Mobile IPv6
Internet Draft
Document: draft-ietf-mip6-ha-switch-03.txt
Intended status: Standards Track
Expires: September, 2007

B. Haley
Hewlett-Packard
V. Devarapalli
Azaire Networks
H. Deng
Hitachi
J. Kempf
DoCoMo USA Labs
March 2007

Mobility Header Home Agent Switch Message
draft-ietf-mip6-ha-switch-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

Abstract

This document specifies a new Mobility Header message type that can be used between a home agent and mobile node to signal a mobile node that it should acquire a new home agent.

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 RFC-2119 [1].

Table of Contents

1. Introduction....2
2. Scenarios....2
2.1 Overloaded....3
2.2 Load Balancing....3
2.3 Maintenance....3
2.4 Functional Load Balancing....3
2.5 Home Agent Renumbering....3
3. Home Agent Switch Message....4
4. Home Agent Operation....6
4.1 Sending Home Agent Switch Messages....6
4.2 Retransmissions....7
4.3 Mobile Node Errors....7
5. Mobile Node Operation....8
5.1 Receiving Home Agent Switch Messages....8
5.2 Selecting a Home Agent....8
6. Operational Considerations....9
7. Procotol Constants....9
8. IANA Considerations....9
9. Security Considerations....9
10. References....10
10.1 Normative References....10
10.2 Informative references....10
Acknowledgments....10
Author's Addresses....11

1. Introduction

RFC 3775 [2] contains no provision to allow a home agent to inform a mobile node that it needs to stop acting as the home agent for the mobile node. For example, a home agent may wish to handoff some of its mobile nodes to another home agent because it has become overloaded or it is going offline.

This protocol describes a signaling message type that can be used to send a handoff notification between a home agent and mobile node.

2. Scenarios

Here are some example scenarios where a home agent signaling message would be useful.

2.1 Overloaded

There are a number of reasons a home agent might be considered overloaded. One might be that it is at, or near, its limit on the number of home bindings it is willing to accept. Another is that it has reached a pre-determined level of system resource usage - memory, cpu cycles, etc. In either case, it would be desirable for a home agent to reduce the number of home bindings before a failure occurs.

2.2 Load Balancing

A home agent might know of other home agents that are not as heavily loaded as itself, learned through some other mechanism outside the scope of this document. An operator may wish to try and balance this load so a failure disrupts a smaller percentage of mobile nodes.

2.3 Maintenance

Most operators do periodic maintenance in order to maintain reliability. If a home agent is being shutdown for maintenance, it would be desirable to inform mobile nodes so they do not lose mobility service.

2.4 Functional Load Balancing

A Mobile IPv6 home agent provides mobile nodes with two basic services - a rendezvous server where correspondent nodes can find the current care-of address for the mobile node, and as an overlay router to tunnel traffic to/from the mobile node at its current care-of address.

A mobility service provider could have two sets of home agents to handle the two functions. The rendezvous function could be handled by a machine specialized for high-speed transaction processing, while the overlay router function could be handled by a machine with high data throughput.

A mobile node would start on the rendezvous server home agent and stay there if it does route optimization. However, if the original home agent detects that the mobile node is not doing route optimization, but instead reverse-tunneling traffic, it could redirect the mobile node to a home agent with better data throughput.

2.5 Home Agent Renumbering

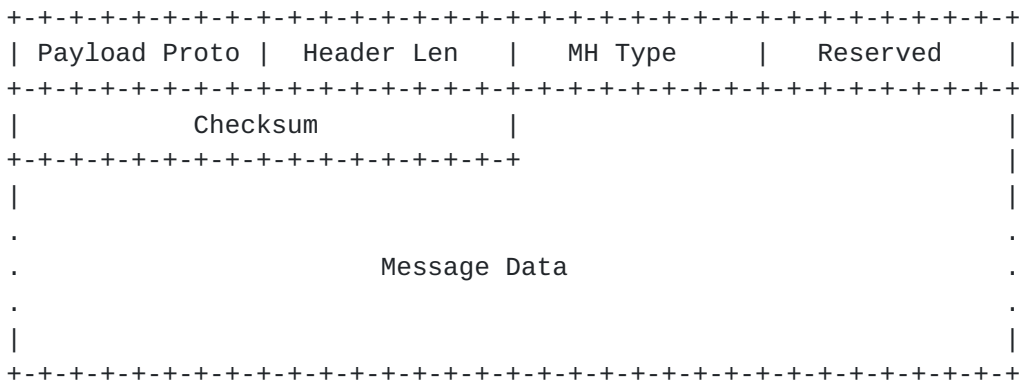
Periodically, a mobility service provider may want to shut-down home agent services at a set of IPv6 addresses and bring service back up at a new set of addresses. Note that this may not involve anything as complex as IPv6 network renumbering, it may just involve changing

the addresses of the home agents. With a signaling message, the service provider could inform mobile nodes to look for a new home agent.

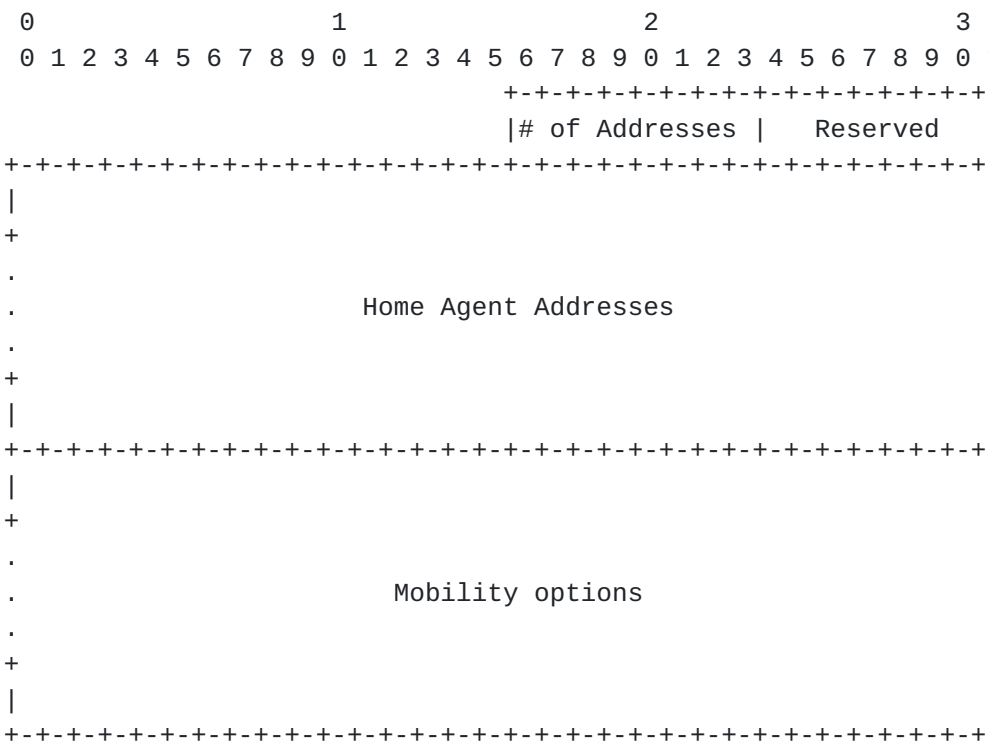
3. Home Agent Switch Message

The Home Agent Switch message is used by the home agent to signal the mobile node that it needs to stop acting as the home agent for the mobile node, and that it should acquire a new home agent. Home Agent Switch messages are sent as described in Section 4.

The message described below follows the Mobility Header format specified in Section 6.1 of [2]:



The Home Agent Switch Message uses the MH Type value (TBD). When this value is indicated in the MH Type field, the format of the Message Data field in the Mobility Header is as follows:



# of Addresses

An 8-bit unsigned integer indicating the number of IPv6 home agent addresses in the message. If set to zero, the mobile node MUST perform home agent discovery.

Reserved

8-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Home Agent Addresses

A list of alternate home agent addresses for the mobile node. The number of addresses present in the list is indicated by the "# of Addresses" field in the Home Agent Switch message.

Mobility options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field

contains zero of more TLV-encoded mobility options. The encoding and format of defined options MUST follow the format specified in Section 6.2 of [2]. The receiver MUST ignore and skip any options with it does not understand.

The Binding Refresh Advice mobility option defined in Section 6.2.4 of [2] is valid for the Home Agent Switch message.

If no home agent addresses and no options are present in this message, no padding is necessary and the Header Len field in the Mobility Header will be set to 0.

4. Home Agent Operation

4.1 Sending Home Agent Switch Messages

When sending a Home Agent Switch message, the sending node constructs the packet as it would any other Mobility Header, except:

- The MH Type field MUST be set to (TBD).
- If alternative home agent addresses are known, the sending home agent SHOULD include them in the list of suggested alternate home agents. The home agent addresses field should be constructed as described in Section 10.5.1 of [2], which will randomize addresses of the same preference in the list.
- The "# of addresses" field MUST be filled-in corresponding to the number of home agent addresses included in the message. If no addresses are present, the field MUST be set to zero, forcing the mobile node to perform home agent discovery by some other means.
- If the home agent is able to continue offering services to the mobile node for some period of time, it MAY include a Binding Refresh Advice mobility option indicating the time (in units of 4 seconds) until the binding will be deleted.

The Home Agent Switch message MUST be authenticated in one of the following ways:

- The home agent to mobile node IPsec ESP authentication SA for integrity protection.
- A home agent to mobile node authentication option, such as [3].

A home agent SHOULD send a Home Agent Switch message when a known period of unavailability is pending so the mobile node has sufficient time to find another suitable home agent.

The sending node does not need to be the current home agent for the mobile node, for example as described in [4], but it MUST have a security association with the mobile node so the message is not rejected. In this case, the Home Agent Switch message SHOULD only contain the address of the home agent sending the message in the Home Agent Addresses field, which implies the mobile node should switch to using the sender as its new home agent.

4.2 Retransmissions

If the home agent does not receive a response from the mobile node - either a Binding Update message to delete its home binding if it is the current home agent, or a Binding Update message to create a home binding if it is not the current home agent, then it SHOULD retransmit the message, until a response is received. The initial value for the retransmission timer is INITIAL-HA-SWITCH-TIMEOUT.

The retransmissions by the home agent MUST use an exponential back-off mechanism, in which the timeout period is doubled upon each retransmission, until either the home agent gets a response from the mobile node to delete its binding, or the timeout period reaches the value MAX-HA-SWITCH-TIMEOUT.

If the home agent included a Binding Refresh Advice mobility option, then it SHOULD delay any retransmissions until at least one half of the time period has expired, or INITIAL-HA-SWITCH-TIMEOUT, whichever value is less.

4.3 Mobile Node Errors

If a mobile node does not understand how to process a Home Agent Switch Message, it will send a Binding Error message as described in Section 5.1.

If a mobile node is unreachable, in other words, it still has a home binding with the home agent after reaching the timeout period of MAX-HA-SWITCH-TIMEOUT, the home agent SHOULD NOT make any conclusions about its status.

In either case, the home agent SHOULD attempt to continue providing services until the lifetime of the binding expires.

Attempts by the mobile node to extend the binding lifetime with a Binding Update message SHOULD be rejected, and a Binding

Acknowledgement SHOULD be returned with status value 129 (Administratively prohibited) as specified in Section 6.1.8 of [2].

5. Mobile Node Operation

5.1 Receiving Home Agent Switch Messages

Upon receiving a Home Agent Switch message, the Mobility Header MUST be verified as specified in [2], specifically:

- The Checksum, MH type, Payload Proto and Header Len fields MUST meet the requirements of Section 9.2 of [2].

- The packet MUST be authenticated, either by the home agent to mobile node IPsec ESP authentication SA for integrity protection, or a home agent to mobile node authentication option.

If the packet is dropped due to the above tests, the receiving node MUST follow the processing rules as Section 9.2 of [2] defines. For example, it MUST send a Binding Error message with the Status field set to 2 (unrecognized MH Type value) if it does not support the message type.

Upon receipt of a Home Agent Switch message, the mobile node MUST stop using its current home agent for services and MUST delete its home binding by sending a Binding Update message as described in [2]. This acts as an acknowledgement of the Home Agent Switch message. Alternately, if the sender of the message is not the current home agent, sending a Binding Update message to create a home binding will act as an acknowledgement of the Home Agent Switch message.

If a Binding Refresh Advice mobility option is present, the mobile node MAY delay the deletion of its home binding and continue to use its current home agent until the calculated time period has expired.

If the Home Agent Switch message contains a list of alternate home agent addresses, the mobile node SHOULD select a new home agent as described in Section 5.2, and establish the necessary IPsec security associations with the new home agent by whatever means required as part of the mobile node/home agent bootstrapping protocol for the home agent's mobility service provider. If no alternate home agent addresses are included in the list, the mobile node MUST first perform home agent discovery.

5.2 Selecting a Home Agent

In most cases, the home agent addresses in the Home Agent Switch message will be of other home agents on the home link of the mobile node. In this case, the mobile node SHOULD select a new home agent from the addresses as they are ordered in the list. If the first address in the list is unable to provide service, then the subsequent addresses in the list should be tried in-order.

In the case that the home agent addresses in the Home Agent Switch message are not all home agents on the home link of the mobile node (the computed prefix is different), the mobile node SHOULD select one on the home link first, if available, followed by home agents not on the home link. Choosing a home agent not on the home link might require a change of the home address for the mobile node, which could cause a loss of connectivity for any connections using the current home address.

6. Operational Considerations

This document does not specify how an operator might use the Home Agent Switch message in its network. However, it might be the case that a home agent provides service for many thousands of mobile nodes. Care should be taken to reduce the signaling overhead required for handing off many mobile nodes to an alternate home agent.

7. Procotol Constants

INITIAL-HA-SWITCH-TIMEOUT	5 seconds
MAX-HA-SWITCH-TIMEOUT	20 seconds

8. IANA Considerations

A new Mobility Header type is required for the following new message described in Section 3:

(TBD) Home Agent Switch message

9. Security Considerations

The Home Agent Switch message MUST be authenticated by one of the following methods:

- The home agent to mobile node IPsec ESP authentication SA for integrity protection as described in [2].

- A home agent to mobile node authentication option, such as [3].

The Home Agent Switch message MAY use the IPsec ESP SA in place for Binding Updates and Acknowledgements as specified in Section 5.1 of [2], in order to reduce the number of configured security associations. This also gives the message authenticity protection.

Some operators may not want to reveal the list of home agents to on-path listeners. In such a case, the Home Agent Switch message should use the home agent to mobile node IPsec ESP encryption SA for confidentiality protection.

10. References

10.1 Normative References

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

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

10.2 Informative references

[3] Patel, A., Leung, K., Khalil, M., Akhtar, H., and Chowdhury, K., "Authentication Protocol for Mobile IPv6", RFC 4285, January, 2006.

[4] Wakikawa, R. (Editor), "Home Agent Reliability Protocol", draft-ietf-mip6-hareliability-01.txt, October, 2006.

Acknowledgments

We would like to thank the authors of a number of previous drafts that contributed content to this document:

- draft-wakikawa-mip6-nemo-haha-spec-00.txt
- draft-deng-mip6-ha-loadbalance-02.txt
- draft-kempf-mip6-ha-alert-00.txt
- draft-haley-mip6-mh-signaling-00.txt

Thanks also to Kilian Weniger, Jixing Liu, Alexandru Petrescu, Jouni Korhonen, and Wolfgang Fritsche for their review and feedback.

Author's Addresses

Brian Haley
Hewlett-Packard Company
110 Spitbrook Road
Nashua, NH 03062, USA
Email: brian.haley@hp.com

Vijay Devarapalli
Azaire Networks
3121 Jay Street
Santa Clara, CA 95054 USA
Email: vijay.devarapalli@azairenet.com

James Kempf
DoCoMo USA Labs
181 Metro Drive
Suite 300
San Jose, CA 95110 USA
Email: kempf@docomolabs-usa.com

Hui Deng
Research & Development Center
Hitachi (China), Investment Ltd.
Beijing Fortune Bldg. 1701, 5 Dong San Huan Bei-Lu
Chao Yang District, Beijing 100004, China
Email: hdeng@hitachi.cn

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND 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.

Acknowledgement

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