Extension to RFC 3775 for Alerting the Mobile Node to Home Agent Unavailability
draft-kempf-mip6-ha-alert-00.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

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

This Internet-Draft will expire on July 28, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

RFC 3775 contains no way for a home agent to notify a mobile node that the home agent will shortly become unavailable, and suggest possible substitutes. A mobile node can suddenly find itself without mobility service. This document describes a simple protocol to inform the mobile node when its home agent is about to become unavailable

and whether the mobile node should re-run bootstrapping to find 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....3
2.1. Periodic Maintenance....3
2.2. Functional Load Balancing....3
2.3. Home Agent Renumbering....4
3. Home Agent Unavailability Message....4
3.1. Validation of HAU Messages....4
3.2. Home Agent Unavailability Message Format....5
4. Home Agent Considerations....6
5. Mobile Node Considerations....6
6. Security Considerations....7
7. Open Questions....7
8. References....8
8.1. Normative References....8
8.2. Informative References....8
Author's Addresses....8
Intellectual Property Statement....8
Disclaimer of Validity....9
Copyright Statement....9
Acknowledgment....9

1. Introduction

RFC 3775 [2] contains no protocol to allow a home agent to inform its mobile nodes that it is about to cease service. Without such functionality, a mobile node can suddenly find itself without its tunneled traffic. Even worse, if the mobile node is route optimizing, it may not discover the problem until much later, after other nodes fail to contact it.

Note that, as a router on the home link, the home agent can use an unmodified RFC 2461 [2] Redirect to tell the mobile node about a new router on the home link, but the message is ambiguous. Is the recommended router a home agent or it just a router only for nodes on the home link? What if the entire link is going down? RFC 2461 only

allows routers to be referred to by their link local address in Redirects, which would not allow a mobile node away from home to find the new home agent. A home agent can also send a Router Advertisement with lifetime zero to indicate that it was becoming unavailable, but this would not provide the mobile node with any indication of a suggested substitute.

In this document, a simple extension of the RFC 3775 Home Agent Discovery message is proposed to allow home agent unavailability alerting. The extension allows a home agent to send an unsolicited Home Agent Discovery message to inform the mobile node about the need to find a new home agent.

2. Scenarios

Here are a few sample scenarios where a home agent unavailability alerting message would be useful.

2.1. Periodic Maintenance

Although many users and engineers would prefer that networking equipment run without ever shutting down, most responsible service providers do periodic maintenance in order to maintain reliability. If a home agent is shut down for maintenance, some way is required to tell the client mobile nodes so they don't lose mobility service.

2.2. Functional Load Balancing

A Mobile IPv6 home agent provides the client with two basic services: a rendezvous server where correspondents can find the current care of address for the mobile node, and - when route optimization isn't used - an overlay router to redirect traffic sent to/from the home address to/from the 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-like home agent and stay there if it does route optimization. However, if the original home agent detects that the mobile node isn't doing route optimization, it could redirect the mobile node to a home agent with better data throughput (of course, any existing TCP sessions would be dropped).

2.3. Home Agent Renumbering

Periodically, a mobility service provider may want to shut down home agent service 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 on the home agents. There are various reasons why a mobility service provider might want to do this; an example is if the mobility service provider revokes the account of a user who the service provider has reason to believe might use the old home agent address to disrupt service for other users. With a service unavailability message, the service provider could inform mobile nodes to look for a new home agent.

3. Home Agent Unavailability Message

A home agent sends a Home Agent Unavailability (HAU) message when an anticipated period of unavailability occurs for the home agent. The message is sent to the mobile node's home address and is tunneled to the mobile node at its care of address.

3.1. Validation of HAU Messages

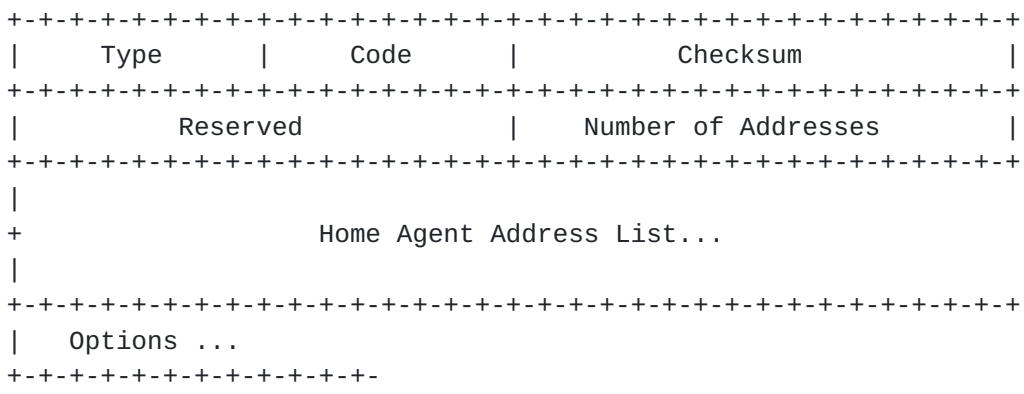
A mobile node MUST silently discard a received HAU message that does not satisfy all of the following validity checks:

- IP Source Address is the global home agent address
- The message is covered by the IPsec ESP SAs for ICMP messages between the home agent and mobile node.
- IP Destination Address is the mobile node's home address.
- ICMP Checksum is valid.
- ICMP Code is TBD.
- ICMP length (derived from the IP length) is 8 or more octets.
- All included options have a length that is greater than zero.

The contents of the Reserved field, and of any unrecognized options MUST be ignored.

3.2. Home Agent Unavailability Message Format

Home agents send HAU packets to inform mobile node clients about pending periods of unavailability. The home agent can recommend a list of substitute home agent addresses, or it can require the mobile node to re-initiate bootstrapping to find a new home agent by setting the length of the substitute list to zero.



IP Fields:

Source Address

MUST be the home agent's global address.

Destination Address

MUST be the mobile node's home address.

ESP Header

The packet MUST be protected by an ESP tunnel mode header for data origin authentication and encryption, used to protect ICMP packets between the home agent and mobile node.

ICMP Fields:

Type 145

Code TBD (assigned by IANA)

Checksum The ICMP checksum

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Number of Addresses

An unsigned integer giving the number of IPv6 home agent addresses in the list to follow. If zero, then the mobile node MUST redo home agent discovery.

Home Agent Address List

List of 128 bit IPv6 addresses for suggested substitute home agents.

Possible Options:

There are no default options. Options can be added by extension.

4. Home Agent Considerations

A home agent SHOULD send a HAU message when a known period of unavailability is pending. The message MUST be sent to all mobile nodes with currently active bindings. If alternative home agent addresses are known, either on the same subnet or a different one, the home agent SHOULD include them in the list of suggested substitute home agents. Otherwise, the home agent MUST set the length of the substitute home agent list to zero, forcing the mobile node to perform home agent discovery by some other means.

5. Mobile Node Considerations

Upon receipt of a HAU message, a mobile node MUST cease utilizing the old home agent for overlay traffic routing. If the HAU message contains a list of substitute home agents, the mobile node SHOULD select a home agent at random 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 substitute home agents are included in the list, the mobile node MUST first perform home agent discovery.

6. Security Considerations

As with other home link ICMP messages in RFC 3775, the HAU message MUST use the home agent to mobile node ESP encryption SA for confidentiality protection, and MUST use the home agent to mobile node ESP authentication SA for integrity protection.

IANA Considerations

A new ICMP Code, TBD, is required for the ICMP Home Agent Discovery message, type 145.

7. Open Questions

- If a home agent has a lot of clients, the IKE traffic and binding updates to the new home agent or agents could result in a lot of congestion. Would it make sense to enable a mode whereby the home agent can transfer the security and binding context to the new home agents, then set a flag in the HAU so that the mobile nodes don't have to re-initialize? Generally, transferring IPsec between hosts ("outside the crypto boundary") is strongly frowned upon by security folks, but one could make an argument that a distributed crypto boundary in which the machines share a strong security association could be set up. The other problem is what new home address to use. One could specify something simple, like the old interface identifier plus subnet prefix from the new home agent subnet, but that disallows subtle address allocation strategies such as CGA or RFC 3041 address privacy. All in all, it seems like a hack. Sme kind of timing randomization on the initialization traffic would reduce the potential for congestion, but not the overall traffic volume.

- If a home agent has lots of clients, it could end up unicasting lots of HAU messages, which could result in a lot of traffic and thus congestion. Would it make more sense to use a multicast message, perhaps to the All Nodes Multicast Address? Or should we introduce an All Mobile Nodes Multicast Address to avoid having fixed nodes on the subnet get the message? If multicast is used, then what security is on the packet? IPsec is for unicast only, so the ICMP SA can't be used.

- Should the HAU include a "remaining lifetime" field, indicating how long the mobile node has before the home agent becomes unavailable?

8. References

8.1. 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.

[3] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998

8.2. Informative References

Author's Addresses

James Kempf
DoCoMo USA Labs
181 Metro Drive
Suite 300
San Jose, CA
95110

Phone: +1 408 451 4711
Email: kempf@docomolabs-usa.com

Intellectual Property Statement

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. By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2004). 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.

Acknowledgment

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