Internet-Draft
Expires: January 1, 2002

O. H. Levkowetz
J. Forslow
H. Sjostrand
ipUnplugged
July 3, 2001

NAT Traversal for Mobile IP using UDP Tunnelling
<draft-levkowetz-mobileip-nat-tunnel-00.txt>

Status of this Memo

Copyright Notice

Abstract

Mobile IP is now being deployed, providing connectivity to mobile users. This is happening well ahead of the widespread use of IPv6, which may not have been expected at the time when the Mobile IP standard was originally formulated. At the same time, networks with private address spaces are proliferating, using NAT devices to reach the public internet. Today NATs are widely deployed in home gateways, as well as in other locations likely to be used by mobile users, such as hotels. The result is that MIP-NAT incompatibility issues have become a major barrier to deployment of Mobile IP in one of its principal uses. This draft describes a known incompatibility between NAT and Mobile IP, and also describes a possible solution using Mobile IP's vendor specific extensions.

Table of Contents

1. Introduction

Mobile IP is expected to become of great benefit as a technology for remote access to mobile-VPNs by allowing the traversal of one or more exterior domains. However, it is likely that the traffic and mobile IP signalling in a remote mobile-VPN access scenario will have to traverse a network address port translation (NAPT) [RFC 2663] at one or more inter-domain borders. The current mobile IP RFC 2002 cannot survive such a NAPT traversal.

The NAPT traversal scenario is expected to be particularly common in the broadband access deployment scenario to residential homes, as many broadband access providers only allocate a private IP address to each house/apartment. Furthermore, it is unlikely that the NAPT in the broadband access operator's network can be controlled by the customer/corporate IT-manager in any way. This may be acerbated by the existence of small private NAPT devices inside residential broadband access routers, supporting multiple IP nodes in a private residential address space.

The following paper describes a possible solution to solve NAPT traversal for mobile IP. The solution makes this possible by way of using the co-located care-of option in a mobile node, enhancements inside the home agent and an extra UDP header in what would otherwise be regular IP-in-IP tunnelled payload data.

1.1 Terminology

Forward Tunnel
: A tunnel that shuttles packets towards the mobile node. It starts at the home agent, and ends at the mobile node's care-of address.

Reverse Tunnel
: A tunnel that starts at the mobile node's care-of address and terminates at the home agent.

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[8].

1.2 Problem description

The major incompatibility between MIP and NATs occurs when the Mobile Node (MN) acquires a co-located care-of address which is a private address. RFC 2002[6], in describing the use of co-located care-of addresses, states that

> "The mode of using a co-located care-of address has the advantage that it allows a mobile node to function without a foreign agent, for example, in networks that have not yet deployed a foreign agent. It does, however, place additional

burden on the IPv4 address space because it requires a pool of addresses within the foreign network to be made available to visiting mobile nodes. It is difficult to efficiently maintain pools of addresses for each subnet that may permit mobile nodes to visit."

However, in most cases involving networks using private addresses and NATs, this option will not be available, and for some time to come many visited networks will not have a foreign agent present. We then get the following situation:

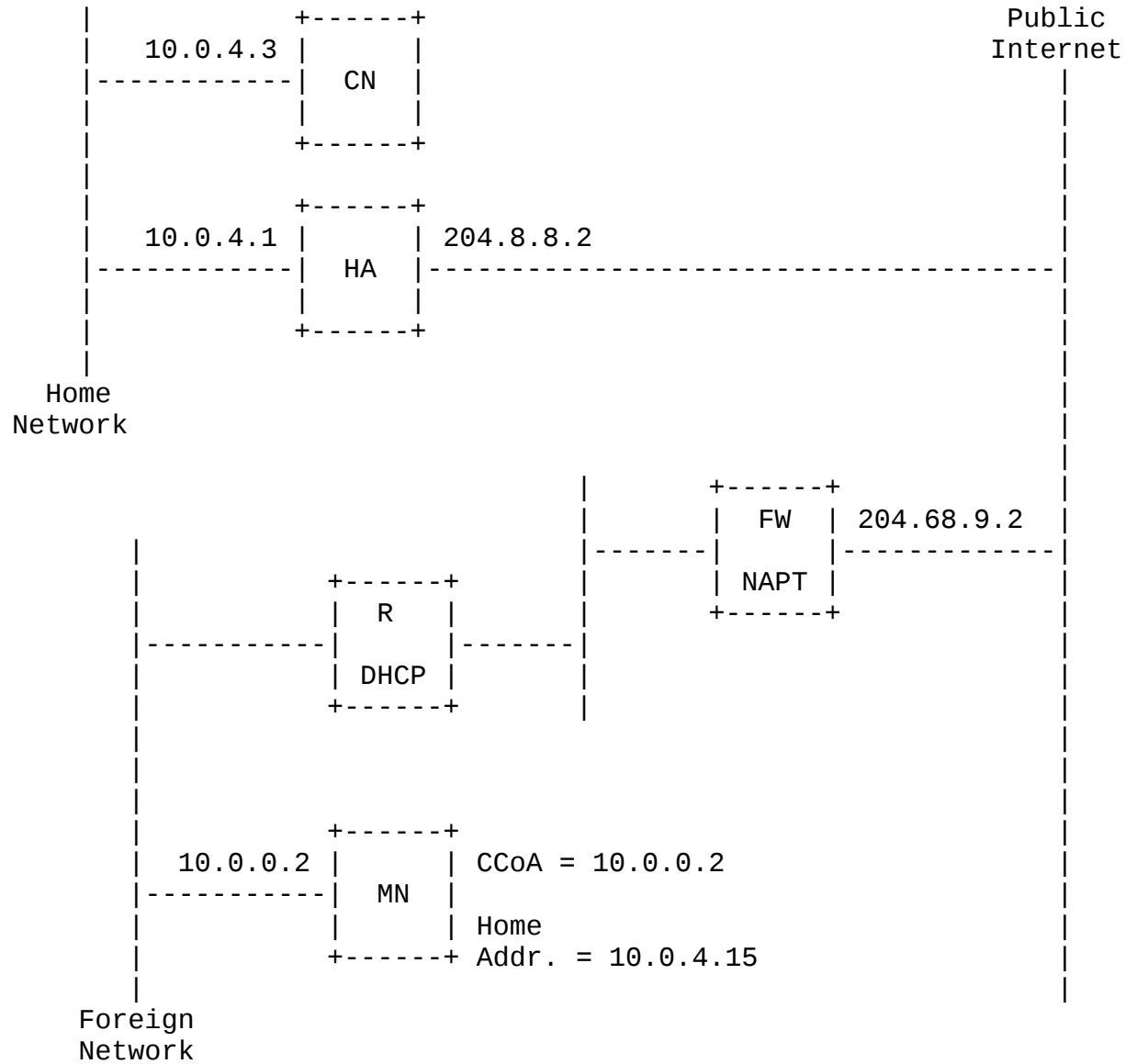


Figure 1

Fig. 1 shows a scenario where the mobile node MN is hidden behind a network address port translation (NAPT) in the foreign network. The

home agent is considered having a public (unique) IP address towards the Internet. A residential broadband access network is shown as the foreign network and is allocating a private IP address to each house/apartment. The mobile users connect to the home agent HA at the office or the internet service provider (seen as the home network).

The mobile node will request a temporary care-of address from the local router R and its DHCP server in the visited network. In fig. 1, the care-of address is set to 10.0.0.2 -- an address that is allocated from within the address realm in the visited network. In addition, the mobile node has a stable address set to 10.0.4.15 -- an address that is allocated from within the address realm of the home network. The details of the registration request procedure will be explained below; however, for now it is enough to know that the registration will survive the traversal of the firewall and its NAPT when the firewall changes the source IP address to its own public address, i.e. 204.68.9.2, and allocates a new UDP source port.

1.3 One possible solution

The home agent will discover that a NAPT traversal has occurred by comparing the source IP address 204.68.9.2 and the care-of address 10.0.0.2. The mobile IP tunnel is then modified to contain a UDP header as well, in order to facilitate traversal of the NAPT with payload datagrams between the mobile node and the correspondent node CN (10.0.4.3). Note also that the source IP header of the registration request as received by the home agent, i.e. 204.68.9.2, will be used as destination IP address for the outer IP header in the mobile IP tunnel as seen from the home agent, instead of the care-of address, i.e. 10.0.0.2, that is normally applied.

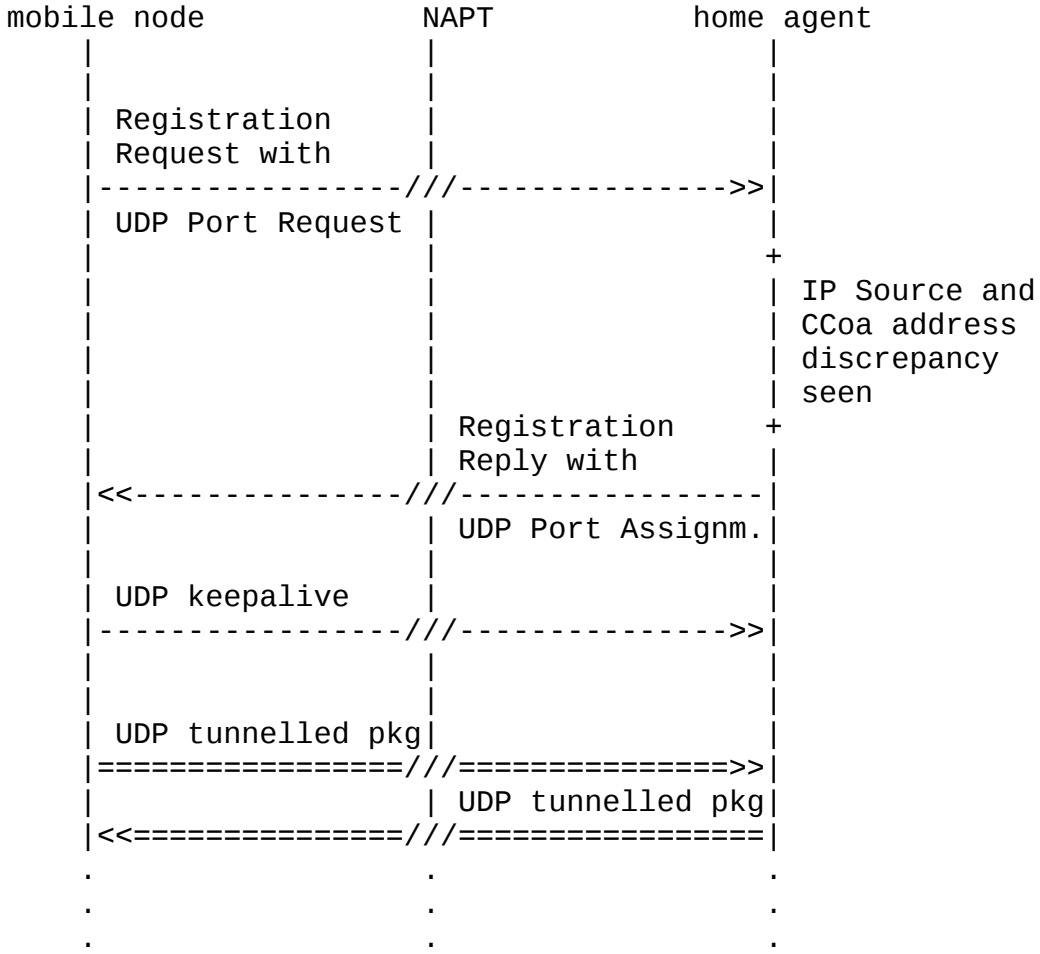
There are two differences in the way payload transfer would be performed when a NAPT is present in the path. First of all the payload datagrams to be sent through the mobile IP tunnel would be encapsulated with an outer IP and UDP header, instead of only an IP header. This will ensure that the datagrams will pass through the NAPT and allow the NAPT to use the UDP source port to create a unique id for the payload session in order to be able to map back to the correct IP address and source UDP port on the inside of the firewall when traffic is coming back from the home agent. The second difference is that the home agent is applying the source IP header of the registration request, i.e. the IP address of the NAPT 204.68.9.2, as the destination IP address also for datagrams destined for the mobile node 3. This is in contrast with the current IETF standard RFC 2002[6], where the home agent is using the care-of address as the destination IP address.

2. ipUnplugged UDP Tunnelling

This section describes a vendor-specific implementation of the solution described above. Briefly, the mobile node may use a vendor specific extension in its Registration Request to indicate that it would like to use IP in UDP Tunnelling instead of standard IP in IP Tunnelling[7] if the home agent sees that the Registration Request seems to have passed trough a NAPT. The home agent may then do a UDP port assignment and send a registration reply with a vendor extension indicating which port to use. IP in UDP Tunnelling will then be used in both directions.

2.1 Basic Message Sequence

The message sequence diagram below exemplifies setting up and using a Mobile IP UDP tunnel as described in this document. The tunnel is set up by inclusion of specific extensions in the initial Mobile IP registration request and reply exchange. Thereafter, any traffic between the mobile node and the home agent are sent trough the UDP tunnel.



2.2 Tunnel Keepalive

As the existence of the bi-directional UDP tunnel through the NAPT is dependent on the NAPT keeping state information associated with a session, as described in RFC 2663[10], and as the NAPT may decide that the session has terminated after a certain time, keepalive messages may be needed to keep the tunnel open. The keepalives should be sent more often than the timeout value used by the NAPT. This timeout should be 4 minutes, according to RFC 2663[10] and as explained in RFC 793[3], but it is conceivable that shorter timeouts may exist in some NAPTs.

The keepalive messages SHALL consist simply of a UDP message with zero length payload, and otherwise conforming to Section 3, and SHALL be sent by the mobile node at least as often as every 4 minutes. The frequency of keepalive messages MAY be configurable within this limitation.

The first keepalive message SHALL be sent by the mobile node immediately after the receipt of the Registration Reply with an UDP Port Assignment Extension (Section 2.4.4), in order to open the NAPT up to incoming tunnelled packets.

2.3 Tunnelling Termination

2.3.1 Mobile Node

Whenever the mobile node detects a change in its network connectivity and initiates a registration, according to RFC 2002[6] section 3.6, it MUST stop using any UDP Tunnelling according to this paper, and return to standard Mobile IP operation as covered by RFC 2002[6]. If UDP Tunnelling is needed, it MUST be re-established without any state kept from earlier Tunnelling, using the extensions described in Section 2.4.2 and Section 2.4.4 in this document.

2.3.2 Home Agent

Whenever the home agent receives a Registration Request from a mobile node with a new care-of address, it MUST stop using any UDP Tunnelling according to this paper. If UDP Tunnelling is needed under the new registration, it MUST be re-established without any state kept from earlier Tunnelling.

This does not apply when the mobile node is re-registering due to the upcoming expiration of the lifetime of its registration, keeping the same care-of address. In this case, termination and re-establishment of Tunnelling SHOULD NOT be done.

2.4 Extension Formats

2.4.1 Vendor Specific Extensions

All Mobile IP extensions described in this paper are Vendor Specific Extensions[11], with the SMI Network Management Private Enterprise Code of ipUnplugged, which is 5925.

As per Section 3.2 and 3.6.1.3 of [6], the sender MUST include these Extensions before the Mobile-Home Authentication Extension in registration messages, so that they are covered by the Mobile-Home Authentication Extension.

2.4.2 UDP Port Request

This extension MAY be used in a Mobile IP Registration Request from the mobile node to the home agent when the mobile node uses a co-located care-of address. It SHALL NOT be used by the mobile node when it is registering with a foreign agent care-of address. It is not defined for use by a foreign agent.

The purpose of this extension is to indicate to the home agent that the mobile node is able to accept IP-UDP Tunnelling if the home agent has an indication that the mobile node resides behind a NAPT. It thus functions as a conditional solicitation for the assignment of a UDP port for the home agent endpoint of the IP-UDP tunnel.

The home agent SHALL use a mismatch between source IP address and care-of address in the Mobile IP Registration Request message as the indication that a mobile node may reside behind a NAPT. If the Registration Request also contains the UDP Port Request extension defined here, the home agent SHALL respond with a registration reply containing the UDP Port Assignment extension described in Section 2.4.4.

If the home agent receives a Registration Request with matching source IP address and co-located care-of address which contains a UDP Port Request Extension, the home agent SHALL NOT respond with a Registration Reply containing a UDP Port Assignment (Section 2.4.4).

The mobile node MAY propose a port number, by setting the 'Proposed UDP Port' field to a value different from zero, and the home agent MAY accept this proposed port.

This extension MAY also be used in a Registration Request during re-registering if an earlier assigned UDP port (Section 2.4.4) turns out to be blocked and unusable.

If the home agent receives a UDP port request when it already has an

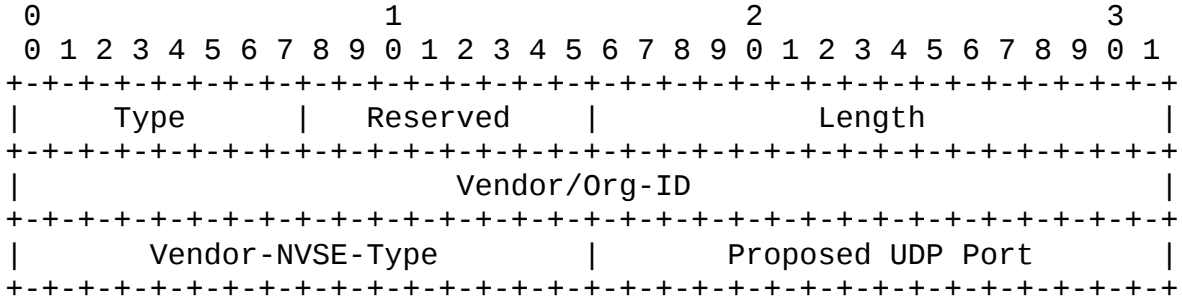
UDP port association for the sending mobile node at the source IP address, it SHALL interpret this as an indication that the prior UDP port assignment is or has become unusable, and SHOULD assign another port for the mobile node to use.

The mobile node MUST NOT request alternative forms of encapsulation by setting the 'M' bit and/or the 'G' bit of a Mobile IP registration request together with this extension.

The well-known Mobile IP port number 434 SHALL NOT be used for the UDP tunnel, neither in port requests or port assignments. Use of this port would require a mechanism to multiplex regular Mobile IP control traffic according to RFC 2002[6] with the tunnel traffic. This document does not provide any mechanisms to do so.

2.4.3 UDP Port Request Extension Format

This extension is a Normal Vendor/Organization Specific Extension (NVSE). The format of this extension is as shown below.



Type	NVSE-TYPE-NUMBER = 134
Reserved	Reserved for future use. MUST be set to 0 on sending, MUST be ignored on reception.
Length	Length in bytes of this extension, not including the Type and Length bytes.
Vendor/Org-ID	The SMI Network Management Private Enterprise Code of ipUnplugged = 5925
Vendor-NVSE-Type	UDP-Port-Request = 17
Proposed UDP Port	The mobile node may propose a port number to use for the Tunnelling, but the home agent is not bound to use this.

2.4.4 UDP Port Assignment

This extension MAY be used in a Mobile IP Registration Reply from the home agent to the mobile node.

The purpose of this extension is to indicate that the home agent

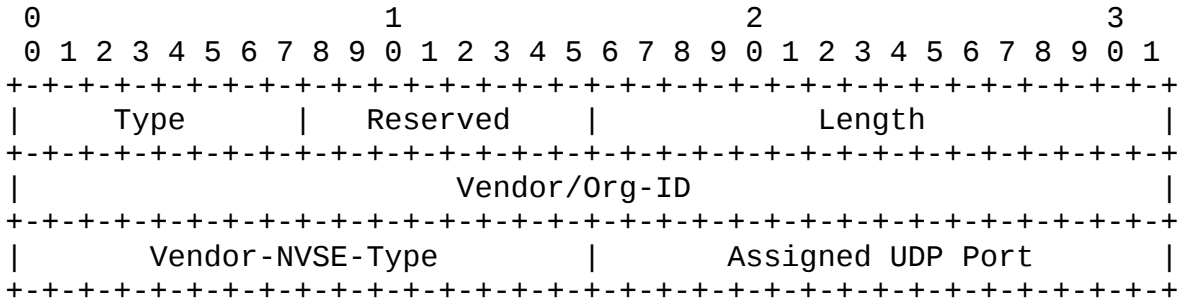
accepts the use of IP-UDP Tunnelling, and to inform the mobile node of the UDP port number of the home agent endpoint of the tunnel. On receipt of this message, the mobile node MUST use IP-UDP Tunnelling when sending IP packets to the home agent, and it MUST expect and accept IP-UDP tunnelled packets from the home agent.

The mobile node MUST use the assigned UDP port number for the IP-UDP tunnel for the lifetime of the mobility binding, unless explicitly reassigned. Reassignment SHALL ONLY be done on request, during re-registration, as described above.

This extension is added to a Mobile IP Registration Reply by the home agent when it has received and accepted a UDP Port Request (Section 2.4.2) from a mobile node.

2.4.5 UDP Port Assignment Extension Format

This extension is a Critical Vendor/Organization Specific Extension (CVSE). The format of this extension is as shown below.



Type	CVSE-TYPE-NUMBER = 38
Reserved	Reserved for future use. MUST be set to 0 on sending, MUST be ignored on reception.
Length	Length in bytes of this extension, not including the Type and Length fields.
Vendor/Org-ID	The SMI Network Management Private Enterprise Code of ipUnplugged = 5925
Vendor-NVSE-Type	UDP-Port-Assignment = 18
Assigned UDP Port	The UDP Port to be used as the home agent endpoint of the UDP tunnel.

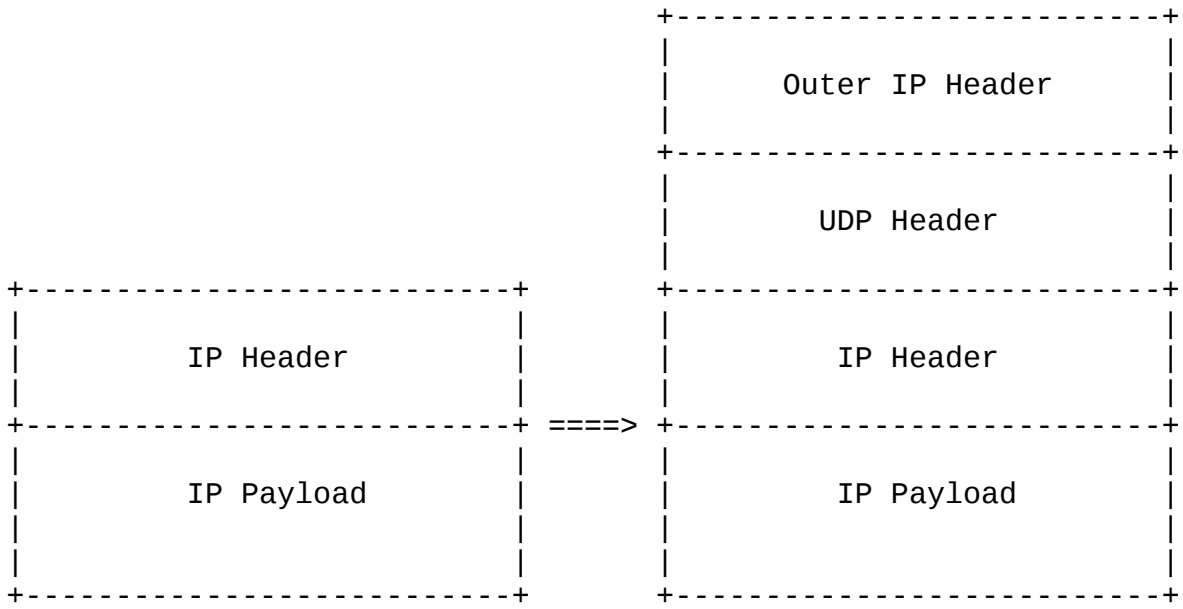
3. IP-in-UDP Tunnelling

IP-in-UDP Tunnelling, or UDP Tunnelling for short, is done completely analogous to RFC 2003[7], with the sole exception of the addition of an UDP header[1] between the outer and inner IP header.

Mobile IP Registration Requests and Registration Replies are already

in the form of UDP messages, and SHALL NOT be tunnelled even when IP-in-UDP Tunnelling is in force.

To encapsulate an IP datagram using IP in UDP encapsulation, an outer IP header[2] and UDP header[1] is inserted before the datagram's existing IP header, as follows:



The outer IP header Source Address and Destination Address, together with the UDP header Source Port and Destination Port, identify the "endpoints" of the tunnel. The inner IP header Source Address and Destination Addresses identify the original sender and recipient of the datagram, respectively. The inner IP header is not changed by the encapsulator, except to decrement the TTL as noted in RFC 2003[7], and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel. If need be, other protocol headers such as the IP Authentication header[4] may be inserted between the outer IP header and the UDP header. Note that the security options of the inner IP header MAY affect the choice of security options for the encapsulating (outer) IP header.

All other provisions and requirements of RFC 2003[7] are in force.

4. Advantages

One advantage with this mechanism for handling NAT devices and private addressing is that the mechanism is backwards compatible with RFC2002[6] and that minimal new procedures are introduced. This proposal uses no new control messages and introduces no additional

signalling latency.

Additionally this proposal does not require any specific port number to be used. This is an advantage since there are existing firewalls that might not allow specific ports. The configuration and negotiation possibility allows a flexible way to get through these firewalls.

This mechanism does not only solves the Mobile IP protocol NAPT traversal problem, but also other protocols that will run above it will benefit. One protocol of particular interest in mobile-VPNs is IPSec. If IKE and IPSec runs on top of Mobile IP, these protocols will not only be capable of surviving mobile node movements between subnets, but also survive NAPT traversal without modifications. Mobile IP is much more suited for handling the NAPT traversal than e.g. IKE[9] with its requirement of a specific port number (500) in both the source and destination field. This proposal allows not only for ESP to be used totally without modifications, but also AH to protect against source address spoofing if desired[12]. Also, there is no limitation between which entities the security associations may be established, the SA's could be set up between the MN and the HA, as well as between the MN and the CN.

Most importantly, this mechanism does not require change of, interaction with or preconditions on the NAT device itself - which would be totally impracticable. The NAT device is typically not controllable by the customer/corporate IT-manager in any way. Many hotel Internet connections are using NAT, airport & wireless services in public areas use NAT. Even some ISP use NAT to connect their clients to the internet, especially in Europe. None of these NAT devices will permit any control or interaction from a host device in a near future.

One alternative solution that could be considered is to create a HTTP session between the Home Agent and the mobile node and then tunnel Mobile IP and IP payload packets on top. The disadvantages of introducing HTTP into the solution is, not only extra overhead, but also its restrictions on real time applications and less optimal mobile node implementations. Another less advantageous alternative is to run Mobile IP over TCP. This would have negative effects on real time applications, as well as the added vulnerability for spoofed TCP connection reset attacks.

5. Security Considerations

The authors do not think this mechanism exposes any security vulnerabilities above those of using IP in IP encapsulation. There are less security issues to open up the HA access rules for a specific UDP port than to allow all IP-IP encapsulation packets in.

However, if the intermediate network is considered insecure, IPSec should be used.

An security advantage of this mechanism is that IKE and IPSec (both ESP and AH), if run on top of Mobile IP, will survive NAPT traversal without modifications. It could be used transparently both between the MN and the HA, as well as between the MN and the CN.

5.1 Firewall Considerations

This is not a general firewall traversal mechanism. However, using IP-in-UDP encapsulation instead of IP-in-IP encapsulation makes it easier to configure a firewall to allow for the traffic. It's simple to allow for UPD packets with a predetermined port number. There could however potentially be an issue with the increasing use of personal firewalls, which are most often deployed with the default settings intact. Some well-known, generally open port numbers could however be used with this proposal, e.g. 80 which is allowed by most firewalls and not used for other services by most HAs.

6. Intellectual property rights

ipUnplugged has one or more patents or patent applications that may be relevant to this internet-draft. If this specification is adopted by IETF and any claims of this or any other ipUnplugged patents are necessary for practicing this standard, any party will be able to obtain a license from ipUnplugged to use any such patent claims under openly specified, reasonable, non-discriminatory terms to implement and fully comply with the standard.

7. Acknowledgements

Much of the text in Section 3 has been taken almost verbatim from RFC 2003, IP Encapsulation within IP[7].

Many thanks to Peter Larsson, Olavi Kumpulianen, ipUnplugged, for essential contributions.

References

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

[2] Postel, J., Editor, "Internet Protocol", STD 5, RFC 791, September 1981.

[3] Postel, J., Editor, "Transmission Control Protocol (TCP) Specification", STD 7, RFC 793, September 1981.

[4] Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.

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

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

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

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

[9] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

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

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

[12] Aboba, B., "IPsec-NAT Compatibility Requirements", draft-ietf-ipsec-nat-reqts-00.txt (work in progress), June 2001.

Authors' Addresses

O. Henrik Levkowetz
ipUnplugged AB
Arenavagen 33
Stockholm S-121 28
SWEDEN

Phone: +46 8 725 9513
EMail: henrik@levkowetz.com

Jan Forslow
ipUnplugged AB
Arenavagen 33
Stockholm S-121 28
SWEDEN

Phone: +46 725 5912
EMail: jan@ipunplugged.com

Hans Sjostrand
ipUnplugged AB
Arenavagen 33
Stockholm S-121 28
SWEDEN

Phone: +46 8 725 5930
EMail: hans@ipunplugged.com

Full Copyright Statement

Acknowledgement

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