Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 10, 2008

G. Bajko
Nokia
H. Tschofenig
Nokia Siemens Networks
July 9, 2007

Firewall friendly Return-Routability Test (RTT) for Mobile IPv6
draft-bajko-mip6-rrtfw-02.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a slightly modified Return Routability Test (RRT) for MIPv6. The herein defined RRT mechanism is intended for CoA exchanges between the MN and the CN. Once the MN and CN find out their peers' valid addresses, an additional mechanism will be used to run connectivity checks to figure out which of the address pairs have connectivity and, if needed, open the required pinholes in the firewalls. The defined mechanism is intended to work with current

firewalls without requiring any support from them. The document also addresses the use of UDP encapsulation to facilitate MIPv6 signaling between involved nodes.

Table of Contents

1. Introduction

Most of today's IP networks are protected by state full firewalls which filter the traffic based on the five tuple (sourceIP, destIP, sourcePort, destPort). This filtering could be supplied to incoming traffic or both incoming and outcoming. The problems which occure when using MIPv6 in firewall protected networks are described in detail in [RFC4487].

Most of the MIPv6 signalling is, as defined in [RFC3775], is secured by IPSec ESP, and most of today's firewalls will drop ESP packets, as there are no default rules defined for this traffic. So the mobile node is not able to successfully complete the registration of it's CoA in the new network and will not be able to communicate with other nodes.

If the the Binding Update (BU) with the home agent (HA) is finished, and the mobile node wants to use route optimization, it will start the Return Routability Procedure (RRT). For this it will send a HoTI and a CoTI message to the corresponend node (CN). The HoTI will be send over the HA to the CN and the CoTI message directly to the CN. Normally the HoTI and the corresponet HoT message will go through, but the CoTI or CoT message will mostly be dropped. So no route optimization is available and all the traffic need to go over the HA.

This document will provide a solution that the MIPv6 signalling will successfully complete. First a new return routability procedure will be shown and then a was to encapsulate messages in UDP to traverse the firewalls.

2. Terminology

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 [RFC2119].

This document uses the following abbreviations:

- CN: Correspondent Node
- CoA: Care of Address
- CoT: Care-of Test
- CoT-ICE: Care-of Test ICE
- CoTI: Care-of Test Init
- CoTI-ICE: Care-of Test Init ICE
- HA: Home Agent

- HoA: Home Address
- HoT Home Test
- HoTI: Home Test Init
- ICE: Interactive Connectivity Establishment
- MN: Mobile Node
- RO: Route Optimization
- RRT: Return Routability Test

3. New Return Routability Procedure

Current firewalls typically create state and filter data traffic based on the five tuple (sourceIP, destIP, Prot, sourcePort, destPort). Filtering may be applied either to only incoming traffic or both incoming and outgoing traffic.

MIP6 [RFC3775] faces a number of problems when used in an environment with firewalls:

- (a) Mobile IP recommends the use of IPsec ESP to protect packets between the MN and its home agent, while today's firewalls, as a default rule, drop ESP packets, thus preventing the use of MIP6. It is possible to configure static pinholes in the firewalls to allow ESP and IKE messages between MN and HA to pass through.[I-D.krishnan-mip6-firewall] describes best current practices on how to configure firewalls to enable MIPv6. Alternatively, UDP encapsulation might be used.
- (b) current firewalls filter on udp and tcp protocol, thus when a firewall is protecting the CN, that firewall might not allow a

HoTI to pass, as that is sent using MH protocol [RFC3775]. If the policy in the firewall would allow wildcard for the protocol instead of filtering on udp or tcp, this problem would be solved as well. Note: here it is assumed that when a HoTI is generated by the MN (i.e. start of route optimisation), then there is already a data connection between the MN and the CN through the HA.

- (c) similar to the above, when a firewall protecting the MN sees a CoTI message, it would need to install state to allow the corresponding CoT to pass and reach the MN. Firewalls that do not support MH and modifying the firewall policy is not acceptable for the administrator, UDP encapsulation might need to be used. This is addressed in section 5.
- (d) a firewall protecting the CN will not allow a CoTI to pass, as that is sent from an untrusted address.
- (e) when both the HA and the MN and/or CN are behind firewalls, then a combination of UDP encapsulation and the modified RRT mechanism defined in this document might need to be used to enable MIPv6 operation.

As a summary, while some of the mobile IPv6 signaling could be enabled using static configurations in the firewalls, there is no way to ensure the same for the signaling and data traffic on the direct path between the MN and the CN.

Without applying route optimization, the MN and the CN would be forced to communicate through their home agents, and that, based on their topological location, could result in increased latency and cost. Such additional delays might not be tolerated by interactive applications sensitive to delays.

In order to ensure a successful deployment of IPv6 and mobile IPv6 in current IP networks, it is important to have mechanisms and guidelines in place which help the smooth operation of the protocol in an environment with firewalls.

4. UDP Encapsulation

This section addresses scenarios a), b) and c) from Section 1.

4.1. Problem Description

When the MN or the HA or both are behind firewalls that block IPsec ESP, then the Binding Update to the Home Agent will fail. To overcome this situation, firewall administrators may configure static pinholes in the firewalls, as described in [I-D.krishnan-mip6-firewall]. When that is not feasible, as an alternative, the MN may use UDP encapsulation to wrap its MIPv6 messages destined to the HA into a UDP/IP header. As the MN can not influence or change the firewall behavior, it has to determine whether there are any firewalls blocking ESP between itself and the HA or not. When there are, it will need to use UDP encapsulation.

Additionally, when the MN or the CN or both are behind firewalls that do not allow packets with MH protocol to pass, the MN, or the CN or both may need to use UDP encapsulation to wrap their MIPv6 messages into a duplicate UDP/IP header. Same applies when the firewall allows MH packets to pass in the in-->out direction but does not install state to allow the corresponding response in the out-->in direction.

4.2. UDP Encapsulation Procedures

4.2.1. Procedures at the MN

When the MN detects that there is a firewall between itself and the HA, it SHOULD start using UDP encapsulation to wrap its MIPv6

signaling messages destined to the HA into new UDP/IP header. When using UDP encapsulation, the MN MUST use UDP port 500.

[Editor's Note: If there is a NAT between the mobile node and the home agent then IKEv2 will enable UDP encapsulation for subsequent traffic. For firewalls this UDP encapsulation can either be provided by IKEv2 or as part of the mobile IP stack. For the usage with RFC 4285 mobile IP has to enable this UDP encapsulation procedure since IKEv2 is not used in this case.]

The MN can detect that there is a firewall on the path by either using an external mechanism like STUN [6] or by simply assuming that if the Binding Update to its HA fails, then that is probably the case.

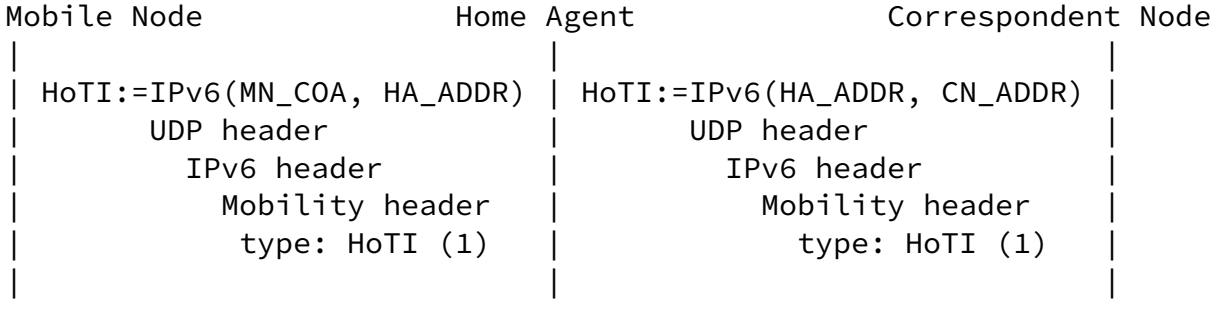
When the MN receives a packet on UDP port 500 from its HA, it MUST inspect the first 8 bytes of the UDP payload. If those are set to zero then the MN received a UDP encapsulated MH packet and it MUST remove the UDP/IP header and process the inner packet as a MH packet.

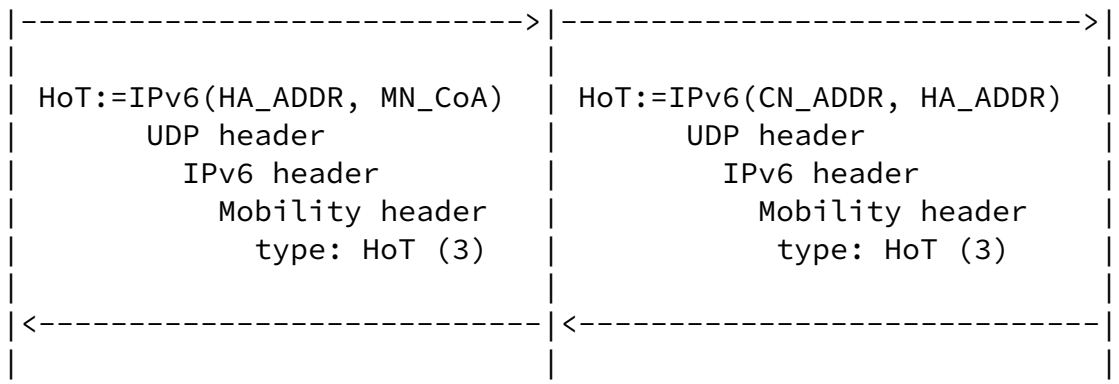
4.2.2. Procedures at the HA

When the HA receives a packet on UDP port 500, it MUST inspect the first 8 bytes of the UDP payload. If those are set to zero then the HA received a UDP encapsulated MH packet and it MUST remove the UDP/IP header and process the inner packet as a MH packet.

The HA MUST also use UDP encapsulation with port 500 when sending a response to a UDP encapsulated MH packet to the MN.

When the HA receives a UDP encapsulated packet containing a HoTI or a HoT or a CoTI-ICE (defined in this document) or a CoT-ICE (defined in this document) MH packet, it MUST decapsulate and re-encapsulate it using UDP port 500 before sending it to the MN or CN, respectively:





4.2.3. UDP encapsulated HoTI/HoT RRT messages

The CoTI-ICE/CoT-ICE messages are treated similarly, only the MH type will have a different value (22 and 23 respectively)

4.2.3.1. Procedures at the CN

When the CN receives a packet on UDP port 500, it MUST inspect the first 8 bytes of the UDP payload. If those are set to zero then the CN received a UDP encapsulated MH packet and it MUST remove the UDP/IP header and process the inner packet as a MH packet.

When the CN receives a UDP encapsulated MH message, it MUST send the response using UDP encapsulation.

5. Enabling Route Optimization Through Firewalls

Route optimization can be enabled by either using dedicated signaling to instruct the firewall to create a pinhole, or using a mechanism which would make the firewall to install pinholes as part of its normal operation. This draft addresses the latter solution.

5.1. Problem Description

This section describes in more details scenario d) from Section 1.

The Return Routability Test defined in [RFC4487] enables the correspondent node to obtain some reasonable assurance that the

mobile node is in fact addressable at its claimed care-of address as

well as at its home address, while keygen tokens are exchanged and combined into a binding management key. In order to enable route optimizations through firewalls, both HoTI and CoTI messages (and the corresponding HoT and CoT) need to successfully pass through. It is assumed that at the time when the MN initiates a route optimization procedure towards the CN, there is already some sort of data communication between the MN and the CN. If the CN is behind firewall and that firewall does have a rule to allow packets from the HoA of the MN to the address of the CN, then there is a good chance that HoTI would also make it through the firewall.

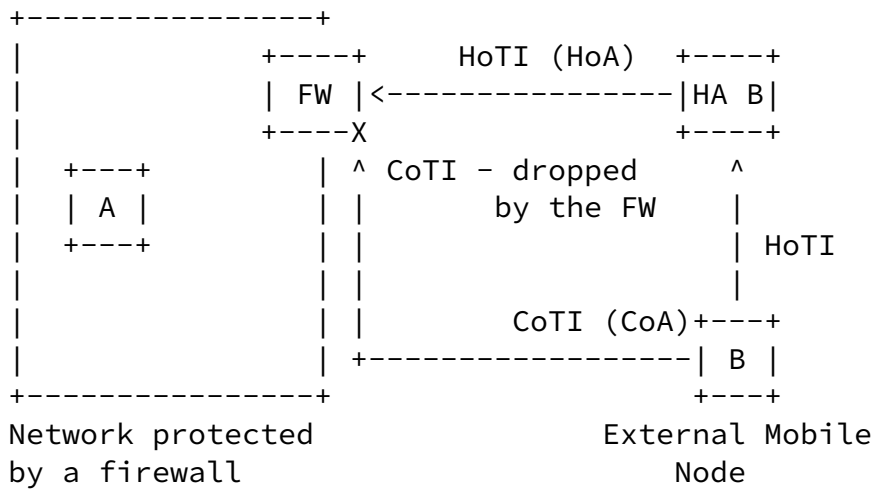
If such a rule does not exist in the firewall protecting the CN, then HoTI will be dropped and the return routability test will fail.

Once HoTI is sent out and a HoT response is received, the MN will send a CoTI message from its current CoA. If there is a firewall protecting the CN, that firewall will drop the CoTI message as it is coming from an untrusted source.

In order to illustrate the problem, let's assume a communication between an inner node A (protected by the firewall), and an external mobile node B. It is assumed that the firewall protecting the CN (node A) is configured in such a way that it allows traffic from the node B's HoA to bypass, therefore MH packets like HoTI are not filtered.

As specified in Mobile IP [RFC3775], the transport and higher layers should use the Home IP address and HoA of node B, and not the local IP address that node B might get while roaming in order to support mobility. The state created in the firewall protecting node A is therefore initially based on the IP address of node A, and the home address of the node B, HoA of node B. If the mobile node B is in its home network, the packets are directly exchanged between the nodes A and B. If the mobile node B is roaming, the session can be maintained thanks to the Home Agent of node B and the reverse tunneling mechanism [RFC3775]. Packets forwarded by the Home Agent to node A will have the source IP address indicating the Home IP address of node B and the destination IP address indicating the IP address of node A. Such packets can thus pass the packet filter inspection in the firewall protecting node A. However, nodes A and B might be located topologically closely together while node B's Home Agent may be far away, resulting in a 'trombone effect' that can create delay and degrade the performance. The Mobile IP specifications have defined the route optimization procedure [RFC3775] in order to solve this issue. The mobile node should first execute a Return Routability Test: the Mobile Node B should send a Home Test Init message (HoTI) via its Home Agent and a Care of Test Init (CoTI)

message directly to its correspondent node A as illustrated in the figure below [RFC4487]:

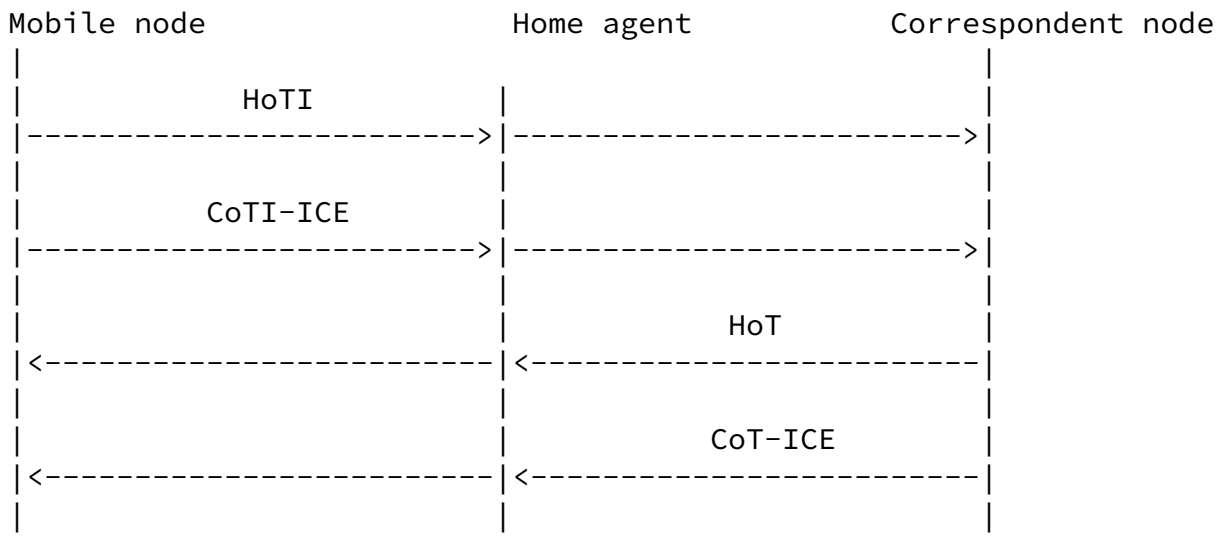


The Care of Test Init message is sent from the new CoA. However, this packet will not match any entry in the packet filter in the firewall and the CoTI message will be dropped. As a consequence, the RRT cannot be completed and Route optimization cannot be applied due to the presence of a firewall.

The above scenario is one from the problem statements described in [RFC4487].

5.2. New RTT Proposal

This document proposes a modified RRT for MIPv6 nodes behind firewalls. In the new RRT mechanism the original HoTI and HoT remain unchanged, while the new CoTI (called CoTI-ICE) and CoT (called CoT-ICE) messages will be routed through the HA in a similar way as HoTI and HoT. While the token exchange for binding management key generation purposes from the original RRT is preserved, the new RRT mechanism will be used to exchange the valid addresses the MN and CN possess. Once the addresses - called candidate addresses - are exchanged, both the MN and CN will run connectivity checks as described in [I-D.tschofenig-mip6-ice] in order to enable and to check the connectivity for the addresses. When a working address pair is found, the MN will send a BU from that CoA to the CN's address.



The new RRT mechanism will not test the connectivity on the direct path between the MN and CN. As that is still needed before the nodes engage in data exchange, a new mechanism, described in [I-D.tschofenig-mip6-ice] is used for this purpose.

5.3. Modified RRT Procedures

5.3.1. Modified RRT Procedures at the MN

The MN following the new RRT procedure defined in this draft MUST NOT send a CoTI, as defined in [RFC3775], to the CN. Instead it MUST generate a CoTI-ICE, as defined in this document. The MN MUST gather its addresses from all its interfaces as described in [I-D.tschofenig-mip6-ice]. The MN MUST form candidate-addresses as described in [I-D.tschofenig-mip6-ice]. The MN MUST put all of its candidate-addresses into a MIP-ICE mobility options defined in [I-D.tschofenig-mip6-ice] and MUST attach it to the CoTI-ICE message.

5.3.2. Modified RRT procedures at the CN

The CN supporting the new RRT procedure defined in this document, upon receiving a CoTI-ICE message MUST NOT send a CoT response, as defined in [RFC3775]. The CN upon receipt of a CoTI-ICE message MUST gather its addresses from all its interfaces as described in

[I-D.tschofenig-mip6-ice]. The CN MUST form candidate-addresses as described in [I-D.tschofenig-mip6-ice]. The CN MUST put all of its candidate-addresses into a MIP-ICE mobility options defined in [I-D.tschofenig-mip6-ice] and MUST attach it to the CoT-ICE message.

5.3.3. HA processing of CoTI-ICE and CoT-ICE

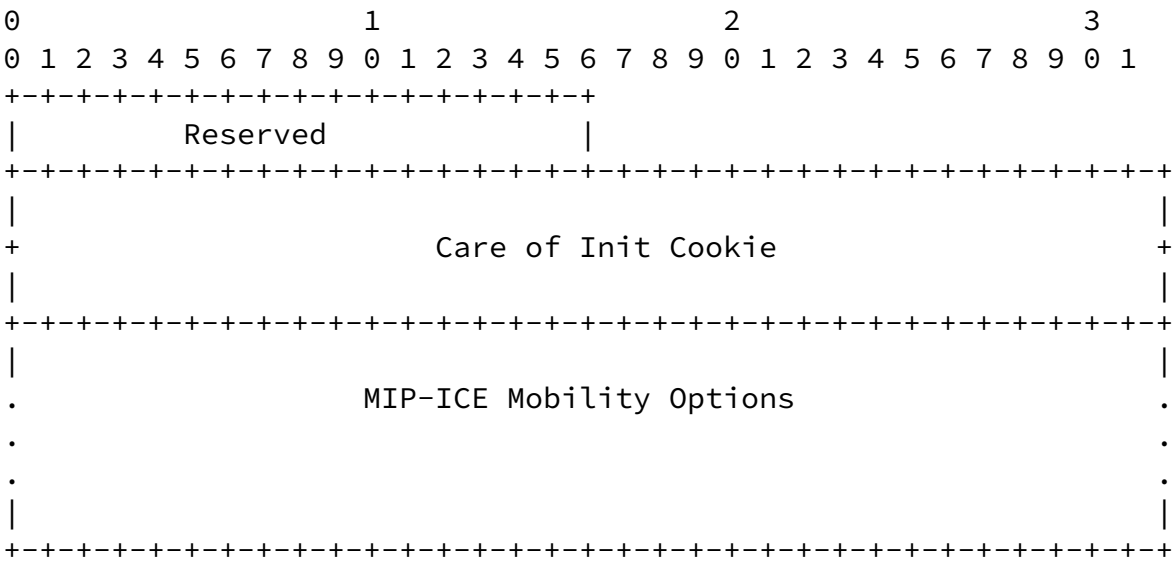
Both CoTI-ICE and CoT-ICE messages MUST be processed by the HA as any other Mobility Header message, as described in [RFC3775].

6. New Mobility Header Types

6.1. CoTI-ICE Message

A mobile node uses the CoTI-ICE message to finalize the return routability procedure and request a care-of keygen token from a correspondent. The CoTI-ICE message uses the MH Type value 22 (to be registered with IANA). A CoTI-FW message MUST include a mobility options carrying the candidate addresses of the MN sending it.

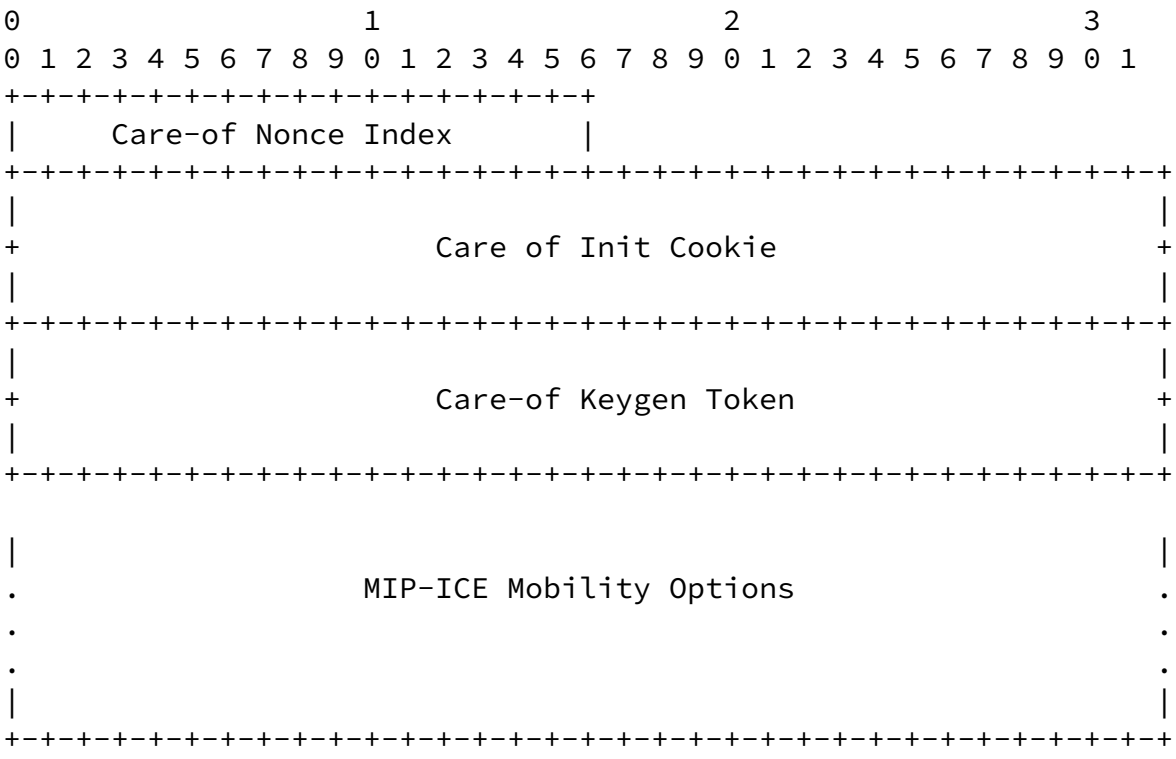
When value 22 is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Care of Init Cookie: as defined in RFC 3775
MIP-ICE Mobility Options: as defined in [I-D.tschofenig-mip6-ice]

6.2. CoT-ICE Message

The Care-of Test ICE (CoT-ICE) message is a response to the Care-of Test Init ICE (CoTI-ICE) message, and is sent from the correspondent node to the mobile node. The Care-of Test ICE message uses the MH Type value 23 (to be registered with IANA). When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



Care of Init Cookie: as defined in RFC 3775
Care-of Keygen Token: as defined in RFC 3775
MIP-ICE Mobility Options: as defined in [I-D.tschofenig-mip6-ice]

7. IANA Considerations

This specification registers new MH type values:

CoTI-ICE message uses MH type value 22.

CoT-ICE message uses MH type value 23.

8. Security Considerations

The security threats described in [I-D.tschofenig-mip6-ice] are inherited in addition to the existing ones mentioned in [RFC3775].

[Editor's Note: More work is needed on the security consideration section particularly since the security properties of the return routability check might be changed.]

9. Acknowledgments

We would like to thank Thomas Schreck for his contributions to this document.

10. References

10.1. Normative References

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

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

[I-D.tschofenig-mip6-ice] Tschofenig, H. and G. Bajko, "Mobile IP Interactive Connectivity Establishment (M-ICE)", draft-tschofenig-mip6-ice-00 (work in progress), June 2007.

10.2. Informative References

[RFC4487] Le, F., Faccin, S., Patil, B., and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem Statement", RFC 4487, May 2006.

[I-D.krishnan-mip6-firewall] Krishnan, S., "Firewall Recommendations for MIPv6", draft-krishnan-mip6-firewall-00 (work in progress), July 2007.

Authors' Addresses

Gabor Bajko
Nokia

Hannes Tschofenig
Nokia Siemens Networks
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.com

Full Copyright Statement

THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).