Issues when translating between IPv4 and IPv6
draft-vanderpol-v6ops-translation-issues-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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/1id-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 July 28, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

During the transition from IPv4 to IPv6 both protocols will be used simultaneously. Most nodes will support both protocols and will be able to communicate via both IPv4 and IPv6 transport. Problems arise when a node only supports IPv4 and it wants to communicate with a node that only supports IPv6. Translation between the two IP protocols might be needed in some cases. This memo discusses the problems involved in translation between IPv4 and IPv6.
Table of Contents

1. Introduction .............................................. 3
2. Terminology .............................................. 3
3. Why is translation between IPv4 and IPv6 needed? ............ 3
4. The basic elements of protocol translation .................. 4
5. The problems with translation between IPv4 and IPv6 ......... 4
   5.1 The problems with address translation .................. 4
5.2 The problems with address discovery ..................... 5
5.2.1 The problem of getting unwanted translated addresses .... 6
5.2.2 The problem of getting AAAA answers for A queries ...... 7
5.3 Scaling problems with NAT in large setups ................ 8
6. IPv4 NAT or NAT-PT? ....................................... 8
7. When is translation between IPv4 and IPv6 needed? ........... 8
8. Security Considerations .................................... 8
   References ................................................. 9
   Authors’ Addresses ........................................ 9
A. Acknowledgements .......................................... 10
   Intellectual Property and Copyright Statements .............. 11
1. Introduction

During the transition from IPv4 to IPv6 both protocols will be used simultaneously. Most nodes will be able to communicate via both IPv4 and IPv6 transport (dual stack nodes). When communicating to a node that supports only one of the protocols, they choose that protocol. When communication via both protocols is possible, they usually default to IPv6. Problems arise when one node only supports IPv4 (IPv4-only) and the node it wants to communicate with only supports IPv6 (IPv6-only). In some cases the nodes can still communicate by using a proxy that supports both IPv4 and IPv6, e.g. by using an HTTP proxy for web traffic. If no such proxies are available and the nodes must communicate, translation between IPv4 and IPv6 could be used as a last resort. This memo discusses the problems involved with translation between IPv4 and IPv6.

2. Terminology

- IPv4-only node - A node that has an IPv4 stack and no IPv6 stack.
- IPv6-only node - A node that has an IPv6 stack and no IPv4 stack.
- dual stack node - A node that has both an IPv4 and an IPv6 stack. It may be connected to an IPv4 network, to an IPv6 network or to both.
- NAT - Network Address Translation. Usually, the translation between a private (RFC1918) IPv4 address and a globally routable IPv4 address and vice versa.
- NAT-PT - Network Address Translation, Protocol Translation. The translation between IPv4 addresses and semantically equivalent IPv6 address and vice versa.
- ALG - Application Level Gateway. A translator that knows how to translate the payload of traffic of a particular application when the payload contains IP addresses. Each application needs its own specific ALG.
- DNS-ALG - An Application Level Gateway for DNS.

3. Why is translation between IPv4 and IPv6 needed?

If one node only supports IPv4 and the other node only supports IPv6, no direct communication is possible. Fortunately, most nodes will be dual stack, which means they support both IP versions. However, nodes that are not upgraded yet support only IPv4. Problems arise...
when IPv6-only devices are introduced in the internet. Those devices can not communicate with IPv4-only nodes. When introducing such devices several questions should be asked.

- Is communication with IPv4-only devices needed or is it acceptable to support communication with dual stack and other IPv6-only nodes only.

- Is it possible to use dual stack proxies? E.g., IPv6-only appliances that offer web services can be reached via IPv4 transport by using dual stack HTTP proxies.

It should also be noted that IPv6-only nodes do not require translation to function. E.g., they can use DNS or email services when these services are setup with dual stack in mind. These issues are explained in [5] and [4]. For DNS resolving they can use a dual stack caching forwarder. For outgoing email they can use a dual stack mail drop. For incoming email they can use POP or IMAP via IPv6 transport to fetch their email from a central email server that receives email via IPv4 and IPv6 transport.

4. The basic elements of protocol translation

An obvious candidate for enabling communication between IPv4-only and IPv6-only nodes is NAT-PT [2]. The NAT-PT mechanism has two components, address and protocol translation as described in SIIT [1] and address discovery. Address and protocol translation is the processing of IP packets by a NAT; address discovery is the mechanism by which an IPv4-only or an IPv6-only node discovers the "translated address" to which packets should be sent. The NAT-PT specification proposes to solve address discovery by using a DNS-ALG, as specified in section 4 of NAT-PT [2].

5. The problems with translation between IPv4 and IPv6

Translation between IPv4 and IPv6 has many different problems. Some of these problems are summarized in the next sections. Section 5.1 summarizes the problems of NAT. Section 5.2 describes the problems with address discovery. Section 5.3 describes the scaling problems in large NAT setups.

5.1 The problems with address translation

Translation between IPv4 and IPv6 has all the problems of classic NAT as described in RFC 2993 [3].

- It breaks applications that have IP addresses in the payload. NAT only translates addresses in the IP headers, not in the payload.
ALGs must be used to translate addresses in the payloads. However, each application needs its own specific ALG. Therefore, it is hard to introduce new applications that need to use addresses in the payload of their packets.

- It breaks security protocols like IPsec and DNSSEC. The IPSec AH header contains a hash of the IP header. If the IP header is modified by the translator, the authenticity of the packet is lost. DNS-ALG cannot translate DNSSEC packets because it does not know the private key of the signature(s).

- It breaks IP multicast. Protocols like PIM, SDR, RTP, etc. have IP addresses in their payloads. NAT boxes need ALGs for all of these. Few if any NAT boxes support all the ALGs needed.

- It is a bottleneck and a single point of failure, because the NAT box needs to build state and therefore all the traffic must pass the NAT box.

5.2 The problems with address discovery

During the transition phase from IPv4 to IPv6 there will be IPv4-only, dual stack or IPv6-only nodes that want to communicate to other IPv4-only, dual stack or IPv6-only nodes. When both nodes do not speak the same version of IP, some translation will be needed. The table below shows the preferred version of IP address with respect to nodes A and B wanting to communicate with each other.
5.2.1 The problem of getting unwanted translated addresses

This section makes an important assumption: it assumes that the NAT-PT acts as a bridge between two networks, one IPv4-only and the other IPv6-only. As a result, the DNS-ALG will translate a DNS request for a AAAA record coming from the IPv6 node into a request for an A record, and vice versa. The problem is that address translation does not know if the traffic originates from an IPv4-only/IPv6-only node or from a dual stack node. When a dual stack node A wants to communicate with an IPv4-only node B, the dual stack node A gets either the IPv4 address of B (preferred) or an IPv6 address which is some kind of translation of the IPv4 address of B. This latter situation is not wanted, because it means unnecessary translation between IPv4 and IPv6. This is shown in the table below.

<table>
<thead>
<tr>
<th>+ A</th>
<th></th>
<th>dual stack</th>
<th>IPv6-only</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4</td>
<td>IPv4 or IPv6</td>
<td>IPv6</td>
</tr>
<tr>
<td>IPv6</td>
<td>t(IPv4)-&gt;IPv6</td>
<td>IPv6</td>
<td>IPv6</td>
</tr>
</tbody>
</table>

\[ t(IPv6)->IPv4 \] means that some translation is involved which produces some IPv4 address for an IPv6-only host.

\[ t(IPv4)->IPv6 \] means that some translation is involved which produces some IPv6 address for an IPv4-only host.
The boxes with XXX-es are the cases where address translation could result in unwanted translation.

5.2.2 The problem of getting AAAA answers for A queries

Within an IPv6 NAT-PT domain, an application asking for an A record could be returned a translated AAAA record.

RFC2766 [2] section 4.2:

"...the DNS-ALG on the NAT-PT device forwards the original AAAA/A6 query to the external DNS system unchanged, as well as an A query for the same node. If an AAAA/A6 record exists for the destination, this will be returned to NAT-PT which will forward it, also unchanged, to the originating host.

If there is an A record for Node-C the reply also returns to the NAT-PT. The DNS-ALG then, translates the reply adding the appropriate PREFIX and forwards it to the originating device with any IPv6 addresses that might have learned."

RFC2766 is not clear on how a DNS-ALG should treat answers to A queries made by nodes within the NAT-PT domain. As a matter of fact, one could fear that a careless DNS-ALG would also intercept them and translate them into a AAAA form. In other words, nodes asking for an A record could be returned a AAAA record. Although this may not be a problem for simple IPv6-only applications, it may be a concern for
applications that ‘walk through’ the DNS structure and may pass information to peers.

5.3 Scaling problems with NAT in large setups

In large networks NAT-PT and/or DNS-ALG boxes can become a serious single point of failure, a bottleneck and a Denial Of Service (DOS) target. It may be necessary to spread the NAT-PT and/or DNS-ALG among several boxes. However, this is a very complicated operation. The NAT-PT and/or DNS-ALG boxes need to build state about address mappings. The setup must be carefully chosen, so that packets that need to be translated are routed through the box that has the proper state.

6. IPv4 NAT or NAT-PT?

Nodes on an IPv6-only network that want to communicate with IPv4-only nodes do not necessarily need to use NAT-PT. If the nodes are dual stack, they can use IPv4-in-IPv6 tunneling through the IPv6-only network. In cases where there are only private IPv4 (RFC1918) addresses available, it still makes sense to use IPv4-in-IPv6 tunneling combined with classical IPv4 NAT, because there is extensive deployment experience with IPv4 NAT, but little experience with NAT-PT.

7. When is translation between IPv4 and IPv6 needed?

Some argue that IPv6-only devices will show up on a large scale soon because of new appliances that do not have enough memory to support both IPv4 and IPv6. Others argue that the cost of a dual or hybrid stack is not much more than that of an IPv6-only stack.

Others think translation is only needed in the final phase of the transition from IPv4 to IPv6. Eventually, almost all nodes will be IPv6 enabled and only a few legacy systems are still IPv4-only. When communicating with those legacy systems, translation might be needed.

8. Security Considerations

As described in section Section 5.1 NAT-PT breaks security protocols like IPsec and DNSSEC. Because all traffic needs to go through the NAT boxes, these boxes can become a target for a DOS attack.

Some argue that an advantage of NAT is that there is no traffic possible to an inside address/port until the NAT box has built state for that address/port combination. That is only partially true. As soon as the inside address/port has sent a packet outside, the NAT box has state for that address/port combination and that address/port
combination is globally reachable. For security reasons, it is much better to have a more controlled security mechanism.

A host inside a NAT-PT network when trying to traverse through the NAT box gets an global address. However, this host can send packets with different spoofed source addresses which will make the NAT box exhaust its address pool. In this case, no other legitimate hosts can communicate to the other side of the translator, because the translator has no more addresses to give. This can be a serious problem in large NAT-PT networks.

References


Authors’ Addresses

Ronald van der Pol
NLnet Labs
Kruislaan 419
Amsterdam 1098 VA
NL

EMail: Ronald.vanderPol@nlnetlabs.nl
Appendix A. Acknowledgements

The authors gratefully acknowledge the contributions of: Rob Austein, Christian Huitema, and Daniel Soohong.
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the
Internet Society.