Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 5, 2013

I. Yamagata
Y. Shirasaki
NTT Communications
A. Nakagawa
Japan Internet Exchange (JPIX)
J. Yamaguchi
Fiber 26 Network
H. Ashida
IS Consulting G.K.
July 4, 2012

NAT444
draft-shirasaki-nat444-06

Abstract

This document describes one of the network models that are designed for smooth transition to IPv6. It is called NAT444 model. NAT444 model is composed of IPv6, and IPv4 with Carrier Grade (CGN).

NAT444 is the only scheme not to require replacing Customer Premises Equipment (CPE) even if IPv4 address exhausted. But it must be noted that NAT444 has serious restrictions i.e. it limits the number of sessions per CPE so that rich applications such as AJAX and RSS feed cannot work well.

Therefore, IPv6 which is free from such a difficulty has to be introduced into the network at the same time. In other words, NAT444 is just a tool to make IPv6 transition easy to be swallowed. It is designed for the days IPv4 and IPv6 co-existence.

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 5, 2013.

Table of Contents

1. Introduction

The only permanent solution of the IPv4 address exhaustion is to deploy IPv6. Now, just before the exhaustion, it's time to make a transition to IPv6.

After the exhaustion, unless ISP takes any action, end users will not be able to get IPv4 address.

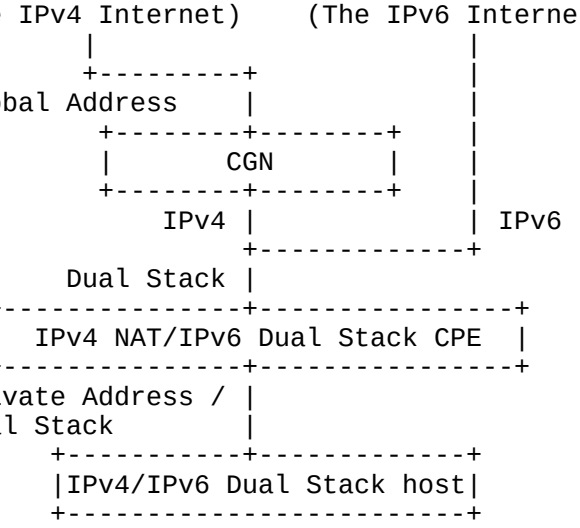
The servers that have only IPv4 address will continue to exist on the Internet after the IPv4 address exhaustion. In this situation, IPv6 only hosts cannot reach IPv4 only hosts.

This document explains NAT444 model that bridges the gap between the coming IPv6 Internet and the present IPv4 Internet.

2. Definition of NAT444 Model

NAT444 Model is a network model that uses two Network Address and Port Translators (NAPTs) with three types of IPv4 address blocks.

The first NAPT is in CPE, and the second NAPT is in Carrier Grade NAT (CGN) [I-D.ietf-behave-lsn-requirements]. CGN is supposed to be installed in the ISP's network.



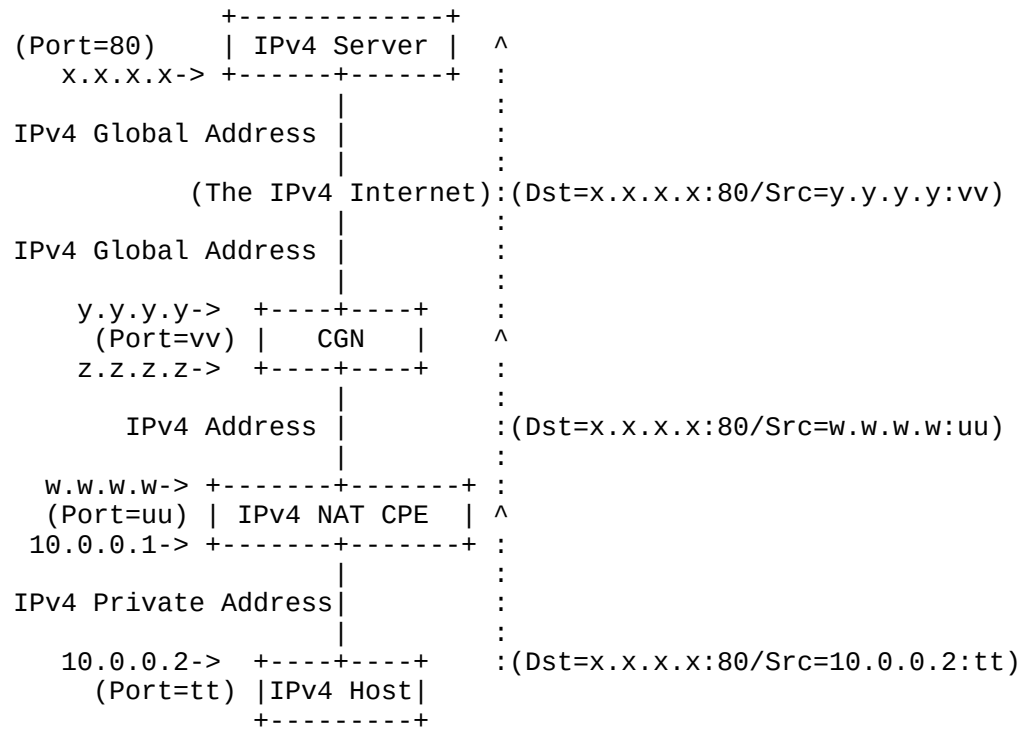
The first IPv4 address block is Private Address [RFC1918] inside CPE. The second one is an IPv4 Address block between CPEs and CGN. The third one is IPv4 Global Addresses that is outside CGN. The ISPs

using NAT444 provide IPv6 connectivity by dual stack model.

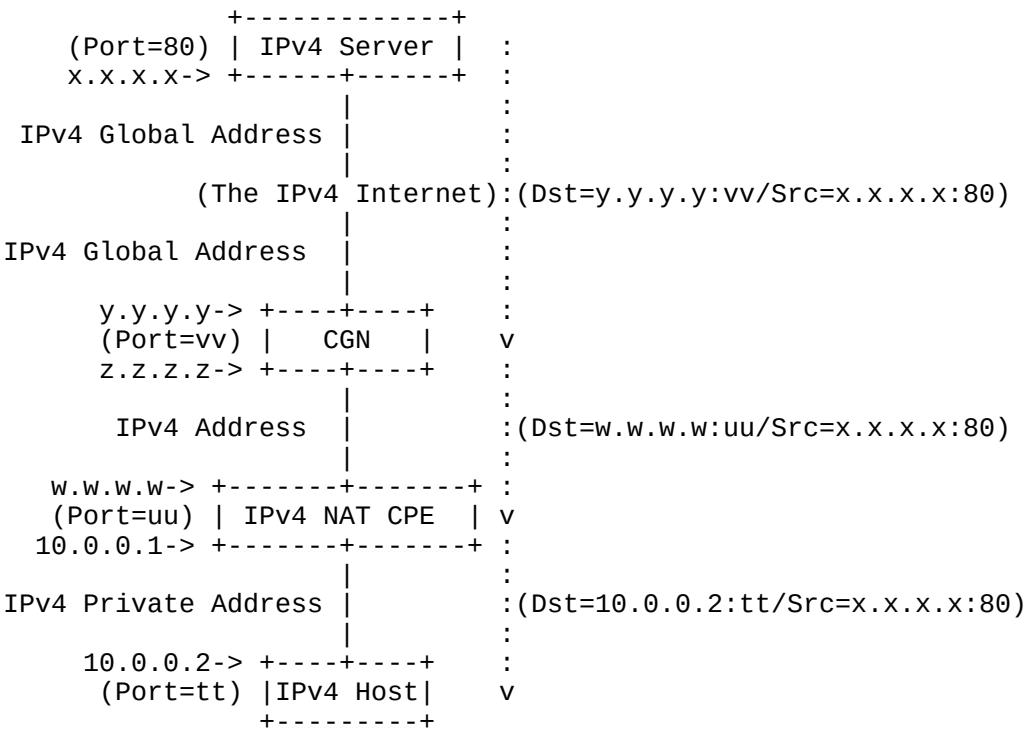
3. Behavior of NAT444 Model

The IPv6 packets from the host reach the IPv6 Internet without using NAT functionality.

The following figure shows the behavior of the IPv4 packet from the host to the IPv4 server via two NATs. The first NAT in CPE overwrites the Source IP Address and Source Port from 10.0.0.2:tt to w.w.w.w:uu. Then the second NAT in CGN overwrites them from w.w.w.w:uu to y.y.y.y:vv. Destination IP Address and Port are not overwritten.



The following figure explains the behavior of returning IPv4 packet via two NATs. The first NAT in CGN overwrites the Destination IP Address and Port Number from y.y.y.y:vv to w.w.w.w:uu. Then the second NAT in CPE overwrites them from w.w.w.w:u to 10.0.0.2:tt.



4. Pros and Cons of NAT444 Model

4.1. Pros of NAT444 Model

This network model has following advantages.

- This is the only network model that doesn’t require replacing CPEs those are owned by customers.
- This network model is composed of the present technology.
- This network model doesn’t require address family translation.
- This network model doesn’t require DNS rewriting.
- This network model doesn’t require additional fragment for the packets because it doesn’t use tunneling technology.

4.2. Cons of NAT444 Model

This network model has some technical restrictions.

- Some application such as SIP requires special treatment, because IP address is written in the payload of the packet. Special treatment means application itself aware double NAPT or both of two NAPTs

support inspecting and rewriting the packets.
- Because both IPv4 route and IPv6 route exist, it doubles the number of IGP route inside the CGN.
- UPnP doesn’t work with double NAPTs.

5. Acknowledgements

Thanks for the input and review by Shin Miyakawa, Shirou Niinobe, Takeshi Tomochika, Tomohiro Fujisaki, Dai Nishino, JP address community members, AP address community members and JPNIC members.

6. IANA Considerations

There are no IANA considerations.

7. Security Considerations

Each customer inside a CGN looks using the same Global Address from outside an ISP. In case of incidents, the ISP must have the function to trace back the record of each customer’s access without using only IP address.

If a Global Address of the CGN is listed on the blacklist, other customers who share the same address could be affected.

8. References

8.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC4925] Li, X., Dawkins, S., Ward, D., and A. Durand, "Softwire Problem Statement", RFC 4925, July 2007.

[I-D.ietf-behave-lsn-requirements] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for Carrier Grade NATs (CGNs)", draft-ietf-behave-lsn-requirements-07 (work in progress), June 2012.

8.2. Informative References

[I-D.shirasaki-isp-shared-addr]
Yamagata, I., Miyakawa, S., Nakagawa, A., Yamaguchi, J., and H. Ashida, "ISP Shared Address", draft-shirasaki-isp-shared-addr-07 (work in progress), January 2012.

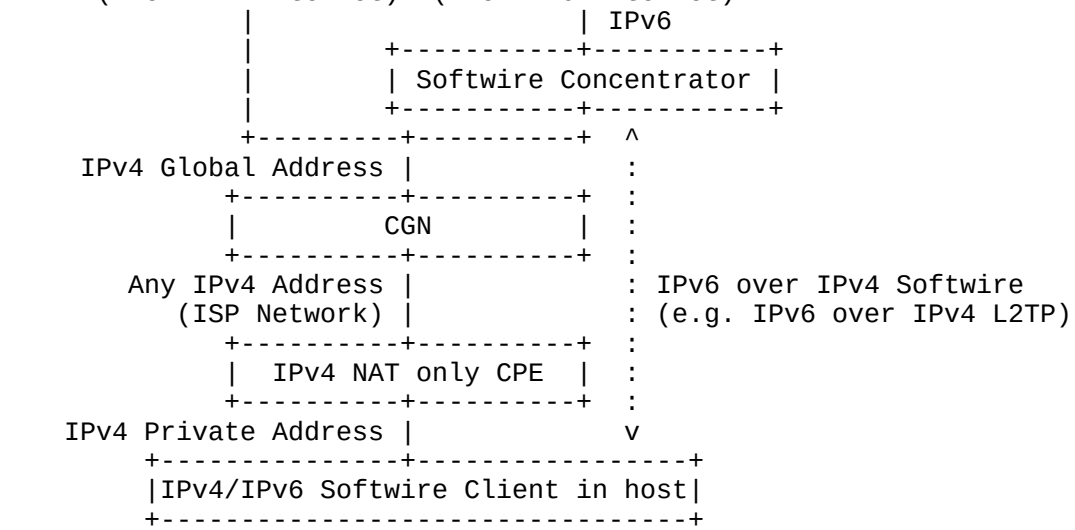
[I-D.shirasaki-nat444-isp-shared-addr]
Yamaguchi, J., Shirasaki, Y., Miyakawa, S., Nakagawa, A., and H. Ashida, "NAT444 addressing models", draft-shirasaki-nat444-isp-shared-addr-07 (work in progress), January 2012.

Appendix A. Example IPv6 Transition Scenario

The steps of IPv6 transition are as follows.

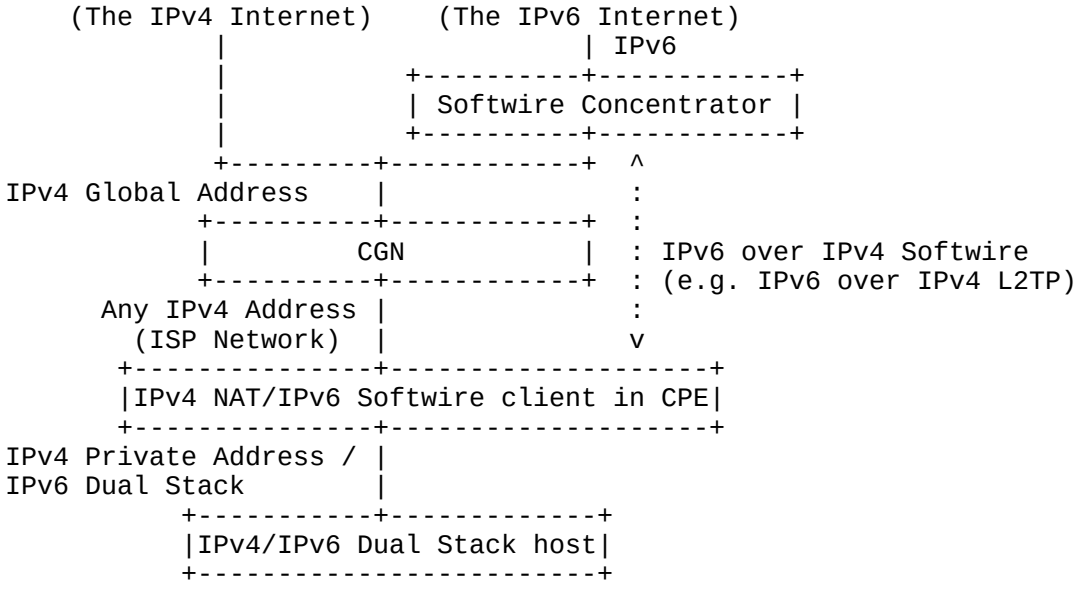
Step 1: Enabling softwire client in host

ISP provides IPv6 connectivity to customers with softwire [RFC4925]. ISP installs CGN and softwire concentrator in its network. A softwire client in host connects to the IPv6 internet via ISP's concentrator. ISP can use existing IPv4 equipments. Customers can just use existing CPE.



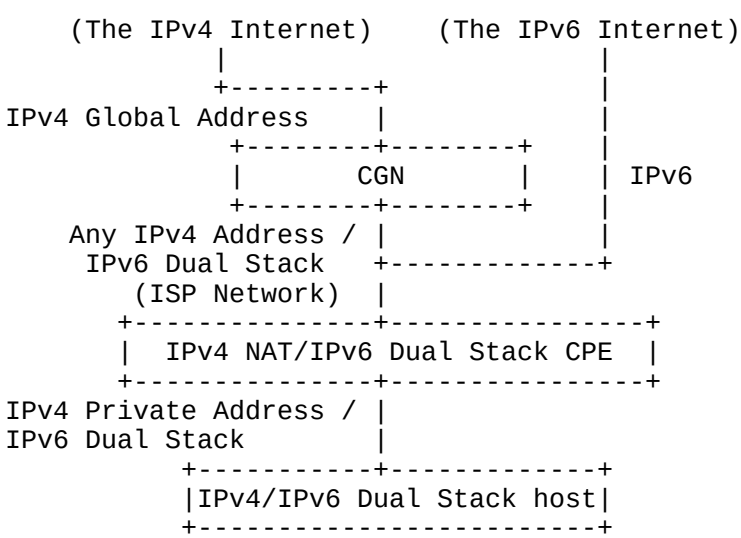
Step 2: Enabling softwire client in CPE

A customer enables softwire client in CPE. A softwire client in CPE connects to the IPv6 internet via ISP's concentrator. A Customer's network is now dual stack.



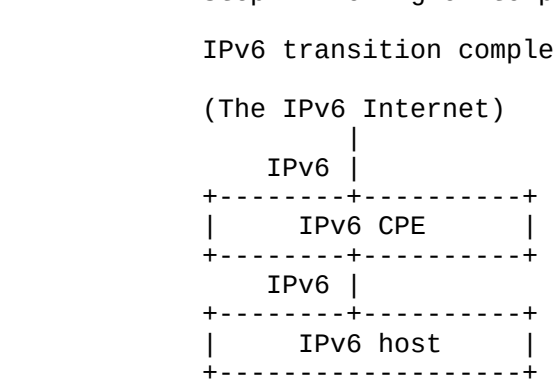
Step 3: Moving on to dual stack

ISP provides dual stack access to CPE. A CPE uplink is now dual stack.



Step 4: Moving on to pure IPv6

IPv6 transition completes.



Authors' Addresses

Ikuhei Yamagata
NTT Communications Corporation
Granpark Tower 17F, 3-4-1 Shibaura, Minato-ku
Tokyo 108-8118
Japan

Phone: +81 3 6733 8671
Email: ikuhei@nttv6.jp

Yasuhiro Shirasaki
NTT Communications Corporation
NTT Hibiya Bldg. 7F, 1-1-6 Uchisaiwai-cho, Chiyoda-ku
Tokyo 100-8019
Japan

Phone: +81 3 6700 8530
Email: yasuhiro@nttv6.jp

Akira Nakagawa
Japan Internet Exchange Co., Ltd. (JPIX)
Otemachi Building 21F, 1-8-1 Otemachi, Chiyoda-ku
Tokyo 100-0004
Japan

Phone: +81 90 9242 2717
Email: a-nakagawa@jpix.ad.jp

Jiro Yamaguchi
Fiber 26 Network Inc.
Haraguchi bldg., 5F, 3-11-4 Kanda Jinbo-cho, Chiyoda-ku
Tokyo 101-0051
Japan

Phone: +81 50 3463 6109
Email: jiro-y@f26n.jp

Hiroyuki Ashida
IS Consulting G.K.
12-17 Odenma-cho, Nihonbashi, Chuo-ku
Tokyo 103-0011
Japan

Email: assie@hir.jp