NAT-PT DNS ALG solutions
draft-hallin-natpt-dns-alg-solutions-01

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 January 22, 2003.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

There is an ongoing discussion about the impact of IPv4 to IPv6 transition mechanisms such as NAT-PT (RFC2766). [NAT-PT-ISSUES] identifies several problems around the DNS ALG functionality in NAT-PT. This document proposes possible solutions to some of the problems illustrated in [NAT-PT-ISSUES] and to additional issues with the DNS ALG functionality in NAT-PT.
Table of Contents

1. Introduction ................................................. 3
2. Solutions to some of the problems described in [NAT-PT-ISSUES] 3
   2.1 AAAA answers for A queries .............................. 3
   2.2 Source Address Selection/Destination ordering ............ 3
   2.3 NAT-PT & IPv6 default router ............................ 7
   2.4 IPv4 Address assignment for incoming connections (IPv4 to
       IPv6) .................................................. 7
3. Solutions to additional problems with the NAT-PT DNS ALG ...... 8
   3.1 Reverse queries from IPv6 to IPv4 ........................ 8
   3.2 Truncated DNS messages ................................. 8
   3.3 DSTM cannot work with NAT-PT DNS-ALG .................... 9
4. Security Considerations .......................................... 9
   References .................................................. 9
   Authors' Addresses ......................................... 10
   Full Copyright Statement .................................... 11
1. Introduction

NAT-PT is an IPv6 to IPv4 transition mechanism that enables IPv6-only clients to use IPv4 services. NAT-PT works by combining protocol translation with [NAT].

Due to the long address format of IPv6 it is believed that IPv6 users will use DNS a lot. To enable DNS traffic through a NAT-PT a special Application Level Gateway (ALG) is provided. The DNS-ALG within a NAT-PT will be a very important component. Some problems have been recognized with the DNS-ALG described in [NAT-PT]. The issues discussed include that packets will be translated even when it is not necessary and that all IPv6 traffic has to go through the NAT-PT, whether or not it is translated. Protocol translation is a potential bottleneck and it is important to limit its use. This document will describe possible solutions to some of these problems as well as to other issues with the DNS ALG functionality in NAT-PT.

2. Solutions to some of the problems described in [NAT-PT-ISSUES]

2.1 AAAA answers for A queries

[NAT-PT-ISSUES] points out that it is not specified in [NAT-PT] how a DNS ALG should treat answers to A queries from internal hosts.

This problem arises due to stateless nature of DNS ALG. If DNS-ALG had kept information about the (A) query, then incoming (A) reply could be mapped to that query using previously stored information. A DNS query contains {queryid, type}, which could be matched against {replyid, type} in the DNS response. Additionally, the tuple {srcaddr, dstaddr, sport, dport, proto} will be used for integrity check. Once a DNS reply is received and processed, the associate state will be removed by DNS ALG.

=> NAT-PT DNS-ALG will match DNS replies with queries using the minimal state stored when a DNS query, sent by IPv6-only nodes, traversed NAT-PT. This will ensure that a host sending (A) query will always receive (A) reply, but not (AAAA) reply.

2.2 Source Address Selection/Destination ordering

[NAT-PT-ISSUES] illustrates that the communication between a node within the NAT-PT domain and an external dual-stack host, will select the translated path over the native IPv6 path.

Let’s assume that an IPv6-only node X within a NAT-PT domain wants to
communicate with a dual-stack host Y on the public Internet. The host Y has published both IPv4 (A) and IPv6 (AAAA) addresses in the DNS. X will query IPv6 (AAAA) for Y. The NAT-PT will intercept the IPv6 DNS query. In the NAT-PT standard it is specified that the DNS-ALG should forward the intercepted IPv6 queries in an unchanged version together with a translated IPv4 DNS query (A) to the DNS server. The DNS server will return both an IPv4 and an IPv6 DNS reply to the NAT-PT. The idea is that the IPv4 DNS reply will have an empty answer section if the destination host is IPv6 and that the IPv6 DNS reply will have an empty answer section if the destination host is IPv4. Both DNS replies are forwarded to the requesting IPv6 client. The IPv6 DNS reply will be forwarded in unchanged form and the IPv4 DNS reply will be translated to an IPv6 DNS reply. The requesting client will receive two IPv6 DNS replies, one empty and one containing the IPv6 address of the destination host. Depending on if the destination host is IPv4 or IPv6, the address will either be a native IPv6 or a translated IPv4 address.

This works fine when communicating with IPv6-only or IPv4-only hosts. Problems occur when the destination host is dual-stack IPv4/IPv6 such as the host Y. The client will then receive two IPv6 DNS replies with answer sections containing addresses. As the prefix associated to the translated address belongs to same site as X’s IPv6 address, when X will use source address selection/destination address ordering it will result to longest prefix match and will choose the "translated" address over the native one. The result is that protocol translation will be used even if native IPv6 communication is possible.

An alternate approach is for the DNS ALG to send the IPv6 DNS query in unchanged form, but ignore to send the translated IPv4 DNS query. The returning IPv6 DNS reply is analysed. If the answer section of the IPv6 DNS reply contains addresses, it is forwarded in unchanged form to the IPv6-only client. A special case is if the IPv6 DNS reply contains the name error flag, in this case the domain name does not exist and the IPv6 DNS reply can be forwarded to the IPv6 only client in unchanged form.

If the answer section of the IPv6 DNS reply does not contain any addresses and the name error flag is not set, it is probable that the destination host is IPv4 and protocol translation is required. The DNS reply is then converted to an IPv4 DNS request and sent to the DNS server. The returning IPv4 DNS reply will be translated to IPv6 and forwarded to the IPv6-only client. The negative effect of this method is increased DNS latency when communicating with IPv4-only hosts. This is because the empty IPv6 DNS message has to arrive to the NAT-PT before the IPv4 (a) request can be sent.
A second alternative is to send both AAAA and A (translated AAAA) queries simultaneously. The returning replies are analyzed. If the answer section does not contain any address, DNS-ALG will silently discard this reply. If the answer section contains an IPv6 address, AAAA reply should be forwarded unchanged. If the first returned reply is an IPv4 address, DNS-ALG will hold this for N time units, after which the A reply will be translated to AAAA and forwarded. Within the time interval of N units, if a AAAA answer is returned, AAAA reply will be sent and (A) will be discarded. The exact value of N is implementation dependant and is usually short enough not to cause a DNS timeout at the IPv6-only client.
IPv6-only client                NAT-PT                IPv4 DNS server

AAAA query

-----------------------

AAAA query (unchanged form)

-----------------------

A query

-----------------------

AAAA reply

-----------------------

A reply

-----------------------

AAAA reply (unchanged form)

-----------------------

A reply (discard)

-----------------------

Figure 3: Case one, the destination host is IPv6 enabled

IPv6-only client                NAT-PT                IPv4 DNS server

AAAA query

-----------------------

AAAA query (unchanged form)

-----------------------

A query

-----------------------

A reply

-----------------------

A reply (hold)

-----------------------

AAAA reply

-----------------------

translated AAAA reply

-----------------------

(discard A)

-----------------------

Figure 4: Case two, the destination host is IPv4-only

=> This solution ensures that communication between nodes within the
NAT-PT domain always use native IPv6 communication when possible.
The price is added DNS latency.

---------------------------------------------------------------------
2.3 NAT-PT & IPv6 default router

The NAT-PT DNS ALG makes the assumption that the DNS traffic goes through the NAT-PT box. [NAT-PT-ISSUES] describes that this is ok when DNS resolution is done over IPv4. However, if it is done over IPv6, there is no reason why the DNS traffic will still go through the NAT-PT box unless the NAT-PT box is also the default IPv6 router of the site. The conclusion is that NAT-PT has to be the only default IPv6 router in the NAT-PT domain to work correctly with DNS-ALG.

This implicates that all IPv6 traffic has to go through the NAT-PT, whether or not it is translated. This raises scalability issues in larger networks. In a network with both IPv6-only and dual-stack hosts, this would require dual-stack hosts to be connected to a NAT-PT. This would not make any sense, since dual-stack hosts have no need for the services a NAT-PT provides (The exception is when NAT-PT is used in conjunction with DSTM).

However, a more scalable approach is that IPv6-only clients connected to the NAT-PT, do all IPv6 DNS resolution over translated IPv4. The IPv6-only clients set NAT-PT_PREFIX:ipv4_dns as their DNS server, where NAT-PT_PREFIX is the NAT-PT prefix in the NAT-PT domain and ipv4_dns is a DNS server in the IPv4 domain. All DNS messages will then be routed through the NAT-PT. Dual-stack nodes will continue to use their ordinary DNS server. Their DNS traffic will not be routed through the NAT-PT. Thus, dual-stack nodes have no contact with the NAT-PT in the network. The NAT-PT is not required to be the default IPv6 router of the site. Only traffic in need of translation will be routed through the NAT-PT. This set up works provided that the IPv4 DNS server supports IPv6 DNS.

An alternate approach is that IPv6-only nodes will define a DNS search list, where the IPv6 DNS server, reachable locally, is defined first, and NAT-PT_PREFIX:ipv4_dns appears next in that order. IPv6-only nodes that want to resolve AAAA (IPv6) names do not have to send DNS queries through NAT-PT.

=> It is not necessary for the NAT-PT to be the only default router in the IPv6 domain. The only traffic that has to go through the NAT-PT is the one that needs to be translated.

2.4 IPv4 Address assignment for incoming connections (IPv4 to IPv6)

IPv4 Address assignment for incoming connections (IPv4 to IPv6) works the same way as described in [NAT-PT]. If a network administrator is
cautious about denial of service attacks, it is possible not to configure forwarding to the IPv6 DNS server. IPv6 nodes with static bindings can still be reached from IPv4 by registering them in the IPv4 DNS server. Another method is to enable IPv6 on IPv4 nodes wanting to communicate with IPv6-only nodes.

3. Solutions to additional problems with the NAT-PT DNS ALG

3.1 Reverse queries from IPv6 to IPv4

The DNS-ALG described in [NAT-PT] does not support reverse queries from IPv6 to IPv4. Reverse querying is an important feature to support. For example, some applications uses reverse queries to check if the result of a name lookup is correct. By using the minor extension to [NAT-PT] presented below reverse querying from IPv6 to IPv4 is enabled.

If the IPv6 address in the IPv6 reverse query starts with the NAT-PT prefix, the DNS-ALG understands that this is a reverse query for an IPv4 node. The DNS-ALG will check for address binding to see if a mapping exists between the IPv6 address in PTR query and an IPv4 address. If there is a mapping the PTR query will be translated to IPv4. The translation works by replacing the string "IP6.INT" with "IN-ADDR.ARPA" and replacing the IPv6 address with the bound IPv4 address (in reverse order). Reverse queries concerning IPv6 addresses that don’t start with the NAT-PT prefix is forwarded to the DNS server in unchanged form. This enables correct reverse lookup of both native IPv6 and translated IPv4 addresses.

=> It is possible to support IPv6 to IPv4 reverse querying with minor additions to [NAT-PT].

3.2 Truncated DNS messages

When the DNS-ALG described in [NAT-PT] translates DNS replies from IPv4 to IPv6, it replaces the included IPv4 addresses with IPv6 addresses. An IPv4 address is 4 bytes long, while an IPv6 address is 16 bytes long. The result is that the translated message will be longer than the original message. DNS messages are usually sent using UDP. When transferring DNS messages over UDP, 512 bytes is the maximum DNS message length.

The obvious approach when implementing a DNS ALG is to truncate
translated DNS messages that exceed the maximum message length. However, some applications have problems with truncated DNS messages. Another possible solution is to remove resource records in the additional section of the DNS message and avoid truncation.

---

=> By removing resource records in the additional section, problems with truncated DNS messages are avoided while essentially providing the same information in the DNS message.

---

3.3 DSTM cannot work with NAT-PT DNS-ALG

[INTERACTION] points out that DSTM mechanism will never be triggered and used, because a host within the IPv6 domain will never receive a DNS response that contains an "A" record.

Section 2.1 presents the same problem. Clearly, the proposed solution will enable DSTM to work with NAT-PT DNS-ALG.

4. Security Considerations

The security issues identified in [NAT-PT-ISSUES] are still unsolved.

References


Authors’ Addresses

Per Hallin
Telia Research AB
SE-123 42 Farsta
Sweden

Phone: +46 8 713 81 08
EMail: Per.A.Hallin@telia.se

Suresh Satapati
Cisco Systems, Inc.
San Jose, CA 95134
USA

EMail: satapati@cisco.com