Mext Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 4, 2009

D. Oulai
S. Krishnan
Ericsson
H. Soliman
Elevate Technologies
March 3, 2009

DSMIPv6 Route Optimization
draft-oulai-mext-dsmip-ro-00.txt

Status of this Memo

Copyright Notice

Abstract

Dual Stack MIPv6 (DSMIP) is a MIPv6 extension to support IPv4 mobility for mobile hosts. While route optimization is well defined for IPv6 traffic, this feature is not defined for IPv4. However, Route Optimization has many advantages as reduced delays and lower load for the Home Agent. This document proposes solutions for the different scenarios where IPv4 route optimization is performed.

Table of Contents

1. Introduction

Dual Stack MIPv6 (DSMIP) is a MIPv6 extension to support IPv4 traffic for mobile hosts [I-D.ietf-mext-nemo-v4traversal]. DSMIP is relevant for situations where applications MUST be run using IPv4 or when the MN is located in an IPv4 only network. DSMIP introduces two new address options: the IPv4 Home Address and the IPv4 CareOf Address options. With those options, a MN can send and receive IPv4 traffic although all the mobility signaling is MIPv6 based. Therefore, there is no need to have a MIPv4 stack on the mobile.

On the other hand, route optimization (RO) is a process that allows a MN to communicate directly with a CN without transiting by an anchor, the Home Agent. There are several benefits from RO as shorter path delay, reduced bandwidth consumption and reduced load on the HA. However, RO is not defined for DSMIP. The problem statement of DSMIP RO can be found in [PS REFERENCE].

This document provides a solution for DSMIP RO. We study two scenarios:

1. MN with a v4HoA
   This scenario implies that the MN has also a v6HoA as all DSMIP signaling is based on the v6HoA. This scenario only considers v6CoA for the MN as the v4CoA case is tackled in the next scenario.

2. MN with a v4CoA only
   In this case, the MN is connected to an IPv4 only network. The scenario considers v6HoA and v4HoA.

We do not consider the situations where the MN has both v6CoA and v4CoA configured as [I-D.ietf-mext-nemo-v4traversal] clearly states that v6CoA SHOULD be preferred over the v4CoA. Moreover, we reuse as much as possible MIPv6 RO mechanisms and add extensions when needed.

2. Conventions used in this document

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 [RFC2119].

3. Terminology

All the general mobility-related terms used in this document are to be interpreted as defined in the Mobile IPv6 [RFC3775] and DSMIP [I-D.ietf-mext-nemo-v4traversal] base specifications.

RRP: Return Routability Procedure

v4CN: IPv4 address of the CN

v6CN: IPv6 address of the CN

v4CoA: IPv4 CareOf Address of the MN

v6CoA: IPv6 CareOf Address of the MN

v4HoA: IPv4 Home Address of the MN

v6HoA: IPv6 Home Address of the MN

v4HoA-map: IPv4 HoA mapped IPv6 address

4. Corresponding Node considerations

To support this specification, a CN MUST be dual-stacked to understand some of the new options introduced here. Note that this specification works also if the CN is in an IPv4 only network. Moreover, all CNs supporting this specification MUST listen the DSMIP UDP port to receive messages sent from v4CoAs as there could be NAT(s) between the MN and the CN. On the other hand, if the HoA type or the CoA type used by the MN differs from the type of address configured by the CN, v4v6 transition mechanisms MUST be used to transfer the packets. However, this is out of scope of this document.

5. Overview

To perform RO for DSMIP, we first need to guarantee that the v6HoA, v6CoA, v4HoA and v4CoA belong to the MN. MIPv6 RRP provides reachability test for the v6HoA and v6CoA only. Therefore, we define some steps for the IPv4 addresses reachability tests. As DSMIP mandates v6HoA for the MN, the v4HoA reachability test MUST also ensure that the v4HoA and v6HoA belong to the same MN. For this reason, the HoT message is encapsulated in a IPv4 header with v4HoA as destination address. If the MN receives the Home Keygen Token, it means that it is reachable by the v4HoA. Note that the v4HoA reachability test and the v6HoA are decoupled for security reasons, which means the CN has to send two different CoT messages for the reachability test. See Section 7.1.1.1 for more details.

The v4CoA reachability test is more complex. Note that this test is performed only if the MN has only a v4CoA because DSMIP specification states that v6CoA SHOULD be prefered over v4CoA. In this test, the CN MUST replace the v6CoA in the keygen token generation by a combination of the source address of the BU, the v4CoA and the UDP port as the MN can be in a private network. This is need to ensure that the generated CareOf Keygen is unique for communication with that mobile node. The CoT message is encapsulated in an IPv4 Header with v4CoA as destination address. See Section 7.2.1.2 for more details.

Another important aspect to perform DSMIP RO is the routing. The UDP encapsulation is used the same way as in [I-D.ietf-mext-nemo-v4traversal] for private addresses. As defining new IPv4 options is not recommended, we have three routing possibilities:

1. IPv6 tunnel
   The IPv4 packet is encapsulated as data in an IPv6 tunnel. The tunnel header is represented by the IPv6 header as in MIPv6 RO. The normal MIPv6 RO process is performed then the IPv4 packet is processed by the IPv4 module.

2. IPv4 mapped address
   This approach only modifies the address in the HoA option and the Type 2 Routing Header. The v6HoA is replaced with an IPv4 mapped IPv6 address. Therefore, MIPv6 RO process is performed and after address swapping and IPSec operations, the endpoint MUST be able to forward the packet to the upper layer considering the IPv4 HoA.

3. IPv4 tunnel
   This is use when the MN only has an v4CoA and IPv6 routing is not

possible. Therefore, we perform an IP in IP tunnelling with the v4CoA as destination address for the outer header. Note that IPv4-UDP encapsulation is performed when NAT is detected.

A new option, IPv4 Route Optimization mode option, is defined in order to negotiate the routing mode (See Section 6.2). This option is included in the CoTI/CoT messages. If the CN responds with a different mode than the one requested by the MN, the MN MUST use the mode advertised by the CN or stop RO process.

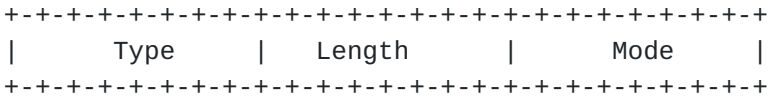
6. Extensions to DSMIP

6.1. Data structures

IPv4 HoA, IPv4 CoA and IPv4 RO mode fields MUST be added to the CN BCE as described in [RFC3775]. IPv4 RO mode and v4CN field MUST be added to the BULE as described in [RFC3775].

6.2. IPv4 Route Optimization mode option

This option is created to negotiate the IPv4 RO mode.



Type - TBD

Length - 3

Mode - 0 : All modes supported
1 : IPv6 encapsulation
2 : IPv4 mapped IPv6 addresses
3 : IPv4 encapsulation
4 : IPv4-UDP encapsulation

IPv4 Route Optimization mode Option

6.3. Route Optimization mode negotiation

The MN MUST include an IPv4 RO mode option in the CoTI message. The choice of the IPv4 RO mode included in the CoTI message can be driven by policies and is out of the scope of this specification. If the CN detects NAT(s) presence, it MUST respond in the CoT message with value 4 (IPv4-UDP) as RO mode. If the CN supports the mode requested by the MN and there is no NAT(s) in between, the CN SHOULD acknowledge the mode chosen by the MN. If the CN responds with a different mode, the MN MUST use the RO mode chosen by the CN. Otherwise, if the CN indicates 0 (All modes supported), the MN uses the mode initially selected in the CoTI message.

6.4. Keygen tokens generation

This section describes the Home and CareOf Keygen generation when v4HoA or v4CoA is involved in the RRP. The token generation process MUST include the IPv4 addresses as the CN is stateless during the RRP.

6.4.1. Home keygen token generation

The CN uses the same formula as used in [RFC3775], which is:

home keygen token :=
First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0)))

In case a v4HoA is involved, the home address is replaced by a combined home address described below:

Combined HoA:= (v6HoA | v4HoA)

6.4.2. CareOf keygen token generation

In case the MN is using a v4CoA, the CareOf keygen token generation is more complex as there could be NAT(s) between the MN and the CN. As the MN could be in a private network, the CoA value used for calculation MUST be unique. The CN uses the same formula as used in [RFC3775], which is:

careOf keygen token :=
First (64, HMAC_SHA1 (Kcn, (careOf address | nonce | 1)))

In case a v4CoA is involved, the careOf address is replaced by a combined careOf address described below:

Combined CoA:=
(v4CoA | Source UDP port | Source IPv4 address of the CoTI message)

This insures that the value used for careOf token calculation is unique even if there are NATs in between.

7. Protocol operation

In this document, we assume that MN and CN are dual stacked. The solutions proposed depend of the addresses configured on the MN and the CN. We assume that the MN knows at which address to reach the CN by using DNS for example.

7.1. Mobile Node with IPv4 Home address

If the MN has v6CoA and v4CoA configured at the same time, [I-D.ietf-mext-nemo-v4traversal] suggests to use the v6CoA. The case where the MN is configured with v4CoA only is tackled in Section 7.2.

7.1.1. Return Routability procedure

The RRP procedure is presented in Figure 1.

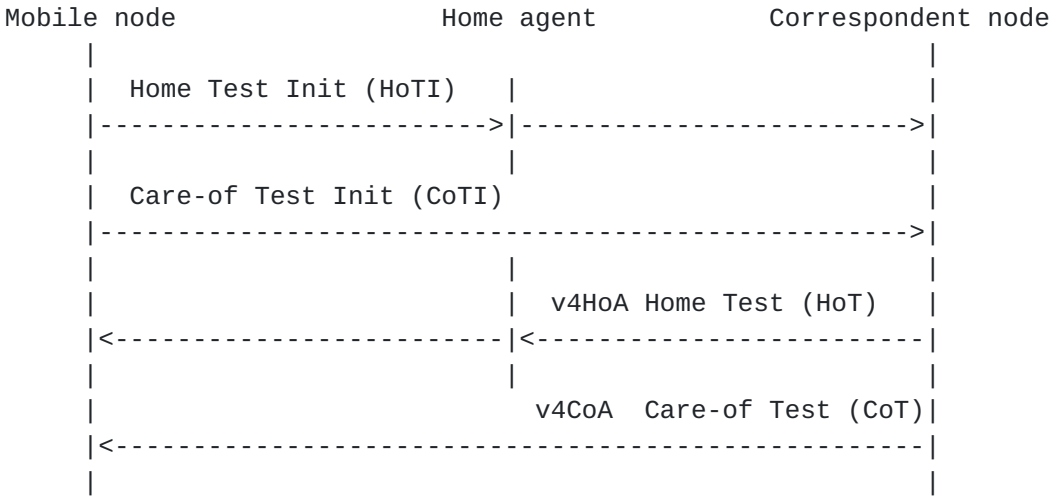


Figure 1: Return Routability procedure for v4HoA and v4CoA

7.1.1.1. Home address reachability test

The MN includes a v4HoA option in the HoTI. If a CN receives a HoTI message without any HoA option, it MUST process it as a request for v6HoA reachability test. In this case, the Home keygen token and the HoT message are generated as described in [RFC3775]. If the HoTI message contains a v4HoA option only, the CN MUST process the message as a v4HoA reachability test. After generating the Home Keygen token based on the v6HoA and the v4HoA, the CN responds with a HoT message.

If a v4HoA reachability test is, the CN MUST encapsulate the HOT

message in an IPv4 header. The HoT message is descried below:

```
External header:
   Src = v4CN
   Dest = v4HoA
Internal header:
   Src = v6CN
   Dest = v6HoA
HoT message
   IPv4 HoA Option = v4HoA
   Other options
```

HoT message for v4HoA reachability test

The MN MUST set the Hop Limit to 1 for the inner IPv6 header. Therefore, the IPv4 tunnel endpoint MUST be also the destination for the HoT message. If the MN receives the HoT message at v4HoA address, it will internally transfer the packet to its IPv6 process as there is an v6inv4 encapsulation. The MN will also noticed that he is the IPv6 endpoint of the HoT message and will process it. If the MN is not the IPv6 endpoint, the HoT message will be dropped because either there is no way of forwarding IPv6 packets or either the MN will decrement the Hop limit to 0. By this way, we can simply check that v4HoA and v6HoA belong to the same MN.

7.1.1.2. CareOf address reachability test

The MN includes a v4HoA option and an IPv4 RO mode option in the CoTI message and the CN responds with a CoT message after generating the CareOf Keygen token based on the v6CoA. Moreover, tokens and Kbm generation are based on the v6CoA address. See Section 6.3 and Section 6.4 for details.

7.1.2. Binding registration

When the Kbm is created, the MN sends a BU to the CN. If the BU is sent to trigger RO for traffic using v6HoA only, the BU is constructed as defined in [RFC3775]. In the case the MN requires v4HoA RO only, it includes the v4HoA option and the parameter built based on the Kbm generated for the v4HoA. If v6HoA and v4HoA RO are required, the MN MUST include both HoA options and both parameters. The MN also inserts an IPv4 Route Optimization mode option containing the value chosen after the CoTI/CoT messages exchange. See Section 6.3. The BU MUST not be encapsulated as IPv6 connectivity exists between MN and CN.
When receiving the BU message, the CN recomputes the Home and CareOf Keygens then the binding management key. Note that distinct BCE will be created for v4HoA and v6HoA. Then, the CN MUST send a BAck. The

CN MUST also include the IPv4 RO mode option in the BAck. Not receiving this option in the BAck means that the CN does not support IPv4 RO.

7.1.3. Packet processing

With IPv6 based routing, two options are possible:

1. Normal MIPv6 RO with encapsulated IPv4 packets
   In this case, the MN and the CN process the packet as in the MIPv6 RO using HoA option and Type 2 Routing Header in the IPv6 external header. The IPv6 header encapsulates an IPv4 packet. When leaving the MN, the addresses are:

```
External header:
   Src = v6CoA
   Dest = v6CN
   HoA option = v6HoA
Internal header:
   Src = v4HoA
   Dest = v4CN
```

   After receiving this packet, the CN performs regular MIPv6 RO process before decapsulating and processing the IPv4 packet. For security reasons, when detecting that there is an IPv4 packet encapsulated in a IPv6 packet that passes the RO process, the MN MUST check if the IPv4 source and destination addresses correspond respectively to the v4HoA and v4CN addresses registered in the related BCE. If not, the packet MUST be discarded. When leaving the CN, the addresses are:

```
External header:
   Src = v6CN
   Dest = v6CoA
   Type 2 Routing Header = v6HoA
Internal header:
   Src = v4CN
   Dest = v4HoA
```

   When receiving this packet, the MN performs regular MIPv6 RO process before decapsulating and processing the IPv4 packet. For security reasons, when detecting that there is an IPv4 packet encapsulated in a IPv6 packet that passes the RO process, the MN MUST check if the IPv4 source and destination addresses correspond respectively to the v4CN and v4HoA addresses registered in the related BCE. If not, the packet MUST be discarded.

2. Normal MIPv6 RO with IPv4 mapped IPv6 addresses
This solution assumes that MN and CN understand IPv4 mapped addresses. An IPv4 mapped address, labeled v4HoA-map address, is formed with the v4HoA. When sending a packet, the MN configures the addresses as below:

IPv6 header:
Src = v6CoA
Dest = v6CN
HoA option = v4HoA-map

After receiving this packet, the CN performs regular MIPv6 RO process. Then, the CN detects the v4HoA-map and forwards the packet to the next layer considering v4HoA as source address. When leaving the CN, the addresses are:

IPv6 header:
Src = v6CN
Dest = v6CoA
Type 2 Routing Header = v4HoA-map

After performing regular MIPv6 RO process, the MN forwards the packet to the next layer considering IPv4 addresses.

7.2. Mobile Node with IPv4 CareOf address only

7.2.1. Return Routability procedure

In this case, it is impossible to use directly the MIPv6 RO process as there is no v6CoA.

7.2.1.1. Home address reachability test

If a v4HoA is configured, the MN SHOULD perform Home address reachability test in the RRP the same way as described in Section 7.1.1.1. Otherwise, process described in [RFC3775] is applied.

7.2.1.2. CareOf address reachability test

For the v4CoA reachability test, the MN sends a CoTI message described below:

```
External header:
   Src = v4CoA
   Dest = v4CN
UDP header
Internal header:
   Src = v6HoA
   Dest = v6CN
CoTI message
   IPv4 CoA Option = v4CoA
   IPv4 RO mode option = 3 or 4
```

The CoTI message MUST include an IPv4 CoA option and be UDP encapsulated as described in [I-D.ietf-mext-nemo-v4traversal]. An IPv4 RO mode option MUST be present with a value equal to 3 (IPv4 encapsulation) or 4 (IPv4-UDP encapsulation). After receiving the CoTI message, due to the presence of an IPv4 CoA option, the CN understand that this is a v4CoA reachability test. The CN calculates the CoA Keygen Token as described in Section 6.4.2. Then, the CN generates a CoT message and send it encapsulated to the MN. The format of the CoT message is described below:

```
External header:
   Src = v4CN
   Dest = v4CoA
UDP header (optional)
Internal header:
   Src = v6CN
   Dest = v6HoA
CoT message
   IPv4 CoA Option = v4CoA
   IPv4 RO mode option = 0 or 3 or 4
```

For security reason, the Hop limit of the IPv6 header MUST be set to 1. Therefore, v4CoA and v6HoA MUST belong to the MN. After receiving the tokens, the MN is able to generate the Kbm.

7.2.2. Binding registration

The procedure here is the same as the one described in Section 7.1.2 except that the BU and BA messages MUST be encapsulated using the chosen RO mode.

7.2.3. Packet processing

In this scenario, we can not use HoA option or Type 2 Routing header as they are not defined for IPv4. Also, source routing is not a good approach as many firewalls will block packets with source routing option. Moreover, defining new options for IPv4 is not recommended

as IPv4 is already widespread. The approach chosen here is to use an IP-in-IP encapsulation. When leaving the MN, the addresses are:

```
External header:
   Src = v4CoA
   Dest = v4CN
Internal header:
   Src = v4HoA
   Dest = v4CN
```

For security reasons, the CN MUST check if the sources of the outer and inner header match in a BCE. If not, the packet MUST be discarded. When leaving the CN, the addresses are:

```
External header:
   Src = v4CN
   Dest = v4CoA
Internal header:
   Src = v4CN
   Dest = v4HoA
```

For security reasons, the MN MUST check if the destination of the outer and inner header match in a BULE. If not, the packet MUST be discarded.

7.2.4. NAT keepalives

When a CN detects NAT(s) in the path, it MUST include a NAT detection option in the CoTI message and the NAT keepalives are performed using the BU and BA messages as described in [I-D.ietf-mext-nemo-v4traversal].

8. Security Considerations

There are no new messages added here and all messages exchanges are secured using the same mechanisms described in [I-D.ietf-mext-nemo-v4traversal] and [RFC3775]. This specification requires to perform IPv4 HoA and CoA reachability tests. For this purpose, the v4HoA and v4CoA are included in the token generation process.

9. IANA Considerations

This specification requires a type for the IPv4 RO mode option included in the mobility header.

10. Normative References

[I-D.ietf-mext-nemo-v4traversal]
Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", draft-ietf-mext-nemo-v4traversal-09 (work in progress), February 2009.

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

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

[RFC4449] Perkins, C., "Securing Mobile IPv6 Route Optimization Using a Static Shared Key", RFC 4449, June 2006.

[RFC4866] Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC 4866, May 2007.

Authors' Addresses

Desire Oulai
Ericsson
8400 Blvd Decarie
Town of Mount Royal, Quebec
Canada

Email: desire.oulai@ericsson.com

Suresh Krishnan
Ericsson
8400 Blvd Decarie
Town of Mount Royal, Quebec
Canada

Email: Suresh.Krishnan@ericsson.com

Hesham Soliman
Elevate Technologies

Email: hesham@elevatemobile.com