DNS Glue RR Survey and Terminology Clarification
draft-koch-dns-glue-clarifications-05

Abstract

This document presents a survey of the use of the term "glue record" in DNS related RFCs and proposes a terminology for the various glue policies seen in different top level domains.

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 http://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 September 10, 2015.

Copyright Notice

Copyright (c) 2015 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 (http://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.
1. Introduction

When delegating zones from a top level domain (TLD) or other DNS zone, some additional information is needed when resolving a name server’s (as per an NS RR) address would involve the particular name
server itself. Such a dependency on itself, direct or indirect, may effectively shadow a part of a zone’s NS RRSet, reducing redundancy, or even render the zone completely unresolvable. This additional information is an amendment to the delegation in the form of glue address records. In the real life DNS multiple strategies to determine necessity or acceptance of glue records co-exist. This document lists a subset of those approaches.

This document also tries to clarify when and where to call an address record "glue record".

Comments should be directed at the author.

Domain names and IP addresses herein are for explanatory purposes only and should not be expected to lead to useful information in real life [RFC2606],[RFC5735]).

1.1. Purpose of this Document

XXX gather intelligence, clarify terminology, list name server naming schemes and glue policies, collect glue related operational and protocol considerations.

1.2. RFC Survey

To find out more about early motivations and strategies for DNS glue records, all existing RFCs were automatically searched for the term "glue" (case insensitive, no word boundaries) and those matching were inspected on a case by case basis. Whenever the term was used in a DNS context, the RFC was added to the list which can be found in the References section. It turned out that, while all early RFCs are consistent in using "glue" only for type A address records for NS RR targets, they apply slightly different logic as to when a glue A RR should be present.

2. Terms

When the term "glue record" was introduced in [RFC0973], it was meant to denominate both data origin and purpose. Data origin is related to the zone, although the glue records do not belong to the authoritative zone data. The purpose is constrained to providing address information for name servers mentioned in NS RRs, which would otherwise not be resolvable. Glue records are address information accompanying a delegation (in the delegating zone).

There is sometimes confusion when data in a DNS response is also called "glue" data, e.g. [RFC2010] starts speaking of "fetching" glue. In a DNS response packet (answer or referral) the address
information for name servers is carried in the additional section. This address information might have originated from glue records but might also come from cached or authoritative data. DNS data in response packets should only be called "glue data" when it is certain and needs to be emphasized that it originates from glue records.

[RFC4472] introduces the concept of ’critical’ and ’courtesy’ additional data.

3. Name Server Naming Strategies

The DNS refers to name servers by their name in NS resource records. The servers’ names can have different relations to both the delegating zone and the zone delegated to them. The following categories describe the naming scheme from the perspective of the delegated zone. They will be illustrated with the help of the "example" TLD zone, which delegates the zone "del.example" to the respective sets of name servers.

"in domain": A name server can be within the delegated domain, which includes the name of the delegated domain itself, e.g., "del.example", "dns.del.example", or "dns.sub.del.example". In all but the first case the name might be part of a subzone of "del.example". This naming scheme is sometimes also called "in-bailiwick".

"sibling domain": A name server’s name can be within the delegating but outside the delegated domain, e.g., "dns.other.example". There are two sub-cases here, depending on the treatment of the "other.example" domain:

"authoritative in sibling zone": When the name server’s name is within the parent domain, but in a separate zone, this is a sibling zone of the delegated zone. XXX Strictly speaking, see "grandchild glue", it might be a nephew/niece zone.

"authoritative in parent zone": A name server’s name may also appear authoritative in the parent zone.

"unrelated": A name server’s name may not share its parent with the delegated domain, e.g., "dns.example.org".

The discussion of the advantages and disadvantages of the three categories or any combination is beyond the scope of this document.
4. Glue Policies

In the DNS tree different policies are applied with respect to registering glue with the delegating zone. "Registering" in this case means that the respective glue information is accepted, requested or required and then attached to the zone data so that it is available at all authoritative servers, i.e. the glue travels with the zone data by AXFR, IXFR or other means. However, it does not make the glue data part of the zone’s authoritative data \[RFC5936\].

This is a list of existing glue policies:

- "never" or "null": Glue RRs are never registered. This currently applies to larger parts of the IN-ADDR.ARPA reverse tree.

  XXX but this interacts with naming schemes to be applied.

- "narrow": Glue RRs are registered if and only if the name server resides within or below the delegated (child) zone (that is, within the delegated domain). This was suggested by \[RFC1034\].

- "wide": Glue RRs are registered if and only if the name server resides below the delegating (parent) zone. If the name server’s name belongs to the parent zone, it is part of the authoritative data and thus there is no need to register glue RRs. This was suggested by \[RFC1033\]. It is used for the root zone.

- "case by case": Glue RRs are registered following the "narrow" policy except where there are (circular) dependencies that demand additional glue RRs.

- "mandatory": Glue RRs are always registered for all name servers. This was suggested by \[RFC0973\].

- "other": Combinations of the above may exist, e.g. if a registry runs multiple sibling domains and decides to register glue RRs whenever a name server resides in or below one of the siblings. This category would also include other policies like "random" or "arbitrary".

Glue RRs are needed only in the delegating zone, regardless of glue policy. See Section 5.1 for a discussion of root zone issues.

Various RFCs have identified extraneous glue RRs as sources of error and confusion ([RFC1713], [RFC1912]).
5. Special Considerations

5.1. Root Server "Glue" in the Root Zone File

As said before, Glue is meant to be present in the delegating zone only. The only exception seems to be root zone which also contains the address records for its authoritative name servers. However, with the current setup the root servers also serve the ARPA domain and with the root zone’s "wide" glue policy this means that there should be glue RRs for this particular set of nameservers, but only in their capacity as ARPA TLD servers.

[The position of the A RRs in the root zone file (which has just editorial value) as well as their TTLs suggest that historically there will have been a different reason].

[The upcoming change in the ARPA NS RRSet in the spirit of [RFC5855] renders this consideration void.]

Also, per operational practice, all root servers are authoritative for the zone they reside in and that is today also reflected by the official delegation for the "root-servers.net" zone. So, they have the authoritative data present and do not need to rely upon the data transported with the root zone.

[To have a complete trust chain available at the root servers leading to their own names, it would be useful to have them configured authoritative for all intermediate zones. It has been suggested before to move the root server’s names to a distinct TLD. Another option would be to move their names to e.g. ROOT-SERVERS.ARPA instead.]

5.2. Using Glue records in responses

Some implementations use Glue information not only during additional section processing, but also in the answer section of responses.

Given an excerpt of the "example" TLD zone file,

```
one.example.       NS dns.one.example.
                 NS dns.two.example.
dns.one.example.   A  192.0.2.53
```

what should a name server authoritative for the example TLD do when asked for the A RR for dns.one.example? Some implementations will put the A RR in the answer section of the response, others will respond with a referral and only copy the glue A RR into the
additional section (the handling of dns.two.example’s A RR is not considered here).

Step 4 of the algorithm in 4.3.2 of [RFC1034] suggests that after copying the NS RRs into the authority section (in step 3b) the cache should be consulted and used to fill the answer section. Depending on whether or not Glue data is considered to reside in the cache (it is definitely not authoritative), one or the other response type will be preferred.

With DNSSEC an A RRSet response originating from glue data will always miss the appropriate signature, because neither does the delegating zone sign the glue RRSet nor does a glue RRSIG (child’s signature covering the address RRSet) exist in that delegating zone. [discuss levels of indirection and operational reasons that lead to the "gluepot response"]

5.3. Registry considerations for maintaining Glue RRs

As explained in [RFC5936], Glue address records are "registered with" a zone, but since they fall underneath (or, sometimes, onto) the next zone cut, they are not part of that zone. Depending on the data model and glue policy in use for a TLD ([RFC5731], [RFC5732]), different side effects may be the consequence of undelegating a domain. The standard zone file format does not allow for the explicit dedication of address records as glue information. Instead, the distinction is made based on the presence or absence of zone cuts. If, for example, the "del.example" domain was delegated to, amongst others, the "dns.del.example" name server, an address record for "dns.del.example" in the "example" TLD zone will be interpreted as glue record. After deleting the "del.example" NS RRSet (the delegation) from the "example" zone, the corresponding address record would have to be deleted, as well. Should it remain, it would be elevated to authoritative data, since there no longer is a zone cut. Such an effect might be highly undesirable and should be avoided.

Custom name server software may be able to keep delegation and glue data separate from the authoritative data so that "dns.del.example" would still exist but would not be elevated to authoritative status. However, this effect is similarly undesirable since the address might be used to fill the additional section for referrals containing NS RRs pointing to "dns.del.example", as if "wide" glue policy was in effect.

With the "wide" glue policy, a glue address record registered with some delegation might not even be related to the delegation of its own second level domain, i.e., the corresponding name server does not
have to be part of the NS RRSet for that domain. Therefore, broader checks have to be applied to avoid the aforementioned undesired effects.

5.4. Glue RRs for multihomed name servers

Some name server names resolve to A or AAAA RRSets consisting of more than one record, i.e. they have multiple addresses. It is recommended that these RRSets be consistent between the child and the parent.

Research is needed to evaluate the effective difference between multiple names and multiple addresses for a name server. These effects heavily depend on server selection algorithms in resolvers.

5.5. Grandchild Glue

When a name server resides within the delegated domain, the delegation needs a glue record with both the "wide" and the "narrow" glue policy. However, the server does not necessarily have its name within the delegated zone since it may belong to a child or grandchild zone of the delegated one.

This is a delegation in the example TLD:

one.example. NS one.example.
             NS dns.one.example.
             NS dns.deep.one.example.

Only the first name server is known to have its name in the delegated zone, where the second and third could both be in separate zones. NB: even dns.one.example. could be a zone delegated from one.example.

As a consequence, it cannot be concluded that any such name server is able to authoritatively serve its own name, e.g., if it does not serve the grandchild zone.

5.6. DNSSEC Considerations

DNSSEC signatures do not cover glue records [RFC3833], [RFC4033].

Using the gluepot to fill the answer section is discouraged with DNSSEC, see Section 5.2.
5.7. IPv6 Considerations

While this document makes no explicit statements about AAAA RRs, similar logic applies except in cases where A and AAAA glue RR interaction requires specific consideration (response packet size, TTL consistency, namespace fragmentation).


5.8. Open Issues

Future versions of this document might expand on these topics:

- Software issues when following NS RRs [I-D.minda-dnsop-using-in-bailiwick-nameservers]
- Mixed IPv4 and IPv6 environments, following the example of [RFC4472].
- TTL considerations: glue data vs. authoritative data as well as NS RRSet TTLs vs A RRSet TTLs
- Circular dependencies and "narrow" glue policy

6. Security Considerations

This section needs more work

7. IANA Considerations

This document does not request any IANA action.

The considerations of the DNS root zone glue policy are explanatory only and do not strive to change this policy. The details of ensuring that root name servers can always respond to priming queries not only with the root NS RRSet, but also a sufficient number of root name server addresses, are covered in [I-D.ietf-dnsop-resolver-priming].

[This section needs more work]

8. References
8.1. Normative References


8.2. Informative References


Appendix A.  Extended RFC Survey

At the time of this writing, 80 RFC documents contained the term "glue", XX of which were DNS related. These latter RFCs were individually inspected to establish a historic record of the use of the term "glue", as outlined in the following subsections. Any comments are solely intended to put the respective RFC into context and to point out similarities and differences. This is not an attempt to update the documents under consideration.

Appendix B.  Document Revision History

This section is to be removed should the draft be published.

$Id: draft-koch-dns-glue-clarifications.xml,v 1.12 2015/03/09 20:04:22 pk Exp$
B.4. Changes from -01 to -02

- Added text about grandchild glue
- Maintenance of references, minor edits

B.5. Changes from -00 to -01

- Mentioned RFC survey
- Added text about root server glue
- New text for using glue in responses

Author’s Address

Peter Koch
DENIC eG
Kaiserstrasse 75-77
Frankfurt  60329
DE

Phone: +49 69 27235 0
Email: pk@DENIC.DE