Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: September 3, 2007

M. Andrews
ISC

March 2, 2007

Locally-served DNS Zones
draft-ietf-dnsop-default-local-zones-01

Status of this Memo

Copyright Notice

Abstract

Practice has shown that there are a number of DNS zones all iterative resolvers and recursive nameservers should, unless configured otherwise, automatically serve. RFC 4193 already 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 usage constraints.

Table of Contents

1. Introduction

Practice has shown that there are a number of DNS [RFC 1034] [RFC 1035] zones all iterative resolvers and recursive nameservers should, unless configured otherwise, automatically serve. These zones include, but are not limited to, the IN-ADDR.ARPA zones for the address space allocated by [RFC 1918] and the IP6.ARPA zones for locally assigned local IPv6 addresses, [RFC 4193].

This recommendation is made because data has shown that significant leakage of queries for these name spaces is occurring, despite instructions to restrict them, and because sacrificial name servers have been deployed to protect the immediate parent name servers for these zones from excessive, unintentional, query load [AS112]. 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 but drop responses for these name spaces also puts a significant load on the root servers. They also cause operational load for the root server operators as they have to reply to queries about why the root servers are "attacking" these clients. Changing the default configuration will address all these issues for the zones listed below in Section 4.

[RFC 4193] already recommends that queries for D.F.IP6.ARPA be handled locally. This document extends the recommendation to cover the IN-ADDR.ARPA zones for [RFC 1918] 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.

It should also help DNS responsiveness for sites which are using [RFC 1918] addresses but do not follow the last paragraph in section 3 of

[RFC 1918].

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 [RFC 2119].

2. Effects on sites using RFC 1918 addresses.

For most sites using [RFC 1918] 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 answers are 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 which have local copies of the zone. In either case the local resolver has a pre-existing configuration for the namespace and won't add the automatic zone.

The main impact will be felt at sites that make use of delegation for reverse lookups for [RFC 1918] addresses and have populated these zones. Typically, such sites will be fully disconnected from the Internet and have their own root servers for their own non-Internet DNS tree. These sites will need to override the default configuration expressed in this document to allow resolution to continue.

3. Changes to Iterative Resolver Behaviour.

Unless configured otherwise, an iterative resolver will now return name errors (RCODE=3) for queries within the lists of zones covered below, 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 is to serve empty (SOA and NS only) zones.

A implementation doing this MUST provide a mechanism to disable this

new behaviour, preferably 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 leakage to the public Internet servers. This document recommends 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 target. The SOA RNAME should default to ".". Implementations SHOULD provide a mechanism to set these values. No address records need to be provided for the name server.

Below is a example of a generic empty zone in master file format. It will produce a negative cache ttl of 3 hours.

```
@ 10800 IN SOA @ . 1 3600 1200 604800 10800
@ 10800 IN NS @
```

The SOA RR is needed to support negative caching [RFC 2308] 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 it they are not intended to control any zone transfer activity.

The NS RR is needed as some UPDATE clients use NS queries to discover they zone to be updated. Having no address records for the name server should abort UPDATE processing in the client

4. Lists Of Zones Covered

The lists below are expected to seed a IANA registry.

4.1. RFC 1918 Zones

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 3330 Zones

See [RFC 3330].

```
0.IN-ADDR.ARPA /* IPv4 "THIS" NETWORK */
127.IN-ADDR.ARPA /* IPv4 LOOP-BACK NETWORK */
254.169.IN-ADDR.ARPA /* IPv4 LINK LOCAL */
2.0.192.IN-ADDR.ARPA /* IPv4 TEST NET */
255.255.255.255.IN-ADDR.ARPA /* IPv4 BROADCAST */
```


4.3. Local IPv6 Unicast Addresses

See [RFC 4291], sections 2.4, 2.5.2 and 2.5.3.

```
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.IP
6.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.IP
6.ARPA
```

4.4. IPv6 Locally Assigned Local Addresses

See [RFC 4193].

```
D.F.IP6.ARPA
```

4.5. IPv6 Link Local Addresses

See [RFC 4291], sections 2.4 and 2.5.6.

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

5. Zones that are Out-Of-Scope

IPv6 site-local addresses, [RFC 4291] sections 2.4 and 2.57, and IPv6 Globally Assigned Local [RFC 4193] addresses 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 C.E.F.IP6.ARPA to F.E.F.IP6.ARPA may still need to be deployed in the short term if the traffic becomes excessive.

For IPv6 Globally Assigned Local addresses [RFC 4291] there has been no decision made about whether the registries 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 above. If they do, then registries will need to take steps to ensure that name servers are provided for these addresses.

This document is also ignoring IP6.INT. IP6.INT has been wound up with only legacy resolvers now generating reverse queries under IP6.INT.

This document has also deliberately ignored names immediately under the root. While there is a subset of queries to the roots which

could be addressed using the techniques described here (e.g. .local and IPv4 addresses) there is also a vast amount of traffic that requires a different strategy (e.g. lookups for unqualied hostnames, IPv6 addresses).

6. IANA Considerations

This document recommends that IANA establish a registry of zones which require this default behaviour, the initial contents of which are in Section 4. More zones are expected to be added, and possibly deleted from this registry over time. Name server implementors are encouraged to check this registry and adjust their implementations to reflect changes therein.

This registry can be amended through "IETF Consensus" as per [RFC 2434] or IETF Review in 2434bis.

IANA should co-ordinate with the RIRs and ICANN to ensure the DNSSEC deployment in the reverse trees that these zone are delegated in a unsecure manner as per Security Considerations.

7. Security Considerations

During the initial deployment phase, particularly where [RFC 1918] 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 full service resolvers have been re-configured.

When DNSSEC is deployed within the IN-ADDR.ARPA and IP6.ARPA namespaces, the zones listed above will need to be delegated as insecure delegations. 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 [RFC 4035] by publishing and using DNSSEC trust anchors. This will protect the clients from accidental leakage of unsigned answers 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

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

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

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

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

[RFC 2308]
Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2398, March 1998.

[RFC 2434]
Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC 3330]
"Special-Use IPv4 Addresses", RFC 3330, September 2002.

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

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

9.2. Informative References

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

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

Addresses", RFC 4193, October 2005.

Appendix A. Change History [To Be Removed on Publication]

A.1. draft-ietf-dnsop-default-local-zones-01.txt

Revised impact description.

Updated to reflect change in IP6.INT status.

A.2. draft-ietf-dnsop-default-local-zones-00.txt

Adopted by DNSOP.

"Author's Note" re-titled "Zones that are Out-Of-Scope"

Add note that these zone are expected to seed the IANA registry.

Title changed.

A.3. draft-andrews-full-service-resolvers-03.txt

Added "Proposed Status".

A.4. draft-andrews-full-service-resolvers-02.txt

Added 0.IN-ADDR.ARPA.

Appendix B. Proposed Status [To Be Removed on Publication]

This Internet-Draft is being submitted for eventual publication as an RFC with a proposed status of Best Current Practice.

Author's Address

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

Email: Mark_Andrews@isc.org

Full Copyright Statement

Intellectual Property

ietf-ipr@ietf.org.

Acknowledgment

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