Sunset4 Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 23, 2015

D. Song
BII
D. Ma
ZDNS
July 22, 2014

Considerations on IPv6-only DNS
draft-davey-sunset4-ipv6onlydns-00

Abstract

Domain name system (DNS)is a key Internet infrastructure service connecting the IP layer and the identifier layer of Internet. This memo describe the behavior and inherent limitation of DNS in IPv4 and dual-stack environment. To ease the problem as well as bringing some incentive to turn off IPv4 as soon as possible, this memo is intended to introduce potential solutions to make some changes on DNS protocol and operation practice in the IPv6 only network.

Table of Contents

1. Introduction

Domain name system (DNS) is a key Internet infrastructure service connecting the IP layer and the identifier layer. It works well for many years with high scalability to support the Internet explosion in IPv4 environment with its original design. However, when new technologies such as IPv6, DNSSEC as well as complicated and unpredictable mid-box/end system implementation introduced to the Internet, the original design of DNS need to be reexamined to meet new requirements.

This memo describes the behavior and inherent limitation of DNS focusing on networking aspect. Along with Internet development, for example in IPv6 transition, some problems emerge and seems hard to be solved. To ease the problem as well as bringing some incentive to turn off IPv4 as soon as possible, this memo is intended to introduce potential solutions to make some changes on DNS protocol and fixed operation practice in the newly developed IPv6 only network.

Note that this memo is written with a joint background of global IPv6 transition. Although significant growth of IPv6 traffic is observed in some pioneer companies [1] and regions, the low IPv6 penetration worldwide indicates that IPv6 is far from fully launched. So to accelerate the transition to a fully connected IPv6 network as soon as possible is one of the requirement this memo want to meet.

Note that some problem and discussion in this memo are not exclusive in IPv6 context. The authors hope new DNS protocol or changes takes full consideration of IPv6-only capability. So the discussion in this memo is in line with the topics both in IETF dnsop and sunset4 WG.

2. Problem Statement

There are three aspects about inherent limitation of DNS in IPv4 and dual-stack environment:

2.1. IPv4 Fallback Problem

When IPv6 is introduce to DNS RFC4772[2], DNS keep the independence of DNS transport protocol and DNS records. Based on this setting, it is feasible to cause IPv4 fallback problem RFC6555 [3] when IPv4-only capable clients use IPv4 connection to query AAAA RR and launch IPv6 connection firstly with bad experience afterwards. It may be caused by the diversity or misconfiguration of end system and stub network. But, it makes little sense for IPv4-only capable users to see IPv6 Internet. In addition, when people decide to turn off IPv4 in their network, how global or local DNS system adjust to the new setting is not discussed fully yet.

2.2. DNS Referral Reaponse Size Issues

This issue is fully described by [4]. Due to the required minimum IP reassembly limit for IPv4, the original DNS standard limited the UDP message size to 512 octets which became ahistorical and practical hard DNS protocol limit, no matter new protocol like IPv6 and EDNS0 RFC6891 [5] introduced. This limit presents some special problems for zones wishing to (1) add more authority servers or (2) advertise the IPv6 addresses of newly updated dual-stack NS name servers, (3) use DNSSEC.

2.3. Scalability on Root Server System

Due to the DNS Referral Response Size Issues, in the early day of Internet, the number of root server is limited to 13. Due to various reasons, this 13 pattern hinder the wide distribution of root zone file as a crucial Internet infrastructure services which is ought to be pervasive. In addition, the uneven distribution of Root server operators also cause heated dispute and distrust.

The problems above is being discussed and solved case by case in IETF community, such as happy eyeballs [3] for IPv4 fall back and EDNS0 [5] for DNS hard limit, Universal anycast [6] for scalability of Root server system. But each of them needs time and effort for wide

separate acceptance and deployment. Instead, this memo trying to answer the question by the virtue of IPv6 along the wave of IPv6 development, especially in IPv6-only context.

3. Proposed Ideas

This section is intended to explore the feasibility to make some changes on DNS protocol and operation practice in the network turning off IPv4 or newly developed IPv6 only network. Specific solutions are proposed as following to answer the problem listed in section 2.

3.1. Separate IPv6 and IPv4 in DNS

To counter the problem describe in section 2.1, one possible approach is to logically separateIPv6 and IPv4 in DNS RR, which means query from IPv4 connection get response with only IPv4-related RR information, vice versa. There is an alternative is to donate a large amount of public DNS servers with only IPv6 connectivity (indicated by the presence of AAAA records) and no IPv4 connectivity (as indicated by the absence of A records) which only server the IPv6 users.

This proposal will introduce new kinds of split-view of DNS dependent on transport protocol. Analysis and test should be done on the coordination between IPv4/IPv6 DNS split-view and DNSSEC deployment with two different content of zone files in the DNS system which may introduce complication involving different ZSK for each zone file.

3.2. IPv6-aware DNS Referral Response Mechanism

In section 2.2, due to the limitation of DNS referral response size, it may occur that when new NS server updated to IPv6, the address cannot be carry in the referral response in the first place without EDNS0 support. It may deliver the incomplete view of IPv6 Internet to IPv6 only recursive server and IPv6-only users. For example, the Root zone and any zones with more than 9-10 authority server may face the problem.

One intuitive thinking is that if the query is on IPv6 connection, the IPv6 addresses should be carried with high priority in DNS response if there is not enough room for all the NS RR. For example, as a key internet public services, IPv6 addresses of root name servers will be entirely contained in the referral response over IPv4 address information in dual-stack environment.

3.3. Enlargement of UDP Minimum Size parameter in IPv6-only Network

The fundamental problem in section 2.2 is the UDP size limitation in DNS protocol. It is caused by the IPv4 MTU setting in the early days of Internet, but it is recognized hard to change even with IPv6 and EDNS0 as well as sophisticated devices with large buffer and high performance. Different from designer of early Internet, current designer of core network and services like IP and DNS is restricted to the diversity and unpredictable behavior on the edge, due to which many problems arise such as security and scalability problem.

That's one reason the memo describe the proposals in IPv6-only context when people start considering turn off their IPv4. New protocol may coined and new devices will be introduced as well as new parameter of UDP minimum size. It will be direct and effective compared with other DNS extension. The internet community like IETF/IAB/ICANN/ISOC should take this opportunity and responsibility serious in which the changes of the core protocol and key parameters should be well managed and planed influencing the evolution of Internet edge step by step, not vice versa.

As to the suggestion on Enlargement of UDP minimum size parameter in IPv6-only Network. This memo give two possible value. One is 1240 octets under the MTU of IPv6 1280 octets. Another is empirical value 4096 octets following the EDNS0 practical setting (6.2.5.Payload Size Selection in RFC6891).

3.4. Introduce more IPv6-only Root Server

Based on the proposal discussed in section 3.3, if the UDP Minimum Size is not confined to 512 octets, it makes possible for zones who want to expand the number their authority server beyond 13. Considering the key service of Root zone in DNS, [6] gives an algorithm that 7 more authority server can be added in the root zone in the IPv6 transport environment (with 1240 octets UDP).

Considering the proposal in section 3.1 in which the DNS referral response contain only IPv6 address for each NS server, the number of IPv6-only authority server for each zone can be expanded to 27 following the same algorithm.

Moreover, the number will increase remarkably if the DNS referral response size parameter is enlarged to 4096 octets which means nearly a hundred IPv6-only root servers can be introduced to make the root zone file distribution more balanced and pervasive. It's meaningful especially for emerging countries in Asia Pacific, African and Latin America areas where direct IPv6-only deployment is workable.

Besides the IPv6 as a premise, to keep integrity of the zone file, in the practice, it can be a mandatory to fully support DNSSEC for the new root server application and selection process. This proposal may give the emerging countries and companies an incentive to fully support both DNSSEC and IPv6, as a reward distributing the root file locally.

4. Security Considerations

...

5. IANA Considerations

...

6. Acknowledgements

Thanks to Paul Vixie forvaluable comments in forming the first version of this memo. Special thanks to the insight from discussion of ICANN ITI panel as well.

7. References

[1] http://www.google.com/intl/en /ipv6/statistics.html

[2] Durand, A., Ihren, J., and P. Savola, "Operational Considerations and Issues with IPv6 DNS", RFC 4472, April 2006.

[3] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual- Stack Hosts", RFC 6555, April 2012.

[4] P. Vixie, A. Kato and J.Abley. "DNS Response Size Issues", draft- ietf-dnsop-respsize-15(Work in Progress), February 2014.

[5] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, April 2013.

[6] Xiaodong Lee, Paul Vixie and Zhiwei Yan. "How to scale the DNS root system?", draft-lee-dnsop-scalingroot-00(Work in Progress), July 3, 2014

Authors' Addresses

Davey Song
BII
2508 Room, 25th Floor, Tower A, Time Fortune
Beijing 100028
P. R. China

Email: songlinjian@gmail.com

Di Ma
ZDNS
No.4, South 4th Street, Zhongguancun
Beijing, Haidian 100190
P. R. China

Email: madi@zdns.cn