Network Working Group
Internet-Draft
Expires: January 10, 2002

S. Vaarala
NetSeal Technologies
July 12, 2001

Mobile IP NAT/NAPT/Firewall Traversal
draft-vaarala-mobileip-nat-traversal-00

Status of this Memo

Copyright Notice

Abstract

Mobile IP and Network Address Translation (NAT) are incompatible. This draft presents a mechanism of establishing a Mobile IP NAT traversal binding in a backwards compatible manner. The NAT traversal is based on using the Mobile IP Home Agent UDP port for encapsulation of data traffic, thus requiring only a single NAT address mapping. The presented method optimizes round trips required to set up the NAT address mapping, which is a critical measure for handover performance.

Table of Contents

1. Introduction

1.1 Overview

Network Address Translation (NAT) [7] is an algorithm for modifying IP packet address and optionally transport protocol fields in order to map private addresses to public addresses. While NAT is inherently incompatible with the Internet Protocol (IP) [1], it is widely deployed in practice, and cannot be ignored in protocol design. In addition to NAT devices there are routers that filter certain kinds of packets in the route between the mobile node and its home agent.

Mobile IP [4] is a protocol that provides IP layer mobility for nodes. While Mobile IP itself is an established protocol, its design does not take NAT devices into account. Thus, Mobile IP will not work when the mobile node resides behind a NAT device (or several NAT devices). Packet filtering routers also pose a problem for Mobile IP connectivity because success in establishing a mobility binding does not ensure that packets can actually be routed between the mobile node and the home agent.

This document presents a simple protocol for UDP-based Mobile IP NAT traversal. The protocol assumes that the network allows communication between an UDP port chosen by the mobile node, and the home agent UDP port 434. The user data is encapsulated in UDP packets that use the same port numbers as the Mobile IP signalling traffic, which has the following advantages. Firstly, only a single NAT mapping is required for both Mobile IP signalling and user data traffic. Secondly, server-to-client data can start flowing as quickly as possible, optimizing handover performance. Thirdly, a successful Mobile IP binding usually indicates that encapsulated packets will flow unfiltered.

The protocol provides a method of NAT detection, and automatic use of NAT traversal if the home agent determines that it is necessary. In addition, the mobile node may request traversal to be used regardless of NAT detection outcome, which is useful if intervening firewalls block some types of traffic but let the Mobile IP traffic pass thru. To keep the NAT mapping constant, empty UDP packets are sent as keepalives in absence of traffic. The keepalive interval is controlled by the home agent, which may be useful since the home agent may have better knowledge of misbehaving NAT devices, and the proper keepalive interval to be used with each such device.

Compatibility with existing Mobile IP implementations is ensured by using the standard Mobile IP vendor extension mechanism to implement the features described.

1.2 Previous work

Similar schemes have been presented previously for both Mobile IP and IPsec. The scheme presented for Mobile IP in [10] assumes a separate UDP port for data encapsulation, which requires extra message exchanges to establish a NAT mapping before server-to-client traffic may begin. Also, firewall traversal may be difficult since the UDP port chosen by the home agent for data encapsulation may be blocked even though the Mobile IP port 434 is not; there is no efficient method of discovering acceptable ports.

The IPsec working group has presented a draft for IPsec NAT traversal [11], which incorporates NAT traversal negotiation into the IKE protocol [12] and reuses the IKE port (UDP port 500) for data encapsulation. A generalization of this approach (reusing a signalling channel for data encapsulation) is used in this document for Mobile IP NAT traversal.

1.3 Terminology

The Mobile IP related terminology described in [4] is used in this document. In addition, the following terms are used:

Traversal Mobility Binding: An extended kind of Mobile IP Mobility Binding, that includes NAT traversal state.

Optimized Traversal: A method of UDP-based NAT traversal where the Mobile IP data port is used for tunnelling of IPv4 packets without extra overhead for any marker octets to distinguish Mobile IP and user data packets.

Non-Optimized Traversal: A method of UDP-based NAT traversal where the Mobile IP data port is used for tunnelling of IPv4 packets. A reserved Mobile IP message type (marker) is used to distinguish data packets from Mobile IP packets.

Data Encapsulation Marker: Mobile IP message type value(s) that are used to distinguish user data packets from Mobile IP packets.

1.4 Specification language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [6].

2. Protocol description

2.1 Overview

The protocol described in this document has functionality (1) to negotiate NAT traversal support in a backwards compatible manner, (2) to detect the presence of NAT device(s), (3) to determine whether NAT traversal should be used or not, and if so, to assign a NAT keepalive interval, and (4) to tunnel data packets. The protocol assumes that the mobile node is registering using a co-located care-of address.

All functionality except data packet tunnelling are performed within the standard Registration Request (RREQ) and Registration Reply (RREP) message exchange. The RREQ message contains a Mobile Node Traversal Extension, which is a Normal Vendor-Specific Extension (NVSE) [9], which indicates that the mobile node supports this protocol. The extension also contains a flag, which indicates that the mobile node requests unconditional tunnelling of data packets, regardless of the outcome of NAT detection performed by the home agent. The extension also contains the data encapsulation marker used by the mobile node.

The home agent detects the presence of NAT device(s) by comparing the source IP address of the RREQ message, and the co-located care-of address contained within the message. A discrepancy indicates that an address translation has been performed. Traversal MUST be enabled if NAT is detected, or if the mobile node has requested unconditional tunnelling. However, the home agent MAY also enable traversal unilaterally. Should traversal be used, a Home Agent Traversal Extension, which is a Critical Vendor-Specific Extension (CVSE) [9], is inserted into the RREP message. The presence of the extension indicates that this protocol is supported by the home agent, and that NAT traversal has been enabled in the mobility binding shared by the mobile node and the home agent. The extension also includes the server data encapsulation marker, and the NAT keepalive interval that the mobile node should use.

If NAT traversal is not used, or if the home agent does not support this protocol, the RREP message will not include the Home Agent Traversal Extension.

Once NAT traversal has been enabled for a given Mobile IP binding, both the home agent and the mobile node encapsulate IPv4 packets inside UDP payloads, using the same ports as in the RREQ/RREP messages. Ordinary Mobile IP packets are differentiated from tunnelled IPv4 packets by means of the Mobile IP message type field. The data encapsulation markers exchanged in the RREQ/RREP message

vendor extensions determine which message type octets serve as data

encapsulation markers for each direction of traffic. Two types of encapsulation behavior are supported: optimized, with eight octet overhead, and non-optimized, with nine octet overhead. Empty UDP packets are used as NAT keepalive messages, should there be no user data or Mobile IP traffic within the NAT keepalive interval. Once the registration lifetime expires, the NAT traversal MUST be stopped. The traversal state is a part of the mobility binding, so a new RREQ/RREP message exchange is required to re-establish NAT traversal.

Since the same UDP port is used for both Mobile IP traffic and encapsulated data traffic, the only requirements for firewalls and NAT devices is to pass traffic between the home agent UDP port 434 and the UDP port chosen by the mobile node. Also, if the RREQ/RREP message exchange succeeds, the data traffic encapsulation will almost certainly pass the routers between the mobile node and the home agent.

2.2 Message exchanges

The notation "src-addr:src-udp-port -> dst-addr:dst-udp-port" is used in the following diagrams to indicate addressing fields of packets. COA is the possibly private co-located care-of address of the mobile node. HA is the home agent address, which is assumed to be a public address. X is the UDP source port used by the mobile node for Mobile IP (or data encapsulation) messages destined to the home agent. This port is assumed static for the duration of a given RREQ/RREP exchange, and the (possible) data encapsulation and keepalive traffic that follows. NAT-COA is the translated COA address, while NAT-X is the possibly translated UDP port X (NAT and NAPT are handled identically in the protocol, so the worst case, ie NAPT, is assumed).

2.2.1 Message exchange with NAT devices present

This exchange of messages takes place when both mobile node and home agent are compliant, and one or more NAT/NAPT devices exist in the route between mobile node and home agent.

```
     mobile node    NAT/NAPT device(s)    home agent
     ===========    ==================    ==========

           ----------------> COA:X -> HA:434
             Registration Request
               + co-located address COA
               + Mobile Node Traversal Extension
                 (U-flag, mobile node encapsulation marker)

                                --------------> NAT-COA:NAT-X -> HA:434
                                  Registration Request

                     Discrepancy:  IP header source address is NAT-COA,
                     while RREQ care-of address field is COA.

                     HA->MN traffic can start flowing.

                                <-------------- HA:434 -> NAT-COA:NAT-X
                                  Registration Reply
                                    + Home Agent Traversal Extension
                                      (home agent encapsulation marker,
                                       NAT keepalive interval)

           <---------------- HA:434 -> COA:X

                     Registration completed, MN->HA traffic can also
                     start flowing.

           [data traffic]

           [NAT keepalive interval passed without traffic, send keepalive]
           ----------------> COA:X -> HA:434
             keepalive (empty UDP)
                                --------------> NAT-COA:NAT-X -> HA:434
```

2.2.2 Message exchange without NAT devices present

This exchange of messages takes place when both mobile node and home agent are compliant, but no NAT/NAPT devices seem to be present.

```
mobile node                          home agent
===========                          ==========

      ----------------------------------> COA:X -> HA:434
        Registration Request
          + co-located address COA
          + Mobile Node Traversal Extension
            (U-flag, mobile node encapsulation marker)

                No discrepancy between the IP header source address
                field and the RREQ care-of address field.

                If the U-flag (unconditional tunnelling requested)
                is set, or if the home agent determines that UDP
                data encapsulation should be performed, the scenario
                reverts to the one described above.

                HA->MN traffic can start flowing.

      <---------------------------------- HA:434 -> COA:X
                          Registration Reply

      [no keepalive traffic, behave as required by RFC 2002.]
```

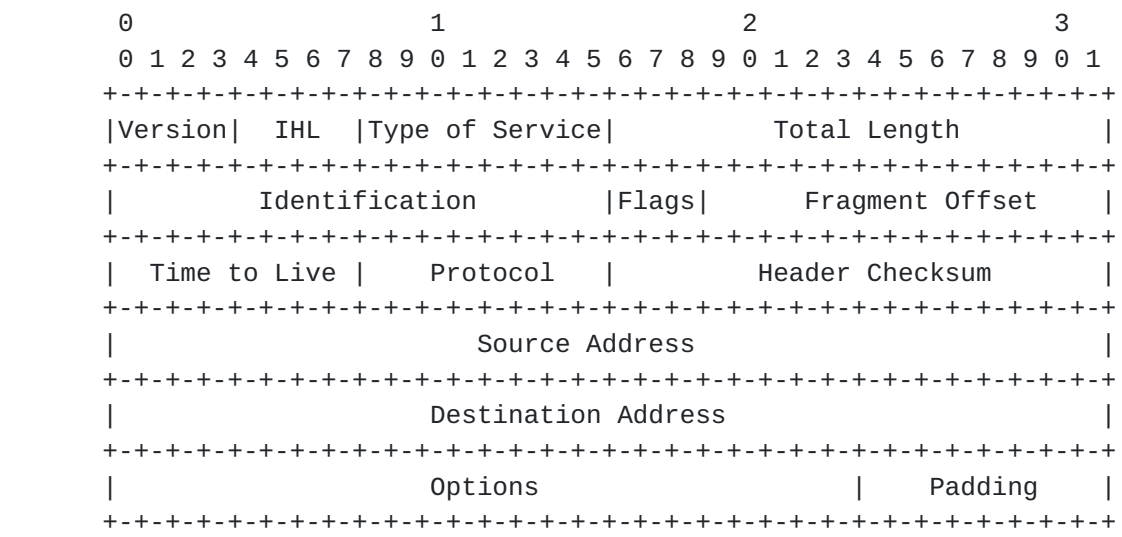
2.2.3 Message exchange with a non-compliant home agent

If the home agent does not support this protocol, it will ignore the NVSE sent by the mobile node. If NAT/NAPT devices are present, the d screpancy in the Mobile IP headers should cause the HA to discard or reject the registration.

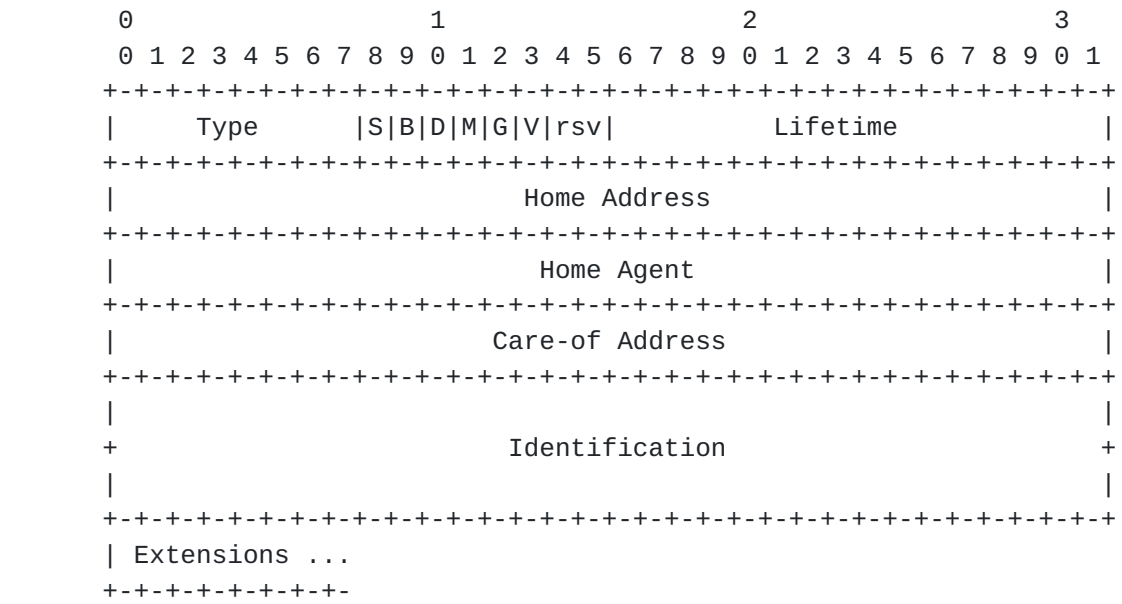
2.3 Packet formats

2.3.1 Data packet encapsulation

Since the same UDP ports are used to send both Mobile IP packets and encapsulated data packets, there must be a method of identifying which kind of packet was received by a mobile node or by a home agent. This protocol uses the first octet of the UDP payload data to make this determination. The IPv4 header has the following format [1]:



The Mobile IP messages have a one octet message type identifier, with rest of the message being message type specific. For instance, Registration Request has the following format [4]:



The first octet of an IPv4 header contains both an IP version field (always 4 for IPv4) and the Internet Header Length field, which is always in the range 5...15. Thus the first octet of IPv4 header is always in the range 0x45...0x4f.

This fact is used by the optimized traversal mode to differentiate packet types. If the first octet of the UDP payload is in the range 0x45...0x4f, the UDP payload (including the first octet) is assumed to be an encapsulated IPv4 packet. Otherwise the payload is assumed to be a Mobile IP message. The optimized traversal mode does not add

extra overhead (in addition to the UDP header), but requires that

the receiver has reserved the Mobile IP message types 0x45...0x4f for data encapsulation markers.

In non-optimized traversal a single message type is used as a data encapsulation marker. The marker message type can be chosen dynamically, and is sent as part of both Mobile Node Traversal Extension and Home Agent Traversal Extension. If the first octet of the UDP payload equals the marker chosen by the receiving host, the UDP payload excluding the first octet is assumed to be an encapsulated IPv4 packet. Otherwise the payload is assumed to be a Mobile IP message. Non-optimized traversal mode adds one octet overhead (in addition to the UDP header), but only requires that a single Mobile IP message type be reserved to serve as a marker. Since the marker is not pre-defined by this protocol, any Mobile IP message type can serve as one; thus there is no possibility of conflict with future Mobile IP message types, as long as there is at least one unused message type to serve as a marker.

Both modes of traversal MUST be supported. The receiving host chooses which type of traversal it expects in packets sent to it, and if non-optimized traversal is used, which marker octet is used. To emphasize, the marker may be different in each direction.

2.3.2 Keepalive message

A keepalive message is an empty UDP packet sent using the same port information as Mobile IP and encapsulated data packets. This packet is differentiated from Mobile IP and encapsulated data packets using the UDP length field (which MUST be eight) [2].

2.3.3 Registration Request

When using this protocol, the Registration Request message consists of an IPv4 header, followed by an UDP header, followed by the fixed Mobile IP Registration Request header [4], followed by extensions, including the Mobile Node Traversal Extension, followed by the Mobile-Home Authentication Extension ([4], Section 3.5.2), which MUST NOT be followed by any extensions.

The UDP source port of the Registration Request may be chosen freely by the mobile node. However, the source port MUST stay constant for the duration of the binding being requested, and for the data/keepalive traffic that follows. This ensures that the NAT mapping stays valid. The mobile node SHOULD use the same source port for all interactions with the home agent.

The Registration Request message fields operate normally, with the following exceptions. The 'D' (decapsulation by mobile node) bit MUST be set, because only co-located care-of address mode is

supported. The 'M' (minimal encapsulation) bit MUST NOT be set, since it conflicts with NAT. The 'G' (generic routing encapsulation, or GRE [8]) bit operates normally, as do the other flag bits. The Care-of Address field is set to the possibly private co-located care-of address.

When simultaneous bindings are used, the usage of traversal applies to each binding individually, ie each binding has a different keepalive interval and potentially different encapsulation markers.

2.3.4 Registration Reply

The Registration Reply message consists of an IPv4 header, followed by an UDP header, followed by the fixed Mobile IP Registration Reply header [4], followed by extensions, possibly including the Home Agent Traversal Extension, followed by the Mobile-Home Authentication Extension, which MUST NOT be followed by any extensions.

The Registration Reply message fields are set normally.

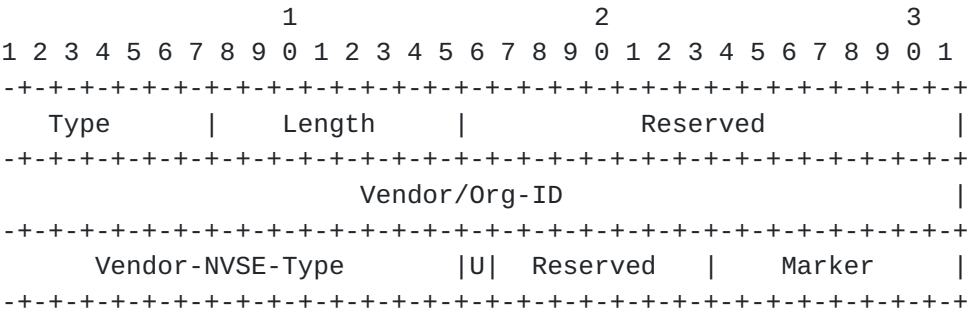
Because there is nothing to guarantee that the NAT mapping is not lost -- data and keepalive packets may be lost, or the NAT device may be rebooted -- the home agent implementation MUST take the special case of a lost NAT mapping into consideration. To avoid a long traffic blackout in such situations the home agent SHOULD set the lifetime of the binding to a conservative value, such as one minute. This ensures that if the NAT mapping is lost, a new one is formed by a new RREQ/RREP exchange in a reasonable time.

The NAT traversal state is conceptually added into the Mobile IP binding state, and thus, it MUST be re-negotiated for every RREQ/RREP message pair exchange.

2.3.5 New extensions

The Normal Vendor-Specific Extensions (NVSE) and Critical Vendor-Specific Extensions (CVSE) used in this document conform to [9]. Unauthenticated extensions MUST NOT be processed.

2.3.5.1 Mobile node traversal extension



The Mobile Node Traversal Extension is a NVSE (Normal Vendor-Specific Extension), which indicates support for this protocol. It is ignored by the receiver if the extension is not supported.

The fields are set as follows:

Type: NVSE-TYPE-NUMBER 134 [9].

Length: 10.

Vendor/Org-Id: 9213, hex 0x23fd, registered to NetSeal Technologies.

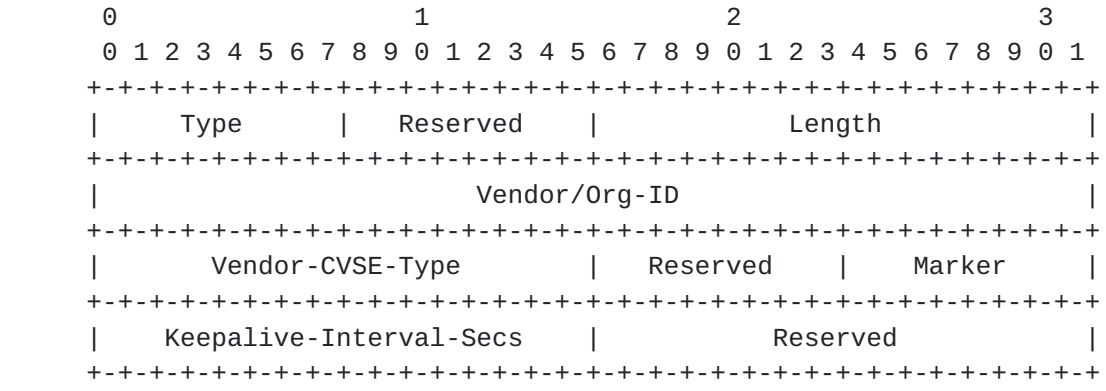
Vendor-NVSE-Type: 16385 (0x4001)

U-flag: Indicates that the mobile node wants to use traversal regardless of the outcome of NAT detection performed by the home agent. This is useful if the route between the mobile node and the home agent works for Mobile IP signalling packets, but not for generic data packets (eg because of firewall filtering rules). If the home agent supports this protocol, it MUST either accept the traversal and reply with a Home Agent Traversal Extension or reject the traversal. The suggested value for the Registration Reply Code field in case of failed registration is 129 ("administratively prohibited").

Marker: If zero, indicates that the mobile node uses optimized traversal. If non-zero, indicates that the mobile node uses non-optimized traversal, and the value of the field is the marker octet to be placed in the UDP payload prior to the actual encapsulated IPv4 packet. The home agent MUST use the encapsulation method and marker octet indicated by the mobile node in encapsulated packets sent to the mobile node.

All reserved fields MUST be set to zero. If a reserved field is non-zero when the extension is received, the whole extension MUST be ignored.

2.3.5.2 Home agent traversal extension



The Home Agent Traversal Extension is a CVSE, which indicates that (1) the home agent supports this protocol, and (2) that the traversal has been enabled for the mobility binding established using the RREQ/RREP exchange.

The fields are set as follows:

Type: CVSE-TYPE-NUMBER 38 [9].

Length: 12.

Vendor/Org-Id: 9213, hex 0x23fd, registered to NetSeal Technologies.

Vendor-CVSE-Type: 16386 (0x4002)

Marker: If zero, indicates that the home agent uses optimized traversal. If non-zero, indicates that the home agent uses non-optimized traversal, and the value of the field is the marker octet to be placed in the UDP payload prior to the actual encapsulated IPv4 packet. The mobile node MUST use the encapsulation method and marker octet indicated by the home agent in encapsulated packets sent to the home agent.

Keepalive-Interval-Secs: Specifies the NAT keepalive interval that the mobile node SHOULD use. A keepalive packet SHOULD be sent if Keepalive-Interval-Secs seconds have elapsed without any signalling or data traffic being sent.

The keepalive interval may depend on specific NAT devices. It may be the case that the home agent is aware of parts of the network, and can "recommend" proper keepalive traffic intervals for mobile nodes. For example, the server wants keepalive traffic to be sent with an interval of 60 seconds by default, but certain problem devices require shorter keepalive packet intervals. These "problem devices" can be configured to the home agent one by one, while other devices

are handled using the default value. Note that the mobile node is incapable of making an informed decision since it does not see the external address that the NAT device assigns to it.

All reserved fields MUST be set to zero. If a reserved field is non-zero when the extension is received, the mobile node MUST assume that the registration failed.

2.4 Version considerations

There are no version negotiation fields in this protocol. If functionality is changed radically new vendor extension IDs are allocated to the new traversal protocol. The mobile node may indicate support for several versions of this protocol by appending several NVSE extensions in the Registration Request message.

If the home agent detects a flag in the currently reserved area of the Mobile Node Traversal Extension that it does not support, it MUST reject the registration. Suggested Code is 134 (poorly formed Request). If the mobile node detects a flag in the currently reserved area, it MUST act as if the registration had failed, and that the binding was not completed.

3. Analysis

3.1 Overhead

This draft does not add significant latency to the ordinary Mobile IP Registration Request / Registration Reply message exchange. In particular, the NAT address mapping is formed when the mobile node sends its first Registration Request message, and is already valid when the home agent receives the packet. Thus, the home agent may start forwarding traffic to the client immediately after receiving the Registration Request (assuming, of course, that the binding is accepted).

In other words, the latency for server-to-client traffic flow is 0.5 roundtrips, and for client-to-server traffic, one roundtrip. The extra data in the form of vendor extensions does add some transmission latency, and may be noticeable especially using slow media.

If optimized data encapsulation is used, there is an eight octet overhead (compared to IP-IP tunnelling) per data packet caused by the UDP header required for traversal. For non-optimized data encapsulation, the corresponding overhead is nine octets per data packet.

3.2 Network requirements

The protocol described in this document works in networks where there are ordinary routers, NAT/NAPT routers, and firewalls that are configured to pass Mobile IP packets (variable mobile node port and fixed home agent port 434). There are no other requirements with regards to UDP ports, and since there are no extra UDP ports for data encapsulation, there is no need to use heuristics to determine which UDP port might actually work for data encapsulation: if the Registration Request is received, both the Registration Reply and encapsulated data is typically received properly.

Since the Mobile IP home agent port is used for data encapsulation, there MUST NOT be foreign agents in the route (which might be confused by such packets). In particular, only the co-located care-of address mode of Mobile IP is supported. (In fact, a DHCP server that also performs NAT is a viable replacement for a FA.)

4. Security considerations

The Traversal Extensions used by this protocol are authenticated by the Mobile IP Mobile-Home Authentication Extension. The presence of the extensions do not seem to cause vulnerabilities, since the information contained in them is not confidential. Support of this protocol may be considered as useful information for an attacker, though.

A strong attacker is free to modify the IP packets sent, and thus eg cause the home agent to mistakenly believe there are NAT device(s) in the route between mobile node and the home agent. However, such modifications require read-write access to the packet flow, which already enable other more powerful attacks to be performed.

5. Intellectual property rights

NetSeal Technologies has no patent applications related to the protocol described in this document.

6. Acknowledgements

Levkowetz et al. have proposed a similar scheme in [10], the difference being a dedicated UDP tunnelling port. Kivinen, Stenberg, Huttunen et al. have proposed a NAT traversal protocol for IPsec [11], which uses the same approach taken here, in particular reusing the NAT address mapping of the signalling channel (in their draft, IKE) for data encapsulation.

The author would like to thank the staff at NetSeal Technologies for useful feedback.

References

[1] Defense Advanced Research Projects Agency (DARPA), Information Processing Techniques Office and , "Internet Protocol", STD 5, RFC 791, September 1981.

[2] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

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

[4] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[5] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[7] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[8] Farinacci, D., Li, T., Hanks, S., Meyer, D. and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[9] Dommety, G. and K. Leung, "Mobile IP Vendor/Organization-Specific Extensions", RFC 3115, April 2001.

[10] Levkowetz, O. H., Forslow, J. and H. Sjostrand, "NAT Traversal for Mobile IP using UDP Tunnelling (Work in Progress)", July 2001.

[11] Huttunen, A., Dixon, W., Swander, B., Kivinen, T., Stenberg, M., Volpe, V. and L. DiBurro, "UDP Encapsulation of IPsec Packets (Work in Progress)", June 2001.

[12] Kivinen, T., Stenberg, M., Huttunen, A., Dixon, W., Swander, B., Volpe, V. and L. DiBurro, "Negotiation of NAT-Traversal in the IKE (Work in Progress)", June 2001.

Author's Address

Sami Vaarala
NetSeal Technologies
P.O Box 38
Niittykatu 6
02201 Espoo

Phone: +358-9-435 310
Fax: +358-9-435 311 00
EMail: sami.vaarala@netseal.com
URI: http://www.netseal.com/

Full Copyright Statement

Acknowledgement

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