Behave WG B. Rajtar
Internet-Draft Hrvatski Telekom
Intended status: Standards Track I. Farrer
Expires: January 16, 2014 Deutsche Telekom AG
A. Vizdal
T-Mobile CZ
X. Li
C. Bao
CERNET Center/Tsinghua University
July 15, 2013

Framework for accessing IPv6 content for IPv4-only clients
draft-rfvlb-behave-v6-content-for-v4-clients-01

Abstract

With the expansion of IPv6 usage and content available on IPv6, it is important that clients with legacy (i.e. non IPv6-capable) operating systems are able to access such content.

This document describes a method for achieving this, including how the method could be implemented in real-world scenarios.

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].

Copyright Notice

Table of Contents

1. Introduction

At the time of writing, IPv6 is still not widely deployed. There are several reasons for this, one of which is that IPv4-only operating systems are still commonplace with end-users and account for a large fraction of overall Internet traffic.

With the growth of IPv6 traffic, servers supporting only IPv6 are appearing on the Internet. An approach for enabling and IPv4-only clients to access this content is described below.

1.1. Solution Requirements

To clarify when this approach is applicable, the following requirements can be named:

1. The content MUST be reachable through IPv6, i.e. the server on which the content is stored must have a valid IPv6 address and a working IPv6 stack.

2. The server hosting the content MUST have a valid AAAA record

3. The client MUST support IPv4 only. The other alternative is also that it supports IPv6, but for some reason uses only IPv4 to access content on the Internet.

4. Client's DNS queries MUST be resolved by a dedicated appliance, i.e. a caching nameserver.

5. All traffic between the client and the server MUST be routed through a device capable of performing translation between IPv4 and IPv6, as described in [RFC6145] and [RFC6052].

It is feasible that requirements (4) and (5) can be combined in one device and managed by the service provider.That would simplify operations and remove the need for a control-plane protocol between the two devices.

1.2. Covered Scenarios

[RFC6144] describes multiple scenarios for IPv4/IPv6 translation. This document is mainly concerned with Scenario 4: An IPv4 Network to the IPv6 Internet, but is also applicable to Scenario 6 (An IPv4 Network to an IPv6 Network). This scenario is not covered in this memo and can be elaborated in future documents, as necessary. Scenario 2, which faces similar challenges (The IPv4 Internet to an IPv6 Network), is covered by [I-D.draft-sun-behave-v4tov6-00].

1.3. Functional elements

Client User end-device, typically a personal computer or similar.

DNS proxy Caching nameserver which proxies DNS queries from the client.

NAT46 translator Translation device which translates incoming IPv4 traffic.

IPv6-only server Device which holds content on an IPv6-only network.

2. Algorithm Description

This section describes how the algorithm works and the roles of every functional element. The steps are in cronological order, and display

the scenario when the IPv4 client initiates a request for ipv6.example.com which is running on an IPv6-only server.

1. The customer types in "ipv6.example.com" into his web browser and initiaties the request for the web page.

2. The client operating system initiates a DNS query for "ipv6.example.com". Since the client uses IPv4, the query is for an A record.

3. The DNS proxy receives the A record query and assumes the client is not IPv6 capable. Therefore, it initiates a DNS query for A and AAAA records for "ipv6.example.com" to the authorative DNS server.

4. If a DNS response is received with only an AAAA record, the DNS proxy assumes that the server is IPv6-only. (In case the proxy receives both A or AAAA records, or just an A record, the A record is returned to the client and the process ends here.)

5. As a response to the client, the proxy returns a fake A record for "ipv6.example.com" pointing at an un-used IPv4 address from the private address space (as described in [RFC1918]).

6. The private IPv4 address and the resolved IPv6 address of "ipv6.example.com" must be kept in the translation table of the NAT46 translator. The time the translation would stay active in the table would be equal to the TTL field of the DNS response. How the DNS-related information is conveyed from the DNS proxy to the translator is out of the scope of this document. In the case the translator and the DNS proxy are functions of the same device, the logic is simplified.

7. All IPv4 traffic from the client to "ipv6.example.com" will be translated to IPv6 as described in [RFC6145]. Unlike NAT-PT described in [RFC2766] (moved to Historic Status by [RFC4966]), the translation is a learned state and not a session triggered state. The destination address of the translated IPv6 packet will be the resolved AAAA record of "ipv6.example.com", while the source IPv6 address will be created according to [RFC6052]. The IPv6 prefix used to create the source IPv6 address must be globally unique and allocated to the device. If there are more IPv6 prefixes on the device, defining which one will be used is out of the scope of this document. The IPv4 address used to create the source IPv6 address is the address of the client.

8. Return IPv6 traffic will be translated by the same device as the outgoing traffic, using IPv6 to IPv4 translation analogous to the

previous step. The source IPv4 address will be the private IPv4 address given by the DNS proxy to the client, while the destination IPv4 address would be the one of the client.

2.1. Flow diagram

In this example, the client is located behind a home gateway and is delegated an IPv4 address of 192.168.1.3. The home gateway is acting as a DNS proxy and as a NAT46 translator.

```
+-----------+       +----------------+   +-----------+ +------------+
|           |       | (Home Gateway) |   |    DNS    | |   ipv6.    |
|  Client   |       |   DNS proxy/   |   |authorative| |example.com |
|192.168.1.3|       |NAT46 translator|   |  server   | |2000:db9::1 |
|           |       |   2000:db8::1  |   |           | |            |
+-----------        +----------------+   +-----------+ +------------+
     |    DNS A query for   |                      |          |
     |  "ipv6.example.com"  |                      |          |
     |--------------------->|DNS A and AAAA query  |          |
     |                      |for "ipv6.example.com"|          |
     |                      |--------------------->|          |
     |                      |   DNS AAAA response  |          |
     |                      |for "ipv6.example.com"|          |
     |DNS A response:       |<---------------------|          |
     |""ipv6.example.com"   |                      |          |
     |is located on 10.1.1.1|                                 |
     |<---------------------|                                 |
     | IPv4 SA:192.168.1.3  | IPv6 SA:2000:db8::192.168.1.3   |
     |   DA:10.1.1.1        | DA:2000:db9::1                  |
     |--------------------->|-------------------------------->|
     | IPv4 SA:10.1.1.1     | IPv6 SA:2000:db9::1             |
     |  DA:192.168.1.3      | DA:2000:db8::192.168.1.3        |
     |<---------------------|<--------------------------------|
     |                      |                                 |
```

3. Usage scenarios

The typical scenario where such a solution can be used is the home network. The customer can have a broadband service with access to IPv6 Internet, but uses an IPv4-only client. The DNS proxy and the translation device would in that case be the home gateway, which would handle the decision-making process, as well as the translation.

However, other scenarios can also be foreseable, such as mobile access, business customers, etc. It's applicable to all scenarios where a DNS proxy is used, as well as a default gateway which can act as a translation device.

4. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

5. Security Considerations

6. Acknowledgements

7. Normative References

[I-D.draft-sun-behave-v4tov6-00]
, .

[RFC1918] , "Address Allocation for Private Internets", .

[RFC2119] , "Key words for use in RFCs to Indicate Requirement Levels", .

[RFC2766] , "Network Address Translation - Protocol Translation (NAT-PT)", .

[RFC4966] , "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", .

[RFC6052] , "IPv6 Addressing of IPv4/IPv6 Translators", .

[RFC6144] , "Framework for IPv4/IPv6 Translation", .

[RFC6145] , "IP/ICMP Translation Algorithm", .

Authors' Addresses

Branimir Rajtar
Hrvatski Telekom
Zagreb
Croatia

Email: branimir.rajtar@t.ht.hr

Ian Farrer
Deutsche Telekom AG
Bonn
Germany

Email: ian.farrer@telekom.de

Ales Vizdal
T-Mobile CZ
Prague
Czech Republic

Email: ales.vizdal@t-mobile.cz

Xing Li
CERNET Center/Tsinghua University
Beijing
China

Email: xing@cernet.edu.cn

Congxiao Bao
CERNET Center/Tsinghua University
Beijing
China

Email: congxiao@cernet.edu.cn