DNS A Record Filtering for the migration from dual stack networks to IPv6 only networks.
draft-hazeyama-sunset4-dns-a-filter-00

Abstract

Filtering out of A records of a DNS response on a DNS proxy, we call it ‘‘DNS A record filtering’’, is an effective and efficient solution as a smooth migration to IPv6 only networks. DNS A record filtering can mitigate fallback problems of dual stack nodes on IPv6 only environment. This memo mentions the components of the DNS A record filter solution, procedure of DNS queries and refers current issues.

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 http://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 January 11, 2014.

Copyright Notice

Copyright (c) 2013 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 (http://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 .................................................. 3
   1.1. Requirements Language .................................. 3
2. Technology and Terminology .................................. 3
3. The mechanism of DNS A Record Filtering ................... 4
   3.1. Assumptions .............................................. 4
   3.2. Components ............................................... 4
   3.3. Procedure ............................................... 6
       3.3.1. IPv6-only hosts ................................... 6
       3.3.2. IPv6-full-capable dual stack host ............... 6
       3.3.3. IPv6-partial-capable dual stack host .......... 7
4. Discussions ................................................... 9
   4.1. Limitation for IPv4 only applications ................. 9
   4.2. CNAME of the reply to an type A query ................ 9
5. Security Considerations .................................... 9
6. IANA Considerations ......................................... 9
7. References ................................................... 10
   7.1. Normative References .................................. 10
   7.2. Informative References ................................. 10
Appendix A. Acknowledgments .................................. 11
Authors’ Addresses ............................................ 11
1. Introduction

In an IPv6 only network [RFC6586], that is composed of DHCP6 and DNS64/NAT64, IPv4/IPv6 dual stack hosts have fallback problems due to the partial IPv6 capability, happy eyeball functions [RFC6555], default route on IPv4 link local address due to the link local assumption[RFC3927], arrival timings of DNS responses, and so on.

As well as so-called DNS AAAA record filtering in IPv4 only networks, filtering out of A records of a DNS response on a DNS proxy, we call it ‘‘DNS A record filter proxy’’, is an effective and efficient solution to mitigate fallback problems of dual stack nodes on IPv6 only environment.

DNS A record filtering solution allows dual stack nodes to resolve names both by IPv4 and IPv6 by notifying the IPv4 address of an DNS A record filter proxy through DHCP4 and the IPv6 address of the DNS A record filter proxy through DHCP6. On the other hand, a DNS A record filter proxy forces dual stack nodes to conduct actual communications after the name query procedure through IPv6, by telling only AAAA or NAT64 mapped AAAA records to dual stack nodes. In this solution, no special action is required on dual stack nodes. A network operator can choose DNS64 and NAT64 location along with their design policy.

1.1. Requirements Language

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 RFC 2119 [RFC2119].

2. Technology and Terminology

In this document, the following terms are used. "Dual Stack" refers to a technique for providing complete support for both Internet protocols -- IPv4 and IPv6 -- in hosts and routers [RFC4213].

"NAT64" refers to a Network Address Translator - Protocol Translator defined in [RFC6052], [RFC6144], [RFC6145], [RFC6146], [RFC6384].

"DNS64" refers DNS extensions to use NAT64 translation from IPv6 clients to IPv4 servers with name resolution mechanisms that is defined in [RFC6147].

"DHCP4" refers Dynamic Host Configuration Protocol for IPv4 that is defined in [RFC2131].

"DHCP6" refers Dynamic Host Configuration Protocol for IPv6. So
called "Stateful DHCP6" is defined in [RFC3315] and "Stateless DHCP6" is defined in [RFC3736]. "DHCP-PD" or "DHCPv6 Prefix Delegation" refers IPv6 Prefix Options for DHCPv6 that is initially defined in [RFC3633] and updated in [RFC6603].

"ND" refers Neighbor Discovery for IP version 6 (IPv6) that is defined in [RFC4861] and updated in [RFC5942].

3. The mechanism of DNS A Record Filtering

3.1. Assumptions

The DNS A record filtering simply filters out ‘‘A record’’ entry of a DNS reply on a DNS proxy. As our assumption, the DNS A record filtering solution is mainly used in an IPv6 only network by combining DNS64/NAT64, DHCPv4 and DHCPv6.

We also assume that hosts are dual stack capable, that is, hosts have ND function and the IPv6 address assignment function by RA at least. Stateful DHCP6, Stateless DHCP6 and IPv6 DNS query functions are preferable to be equipped by hosts.

3.2. Components

The components of the network, where this DNS A record filtering is employed, are as follows;

- DHCPv4 server: this DHCPv4 server offers a private IPv4 address to mitigate the long fall back problem due to the IPv4 link local assumption. The DHCPv4 server also offers the IPv4 address of the DNS A record filter proxy. To avoid the selection of the IPv4 by Happy Eyeball [RFC6555] in a dual stack host, this DHCPv4 server MUST NOT provide the IPv4 default route.

- DHCPv6 server: this DHCPv6 server MUST provide the IPv6 address of the DNS A record filter proxy. Both stateful DHCPv6 and stateless DHCPv6 can be employed. If the subnet is composed of a security switch and/or security wi-fi controllers, stateful DHCPv6 is preferable to avoid the blocking due to the multiple temporary IPv6 address on a host.

- DNS A record filter proxy: this DNS proxy is the key component of this solution. The DNS proxy SHOULD be located on the leaf subnet. The DNS proxy has a private IPv4 address that SHOULD be the same subnet address provided by the DHCPv4. The DNS proxy has an IPv6 address that is announced to hosts through DHCPv6.
DNS64 server: at least, one DNS64 server is required. The DNS A record filter proxy forwards all queries to this DNS64 server directly, or several DNS forwarder can be placed for load balancing of DNS64 servers.

Authoritative DNS servers: these authoritative DNS servers would be queried by DNS64 servers. These authoritative DNS servers MUST NOT return inappropriate replies mentioned in [RFC4074] to kick the fallback function of DNS64 servers.

NAT64 translators: at least, one NAT64 translator is placed that can be reached by hosts through IPv6. A NAT64 translator can be settled as the gateway of the leaf subnet, or an aggregated translator of the intra network, or a global reachable open translator. Several NAT64 translators can be registered in DNS64 servers for the load balancing or for handling different IPv4 prefixes by each NAT64 translator.

Figure 1 shows a sample network topology of this solution.

A sample network topology of DNS A record filtering.
3.3. Procedure

3.3.1. IPv6-only hosts

The procedure on IPv6-only hosts is as follows;

- The host connects to the leaf subnet in layer 2 level.
- The host gets global IPv6 address through RA or stateful DHCP6, and also learns the IPv6 address of the DNS A record filter proxy.
- When the host connects to an URL, the hosts queries by type ANY or by type AAAA to the DNS A record filter proxy through IPv6.
- The DNS A record filter proxy forwards the received the type ANY query to the upper DNS forwarder or DNS64 server.
- When the host connects to the URL, the DNS64 server forwards the issued FQDN to the upper authoritative DNS.
  * If the FQDN has AAAA record, the DNS64 returns AAAA record to the DNS A record filter proxy.
  * If the FQDN has only A record, the DNS64 returns NAT64 prefix mapped AAAA record to the DNS A record filter proxy.
  * The DNS64 server or the upper DNS forwarder may return A record to the DNS A record filter proxy with AAAA record.
- When the DNS A record filter proxy receives the reply, the DNS A record filter proxy filters out A record if the reply contains A record.
- The DNS A record filter proxy returns only AAAA records to the host.
- The host access to the issued URL through the IPv6 address of the destination or the NAT64 prefix mapped address.

3.3.2. IPv6-full-capable dual stack host

An IPv6-full-capable dual stack node equips DHCP6 function and IPv6 DNS query function, therefore, IPv6-full-capable dual stack node can send DNS queries through both IPv4 and IPv6.

The procedure on IPv6-full-capable dual stack hosts (like Windows 7,
etc.) is as follows;

- The host connects to the leaf subnet in layer 2 level.
- The host gets a global IPv6 address through RA or stateful DHCP6, and also learns the IPv6 address of the DNS A record filter proxy.
- The host also gets a private IPv4 address through DHCP4, and also learns the IPv4 address of the DNS A record filter proxy.
- The network connectivity check sequence of the Operating System may run, then, IPv6 will be selected on the host because the IPv4 is not global reachable.
- When the host connects to an URL, the host queries by type ANY to the DNS A record filter proxy through IPv6.
- The DNS A record filter proxy forwards the received type ANY query to the upper DNS forwarder or DNS64 server.
- When the DNS64 server receives the query, the DNS64 server forwards the issued FQDN to the upper authoritative DNS.
  * If the FQDN has AAAA record, the DNS64 returns AAAA record to the DNS A record filter proxy.
  * If the FQDN has only A record, the DNS64 returns NAT64 prefix mapped AAAA record to the DNS A record filter proxy.
  * The DNS64 server or the upper DNS forwarder may return A record to the DNS A record filter proxy with AAAA record.
- When the DNS A record filter proxy receives the reply, the DNS A record filter proxy filters out A record if the reply contains A record.
- The DNS A record filter proxy returns only AAAA records to the host.
- The host access to the issued URL by using the IPv6 address of the destination or the NAT64 prefix mapped address.

### 3.3.3. IPv6-partial-capable dual stack host

An IPv6-partial-capable dual stack node does not equip either DHCP6 function or IPv6 DNS query function, therefore, IPv6-partial-capable dual stack node will send DNS queries through only IPv4. However, IPv6-partial-capable dual stack can recognize AAAA record or IPv6
address.

The procedure on IPv6-partial-capable dual stack host is as follows;

- The host connects to the leaf subnet in layer 2 level.
- The host gets a global IPv6 address through RA.
- The host also gets a private IPv4 address through DHCP4, and also learns the IPv4 address of the DNS A record filter proxy.
- The network connectivity check sequence of the Operating System may run, then, IPv6 may be selected on the IPv6-preferred host because the IPv4 is not global reachable. In some case, the network connectivity check may pass by name resolution to the anchor server, or the network connectivity may run again with certain interval.
- When the host connects to an URL, the host queries by type ANY to the DNS A record filter proxy through IPv4.
- The DNS A record filter proxy forwards the received type ANY query to the upper DNS forwarder or DNS64 server through IPv6.
- When the DNS64 server receives the query, the DNS64 server forwards the issued FQDN to the upper authoritative DNS.
  * If the FQDN has AAAA record, the DNS64 returns AAAA record to the DNS A record filter proxy.
  * If the FQDN has only A record, the DNS64 returns NAT64 prefix mapped AAAA record to the DNS A record filter proxy.
  * The DNS64 server or the upper DNS forwarder may return A record to the DNS A record filter proxy with AAAA record.
- When the DNS A record filter proxy receives the reply, the DNS A record filter proxy filter out A record if the reply contains A record.
- The DNS A record filter proxy returns only AAAA records to the host.
- The host access to the issued URL by using the IPv6 address of the destination or the NAT64 prefix mapped address.
4. Discussions

4.1. Limitation for IPv4 only applications

As mentioned in [RFC6586], IPv4-only (or IPv6-incapable) applications exist. Such IPv4-only applications will not work on this DNS A record filtering environment. It is preferable that such IPv4-only applications become dual stack applications if possible.

4.2. CNAME of the reply to an type A query

We conducted a field trial of this DNS A record filter solution in Interop Tokyo 2013. We provided an IPv6-only Wi-Fi access with this DNS A record filter solution. We used the current Debian release and bind 9.9.2-p1 patch provided from WIDE project as the DNS A Record filter proxy.

In the hot stage of Interop Tokyo 2013, we met a trouble case of the current DNS A record filter. In the trouble case, a host used Firefox browser and crawled several web pages for test. In some web page, several contents were lost. We inspected by packet captures, the reply of the A query to the host arrived faster than the arrival of the reply of AAAA record. The reply of A query contained as type CNAME, that was not filtered in the current bind A filter patch. (The A filter patch removed type A record of the CNAME.) On the other hand, in a successful case, the reply of AAAA record, that contained type CNAME and type AAAA of the CNAME, arrived faster than the type A reply.

Of course, we have to conduct further investigation and tests, the CNAME on a type A reply would be removed by DNS A filter proxy as well as type A record on the type A reply.

5. Security Considerations

As well as mentioned in [RFC6586], the use of IPv6 instead of IPv4 by itself does not make a big security difference.

6. IANA Considerations

This document has no IANA implications.

7. References
7.1. Normative References


7.2. Informative References


Appendix A. Acknowledgments


O. Onoe of Sony Corporation for his deep inspection and testing of end node devices in WIDE project meeting in September 2012.

Interop Tokyo 2013 NOC members and Nano Opt Media for providing a field trial of this DNS A Record Filter solution as a service network. Especially, K. Mano of A10 Networks and STM members for their deep inspection and testing.

Authors’ Addresses

Hiroaki Hazeyama
NAIST / WIDE Project
Takayama 8916-5
Nara,
Japan

Phone: +81 743 72 5216
Email: hiroa-ha@is.naist.jp
Tomohiro Ishihara
Univ. of Tokyo / WIDE Project
3-8-1 Komaba, Meguro
Tokyo,
Japan

Email: sho@c.u-tokyo.ac.jp

Osamu Nakamura
Keio Univ. / WIDE Project
5322 Endo
Kanagawa,
Japan

Email: osamu@wide.ad.jp