Behave WG
Internet-Draft
Intended status: Standards Track
Expires: January 02, 2014

B. Rajtar
Hrvatski Telekom
I. Farrer
Deutsche Telekom AG
A. Vizdal
T-Mobile CZ
X. Li
C. Bao
CERNET Center/Tsinghua University

July 01, 2013

Framework for accessing IPv6 content for IPv4-only clients
draft-rfvlb-behave-v6-content-for-v4-clients-00

Abstract

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

This document describes how this can be achieved and how it can be implemented in a real-world scenario.

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].

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 02, 2014.

Table of Contents

1. Introduction

At the time of writing, IPv6 is still not widely deployed. Several reasons can be named, one of which is the fact that IPv4-only operating systems are still used by many end customers and account for a large fraction of total Internet traffic. Also, with the introduction of Carrier-Grade NAT, exhaustion of IPv4 address space is no longer an issue which would be the key driver of the transition to IPv6.

With the growth of IPv6 traffic, servers only supporting IPv6 are appearing on the Internet and IPv4-only clients must be able to access content available on them. The following sections describe a methodology how this can achieved.

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. As can be seen later in the document, this in turn implies that the server must have a valid AAAA record.

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

3. Client's DNS queries must be proxied by a dedicated appliance.

4. All traffic between the client and the server must pass through a device capable of performing translation between IPv4 and IPv6, as described in [RFC6145] and [RFC6052].

It is feasible that requirements three and four can be combined in one device and managed by the service provider.

1.2. Covered Scenarios

As described in [RFC6144], there are multiple scenarios for IPv4/IPv6 translation. This document covers mainly Scenario 4: An IPv4 Network to the IPv6 Internet, but is not limited to be used for the following scenarios as well:

- Scenario 2: The IPv4 Internet to an IPv6 Network

- Scenario 6: An IPv4 Network to an IPv6 Network

These scenarios are not subject of this draft and can be elaborated in future documents, if deemed necessary.

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 example.com which is running on an IPv6-only server.

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

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

3. DNS proxy perceives that the query is for an A resource record only and assumes the client is not IPv6 capable. Therefore, it initiates a DNS query for A and AAAA records for "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 "example.com" pointing at an IPv4 address from the private address space (as described in [RFC1918]).

6. The private IPv4 address and the resolved IPv6 address of "example.com" must be kept in translation table at the device which performs the actual translation. 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 translation device is out of the scope of this document.

7. All IPv4 traffic from the client to "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 configured state and not a session triggered state. The destination address of the translated IPv6 packet will be the resolved AAAA record of "example.com", while the source IPv6 address will be created according to [RFC6052]. The IPv4 address and IPv6 prefix used to create the source IPv6 address are out of the scope of this document.

8. Return IPv6 traffic will be translated at the same device as the outgoing traffic, using IPv6 to IPv4 translation analogous to the one described in previous step. The source IPv4 address would 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.

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 as well.

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

[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