            Representing Internet Protocol version 6 (IPv6)
                Addresses in the Domain Name System (DNS)

Status of this Memo

Copyright Notice

Abstract

   This document clarifies and updates the standards status of RFCs that
   define direct and reverse map of IPv6 addresses in DNS. This
   document moves the A6 and Bit label specifications to experimental
   status.

1. Introduction

   The IETF had begun the process of standardizing two different address
   formats for IPv6 addresses AAAA [RFC1886] and A6 [RFC2874] and both
   are at proposed standard. This had led to confusion and conflicts on
   which one to deploy. It is important for deployment that any
   confusion in this area be cleared up, as there is a feeling in the
   community that having more than one choice will lead to delays in the
   deployment of IPv6. The goal of this document is to clarify the
   situation.

   This document also discusses issues relating to the usage of Binary
   Labels [RFC 2673] to support the reverse mapping of IPv6 addresses.

   This document is based on extensive technical discussion on various
   relevant working groups mailing lists and a joint DNSEXT and NGTRANS
   meeting at the 51st IETF in August 2001. This document attempts to
   capture the sense of the discussions and reflect them in this
   document to represent the consensus of the community.

The main arguments and the issues are covered in a separate document
[RFC3364] that reflects the current understanding of the issues.
This document summarizes the outcome of these discussions.

The issue of the root of reverse IPv6 address map is outside the
scope of this document and is covered in a different document
[RFC3152].

1.1 Standards Action Taken

This document changes the status of RFCs 2673 and 2874 from Proposed
Standard to Experimental.

2.   IPv6 Addresses: AAAA RR vs A6 RR

Working group consensus as perceived by the chairs of the DNSEXT and
NGTRANS working groups is that:

a) AAAA records are preferable at the moment for production
   deployment of IPv6, and

b) that A6 records have interesting properties that need to be better
   understood before deployment.

c) It is not known if the benefits of A6 outweigh the costs and
   risks.

2.1 Rationale

There are several potential issues with A6 RRs that stem directly
from the feature that makes them different from AAAA RRs: the ability
to build up addresses via chaining.

Resolving a chain of A6 RRs involves resolving a series of what are
nearly-independent queries. Each of these sub-queries takes some
non-zero amount of time, unless the answer happens to be in the
resolver's local cache already. Other things being equal, we expect
that the time it takes to resolve an N-link chain of A6 RRs will be
roughly proportional to N. What data we have suggests that users are
already impatient with the length of time it takes to resolve A RRs
in the IPv4 Internet, which suggests that users are not likely to be
patient with significantly longer delays in the IPv6 Internet, but
terminating queries prematurely is both a waste of resources and
another source of user frustration. Thus, we are forced to conclude
that indiscriminate use of long A6 chains is likely to lead to
increased user frustration.

The probability of failure during the process of resolving an N-link
A6 chain also appears to be roughly proportional to N, since each of
the queries involved in resolving an A6 chain has roughly the same
probability of failure as a single AAAA query.

Last, several of the most interesting potential applications for A6
RRs involve situations where the prefix name field in the A6 RR
points to a target that is not only outside the DNS zone containing
the A6 RR, but is administered by a different organization entirely.
While pointers out of zone are not a problem per se, experience both
with glue RRs and with PTR RRs in the IN-ADDR.ARPA tree suggests that
pointers to other organizations are often not maintained properly,
perhaps because they're less susceptible to automation than pointers
within a single organization would be.

2.2 Recommended Standard Action

Based on the perceived consensus, this document recommends that RFC
1886 stay on standards track and be advanced, while moving RFC 2874
to Experimental status.

3. Bitlabels in the Reverse DNS Tree

RFC 2673 defines a new DNS label type. This was the first new type
defined since RFC 1035 [RFC1035]. Since the development of 2673 it
has been learned that deployment of a new type is difficult since DNS
servers that do not support bitlabels reject queries containing bit
labels as being malformed. The community has also indicated that
this new label type is not needed for mapping reverse addresses.

3.1 Rationale

The hexadecimal text representation of IPv6 addresses appears to be
capable of expressing all of the delegation schemes that we expect to
be used in the DNS reverse tree.

3.2 Recommended Standard Action

RFC 2673 standard status is to be changed from Proposed to
Experimental. Future standardization of these documents is to be
done by the DNSEXT working group or its successor.

4. DNAME in IPv6 Reverse Tree

   The issues for DNAME in the reverse mapping tree appears to be
   closely tied to the need to use fragmented A6 in the main tree: if
   one is necessary, so is the other, and if one isn't necessary, the
   other isn't either. Therefore, in moving RFC 2874 to experimental,
   the intent of this document is that use of DNAME RRs in the reverse
   tree be deprecated.

5. Acknowledgments

   This document is based on input from many members of the various IETF
   working groups involved in this issues. Special thanks go to the
   people that prepared reading material for the joint DNSEXT and
   NGTRANS working group meeting at the 51st IETF in London, Rob
   Austein, Dan Bernstein, Matt Crawford, Jun-ichiro itojun Hagino,
   Christian Huitema. Number of other people have made number of
   comments on mailing lists about this issue including Andrew W.
   Barclay, Robert Elz, Johan Ihren, Edward Lewis, Bill Manning, Pekka
   Savola, Paul Vixie.

6. Security Considerations

   As this document specifies a course of action, there are no direct
   security considerations. There is an indirect security impact of the
   choice, in that the relationship between A6 and DNSSEC is not well
   understood throughout the community, while the choice of AAAA does
   leads to a model for use of DNSSEC in IPv6 networks which parallels
   current IPv4 practice.

7. IANA Considerations

   None.

Normative References

   [RFC1035] Mockapetris, P., "Domain Names - Implementation and
              Specification", STD 13, RFC 1035, November 1987.

   [RFC1886] Thompson, S. and C. Huitema, "DNS Extensions to support IP
              version 6", RFC 1886, December 1995.

   [RFC2673] Crawford, M., "Binary Labels in the Domain Name System",
              RFC 2673, August 1999.

   [RFC2874] Crawford, M. and C. Huitema, "DNS Extensions to Support
              IPv6 Address Aggregation and Renumbering", RFC 2874, July
              2000.

   [RFC3152]   Bush, R., "Delegation of IP6.ARPA", BCP 49, RFC 3152
               August 2001.

Informative References

   [RFC3364]   Austein, R., "Tradeoffs in Domain Name System (DNS)
               Support for Internet Protocol version 6 (IPv6)", RFC 3364,
               August 2002.

Editors' Addresses

   Randy Bush
   EMail: randy@psg.com

   Alain Durand
   EMail: alain.durand@sun.com

   Bob Fink
   EMail: fink@es.net

   Olafur Gudmundsson
   EMail: ogud@ogud.com

   Tony Hain
   EMail: hain@tndh.net

Full Copyright Statement

Acknowledgement