Internet Engineering Task Force (IETF)
Request for Comments: 6303
BCP: 163
Category: Best Current Practice
ISSN: 2070-1721

M. Andrews
ISC

July 2011

Locally Served DNS Zones

Abstract

Experience with the Domain Name System (DNS) has shown that there are a number of DNS zones that all iterative resolvers and recursive nameservers should automatically serve, unless configured otherwise. RFC 4193 specifies that this should occur for D.F.IP6.ARPA. This document extends the practice to cover the IN-ADDR.ARPA zones for RFC 1918 address space and other well-known zones with similar characteristics.

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6303.

Copyright Notice

Copyright (c) 2011 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

Experience with the Domain Name System (DNS, [RFC1034] and [RFC1035]) has shown that there are a number of DNS zones that all iterative resolvers and recursive nameservers SHOULD automatically serve, unless intentionally configured otherwise. These zones include, but are not limited to, the IN-ADDR.ARPA zones for the address space allocated by [RFC1918] and the IP6.ARPA zones for locally assigned unique local IPv6 addresses defined in [RFC4193].

This recommendation is made because data has shown that significant leakage of queries for these namespaces is occurring, despite instructions to restrict them, and because it has therefore become necessary to deploy sacrificial nameservers to protect the immediate parent nameservers for these zones from excessive, unintentional query load [AS112] [RFC6304] [RFC6305]. There is every expectation that the query load will continue to increase unless steps are taken as outlined here.

Additionally, queries from clients behind badly configured firewalls that allow outgoing queries for these namespaces, but drop the responses, put a significant load on the root servers (forward zones but not reverse zones are configured). They also cause operational load for the root server operators, as they have to reply to enquiries about why the root servers are "attacking" these clients. Changing the default configuration will address all these issues for the zones listed in Section 4.

[RFC4193] recommends that queries for D.F.IP6.ARPA be handled locally. This document extends the recommendation to cover the IN-ADDR.ARPA zones for [RFC1918] and other well-known IN-ADDR.ARPA and IP6.ARPA zones for which queries should not appear on the public Internet.

It is hoped that by doing this the number of sacrificial servers [AS112] will not have to be increased, and may in time be reduced.

This recommendation should also help DNS responsiveness for sites that are using [RFC1918] addresses but do not follow the last paragraph in Section 3 of [RFC1918].

1.1. Reserved Words

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. Effects on Sites Using RFC 1918 Addresses

For most sites using [RFC1918] addresses, the changes here will have little or no detrimental effect. If the site does not already have the reverse tree populated, the only effect will be that the name error responses will be generated locally rather than remotely.

For sites that do have the reverse tree populated, most will either have a local copy of the zones or will be forwarding the queries to servers that have local copies of the zone. Therefore, this recommendation will not be relevant.

The most significant impact will be felt at sites that make use of delegations for [RFC1918] addresses and have populated these zones. These sites will need to override the default configuration expressed in this document to allow resolution to continue. Typically, such sites will be fully disconnected from the Internet and have their own root servers for their own non-Internet DNS tree.

3. Changes to Iterative Resolver Behaviour

Unless configured otherwise, an iterative resolver will now return authoritatively (AA=1) name errors (RCODE=3) for queries within the zones in Section 4, with the obvious exception of queries for the zone name itself where SOA, NS, and "no data" responses will be returned as appropriate to the query type. One common way to do this all at once is to serve empty (SOA and NS only) zones.

An implementation of this recommendation MUST provide a mechanism to disable this new behaviour, and SHOULD allow this decision on a zone-by-zone basis.

If using empty zones one SHOULD NOT use the same NS and SOA records as used on the public Internet servers, as that will make it harder to detect the origin of the responses and thus any leakage to the public Internet servers. It is RECOMMENDED that the NS record defaults to the name of the zone and the SOA MNAME defaults to the name of the only NS RR's (Resource Record's) target. The SOA RNAME SHOULD default to "nobody.invalid." [RFC2606]. Implementations SHOULD provide a mechanism to set these values. No address records need to be provided for the nameserver.

Below is an example of a generic empty zone in master file format. It will produce a negative cache Time to Live (TTL) of 3 hours.

```
@ 10800 IN SOA @ nobody.invalid. 1 3600 1200 604800 10800
@ 10800 IN NS @
```

The SOA RR is needed to support negative caching [RFC2308] of name error responses and to point clients to the primary master for DNS dynamic updates.

SOA values of particular importance are the MNAME, the SOA RR's TTL, and the negTTL value. Both TTL values SHOULD match. The rest of the SOA timer values MAY be chosen arbitrarily since they are not intended to control any zone transfer activity.

The NS RR is needed as some UPDATE [RFC2136] clients use NS queries to discover the zone to be updated. Having no address records for the nameserver is expected to abort UPDATE processing in the client.

4. Lists Of Zones Covered

The following subsections are the initial contents of the IANA registry as described in the IANA Considerations section. Following the caveat in that section, the list contains only reverse zones corresponding to permanently assigned address space. The zone name is the entity to be registered.

4.1. RFC 1918 Zones

The following zones correspond to the IPv4 address space reserved in [RFC1918].

Zone
10.IN-ADDR.ARPA
16.172.IN-ADDR.ARPA
17.172.IN-ADDR.ARPA
18.172.IN-ADDR.ARPA
19.172.IN-ADDR.ARPA
20.172.IN-ADDR.ARPA
21.172.IN-ADDR.ARPA
22.172.IN-ADDR.ARPA
23.172.IN-ADDR.ARPA
24.172.IN-ADDR.ARPA
25.172.IN-ADDR.ARPA
26.172.IN-ADDR.ARPA
27.172.IN-ADDR.ARPA
28.172.IN-ADDR.ARPA
29.172.IN-ADDR.ARPA
30.172.IN-ADDR.ARPA
31.172.IN-ADDR.ARPA
168.192.IN-ADDR.ARPA

4.2. RFC 5735 and RFC 5737 Zones

The following zones correspond to those address ranges from [RFC5735] and [RFC5737] that are not expected to appear as source or destination addresses on the public Internet; as such, there are no globally unique names associated with the addresses in these ranges.

The recommendation to serve an empty zone 127.IN-ADDR.ARPA is not an attempt to discourage any practice to provide a PTR RR for 1.0.0.127.IN-ADDR.ARPA locally. In fact, a meaningful reverse mapping should exist, but the exact setup is out of the scope of this document. Similar logic applies to the reverse mapping for ::1 (Section 4.3). The recommendations made here simply assume that no other coverage for these domains exists.

Zone	Description
0.IN-ADDR.ARPA	IPv4 "THIS" NETWORK
127.IN-ADDR.ARPA	IPv4 Loopback NETWORK
254.169.IN-ADDR.ARPA	IPv4 LINK LOCAL
2.0.192.IN-ADDR.ARPA	IPv4 TEST-NET-1
100.51.198.IN-ADDR.ARPA	IPv4 TEST-NET-2
113.0.203.IN-ADDR.ARPA	IPv4 TEST-NET-3
255.255.255.255.IN-ADDR.ARPA	IPv4 BROADCAST

4.3. Local IPv6 Unicast Addresses

The reverse mappings ([RFC3596], Section 2.5 ("IP6.ARPA Domain")) for the IPv6 Unspecified (::) and Loopback (::1) addresses ([RFC4291], Sections 2.4, 2.5.2, and 2.5.3) are covered by these two zones:

Zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.\ 0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.\ 0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA

Note: Line breaks and escapes ('\') have been inserted above for readability and to adhere to line width constraints. They are not parts of the zone names.

4.4. IPv6 Locally Assigned Local Addresses

Section 4.4 of [RFC4193] already required special treatment of:

Zone
D.F.IP6.ARPA

4.5. IPv6 Link-Local Addresses

IPv6 Link-Local Addresses as described in [RFC4291], Section 2.5.6 are covered by four distinct reverse DNS zones:

Zone
8.E.F.IP6.ARPA
9.E.F.IP6.ARPA
A.E.F.IP6.ARPA
B.E.F.IP6.ARPA

4.6. IPv6 Example Prefix

IPv6 example prefix [RFC3849].

Zone
8.B.D.0.1.0.0.2.IP6.ARPA

Note: 8.B.D.0.1.0.0.2.IP6.ARPA is not being used as an example here.

5. Zones That Are Out of Scope

IPv6 site-local addresses (deprecated, see [RFC4291] Sections 2.4 and 2.5.7), and IPv6 non-locally assigned local addresses ([RFC4193]) are not covered here.

It is expected that IPv6 site-local addresses will be self correcting as IPv6 implementations remove support for site-local addresses. However, sacrificial servers for the zones C.E.F.IP6.ARPA through F.E.F.IP6.ARPA may still need to be deployed in the short term if the traffic becomes excessive.

For IPv6 non-locally assigned local addresses (L = 0) [RFC4193], there has been no decision made about whether the Regional Internet Registries (RIRs) will provide delegations in this space or not. If they don't, then C.F.IP6.ARPA will need to be added to the list in Section 4.4. If they do, then registries will need to take steps to ensure that nameservers are provided for these addresses.

IP6.INT was once used to provide reverse mapping for IPv6. IP6.INT was deprecated in [RFC4159] and the delegation removed from the INT zone in June 2006. While it is possible that legacy software continues to send queries for names under the IP6.INT domain, this document does not specify that IP6.INT be considered a local zone.

This document has also deliberately ignored names immediately under the root domain. While there is a subset of queries to the root nameservers that could be addressed using the techniques described here (e.g., .local, .workgroup, and IPv4 addresses), there is also a vast amount of traffic that requires a different strategy (e.g., lookups for unqualified hostnames, IPv6 addresses).

6. IANA Considerations

IANA has established a registry of zones that require this default behaviour. The initial contents of this registry are defined in Section 4. Implementors are encouraged to periodically check this registry and adjust their implementations to reflect changes therein.

This registry can be amended through "IETF Review" as per [RFC5226]. As part of this review process, it should be noted that once a zone is added it is effectively added permanently; once an address range starts being configured as a local zone in systems on the Internet, it will be impossible to reverse those changes.

IANA should coordinate with the RIRs to ensure that, as DNS Security (DNSSEC) is deployed in the reverse tree, delegations for these zones are made in the manner described in Section 7.

7. Security Considerations

During the initial deployment phase, particularly where [RFC1918] addresses are in use, there may be some clients that unexpectedly receive a name error rather than a PTR record. This may cause some service disruption until their recursive nameserver(s) have been re-configured.

As DNSSEC is deployed within the IN-ADDR.ARPA and IP6.ARPA namespaces, the zones listed above will need to be delegated as insecure delegations, or be within insecure zones. This will allow DNSSEC validation to succeed for queries in these spaces despite not being answered from the delegated servers.

It is recommended that sites actively using these namespaces secure them using DNSSEC [RFC4035] by publishing and using DNSSEC trust anchors. This will protect the clients from accidental import of unsigned responses from the Internet.

8. Acknowledgements

This work was supported by the US National Science Foundation (research grant SCI-0427144) and DNS-OARC.

9. References

9.1. Normative References

[RFC1034] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", STD 13, RFC 1035, November 1987.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

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

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, March 1998.

[RFC2606] Eastlake 3rd, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, June 1999.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC4159] Huston, G., "Deprecation of "ip6.int"", BCP 109, RFC 4159, August 2005.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

9.2. Informative References

[AS112] "AS112 Project", <http://www.as112.net/>.

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, July 2004.

[RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", BCP 153, RFC 5735, January 2010.

[RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation", RFC 5737, January 2010.

[RFC6304] Abley, J. and W. Maton, "AS112 Nameserver Operations", RFC 6304, July 2011.

[RFC6305] Abley, J. and W. Maton, "I'm Being Attacked by PRISONER.IANA.ORG!", RFC 6305, July 2011.

Author's Address

Mark P. Andrews
Internet Systems Consortium
950 Charter Street
Redwood City, CA 94063
US

EMail: marka@isc.org