NSIS Working Group
Internet-Draft
Expires: January 17, 2005

M. Martin
M. Brunner
M. Stiemerling
NEC
July 19, 2004

SIP NSIS Interactions for NAT/Firewall Traversal
draft-martin-nsis-nslp-natfw-sip-01

Status of this Memo

Copyright Notice

Abstract

The NSIS NAT/FW NSLP provides traversal facilities for other application layer protocols. This document describes the interactions between SIP and NSIS signaling, to enable two NSIS aware SIP end applications to communicate normally through a network of NSIS Aware nodes, in a variety of NAT topologies.

Table of Contents

1. Introduction

The NSIS NAT/FW NSLP allows other application layer protocols to establish tunnels through aribtrarily complex NAT and Firewall network deployments. This means the applications themselves have to know NSIS and its abilities, in order to request such tunnels at the appropiate time, for the appropiate flows.

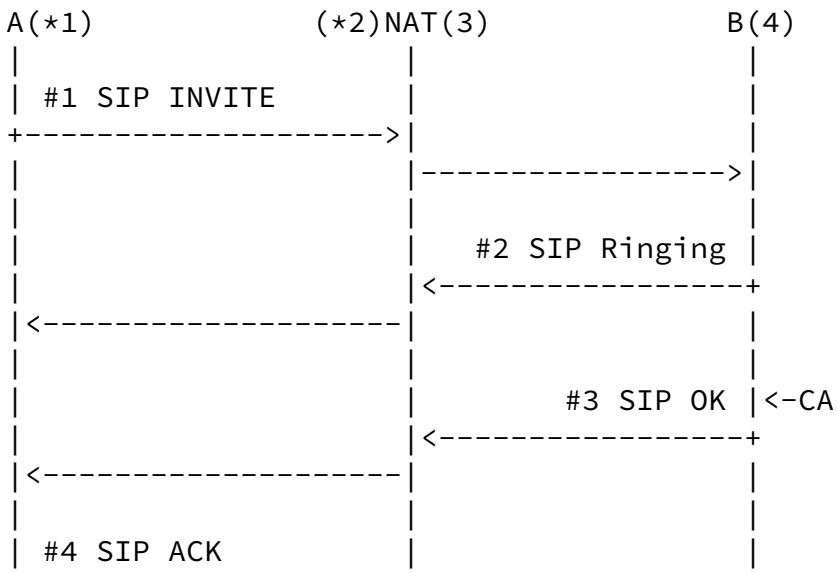
In the case of SIP, several parameters are to be taken into consideration. The nature of the SIP signaling flow results in precise slots where NSIS signaling should take place. This good timing will allow us to minimize the creation of useless pinholes and reduce the waiting times, both before and after the receiver has accepted the SIP call.

This draft discusses the necessary interleaving between the SIP and NSIS Signaling messages, in a combination of network topologies, based on the presence of Middleboxes along the data path.

The draft is meant as a usage recommendation. As such, it starts with a description of the problems, and a case by case solution analysis, ended with a comparison of the obtained results and a final flow recommendation

2. Problem Description

Figure 1 shows a typical network scenario. The Caller, from now on, A, sits behind a NAT, with private IP 1, and has NAT as a gateway, through the private address 2. The NAT has a public interface, with address 3, and B (from now on, the Callee) awaits the call using the public IP 4. Note how addresses prefixed with * (*1, *2) denote private addresses which can not be reached from the internet unless a NAT binding state is installed in the NAT. CA represents the instant in which B accepts the call.



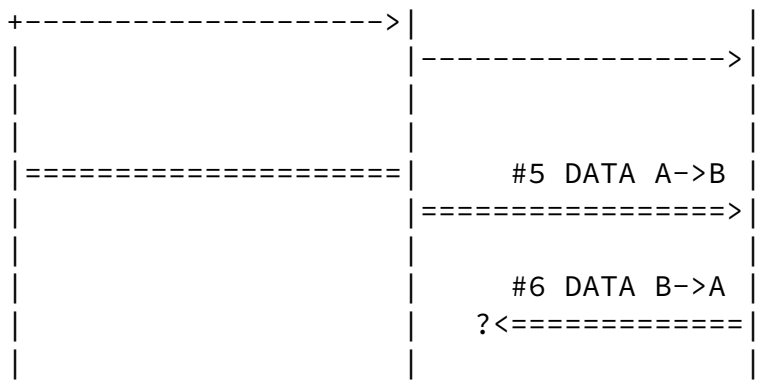


Figure 1: SIP signaling without NSIS

The message flow is described now using the message numbers in the figure. The syntax "(U:V->X:Y): message" denotes a message from address U (or box U), port V, towards address X (or box X), port Y, with the literarily translated meaning "message"

#1 SIP INVITE (A:? -> B:SIP): I await data on *1, port x

This packet contains the information regarding what ports A will expect to receive data on. Notice that the packet is being sent to B, a public IP, with listening information regarding *1, a private IP address. Notice also that A sends a packet from *1 towards 4, but it is intercepted by the NAT, which changes the original address *1 for 3, and remembers the connection to reroute returning packets.

#2 SIP Ringing (B:SIP -> 2:?): Ringing B's phone
The ringing simply inplies that there's something SIP aware on B, and that it's ringing B's phone. Notice that, from B's point of view, the packet came from 2, and not from *1, and so, that's where it will send it's reply. Still, that's the IP layer. The SIP layer will still think that the adta must be sent to *1. When the packet reaches 2, the NAT will remember the binding and change the destination address back to *1. It will then forward the packet back to *1.

#3 SIP OK (B:SIP -> 2:?): Call accepted, I listen on 4:y
This OK means that the user accepted the call. It also informs A on where to send his data: towards 4:y. Note that now 4 is a public address, so both the ip header address (4) and the application layer

address (also 4) are reachable.

4# SIP ACK (A:? -> B:SIP): All is fine, start transmitting. ACK means the ports are accepted and the call can start in the slected data ports on both sides.

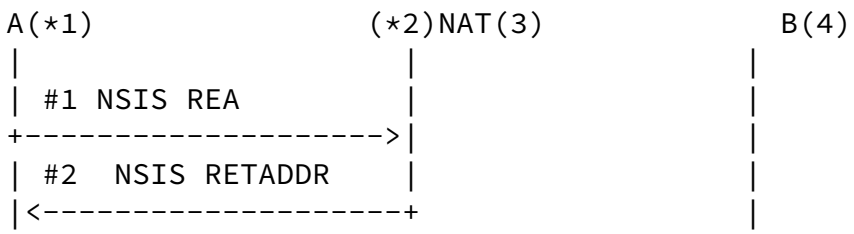
5# DATA (A:? -> B:y) and 6# DATA (B:? -> *1:x): Voice,image, video.. This is the actual data being transmited. It is sent to the addresseses specified in packets numer #1 abd #3, which means B is trying to connect to a private address in #6. Either #6 will not be routable to its destination, or will be sent to the private address, but in B's private network. Either way, #5 succeeds but #6 never arrives.

This simple example shows how the presence of a NAT breaks the data flow and prevents SIP initiated sessions to succeed. Had the NAT been on the receiver's side, we would not have known where to send #1, as we would not know B's public address withouth the mediation of a proxy. Still, even in the case of using a proxy, SIP does not currently cover this situation.

3. NSIS Signaling for the Caller behind a NAT case

This section shows how the NAT/FW traversal NSLP can be used to enable communications in the problem scenario of Section 2.

The following message flow shows the SIP-NSIS Interactions:



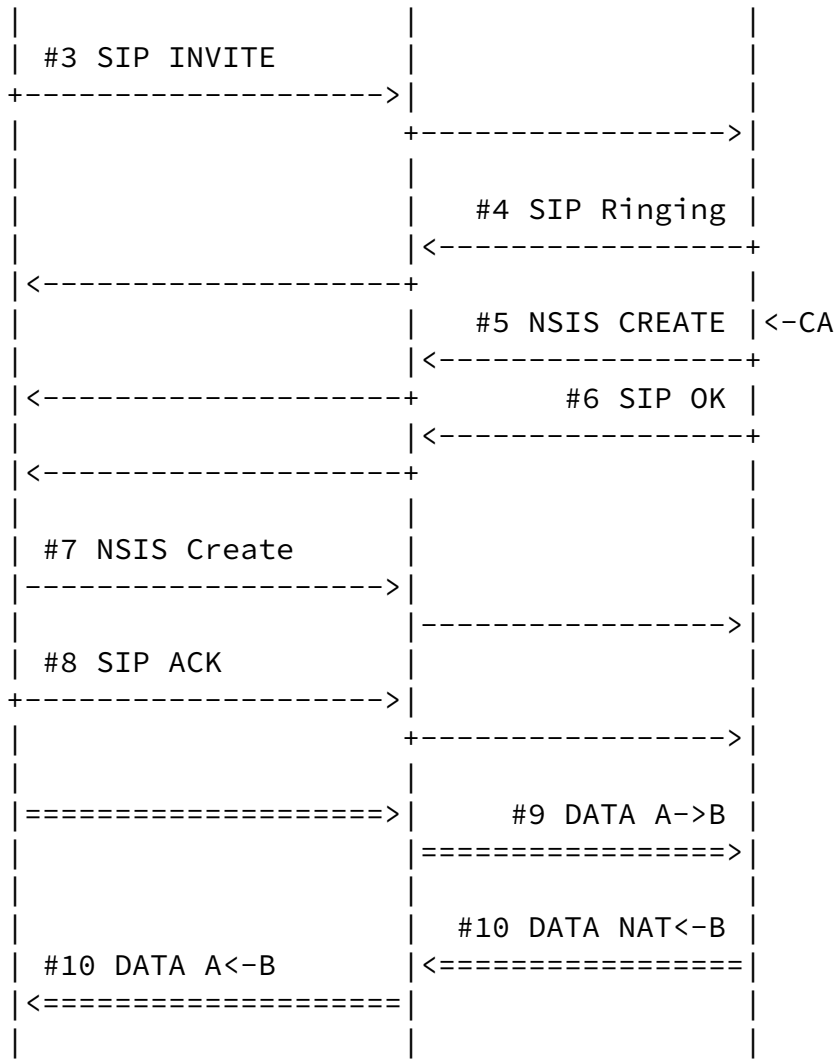


Figure 2: Caller behind a NAT

Because A wants to call B, it first sends a RESERVE-EXTERNAL-ADDRESS (REA) NSIS message. If there is a NAT, as is the case, it will

reply with the allocated public address, using am NSIS RETADDR RESPONSE message. If there was no NAT, A continues its normal operation after a timeout. Normal SIP behavior follows, except that the source address in the SIP INVITE packet has been changed by the one provided by the NSIS RETADDR packet.

When B receives the SIP INVITE message, it assumes there might be

middleboxes in the path, so it tries to open a path by sending an NSIS Create message to the address provided in the SIP INVITE which is were it will eventually send the voice stream.

The NSIS CREATE message reaches the NAT and activates the state that the NSIS RESERVE previously provided, and the message is forwarded inside, in case there where other middleboxes that needed to be open. At this stage, B might or might not want to wait for the NSIS success RESPONSE message, issued by A as a reply to the NSIS CREATE. This message is not shown in the figure.

Once the path has been created, normal SIP behavior follows, and the communication succeeds.

This scheme scales to several middleboxes, since the NSIS REA messages reserve states in all the middleboxes until an edge NAT is encountered.

4. NSIS Signaling for the Callee behind the NAT case

For the callee to be able to receive calls, there has to be a SIP Proxy that forwards the signaling messages from the public internet into the private network. For this reason, it is a safe assumption that A and B will be able to communicate signaling messages independently of the scenario.

With that in mind, the scenario becomes practically symetrical to the one with the caller behind a NAT. The message flow follows. Notice that SIP messages ignore proxies, since they are routed through the proxy, not shown in the diagram.

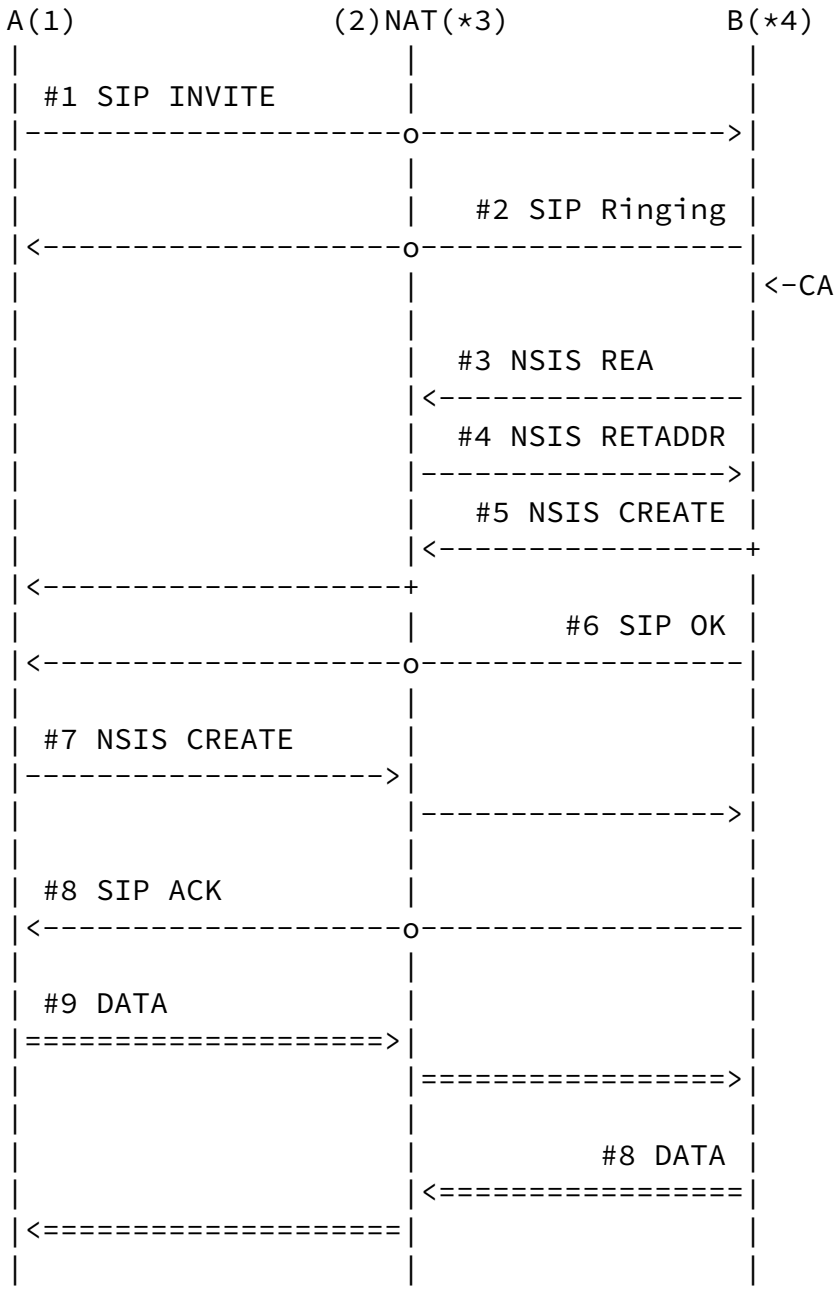
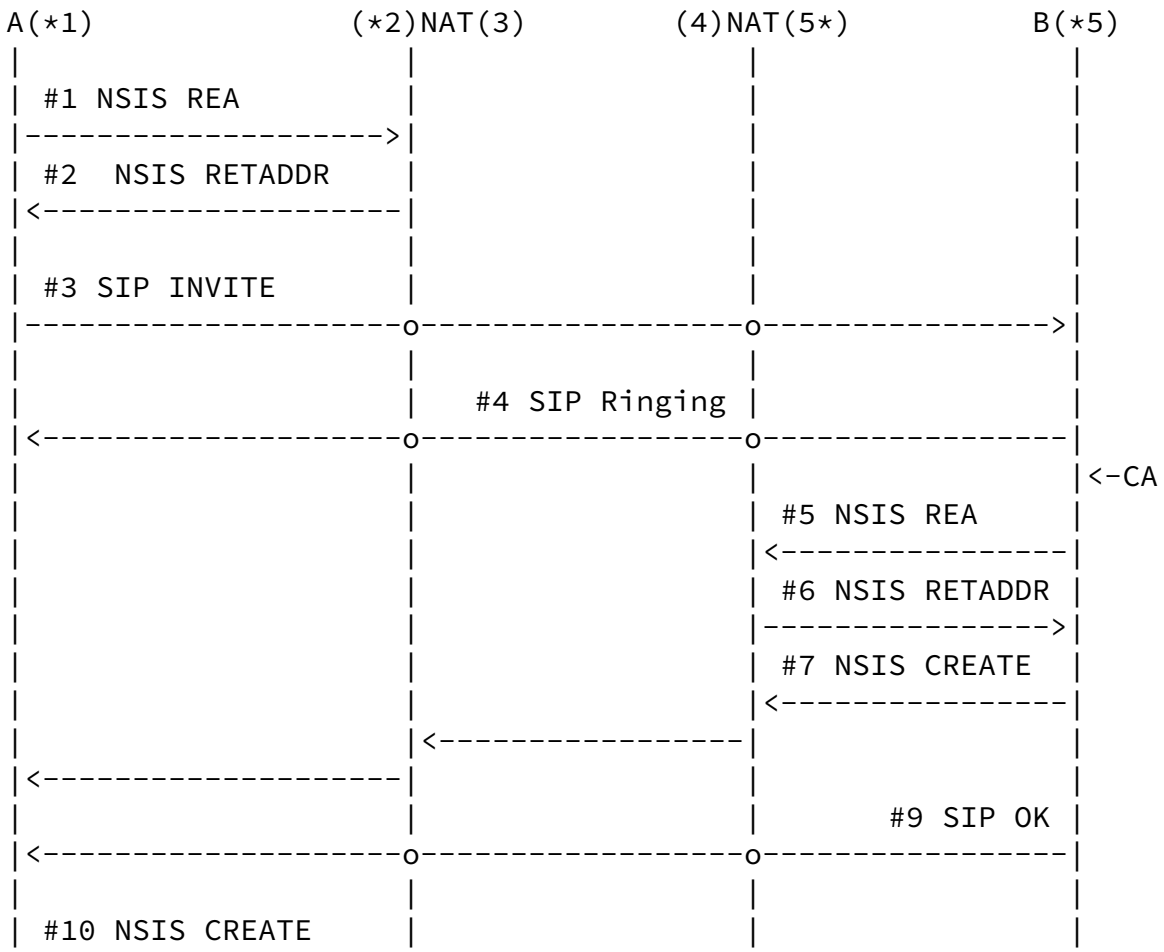
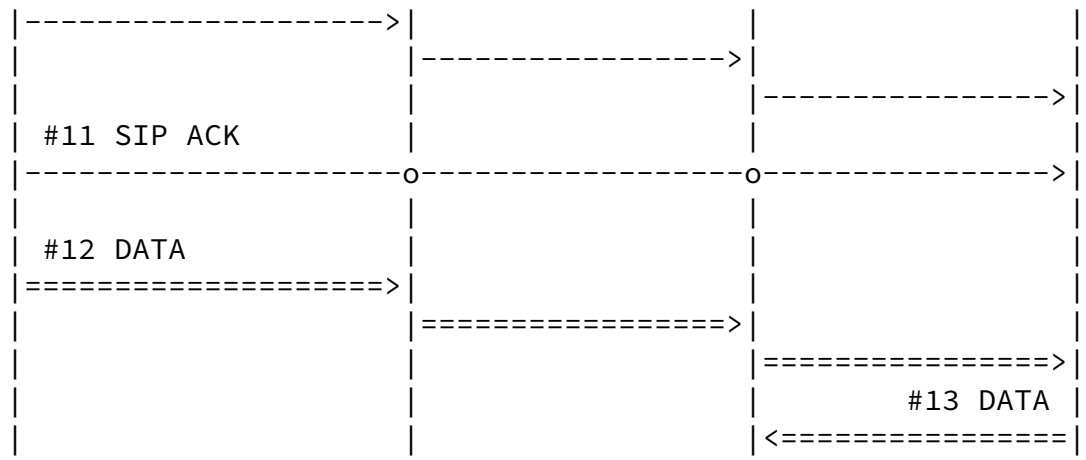


Figure 3: Callee behind a NAT

5. NSIS Signaling for the Caller and the Callee behind a NAT case

Even though this case seems similar, or a simmple summation at least, of the two previous cases, there are some specific issues that need to be looked at carefully. We will start with the message flow, as a prior step to the discussion. Again, notice that the SIP messages reach A and B thanks to the SIP proxy that has to be installed at the edge of the network. This proxy is not shown in the figure.





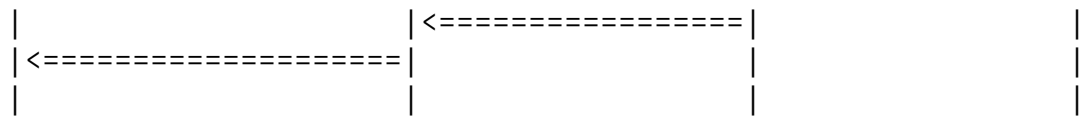
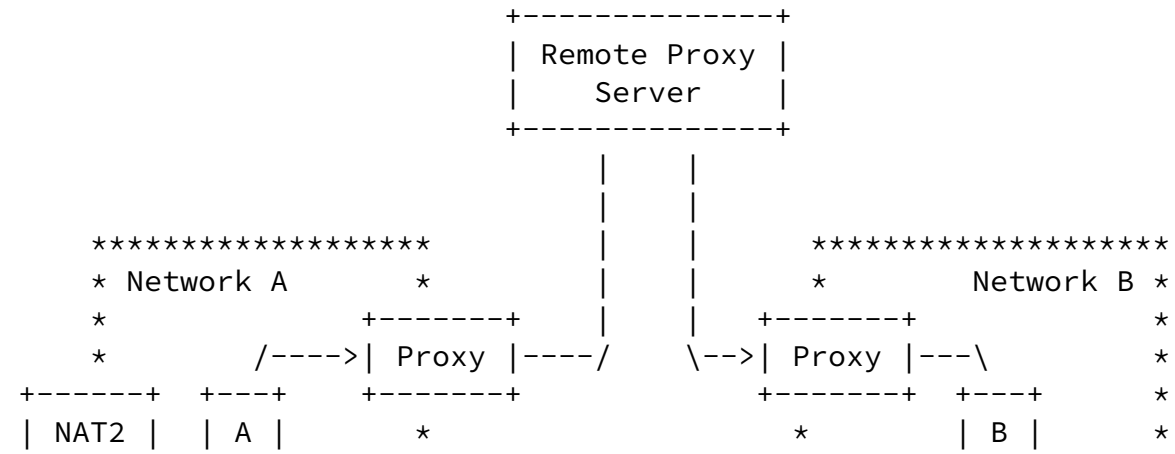


Figure 4: Caller and Callee behind a NAT

Everything works as expected, but there is a hidden pitfall in the above diagram: When A first makes its reservation, it does not know where to send that packet. If the objective is to get out of the NAT, any public IP would do, but that might lead to route optimization problems in certain scenarios

Let's consider the scenario in Figure 5, where A is in a multihomed network that can access the internet through different NATs:



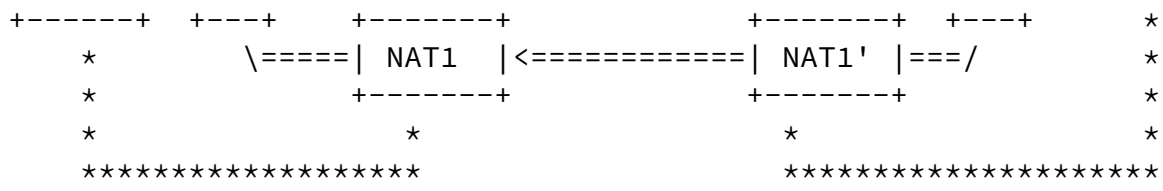
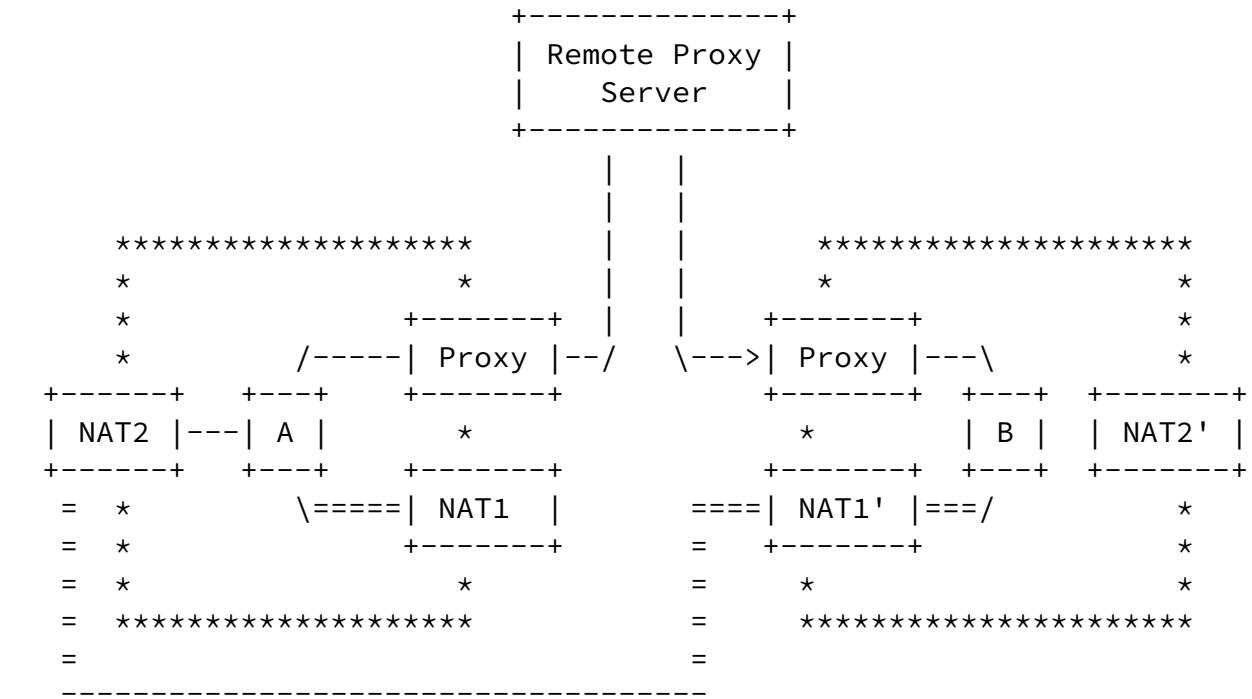


Figure 5: Optimization scenario

The figure shows the route that the SIP packets will follow, through the SIP proxies, and the optimal route for the DATA arriving at A, which is from NAT1' to NAT. This would be the case if the NSIS REA message had originally gone out NAT1, because the public address would be allocated there.

On the other hand, if the NSIS REA mesage went out NAT2, the

communication paths would become:



```
 ---- : SIP Signalization
 ==== : NSIS Signaling and Data transfer
```

Figure 6: Sub optimal route

This comes to show that the "Blind shot" that A performs when first reserving the address has a severe impact on the choosen path in multihomed scenarios, and might lead to longer or less efficient routes.

If we assume that routers are able to calculate the most optimal routes, then the solution is in sending the NSIS REA message on the path to B, but that is unkown at that moment. Still, we do have the SIP Proxy of B. Note that this would be the first Via Header in the SIP OK message, since there is no way we can communicate with B if there is not a SIP Proxy in its network.

Thus, by pointing the NSIS REA message towards B, we have a pretty good assurance that the optimal path (as calculated by the routers) will be chosen.

6. Conclusions

This draft proposes the mechanisms required to use SIP with NSIS, in order to enable the communication through scenarios with obstructing Middleboxes.

Although further analisys is still required to fine tune this interactions, a first valuable result arises: the use of the SIP Proxy as a target for NSIS REA messages is very likely to aid in the coice of the optimal route in the multihomed scenario.

7. Security Considerations

The NAT/Firewall traversal NSLP deals with very security sensitive issues, and a good security infrastructure is required. An evaluation of the possible threads can be found in [1] and a securit proposal is available at [3].

8. References

8.1 Normative References

[1] Tschofenig, H. and D. Kroeselberg, "Security Threats for NSIS", DRAFT draft-ietf-nsis-threats-05.txt, June 2004.

8.2 Informative References

[2] Tschofenig, H., Buechli, M., Van den Bosch, S. and H. Schulzrinne, "NSIS Authentication, Authorization and Accounting Issues", draft-tschofenig-nsis-aaa-issues-01 (work in progress), March 2003.

[3] Martin, M., Brunner, M., Stiemerling, M., Girao, J. and C. Aoun, "A NAT/Firewall NSLP security infrastructure", DRAFT draft-martin-nsis-nslp-natfw-security-01.txt, February 2004.

[4] Stiemerling, M., Tschofenig, H., Martin, M. and C. Aoun, "A NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", DRAFT draft-ietf-nsis-nslp-natfw-03.txt, July 2004.

Authors' Addresses

Miquel Martin
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 905 11 16
EMail: miquel.martin@netlab.nec.de
URI:

Marcus Brunner
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 905 11 29
EMail: brunner@ccrle.nec.de
URI: http://www.brubers.org/marcus

Martin Stiemerling
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 905 11 13
EMail: stiemerling@netlab.nec.de
URI:

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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