Workgroup: Network Working Group
Internet-Draft: draft-matsuhira-m4p6e-16
Published: 4 April 2024
Intended Status: Informational
Expires: 6 October 2024
Authors: N. Matsuhira
Neptela

Multiple IPv4 address and port number - IPv6 address mapping encapsulation (M4P6E)

Abstract

This document specifies Multiple IPv4 address and port number - IPv6 address mapping encapulation (M4P6E) specification.

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 https://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 6 October 2024.

Copyright Notice

Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

This document provides Multiple IPv4 address and port number - IPv6 address mapping encapulation (M4P6E) base specification.

M4P6E provide IPv4 address sharing function without Network Address Translation (NAT [RFC1631]). M4P6E require IPv6 network.

2. Architecture of M4P6E

Figure 1 shows M4P6E address architecture. M4P6E address consists four parts, M4P6E prefix, IPv4 network plane ID, IPv4 address, and Port number.

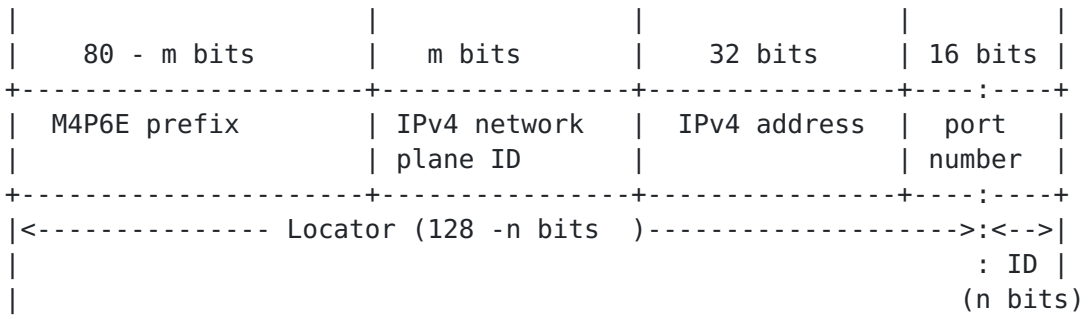

Figure 1

In M4P6E, boundary of locator and identifier is in port number part, that mean, M4P6E use upper part of port number as locator, and lower part of port number as identifier.

3. M4P6E address format

Figure 2 show a example of M4P6E address format. In this example, 16bits IPv4 network plane ID is used, that provide 65535 IPv4 network plane.

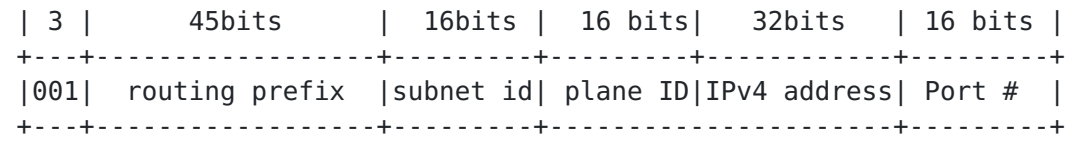

Figure 2

4. Using M4P6E in client server environments

4.1. Client environments

Figure 3 shows a example of M4P6E usage in client environments. In this document, NAPT is IPv4 - IPv4 Netowrk address and port number translator. Coopetation with NAPT, M4P6E provide IPv4 address sharing with different users.

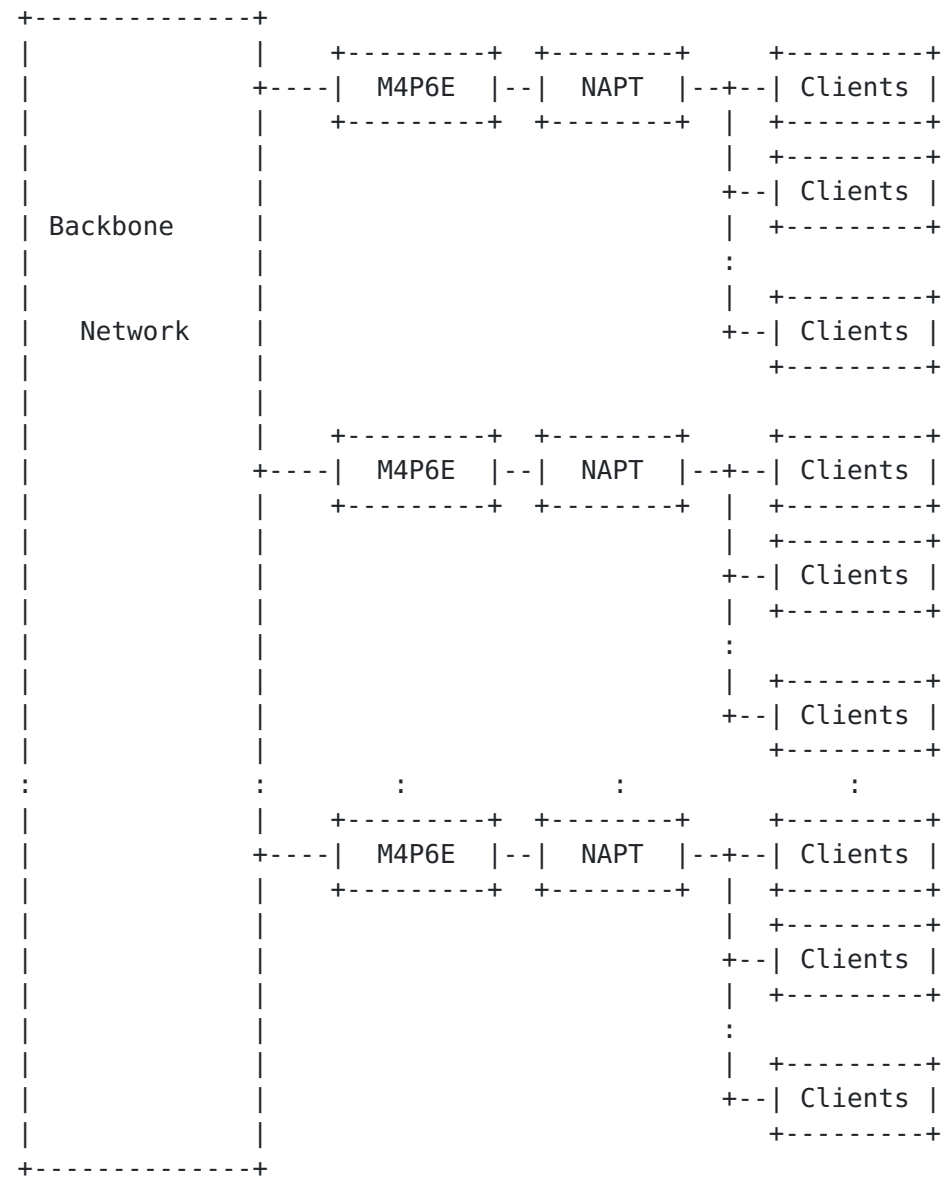

Figure 3

4.2. Server environments

Figure 4 shows an example of M4P6E usage in server environments. In this example, server terminate M4P6E tunnel. This case, Server require at least one port number per server, that mean, 128bits host route advertise for server access via IPv4. This case, full access is provided via IPv6.

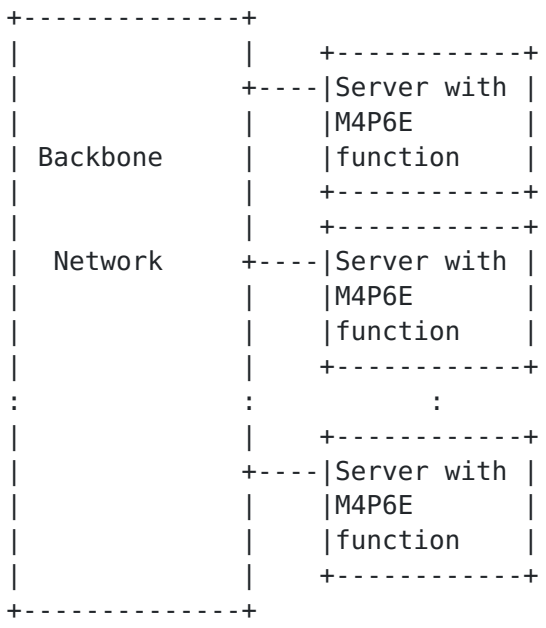

Figure 4

4.3. Data Center Environments

Figure 5 shows an example of M4P6E usage in Data Center environments. In this example, M4P6E is used only in Data Center Backend Network closely. Client which is connected via backbone network does not know the exists of M4P6E. M4P6E can provide at least one port number per server, this case, 128bits host route is advertised, however this route in advertised only in data center backbone network. Ofcource, IPv6 address may allocated to the server, so full access is provided via IPv6.

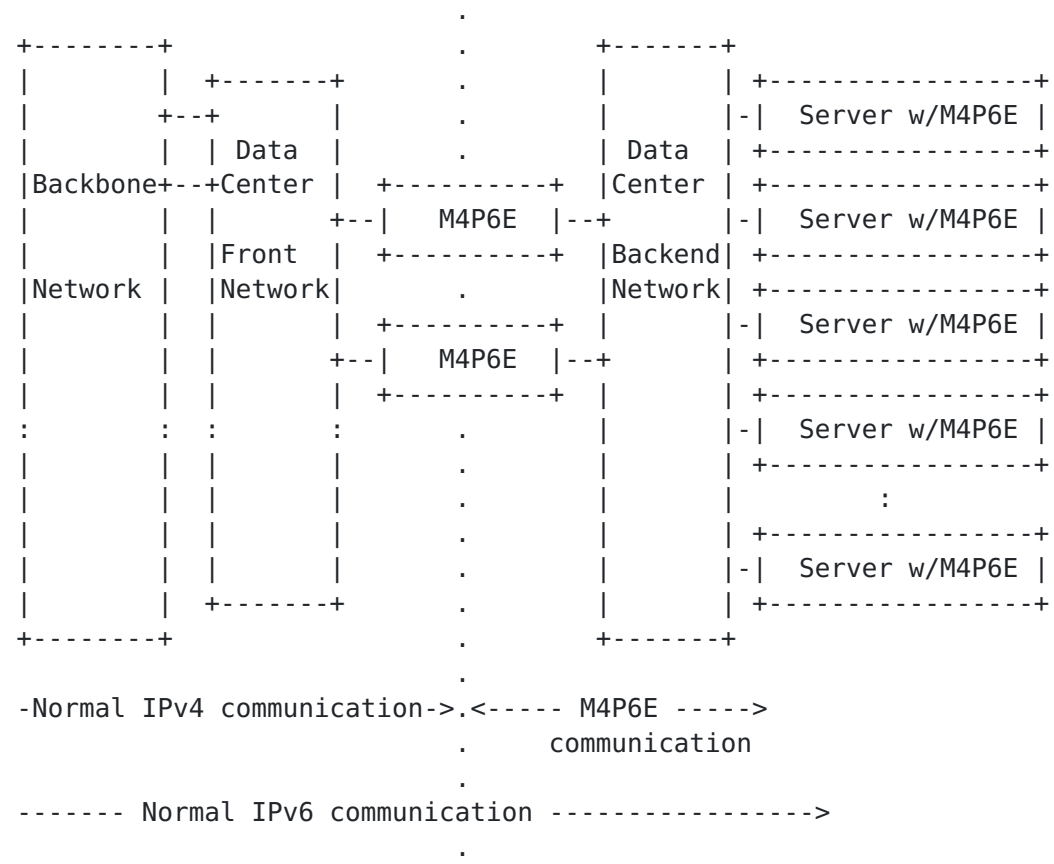

Figure 5

5. Port Number Issue

M4P6E require port number of transport layer. M4P6E can not support ICMPv4 [RFC0792]. The function provided by ICMPv4 does not work in M4P6E environments, such as Path MTU Discovery [RFC1191], ping command, etc.

M4P6E can not also support IPv4 IPsec ESP [RFC4303] because transport header is encrypted.

6. IANA Considerations

This document makes no request of IANA.

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

7. Security Considerations

M4P6E use automatic tunneling technologies. Security consideration related tunneling technologies are discussed in RFC2893 [RFC2893], RFC2267 [RFC2267], etc.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

8.2. References

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, DOI 10.17487/RFC1191, November 1990, <https://www.rfc-editor.org/info/rfc1191>.

[RFC1631] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, DOI 10.17487/RFC1631, May 1994, <https://www.rfc-editor.org/info/rfc1631>.

[RFC2267] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2267, DOI 10.17487/RFC2267, January 1998, <https://www.rfc-editor.org/info/rfc2267>.

[RFC2893] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, DOI 10.17487/RFC2893, August 2000, <https://www.rfc-editor.org/info/rfc2893>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

Author's Address

Naoki Matsuhira
Neptela
Japan

Email: matsuhira.ietf@gmail.com