

Network Working Group
Internet-Draft
Updates: [6304](#) (if approved)
Intended status: Experimental
Expires: December 30, 2013

J. Abley
ICANN
B. Dickson
June 28, 2013

AS112 Redirection using DNAME
draft-jabley-dnsop-as112-dname-00

Abstract

Many sites connected to the Internet make use of IPv4 addresses that are not globally unique. Examples are the addresses designated in [RFC 1918](#) for private use within individual sites.

Devices in such environments may occasionally originate Domain Name System (DNS) queries (so-called "reverse lookups") corresponding to those private-use addresses. Since the addresses concerned have only local significance, it is good practice for site administrators to ensure that such queries are answered locally. However, it is not uncommon for such queries to follow the normal delegation path in the public DNS instead of being answered within the site.

It is not possible for public DNS servers to give useful answers to such queries. In addition, due to the wide deployment of private-use addresses and the continuing growth of the Internet, the volume of such queries is large and growing. The AS112 project aims to provide a distributed sink for such queries in order to reduce the load on the IN-ADDR.ARPA authoritative servers. The AS112 project is named after the Autonomous System Number (ASN) that was assigned to it.

The AS112 project does not accommodate the addition and removal of DNS zones elegantly. Since additional zones of definitively local significance are known to exist, this presents a problem. This document describes modifications to the deployment and use of AS112 infrastructure that will allow zones to be added and dropped much more easily.

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 December 30, 2013.

Copyright Notice

Copyright (c) 2013 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.

Table of Contents

1.	Introduction	4
2.	Design Overview	5
3.	AS112 Operations	6
3.1.	Extensions to Support DNAME Redirection	6
3.2.	Redirection of Query Traffic to AS112 Servers	6
4.	Continuity of AS112 Operations	8
5.	Candidate Zones for AS112 Redirection	9
6.	DNAME Deployment Considerations	10
7.	IAB Considerations	11
8.	IANA Considerations	12
8.1.	Address Assignment	12
8.2.	Hosting of AS112.ARPA	12
8.3.	Delegation of AS112.ARPA	13
9.	Security Considerations	14
10.	Acknowledgements	15
11.	References	16
11.1.	Normative References	16
11.2.	Informative References	16
Appendix A.	Updates to RFC6304	17
A.1.	Changes to Section 2.1 , Zones	17
A.2.	Changes to Section 2.2 , Nameservers	17
A.3.	Changes to Section 3.4 , Routing Software	17
A.4.	Changes to Section 3.5 , DNS Software	17
A.5.	Changes to Section 3.6 , Testing a Newly Installed Node	17
A.6.	Changes to Section 6 , On the Future of AS112 Nodes	17
A.7.	Changes to Section 8 , Security Considerations	18
A.8.	Changes to Appendix A , History	18
Appendix B.	Editorial Notes	19
B.1.	Change History	19
	Authors' Addresses	20

1. Introduction

The AS112 project is described in detail in [[RFC6304](#)].

The AS112 nameservers (PRISONER.IANA.ORG, BLACKHOLE-1.IANA.ORG and BLACKHOLE-2.IANA.ORG) are required to answer authoritatively for each and every zone that is delegated to them.

If a zone is delegated to AS112 nameservers without those nameservers being configured ahead of time to answer authoritatively for that zone, there is a detrimental impact on clients following referrals for queries within that zone. This misconfiguration is colloquially known as a "lame delegation".

AS112 nameserver operators are only loosely-coordinated, and hence adding support for a new zone (or, correspondingly, removing support for a zone that is no longer delegated to the AS112 nameservers) is difficult to accomplish with accuracy; testing AS112 nameservers remotely to see whether they are configured to answer authoritatively for a particular zone is similarly challenging since AS112 nodes are distributed using anycast [[RFC4786](#)].

This document proposes that instead of delegating individual zones to AS112 nameservers, DNAME [[RFC6672](#)] redirection be used instead. This approach has the advantage that query traffic for arbitrary parts of the namespace can be directed to AS112 servers without those servers having to be reconfigured every time a zone is added or removed.

2. Design Overview

A new zone, EMPTY.AS112.ARPA, is delegated to a single nameserver BLACKHOLE.AS112.ARPA (IPv4 address TBAv4-1, IPv6 address TBAv6-1).

The IPv4 address TBAv4-1 has been assigned by the IANA such that the address is coverable by a single IPv4 /24 prefix, and that no other address covered by that prefix is in use. The IPv6 address TBAv6-1 has been similarly assigned such that no other address within a covering /48 is in use. This addressing plan accommodates the anycast distribution of the BLACKHOLE.AS112.ARPA service using a single IPv4 service prefix and a single IPv6 service prefix. See [\[RFC4786\]](#) for more discussion of anycast service distribution; see [Section 8](#) for the specific requests this document makes of the IANA.

Some or all of the existing AS112 nodes should be extended to support these new nameserver addresses, and to host the EMPTY.AS112.ARPA zone. See [Section 3.1](#) for guidance to AS112 server operators.

Each part of the DNS namespace for which it is desirable to sink queries at AS112 nameservers should be redirected to the EMPTY.AS112.ARPA zone using DNAME [\[RFC6672\]](#). See [Section 3.2](#) for guidance to zone administrators.

3. AS112 Operations

3.1. Extensions to Support DNAME Redirection

The guidance provided in [[RFC6304](#)] is extended to include configuration of the TBAv4-1, and TBAv6-1 addresses, and the corresponding announcement of covering routes for those addresses, and to host the EMPTY.AS112.ARPA zone.

IPv4-only AS112 nodes should only configure the TBAv4-1 nameserver address; IPv6-only AS112 nodes should only configure the TBAv6-1 nameserver address.

It is only necessary for a single AS112 server operator to implement these extensions for this mechanism to function as intended. It is beneficial if many more than one AS112 server operators make these changes, however, since that provides for greater distribution and capacity for the nameservers serving the EMPTY.AS112.ARPA zone. It is not necessary for all AS112 server operators to make these changes for the mechanism to be viable.

Detailed instructions for the implementation of these extensions is included in [Appendix A](#).

3.2. Redirection of Query Traffic to AS112 Servers

Once the EMPTY.AS112.ARPA zone has been deployed using the nameservers described in [Section 3.1](#), redirections may be installed in the DNS namespace for queries that are intended to be answered by the AS112 infrastructure.

For example, reverse queries corresponding to TEST-NET-1 (192.0.2.0/24) [[RFC5737](#)] could be redirected to AS112 nameservers by installing a DNAME resource record in the 192.IN-ADDR.ARPA zone, as illustrated in Figure 1.

```
@ORIGIN 192.IN-ADDR.ARPA.  
...  
2.0.IN-ADDR.ARPA. IN DNAME EMPTY.AS112.ARPA.  
...
```

Figure 1

There is no practical limit to the number of redirections that can be configured in this fashion. Redirection of a particular part of the namespace to EMPTY.AS112.ARPA can be removed at any time, under the control of the administrators of the corresponding part of the DNS namespace. No changes to deployed AS112 nodes incorporating the

extensions described in this document are required to support additional redirections. A list of possible candidates for AS112 redirection can be found in [Section 5](#).

DNAME resource records deployed for this purpose can be signed with DNSSEC [[RFC4033](#)], providing a secure means of authenticating the legitimacy of each redirection.

4. Continuity of AS112 Operations

Existing guidance to AS112 server operators to accept and respond to queries directed at the PRISONER.IANA.ORG, BLACKHOLE-1.IANA.ORG and BLACKHOLE-2.IANA.ORG nameservers should continue to be followed, and no changes to the delegation of existing zones hosted on AS112 servers should occur. These measures are intended to provide continuity of operations for zones currently delegated to AS112 servers and avoid any accidental client impact due to the changes proposed in this document.

Once it has become empirically and quantitatively clear that the EMPTY.AS112.ARPA zone is well-hosted to the extent that it is thought that the existing, unmodified AS112 servers host 10.IN-ADDR.ARPA, the decision might be made to replace the delegation of those [[RFC1918](#)] zones with DNAME redirection. Once implemented, the PRISONER.IANA.ORG, BLACKHOLE-1.IANA.ORG and BLACKHOLE-2.IANA.ORG nameservers could be retired. This document gives no such direction to the IANA, however.

5. Candidate Zones for AS112 Redirection

All zones listed in [[RFC6303](#)] are candidates for AS112 redirection. No doubt there are many others that are worth mentioning. Future revisions of this draft should mention them.

This document is concerned with provision of the AS112 redirection service, and does not specify that any particular AS112 redirection be put in place.

6. DNAME Deployment Considerations

DNAME was specified a significant time following the original implementations of [\[RFC1035\]](#), and hence universal deployment cannot be expected. [\[RFC6672\]](#) specifies a fall-back mechanism which makes use of synthesised CNAME RRs for this reason.

It is a fundamental design requirement of AS112 service that responses be cached. We can safely declare DNAME support on the authoritative server to be a prerequisite for DNAME redirection, but the cases where individual elements in resolver chains do not support DNAME processing deserve closer examination.

The expected behaviour when a DNAME response is supplied to a resolver that does not support DNAME is that the accompanying, synthesised CNAME will be accepted and cached. Re-query frequency will be determined by the TTLs returned by the DNAME-responding authoritative servers.

Resolution of the CNAME target is straightforward and functions exactly as the AS112 project has operated since it was deployed. The negative caching [\[RFC2308\]](#) of the CNAME target follows the parameters defined in the target zone, EMPTY.AS112.ARPA. This has the side-effects that all redirected names ultimately landing on an AS112 node will be negatively-cached with the same parameters, but this lack of flexibility seems non-contraversial; the effect of reducing the negative cache TTL would be increased query volume on the AS112 node operator concerned, and hence controls seem well-aligned with operation.

Validating resolvers (i.e. those requesting and processing DNSSEC [\[RFC4033\]](#) metadata) are required to implement DNAME, and hence should not make use of synthesised CNAME RRs. The lack of signature over a received CNAME RR should hence not limit the ability to sign the redirection point, and for those signatures to be validated.

In the case where a recursive server implements DNAME, but DNAME is not implemented in a stub resolver, CNAME synthesis will again provide a viable path.

DNAME support on AS112 nodes themselves is never required under this proposal.

7. IAB Considerations

This document proposes a delegation within the ARPA domain, and, in accordance with [[RFC3172](#)], IAB review and approval of the delegation of AS112.ARPA as described in [Section 8](#) is required.

Once IAB approval has been obtained, this section may be removed prior to publication or updated to include text that confirms the IAB's decision, at the IAB's discretion.

8. IANA Considerations

8.1. Address Assignment

The IANA is requested to assign one IPv4 /24 netblock and one IPv6 /48 netblock that, to the best of their knowledge, should be suitable for announcement as a single IPv4 /24 prefix and a single IPv6 prefix on the global Internet, respectively.

Once assigned, all occurrences of TBAv4 in this document should be replaced by the IPv4 netblock assigned, in conventional notation. Occurrences of TBAv4-1 should be replaced with an address from the netblock with lowest octet set to 1. Similarly, all occurrences of TBAv6 in this document should be replaced by the IPv6 netblock assigned, in conventional notation, and TBAv6-1 replaced with an address from that netblock with the lowest 48 bits set to the value 1. Once those changes are made, this paragraph may be removed prior to publication.

The netblocks assigned by the IANA for this purpose are TBAv4 and TBAv6.

8.2. Hosting of AS112.ARPA

The IANA is requested to host and sign the zone AS112.ARPA using nameservers and DNSSEC signing infrastructure of their choosing, as shown in Figure 2. SOA RDATA may be adjusted by the IANA to suit their operational requirements.

```
$ORIGIN AS112.ARPA.
```

```
$TTL 3600
```

```
@      IN      SOA      BLACKHOLE.AS112.ARPA. NOC.DNS.ICANN.ORG. (
                                1              ; serial
                                10800           ; refresh
                                3600            ; retry
                                1209600         ; expire
                                3600 )          ; negative cache TTL
```

```
NS      A.IANA-SERVERS.NET.
```

```
NS      B.IANA-SERVERS.NET.
```

```
NS      C.IANA-SERVERS.NET.
```

```
BLACKHOLE      A      TBAv4-1
```

```
AAAA          TBAv6-1
```

```
EMPTY          NS      BLACKHOLE
```


Figure 2

8.3. Delegation of AS112.ARPA

Once the AS112.ARPA zone is being hosted in production, the IANA is requested to arrange delegation from the ARPA zone according to normal IANA procedure for ARPA zone management, to the nameservers used in carrying out the direction in [Section 8.2](#). The following metadata is suggested for the delegation, but may be changed by the IANA if required:

+-----+-----+	
Name	Value
+-----+-----+	
Domain:	AS112.ARPA
Administrative	Internet Architecture Board (IAB) c/o IETF
Contact:	Administrative Support Activity, ISOC
Technical	Internet Assigned Numbers Authority (IANA)
Contact:	
Nameservers:	As chosen by the IANA, see Section 8.2
DS-RDATA:	As chosen by the IANA, see Section 8.2
+-----+-----+	

9. Security Considerations

This document presents no known additional security concerns to the Internet.

For security considerations relating to AS112 service in general, see [[RFC6304](#)].

10. Acknowledgements

Your name here, etc.

11. References

11.1. Normative References

- [RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", [RFC 2308](#), March 1998.
- [RFC6304] Abley, J. and W. Maton, "AS112 Nameserver Operations", [RFC 6304](#), July 2011.
- [RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", [RFC 6672](#), June 2012.

11.2. Informative References

- [RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), February 1996.
- [RFC3172] Huston, G., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")", [BCP 52](#), [RFC 3172](#), September 2001.
- [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), March 2005.
- [RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", [BCP 126](#), [RFC 4786](#), December 2006.
- [RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", [RFC 5737](#), January 2010.
- [RFC6303] Andrews, M., "Locally Served DNS Zones", [BCP 163](#), [RFC 6303](#), July 2011.

Appendix A. Updates to RFC6304

The following changes are required to [[RFC6304](#)] to provide support for AS112 redirection. It is proposed that a successor document to [[RFC6304](#)] be prepared for joint publication with this document in the interests of providing clear advice to prospective new AS112 operators. The following sub-sections are hence provided mainly only to describe the scope of the changes required for 6304bis, and are not intended for publication in this document. References to this section in this document should ultimately be replaced with references to 6304bis.

A.1. Changes to Section 2.1, Zones

The list of zones that the AS112 nameserver should answer authoritatively for is extended to include EMPTY.AS112.ARPA.

A.2. Changes to Section 2.2, Nameservers

The nameserver BLACKHOLE.AS112.ARPA (IPv4 address TBAv4-1, IPv6 address TBAv6-1) is added to the list of nameserver addresses that the AS112 node should support. The IPv4 prefix TBAv4/24 and the IPv6 prefix TBAv6/48 are added as new prefixes to be originated.

A.3. Changes to Section 3.4, Routing Software

The sample configuration provided in this section is extended to accommodate the IPv4 and IPv6 service prefixes associated with AS112 redirection, TBAv4/24 and TBAv6/48, respectively.

A.4. Changes to Section 3.5, DNS Software

The sample configuration provided in this section is extended to accommodate the TBAv4-1 and TBAv6-1 addresses and the EMPTY.AS112.ARPA zone. The contents of the EMPTY.AS112.ARPA zone should be specified (nameservers differ from that included as "db.empty").

A.5. Changes to Section 3.6, Testing a Newly Installed Node

Testing should be extended to test for correct hosting of the EMPTY.AS112.ARPA zone.

A.6. Changes to Section 6, On the Future of AS112 Nodes

A reference to this document should be included.

[A.7.](#) Changes to [Section 8](#), Security Considerations

Mention should be made that AS112 redirection, as specified in this document, supports DNSSEC in the sense that the DNAME records which signal the redirection can be signed.

[A.8.](#) Changes to [Appendix A](#), History

A reference to this document should be included.

[Appendix B](#). Editorial Notes

This section (and sub-sections) to be removed prior to publication.

[B.1](#). Change History

00 Initial write-up of Brian's idea, circulated for the purposes of entertainment.

Authors' Addresses

Joe Abley
ICANN
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

Phone: +1 519 670 9327
Email: joe.abley@icann.org

Brian Dickson
703 Palmer Drive
Herndon, VA 20170

Email: brian.peter.dickson@gmail.com

