

Internet Engineering Task Force (IETF)  
Request for Comments: 6264  
Category: Informational  
ISSN: 2070-1721

S. Jiang  
D. Guo  
Huawei  
B. Carpenter  
University of Auckland  
June 2011

## An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition

### Abstract

Global IPv6 deployment was slower than originally expected. As IPv4 address exhaustion approaches, IPv4 to IPv6 transition issues become more critical and less tractable. Host-based transition mechanisms used in dual-stack environments cannot meet all transition requirements. Most end users are not sufficiently expert to configure or maintain host-based transition mechanisms. Carrier-Grade NAT (CGN) devices with integrated transition mechanisms can reduce the operational changes required during the IPv4 to IPv6 migration or coexistence period.

This document proposes an incremental CGN approach for IPv6 transition. It can provide IPv6 access services for IPv6 hosts and IPv4 access services for IPv4 hosts while leaving much of a legacy ISP network unchanged during the initial stage of IPv4 to IPv6 migration. Unlike CGN alone, incremental CGN also supports and encourages smooth transition towards dual-stack or IPv6-only ISP networks. An integrated configurable CGN device and an adaptive home gateway (HG) device are described. Both are reusable during different transition phases, avoiding multiple upgrades. This enables IPv6 migration to be incrementally achieved according to real user requirements.

### Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc6264>.

## Copyright Notice

Copyright (c) 2011 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction .....	2
2. An Incremental CGN Approach .....	4
2.1. Incremental CGN Approach Overview .....	4
2.2. Choice of Tunneling Technology .....	5
2.3. Behavior of Dual-Stack Home Gateway .....	6
2.4. Behavior of Dual-Stack CGN .....	6
2.5. Impact for Existing Hosts and Unchanged Networks .....	7
2.6. IPv4/IPv6 Intercommunication .....	7
2.7. Discussion .....	8
3. Smooth Transition towards IPv6 Infrastructure .....	8
4. Security Considerations .....	10
5. Acknowledgements .....	10
6. References .....	10
6.1. Normative References .....	10
6.2. Informative References .....	11

## 1. Introduction

Global IPv6 deployment did not happen as was forecast 10 years ago. Network providers were hesitant to make the first move while IPv4 was and is still working well. However, IPv4 address exhaustion is imminent. The dynamically updated IPv4 Address Report [IPUSAGE] has analyzed this issue. IANA unallocated address pool exhaustion occurred in February 2011, and at the time of publication, the site predicts imminent exhaustion for Regional Internet Registry (RIR)

unallocated address pools. Based on this fact, the Internet industry appears to have reached consensus that global IPv6 deployment is inevitable and has to be done expeditiously.

IPv4 to IPv6 transition issues therefore become more critical and complicated for the approaching global IPv6 deployment. Host-based transition mechanisms alone are not able to meet the requirements in all cases. Therefore, network-based supporting functions and/or new transition mechanisms with simple user-side operation are needed.

Carrier-Grade NAT (CGN) [CGN-REQS], also called NAT444 CGN or Large Scale NAT, compounds IPv4 operational problems when used alone but does nothing to encourage IPv4 to IPv6 transition. Deployment of NAT444 CGN allows ISPs to delay the transition and therefore causes double transition costs (once to add CGN and again to support IPv6).

CGN deployments that integrate multiple transition mechanisms can simplify the operation of end-user services during the IPv4 to IPv6 migration and coexistence periods. CGNs are deployed on the network side and managed/maintained by professionals. On the user side, new home gateway (HG) devices may be needed too. They may be provided by network providers, depending on the specific business model. Dual-stack lite [DS-LITE], also called DS-Lite, 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. Theoretically, DS-Lite can be used with double encapsulation (IPv4-in-IPv6-in-IPv4), but this seems even less likely to be accepted by an ISP and is not discussed in this document.

This document proposes an incremental CGN approach for IPv6 transition. It does not define any new protocols or mechanisms but describes how to combine existing proposals in an incremental deployment. The approach is similar to DS-Lite but the other way around. It mainly combines v4-v4 NAT with v6-over-v4 tunneling functions. It can provide IPv6 access services for IPv6-enabled hosts and IPv4 access services for IPv4 hosts while leaving most of legacy IPv4 ISP networks unchanged. The deployment of this technology does not affect legacy IPv4 hosts with global IPv4 addresses at all. It is suitable for the initial stage of IPv4 to IPv6 migration. It also supports transition towards dual-stack or IPv6-only ISP networks.

A smooth transition mechanism is also described in this document. It introduces an integrated configurable CGN device and an adaptive HG device. Both CGN and HG are reusable devices during different transition periods, so they do not need to be replaced as the transition proceeds. This enables IPv6 migration to be incrementally achieved according to the real user requirements.



stack host is treated as an IPv4 host when it uses IPv4 access service and as an IPv6 host when it uses an IPv6 access service. In order to enable IPv4 hosts to access the IPv6 Internet and IPv6 hosts to access IPv4 Internet, NAT64 can be integrated with the CGN; see Section 2.6 for details regarding IPv4/IPv6 intercommunication. The integration of such mechanisms is out of scope for this document.

Two types of devices need to be deployed in this approach: a dual-stack home gateway (HG) and a dual-stack CGN. The dual-stack home gateway integrates both IPv6 and IPv4 forwarding and v6-over-v4 tunneling functions. It should follow the requirements of [RFC6204], including IPv6 prefix delegation. It may also integrate v4-v4 NAT functionality. The dual-stack CGN integrates v6-over-v4 tunneling and v4-v4 CGN functions as well as standard IPv6 and IPv4 routing.

The approach does not require any new mechanisms for IP packet forwarding or encapsulation or decapsulation at tunnel endpoints. The following sections describe how the HG and the incremental CGN interact.

## 2.2. Choice of Tunneling Technology

In principle, this model will work with any form of tunnel between the dual-stack HG and the dual-stack CGN. However, tunnels that require individual configuration are clearly undesirable because of their operational cost. Configured tunnels based directly on [RFC4213] are therefore not suitable. A tunnel broker according to [RFC3053] would also have high operational costs and be unsuitable for home users.

6rd [RFC5569, RFC5969] technology appears suitable to support v6-over-v4 tunneling with low operational cost. Generic Routing Encapsulation (GRE) [RFC2784] with an additional auto-configuration mechanism is also able to support v6-over-v4 tunneling. Other tunneling mechanisms such as 6over4 [RFC2529], 6to4 [RFC3056], the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) [RFC5214], or Virtual Enterprise Traversal (VET) [RFC5558] could be considered. If the ISP has an entirely MPLS infrastructure between the HG and the dual-stack CGN, it would also be possible to use a IPv6 Provider Edge (6PE) [RFC4798] tunnel directly over MPLS. This would, however, only be suitable for an advanced HG that is unlikely to be found as a consumer device and is not further discussed here. To simplify the discussion, we assume the use of 6rd.

### 2.3. Behavior of Dual-Stack Home Gateway

When a dual-stack home gateway receives a data packet from a host, it will determine whether the packet is an IPv4 or IPv6 packet. The packet will be handled by an IPv4 or IPv6 stack as appropriate. For IPv4, and in the absence of v4-v4 NAT on the HG, the stack will simply forward the packet to the CGN, which will normally be the IPv4 default router. If v4-v4 NAT is enabled, the HG translates the packet source address from an HG-scope private IPv4 address into a CGN-scope IPv4 address, performs port mapping if needed, and then forwards the packet towards the CGN. The HG records the v4-v4 address and port mapping information for inbound packets, like any other NAT.

For IPv6, the HG needs to encapsulate the data into an IPv4 tunnel packet, which has the dual-stack CGN as the IPv4 destination. The HG sends the new IPv4 packet towards the CGN, for example, using 6rd.

If the HG is linked to more than one CGN, it will record the mapping information between the tunnel and the source IPv6 address for inbound packets. Detailed considerations for the use of multiple CGNs by one HG are for further study.

IPv4 packets from the CGN and encapsulated IPv6 packets from the CGN will be translated or decapsulated according to the stored mapping information and forwarded to the customer side of the HG.

### 2.4. Behavior of Dual-Stack CGN

When a dual-stack CGN receives an IPv4 data packet from a dual-stack home gateway, it will determine whether the packet is a normal IPv4 packet, which is non-encapsulated, or a v6-over-v4 tunnel packet addressed to a tunnel endpoint within the CGN. For a normal IPv4 packet, the CGN translates the packet source address from a CGN-scope IPv4 address into a public IPv4 address, performs port mapping if necessary, and then forwards it normally to the IPv4 Internet. The CGN records the v4-v4 address and port mapping information for inbound packets, just like a normal NAT does. For a v6-over-v4 tunnel packet, the tunnel endpoint within the CGN will decapsulate it into the original IPv6 packet and then forward it to the IPv6 Internet. The CGN records 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 a further v6-over-v4 tunnel to connect to the IPv6 Internet.

Packets from the IPv4 Internet will be appropriately translated by the CGN and forwarded to the HG, and packets from the IPv6 Internet will be tunneled to the appropriate HG, using the stored mapping information as necessary.

## 2.5. Impact for Existing Hosts and Unchanged Networks

This approach does not affect the unchanged parts of ISP networks at all. Legacy IPv4 ISP networks and their IPv4 devices remain in use. The existing IPv4 hosts, shown as the lower right box in Figure 1, having either global IPv4 addresses or behind v4-v4 NAT, can connect to the IPv4 Internet as it is now. These hosts, if they are upgraded to become dual-stack hosts, can access the IPv6 Internet through the IPv4 ISP network by using IPv6-over-IPv4 tunnel technologies. (See Section 2.7 for a comment on MTU size.)

## 2.6. IPv4/IPv6 Intercommunication

For obvious commercial reasons, IPv6-only public services are not expected as long as there is a significant IPv4-only customer base in the world. However, IPv4/IPv6 intercommunication may become an issue in many scenarios.

The IETF is expected to standardize a recommended IPv4/IPv6 translation algorithm, sometimes referred to as NAT64. It is specified in the following:

- o "Framework for IPv4/IPv6 Translation" [RFC6144]
- o "IPv6 Addressing of IPv4/IPv6 Translators" [RFC6052]
- o "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers" [RFC6147]
- o "IP/ICMP Translation Algorithm" [RFC6145]
- o "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers" [RFC6146]
- o "An FTP ALG for IPv6-to-IPv4 Translation" [FTP-ALG]

The service, as described in the IETF's "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment" [RFC6180], provides for stateless translation between hosts in an IPv4-only domain or hosts that offer an IPv4-only service and hosts with an IPv4-embedded IPv6 address in an IPv6-only domain. It additionally provides access from IPv6 hosts with general format addresses to hosts in an IPv4-only domain or hosts that offer an IPv4-only service. It does not provide any-to-any translation. One result is that client-only hosts in the IPv6 domain gain access to IPv4 services through stateful translation. Another result is that the IPv6 network operator has

the option of moving servers into the IPv6-only domain while retaining accessibility for IPv4-only clients through stateless translation of an IPv4-embedded IPv6 address.

Also, "Architectural Implications of NAT" [RFC2993] applies across the service just as in IPv4/IPv4 translation: apart from the fact that a system with an IPv4-embedded IPv6 address is reachable across the NAT, which is unlike IPv4, any assumption on the application's part that a local address is meaningful to a remote peer and any use of an IP address literal in the application payload is a source of service issues. In general, the recommended mitigation for this is as follows:

- o Ideally, applications should use DNS names rather than IP address literals in URLs, URIs, and referrals, and in general be network layer agnostic.
- o If they do not, the network may provide a relay or proxy that straddles the domains. For example, an SMTP Mail Transfer Agent (MTA) with both IPv4 and IPv6 connectivity handles IPv4/IPv6 translation cleanly at the application layer.

## 2.7. Discussion

For IPv4 traffic, the incremental CGN approach inherits all the problems of CGN address-sharing techniques [ADDR-ISSUES] (e.g., scaling and the difficulty of supporting well-known ports for inbound traffic). Application-layer problems created by double NAT are beyond the scope of this document.

For IPv6 traffic, a user behind the DS HG will see normal IPv6 service. We observe that an IPv6 tunnel MTU of at least 1500 bytes would ensure that the mechanism does not cause excessive fragmentation of IPv6 traffic or excessive IPv6 path MTU discovery interactions. This, and the absence of NAT problems for IPv6, will create an incentive for users and application service providers to prefer IPv6.

ICMP filtering [RFC4890] may be included as part of CGN functions.

## 3. Smooth Transition towards IPv6 Infrastructure

Transition from pure NAT444 CGN or 6rd to the incremental CGN approach is straightforward. The HG and CGN devices and their locations do not have to be changed; only software upgrading may be needed. In the ideal model, described below, even software upgrading is not necessary; reconfiguration of the devices is enough. NAT444 CGN solves the public address shortage issues in the current IPv4



infrastructure. However, it does not contribute towards IPv6 deployment at all. The incremental CGN approach can inherit NAT444 CGN functions while providing overlay IPv6 services. 6rd mechanisms can also transform smoothly into this incremental CGN model. However, the home gateways need to be upgraded correspondingly to perform the steps described below

The incremental CGN can also easily be transitioned to an IPv6-enabled infrastructure, in which the ISP network is either dual-stack or IPv6-only.

If the ISP prefers to move to dual-stack routing, the HG should simply switch off its v6-over-v4 function when it observes native IPv6 Router Advertisement (RA) or DHCPv6 traffic and then forward both IPv6 and IPv4 traffic directly while the dual-stack CGN keeps only its v4-v4 NAT function.

However, we expect ISPs to choose the approach described as incremental CGN here because they intend to avoid dual-stack routing and to move incrementally from IPv4-only routing to IPv6-only routing. In this case, the ideal model for the incremental CGN approach is that of an integrated configurable CGN device and an adaptive HG device. The integrated CGN device will be able to support multiple functions, including NAT444 CGN, 6rd router (or an alternative tunneling mechanism), DS-Lite, and dual-stack forwarding.

The HG has to integrate the corresponding functions and be able to detect relevant incremental changes on the CGN side. Typically, the HG will occasionally poll the CGN to discover which features are operational. For example, starting from a pure IPv4-only scenario (in which the HG treats the CGN only as an IPv4 default router), the HG would discover (by infrequent polling) when 6rd became available. The home user would then acquire an IPv6 prefix. At a later stage, the HG would observe the appearance of native IPv6 Route Advertisement messages or DHCPv6 messages to discover the availability of an IPv6 service including DS-Lite. Thus, when an ISP decides to switch from incremental CGN to DS-Lite CGN, only a configuration change or a minor software update is needed on the CGNs. The home gateway would detect this change and switch automatically to DS-Lite mode. The only impact on the home user will be to receive a different IPv6 prefix.

In the smooth transition model, both CGN and HG are reusable devices during different transition periods. This avoids potential multiple upgrades. Different regions of the same ISP network may be at different stages of the incremental process, using identical

equipment but with different configurations of the incremental CGN devices in each region. Thus, IPv6 migration may be incrementally achieved according to the real ISP and customer requirements.

#### 4. Security Considerations

Security issues associated with NAT have been documented in [RFC2663] and [RFC2993]. Security issues for large-scale address sharing, including CGN, are discussed in [ADDR-ISSUES]. The present specification does not introduce any new features to CGN itself and hence no new security considerations. Security issues for 6rd are documented in [RFC5569] and [RFC5969], and those for DS-Lite are discussed in [DS-LITE].

Since the tunnels proposed here exist entirely within a single ISP network between the HG/CPE and the CGN, the threat model is relatively simple. [RFC4891] describes how to protect tunnels using IPsec, but an ISP could reasonably deem its infrastructure to provide adequate security without the additional protection and overhead of IPsec. The intrinsic risks of tunnels are described in [RFC6169], which recommends that tunneled traffic should not cross border routers. The incremental CGN approach respects this recommendation. To avoid other risks caused by tunnels, it is important that any security mechanisms based on packet inspection and any implementation of ingress filtering are applied to IPv6 packets after they have been decapsulated by the CGN. The dual-stack home gateway will need to provide basic security functionality for IPv6 [RFC6092]. Other aspects are described in [RFC4864].

#### 5. Acknowledgements

Useful comments were made by Fred Baker, Dan Wing, Fred Templin, Seiichi Kawamura, Remi Despres, Janos Mohacsi, Mohamed Boucadair, Shin Miyakawa, Joel Jaeggli, Jari Arkko, Tim Polk, Sean Turner, and other members of the IETF V6OPS working group.

#### 6. References

##### 6.1. Normative References

- [RFC2529] Carpenter, B. and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC 2529, March 1999.
- [RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

- [RFC5569] Despres, R., "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC 5569, January 2010.
- [RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.

## 6.2. Informative References

- [RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.
- [RFC2993] Hain, T., "Architectural Implications of NAT", RFC 2993, November 2000.
- [RFC3053] Durand, A., Fasano, P., Guardini, I., and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.
- [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.
- [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
- [RFC4798] De Clercq, J., Ooms, D., Prevost, S., and F. Le Faucheur, "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)", RFC 4798, February 2007.
- [RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.
- [RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.
- [RFC4891] Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC 4891, May 2007.
- [RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.
- [RFC5558] Templin, F., Ed., "Virtual Enterprise Traversal (VET)", RFC 5558, February 2010.

- [RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.
- [RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.
- [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.
- [RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.
- [RFC6169] Krishnan, S., Thaler, D., and J. Hoagland, "Security Concerns with IP Tunneling", RFC 6169, April 2011.
- [RFC6180] Arkko, J. and F. Baker, "Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment", RFC 6180, May 2011.
- [RFC6204] Singh, H., Beebe, W., Donley, C., Stark, B., and O. Troan, Ed., "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011.
- [IPUSAGE] G. Huston, IPv4 Address Report, June 2011, <http://www.potaroo.net/tools/ipv4/index.html>.
- [DS-LITE] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", Work in Progress, May 2011.
- [ADDR-ISSUES] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", Work in Progress, March 2011.

[CGN-REQS] Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common requirements for IP address sharing schemes", Work in Progress, March 2011.

[FTP-ALG] van Beijnum, I., "An FTP ALG for IPv6-to-IPv4 Translation", Work in Progress, May 2011.

#### Authors' Addresses

Sheng Jiang  
Huawei Technologies Co., Ltd  
Huawei Building, No.3 Xinxu Rd.,  
Shang-Di Information Industry Base, Hai-Dian District  
Beijing 100085  
P.R. China  
EMail: jiangsheng@huawei.com

Dayong Guo  
Huawei Technologies Co., Ltd  
Huawei Building, No.3 Xinxu Rd.,  
Shang-Di Information Industry Base, Hai-Dian District  
Beijing 100085  
P.R. China  
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

