v6ops
Internet-Draft
Intended status: Informational
Expires: April 13, 2019

C. Byrne
T-Mobile USA
J. Palet Martinez
The IPv6 Company

October 10, 2018

IPv6-Ready DNS/DNSSSEC Infrastructure
draft-bp-v6ops-ipv6-ready-dns-dnssec-00

Abstract

This document defines the timing for implementing a worldwide IPv6-Ready DNS and DNSSEC infrastructure, in order to facilitate the global IPv6-only deployment.

A key issue for this, is the need for a global support of DNSSEC and DNS64, which in some scenarios do not work well together. This document states that any DNSSEC signed resources records should include a native IPv6 resource record as the most complete and expedient path to solve any deployment conflict with DNS64 and DNSSEC

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 https://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 April 13, 2019.

Copyright Notice

Copyright (c) 2018 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 (https://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

One of the main issues to ensure the best path for the IPv4 to IPv6 transition and the support of an IPv6-only Internet, is to ensure that all the services remain accessible by means of DNS.

One of the alternatives is the use of NAT64 ([RFC6146]) and DNS64 ([RFC6147]), sometimes by means 464XLAT ([RFC6877]), which will help to ensure that, when a network or part of it, becomes IPv6-only, still can have access to IPv4-only resources.

DNS64 ([RFC6147]) is a widely deployed technology allowing hundreds of millions of IPv6-only hosts/networks to reach IPv4-only resources. DNSSEC is a technology used to validate the authenticity of information in the DNS, however, as DNS64 ([RFC6147]) modifies DNS answers and DNSSEC is designed to detect such modifications, DNS64 ([RFC6147]) can break DNSSEC in some circumstances.

Furthermore, the deployment of those transition mechanisms means that the cost of the transition is on the back of the service provider, because the investment required in the devices that take care of that transition services and the support of the helpdesks to resolve issues. So in the end, all that cost is indirectly charged to the end-user, which is unfair.

It seems obvious that should not be that way, and the end-goal is a situation where we get rid-off IPv4-only services, and meanwhile, the

cost borne by the IPv4 laggards operating those services.

This document provides the steps to be able to tackle that situation and advance with the global IPv6 deployment in a fair way.

The document also states that the most complete and expedient path to avoid any negative interactions is, for the DNSSEC signed resources, to always include IPv6 AAAA resources records. As stated in [RFC6540], IPv6 [RFC8200] is not optional and failing to support IPv6 may result in failure to communicate on the Internet, especially when DNSSEC signed IPv4-only resources are present.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. The Conflict Between DNS64 and DNSSEC

DNS64 ([RFC6147]) is a key part of widely deployed IPv6-only transition mechanism such as 464XLAT ([RFC6877]) and Happy Eyeballs version 2 ([RFC8305]). Currently, hundreds of millions of hosts rely on DNS64 ([RFC6147]) for access to the Internet. A core function of DNS64 ([RFC6147]) is generating an inauthentic AAAA DNS record when an authentic AAAA DNS record for a host is not available from the authoritative nameserver. DNSSEC's fundamental feature is detecting and denying inauthentic DNS resource records. While DNS64 ([RFC6147]) outlines may work in harmony with DNSSEC, the preconditions may not always exist for harmony to be achieved.

4. Resolving the DNS64 and DNSSEC Conflict by Requiring AAAA

DNS64 ([RFC6147]) and DNSSEC are both important components of the current and future Internet. The limitation for how these protocols interact is unlikely to changes. Deploying DNSSEC and IPv6 are both commonly achievable for a typical Internet system operator using their own systems or using a third-party service. The resolution to the DNS64 ([RFC6147]) and DNSSEC conflict is to simply deploy both, IPv6 and DNSSEC in tandem.

Deploying DNSSEC signed IPv4 resources records without matching IPv6 records is a risk and not recommend.

Ultimately, this guidance is simply restating [RFC6540], that IPv6 is mandatory for all Internet systems.

5. Ensuring a smooth IPv4-IPv6 transition by Requiring AAAA

Similarly, to what is stated in the precedent section for DNS64 ([RFC6147]) and DNSSEC, a smoother and less painful transition from IPv4 to IPv6, and the succesful deployment of an IPv6-only Internet, can be facilitated by requiring AAAA resource records at every DNS instance.

6. Definition of IPv6-Ready DNS/DNSSEC Infrastructure

In the context of this document, and others that may be generated as a consequence of it, "IPv6-Ready DNS/DNSSEC Infrastructure" means that a DNS/DNSSEC server (root, TLD, authoritative NS, others) is fully accessible and operational if queried either from a remote dual-stack network or an IPv6-only network.

In general, that means having AAAA RRs in addition to A RRs, ensuring that PMTUD works correctly and fragmentation is correctly handled.

In case DNSSEC is implemented with IPv4, it MUST support also IPv6-only operation according the above considerations.

7. Implementation timing

Towards the implementation of the worldwide IPv6-Ready DNS/DNSSEC infrastructure, considering that there are no excuses for a DNS operator to support IPv6, the following deadlines are defined counting since the date this document becomes an RFC:

1. All the root and TLDs MUST be IPv6-Ready in 6 months.

2. All the DNSSEC signed zones MUST be IPv6-Ready in 6 months.

3. All the authoritative NS MUST be IPv6-Ready in 12 months.

4. The remaining RRs in other DNS servers, MUST be IPv6-Ready in 18 months.

Probing mechanisms to verify that the relevant AAAA are fully operational MUST be setup by IANA. If there is a failure at the deadline in complying with those requirements, the relevant NS, MUST be temporarily suspended until there is a subsequent successful verification.

8. Security Considerations

DNSSEC is a good security practice. Providing AAAA DNSSEC signed records wherever a DNSSEC signed A record is used ensures the most effective use of DNSSEC.

9. IANA Considerations

IANA and ICANN are instructed by means of this document, to take the relevant measures for ensuring the steps towards the above indicated implementation timing.

It is suggested that frequent warnings are provided to the relevant stakeholders, in advance to each of the deadlines.

10. Acknowledgements

The author would like to acknowledge the inputs of ... TBD.

11. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, DOI 10.17487/RFC6147, April 2011, <https://www.rfc-editor.org/info/rfc6147>.

[RFC6540] George, W., Donley, C., Liljenstolpe, C., and L. Howard, "IPv6 Support Required for All IP-Capable Nodes", BCP 177, RFC 6540, DOI 10.17487/RFC6540, April 2012, <https://www.rfc-editor.org/info/rfc6540>.

[RFC6877] Mawatari, M., Kawashima, M., and C. Byrne, "464XLAT: Combination of Stateful and Stateless Translation", RFC 6877, DOI 10.17487/RFC6877, April 2013, <https://www.rfc-editor.org/info/rfc6877>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8305] Schinazi, D. and T. Pauly, "Happy Eyeballs Version 2: Better Connectivity Using Concurrency", RFC 8305, DOI 10.17487/RFC8305, December 2017, <https://www.rfc-editor.org/info/rfc8305>.

Authors' Addresses

Cameron Byrne
T-Mobile USA
Bellevue, WA
United States of America

Email: Cameron.Byrne@T-Mobile.com

Jordi Palet Martinez
The IPv6 Company
Molino de la Navata, 75
La Navata - Galapagar, Madrid 28420
Spain

Email: jordi.palet@theipv6company.com
URI: http://www.theipv6company.com/