3597].
The DNAME RR causes type NS additional section processing.

2.2. The DNAME Substitution

DNAMEs cause a name substitution to happen to query names. This is called The DNAME Substitution. The suffix ownername of the DNAME is replaced by the target of the DNAME. The owner name of the DNAME is not itself redirected, only domain names below the owner name are redirected. Only whole labels are replaced. A name is considered below the owner name if it has more labels than the owner name, and the labels of the owner name appear at the end of the name. See the table of examples for common cases and corner cases.

In the table below, the QNAME refers to the query name. The owner is the DNAME owner domain name, and the target refers to the target of the DNAME record. The result is the resulting name of performing the DNAME Substitution on the query name. "no match" means that the query did not match the DNAME and thus no substitution is performed, the QNAME did not change. The examples 'cyc' and 'shortloop' contain loops.

<table>
<thead>
<tr>
<th>QNAME</th>
<th>owner</th>
<th>DNAME</th>
<th>target</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.</td>
<td>example.com.</td>
<td>example.net.</td>
<td></td>
<td>&lt;no match&gt;</td>
</tr>
<tr>
<td>example.com.</td>
<td>example.com.</td>
<td>example.net.</td>
<td></td>
<td>&lt;no match&gt;</td>
</tr>
<tr>
<td>a.example.com.</td>
<td>example.com.</td>
<td>example.net.</td>
<td>a.example.net.</td>
<td>a.example.net.</td>
</tr>
<tr>
<td>a.b.example.com.</td>
<td>example.com.</td>
<td>example.net.</td>
<td>a.b.example.net.</td>
<td></td>
</tr>
<tr>
<td>ab.example.com.</td>
<td>b.example.com.</td>
<td>example.net.</td>
<td></td>
<td>&lt;no match&gt;</td>
</tr>
<tr>
<td>foo.example.com.</td>
<td>example.com.</td>
<td>example.net.</td>
<td>foo.example.net.</td>
<td></td>
</tr>
<tr>
<td>a.x.example.com.</td>
<td>x.example.com.</td>
<td>example.net.</td>
<td>a.example.net.</td>
<td></td>
</tr>
<tr>
<td>a.example.com.</td>
<td>example.com.</td>
<td>y.example.net.</td>
<td>a.y.example.net.</td>
<td></td>
</tr>
<tr>
<td>shortloop.x.x.</td>
<td>x.</td>
<td>.</td>
<td>shortloop.x.</td>
<td></td>
</tr>
<tr>
<td>shortloop.x.</td>
<td>x.</td>
<td>.</td>
<td>shortloop.</td>
<td></td>
</tr>
</tbody>
</table>

Table. DNAME Substitution Examples.

It is possible for DNAMEs to form loops. Just like CNAMEs can form loops. DNAMEs and CNAMEs can chain together to form loops. A single corner case DNAME can form a loop. Resolvers and servers should be cautious in devoting resources to a query, but be aware that fairly long chains of DNAMEs may be valid.

The domain name can get too long during substitution. If this occurs the server returns an RCODE of YXDOMAIN [RFC2136]. The DNAME record and its signature are included in the answer as proof for the YXDOMAIN (value 6) RCODE.
2.3. Names next-to and below a DNAME record

Other resource records MUST NOT exist below a DNAME. To get the contents for names below a DNAME, the DNAME redirection must be invoked and the resulting target queried. A server SHOULD refuse to load a zone that has data below a domain with a DNAME resource record. Also a server SHOULD refuse to load a zone beneath a DNAME record from another zone.

DNAME is a singleton type, only one DNAME is allowed per name. The owner name that has a DNAME, can only have one DNAME RR, and no CNAME RRs can exist at that name. These rules make sure that for a single domain name only one redirection exists, and thus no confusion which one to follow. A server SHOULD refuse to load a zone that violates these rules.

These rules allow DNAME records to be queried through DNAME unaware caches.

2.4. Compression of the DNAME record.

The DNAME owner name can be compressed like any other owner name. The target DNAME RDATA name of MUST NOT be sent out in compressed form, so that DNAME can be treated as an unknown type.

Although the previous specification talked about signaling to allow compression of the target name, no such signaling is done. Signaling complicates the protocol unnecessarily.

RFC2672 claimed that the EDNS version had a meaning for understanding of DNAME and DNAME target name compression. This document updates RFC2672, there is no EDNS version signaling for DNAME.

3. Processing

3.1. Wildcards

The use of DNAME in conjunction with wildcards is discouraged [RFC4592]. Thus records of the form "*.example.com DNAME example.net" SHOULD NOT be used.

The interaction between the expansion of the wildcard and the redirection of the DNAME is non-deterministic. Because the processing is non-deterministic, DNSSEC validating resolvers may not be able to validate a wildcarded DNAME.

A server MAY give a warning that the behaviour is unspecified if such a wildcarded DNAME is loaded.
3.2. DNAME bit in NSEC type map

When a validator checks the NSEC RRs returned on a name error response, it SHOULD check that the DNAME bit is not set. If the DNAME bit is set then the DNAME substitution should have been done, but has not. In the same vein, for a no error/no data response the CNAME bit in the NSEC RR bitmap should not be set.

3.3. CNAME synthesis

On the server side, the DNAME RR record is always included in the answer section of a query. A CNAME RR record with TTL 0 is synthesized for old resolvers, specifically for the QNAME in the query. DNSSEC [RFC4033], [RFC4034], [RFC4035] says that the synthesized CNAME does not have to be signed. The DNAME has an RRSIG and a validating resolver can check the CNAME against the DNAME record and validate the DNAME record.

The TTL of the synthesized CNAME record MAY be set to the TTL of the DNAME record. This enables older caches store the CNAMEs without a need to re-query for them. This updates RFC2672 which stated the TTL had to be zero.

It does not make sense for the authoritative server to follow the chain of DNAMEs, CNAMEs and wildcards outside of the zone of the query, as modern resolvers will remove out-of-zone information from the answer.

The EDNS DNSSEC-OK bit signals understanding of the DNAME record [RFC4034]. If set, the synthesized CNAME MAY be omitted, since it is not signed and therefore not useful for validation and a waste of bandwidth. This is a change from RFC2672, which specified CNAMEs had to be synthesized for all EDNS0, or non-extended queries.

Resolvers MUST be able to handle a synthesized CNAME TTL of zero or equal to the TTL of the corresponding DNAME record. The TTL of zero means that the CNAME can be discarded immediately after processing the answer.

Servers MUST be able to answer a query for a synthesized CNAME. An answer containing the synthesized CNAME cannot contain an error (since a CNAME has been followed), as per RFC 1034 CNAME rules.

3.4. Processing

TBD: An issue with some firewalls and middleboxes, and perhaps windows XP/2003 resolvers potentially responding badly to DNAME records (dropping packets),
TBD: Is this useful to specify? Resolvers MUST be able to handle unsigned responses with only the CNAME, or with the DNAME only, or both CNAME and DNAME. Resolvers that query with DNSSEC_OK MUST be able to handle signed responses with only the DNAME, or with the unsigned synthesized CNAME included.

Caches MUST NOT allow data to be cached below a DNAME. Except CNAME records or perhaps NSEC3 records and their signatures. CNAME records below a DNAME MUST be re-synthesized from the DNAME, or checked against the DNAME record before sending them out. This improves consistency of the DNAME and CNAME records below it.

4. DNAME Discussions in Other Documents

In [RFC2181], in Section 10.3., the discussion on MX and NS records touches on redirection by CNAMEs, but this also holds for DNAMEs.

Excerpt from 10.3. MX and NS records (in RFC 2181).

The domain name used as the value of a NS resource record, or part of the value of a MX resource record must not be an alias. Not only is the specification clear on this point, but using an alias in either of these positions neither works as well as might be hoped, nor well fulfills the ambition that may have led to this approach. This domain name must have as its value one or more address records. Currently those will be A records, however in the future other record types giving addressing information may be acceptable. It can also have other RRs, but never a CNAME RR.

RFC 4592 [RFC4592] says that DNAMEs are discouraged at wildcards. DNAMEs and CNAMEs can form loops.

DNAME is discussed in RFC 3363, section 4, on A6 and DNAME. DNAME is NOT RECOMMENDED for use in the IPv6 reverse tree [RFC3363]. And from [RFC4294], all references to DNAME should have been removed. There needs to be a better clarification of the status of DNAME in RFC 3363 which would be to drop all constraints on having DNAME RRs in these zones.

5. Issues with DNAME

There are several issues to be aware of about the use of DNAME.
5.1. DNAME Apex not Redirected itself

The owner name of a DNAME is not redirected itself. The reason for the original decision was that in this way (without DNAME owner affected) one can have a DNAME at the zone apex, next to the SOA, NS records, without problem. Then use this to point queries to this zone to other zones. Hosting two identical zones for example, there still is a need to duplicate the resource records at the zone apex. Another reason for excluding the DNAME owner from the DNAME substitution is that one can then query for the DNAME through RFC 1034 [RFC1034] caches.

This means that DNAME does not mirror a zone completely, as it does not mirror the zone apex. It can be used if the zone apex records are duplicated to provide a summary of the rest of the zone.

The rules on DNAME RRs mean that it is not allowed at the same domain name as NS records unless there is also a SOA record there. This means DNAME RRs are not allowed at the parent side of a delegation point. DNAME is allowed at a zone apex.

5.2. MX, NS and PTR Records Must Point to Target of DNAME

The names listed as target names of MX, NS and PTR records must be canonical hostnames. This means no CNAME or DNAME redirection may be present during DNS lookup of the address records for the host. This is discussed in RFC 2181 [RFC2181], section 10.3, and RFC 1912 [RFC1912], section 2.4.

The upshot of this is that although the lookup of a PTR record can involve DNAMEs, the name listed in the PTR record can not fall under a DNAME. The same holds for NS and MX records. For example, when punycode alternates for a zone use DNAME then the NS, MX and PTR records that point to that zone must use names without punycode in their RDATA. What must be done then is to have the domain names with DNAME substitution already applied to it as the MX, NS, PTR data. These are valid canonical hostnames.

5.3. NSEC3 and DNAME

NSEC3 records and their signatures are allowed to exist below a DNAME. This is because of the nature of NSEC3 RRs in DNSSEC, which creates hashed owner names that exist below the apex. This is an exception to the rule that there MUST NOT be any other RRs under a DNAME RR, if the DNAME RR exists at the zone apex.

TBD: This is a new issue, but the same as the NSEC3 draft.
Queries for NSEC3 owner names are redirected as if there were no such NSEC3 present.

There is no significant extra hashing cost for NSEC3 signed zones when answering queries with DNAME substitution.

5.4. Validators Must Understand DNAME

Examples of why DNSSEC validators MUST understand DNAME.

5.4.1. DNAME in Bitmap Causes Invalid Name Error

;; Header: QR AA DO RCODE=3(NXDOMAIN)
;; Question
foo.bar.example.com. IN A
;; Answer
bar.example.com. NSEC dub.example.com. A DNAME
bar.example.com. RRSIG NSEC [valid signature]

If you receive this answer, then only by understanding that the DNAME bit means that foo.bar.example.com needed to have been redirected by the DNAME, the validator can see that it is a BOGUS reply from an attacker, that collated existing records from the DNS to create a confusing reply.

If the DNAME bit had not been set in the NSEC record above, then the answer would have validated as a correct name error response.

5.4.2. Valid Name Error Response Involving DNAME in Bitmap

;; Header: QR AA DO RCODE=3(NXDOMAIN)
;; Question
cee.example.com. IN A
;; Answer
bar.example.com. NSEC dub.example.com. A DNAME
bar.example.com. RRSIG NSEC [valid signature]

If the query had been cee.example.com as shown above, then this answer would have been validated, because ‘cee’ does not get redirected by the DNAME at ‘bar’.

5.4.3. Response With Synthesized CNAME
;; Header: QR AA DO RCODE=0(NOERROR)
;; Question
foo.bar.example.com. IN A
;; Answer
bar.example.com. DNAME bar.example.net.
bar.example.com. RRSIG DNAME [valid signature]
foo.bar.example.com. CNAME foo.bar.example.net.

The answer shown above has the synthesized CNAME included. However, the CNAME has no signature, since the server cannot sign the keys online (it is a slow operation and exposes the signing key). So it cannot be trusted. It could be altered by an attacker to be foo.bar.example.com CNAME bla.bla.example. The DNAME record does have its signature included, since it does not change for every query name. The validator must verify the DNAME signature and then recursively resolve further to query for the foo.bar.example.net A record.

6. IANA Considerations

The main purpose of this draft is to discuss issues related to the use of DNAME RRs in a DNS zone. The original document registered the DNAME Resource Record type code 39 (decimal). No further action is required on the part of IANA.

7. Security Considerations

DNAME redirects queries elsewhere, which may impact security based on policy and the security status of the zone with the DNAME and the redirection zone’s security status.

If a validating resolver accepts wildcarded DNAMEs, this creates security issues. Since the processing of a wildcarded DNAME is non-deterministic and the CNAME that was substituted by the server has no signature, the resolver may choose a different result than what the server meant, and consequently end up at the wrong destination. Use of wildcarded DNAMEs is discouraged in any case [RFC4592].

A validating resolver MUST understand DNAME, according to [RFC4034]. In Section 5.4 examples are given that illustrate this need. These examples are shown with NSEC records, but similar cases exist for NSEC3.

8. Document History

00-01. Small language issues. Removed wording of ‘delegation’ for dname use to alias a whole zone from parent side (registration tool). Names under a DNAME are not canonical. Synthesized CNAME is not
signed. Rewritten entirely as an update to the rfc.

9. Acknowledgments

The authors of this draft would like to acknowledge Matt Larson for
beginning this effort to address the issues related to the DNAME RR
type.

10. Normative References


[RFC1912] Barr, D., "Common DNS Operational and Configuration

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound,
"Dynamic Updates in the Domain Name System (DNS UPDATE)",
RFC 2136, April 1997.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS

[RFC2672] Crawford, M., "Non-Terminal DNS Name Redirection",
RFC 2672, August 1999.

[RFC3363] Bush, R., Durand, A., Fink, B., Gudmundsson, O., and T.
Hain, "Representing Internet Protocol version 6 (IPv6)
Addresses in the Domain Name System (DNS)", RFC 3363,
August 2002.

[RFC3597] Gustafsson, A., "Handling of Unknown DNS Resource Record

Rose, "DNS Security Introduction and Requirements",

Rose, "Resource Records for the DNS Security Extensions",

Rose, "Protocol Modifications for the DNS Security


Authors' Addresses

Scott Rose
NIST
100 Bureau Dr.
Gaithersburg, MD 20899
USA

Phone: +1-301-975-8439
Fax:  +1-301-975-6238
EMail: scottr@nist.gov

Wouter Wijngaards
NLnet Labs
Kruislaan 419
Amsterdam 1098 VA
The Netherlands

Phone: +31-20-888-4551
Fax:  +31-20-888-4462
EMail: wouter@nlnetlabs.nl
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).