MIP6 Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 7, 2008

V. Devarapalli
Azaire Networks

October 5, 2007

Mobile IPv6 Experimental Messages
draft-ietf-mip6-experimental-messages-03.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a new experimental Mobility Header message and a mobility option that can be used for experimental extensions to the Mobile IPv6 protocol.

Table of Contents

1. Introduction 3
2. Terminology 4
3. Experimental Mobility Header message 4
4. Experimental Mobility Option 5
5. Security Considerations 5
6. IANA Considerations 6
7. Acknowledgements 6
8. References 6
8.1. Normative References 6
8.2. Informative References 6
Author's Address 7
Intellectual Property and Copyright Statements 8

1. Introduction

When experimenting with a protocol or defining a new extension to a protocol, one needs either a protocol number, a new message or an option to carry the information related to the experiment. Most implementations end up using unassigned values for the new messages. Many times this creates problems when the same value is assigned through the IETF standards action, by IANA or if the implementation gets deployed with these messages. Therefore it is considered a good practice to set aside some code points that identify the experimental protocols or messages for experimental purposes. The need for experimental messages is shown in [3].

This document defines new messages for experimenting with extensions to the Mobile IPv6 protocol. These messages should be strictly used for experiments. Experiments that are successful should be standardized in the IETF. An implementation MUST NOT be released or deployed with the experimental messages.

This document defines a new Mobility Header message, the Experimental Mobility message that can be sent at any time by the mobile node, the home agent or the correspondent node. Since Mobility Header messages cannot be combined and sent in one packet, there is always only one Mobility Header message in any Mobile IPv6 packet. Home agent or correspondent node implementations that do not recognize the mobility message type, discard the message and send Binding Error message as described in [2], with the Status field set to 2 (unrecognized MH Type value). Mobile nodes that do not recognize the mobility message type should discard the message and send an ICMP Parameter problem with code 0.

This document also defines a new mobility option, the Experimental Mobility option, which can be carried in any Mobility Header message. Mobility options, by definition, can be skipped if an implementation does not recognize the mobility option type [2].

The messages defined in this document can also be used for NEMO [4] and Proxy Mobile IPv6 [5] since these protocols also use Mobility Header messages.

Experimental code points could potentially disrupt a deployed network when experiments using these code points are performed in the network. Therefore the network scope of support for experimental values should carefully be evaluated before deploying any experiment across extended network domains, such as the public Internet.

Experimental mechanisms should only be used for actual experimentation. By design, only a single code point is allocated

for the message and another one for the option. This limits the number of experiments among a set of peers to one at a time. When experimental mechanisms are shown to be useful and there is a desire to deploy them beyond the experiment they should be standardized and given new code points.

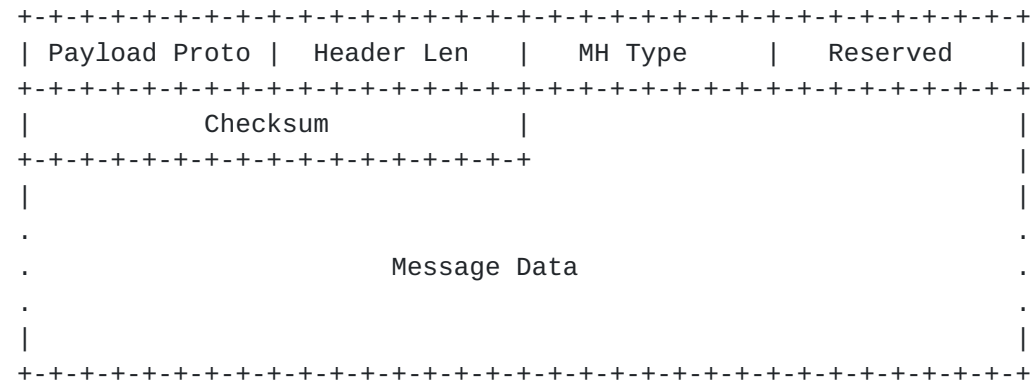
2. Terminology

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 [1].

3. Experimental Mobility Header message

The Experimental Mobility Header message is based on the Mobility Header message defined in Section 6.1 of RFC 3775 [2]. There are no fields in the message beyond the required fields in the Mobility Header. The 'MH Type' field in the Mobility Header indicates that it is an Experimental Mobility Header message.

If no data is present in the message, two bytes of padding is required. The 'Header Len' field in the Mobility Header is set to 0, since the first 8 octets are excluded while calculating the length of the Mobility Header message.

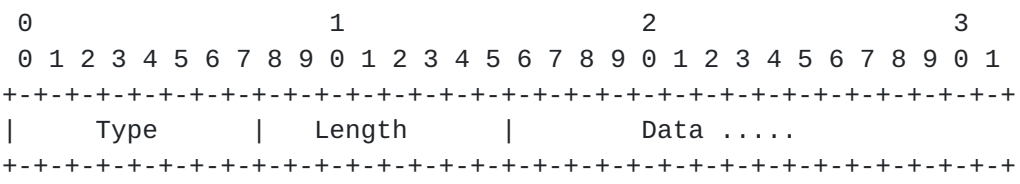


See RFC 3775 [2] for a description of the 'Payload Proto', 'Header Len', 'MH Type', 'Reserved' and the 'Checksum' fields.

The 'Message Data' field carries the data specific to the experimental protocol extension. The total length of the message is indicated by the 'Header Len' field in the Mobility Header.

4. Experimental Mobility Option

The Experimental mobility option can be included in any Mobility Header message. If the Mobility Header message includes a Binding Authorization Data option [2], then the Experimental Mobility Option should appear before the Binding Authorization Data option.



Type

A 8-bit field indicating that it is an experimental mobility option.

Length

A 8-bit indicating the length of the option in octets excluding the Type and Length fields.

Data

Data related to the experimental protocol extension.

5. Security Considerations

Protection for the Experimental Mobility Header message and mobility option depends on the experiment that is being carried out and the kind of information that is being carried in the messages. If these messages carry information that should not be revealed on the wire or that can affect the binding cache entry at the home agent or the correspondent node, they should be protected in a manner similar to Binding Updates and Binding Acknowledgements.

Security analyzers such as firewalls and network intrusion detection monitors often rely on unambiguous interpretations of the fields described in this document. As new values for the fields are assigned, existing security analyzers that do not understand the new values may fail, resulting in either loss of connectivity, if the analyzer declines to forward the unrecognized traffic, or in loss of security if it does forward the traffic and the new values are used as part of an attack.

When experimental code points are deployed within an administratively self-contained network domain, it must be ensured that that each code point is used consistently to avoid interference between experiments. When experimental code points are used in traffic that crosses multiple administrative domains, the experimenters should assume that there is a risk that the same code points will be used simultaneously by other experiments and thus that there is a possibility that the experiments will interfere. Particular attention should be given to security threats that such interference might create. Please see RFC 4727 for more details [6].

6. IANA Considerations

The Experimental Mobility Header message defined in Section 3, should have the type value allocated from the same space as the 'MH Type' field in the Mobility Header [2].

The Experimental mobility option defined in Section 4, should have the type value allocated from the same space as Mobility Options [2].

7. Acknowledgements

The author would like to thank Jari Arkko and Basavaraj Patil with whom the contents of this document were discussed first.

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 J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

8.2. Informative References

[3] Narten, T., "Assigning Experimental and Testing Numbers Considered Useful", BCP 82, RFC 3692, January 2004.

[4] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[5] Gundavelli, S., "Proxy Mobile IPv6",

draft-sgundave-mip6-proxymip6-02 (work in progress), March 2007.

[6] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", RFC 4727, November 2006.

Author's Address

Vijay Devarapalli
Azaire Networks
4800 Great America Pkwy
Santa Clara, CA 95054
USA

Email: vijay.devarapalli@azairenet.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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