

sunset4
Internet-Draft
Intended status: Standards Track
Expires: May 27, 2018

J. Palet Martinez
The IPv6 Company
November 23, 2017

Towards a Worldwide IPv6-Ready DNS Infrastructure
draft-palet-sunset4-ipv6-ready-dns-00

Abstract

This document defines the timing for implementing an IPv6-Ready global DNS infrastructure, worldwide, in order to allow the global IPv6-only deployment.

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 May 27, 2018.

Copyright Notice

Copyright (c) 2017 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	2
2.	Definition of IPv6-Ready DNS Infrastructure	2
3.	Implementation timing	3
4.	Security Considerations	3
5.	IANA Considerations	3
6.	Acknowledgements	4
7.	Normative References	4
	Author's Address	4

[1.](#) Introduction

The sunset4 WG is working to define the complete transition of Internet to IPv6, covering a wide range of aspects, horizontal to several IETF areas.

One of the main issues is to ensure that, when IPv4 is shutdown, or even during the transition phase towards that goal, all the services remain accesible by means of DNS.

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

However, as DNS64 modifies DNS answers and DNSSEC is designed to detect such modifications, DNS64 can break DNSSEC.

Furthermore, the deployment of those transition mechanism 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 call-centers 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.

[2.](#) Definition of IPv6-Ready DNS Infrastructure

In the context of this document, and others that may be generated as a consequence of it, "IPv6-Ready DNS Infrastructure" means that a DNS server (root, TLD, authoritative NS) is fully accesible and

operational if queried from a remote dual-stack and 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 below defined timing.

3. Implementation timing

Towards the implementation of the worldwide IPv6-Ready DNS infrastructure, the following deadlines are defined counting since the date this document becomes an RFC:

1. Root and TLDs MUST be IPv6-Ready in 6 months.
2. Authoritative NS MUST be IPv6-Ready in 12 months.
3. DNSSEC authoritative MUST be IPv6-Ready in 18 months.
4. Other A RRs, MUST be IPv6-Ready in 24 months.
5. Other RRs, MUST be IPv6-Ready in 30 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.

4. Security Considerations

This document does not have any new specific security considerations.

5. IANA Considerations

IANA/ICANN is 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.

6. Acknowledgements

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

7. Normative References

- [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>>.

Author's Address

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/>

