Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 24, 2014

C. Xie
Q. Sun
Q. He
China Telecom
C. Zhou
Huawei Technologies
X. Li
C. Bao
CERNET Center/Tsinghua University

October 21, 2013

4to6: The Approach for IPv4-only users to access IPv6-only Content

draft-sun-v4tov6-00

Abstract

Current approaches can not solve the scenario that the users from IPv4 Internet to access IPv6-only content. When IPv6 content are becoming more and more popular, it is important to ensure that IPv6-only content can be reachable from legacy IPv4-only clients via some IPv4-only network. This document proposes an approach for IPv4-only users to access IPv6-only content, and can also achieve address sharing in the server side. It is designed to cover the Scenario 2 in [RFC6144].

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 April 24, 2014.

Copyright Notice

Table of Contents

1. Introduction

Currently, IPv4 addresses for servers are also facing address shortage problem. When IPv4 addresses are becoming a more scarce resource, it will cost more for content providers to keep using so many IPv4 addresses as today. Besides, the upcoming new applications, e.g. cloud computing, etc., are consuming more and more IPv4 addresses. Therefore, it is better for content provider to upgrade to IPv6 directly.

Scenario 2 in [RFC6144] is important for this use case. Not only could servers move directly to IPv6 without trudging through a difficult transition period, but they could do so without risk of losing connectivity with the IPv4-only Internet. In addition, when address sharing can be achieved, the content providers can further save money by requiring less IPv4 addresses and reduce the operational complexity by using IPv6 single-stack servers. For Data Center Operators, they can offer service to more ICPs with limited IPv4 addresses.

There are several requirements in the design:

1.Considering IPv4 address has been a scarce resource, the amount of public IPv4 addresses consumed by the translator should be less than that the number of IPv6 servers in the IPv6 network.

2. It should not require extra modifications on the server-side and on the client-side, e.g. by using a dynamic port number in the server, implementing a TURN client, etc.

3. It should not require modification on existing DNS architecture. Otherwise, it would be difficult to deploy in reality.

Existing solutions have not solved this scenario well. NAT-PT[RFC2766]can be used in this scenario, but it requires a tightly coupled DNS Application Level Gateway (ALG) in the translator, and have been deprecated by the IETF [RFC4966]. The stateless translation solution [RFC6219] can work too, but since each IPv6 server will consume one IPv4 public address, it is not suitable to deploy in situation that operators are running out of IPv4 address. [RFC6156] can be used for IPv4 client to communicate with IPv6 client. But this requires the IPv4 client and IPv6 client to implement a TURN client. Therefore, it is not suitable for C-S(Client-Server) and B-S (Browser-Server) mode.

[I-D.rfvlb-behave-v6-content-for-v4-clients] can work for IPv4-only user to access IPv6 content. But since it uses private IPv4 address

to mapping the IPv6 server, it can only be used for IPv4 network to reach IPv6 network.

This document is designed for IPv4 Internet to reach IPv6 network. It is not a new protocol, but just to make use of existing protocols and funtionalities. It can achieve high IPv4 address sharing ratio for IPv6 servers, and there is no impact on the server/client and existing DNS architecture.

2. Terminology

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 [RFC2119].

Terminology defined in [RFC6144] is used extensively in this document. Besides, this document uses the following terminologies:

IPv6-converted addresses: IPv4 addresses used to represent IPv6 nodes in an IPv4 Internet. They have an explicit mapping relationship to IPv6 addresses.

IPv6-converted port: The port number used to distinguish the traffic destinated to different IPv6 servers from the same IPv4 client.

NAT46: a stateful IPv4/IPv6 translation functionality. It is consistent with IP/ICMP translation [RFC6145].

3. Overall solution architecture for IPv4 Internet to access IPv6 network

The 4to6 solution is used for IPv4 clients in IPv4 Internet to reach IPv6 servers . It is designed for HTTP applications specially.

In order to achieve the translation initiated from the IPv4 side, two addresses need to be determined by NAT46 translator. The first one is the IPv6-converted address of the IPv6 server, which is is selected from the IPv4 address pool configured in NAT46. The second one is the IPv4-converted address for the IPv4 client, which can be synthetized using the stateless approach defined in [RFC6052].

In HTTP, since the traffic can be redirected to a different service port, it is able to achieve address sharing for IPv6 servers by using distinctive port numbers (denoted as IPv6-converted port) in IPv4 client's upstream traffic . Therefore, one IPv4 address can support up to thousands of IPv6 servers in theory.

The overall architecture of the 4to6 solution is depicted in the following figure.

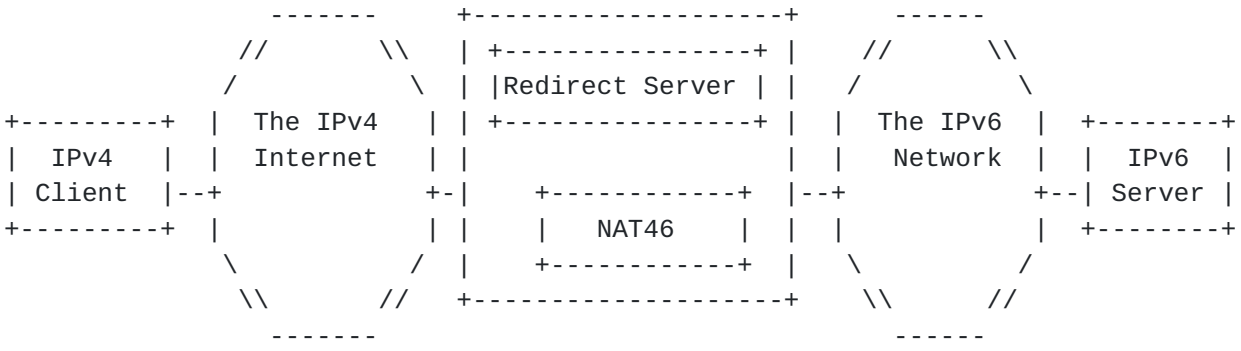

Figure 1: Overall solution for IPv4 Internet to IPv6 network

It consists of several functionalities:

1. NAT46: This functionality is consistent with [RFC6145]. It keeps the binding table between the IPv6 server address, IPv6 service port, IPv6-converted address and IPv6-converted port. When an IPv4 packet initiated from the IPv4 client arrives at the NAT46, NAT46 will extract the destination address and the destination port, lookup the binding table and then translate it to an IPv6 packet. It will take similar action to the downstream packet from the IPv6 server.

2. Redirect Server: A redirect server is used to redirect traffic to a different IPv6-converted address and IPv6-converted port. Since the A record for a given IPv6 server is always the IPv4 address of the redirect server, the first packet from the IPv4 client will be routed to the redirect server. The redirect server will return IPv6-converted address and IPv6-converted port to the client by querying from the NAT46.

In 4to6 solution, only the first TCP flow will be treated by the redirect server. The subsequent traffic will be translated directly by the NAT46.

4. The Workflow of 4to6 Solution

The workflow of this apporach is as follows:

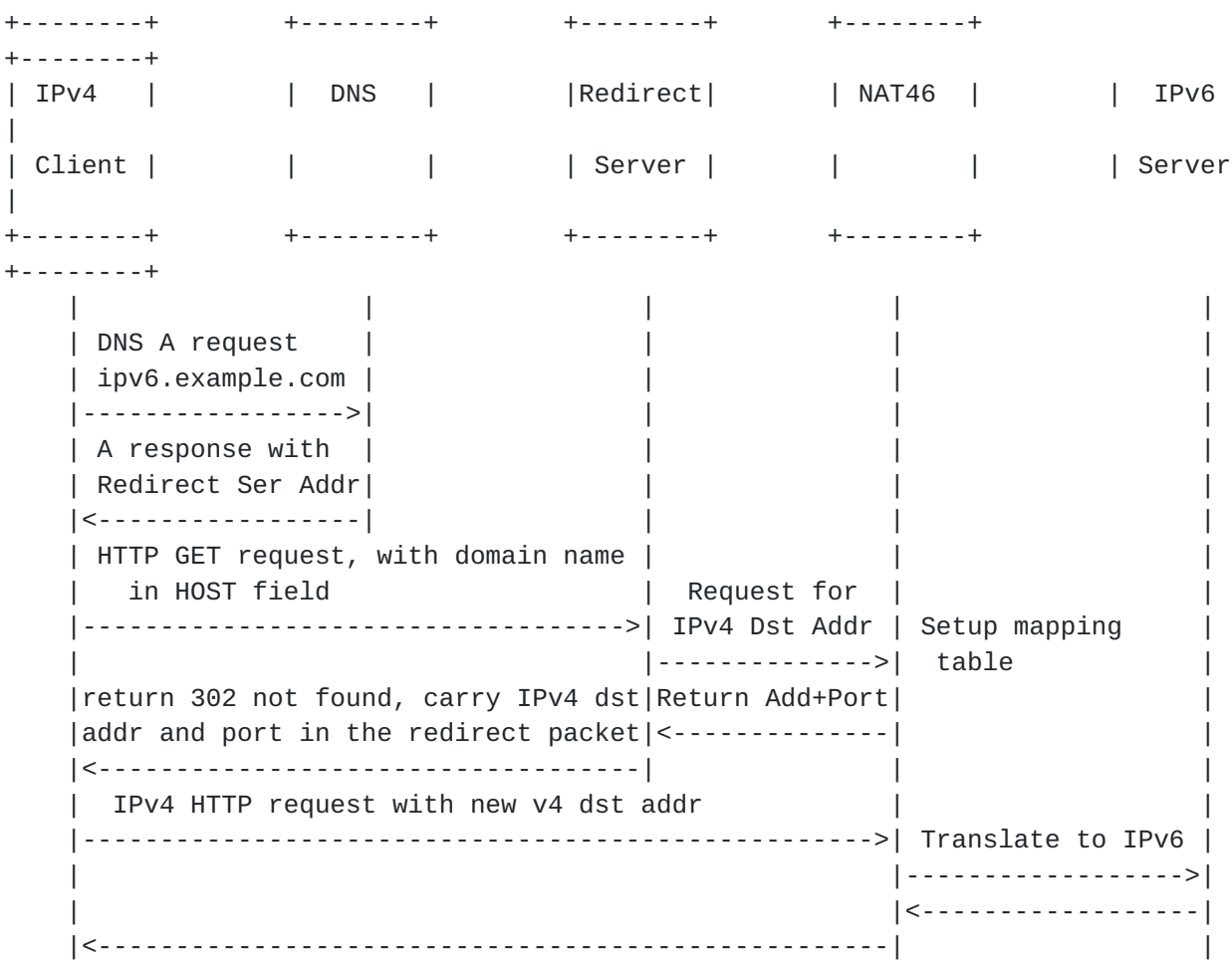

Figure 2: Workflow of Proxy-lite Approach

1. An IPv4 client initiates a DNS query for A record (e.g. ipv6.example.com).

2. In DNS server, the address of the redirect server is configured as the A record for ipv6.example.com and returns to the IPv4 client.

3. The IPv4 client sends HTTP GET request. The domain name (e.g. ipv6.example.com) is carried in HOST field.

4. The redirect server interprets the domain name, and sends the request to get IPv6-converted address to NAT46 (carrying the address of IPv4 client and the destination port). The specific protocol for the request is now out of scope.

5. NAT46 selects IPv6-converted address and IPv6-converted port by lookuping the binding table. It will also keep the destination port in the binding table.

6. NAT46 returns the IPv6-converted address and IPv6-converted port to redirect server and the redirect server in turn returns IPv6-converted address in HTTP redirect packet with HTTP error "302 not

found".

7. IPv4 client replaces the destination IPv4 address with the returned IPv6-converted address. The IPv4 traffic is routed to the NAT46.

8. NAT46 extracts the destination address and destination port in the IPv4 traffic. It will lookup the binding table maintained in NAT46 and NAT46 translates the IPv4 packet to IPv6 packet according to [RFC6145].

5. IANA Considerations

No requirement on IANA.

6. Acknowledgements

The authors would like to thank Dan Wing, Fred Baker and Jari Arkko for their review and comments.

7. References

7.1. Normative References

[I-D.rfvlb-behave-v6-content-for-v4-clients] Rajtar, B., Farrer, I., Ales, V., Li, X., and C. Bao, "Framework for accessing IPv6 content for IPv4-only clients", draft-rfvlb-behave-v6-content-for-v4-clients-01 (work in progress), July 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

[RFC4966] Aoun, C. and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6156] Camarillo, G., Novo, O., and S. Perreault, "Traversal Using Relays around NAT (TURN) Extension for IPv6", RFC 6156, April 2011.

[RFC6219] Li, X., Bao, C., Chen, M., Zhang, H., and J. Wu, "The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition", RFC 6219, May 2011.

7.2. Informative References

Authors' Addresses

Chongfeng Xie
China Telecom
P.R.China

Phone: 86 10 58552116
Email: xiechf@ctbri.com.cn

Qiong Sun
China Telecom
P.R.China

Phone: 86 10 58552936
Email: sunqiong@ctbri.com.cn

Qi He
China Telecom
P.R.China

Phone: 86 10 58552332
Email: heqi@ctbri.com.cn

Cathy Zhou
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone:
Email: cathy.zhou@huawei.com

Xing Li
CERNET Center/Tsinghua University
Room 225, Main Building
Beijing 100084
P.R.China

Phone: +86 10 6278 5983
Email: xing@cernet.edu.cn

Congxiao Bao
CERNET Center/Tsinghua University
Room 225, Main Building
Beijing 100084
P.R.China

Phone: +86 10 6278 5983
Email: congxiao@cernet.edu.cn