           Configuration Issues Facing Full Service DNS Resolvers
                 In The Presence of Private Network Addressing
                   draft-andrews-full-service-resolvers-00.txt

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   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."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt.

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on February 19, 2006.

Copyright Notice

Abstract

   Practice has shown that there are a number of zones all full service
   resolvers should, unless configured otherwise, automatically serve.
   [draft-ietf-ipv6-unique-local-addr] already specifies that this
   should occur for D.F.IP6.ARPA. This document extends the practice to
   cover the IN-ADDR.ARPA zones for RFC1918 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 zones all full service
resolvers 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 [RFC1918] and the IP6.ARPA zones
for locally assigned local IPv6 addresses, [draft-ietf-ipv6-unique-
local-addr].

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 below.

[draft-ietf-ipv6-unique-local-addr] 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 [RFC1918] and
other well known IN-ADDR.ARPA and IP6.ARPA zones for which queries
should not appear on the 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
[RFC1918] addresses but are misconfigured.

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 RFC1918 addresses.

Sites using [RFC1918] addresses should already be serving these
queries internally, without referring them to public name servers on
the Internet.

The main impact will be felt on sites that make use of recursion for
reverse lookups for [RFC1918] 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 or make use of local delegation overrides (otherwise known
as "forwarding") to reach the private servers for these reverse
zones. These sites will need to override the default configuration
proposed in this draft to allow resolution to continue.

Other sites that use [RFC1918] addresses and either have local copies
of the reverse zones or don't have reverse zones configured should
see no difference other than the name error appearing to come from a
different source.

3. Changes To Full Service Resolver Behaviour.

Unless configured otherwise, a full service resolver will return name
errors for queries within the list of zones covered below. One
common way to do this is to serve empty (SOA and NS only) zones.

A server doing this MUST provide a mechanism to disable this
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 from the public Internet servers. This document
recommends that the NS record default to the name of the zone and the
SOA MNAME default to the name of the zone. 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.

e.g.
     @ 10800 IN SOA @ . 1 3600 1200 604800 10800
     @ 10800 IN NS @

4. List Of Zones Covered.

4.1. RFC1918 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. RFC3330 Zones

    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 Uni-cast Addresses

    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.\

   IP6.ARPA

[4.4](). IPv6 Locally Assigned Local Address

   D.F.IP6.ARPA

[4.5](). IPv6 Link Local Addresses

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

[5](). Author's Note:

   IPv6 site-local addresses and IPv6 Globally Assigned Local 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 howsever, 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 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 the IP6.INT counterpart for the
   IP6.ARPA addresses above. IP6.INT is in the process of being wound
   up with clients already not querying for this suffix.

   This document has also deliberately ignored zones immediately under
   the root. The author believes other methods would be more applicable
   for dealing with the excess / bogus traffic these generate.

IANA Considerations

   This document recommends that IANA establish a registry of zones
   which require this default behaviour, the initial contents are above.
   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.

Security Considerations

   During the initial deployment phase, particularly where [RFC1918]

addresses are in use, there may be some clients that unexpectedly
receive 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. This is good just on general principles. It will
also protect the clients from accidental leakage of answers from the
Internet which will be unsigned.

6. Acknowledgements

References

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

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

Informative References

[draft-ietf-ipv6-unique-local-addr]
           Hinden, R., Haberman, B., "Unique Local IPv6 Unicast
           Addresses", draft-ietf-ipv6-unique-local-addr-09.txt,
           work-in-progress, January 2005.

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

Author's Address:

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

   Email: Mark_Andrews@isc.org