NETLMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 11, 2009

V. Devarapalli (ed.)
WiChorus
R. Koodli (ed.)
Starent Networks
H. Lim
N. Kant
Stoke
S. Krishnan
Ericsson
J. Laganier
DOCOMO Euro-Labs
April 9, 2009

Heartbeat Mechanism for Proxy Mobile IPv6
draft-ietf-netlmm-pmipv6-heartbeat-07.txt

Status of this Memo

Copyright Notice

Abstract

Proxy Mobile IPv6 is a network-based mobility management protocol. The mobility entities involved in the Proxy Mobile IPv6 protocol, the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA), setup tunnels dynamically to manage mobility for a mobile node within the Proxy Mobile IPv6 domain. This document describes a heartbeat mechanism between the MAG and the LMA to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

Table of Contents

1. Introduction 4
2. Terminology 4
3. Heartbeat Mechanism 4
3.1. Failure Detection 5
3.2. Restart Detection 6
3.3. Heartbeat Message 7
3.4. Restart Counter Mobility Option 8
4. Exchanging Heartbeat Messages over an IPv4 Transport Network 9
5. Configuration Variables 9
6. Security Considerations 10
7. IANA Considerations 10
8. Acknowledgments 10
9. References 11
9.1. Normative References 11
9.2. Informative References 11
Authors' Addresses 11

1. Introduction

Proxy Mobile IPv6 [RFC5213] enables network-based mobility for IPv6 hosts that do not implement any mobility protocols. The protocol is described in detail in [RFC5213]. In order to facilitate the network-based mobility, the PMIPv6 protocol defines a Mobile Access Gateway (MAG), which acts as a proxy for the Mobile IPv6 [RFC3775] signaling, and the Local Mobility Anchor (LMA) which acts similar to a Home Agent, anchoring a Mobile Node's sessions within a Proxy Mobile IPv6 (PMIPv6) domain. The LMA and the MAG establish a bidirectional tunnel for forwarding all data traffic belonging to the Mobile Nodes.

In a distributed environment such as a PMIPv6 domain consisting of LMA and MAGs, it is necessary for the nodes to 1) have a consistent state about each other's reachability, and 2) quickly inform peers in the event of recovery from node failures. So, when the LMA restarts after a failure, the MAG should (quickly) learn about the restart so that it could take appropriate actions (such as releasing any resources). When there are no failures, a MAG should know about LMA's reachability (and vice versa) so that the path can be assumed to be functioning.

This document specifies a heartbeat mechanism between the MAG and the LMA to detect the status of reachability between them. This document also specifies a mechanism to indicate node restarts; the mechanism could be used to quickly inform peers of such restarts. The heartbeat message is a mobility header message (protocol type 135) which is periodically exchanged at a configurable threshold of time or sent unsolicited soon after a node restart. This document does not specify the specific actions (such as releasing resources) that a node takes as a response to processing the heartbeat messages.

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 [RFC2119].

3. Heartbeat Mechanism

The MAG and the LMA exchange heartbeat messages every HEARTBEAT_INTERVAL seconds to detect the current status of reachability between them. The MAG initiates the heartbeat exchange to test if the LMA is reachable by sending a Heartbeat Request message to the LMA. Each Heartbeat Request contains a sequence

number that is incremented monotonically. The sequence number on the last Heartbeat Request message is always recorded by the MAG, and is used to match the corresponding Heartbeat Response. Similarly, the LMA also initiates a heartbeat exchange with the MAG, by sending a Heartbeat Request message, to check if the MAG is reachable. The format of the Heartbeat message is described in Section 3.3.

A Heartbeat Request message can be sent only if the MAG has at least one proxy binding cache entry at the LMA for a mobile node attached to the MAG. If there are no proxy binding cache entries at the LMA for any of the mobile nodes attached to the MAG, then the heartbeat message SHOULD NOT be sent. Similarly, the LMA SHOULD NOT send a Heartbeat Request message to a MAG if there is no active binding cache entry created by the MAG. A PMIPv6 node MUST respond to a Heartbeat Request message with a Heartbeat Response message, irrespective of whether there is an active binding cache entry.

The HEARTBEAT_INTERVAL SHOULD NOT be configured to a value less than 30 seconds. Deployments should be careful in setting the value for the HEARTBEAT_INTERNVAL. Sending heartbeat messages too often may become an overhead on the path between the MAG and the LMA. It could also create congestion in the network and negatively affect network performance. The HEARTBEAT_INTERVAL can be set to a much larger value on the MAG and the LMA, if required, to reduce the burden of sending periodic heartbeat messages.

If the LMA or the MAG do not support the heartbeat messages, they respond with a Binding Error message with status set to '2' (unrecognized MH type value) as described in [RFC3775]. When the Binding Error message with status set to '2' is received in response to Heartbeat Request message, the initiating MAG or the LMA MUST NOT use heartbeat messages with the other end again.

If a PMIPv6 node has detected that a peer PMIPv6 node has failed or restarted without retaining the PMIPv6 session state, it should mark the corresponding binding update list or binding cache entries as invalid. The PMIPv6 node may also take other actions which are outside the scope of this document.

The detection of failures and restarts events may be signaled to network operators by using asynchronous notifications. Future work may define such notifications in a SMIv2 Management Information Base (MIB) module.

3.1. Failure Detection

A PMIPv6 node, (MAG or LMA) matches every received Heartbeat Response to the Heartbeat Request sent using the sequence number. Before

sending the next Heartbeat Request, it increments a local variable MISSING_HEARTBEAT if it has not received a Heartbeat Response for the previous request. When this local variable MISSING_HEARTBEAT exceeds a configurable parameter MISSING_HEARTBEATS_ALLOWED, the PMIPv6 node concludes that the peer PMIPv6 node is not reachable. If a Heartbeat Response message is received, the MISSING_HEARTBEATS counter is reset.

3.2. Restart Detection

The section describes a mechanism for detecting failure recovery without session persistence. In case the LMA or the MAG crashes and re-boots and loses all state with respect to the PMIPv6 sessions, it would be beneficial for the peer PMIPv6 node to discover the failure and the loss of session state and establish the sessions again.

Each PMIPv6 node (both the MAG and LMA) MUST maintain a monotonically increasing Restart Counter that is incremented every time the node re-boots and looses PMIPv6 session state. The counter MUST NOT be incremented if the recovery happens without losing state for the PMIPv6 sessions active at the time of failure. This counter MUST be treated as state that is preserved across reboots. A PMIPv6 node includes a Restart Counter mobility option, described in Section 3.4 in an Heartbeat Response message to indicate the current value of the Restart Counter. Each PMIPv6 node MUST also store the Restart Counter for all the peer PMIPv6 nodes that it has sessions with currently. Storing the Restart Counter values for peer PMIPv6 nodes does not need to be preserved across reboots.

The PMIPv6 node that receives the Heartbeat Response message compares the Restart Counter value with the previously received value. If the value is different, the receiving node assumes that the peer PMIPv6 node had crashed and recovered. If the Restart Counter value changes or if there was no previously stored value, the new value is stored by the receiving PMIPv6 node.

If a PMIPv6 node restarts and looses PMIPv6 session state, it SHOULD send an unsolicited Heartbeat Response message with an incremented Restart Counter to all the PMIPv6 nodes that had previously established PMIPv6 sessions. Note that this is possible only when the PMIPv6 node is capable of storing information about the peers across reboots. The unsolicited Heartbeat Response message allows the peer PMIPv6 nodes to quickly discover the restart. The sequence number field in the unsolicited Heartbeat Response is ignored and no response is necessary; the nodes will synchronize during the next Request and Response exchange.

3.3. Heartbeat Message

The Heartbeat Message is based on the Mobility Header defined in Section 6.1 of [RFC3775]. The 'MH type' field in the Mobility Header indicates that it is a Heartbeat Message. The value MUST be set to <IANA-TBD1>. This document does not make any other changes to the Mobility Header message. Please refer to [RFC3775] for a description of the fields in the Mobility Header Message.

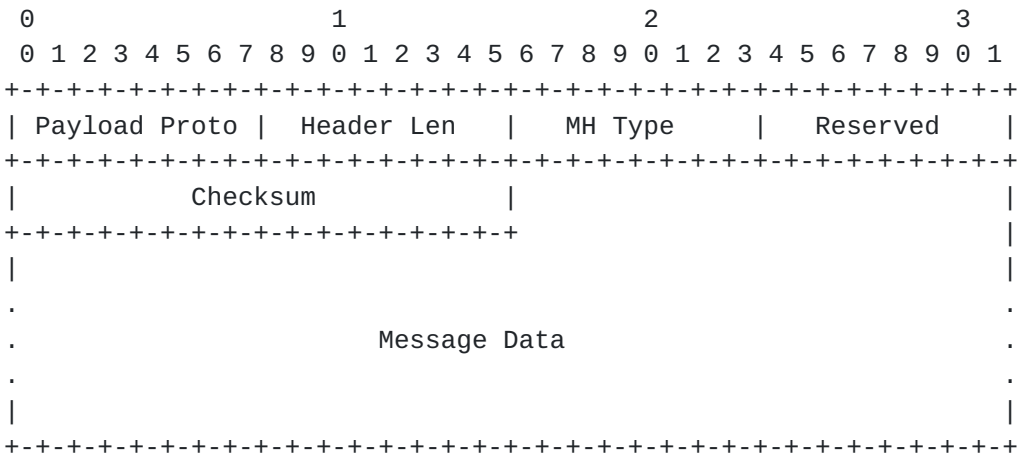

Figure 1: Mobility Header Message Format

The Heartbeat Message follows the 'Checksum' field in the above message. The following illustrates the message format for the Heartbeat Mobility Header message.

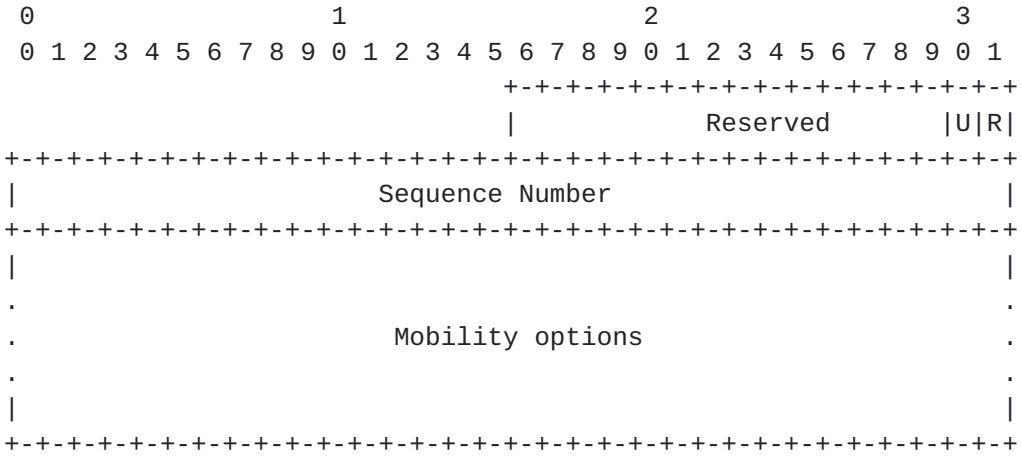

Figure 2: Heartbeat Message Format

Reserved

Set to 0 and ignored by the receiver.

'U'

Set to 1 in Unsolicited Heartbeat Response. Otherwise set to 0.

'R'

A 1-bit flag that indicates whether the message is a request or a response. When the 'R' flag is set to 0, it indicates that the Heartbeat message is a request. When the 'R' flag is set to 1, it indicates that the Heartbeat message is a response.

Sequence Number

A 32-bit sequence number used for matching the request to the reply.

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 or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. At the time of writing this document, the Restart Counter Mobility Option, described in Section 3.4, is the only valid option in this message.

3.4. Restart Counter Mobility Option

The following shows the message format for a new mobility option for carrying the Restart Counter Value in the Heartbeat message. The Restart Counter Mobility Option is only valid in a Heartbeat Response message. It has an alignment requirement of 4n+2.

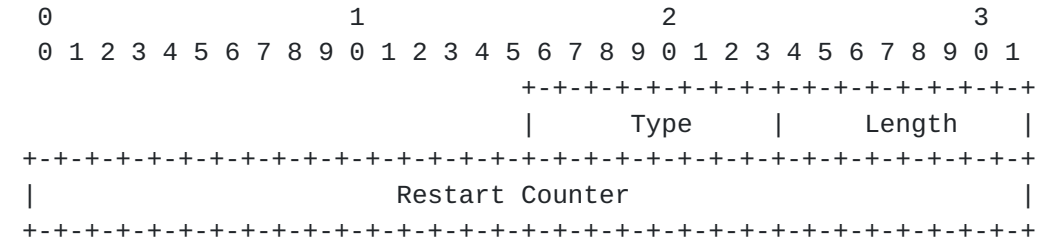

Figure 3: Restart Counter Mobility Option

Type

A 8-bit field that indicates that it is a Restart Counter mobility option. It MUST be set to <IANA-TBD2>.

Length

A 8-bit field that indicates the length of the option in octets excluding the 'Type' and 'Length' fields. It is set to '4'.

Restart Counter

A 32-bit field that indicates the current Restart Counter value.

4. Exchanging Heartbeat Messages over an IPv4 Transport Network

In some deployments, the network between the MAG and the LMA may not be capable of transporting IPv6 packets. In this case, the Heartbeat messages are tunneled over IPv4. If the Proxy Binding Update and Proxy Binding Acknowledgment messages are sent using UDP encapsulation to traverse NATs, then the Heartbeat messages are also sent with UDP encapsulation. The UDP port used would be the same as the port used for the Proxy Binding Update and Proxy Binding Acknowledgement messages. For more details on tunneling Proxy Mobile IPv6 signaling messages over IPv4, see [I-D.ietf-netlmm-pmip6-ipv4-support].

5. Configuration Variables

The LMA and the MAG must allow the following variables to be configurable.

HEARTBEAT_INTERVAL

This variable is used to set the time interval in seconds between two consecutive Heartbeat Request messages. The default value is 60 seconds. It SHOULD NOT be set to less than 30 seconds or larger than 3600 seconds.

MISSING_HEARTBEATS_ALLOWED

This variable indicates the maximum number of consecutive Heartbeat Request messages that a PMIPv6 node did not receive a response for before concluding that the peer PMIPv6 node is not reachable. The default value for this variable is 3.

6. Security Considerations

The heartbeat messages are just used for checking reachability between the MAG and the LMA. They do not carry information that is useful for eavesdroppers on the path. Therefore, confidentiality protection is not required. Integrity protection using IPsec [RFC4301] for the heartbeat messages MUST be supported on the MAG and the LMA. RFC 5213 [RFC5213] describes how to protect the Proxy Binding Update and Acknowledgment signaling messages with IPsec. The Heartbeat message defined in this specification is merely another subtype of the same Mobility Header protocol that is already being protected by IPsec. Therefore, protecting this additional message is possible using the mechanisms and security policy models from these RFCs. The security policy database entries should use the new MH Type, the Heartbeat Message, for the MH Type selector.

If dynamic key negotiation between the MAG and the LMA is required, IKEv2 [RFC4306] should be used.

7. IANA Considerations

The Heartbeat message defined in Section 3.3 must have the type value allocated from the same space as the 'MH Type' name space in the Mobility Header defined in RFC 3775 [RFC3775].

The Restart Counter mobility option defined in Section 3.4 must have the type value allocated from the same name space as the Mobility Options defined in RFC 3775 [RFC3775].

8. Acknowledgments

A heartbeat mechanism for a network-based mobility management protocol was first described in [I-D.giaretta-netlmm-dt-protocol]. The authors would like to thank the members of a NETLMM design team that produced that document. The mechanism described in this document also derives from the path management mechanism described in [GTP].

We would like to thank Alessio Casati for first suggesting a fault handling mechanism for Proxy Mobile IPv6.

9. References

9.1. Normative References

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

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[I-D.ietf-netlmm-pmip6-ipv4-support] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", draft-ietf-netlmm-pmip6-ipv4-support-10 (work in progress), March 2009.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

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

9.2. Informative References

[I-D.giaretta-netlmm-dt-protocol] Giaretta, G., "The NetLMM Protocol", draft-giaretta-netlmm-dt-protocol-02 (work in progress), October 2006.

[GTP] 3rd Generation Partnership Project, "3GPP Technical Specification 29.060 V7.6.0: "Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 7)"", July 2007.

Authors' Addresses

Vijay Devarapalli
WiChorus
3950 North First Street
San Jose, CA 95134
USA

Email: vijay@wichorus.com

Rajeev Koodli
Starent Networks
USA

Email: rkoodli@starentnetworks.com

Heeseon Lim
Stoke
5403 Betsy Ross Drve
Santa Clara, CA 95054
USA

Email: hlim@stoke.com

Nishi Kant
Stoke
5403 Betsy Ross Drive
Santa Clara, CA 95054
USA

Email: nishi@stoke.com

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

Email: suresh.krishnan@ericsson.com

Julien Laganier
DOCOMO Euro-Labs
Landsbergerstrasse 312
Munich, D-80687
Germany

Email: julien.IETF@laposte.net