Network Working Group
Internet-Draft
Expires: August 24, 2004

T. Larsson
E. Gustafsson
H. Levkowetz
Ericsson

February 21, 2004

Use of MIPv6 in IPv4 and MIPv4 in IPv6 networks
draft-larsson-v6ops-mip-scenarios-01

Status of this Memo

Copyright Notice

Abstract

This document considers a heterogeneous network environment with interconnected IPv4 (public/private) and IPv6 networks. The document identifies the scenarios relevant for mobility management in such a heterogeneous network environment, lists work relevant to deploying Mobile IP under these conditions, and gives an inventory of possible

solutions.

Table of Contents

1. Introduction

1.1 Background

The Mobile IPv4 [RFC3344] protocol was designed for mobility management in pure IPv4 networks. Similarly, Mobile IPv6 [RFC3775] has been designed for mobility management in pure IPv6 networks. As IPv6 is introduced, it will most likely be through stepwise deployment, resulting in a heterogeneous network environment with interconnected IPv4 and IPv6 networks, where the IPv4 networks can be either of public or private address realm. It is probable that this type of network environment will be common for a long period of time.

A heterogeneous network environment, as described above, requires a solution for mobility management that runs over both IPv4 and IPv6 networks, including support for public as well as private IPv4 address spaces. This means that the mobility management solution needs to be able to cope with the Network Address Translators (NATs) [RFC2663] and Network Address Port Translators (NAPTs) [RFC2663] that are already deployed between public and private IPv4 address spaces. The term NAT refers to both NATs and NAPTs in the remainder of this document.

Mobile IPv4 defines a mechanism which enables nodes to change their point of attachment to the Internet without changing their IP address, i.e. IPv4 home address. Mobile IPv6 defines a similar mechanism for IPv6 networks. A solution for mobility management in a heterogeneous network environment should make it possible for nodes to change their point of attachment to the Internet without changing their IPv4 and IPv6 addresses, i.e. IPv4 home address and IPv6 home address. This will make it possible for the mobile nodes to maintain seamless connectivity for both their IPv4 and IPv6 applications.

1.2 Scope

The scope of this document is to identify the network and handoff scenarios relevant for mobility management in combined IPv4 (public/private) and IPv6 networks. We also provide an overview of related work that has been published earlier. Lastly, we list possible solutions, compliant to Mobile IP, and summarize their properties and applicability to the network and handoff scenarios.

The purpose of this document is explicitly not to describe any particular problem that has to be solved within this area. A problem statement needs to express many parameters related to the characteristics of access technology (cellular, 802.3, 802.11, 802.16, 802.20 etc.), predominant traffic (VoIP, Browsing, Terminal access, multimedia streams, ...), reachability requirements (global

or intra-network only reachability) and conceivably other. Individual problem statements are needed to lay out these parameters - this document seeks to define the field of combinations of the base IP and MIP technologies which should be considered when looking at possible solutions to individual problem statements.

Dynamic assignment of address in the home network, i.e., dynamic Mobile IP Home Address assignment is not covered here. If such assignments are done dynamically, they still happen only at the time of initial registration, not at every handoff. They therefore do not affect handoff characteristics, and also do not affect tunnel overhead, and thus are out of scope for this document.

Network attachment is also out of scope for this document. It is assumed that in any combination of the conceivable solutions discussed below, it is first necessary to determine whether one is attached to a new network or to one where connectivity has already been established. In a new network it is then, for all discussed solutions, necessary to obtain an address in the visited network, and the details of that operation would not affect the tunneling overhead or choice of tunneling technology. We somewhat arbitrarily choose to ignore the one case which is slightly different in this respect - the case where a MIPv4 FA (Foreign Agent) is present in the visited network. In this case, the task of obtaining a local address is unnecessary, but it is still necessary for the Mobile Node to determine that there is an FA present.

1.3 Earlier work

The issue has in parts been described earlier in [I-D.ietf-ngtrans-moving], [I-D.tsao-mobileip-dualstack-model], [I-D.tsirtsis-dsmip-problem], [I-D.soliman-v4v6-mipv4] and [I-D.tsirtsis-v4v6-mipv4]. None of these drafts, however, provides an exhaustive list of scenarios for mobility in combined IPv4 (public/private) and IPv6 networks.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.

3. Problem description

This draft outlines scenarios for mobility management in heterogeneous network environments, i.e. including public and private

IPv4 address spaces, IPv6 address spaces as well as NATs and NAPTs.

Although there is currently no standardized Mobile IP-based solution that handles all the different aspects of this type of network scenario, a number of solutions for Mobile IP across heterogeneous networks have been proposed. This draft outlines possible solutions, and comments on what types of network scenarios they apply to.

To be able to analyze solutions for Mobile IP mobility over heterogeneous networks, we have estimated parameters such as transport overhead (e.g. tunneling), handoff latency (e.g. number of signaling roundtrips between the mobile node and its home network), and signaling overhead (e.g. tunneling of registration messages, or keep-alive messages) for the different solutions. These parameters, in combination with deployment issues and impact on existing infra-structure, assumed or imposed by the different solutions, give an overview of the their suitability in different deployment scenarios.

The issue of handoff latency would be especially important in cases where Mobile IP provides mobility for real-time applications, e.g. Voice over IP calls. In these cases, an absolute minimum of signaling roundtrips is required at each handoff. Also, when running real-time applications, a mobile node cannot afford to await timeouts in deciding which mobility signaling mechanism to use when arriving at a new access network.

Overhead, for transport or signaling, may be significant in the case of wireless access networks, where traffic over the air needs to be kept at a minimum. Furthermore, requirements on introducing additional authentication mechanisms and systems for subscription/ user management are also a key factor in evaluating different solutions.

This draft does not consider performance in terms of mechanisms for movement detection.

A summary of the proposed solutions and a discussion about their properties is provided in the conclusions section.

4. Scenarios

This section describes relevant network scenarios for mobility in IPv4 (public/private) and IPv6 networks. We also outline deployment cases and discuss which network scenarios that need to be fulfilled for a solution to fully support mobility over heterogeneous access networks.

In the tables below, "MN" refers to the IP version run on the MN

(requested by application), "MIP" refers to the Mobile IP version run on the MN and on the HA, "Access" reflects the IP version run on the access network (visited or home), and "Transport" refers to the transport network between the visited and the home network.

The scenarios are based on the following general assumptions:

- o The MN supports and runs Mobile IP; either MIPv4 or MIPv6.
- o The MN is associated with a HA supporting the same Mobile IP version as the MN.
- o If the access network runs IPv4, there may or may not be FA support. A Mobile IPv4-compliant solution should be able to handle both cases.
- o If the MN, HA and CN run MIPv6, a MIPv6-compliant solution should support route optimization between the MN and the CN. Alternatively, the MN should know precisely under what conditions to use route optimization and when to use reverse tunneling.

Scenarios including Network Address Translation - Protocol Translation (NAT-PT) [RFC2766] nodes, which will be found on the boundaries between IPv6 networks and IPv4 networks, are not included in this document. The use of NAT-PT has been analyzed in several other documents ([I-D.satapati-v6ops-natpt-applicability], [I-D.ietf-v6ops-3gpp-analysis]) where the use of NAT-PT as a general-purpose transition mechanism is discouraged. NAT-PT should only be viewed as a short-term solution in specific deployment scenarios.

Table 1: Network scenarios without NAT/NAPT between the access network and the transport network.

#	MN	MIP	Access	Transport	Description
1	IPv4	MIPv4	IPv4	IPv4	"Native MIPv4"
2	IPv6	MIPv4	IPv4	IPv4	"IPv6 in MIPv4"
3	IPv4	MIPv6	IPv4	IPv4	"IPv4 in MIPv6 over IPv4"
4	IPv6	MIPv6	IPv4	IPv4	"MIPv6 over IPv4"
5	IPv4	MIPv4	IPv6	IPv6	"MIPv4 over IPv6"
6	IPv6	MIPv4	IPv6	IPv6	"IPv6 in MIPv4 over IPv6"
7	IPv4	MIPv6	IPv6	IPv6	"IPv4 in MIPv6"
8	IPv6	MIPv6	IPv6	IPv6	"Native MIPv6"

Table 2: Network scenarios with NAT/NAPT between the access network and the transport network.

#	MN	MIP	Access	Transport	Description
9	IPv4	MIPv4	IPv4-priv	IPv4	"Native MIPv4"
10	IPv6	MIPv4	IPv4-priv	IPv4	"IPv6 in MIPv4"
11	IPv4	MIPv6	IPv4-priv	IPv4	"IPv4 in MIPv6 over IPv4"
12	IPv6	MIPv6	IPv4-priv	IPv4	"MIPv6 over IPv4"

Based on the network scenarios in Table 1 and 2, we can derive different handoff scenarios, i.e. as the mobile node moves between access networks supporting different IP versions. Table 3 describes the handoff scenarios generated from the network scenarios in Table 1. The column "Access handoff" describes bi-directional handoff scenarios, e.g. "IPv4-IPv6" refers to handoffs from an IPv4 to an IPv6 access network, as well as from an IPv6 to an IPv4 access network.

Table 3: Handoff scenarios generated from Table 1.

#	MN	MIP	Access handoff	Description
a	IPv4	MIPv4	IPv4-IPv4	"Native MIPv4"
b	IPv6	MIPv4	IPv4-IPv4	"IPv6 in MIPv4"
c	IPv4	MIPv4	IPv4-IPv6	"MIPv4 over IPv6"
d	IPv6	MIPv4	IPv4-IPv6	"IPv6 in MIPv4 over IPv6"
e	IPv4	MIPv4	IPv4-IPv6	"MIPv4 over IPv6"
f	IPv6	MIPv4	IPv4-IPv6	"IPv6 in MIPv4 over IPv6"
g	IPv4	MIPv4	IPv6-IPv6	"MIPv4 over IPv6"
h	IPv6	MIPv4	IPv6-IPv6	"IPv6 in MIPv4 over IPv6"
i	IPv4	MIPv6	IPv4-IPv4	"IPv4 in MIPv6 over IPv4"
j	IPv6	MIPv6	IPv4-IPv4	"MIPv6 over IPv4"
k	IPv4	MIPv6	IPv4-IPv6	"IPv4 in MIPv6 over IPv4"
l	IPv6	MIPv6	IPv4-IPv6	"MIPv6 over IPv4"
m	IPv4	MIPv6	IPv4-IPv6	"IPv4 in MIPv6 over IPv4"
n	IPv6	MIPv6	IPv4-IPv6	"MIPv6 over IPv4"
o	IPv4	MIPv6	IPv6-IPv6	"IPv4 in MIPv6"
p	IPv6	MIPv6	IPv6-IPv6	"Native MIPv6"

Table 4 complements Table 3 by describing handoff cases generated from Tables 1 and 2, i.e. between IPv6 and public/private IPv4 address spaces.

Table 4: Handoff scenarios to/from private IPv4, generated from Table 1 and 2.

#	MN	MIP	Access handoff	Description
aa	IPv4	MIPv4	IPv4 - IPv4-priv	"Native MIPv4"
bb	IPv6	MIPv4	IPv4 - IPv4-priv	"IPv6 in MIPv4"
cc	IPv4	MIPv4	IPv6 - IPv4-priv	"MIPv4 over IPv6"
dd	IPv6	MIPv4	IPv6 - IPv4-priv	"IPv6 in MIPv4 over IPv6"
ee	IPv4	MIPv4	IPv6 - IPv4-priv	"MIPv4 over IPv6"
ff	IPv6	MIPv4	IPv6 - IPv4-priv	"IPv6 in MIPv4 over IPv6"
gg	IPv4	MIPv6	IPv4 - IPv4-priv	"IPv4 in MIPv6 over IPv4"
hh	IPv6	MIPv6	IPv4 - IPv4-priv	"MIPv6 over IPv4"
ii	IPv4	MIPv6	IPv6 - IPv4-priv	"IPv4 in MIPv6 over IPv4"
jj	IPv6	MIPv6	IPv6 - IPv4-priv	"MIPv6 over IPv4"
kk	IPv4	MIPv6	IPv6 - IPv4-priv	"IPv4 in MIPv6 over IPv4"
ll	IPv6	MIPv6	IPv6 - IPv4-priv	"MIPv6 over IPv4"

Regarding deployment of Mobile IP, we identify three main cases:

- o Case I (MIPv4-based): Mobile IPv4 is already deployed in an operator's/ISP's networks, and a solution is needed to allow Mobile IPv4 to work over both IPv4 and IPv6 address spaces.
- o Case II (MIPv6-based): Mobile IPv4 is not deployed, but the operator/ISP plans to deploy Mobile IPv6 directly, and needs a solution to allow Mobile IPv6 to work over both IPv4 and IPv6 networks.
- o Case III (MIPv4-MIPv6): Mobile IPv4 is deployed by an operator/ISP who now plans to migrate to Mobile IPv6, and therefore needs a solution for Mobile IPv4-Mobile IPv6 migration.

These deployment cases are reflected in solutions proposed for mobility over IPv4/IPv6 networks.

For a mobility solution to fulfill the requirement of supporting "heterogeneous access networks", it should support both IPv4 and IPv6 applications running continuously on the mobile node, while the mobile node moves between IPv6 and IPv4 (public and private) access networks. In essence, this means that the mobile node must be able to communicate with its home agent over both IPv4 and IPv6 networks, and that the Mobile IP stack in the mobile node (MIPv4 or MIPv6) must provide Mobile IP transport for both IPv4 and IPv6 sockets.

This can be provided in any of the three deployment scenarios described above:

o A solution for deployment case I (MIPv4-based) needs to handle network scenarios 1-2, 5-6 in Table 1 and 9-10 in Table 2, as well as handoff scenarios a-h in Table 3 and aa-ff in Table 4.
o A solution for deployment case II (MIPv6-based) needs to handle network scenarios 3-4, 7-8 in Table 1 and 11-12 in Table 2, as well as handoff scenarios i-p in Table 3 and gg-ll in Table 4.
o A solution for deployment case III (MIPv4-MIPv6) needs to handle network scenarios 1-2, 7-8 in Table 1 and 9-10 in Table 2. The handoff scenarios listed in Tables 3 and 4 are not really applicable to this type of solution. As the aim is to address MIPv4-MIPv6 interworking, we may assume that MIPv4 and MIPv6 run in parallel on the MN and the HA, and that the MN will be able to shift MIP version during a handoff, accommodating to the IP version of its current access network. For this to work, the MIP stack in the MN also needs to provide the appropriate MIP transport for both IPv4 and IPv6 sockets.

Solutions for Mobile IP mobility management over IPv4/IPv6 networks can be roughly divided into two main categories: (a) solutions defining extensions to the Mobile IP standards (MIPv4/MIPv6), and (b) solutions based on existing Mobile IP standards combined with existing transition mechanisms. When relying on existing transition mechanisms, we add to the network scenarios in Tables 1 and 2 by allowing the transport network to have a different IP version than the access network. The transition mechanism is assumed to handle for instance a scenario with a Mobile IPv6 mobile node, an IPv4 access network and an IPv6 transport network. While a transition mechanism would allow native Mobile IPv6 signaling over an IPv4 access network, extensions to the mobility protocol would still be needed for e.g. the Mobile IPv6 host to provide Mobile IPv6 transport for IPv4 payload.

Related work and possible solutions are discussed in the following sections.

5. Related work

The following lists related work, explains how it relates to the different deployment cases, and reflects upon its applicability to Mobile IP-based mobility management over heterogeneous address spaces. Different solutions are further evaluated in coming sections and in the appendixes.

5.1 Dual-stack Mobile IPv4-Mobile IPv6

Implementing dual-stack (DS) nodes with support for standard Mobile IPv4 and Mobile IPv6 is described in [I-D.tsao-mobileip-dualstack-model]. This implementation includes an address mapper, located

between the IP layer and the Mobile IP layer, which can associate a home address of one IP version with a care-of address of another IP version. By dispatching IPv4/IPv6 packets to the correct layers, the address mapper provides a transparent service to upper layer protocols.

The dual-stack MIPv4-MIPv6 solution addresses the network scenario cases 1-8 in Table 1, and cases 9, 10 in Table 2. This solution also addresses handoff between IPv4 and IPv6 access networks.

The dual-stack MIPv4-MIPv6 solution supports deployment case III, of co-existing Mobile IPv4 and Mobile IPv6. However, drawbacks of this solution, also pointed out in [I-D.tsirtsis-dsmip-problem], are that the mobile node and home agent both need to support two sets of mobility protocols, that the mobile node needs to send two sets of signalling messages at each handoff, and that network administrators need to run and maintain two sets of mobility management systems, including subscription management, on the same network.

5.2 Enhanced Mobile IPv4

Extending Mobile IPv4 to support IPv6 address spaces supports deployment case I, i.e. where an operator/ISP already has Mobile IPv4 running, and aims to support IPv6 address spaces by enhancing Mobile IPv4. This type of solution addresses network scenario cases 1-2, 5-6 in Table 1, and cases 9-10 in Table 2. It also addresses handoff cases a-h in Table 3 and handoff cases aa-ff in Table 4. That is, cases with descriptions "Native MIPv4", "IPv6 in MIPv4", "MIPv4 over IPv6" and combinations of these.

A solution of this kind consists of two parts:

1. Enhance MIPv4 to provide support for tunneling MIPv4 packets over IPv6 transports. This solves scenario 5 in addition to 1, and scenario 6 if combined with the enhancement below. We denote such a solution "MIPv4o".
2. Enhance MIPv4 to carry IPv6 payloads. This solves scenario 2, and scenario 6 if combined with the enhancement above. We denote such a solution "MIPv4x".

MIPv4 enhanced in both respect we will denote "MIPv4xo".

A solution to part 1 above is proposed in [I-D.tsirtsis-v4v6-mipv4]. This solution assumes dual-stack nodes with Mobile IPv4 support (HA, MN, FA), and defines extensions to Mobile IPv4 to support IPv6 home address and IPv6 care-of address for the mobile node. Relying on today's standard Mobile IPv4, this solution supports both public and private IPv4 address spaces, and supports scenario cases 1, 5 and 9.

5.3 Enhanced Mobile IPv6

Extending Mobile IPv6 to support IPv4 address spaces supports deployment case II, i.e. where an operator/ISP deploys Mobile IPv6 without having deployed Mobile IPv4, and thus seeks to support IPv4 address spaces by enhancing Mobile IPv6.

This type of solution addresses network scenario cases 3-4, 7-8 in Table 1, and handoff cases i-p in Table 3. In summary, cases with descriptions "Native MIPv6", "IPv4 in MIPv6", "MIPv6 over IPv4" and combinations of these.

A solution of this kind consists of two parts:
1. Enhance MIPv6 to provide support for tunneling MIPv6 packets over IPv4 transports. This solves scenario 4 in addition to 8, and scenario 3 if combined with the enhancement below. We denote such a solution "MIPv6o".
2. Enhance MIPv6 to carry IPv4 payloads. This solves scenario 7, and scenario 3 if combined with the enhancement above. We denote such a solution "MIPv6x".

MIPv6 enhanced in both respect we will denote "MIPv6xo".

The draft [I-D.soliman-v4v6-mipv4] proposes an enhanced Mobile IPv6 solution to the first part above, for public IPv4 address spaces only. This solution assumes dual-stack nodes (HA, MN), and extends Mobile IPv6 so that the MN can simultaneously maintain connections to its IPv4 and IPv6 home address respectively.

If this solution was further enhanced to support private IPv4 address spaces, it would also support network scenario case 12 in Table 2, and handoff cases hh, jj and ll in Table 4. This would, however, generate additional overhead.

5.4 ISATAP

ISATAP [I-D.ietf-ngtrans-isatap] specifies a protocol connecting IPv6 hosts and routers within IPv4 sites. ISATAP allows dual-stack nodes that do not share a link with an IPv6 router to automatically tunnel packets to the IPv6 next-hop address through IPv4, i.e. the site's IPv4 infrastructure is treated as a link layer for IPv6. ISATAP enables automatic IPv6-in-IPv4 tunneling for both public and private IPv4 addresses. Use of private IPv4 addresses will, however, require that no NAT(s) exist between the host and the ISATAP router. A NAT can be deployed in parallel with the ISATAP router if the ISATAP router provides global IPv4 connectivity in parallel with IPv6 connectivity.

In combination with Mobile IPv6 [RFC3775], ISATAP can provide

mobility support for deployment case II (MIPv6-based).

5.5 Teredo

The Teredo solution [I-D.huitema-v6ops-teredo] addresses the generic issue of providing IPv6 service to nodes located behind one or several IPv4 NATs. The mechanism for achieving this is tunneling of IPv6 over UDP through the NATs. The key components of the Teredo service are: (i) Teredo client - a node that has IPv4 and needs IPv6 connectivity; (ii) Teredo server - provides IPv6 connectivity to Teredo clients; (iii) Teredo relay - IPv6 router forwarding traffic to Teredo clients; and (iv) Teredo IPv6 address - IPv6 address consisting of the specific Teredo prefix, Teredo server IPv4 address, client IPv4 address, client UDP port number and a flag indicating type of NAT. (Teredo provides connectivity through the most usual types of NATs, and for those for which full connectivity is not possible, workarounds may be devised which sacrifice MIPv6 route optimization.)

The normal operation mode of Teredo involves three actors: Teredo client needing IPv6 connectivity behind a NAT, Teredo servers providing the service, and Teredo relays providing for the interconnection between the Teredo service and the native IPv6 Internet. The relays are connected to the IPv6 Internet and participate in IPv6 routing. They announce the Teredo IPv6 prefix and are able to relay IPv6 packets over IPv4 UDP towards the client. Teredo servers enable NAT traversal and are designed so that when NAT traversal is guaranteed, packets flow on a direct path between source and destination. It should be noted, however, that Teredo's default mode of operation requires changes in the IPv6 routers, e.g. Teredo relays.

Another possibility is to deploy Teredo as a stateful tunnel server instead of the default mode where it is stateless. The Teredo server will then act as a tunnel broker, i.e. the Teredo server will be the end-point of the tunnel and all traffic needs to be tunneled through it. This eliminates the need for relays and makes Teredo useful in supporting IP mobility, e.g. in combination with Mobile IPv6 [RFC3775] and enhanced MIPv6 as discussed above [I-D.soliman-v4v6-mipv4].

5.6 STEP

The STEP draft [I-D.savola-v6ops-conftun-setup] describes mechanisms to establish IPv6-in-IPv4 tunnels between an ISP and its customer. During the STEP procedure, the customer discovers (using one of many possible methods) the IPv4 tunnel end-point of the ISP, and a tunnel is then established between the customer and the ISP. STEP addresses

NAT traversal through use of either protocol 41 (IPv6 over IPv4 tunnels) or UDP encapsulation.

One of the main ideas behind STEP is to provide this tunnel service without additional protocol specification or substantial modifications to IPv6 or IPv4 implementations either at the ISP or customer side, i.e. existing mechanisms for e.g. prefix delegation and authentication are used.

In combination with Mobile IPv6, STEP can provide mobility support for deployment case II (MIPv6-based).

5.7 6to4

The draft [I-D.kahng-mobileip-moving6to4] proposes a solution based on 6to4 for MIPv6 mobility management over IPv6 transition networks (IPv6 sites interconnected over an IPv4 wide area network). The main focus of this draft is selection of home address and care-of address when both IPv6 and 6to4 addresses are available.

This solution primarily addresses cases where the mobile node has IPv6 connectivity to a correspondent node, and where either the mobile node, the correspondent node, or both move between IPv6 and 6to4 access networks. Although the draft does not mention native IPv4 access networks, this scenario may also be supported through implementation of the 6to4 router in the mobile node itself. For such a solution to work, the home network needs 6to4 functionality in order to receive packets from the mobile node. The same applies to the correspondent node (or its access network), in case route optimization is used. Also, the solution would in most cases not support NAT traversal between the mobile node and its home agent, or between the mobile node and the correspondent node. I.e., only traversal of NATs allowing IPv6-in-IPv4 tunnels through would be supported. It should be noted, however, that the 6to4 solution [RFC3056] states that the 6to4 mechanism is almost entirely implemented in border routers, rather than hosts.

In itself, this solution addresses only in part deployment case II. However, combined with, e.g. Teredo, it addresses deployment case II in its entirety, including NAT traversal.

5.8 Doors

Another way of using the 6to4 mechanism to support Mobile IPv6 over IPv4 is named Doors [I-D.thubert-nemo-ipv4-traversal]. The proposed Doors mechanism adds some features, notably NAT traversal, to that provided by using base 6to4, but the description does not go into sufficient detail that it was judged necessary (at the level of this

document) to do a separate analysis of Doors, as distinct from base 6to4 [RFC3056].

5.9 TSP

The Tunnel Setup Protocol (TSP) [I-D.blanchet-v6ops-tunnelbroker-tsp] is a protocol to set up tunnels between a client and a tunnel server, possibly through a broker. This protocol, which uses XML messaging and SASL authentication, can negotiate the setup of, e.g. IPv6-in-IPv4, IPv6-in-UDP-in-IPv4 or IPv4-in-IPv6 tunnels.

To set up a tunnel, once the client has located a server or broker, it sends the current protocol version it supports, and the server replies with a list of capabilities supported for authentication and tunnels. The client then authenticates itself to the server and, upon successful authentication, requests a tunnel setup to the server.

Provided that TSP is deployed, it could be used to set up IPv6-in-IPv4 or IPv6-in-UDP-in-IPv4 tunnels that would allow MIPv6 mobile nodes connectivity over IPv4 networks. In this case, TSP would address deployment case II (MIPv6-based). If used to set up IPv4-in-IPv6 tunnels, TSP would also address deployment case I (MIP4-based).

6. Possible Solutions

This section describes and evaluates different combinations of the solutions discussed in the previous section, including how these combinations apply to the different deployment cases. Rough performance estimations, in terms of added transport overhead and roundtrips for handoff signaling, are also listed - below and in the appendixes.

As mentioned earlier, there are roughly two categories of solutions: based on extensions to the Mobile IP protocols, or based on existing transition mechanisms. There are three solutions extending the Mobile IP protocols: "Dual-stack MIPv4-MIPv6", "Enhanced MIPv4" and "Enhanced MIPv6". As for solutions relying on existing transition mechanisms, we identify the following: "MIPv6 with ISATAP", "MIPv6 with Teredo and 6to4", "MIPv6 with STEP", and "MIPv6 or MIPv4 with TSP".

In general, transition mechanisms solve the issue of transporting, e.g. MIPv6 over an IPv4 network (public or private). Mechanisms in the host for allowing the Mobility protocol to transport multiple IP protocol versions, rather than only the native IP protocol version, need to be addressed through extensions to the Mobility protocol (MIPv4x/MIPv6x).

6.1 Dual-stack MIPv4-MIPv6

The DS MIPv4-MIPv6 solution [I-D.tsao-mobileip-dualstack-model], addresses deployment case III, of co-existing MIPv4 and MIPv6. Through its implementation of dual stacks as well as dual MIP protocols, this solution generates overhead, compared to native MIPv4 or MIPv6.

First, the MN needs to implement MIPv4, MIPv6 and an address mapper. The HA also needs to implement both MIPv4 and MIPv6. This includes implementation of double sets of security bindings, subscription management etc.

Second, double sets of registration/binding update signaling messages, MIPv4 and MIPv6, are generated at each handoff. This results in a total of four signaling messages for each handoff, equaling to two signaling roundtrips between the MN and the HA. The signaling messages for MIPv4 and MIPv6 are, however, sent in parallel. Therefore, the latency for handoff signaling should correspond to one roundtrip rather than two. The overhead though, counted in number of signaling messages, is twice as much as for stand-alone MIPv4 or MIPv6 signaling. Also, there is additional overhead due to tunneling of registration messages; either MIPv4 registration in IPv6, or MIPv6 binding update in IPv4. As for transport overhead, this solution compares to native MIPv4 or MIPv6.

6.2 Enhanced MIPv4

Enhanced MIPv4 addresses deployment case I by extending native MIPv4 to support both IPv4 and IPv6 home addresses at the same time. Enhanced MIPv4 affects the MN and the HA, as both the MN and the HA need to be configured with each other's IPv4 and IPv6 addresses.

The number of signaling messages at a handoff is the same as for native MIPv4 - registration request and reply, generating a total of one signaling roundtrip. This solution also adds a few extensions to the registration request/reply messages: a skippable IPv6 home address extension of 20 bytes, and a skippable IPv6 compatibility extension of 4 bytes, in order to transport MIPv4 over IPv6 (MIPv4o). Another extension of length 4 bytes is needed to arrange for carrying IPv6 payloads in MIPv4 (MIPv4x). Also, in case of an IPv6 access network, the registration signaling is tunneled in IPv6, generating an extra 40 bytes overhead (IPv6 header).

As for the transport overhead, Enhanced MIPv4 generates an additional 40 bytes (IPv6 header) due to tunneling over IPv6 networks.

6.3 Enhanced MIPv6

Enhanced MIPv6 addresses deployment case II by extending native MIPv6 to support both a (public) IPv4 and IPv6 home address simultaneously (MIPv6o). Introducing enhanced MIPv6 affects the MN and the HA. The MN must, in addition to the Mobile IPv6 configuration, be configured with the IPv4 address of the home agent, and must possibly also be configured with an IPv4 home address. (The IPv4 home address can be dynamically requested as well.) The HA needs to store the MN's IPv4 and IPv6 home addresses, as well as the current care-of-address(es). This means two entries in the binding update list of the HA; one for the IPv6 home address and one for the IPv4 home address.

The number of signaling messages at each handoff is the same as for Mobile IPv6. This means a total of two signaling messages, e.g. one binding update and one binding acknowledgement at each handoff, resulting in one signaling roundtrip. The signaling overhead is somewhat larger compared to Mobile IPv6, i.e. the binding update is extended with 6 bytes (IPv4 home address option) and the binding acknowledgement is extended with 8 bytes (IPv4 address acknowledgement option). In order to arrange to carry IPv4 in MIPv6 (MIPv6x, scenarios 3 and 7), a further extension of length 4 bytes is needed. Additional tunneling overhead for signaling will also be generated in IPv4 access networks due to the fact that the MIPv6 binding updates must be encapsulated in IPv4, i.e. 20 bytes.

As for transport overhead, in IPv4 access networks the traffic is tunneled IPv6-in-IPv4, thus adding an extra 20 bytes (IPv4 header) compared to native MIPv6.

It should be noted that this solution does not support route optimization when the mobile node is located in an IPv4 access network.

As mentioned earlier, the Enhanced Mobile IPv6 solution could be further enhanced to support private IPv4 address spaces, i.e. to support NAT traversal. By doing so, the solution would support deployment case II in its entirety, at the cost of additional overhead.

6.4 MIPv6 with ISATAP

As mentioned earlier, ISATAP in combination with Mobile IPv6 [RFC3775] provides mobility support for deployment case II. Deployment-wise, this solution assumes an ISATAP router with IPv6 connectivity in the access network, and an ISATAP client in the MN. This solution allows Mobile IPv6 route optimization.

The operation of ISATAP is independent of Mobile IPv6. This means that Mobile IPv6 signaling will take place after ISATAP router discovery (e.g. discovery of ISATAP router IPv4 address). The handoff latency will therefore depend on the method for ISATAP router discovery. This will generate at least one signalling roundtrip (within the access network) before address configuration and Mobile IPv6 signalling can take place.

Overhead in the ISATAP case, compared to native IPv6, includes IPv4 encapsulation of router solicitations, router advertisements, Mobile IPv6 signaling and Mobile IPv6 traffic, i.e. generating an additional 20 bytes in overhead per message (between the mobile node and the ISATAP router).

While ISATAP enables Mobile IPv6 signaling and tunneling over IPv4, it does not solve the host-internal issue of providing Mobile IPv6 transport for IPv4 applications. This would require extensions to Mobile IPv6 (MIPv6x). Given such extensions, Mobile IPv6 with ISATAP solves scenarios 3-4 and 7-8 in Table 1 (with IPv6 transport network), scenarios 11-12 in Table 2, scenarios i-p in Table 3 and scenarios gg-ll in Table 4.

6.5 MIPv6 with Teredo and 6to4

Another alternative for deployment case II is MIPv6 with Teredo and 6to4. Teredo would be used when the mobile node would find itself behind a NAT, while 6to4 would be used otherwise. This solution requires that a MN using regular MIPv6 for mobility be enhanced with both a Teredo client implementation and a local 6to4 implementation.

MIPv6 in combination with Teredo covers scenarios 11-12 of Table 2, while MIPv6 in combination with a 6to4 implementation in the local stack covers scenario 3-4 in Table 1. Scenario 8 is covered natively by MIPv6. Scenario 7 is not solved by any combination of regular MIPv6 and other transition mechanisms - it requires an extension to MIPv6. Given such an extension to MIPv6 (MIPv6x), this solution would also cover scenarios i-p in Table 3 and scenarios gg-ll in Table 4.

During handoff to a public IPv4 address, the 6to4 stack will construct a 6to4 IPv6 address after the public IPv4 address has been acquired, and MIPv6 will use that address to communicate with the IPv6 home network and the MIPv6 home agent. There are no added registration messages. The transport overhead will be 20 bytes.

In the Teredo case, the mobile node would be pre-configured with the address of its Teredo server, and would not have to search for it.

On the other hand, in the Teredo case the mobile node will have to run the Teredo qualification procedure, which may require as little as one additional roundtrip, but in the worst case may require as much as 12 seconds plus one round-trip in order to determine the type of NAT. The Teredo client may also have to send a Teredo bubble through the NAT before traffic can be received from a correspondent node, which we count as yet another half roundtrip, compared with MIPv6.

Route optimization for MIPv6 works when MIPv6 is used with Teredo/6to4, but note that there may still be a triangular routing through a Teredo Relay, if the host with which the mobile node is communicating is not itself Teredo enabled.

6.6 MIPv6 with STEP

STEP in combination with Mobile IPv6 [RFC3775] provides mobility support for deployment case II (i.e. MIPv6 based). Deployment-wise, this solution will require a tunnel router in the ISP's network that provides IPv6 connectivity, and a client in MN that handles e.g. discovery of the tunnel router. This solution allows Mobile IPv6 route optimization.

The operation of STEP is independent of Mobile IPv6. This means that Mobile IPv6 signaling will take place after the discovery of the IPv4 tunnel end-point address. The handoff latency will therefore depend on the method for tunnel router discovery. This will generate at least one signalling roundtrip before address configuration and Mobile IPv6 signalling can take place.

Overhead in the STEP case, compared to native IPv6, includes IPv4 or UDP encapsulation of router solicitations, router advertisements, Mobile IPv6 signaling and Mobile IPv6 traffic, i.e. generating an additional 20 (IPv4 encapsulation) or 28 bytes (UDP encapsulation) in overhead per message.

While STEP enables Mobile IPv6 signaling and tunneling over IPv4, it does not solve the host-internal issue of providing Mobile IPv6 transport for IPv4 applications. This would require extensions to Mobile IPv6. Given such extensions (MIPv6x), Mobile IPv6 with STEP solves scenarios 3-4 and 7-8 in Table 1 (with IPv6 transport network), scenarios 11-12 in Table 2, scenarios i-p in Table 3 and scenarios gg-ll in Table 4.

6.7 MIPv6 or MIPv4 with TSP

Assuming that TSP is deployed, it could be used to set up IPv6-in-IPv4 or IPv6-in-UDP-in-IPv4 tunnels to allow MIPv6 mobile nodes

connectivity over IPv4 access networks, hereby addressing deployment case II. With an extension to the MIPv6 host, allowing MIPv6 transport for IPv4 sockets, this solution covers scenarios 3-4, 7-8 in Table 1, 11-12 in Table 2, i-p in Table 3 and gg-ll in Table 4.

Deployment case I can be addressed by using TSP to set up IPv4-in-IPv6 tunnels. With an extension to the MIPv4 host (MIPv4x), allowing MIPv4 transport for IPv6 sockets, this solution covers scenarios 1-2, 5-6 in Table 1, 9-10 in Table 2, a-h in Table 3 and aa-ff in Table 4.

In addition to deployment of TSP clients and servers, these solutions requires deployment of SASL [RFC2222] for authentication of the tunnel setup signaling. The signaling between client and server to set up a tunnel (including SASL authentication) amounts to three roundtrips. Depending on deployment, a client may also need to locate a broker/server, thereby generating more signaling roundtrips. Once the signaling between the TSP client and server is finished, MIPv4/MIPv6 registration can start. Thus, in total, this method generates at least three signaling roundtrips before MIPv4/MIPv6 signaling starts.

In case of MIPv6, if the mobile node is located in an IPv4 access network, the MIPv6 binding update messages are sent either through an IPv6-in-IPv4 tunnel, generating an overhead of 20 bytes (IPv4 header) or through an IPv6-in-UDP-in-IPv4 tunnel, generating an overhead of 28 bytes (IPv4 plus UDP header), compared to native MIPv6. Similarly, the transport overhead amounts to 20 or 28 bytes.

In case of MIPv4, when the mobile node is located in an IPv6 access network, the MIPv4 registration messages are sent through an IPv4-in-IPv6 tunnel, generating an overhead of 40 bytes (IPv6 header), compared to native MIPv4. This overhead applies to the transport as well.

Theoretically, MIPv6 with TSP allows for MIPv6 route optimization through the TSP server. Depending on where the server is located though, compared to the MN and the CN, the route may be more or less triangular.

7. Conclusions

We have outlined network and handoff scenarios for mobility over IPv4 (public and private) and IPv6 address spaces. We have also listed and commented on related work and evaluated possible solutions for solving mobility in these scenarios in a way compliant with Mobile IP.

In general terms, three problems need to be solved: (1) tunneling of

packets over the access network (IPv4 over IPv6, or IPv6 over IPv4); (2) NAT traversal; and (3) enhancement of MIPv4 to carry IPv6 payloads and/or enhancement of MIPv6 to carry IPv4 payloads. A solution for problem (3) needs to be included in all proposed solutions, except "Dual-stack MIPv4-MIPv6" where this is already solved.

From the evaluations, we can draw the following conclusions:

- o Solution Dual-stack MIPv4-MIPv6 fulfills deployment case III.
- o Solution Enhanced MIPv4 fulfills deployment case I.
- o Solution MIPv4 with TSP fulfills deployment case I.
- o Solution Enhanced MIPv6 partly fulfills deployment case II. NAT traversal is not supported.
- o Solution MIPv6 with ISATAP fulfills deployment case II.
- o Solution MIPv6 with Teredo and 6to4 fulfills deployment case II.
- o Solution MIPv6 with STEP fulfills deployment case II.
- o Solution MIPv6 with TSP fulfills deployment case II.

For these solutions, we can list the following properties:

- o Solution Dual-stack MIPv4-MIPv6 generates two extra signaling messages at handoff but no additional handoff latency. It requires implementation of double mobility protocols including authentication and subscription management.
- o Solution Enhanced MIPv4 generates no additional handoff latency.
- o Solution MIPv4 with TSP generates at least 3 extra signaling roundtrips at handoff.
- o Solution Enhanced MIPv6 generates no additional handoff latency. If extended to support NAT traversal, this solution would generate additional overhead when NAT traversal would be in use. Also, this solution does not allow for route optimization.
- o Solution MIPv6 with ISATAP generates at least 1 extra signaling roundtrip at handoff.
- o Solution MIPv6 with Teredo and 6to4 generates at least 1 additional signaling roundtrips at handoff, and has a worst case scenario of 12 seconds plus one roundtrip during handoff.
- o Solution MIPv6 with STEP generates at least 1 extra signaling roundtrip at handoff.
- o Solution MIPv6 with TSP generates at least 3 extra signaling roundtrips at handoff.

In general, all the described solutions generate an additional 20 or 40 bytes transport overhead, depending on whether traffic is tunneled over IPv4 or IPv6 networks. The Teredo-based, STEP-based and TSP-based solutions, though, generate 28 bytes of transport overhead for NAT traversal (IPv4 header and UDP header).

From this, we draw the following conclusions:

Deployment case I is solved by "Enhanced MIPv4". This solution also adds minimal handoff latency and transport overhead, compared to native MIPv4. Deployment case I can also be solved by "MIPv4 with TSP".

Deployment case II can either be solved by standardizing extensions to Mobile IPv6, i.e. "Enhanced MIPv6" together with a solution for NAT traversal, or by Mobile IPv6 combined with transition mechanisms. In the latter case, there are three main solutions: "MIPv6 with ISATAP", "MIPv6 with Teredo and 6to4", "MIPv6 with STEP" or MIPv6 with TSP". The performance of these solutions largely depend on the deployment and performance of the different transition mechanisms.

The solution "Dual-stack MIPv4-MIPv6" requires twice the amount of implementation as solution "Enhanced MIPv4", while providing approximately the same performance in terms of handoff latency and transport overhead. This solution is, however, the only one supporting deployment case III.

8. Security Considerations

This document defines no new protocols for the internet, and has no direct security implications. Note however that there are a number of security implications in dealing with NAT traversal. In the case of Teredo [I-D.huitema-v6ops-teredo] and MIPv4 with NAT traversal [RFC3519], these security considerations are well described in the respective documents.

However, if it is decided to enhance MIPv6 with the extensions and mechanisms necessary to function in an IPv4 environment, the same care has to be taken with any NAT traversal mechanism for MIPv6.

9. IANA Considerations

This document does not require any new number assignments from IANA, and does not define any new numbering spaces to be administered by IANA.

RFC-Editor: Please remove this section before publication.

10. References

10.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

10.2 Informative References

[RFC2222] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3024] Montenegro, G., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[RFC3519] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, May 2003.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3904] Huitema, C., Austein, R., Satapati, S., and R. van der Pol, "Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks", RFC 3904, September 2004.

[I-D.ietf-ngtrans-moving]
Tsao, S., "Moving in a Dual Stack Internet", draft-ietf-ngtrans-moving-01 (work in progress), March 2002.

[I-D.tsirtsis-dsmip-problem]
Tsirtsis, G. and H. Soliman, "Mobility management for Dual stack mobile nodes A Problem Statement", draft-tsirtsis-dsmip-problem-03 (work in progress), October 2004.

[I-D.soliman-v4v6-mipv4]
Soliman, H. and G. Tsirtsis, "Dual Stack Mobile IPv6", draft-soliman-v4v6-mipv4-01 (work in progress), October 2004.

[I-D.tsirtsis-v4v6-mipv4]
Tsirtsis, G. and H. Soliman, "Dual Stack Mobile IPv4", draft-tsirtsis-v4v6-mipv4-00 (work in progress), August 2003.

[I-D.kahng-mobileip-moving6to4]
Kahng, H., "An interconnection mechanism of Mobile IPv6 using 6to4", draft-kahng-mobileip-moving6to4-00 (work in progress), September 2003.

[I-D.huitema-v6ops-teredo]
Huitema, C., "Teredo: Tunneling IPv6 over UDP through NATs", draft-huitema-v6ops-teredo-04 (work in progress), January 2005.

[I-D.ietf-ngtrans-isatap]
Templin, F., Gleeson, T., Talwar, M., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", draft-ietf-ngtrans-isatap-24 (work in progress), January 2005.

[I-D.savola-v6ops-conftun-setup]
Savola, P., "Simple IPv6-in-IPv4 Tunnel Establishment Procedure (STEP)", draft-savola-v6ops-conftun-setup-02 (work in progress), January 2004.

[I-D.blanchet-v6ops-tunnelbroker-tsp]
Parent, F. and M. Blanchet, "IPv6 Tunnel Broker with the Tunnel Setup Protocol(TSP)", draft-blanchet-v6ops-tunnelbroker-tsp-01 (work in progress), June 2004.

[I-D.ietf-v6ops-3gpp-analysis]
Wiljakka, J., "Analysis on IPv6 Transition in 3GPP Networks", draft-ietf-v6ops-3gpp-analysis-11 (work in progress), October 2004.

[I-D.satapati-v6ops-natpt-applicability]
Satapati, S., "NAT-PT Applicability", draft-satapati-v6ops-natpt-applicability-00 (work in progress), October 2003.

[I-D.thubert-nemo-ipv4-traversal]
Thubert, P., Molteni, M., and P. Wetterwald, "IPv4 traversal for MIPv6 based Mobile Routers", draft-thubert-nemo-ipv4-traversal-01 (work in progress), May 2003.

[I-D.tsao-mobileip-dualstack-model]
Tsao, S. and W. Boehm, "Mobility Support for IPv4 and IPv6 Interconnected Networks", draft-tsao-mobileip-dualstack-model-02.txt (work in progress), February 2000.

Authors' Addresses

Tony Larsson
Ericsson
Torshamnsgatan 23
SE-164 80 Stockholm
Sweden

Email: tony.larsson@ericsson.com

Eva Gustafsson
Ericsson
Torshamnsgatan 23
SE-164 80 Stockholm
Sweden

Email: eva.gustafsson@ericsson.com

Henrik Levkowetz
Ericsson
Torsgatan 71
Stockholm S-113 37
SWEDEN

Phone: +46 708 32 16 08
Email: henrik@levkowetz.com

Appendix A. Supported scenarios per solution

Table 5: This table indicates which of the network scenarios 1-12 are supported by each of the proposed solutions. Note that the solutions for deployment case II (MIPv6-based) are assumed to include mechanisms in the host to provide MIPv6 transport for IPv4 sockets (MIPv6x).

	DS MIP4 /6	Enh. MIP4 (xo)	MIP4x +TSP	Enh. MIP6 (xo)	MIP6x+ ISATAP	MIP6x+ Teredo +6to4	MIP6x +STEP	MIP6x +TSP
1	x	x	x					
2	x	x	x					
3	x			x	x	x	x	x
4	x			x	x	x	x	x
5	x	x	x					
6	x	x	x					
7	x			x	x	x	x	x
8	x			x	x	x	x	x
9	x	x	x					
10	x	x	x					
11					x	x	x	x
12					x	x	x	x

Table 6: This table indicates which of the handoff scenarios a-p and aa-ll are supported by each of the proposed solutions. Note that the solutions for deployment case II (MIPv6-based) are assumed to include mechanisms in the host to provide MIPv6 transport for IPv4 sockets (MIPv6x).

	DS MIP4 /6	Enh. MIP4 (xo)	MIP4x +TSP	Enh. MIP6 (xo)	MIP6x+ ISATAP	MIP6x+ Teredo +6to4	MIP6x +STEP	MIP6x +TSP
a	x	x	x					
b	x	x	x					
c	x	x	x					
d	x	x	x					
e	x	x	x					
f	x	x	x					
g	x	x	x					
h	x	x	x					
i	x			x	x	x	x	x
j	x			x	x	x	x	x
k	x			x	x	x	x	x
l	x			x	x	x	x	x
m	x			x	x	x	x	x
n	x			x	x	x	x	x
o	x			x	x	x	x	x
p	x			x	x	x	x	x
aa	x	x	x					
bb	x	x	x					
cc	x	x	x					
dd	x	x	x					
ee	x	x	x					
ff	x	x	x					
gg					x	x	x	x
hh					x	x	x	x
ii					x	x	x	x
jj					x	x	x	x
kk					x	x	x	x
ll					x	x	x	x

Appendix B. Transport overhead per solution

The following lists transport overhead for the different solutions, sorted after deployment cases.

Deployment case I (MIPv4-based).

- o Solution Enhanced MIPv4 adds 40 bytes transport overhead (IPv6 header), compared to native MIPv4.
- o Solution MIPv4 with TSP adds 40 bytes transport overhead (IPv6 header), compared to native MIPv4.

Deployment case II (MIPv6-based).

- o Solution Enhanced MIPv6 adds 20 bytes transport overhead (IPv4 header), compared to native MIPv6.
- o Solution MIPv6 with ISATAP adds 20 bytes transport overhead (IPv4 header) compared to native MIPv6, but only in the access network.
- o Solution MIPv6 with Teredo adds 28 bytes transport overhead (IPv4 header + UDP header) compared to native MIPv6.
- o Solution MIPv6 with 6to4 adds zero transport overhead, compared to native MIPv6.
- o Solution MIPv6 with STEP adds 20/28 bytes transport overhead (IPv4 or IPv4 + UDP header), compared to native MIPv6.
- o Solution MIPv6 with TSP adds 20/28 bytes transport overhead (IPv4 or IPv4 + UDP header), compared to native MIPv6.

Deployment case III (MIPv4-MIPv6).

- o Solution Dual-stack MIPv4-MIPv6 adds zero transport overhead, compared to native MIPv4 or native MIPv6, respectively.

Appendix C. Registration message roundtrips per solution

The following lists the number of registration message roundtrips for the different solutions, sorted after deployment cases.

Deployment case I (MIPv4-based).

- o Solution Enhanced MIPv4 adds zero roundtrips, compared to native MIPv4.
- o Solution MIPv4 with TSP adds at least 3 roundtrips, compared to native MIPv4.

Deployment case II (MIPv6-based).

- o Solution Enhanced MIPv6 adds zero roundtrips, compared to native MIPv6.
- o Solution MIPv6 with ISATAP adds at least 1 roundtrip, compared to native MIPv6.
- o Solution MIPv6 with Teredo and 6to4 adds at least 1 roundtrip in the Teredo case, compared to native MIPv6.
- o Solution MIPv6 with STEP adds at least 1 roundtrip, compared to native MIPv6.
- o Solution MIPv6 with TSP adds at least 3 roundtrips, compared to native MIPv6.

Deployment case III (MIPv4-MIPv6).

- o Solution Dual-stack MIPv4-MIPv6 adds zero roundtrips, compared to native MIPv4 or native MIPv6, respectively.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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