

Network Working Group
Internet Draft
Intended status: Informational
Expires: August 29, 2009

S. Jiang
D. Guo
Huawei Technologies Co., Ltd
B. Carpenter
University of Auckland
March 1, 2009

An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition
draft-jiang-incremental-cgn-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on August 29, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

Global IPv6 deployment was slower than originally expected in the last ten years. As IPv4 address exhaustion gets closer, the IPv4/IPv6 transition issues become more critical and complicated. Host-based transition mechanisms are not able to meet the requirements while most end users are not sufficiently expert to configure or maintain these transition mechanisms. Carrier Grade NAT with integrated transition mechanisms can simplify the operation of end users during the IPv4/IPv6 migration or coexistence period. This document proposes an incremental Carrier-Grade NAT (CGN) solution for IPv6 transition. It can provide IPv6 access services for IPv6-enabled end hosts and IPv4 access services for IPv4 end hosts while remaining most of legacy IPv4 ISP networks unchanged. It is suitable for the initial stage of IPv4/IPv6 migration. Unlike CGN alone, it also supports and encourages transition towards dual-stack or IPv6-only ISP networks.

Table of Contents

| | | |
|----------------------|--|-------------------|
| 1. | Introduction..... | 3 |
| 2. | Terminology..... | 4 |
| 3. | An Incremental CGN Solution..... | 4 |
| 3.1. | Incremental CGN Solution Overview..... | 4 |
| 3.2. | Behaviour of Dual-stack Home Gateway..... | 5 |
| 3.3. | Behaviour of Dual-stack Carrier-Grade NAT..... | 5 |
| 3.4. | Impact for end hosts and remaining networks..... | 6 |
| 4. | Migration towards IPv6 Core Network..... | 6 |
| 5. | Security Considerations..... | 6 |
| 6. | IANA Considerations..... | 7 |
| 7. | References..... | 7 |
| 7.1. | Normative References..... | 7 |
| 7.2. | Informative References..... | 7 |
| | Author's Addresses..... | 9 |

1. Introduction

Up to now, global IPv6 deployment does not happen as was expected 10 years ago. The progress was much slower than originally expected. Network providers were hesitant to take the first move while IPv4 was and is still working well. However, IPv4 address exhaustion is now confirmed to happen soon. The dynamically-updated IPv4 Address Report [[IPUSAGE](#)] has analyzed this issue. It predicts early 2011 for IANA unallocated address pool exhaustion and middle 2012 for RIR unallocated address pool exhaustion. Based on this fact, the Internet industry appears to have reached consensus that global IPv6 deployment is inevitable and has to be done quite quickly.

IPv4/IPv6 transition issues therefore become more critical and complicated for the soon-coming global IPv6 deployment. Host-based transition mechanisms alone are not able to meet the requirements. They are too complicated for most end users who do not have enough technical knowledge to configure or maintain these transition mechanisms. New transition mechanisms with simple user-side operation are needed.

Carried Grade NAT (CGN) alone creates operational problems, but does nothing to help IPv4/IPv6 transition. In fact it allows ISPs to delay the transition, and therefore causes double transition costs (once to add CGN, and again to support IPv6).

Carrier-Grade NAT that integrates multiple transition mechanisms can simplify the operation of end user services during the IPv4/IPv6 migration or coexistence period. CGNs are deployed on the network side and managed/maintained by professionals. On the user side, new CPE devices may be needed too. They may be provided by network providers, depending on the specific business model. Dual-stack lite [[DSLite](#)] is a CGN-based solution that supports transition, but it requires the ISP to upgrade its network to IPv6 immediately. Many ISPs hesitate to do this as the first step.

This document proposes an incremental CGN solution for IPv6 transition. The solution is similar to DS Lite, but the other way around. Technically, it mainly combines v4-v4 NAT with v6-over-v4 tunnelling functions along with some minor adjustment. It can provide IPv6 access services for IPv6-enabled end hosts and IPv4 access services for IPv4 end hosts, while leaving most of legacy IPv4 ISP networks unchanged. The deployment of this solution does not affect legacy IPv4 hosts with global IPv4 addresses at all. It is suitable for the initial stage of IPv4/IPv6 migration. It also supports transition towards dual-stack or IPv6-only ISP networks.

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].

3. An Incremental CGN Solution

Most ISP networks are still IPv4. Network providers are starting to provide IPv6 access services for end users. However, at the initial stage of IPv4/IPv6 migration, IPv4 connectivity and traffic would be the majority for ISP networks. ISPs would like to minimize the changes on their IPv4 networks. Switching the whole ISP network into IPv6-only would be considered as a radical strategy. Switching the whole ISP network to dual stack is less radical, but introduces operational costs and complications.

3.1. Incremental CGN Solution Overview

The incremental CGN solution we propose is illustrated as the following figure.

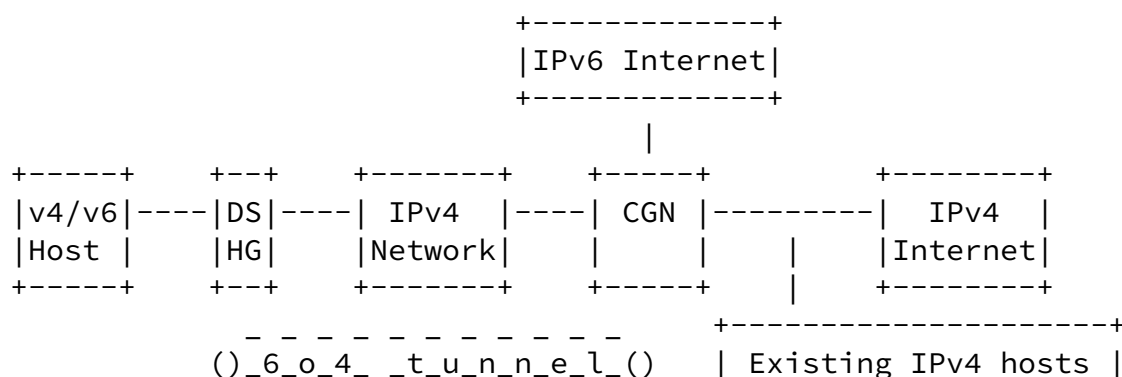


Figure 1: Phase 1 of incremental CGN solution with IPv4 ISP network

DS HG = Dual-Stack Home Gateway.

The above figure shows only Phase 1, in which the ISP has not significantly changed its IPv4 network. This solution enables IPv4 hosts to access the IPv4 Internet and IPv6 hosts to access the IPv6 Internet. A dual stack host can be treated as an IPv4 host when it uses IPv4 access service and as an IPv6 host when it uses IPv6 access service. In order to enable IPv4 hosts to access IPv6 Internet and IPv6 hosts to access IPv4 Internet, NAT-PT [RFC2766, [RFC4966](#)] (or its replacement) can be integrated with CGN. The integration of NAT-PT is out of scope for this document

Two new types of devices need to be deployed in this solution: a dual-stack home gateway, which may follow the requirements of [[6CPE](#)], and dual-stack Carrier-Grade NAT. The dual-stack home gateway integrates IPv4 forwarding and v6-over-v4 tunnelling functions. It may integrate v4-v4 NAT function, too. The dual-stack CGN integrates v6-over-v4 tunnelling and carrier-grade v4-v4 NAT functions. Modified 6RD [[6RD](#)] technology may be used to support v6-over-v4 tunnelling. Other tunnelling mechanisms such as ISATAP [[RFC5214](#)] could also be considered, but 6RD appears to fit well and allows re-use of existing support for 6to4 [[RFC3056](#)].

3.2. Behaviour of Dual-stack Home Gateway

When a dual-stack home gateway receives a data packet from an end host, it firstly checks whether the packet is IPv4 or IPv6. For IPv4 data, the HG can directly forward it if there is no v4-v4 NAT running on the HG. Or the HG translates packet source address from a HG-scope private IPv4 address into a CGN-scope private IPv4 address. The HG should record the v4-v4 address mapping information for inbound packets, just like normal NAT does.

For IPv6 data, the HG needs to encapsulate the data into an IPv4 tunnel, which sets the dual-stack CGN as another end. Then the HG sends the new IPv4 packet towards CGN.

The HG should record the mapping information between the tunnel and the source IPv6 address for inbound packets if HG uplinks to more

than one CGN. Detailed considerations for the use of multiple CGNs by one HG are for further study.

3.3. Behaviour of Dual-stack Carrier-Grade NAT

When a dual-stack CGN receives a data packet from a dual-stack home gateway, it firstly checks whether the packet is a normal IPv4 packet or a v6-over-v4 tunnel packet. For a normal IPv4 packet, the CGN translates packet source address from a CGN-scope private IPv4 address into a public IPv4 address, and then send it to IPv4 Internet. The CGN should record the v4-v4 address mapping information for inbound packets, just like normal NAT does. For a v6-over-v4 tunnel packet, the CGN needs to decapsulate it into the original IPv6 packet and then send it to IPv6 Internet. The CGN should record the mapping information between the tunnel and the source IPv6 address for inbound packets.

Depending on the deployed location of the CGN, it may use v6-over-v4 tunnels to connect to the IPv6 Internet.

[3.4.](#) Impact for end hosts and remaining networks

This solution does not affect the remaining networks at all. Legacy IPv4 ISP networks and their IPv4 devices remain in use. The existing IPv4 hosts, shown as the right box in Figure 1, either having global IPv4 addresses or behind v4-v4 NAT can connect to IPv4 Internet as it is now.

[3.5.](#) Discussion

It should be noted that for IPv4 traffic, this solution inherits all the problems of CGN (e.g., scaling, and the difficulty of supporting well-known ports for inbound traffic). Application layer problems created by double NAT are for further study.

However, for IPv6 traffic, a user behind the DS HG will see normal IPv6 service. It is strongly recommended that all IPv6 tunnels support a large MTU, at least 1500 bytes, to avoid fragmentation problems. This, and the absence of NAT problems for IPv6, will create an incentive for users and application service providers to prefer IPv6.

[4. Migration towards IPv6 Core Network](#)

When the core network starts transition to IPv6, this solution can easily be transitioned into Phase 2, in which the ISP network is either dual-stack or IPv6-only. For dual-stack ISP networks, dual-stack home gateways can simply switch off the v6-over-v4 function and forward both IPv6 and IPv4 traffic directly; dual-stack CGN should only keep v4-v4 NAT function. For IPv6-only ISP networks, the dual-stack lite solution, which also has dual-stack home gateway and CGN devices, can be adopted for Phase 2. The best business model for this solution is that CPE has integrated the functions for both Phase 1 and 2, and can automatically detect the change. Then when ISPs decide to switch from Phase 1 to Phase 2, it may be that only a configuration change or a minor software update is needed on the CGNs. The DS HG will then switch automatically to basic dual stack or DSLite mode. The only impact on the home user will be to receive a different IPv6 prefix. Note that if the 6RD mechanism is used in Phase 1, the user will most likely have a /64 prefix during Phase 1, but could get a shorter prefix such as /56 in Phase 2. This would be an improved service offering available as a result of the Phase 1 to Phase 2 transition.

[5. Security Considerations](#)

Security issues associated with NAT have been documented in [[RFC2663](#)] and [[RFC2993](#)].

Jiang, et al.

Expires August 29, 2009

[Page 6]

Internet-Draft [draft-jiang-incremental-cgn-00.txt](#)

March 2009

Further security analysis will be needed to understand double NAT security issues and tunnel security issues. However, since the tunnel exists entirely in a single ISP network, between the CPE and the CGN, the threat model is relatively simple. [[RFC4891](#)] describes how to protect tunnels using IPSec, but it is not clear whether this would be an important requirement.

The dual-stack home gateway will need to provide basic security for IPv6 [[6CPESec](#)]. Other aspects are described in [[RFC4864](#)].

[6. IANA Considerations](#)

This draft does not request any IANA action.

[7. References](#)

7.1. Normative References

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

7.2. Informative References

- [RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", [RFC 2663](#), August 1999.
- [RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", [RFC 2766](#), February 2000.
- [RFC2993] Hain, T., "Architectural Implications of NAT", [RFC 2993](#), November 2000.
- [RFC3056] B. Carpenter, K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", [RFC3056](#), February 2001.
- [RFC4864] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, "Local Network Protection for IPv6", [RFC4864](#), May 2007.
- [RFC4891] R. Graveman, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", [RFC4891](#), May 2007.
- [RFC4966] Aoun, C. and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", [RFC 4966](#), July 2007.

Jiang, et al.

Expires August 29, 2009

[Page 7]

Internet-Draft [draft-jiang-incremental-cgn-00.txt](#)

March 2009

- [RFC5214] F. Templin, T. Gleeson, and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", [RFC 5214](#), March 2008.
- [DSLite] A. Durand, R. Droms, B. Haberman, J. Woodyatt, "Dual-stack lite broadband deployments post IPv4 exhaustion", [draft-durand-softwire-dual-stack-lite-01](#), work in progress.
- [IPUSAGE] Huston, G., IPv4 Address Report, March 2009, <http://www.potaroo.net/tools/ipv4/index.html>.
- [6RD] R. Despres, "IPv6 Rapid Deployment on IPv4 infrastructures

(6rd)", [draft-despres-6rd-02](#), work in progress.

- [6CPE] H. Singh, "IPv6 CPE Router Recommendations", [draft-wbeebee-ipv6-cpe-router-03](#), work in progress.
- [6CPESec] J. Woodyatt, "Recommended Simple Security Capabilities in Customer Premises Equipment for Providing Residential IPv6 Internet Service", [draft-ietf-v6ops-cpe-simple-security-03](#), work in progress.

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxu Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836774

Email: shengjiang@huawei.com

Dayong Guo
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxu Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836284
Email: guoseu@huawei.com

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand
Email: brian.e.carpenter@gmail.com