Domain Name System Operations
Internet-Draft
Updates: RFC1035 (if approved)
Intended status: Standards Track
Expires: 19 December 2025

J. Abley
Cloudflare
W. Hardaker
USC/ISI
W. Kumari
Google, Inc.

17 June 2025

Signalling a Zone Cut to Nowhere in the DNS
draft-jabley-dnsop-zone-cut-to-nowhere-00

Abstract

This document defines a standard means to signal that a zone cut exists in the DNS without specifying a set of nameservers to which a child zone is delegated. This is useful in situations where it is important to make it clear to clients that a zone cut exists, but when the child zone is only provisioned in a private namespace.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ableyjoe.github.io/draft-jabley-dnsop-zone-cut-to-nowhere/draft-jabley-dnsop-zone-cut-to-nowhere.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-jabley-dnsop-zone-cut-to-nowhere/.

Discussion of this document takes place on the Domain Name System Operations Working Group mailing list (mailto:dnsop@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnsop/. Subscribe at https://www.ietf.org/mailman/listinfo/dnsop/.

Source for this draft and an issue tracker can be found at https://github.com/ableyjoe/draft-jabley-dnsop-zone-cut-to-nowhere.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The DNS protocol, as originally specified in [RFC1034] and [RFC1035], describes a single, global, hierarchical namespace that is separated into zones. The boundary between a parent zone and a child zone is indicated using a zone cut. Zone cuts are specified using specific resource records which are published within the parent and child zones; the parent-side resource records are revealed during DNS resolution by way of referral responses from nameservers.

Private DNS namespaces also exist. A user of a private network might be able to resolve names using local DNS infrastructure that are not visible to other users of other networks. This is often an intentional and deliberate configuration by network operators, for example to provide name resolution for internal, private services that are not available to users of other networks.

When a device or application uses the DNS protocol to resolve both internal names and external names published in the global DNS namespace, ambiguity can result. For example, DNS responses from Internet-reachable nameservers might indicate that a particular name published in an internal namespace does not exist, while an internal nameserver might be configured to respond differently. Since mobile devices can attach to different networks and can cache DNS responses obtained from different namespaces, this ambiguity can cause headaches. A DNSSEC-aware resolver on a mobile device might cache a signed, negative response from an external nameserver for a particular name and might treat a subsequent, positive response from an internal nameserver for the same name as bogus, preventing the response from being used by an application.

This document provides a means of signalling the existence of a zone cut in a namespace in circumstances where the child zone only exists in a different namespace from the parent. We refer to this type of zone cut as a "zone cut to nowhere" and introduce the corresponding terms "delegation to nowhere" and "referral to nowhere" in Section 2.

2. 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.

This document uses DNS terminology as described in [RFC9499]. Familiarity with terms defined in that document is assumed.

This document also uses the following new terms:

1. "Zone cut to nowhere" -- a zone cut where the parent zone and the child zone are provisioned in different namespaces. A zone cut to nowhere is a signal provided by the administrator of a parent zone that a child zone exists, but is not able to be used in the DNS namespace of the parent.

2. "Delegation to nowhere" -- a delegation from a parent to a child across a zone cut to nowhere.

3. "Referral to nowhere", "Referral response to nowhere" -- a DNS response received from a nameserver that reveals the existence of a delegation to nowhere.

3. Publishing a Delegation to Nowhere

A zone cut to nowhere is implemented in a parent zone using a single NS resource record with an empty target (an empty NSDNAME, in the parlance of [RFC1035]). A zone cut to nowhere between the parent zone EXAMPLE.ORG and the child zone DUCKLING.EXAMPLE.ORG with a TTL of 3600 seconds would be described in zone file syntax as follows:

```
; zone data published in an external nameserver

$ORIGIN EXAMPLE.ORG.

; the zone DUCKLING.EXAMPLE.ORG exists, but in another
; namespace

DUCKLING  3600  IN  NS  .
```

A zone cut to nowhere may also be provisioned as a secure delegation. This allows a DNSSEC-aware consumer of a referral response to obtain and cache a DNSSEC trust anchor for the child zone, for use when it is able to receive a signed response from a nameserver that includes the child zone in its namespace.

```
$ORIGIN EXAMPLE.ORG.

; the signed zone PUPPY.EXAMPLE.ORG exists,
; but in another namespace

PUPPY  3600  IN  DS  [...]
                 NS  .
```

An NS RRSet in a parent zone which includes multiple NS resource records is not a delegation to nowhere, even if one of the NS resource records within the RRSet has an empty target.

```
        KITTEN  3600  IN  NS  A.CAT-SERVERS.EXAMPLE.
                          NS  B.CAT-SERVERS.EXAMPLE.
                          NS  .                      ; unusual
                          NS  C.CAT-SERVERS.EXAMPLE.
```

This NS RRSet does not encode a delegation to nowhere, since other NS resource records exist in addition to the record with the empty target (marked with a comment as "unusual"). This configuration may have some other meaning in a different context, however, and is specifically not addressed by this specification.

4. Interpreting a Referral to Nowhere

No special processing is necessary in order to interpret a referral response to nowhere. Individual RRSets present in a referral response to nowhere can safely be interpreted and processed in an identical fashion to any other referral response where the authoritative servers for the child zone cannot themselves be resolved, and hence cannot be reached.

5. Applicability

When a child zone is known to exist in another namespace, and when that other namespace is intended for use with the DNS, a delegation to nowhere MAY be provisioned in the parent zone to signal that the child zone exists in some other namespace. In such circumstances the parent zone MAY be the root zone, or any other zone.

A secure delegation to nowhere MAY be provisioned if the keys used for signing in the child zone are known to the administrator of the parent zone. In the case where differently-signed (or unsigned) child zones are known to exist in different namespaces, a secure delegation SHOULD NOT be used.

The use of a delegation to nowhere in this document is described for the IN class only. Use of this mechanism in other classes is not addressed by this specification.

Name resolution protocols other than the DNS are also used by some systems, for names that are syntactically equivalent to domain names in the DNS. In some cases, names resolved by those non-DNS protocols are anchored in a specific domain that is consequently reserved for their use in the DNS, to avoid name collisions. Examples of such reservations in the DNS are the LOCAL top-level domain reserved for

use by Multicast DNS [RFC6762] and the ALT top-level domain reserved use in general for non-DNS resolution protocols [RFC9476]. Domains that are not intended for use with the DNS as their resolution protocol SHOULD NOT be provisioned in the DNS as delegations to nowhere, since there is no DNS namespace ambiguity that such a configuration could help with.

6. Examples

6.1. Internal Namespace as a Subdomain of a Public Domain

A company uses names within the EXAMPLE.COM domain both for internal services it provides to its employees and for public services that are made available to the general public over the Internet.

The company also provides certain services that are only available to users of devices attached to its internal network. Those services are named within the subdomain CORP.EXAMPLE.COM. The company does not wish those internal services to be visible to external users.

We say that the EXAMPLE.COM zone exists in the global DNS namespace and that the CORP.EXAMPLE.COM zone exists only in a private DNS namespace.

The company publishes a CORP.EXAMPLE.COM zone on DNS nameservers attached to its internal network. The company configures the DNS resolvers used by devices attached to its internal network to be aware that the CORP.EXAMPLE.COM zone is served by those internal nameservers, such that queries sent from devices inside the company’s network can resolve names in the CORP.EXAMPLE.COM domain.

```
$ORIGIN CORP.EXAMPLE.COM.
; internal zone only served in our internal network

@      3600  IN  SOA   [...]

; the internal zone CORP.EXAMPLE.COM is served by the internal
; nameservers NS1.CORP.EXAMPLE.COM and NS2.CORP.EXAMPLE.COM

               NS    NS1
               NS    NS2

NS1            A     198.51.100.37
               AAAA  2001:db8:2:1::2c

NS2            A     203.0.113.56
NS2            AAAA  2001:db8:2:3::2d

; the internal intranet web server is INTRANET.CORP.EXAMPLE.COM

INTRANET       A     198.51.100.74
               AAAA  2001:db8:2:1::f8

; the management address of an internal network device known
; as BACKBONE-SW.CORP.EXAMPLE.COM

BACKBONE-SW    A     198.51.100.65
```

The company publishes an EXAMPLE.COM zone on nameservers that are general reachable over the Internet -- that is, the nameservers are reachable and the COM zone returns referrals for the EXAMPLE.COM zone to those nameservers. The EXAMPLE.COM zone includes names that the company wants clients to be able to resolve regardless of what network they are connected to.

```
$ORIGIN EXAMPLE.COM.

; the public zone EXAMPLE.COM is published to the Internet

@      3600  IN  SOA   [...]

; the public zone EXAMPLE.COM is served by the nameservers
; NS1.EXAMPLE.COM and NS2.EXAMPLE.COM which are reachable
; over the Internet

             NS    NS1
             NS    NS2

; Internet mail for EXAMPLE.COM is handled by the server
; MAIL.EXAMPLE.COM

             MX    10 MAIL.EXAMPLE.COM.

; The public nameservers NS1.EXAMPLE.COM and NS2.EXAMPLE.COM

NS1          A     192.0.2.25
NS1          AAAA  2001:db8:e0::2a

NS2          A     192.0.2.27
NS2          AAAA  2001:db8:e0::2b

; MAIL.EXAMPLE.COM and WWW.EXAMPLE.COM are intended to be used
; from anywhere, not just by internal clients, so they are
; named in the global namespace

MAIL         A     192.0.2.41
MAIL         A     2001:db8:e0::f1

WWW          A     192.0.2.58
WWW          AAAA  2001:db8:e0::5e

; CORP.EXAMPLE.COM is our internal namespace. Delegate the
; corresponding zone to nowhere

CORP         NS    .
```

6.2. General Purpose Top-Level Domain for Internal Namespaces

Suppose it has been decided that the top-level domain INTERNAL be reserved for use in private namespaces. The root zone of the global DNS is signed using DNSSEC [RFC4033]; that is, DNSSEC-specific RRSets are published in the root zone that allow DNSSEC-aware resolvers to be sure with cryptographic certainty whether particular top-level domains exist in the public namespace.

A delegation to nowhere for the INTERNAL top-level domain in the root zone of the global DNS namespace would provide an unambiguous signal to resolvers that INTERNAL does exist in other namespaces. An insecure delegation to nowhere is appropriate in this example since there is no single trust anchor that could be used to provide a secure delegation to zones in multiple namespaces that have different, non-cooperating administrators.

```
$ORIGIN .

; the INTERNAL top-level domain is delegated to nowhere, to
; facilitate its use in private namespaces

INTERNAL  172800  IN  NS  .
```

7. Updates to RFC 1035

This document updates Section 3.3.11 of [RFC1035] as follows:

> NSDNAME MAY be specified as a single, zero-length label. An NS RRSet that consists of a single NS resource record with empty NSDNAME is used to indicate that a zone cut exists without providing any authoritative nameservers for the child zone. The purpose of such an RRSet is to confirm that the child zone exists, but in a different namespace from the parent (e.g. in a private namespace).

8. Other Uses of the Empty Name in the DNS

In [RFC7505] an MX resource record with an empty target (called EXCHANGE in [RFC1035]) is specified to mean that the corresponding domain name does not accept e-mail. In effect, the empty field is used to indicate that there is no host available to use for e-mail delivery.

In [RFC2782] an SRV ’Target of "." means that the service is decidedly not available at this domain.’

[RFC9460], Section 2.5 notes that 'For AliasMode SVCB RRs, a TargetName of "." indicates that the service is not available or does not exist.'

These uses of the empty name are conceptually consistent with the meaning defined in this document: that using an empty name is to be interpreted as the corresponding function not being available.

9. Operational Considerations

The empty name is not known to have been widely used as an NS target, although it has been used as an MX target, as described in Section 8. It is a reasonable concern that if delegations to nowhere became prevalent, or if names related to such zone cuts were associated with significant traffic, some operational problem might result. For example, DNS software that made incompatible assumptions about DNS responses might fail, or harmful traffic to root servers might result.

Some experiments carried out by the authors to assess the likelihood of such problems are described in Appendix A. The results of those experiments do not suggest that the widespread use of delegations to nowhere would lead to operational problems.

10. Security Considerations

This document provides a means for both internal and global namespaces to be provisioned using DNSSEC, allowing a DNSSEC-aware, mobile resolver to maintain a consistent chain of trust regardless of whether a private, child namespace exists from it's particular vantage point. The ability to support this configuration cleanly has better security properties than configurations that are ambiguous.

11. IANA Considerations

This document has no IANA actions.

The example of the designated top-level domain INTERNAL being provisioned as a delegation of INTERNAL to nowhere from the root zone was intentionally chosen in order to make it clear that such a configuration is allowed, is consistent with this specification and facilitates the use of private namespaces named under such a top-level domain with less ambiguity than might otherwise occur. This document does not provide any operational direction to the IANA, however.

12. References

12.1. 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/rfc/rfc1034>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/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/rfc/rfc2119>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/rfc/rfc4033>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/rfc/rfc9499>.

12.2. Informative References

[Byrne1985] Byrne, D., "Road to Nowhere", from the album "Little Creatures", Sire Records, 3 June 1985.

[Powers2006] Powers, T., "Three Days to Never", William Morrow & Company, ISBN 978-0380976539, 8 August 2006.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <https://www.rfc-editor.org/rfc/rfc2782>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/rfc/rfc6762>.

[RFC7505] Levine, J. and M. Delany, "A "Null MX" No Service Resource Record for Domains That Accept No Mail", RFC 7505, DOI 10.17487/RFC7505, June 2015, <https://www.rfc-editor.org/rfc/rfc7505>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/rfc/rfc9460>.

[RFC9476] Kumari, W. and P. Hoffman, "The .alt Special-Use Top-Level Domain", RFC 9476, DOI 10.17487/RFC9476, September 2023, <https://www.rfc-editor.org/rfc/rfc9476>.

Appendix A. Experiments

Wes has committed acts of science. He will describe them here.

Acknowledgments

The authors stand ready to acknowledge all contributions from their friends and colleagues.

The phrase "delegation to nowhere" was inspired by the misremebered title of a novel by Tim Powers entitled "Two Days to Nowhere", in which characters deal with ambiguous realities by way of supernatural sensitivity, time travel and alcohol. This seemed like a good metaphor for the problem of provisioning overlapping namespaces in the DNS.

Unfortunately, it appears that Tim Powers wrote no such book, although he did publish the similarly-named novel "Three Days to Never" [Powers2006] which is perhaps what I was thinking of. And it’s certainly true that much of his writing features ambiguity, the supernatural and excessive drinking. Memory is a tricky thing.

The song "Road to Nowhere" [Byrne1985] from the 1985 Talking Heads album "Little Creatures" would perhaps have been a better inspiration for the terminology. It’s a shame that’s not what happened.

Authors’ Addresses

Joe Abley
Cloudflare
Email: jabley@cloudflare.com

Wes Hardaker
USC/ISI
Email: ietf@hardakers.net

Warren Kumari
Google, Inc.
Email: warren@kumari.net