Network Working Group
Internet-Draft
Expires: December 21, 2006

T. Chown
University of Southampton

June 19, 2006

The Cost of Application Development with NATs
draft-chown-cost-of-nat-00

Status of this Memo

Copyright Notice

Abstract

The deployment of IP Network Address Translators (NATs) for IPv4 has become very pervasive in the last 10-12 years. The original goal of NAT was to conserve IP address space, but the technology has now become very popular in home and SOHO type networks, as well as many larger organisations, for a variety of reasons. At the same time, the introduction of NAT adds a cost for application and service developers. This document presents a brief overview of the history of NAT, alongside a list of ongoing work related to NAT workarounds for current IETF protocol designs. The document intends to present a

neutral view of the cost of NAT for discussion in the IETF and wider community.

Table of Contents

1. Introduction

In this text, we present a very brief overview of the origins of IP Network Address Translation (NAT), before looking at a wide range of ongoing IETF protocol and related design that is currently having to consider or work around NAT deployments. We include sections on:

- NAT traversal techniques
- Ongoing IETF work due to the presence of NATs
- Other NAT considerations

One goal of the text is to try to present an objective view of the cost of NAT in terms of application and service deployment. A by-product of the document may be to encourage application designers to consider IPv6 versions of applications, for which such workarounds are not required. It also highlights the long-term cost should NATs be deployed for IPv6 networks. While NATs are here to stay for IPv4, their introduction for IPv6 should be debated carefully.

This document may well overlap with some ongoing work in the BEHAVE Working Group of the IETF. The aim at present is to capture NAT issues in this text. The value of the text, and the purposes to which it may be placed, are open for discussion, possibly within that WG.

The basic specification of NAT [1] has been in existence for 12 years at the time of writing, and has since been extended [7]. The technology has undoubtedly allowed the Internet to grow with the limitations of IPv4 address space, by allowing multiple client devices to run local private [2] IP addresses on internal networks while often sharing just a single global IP address externally.

The pros and cons of using NAT, in terms of the architectural implications, have been documented before [6]. Protocol complications have also been described in a separate text [8]. Those keen to see the original Internet goal of transparency [5] retained have documented arguments in favour of avoiding the use of NAT. Whatever is written, the fact is that NAT is universally popular for its ease of deployment, in particular for home networking. However, there is a cost, and that is shifted to the application and protocol designers, who have to work around the limitations that NAT devices impose.

Some efforts have been made in terms of classifying NATs, for example NAT Classification Test Results [26], which is an ongoing IETF draft.

The IPv6 protocol [3] does not explicitly preclude the use of NAT. However, it is argued that the very raison d'etre of IPv6 is universal global addressability, and to use NAT would defeat the very purpose of deploying the new protocol. A work in progress on IPv6 Network Architecture Protection [24] describes how IPv6 protocol features can be used to achieve the same effect as NAT for site networks.

2. Specific NAT Traversal Methods

There are some existing well-known (public) NAT traversal methods.

2.1. ICE

The Interactive Connectivity Establishment (ICE) [21] protocol is a protocol for NAT traversal for multimedia session signaling protocols based on the offer/answer model, such as the Session Initiation Protocol (SIP). An additional draft has been published on reducing the amount of messaging required [27].

2.2. SIMCO

A draft of the Simple Middlebox Configuration (SIMCO) Protocol v3.0 [32] describes a protocol for controlling middleboxes such as firewalls and network address translators.

2.3. STUN

Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), or STUN before [10] offers one method of NAT traversal for UDP traffic. STUN is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet, as well as the global IP address used by the NAT. There is a STUN update [20] draft in progress. Another draft discusses a STUN-based Signalling Framework [31].

2.4. TURN

The TURN protocol [18] is now the subject of a draft describing it as a usage of STUN.

3. Application and Service Considerations

An existing RFC discusses application design guidelines [9] when considering NATs. The document provides recommendations to authors

of new protocols about the effects to consider when designing new protocols such that special handling is not required at NAT gateway points. It discusses the limitations, including the lack of availability of end-to-end IPsec. It makes recommendations such as using domain names rather than IP addresses where possible. The document lacks any firm conclusion, but presents a set of issues well.

3.1. HIP

The IRTF HIP WG is working on Middlebox Traversal Issues of Host Identity Protocol (HIP) Communication [25]. The text identifies and discusses issues in the current HIP specifications that affect communication across these types of middleboxes. Some HIP extensions for NAT traversal are defined in another draft [30].

3.2. IPv6

The Teredo [11] protocol specifies an IPv6 tunnelling mechanism that can work through NAT devices.

There is also an extension of TURN proposed in a draft on using a TURN extension for IPv4/IPv6 transition [19].

3.3. NSIS

The NSIS WG is working on a NAT/Firewall NSIS Signaling Layer Protocol (NSLP) [22]. NSLP allows hosts to signal along a data path for Network Address Translators and firewalls to be configured according to the data flow needs. A separate draft talks about NAT issues for the General Internet Signalling Transport (GIST) protocol [28].

3.4. Peer to Peer Applications

An overview of peer-to-peer application usage across NATs [33] is underway as a draft, as is a general text on application design guidelines for NAT traversal, with a focus on peer to peer [13].

3.5. SIP

An RFC has been published [12] that describes NAT considerations, referring to STUN and UPnP support, and there is also a draft on BCP for NAT traversal and SIP [23] and another draft on the problem statement for SIP-signalled P2P applications with NATs and middleboxes [29].

4. Other NAT-Related Issues

4.1. IPsec

Issues surrounding tunnel mode IPsec and NATs are described in guidelines [4].

4.2. General NAT Behavioural Requirements

The BEHAVE WG has produced a draft on NAT behavioural requirements [15]. The document defines basic terminology for describing different types of NAT behaviour when handling Unicast UDP and also defines a set of requirements that would allow many applications, such as multimedia communications or on-line gaming, to work consistently. A companion document provides similar text for NATs and ICMP [16] and for unicast TCP [17].

4.3. Topologies

There is a draft on problems caused by complex, for example multi-layer, NAT topologies [14], and how these complicate NAT traversal.

4.4. Tunnels

There is a general problem for tunnel methods, for example GRE, where demultiplexing multiple GRE tunnels to many nodes behind a NAT is problematic. This can impact IPv6 (for example 6to4) and Multicast (for example AMT) tunnel handling.

5. Conclusions

The IETF has created a WG (BEHAVE) to look at the issues of NAT traversal; this WG has focused on general documents at a more focused protocol level. This document looks to take a broader view, to highlight the volume of effort ongoing in NAT traversal. There are examples of ongoing drafts resulting from the presence of NATs in at least the SIP, NSIS, HIP, IPv6 and Multicast WGs of the IETF, in addition to WGs involving P2P application usage.

This text is still very much in draft format. We aim to focus on the structure for the -01 release. Any comments to the author welcomed.

6. Security Considerations

There are no specific security considerations in this document.

7. IANA Considerations

There are no IANA considerations for this document.

8. Informative References

[1] Egevang, K. and P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.

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

[3] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[4] Srisuresh, P., "Security Model with Tunnel-mode IPsec for NAT Domains", RFC 2709, October 1999.

[5] Carpenter, B., "Internet Transparency", RFC 2775, February 2000.

[6] Hain, T., "Architectural Implications of NAT", RFC 2993, November 2000.

[7] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[8] Holdrege, M. and P. Srisuresh, "Protocol Complications with the IP Network Address Translator", RFC 3027, January 2001.

[9] Senie, D., "Network Address Translator (NAT)-Friendly Application Design Guidelines", RFC 3235, January 2002.

[10] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[11] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.

[12] Sinnreich, H., Lass, S., and C. Stredicke, "SIP Telephony Device Requirements and Configuration", RFC 4504, May 2006.

[13] Ford, B., "Application Design Guidelines for Traversal through Network Address Translators", draft-ford-behave-app-02 (work in progress), March 2006.

[14] Ford, B. and P. Srisuresh, "Complications from Network Address Translator Deployment Topologies", draft-ford-behave-top-01 (work in progress), March 2006.

[15] Audet, F. and C. Jennings, "NAT Behavioral Requirements for Unicast UDP", draft-ietf-behave-nat-udp-07 (work in progress), June 2006.

[16] Srisuresh, P., "NAT Behavioral Requirements for ICMP protocol", draft-ietf-behave-nat-icmp-00 (work in progress), May 2006.

[17] Guha, S., "NAT Behavioral Requirements for Unicast TCP", draft-ietf-behave-tcp-00 (work in progress), February 2006.

[18] Rosenberg, J., "Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)", draft-ietf-behave-turn-00 (work in progress), March 2006.

[19] Camarillo, G. and O. Novo, "Traversal Using Relay NAT (TURN) Extension for IPv4/IPv6 transition", draft-ietf-behave-turn-ipv6-00 (work in progress), March 2006.

[20] Rosenberg, J., "Simple Traversal of UDP Through Network Address Translators (NAT) (STUN)", draft-ietf-behave-rfc3489bis-03 (work in progress), March 2006.

[21] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", draft-ietf-mmusic-ice-08 (work in progress), March 2006.

[22] Stiemerling, M., "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw-11 (work in progress), April 2006.

[23] Boulton, C., "Best Current Practices for NAT Traversal for SIP", draft-ietf-sipping-nat-scenarios-04 (work in progress), March 2006.

[24] Velde, G., "IPv6 Network Architecture Protection", draft-ietf-v6ops-nap-02 (work in progress), October 2005.

[25] Stiemerling, M., "NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) Communication", draft-irtf-hiprg-nat-03 (work in progress), June 2006.

[26] Jennings, C., "NAT Classification Test Results", draft-jennings-behave-test-results-01 (work in progress),

July 2005.

[27] Cooper, E. and P. Matthews, "Eliminating Duplicate Connectivity Checks in ICE", draft-matthews-mmusic-ice-eliminating-duplicates-00 (work in progress), June 2006.

[28] Pashalidis, A. and H. Tschofenig, "GIST NAT Traversal", draft-pashalidis-nsis-gimps-nattraversal-02 (work in progress), March 2006.

[29] Quittek, J., "Problem Statement for SIP-signalled Peer-to-Peer Communication across Middleboxes", draft-quittek-p2p-sip-middlebox-00 (work in progress), March 2006.

[30] Schmitt, V., "HIP Extensions for the Traversal of Network Address Translators", draft-schmitt-hip-nat-traversal-01 (work in progress), June 2006.

[31] Shore, M., "A STUN-Based Signaling (SBS) Framework", draft-shore-stun-signaling-00 (work in progress), December 2005.

[32] Stiemerling, M., "Simple Middlebox Configuration (SIMCO) Protocol Version 3.0", draft-stiemerling-midcom-simco-08 (work in progress), December 2005.

[33] Srisuresh, P., "State of Peer-to-Peer(P2P) Communication Across Network Address Translators(NATs)", draft-srisuresh-behave-p2p-state-03 (work in progress), June 2006.

Author's Address

Tim Chown
University of Southampton
Southampton, Hampshire SO17 1BJ
United Kingdom

Email: tjc@ecs.soton.ac.uk

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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