MIP4 Working Group	H. Deng	
Internet-Draft	China Mobile	
Intended status: Standards Track	H. Levkowetz	
Expires: April 28, 2011	Netnod	
	V. Devarapalli	
	WiChorus	
	S. Gundavelli	
	Cisco Systems	
	B. Haley	
	Hewlett-Packard Company	
	October 25, 2010	

TOC

Generic Notification Message for Mobile IPv4
draft-ietf-mip4-generic-notification-message-16

Abstract

This document specifies protocol enhancements that allow Mobile IPv4 entities to send and receive explicit notification messages using a Mobile IPv4 message type designed for this purpose.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on April 28, 2011.

Copyright Notice

Table of Contents

---

1. Introduction

TOC

In some situations, there is a need for Mobile IPv4 entities, such as the home agent(HA), foreign agent(FA) and mobile node(MN) to send and receive asynchronous notification messages during a mobility session. 'Asynchronous messages' in this context is used to mean messages which are not synchronous with the Registration Request and Registration Reply messages of the base Mobile IP Specification [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). The base Mobile IP Specification does not have a provision for this.
This document defines a generic message and a notification model that can be used by Mobile IPv4 entities to send various notifications. It also defines a corresponding acknowledgement message to allow for reliable delivery of notifications. Only the following extensions may be present in these new messages, as defined by this document:

- MN-HA Authentication Extension
- MN-FA Authentication Extension
- FA-HA Authentication Extension
- Message String Extension

The semantics of receiving a generic notification message with a Message String Extension are null; i.e., it has no effect on the state of a mobile node's existing registration. See Section 3.1 (Notification Message - Examples) for some application examples that motivate the new messages defined in this document.

2. Terminology

TOC

It is assumed that the reader is familiar with the terminology used in [RFC4917] (Sastry, V., Leung, K., and A. Patel, “Mobile IPv4 Message String Extension,” June 2007.), [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). In addition, this document frequently uses the following terms:

Notification Message A message from a mobility agent to a MN or other mobility agent to asynchronously notify it about an event that is relevant to the mobility service it is currently providing.

Generic Notification Message A Notification Message in the context of Mobile IPv4 with a well-defined envelope format and extensibility, and with certain limitations on how extensions may be defined and used, but otherwise generally available for notification purposes within the Mobile IPv4 protocol. Abbreviated 'GNM' in this document.

Generic Notification Acknowledgement Message An acknowledgement of a received Generic Notification Message. Abbreviated 'GNAM' 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, [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

3. Notification Message - Usage Scenarios

TOC

3.1. Notification Message - Examples

TOC

The simplest usage scenario for a notification message is one where the notification has no semantic meaning within the protocol; it is only carrying a message which can be displayed to a user or an operator (depending on which is the receiving entity -- see more on this below, in Section 3.2 (Notification Message - Topology)). Examples of such usage is messages from operator to user about billing or service

related events ("You have used nearly all of your prepaid quota; there is only XX MB left -- please purchase further service if you are going to need it."; or "You have now used data transfer services for the amount of $XXX since your last bill; this is above the notification threshold for your account.") or messages about service interruptions, and more. These examples are all supported by the use of the Mobile IPv4 Generic Notification Message together with the Message String Extension, as defined in this document.

There are also other examples, which cannot be implemented solely using the messages and extensions defined in this document. Some of these are described briefly below, and covered slightly more extensively in Section 5 (Future Extensibility).

One example of an application of an extended Generic Notification Message is that during handover between CDMA 2000 1x EV-DO and Wireless LAN, the PPP resource on the CDMA side has to be removed on the FA (PDSN) to avoid over-charging subscribers. To address this, the Registration Revocation Message was defined in [RFC3543] (Glass, S. and M. Chandra, “Registration Revocation in Mobile IPv4,” August 2003.), but it would have been preferable to have had it defined as a separate message (i.e., the Generic Notification Message) with a Registration Revocation extension.

Other applications are HA switch over (before HA decide to go off-line it would like to notify the MNs to register with another candidate HA), NEMO prefix changes (MN is notified by HA about NEMO prefix changes and service or billing related events, which is an operational requirement), Load balancing (HA wants to move some of the registered MNs to other HAs), Service Termination (due to end of prepaid time), and Service Interruption (due to system maintenance).

3.2. Notification Message - Topology

TOC

There are several scenarios where a mobility agent could initiate notification events. Some of these are described in the following Sections.

3.2.1. Notification Message between a Home Agent and a Mobile Node

TOC

TOC

3.2.1.1. Mobile Registered using a Foreign Agent Care-of Address

In this case, the HA cannot directly notify the MN, but must send the notification via the FA, vice versa.

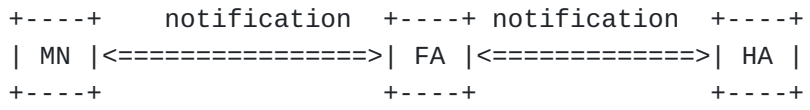


Figure 1: HA notifies MN or MN notifies HA through FA

3.2.1.2. Mobile Registered using a Co-located Care-of Address

TOC

In this case, the MN has registered with the home agent directly, so the notification message can go directly to the MN.
The notification mechanism as specified here does not support the case of Co-located CoA mode with registration through a FA (due to the 'R' bit being set in the FA's advertisement messages).

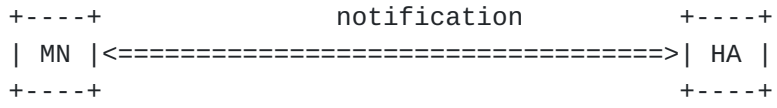


Figure 2: HA directly notifies MN or MN directly notifies HA

3.2.2. Notification Message between a Foreign Agent and a Mobile Node

TOC

There are two cases where a FA may send notification messages to a MN, one where it is relaying a message, the other where the notification is triggered by a message from another network entity, for example a AAA

node(notification messages between a AAA entity and the FA could be based on RADIUS or Diameter, but this is out of scope for this document). If the notification is initiated by a FA, the FA may need to also notify the HA about the event.

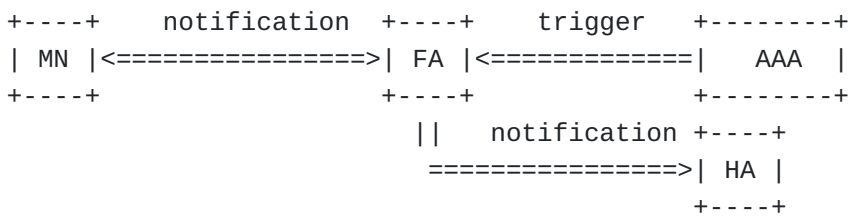


Figure 3: FA notifies MN

3.2.3. Notification Message between a Home Agent and a Foreign Agent

TOC

The HA may also need to send a notification to the FA, but not to the MN, The FA may also need to send a notification to the HA, as illustrated below:

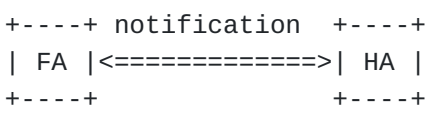


Figure 4: HA notifies FA or FA notifies HA

4. Generic Notification Message and Considerations

TOC

This section describes in detail the Generic Notification Message (GNM), Generic Notification Acknowledgement Message (GNAM), and some

considerations related to the handling of these messages in the MN, FA and HA.
The MN and HA MUST maintain the following information, FA also needs to maintain both the HA's and MN's direction the below information:

- the IP source address of the Registration Request/Reply

- the IP destination address of the Registration Request/Reply

- the UDP source port of the Registration Request/Reply

- the UDP destination port of the Registration Request/Reply

The sending node always sends the GNM message following the same procedure for sending Registration Request as in Section 3.3 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) and the receiving node follows the same procedure for Registration Reply as in Section 3.4. of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) when sending GNAM.

4.1. Generic Notification Message

TOC

A GNM is sent by a mobility agent to inform another mobility agent, or a MN, of MIP-related information in the form of a Message String Extension [RFC4917] (Sastry, V., Leung, K., and A. Patel, “Mobile IPv4 Message String Extension,” June 2007.). These messages MUST use the same IP and UDP headers as any previous Registration Request(RRQ) or Reply (RRP) message to the same entity. This would support NAT traversal and ensure same security association used for GNM/GNAM and RRQ/RRP. The GNM is defined as follows:
IP Fields:

Source Address Typically copied from the destination address of the last Registration Reply/Request message that the agent received from the agent to which it is sending the GNM.

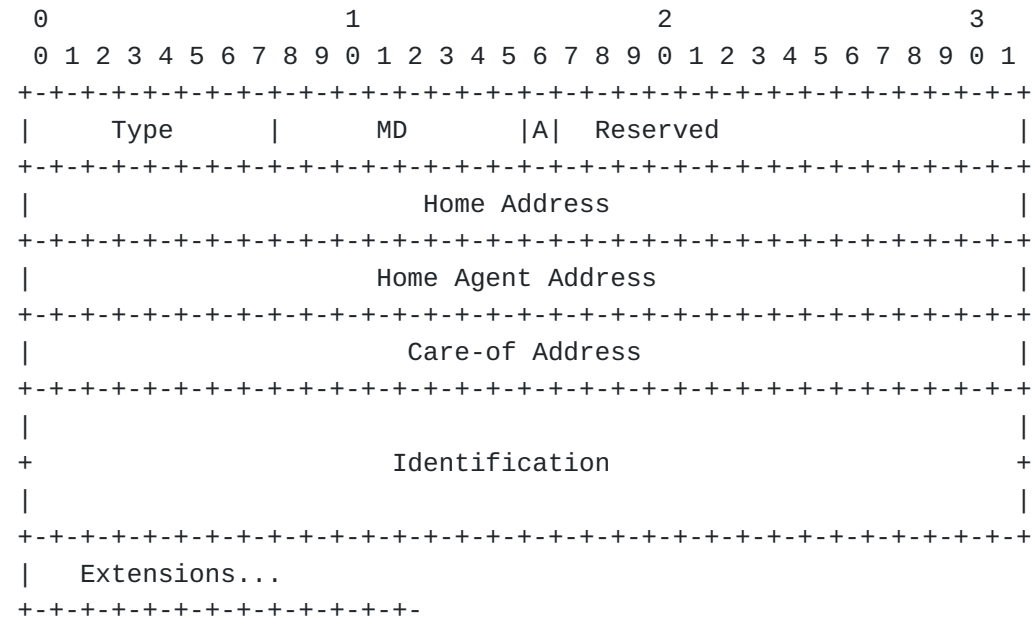
Destination Address Copied from the source address of the last Registration Reply/Request message that the agent received from the agent to which it is sending the GNM.

UDP Fields:

Source Port
: Typically copied from the destination port of the last Registration Reply/Request message that the agent received from the agent to which it is sending the GNM.

Destination Port Copied from the source port of the last Registration Reply/Request message that the agent received from the agent to which it is sending the GNM.

The UDP header is followed by the Mobile IP fields shown below:



Type (To be assigned by IANA)
MD: Message Direction

This memo defines the semantics of the following MD field value:

0 -- Message sent by the HA to the MN

1 -- Message sent by the HA to the FA

2 -- Message sent by the MN to the HA

3 -- Message sent by the MN to the FA

4 -- Message sent by the FA to the MN

5 -- Message sent by the FA to the HA

A

> This bit indicates whether the notification message MUST be acknowledged by the recipient. If "A" bit has been set during the message, but the sender doesn't receive any acknowledgement message, then the sender will have to re-send the notification message again.
>
> Set to "1" to indicate that acknowledgement is REQUIRED.
>
> Set to "0" to indicate that acknowledgement is OPTIONAL.

Reserved

> MUST be sent as 0, and ignored when received.

Home Address

> The home IP address of the mobile node.

Home Agent Address

> The IP address of the mobile node's HA.

Care-of Address

> The mobile node's care-of address, either the Co-located Care-of Address or the foreign agent care-of address.

Identification

> A 64-bit number, constructed by the sender, used for matching GNM with GNAM, and for protecting against replay attacks of notification messages. See Section 7.1.1 (Replay Protection using Timestamps) and Section 7.1.2 (Replay Protection using Nonces) for more on the use of timestamps and nonces in this field. Support for the use of timestamps is REQUIRED and support for nonces is OPTIONAL.

Extensions

> The fixed portion of the GNM is followed by one or more extensions which may be used with this message, and by one or more authentication extensions as defined in Section 3.5 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
>
> Apart from the Authentication Extensions mentioned below, only one extension is defined in this document as permitted for use with the GNM: the Message String Extension defined in [RFC4917] (Sastry, V., Leung, K., and A. Patel, “Mobile IPv4 Message String Extension,” June 2007.).
>
> This document requires the MN-HA Authentication Extension (AE) to be used when this message is sent between the MN and the HA; MN-FA AE

and FA-HA AE are OPTIONAL. This document also requires the use of the MN-FA AE when this message is sent between the MN and the FA; where the MN-HA AE and FA-HA AE are not needed. This document finally require the use of the FA-HA AE when this message is sent between the FA and the HA, and the MN-HA AE and MN-FA AE are not needed. This could be determined based on the "MD" value.
See Sections 3.6.1.3 and 3.7.2.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) for the rules on the order of these extensions as they appear in Mobile IPv4 RRQ and RRP messages. The same rules are applicable to GNM and GNAM.

4.2. Generic Notification Acknowledgment Message

TOC

A GNAM is sent by mobility agents or MNs to indicate the successful receipt of a GNM.
IP Fields:

Source Address Typically copied from the destination address of the GNM to which the agent is replying.

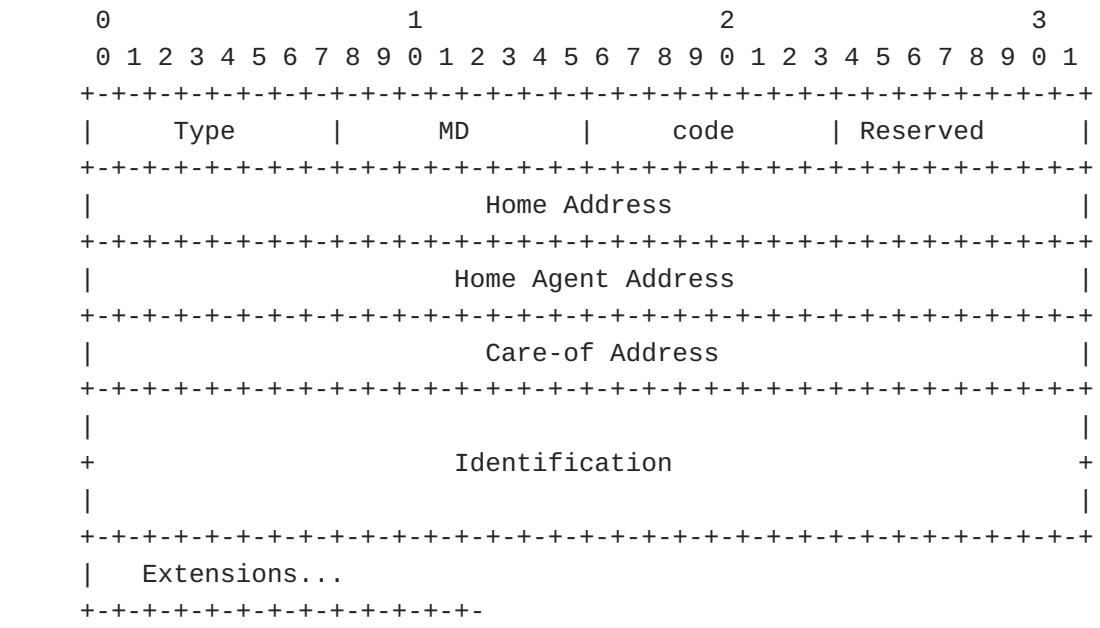
Destination Address Copied from the source address of the GNM to which the agent is replying.

UDP Fields:

Source Port Copied from the destination port of the corresponding GNM.

Destination Port Copied from the source port of the corresponding GNM.

The UDP header is followed by the Mobile IP fields shown below:



Type (To be assigned by IANA)
MD: Message Direction

> This memo defines the semantics of the following MD field value:
>
> 0 -- Message sent by the HA to the MN
>
> 1 -- Message sent by the HA to the FA
>
> 2 -- Message sent by the MN to the HA
>
> 3 -- Message sent by the MN to the FA
>
> 4 -- Message sent by the FA to the MN
>
> 5 -- Message sent by the FA to the HA

code

> A value indicating the result of the GNM. See below for a list of currently defined Code values.

Notification successful

> 0 -- notification accepted

Notification denied by the HA

> 128 -- reason unspecified

129 -- administratively prohibited

130 -- insufficient resources

131 -- mobile node failed authentication

132 -- foreign agent failed authentication

133 -- notification Identification mismatch

Notification denied by the FA

64 -- reason unspecified

65 -- administratively prohibited

66 -- insufficient resources

67 -- mobile node failed authentication

68 -- home agent failed authentication

69 -- notification Identification mismatch

Notification denied by the mobile node

192 -- reason unspecified

193 -- administratively prohibited

194 -- insufficient resources

195 -- foreign agent failed authentication

196 -- home agent failed authentication

197 -- notification Identification mismatch

Home Address

The home IP address of the mobile node.

Home Agent Address

The IP address of the sender's home agent.

Care-of Address

The mobile node's care-of address, either the Co-located Care-of Address or the foreign agent care-of address.

Identification

> A 64-bit number used for matching GNM message with GNAM message and for protecting against replay attacks of registration messages. See Section 7.1.1 (Replay Protection using Timestamps) and Section 7.1.2 (Replay Protection using Nonces) for more on the use of timestamps and nonces in this field. Support for the use of timestamps is REQUIRED and support for nonces is OPTIONAL. The value is based on the Identification field from the GNM message from the sender, and on the style of replay protection used in the security context between the sender and its receiver (defined by the mobility security association between them, and SPI value in the authorization-enabling extension).

Extensions

> The fixed portion of the GNAM is followed by one or more extensions which may be used with this message, and by one or more authentication extensions as defined in Section 3.5 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
>
> This document REQUIRES the MN-HA Authentication Extension (AE) to be used when this message is sent between the MN and the HA; MN-FA AE and FA-HA AE are OPTIONAL. This document also requires the use of the MN-FA AE when this message is sent between the MN and the FA; where the MN-HA AE and FA-HA AE are not needed. This document finally requires the use of the FA-HA AE when this message is sent between the FA and the HA, and the MN-HA AE and MN-FA AE are not needed. This could be determined based on the "MD" value.
> See Sections 3.6.1.3 and 3.7.2.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) for the rules on the order of these extensions as they appear in Mobile IPv4 RRQ and RRP messages. The same rules are applicable to GNM and GNAM.

4.3. Notification Retransmission

TOC

If "A" flag has been set during the GNM message, but the sender doesn't receive any GNAM message within a reasonable time, then another GNM will be retransmitted. When timestamps are used, a new registration Identification is chosen for each retransmission; Thus it counts as a new GNM. When nonces are used, the unanswered GNM message is retransmitted unchanged; thus the retransmission does not count as a new GNM (Section 7.1 (Replay Protection for GNM, GNAM messages)). In this way a retransmission will not require the receiver to re-synchronize with the sender by issuing another nonce in the case in

which the original GNM message (rather than its GNAM message) was lost by the network.
The maximum time until a new GNM message is sent SHOULD be no greater than the requested Lifetime of the last GNM message. The minimum value SHOULD be large enough to account for the size of the messages, twice the round trip time for transmission to the receiver, and at least an additional 100 milliseconds to allow for processing the messages before responding. The round trip time for transmission to the receiver will be at least as large as the time REQUIRED to transmit the messages at the link speed of the sender's current point of attachment. Some circuits add another 200 milliseconds of satellite delay in the total round trip time to the receiver. The minimum time between GNM MUST NOT be less than 1 second. Each successive retransmission timeout period SHOULD be at least twice the previous period, as long as that is less than the maximum as specified above.

4.4. General Implementation Considerations

TOC

Implementations of this specifications should provide support for management of the various settings related to the notification messages. In particular, it should be possible to do the following:

> * List the notification messages supported
>
> * Show enabled/disabled status for notification message support, overall and in detail.
>
> * Show the value of the maximum and minimum retransmission times.
>
> * Enable and disable notification support entirely.
>
> * Enable and disable the individual notification messages supported.
>
> * Set the value of the maximum and minimum retransmission times described in Section 4.3 (Notification Retransmission).

4.5. Mobile Node Considerations

TOC

It is possible that the MN MAY receive a GNM from a FA or HA. Both in the case of FA-CoA and Co-located CoA, the MN MAY reply with a GNAM based on the "A" flag in the GNM message.

4.5.1. Receiving Generic Notification Messages

TOC

When the MN is using FA-CoA and receives a Notification message, if the "MD" value is 0, it means that the notification message came from the HA. If the "MD" value is 4, the notification came from the FA.
If this notification message came from a FA and the MN accepts the FA's GNM, then it will process the notification extension according to the specific rules for that extension.
The MN MUST check for the presence of an authorization-enabling extension, and perform the indicated authentication. Exactly one authorization-enabling extension MUST be present in the GNM, if this message came from a FA, then MN-FA AE MUST be present. If no MN-FA AE is found, or if more than one MN-FA AE is found, or if the Authenticator is invalid, then the MN MUST reject the GNM and MAY send a GNAM to the FA with Code 195, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The MN MUST do no further processing with such a notification, though it SHOULD log the error as a security exception.
The MN MUST check that the Identification field is correct using the context selected by the SPI within mandatory authentication extension like MN-FA AE or MN-HA AE. See Section 7.1 (Replay Protection for GNM, GNAM messages) for a description of how this is performed. If incorrect, the MN MUST reject the GNM and MAY send a GNAM to the initiator with Code 197, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The MN MUST do no further processing with such a notification, though it SHOULD log the error as a security exception.
The MN MUST also check that the extensions present in the Generic Notification Message are permitted for use with the GNM. If not, the MN MUST silently discard the message. It MUST NOT do any further processing with such a notification, though it SHOULD log the error.
After this, the MN MAY reply GNAM back to the FA. If the "A" flag is set in the GNM, then the MN MUST send the GNAM.
If this notification message came from the HA, relayed by the FA, or is a Co-located CoA, then the MN-HA AE MUST be checked and the MN MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, then the MN MUST reject the GNM and MAY send a GNAM to the initiator with Code 196, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The MN MUST do no further processing with such a notification, though it SHOULD log the error as a security exception.
If the MN accepts the HA's GNM, then it will process it according to the specific rules for that extension. After that, the MN MAY reply with a GNAM with Code 0 back to the HA based on the "A" flag in the GNM.

4.5.2. Sending Generic Notification Acknowledgement Messages

TOC

Both in the case of a Co-located CoA and FA-CoA, the MN MAY reply with a GNAM based on the "A" flag in the GNM as follows:
If the GNM was initiated from the FA to the MN ("MD" value is set to 4), then MN-FA AE MUST be the last extension in order to protect all other non-authentication extensions as defined in Section 3.5.3 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
In the case of a FA-CoA, the source address is the MN's address, the destination address is the FA's address.
The Code field of the GNAM is chosen in accordance with the rules specified in Section 4.2 (Generic Notification Acknowledgment Message).
When replying to an accepted notification, a MN SHOULD respond with Code 0.
There are a number of reasons the MN might reject a notification such as administrative in nature returning a GNAM with a code of 193, similarly and provides the Code value 192 or 194 for the unspecified reason and insufficient resources.
If the GNM was initiated from the HA to the MN ("MD" value is set to 0) and in the case of Co-located CoA, then MN-HA AE MUST be the last extension in order to protect all other non-authentication extensions as defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.)
In the case of a FA-CoA, the source address is the MN's HoA address and the destination address is the FA's address ("MD" value is set to 2), the ordering of the extension is: any non-authentication Extensions used only by the HA, followed by the MN-HA AE defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.), followed by any non-authentication Extensions used only by the FA, followed by the MN-FA AE defined in Section 3.5.3 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).

4.5.3. Sending Generic Notification Messages

TOC

The MN may either send a GNM to notify the FA or HA.
If the message is sent to the FA, then the source address is the MN's address, and the destination address is the FA's address
If the FA is the target of this notification message, then the "MD" value is set to 3, MN-FA AE MUST be the last extension in order to protect all other non-authentication extensions. Computing Authentication Extension Value is the same as Section 3.5.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
If the FA is working only as a relay agent, then the "MD" value is set to 2, and the ordering of the extension is: the notification extension, followed by any non-authentication extension expected to be used by HA,

followed by MN-HA AE defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.), followed by any non-authentication Extensions used only by the FA, followed by The MN-FA AE defined in Section 3.5.3 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). Computing Authentication Extension Value is the same as Section 3.5.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
In the case of a Co-located CoA, the MN MAY send a notification message directly to the HA if it needs to be notified. The "MD" value is set to 2, and the ordering of the extension is: the notification extension, followed by any non-authentication extension expected to be used by HA, followed by MN-HA AE defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
The MN chooses the Identification field in accordance with the style of replay protection it uses with its HA. This is part of the mobility security association the MN shares with its HA. See Section 7.1 (Replay Protection for GNM, GNAM messages) for the method by which the MN computes the Identification field.

4.5.4. Receiving Generic Notification Acknowledgement Messages

TOC

In the case of a FA-CoA, if the MN receives this message, and the "MD" value is set to 0, it means that the GNAM came from HA
If the "MD" value is set to 4, then the MN-FA AE MUST be checked, and the MN MUST check the Authenticator value in the Extension. If no MN-FA AE is found, or if more than one MN-FA AE is found, or if the Authenticator is invalid, then the MN MUST silently discard the GNAM. In addition, the low-order 32 bits of the Identification field in the GNAM MUST be compared to the low-order 32 bits of the Identification field in the most recent GNM sent to the replying agent. If they do not match, then the GNAM MUST be silently discarded.
If the "MD" value is set to 0, then the MN-HA AE MUST be checked, and the MN MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, then the MN MUST silently discard the GNAM.
If the MN accepted this message, then the MN MAY also process it based on the notification event.
In the case of a Co-located CoA, if the MN received this message, then the MN-HA AE MUST be checked, and the MN MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, then the MN MUST silently discard the Notification Acknowledgement message.

TOC

4.6. Foreign Agent Consideration

The FA may initiate a GNM to the MN or the HA. Additionally, the FA also relays GNM and GNAM messages between the MN and its HA as long as there is an active binding for the MN at the FA.

4.6.1. Receiving Generic Notification Messages

TOC

If the FA receives a GNM, and the "MD" value is set to 0, then it means that the HA is asking the FA to relay the message to the MN. If the "MD" value is set to 1, then it means that the target of the notification is the FA. If the "MD" value is set to 2, then it means that the MN is asking the FA to relay the message to the HA. If the "MD" value is set to 3, then it means that the notification came from the MN to the FA.
If the "MD" value is set to 0, then the FA MAY validate the FA-HA AE if present. If the FA-HA AE is invalid, then all extensions between the HA-MN AE and the HA-FA AE MUST be removed, FA SHOULD relay the GNM to the MN's home address as specified in the Home Address field of the GNM, MN will eventually validate the MN-HA AE to ensure that all information sent to the MN is integrity protected. If the FA-HA AE is valid, FA MUST relay the GNM to the MN's home address as specified in the Home Address field of the GNM. The FA MUST NOT modify any of the fields beginning with the fixed portion of the GNM through the MN-HA AE or other authentication extension supplied by the HA as an authorization-enabling extension for the MN.
Furthermore, the FA MUST process and remove any extensions following the MN-HA AE. If the FA shares a mobility security association with the MN, the FA MAY append any of its own non-authentication extensions which of relevance to the MN. In this case, the FA MUST append the MN-FA AE after these non-authentication extensions.
If the "MD" value is set to 1, the FA-HA AE MUST be checked, and the FA MUST check the Authenticator value in the Extension. If no FA-HA AE is found, or if more than one FA-HA AE is found, or if the Authenticator is invalid, the FA MUST reject the GNM and MAY send a GNAM to the HA with Code 68, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The FA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception. The FA MUST check that the Identification field is correct using the context selected by the SPI within mandatory FA-HA AE. See Section 7.1 (Replay Protection for GNM, GNAM messages) for a description of how this is performed. If incorrect, the FA MUST reject the GNM and MAY send a GNAM to the initiator with Code 69, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The FA MUST do no further

processing with such a notification, though it SHOULD log the error as a security exception.
The FA MUST also check that the extensions present in the Generic Notification Message are permitted for use with the GNM. If not, the FA MUST silently discard the message. It MUST NOT do any further processing with such a notification, though it SHOULD log the error.
If FA accepts the HA's GNM, it will process it based on the specific rules for that extension. The FA MAY then reply with a GNAM with Code 0 back to the MN based on the "A" flag in the GNM.
In the case of a FA-CoA and if the "MD" value is set to 2, if the FA received this message, and if the MN-FA AE is present, the MN-FA AE MUST be checked, and the FA MUST check the Authenticator value in the Extension. If no MN-FA AE is found, or if more than one MN-FA AE is found, or if the Authenticator is invalid, the FA MUST silently discard the GNM message. If MN-FA is valid, FA MUST relay the GNM to the HA's address as specified in the Home Agent Address field of the GNM, HA will eventually validate the MN-HA AE to ensure that all information sent to the HA is integrity protected. The FA MUST NOT modify any of the fields beginning with the fixed portion of the GNM through the MN-HA AE or other authentication extension supplied by the MN as an authorization-enabling extension for the HA.
Furthermore, the FA MUST process and remove any Extensions following the MN-HA AE, and MAY append any of its own non-authentication Extensions of relevance to the HA if applicable, and MUST append the FA-HA AE, if the FA shares a mobility security association with the HA.
If the "MD" value is set to 3, the MN-FA AE MUST be checked, and the FA MUST check the Authenticator value in the Extension which is the same as the Section 3.7.2.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). If no MN-FA AE is found, or if more than one MN-FA AE is found, or if the Authenticator is invalid, the FA MUST reject the GNM and MAY send a GNAM to the MN with Code 67, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The FA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception.
The FA MUST check that the Identification field is correct using the context selected by the SPI within mandatory MN-FA AE. See Section 7.1 (Replay Protection for GNM, GNAM messages) for a description of how this is performed. If incorrect, the FA MUST reject the GNM and MAY send a GNAM to the initiator with Code 69, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The FA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception.
If FA accepts the MN's GNM, it will process it based on the specific rules for that extension. The FA MAY then reply with a GNAM with Code 0 back to the MN based on the "A" flag in the GNM.

4.6.2. Sending Generic Notification Acknowledgement Messages

TOC

The FA may need to either relay a GNAM message between the MN and the HA or send one as a response to a GNM message that was sent to it. In both cases, the GNAM message is defined as follows:
The source address is the FA address, the destination address is HA's or MN's home address.
The Code field of the GNAM is chosen in accordance with the rules specified in Section 4.2 (Generic Notification Acknowledgment Message).
When replying to an accepted notification, a FA SHOULD respond with Code 0.
There are a number of reasons the FA might reject a notification such as administrative in nature returning a GNAM with a code of 65, similarly and provides the Code value 64 or 66 for the unspecified reason and insufficient resources.
If the FA is only relaying this message to the HA, the FA MUST NOT modify any of the fields beginning with the fixed portion of the GNAM through the including the MN-HA AE or other authentication extension supplied by the MN as an authorization-enabling extension for the MN. Furthermore, the foreign agent MUST process and remove any Extensions following the MN-HA AE. If the FA shares a mobility security association with the HA, the FA MAY append any of its own non-authentication extensions which of relevance to the HA, In this case the FA MUST append the FA-HA AE after these non-authentication extensions.
If the notification message is from the HA to the FA then the "MD" value is set to 5 and the ordering of the extension is: any non-authentication Extensions used only by the FA, followed by The FA-HA AE defined in Section 3.5.4 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
If the notification message is from the MN to the FA then the "MD" value is set to 4 and the ordering of the extension is: any non-authentication Extensions used only by the FA, followed by The MN-FA AE defined in Section 3.5.3 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).

4.6.3. Sending Generic Notification Messages

TOC

If the FA is initiating a notification to the MN using the GNM, it MAY also notify the HA as well.
In the message to the MN, the source address is the FA address, the destination address is the MN's address, the "MD" value is set to 4, and the ordering of the extension is: the notification extension, followed by any non-authentication Extensions used only by the MN, followed by The MN-FA AE defined in Section 3.5.3 of [RFC3344]

(Perkins, C., “IP Mobility Support for IPv4,” August 2002.). Computing Authentication Extension Value is the same as Section 3.5.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) except the payload is the notification other than registration.
In the message to the HA, the source address is the FA's address, the destination address is the HA's address (the "MD" value is set to 5), and the ordering of the extension is: notification extension, followed by any non-authentication Extensions used only by the HA, followed by The FA-HA AE defined in Section 3.5.4 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). Computing Authentication Extension Value is the same as Section 3.5.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) except the payload is the notification other than registration.

4.6.4. Receiving Generic Notification Acknowledgement Messages

TOC

In the case of a FA-CoA, if the FA receives this message, and the "MD" value is set to 3, it means that the notification acknowledgement message came from the MN, otherwise it came from the HA.
If the "MD" value is set to 1, the FA-HA AE MUST be checked, and the FA MUST check the Authenticator value in the Extension. If no FA-HA AE is found, or if more than one FA-HA AE is found, or if the Authenticator is invalid, the FA MUST silently discard the Notification Acknowledgement message. If the FA accepted this message, the FA MAY also process it based on the notification event.
If the "MD" value is set to 3, if the MN-FA AE is present, it MUST be checked, and the FA MUST check the Authenticator value in the Extension. If no MN-FA AE is found, or if more than one MN-FA AE is found, or if the Authenticator is invalid, the FA MUST silently discard the GNAM message. If the FA accepted this message, the FA MAY also process it based on the notification event.
In the case of a FA-CoA and if the "MD" value is set to 2, if the FA received this message, and if the MN-FA AE is present, the MN-FA AE MUST be checked, and the FA MUST check the Authenticator value in the Extension. If no MN-FA AE is found, or if more than one MN-FA AE is found, or if the Authenticator is invalid, the FA MUST silently discard the GNAM message. If FA accepted the MN's GNAM message, it MUST relay this message to the HA. The FA MUST NOT modify any of the fields beginning with the fixed portion of the GNAM message through the including the MN-HA AE or other authentication extension supplied by the HA as an authorization-enabling extension for the MN. Furthermore, the FA MUST process and remove any Extensions following the MN-HA AE and MAY append any of its own non-authentication Extensions of relevance to the HA, if applicable, and MUST append the FA-HA AE, if the FA shares a mobility security association with the HA.

4.7. Home Agent Consideration

TOC

The HA MAY initiate a GNM message to both the mobile node and FA, and it also MAY receive a GNAM message from both the FA and MN. The HA also MAY receive a GNM message from the FA, but only when there is a binding for a MN. If the HA receives a GNM from a FA and there is no corresponding MN registration, the HA SHOULD drop the GNM message.

4.7.1. Sending Generic Notification Messages

TOC

In the case of a FA-CoA, the HA may either send a GNM to notify the FA, or have the FA relay the GNM to the MN if the MN needs to be notified. If the message is from the HA to the FA, the source address is the HA's address, and the destination address is the FA's address
If the FA is working only as a relay agent, the "MD" value is set to 0, and the ordering of the extension is: the notification extension, followed by any non-authentication extension expected to be used by MN, followed by MN-HA AE defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.), followed by any non-authentication Extensions used only by the FA, followed by The FA-HA AE defined in Section 3.5.4 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). Computing Authentication Extension Value is the same as Section 3.5.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
If the FA is the target of this notification message, then the "MD" value is set to 1, and the ordering of the extension is: the notification extension, followed by any non-authentication Extensions used only by the FA, followed by The FA-HA AE defined in Section 3.5.4 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). Computing Authentication Extension Value is the same as Section 3.5.1 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
In the case of a Co-located CoA, the HA MAY send a notification message directly to the MN if it needs to be notified. The "MD" value is set to 0, and the ordering of the extension is: the notification extension, followed by any non-authentication extension expected to be used by MN, followed by MN-HA AE defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).

TOC

4.7.2. Receiving Generic Notification Acknowledgement Messages

In the case of a FA-CoA, if the HA receives this message, and the "MD" value is set to 2, it means that the GNAM message came from MN.
If the "MD" value is set to 5, and the HA accepted this message, the HA MAY also process it based on the notification event. The FA-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If no FA-HA AE is found, or if more than one FA-HA AE is found, or if the Authenticator is invalid, the HA MUST silently discard the GNAM message.
If the "MD" value is set to 2, in the case of a FA-CoA, and if FA-HA AE is present, the FA-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If more than one FA-HA AE is found, or if the Authenticator is invalid, the HA MUST silently discard the GNAM message. Anyway, MN-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, the HA MUST silently discard the GNAM. If the HA accepted this message, the HA MAY also process it based on the notification event.
If the "MD" value is set to 2, in the case of a Co-located CoA, MN-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, the HA MUST silently discard the GNAM. If the HA accepted this message, the HA MAY also process it based on the notification event.

4.7.3. Receiving Generic Notification Messages

TOC

The HA MAY receive a GNM message sent from the FA. When the HA receives this message, if the the "MD" value is set to 5, this message came from FA. FA-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If no FA-HA AE is found, or if more than one FA-HA AE is found, or if the Authenticator is invalid, the HA MUST reject the GNM and MAY send a GNAM to the FA with Code 132, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The HA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception.
The HA MUST check that the Identification field is correct using the context selected by the SPI within mandatory authentication extension like MN-HA AE or FA-HA AE. See Section 7.1 (Replay Protection for GNM, GNAM messages) for a description of how this is performed. If incorrect, the HA MUST reject the GNM and MAY send a GNAM to the initiator with Code 133, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection

for GNM, GNAM messages). The HA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception. If HA accepts the FA's GNM message, it will process it based on the notification extension. Furthermore, the HA MAY reply with a GNAM message with Code 0 back to the FA based on the "A" flag in the GNM message.

If the the "MD" value is set to 2, this message come from MN, in the case of FA-COA, if FA-HA AE is present, it MUST be checked, and the HA MUST check the Authenticator value in the Extension. If more than one FA-HA AE Extension is found, or if the Authenticator is invalid, the HA MUST reject the GNM and MAY send a GNAM to the FA with Code 132, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The HA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception. And MN-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, the HA MUST reject the GNM and MAY send a GNAM to the MN with Code 131, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The HA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception. If HA accepts the MN's GNM message, it will process it based on the notification extension. Furthermore, the HA MAY reply with a GNAM message back to the MN with Code 0 based on the "A" flag in the GNM message.

If the the "MD" value is set to 2, in the case of a Co-located CoA, the MN-HA AE MUST be checked, and the HA MUST check the Authenticator value in the Extension. If no MN-HA AE is found, or if more than one MN-HA AE is found, or if the Authenticator is invalid, the HA MUST reject the GNM and MAY send a GNAM to the MN with Code 131, including an Identification field computed in accordance with the rules specified in Section 7.1 (Replay Protection for GNM, GNAM messages). The HA MUST do no further processing with such a notification, though it SHOULD log the error as a security exception. If HA accepts the MN's GNM message, it will process it based on the notification extension. Furthermore, the HA MAY reply with a GNAM message back to the MN with Code 0 based on the "A" flag in the GNM message.

The HA MUST also check that the extensions present in the Generic Notification Message are permitted for use with the GNM. If not, the HA MUST silently discard the message. It MUST NOT do any further processing with such a notification, though it SHOULD log the error.

TOC

4.7.4. Sending Generic Notification Acknowledgement Messages

If the GNM message came from the FA only, and if the "A" flag is set in the GNM message, then the HA MUST send a GNAM message. The message is as follows: The source address is HA's address, the destination address is the FA's address, the "MD" value is set to 1. The ordering of the extension is: any non-authentication Extensions used only by the FA, followed by The Foreign-Home Authentication extension defined in Section 3.5.4 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
The Code field of the GNAM is chosen in accordance with the rules specified in Section 4.2 (Generic Notification Acknowledgment Message).
When replying to an accepted GNM, a MN SHOULD respond with Code 0.
If the GNM message came from the MN, and if the "A" flag is set in the GNM message, then the HA MUST send a GNAM message. The message is as follows: The source address is HA's address, the destination address is the FA's address, the "MD" value is set to 0. The ordering of the extension is: any non-authentication Extensions used only by the MN, followed by the MN-HA AE defined in Section 3.5.2 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.), optionally followed by any non-authentication Extensions used only by the FA, optionally followed by The MN-FA AE defined in Section 3.5.3 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.)

---

5. Future Extensibility

TOC

This document defines the Generic Notification Message used with the Message String Extension [RFC4917] (Sastry, V., Leung, K., and A. Patel, “Mobile IPv4 Message String Extension,” June 2007.).
It is however possible to define new notification-related extensions for use with the Generic Notification Message, for cases where the notification is intended to have a semantic content and is intended for the HA, FA or MN, rather than for the user.

5.1. Examples of Possible Extensions

TOC

One example of such usage, which would have been defined in this document if it hadn't already been defined as a separate message is the Registration Revocation Message (Glass, S. and M. Chandra, “Registration Revocation in Mobile IPv4,” August 2003.) [RFC3543]. This is a message sent from the HA to FA(s) or MN to notify the receiving node that a currently active registration is being revoked. The use case for this is clearly laid out in [RFC3543] (Glass, S. and M. Chandra, “Registration Revocation in Mobile IPv4,” August 2003.).

Another example would be managed maintenance switch-over between HA instances, where a HA due to go down for maintenance could direct the MNs registered with it to re-register with another specified HA. Such a message could also be used for managed load balancing. There is currently no support for such forced switch-over in the Mobile IPv4 protocol.

Yet another example is when the prefix set handled by an MIPv4 NEMO [RFC5177] (Leung, K., Dommety, G., Narayanan, V., and A. Petrescu, "Network Mobility (NEMO) Extensions for Mobile IPv4," April 2008.) HA changes; to ensure proper routing, the mobile router needs to be notified about the change so that its internal routing rules may be updated.

One final example is home network changes which require host configuration changes, for instance a change of address for the DNS server or another network server; again this is a case where the HA would want to notify the MN of the change, so that service interruptions can be avoided.

5.2. Extension Specification

TOC

In order to avoid making the MIPv4 Generic Notification Message a generic protocol extension mechanism by which new protocol mechanisms could be implemented without appropriate discussion and approval, any new extensions which are to be used with the Generic Notification Message must be registered with IANA, where registration is limited by the 'RFC Required' policy defined in [RFC5226] (Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," May 2008.)

If additional extensions are specified for use with the Generic Notification Message, the practice exemplified in [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.) and related specification should be followed. Generally it has not been necessary so far to provide versioning support within individual extensions; in a few cases it has been necessary to define new extensions with new extension numbers where a generalizations of a pre-existing extension has been needed, and with the current rate of extension number consumption that seems to be an acceptable approach.

If at some point extensions are specified for use with the Generic Notification Message which overlap pre-existing notification messages, the authors of the specification should consider providing a method to flag which notification messages are supported, and which notification message usage is requested, in a manner similar to the way tunnelling method capabilities and usage requests are flagged in the Mobile IPv4 Base Specification (Perkins, C., "IP Mobility Support for IPv4," August 2002.) [RFC3344].

Encoded in the extension number of Mobile IPv4 extensions is the notion of 'skippable' and 'not skippable' extensions; see Section 1.8 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). This notion is also applicable when extensions are used with the Generic Notification Message: It is not required that a receiver understand a skippable extension, but a non-skippable extension needs to be handled according to Section 1.8 of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) (i.e., the message must be silently discarded if the extension is not recognized). This document does not specify any change from the Mobile IPv4 Base Specification (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) [RFC3344] in this respect.

---

6. IANA Considerations

TOC

This document defines two new messages, the Generic Notification Message described in Section 4.1 (Generic Notification Message), and the Generic Notification Acknowledgement Message, described in Section 4.2 (Generic Notification Acknowledgment Message). The message numbers for these two message numbers are to be allocated from the same number space used by the Registration Request and Registration Reply messages in [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).

The Generic Notification Message may only carry extensions which are explicitly permitted for use with this message. This document defines 4 extensions which are permitted, in Section 4.1 (Generic Notification Message). IANA must establish a register of Mobile IPv4 extensions which are permitted for use with the Generic Notification Message. Approval of new extensions which are permitted for use with the Generic Notification Message requires that they be defined in an RFC according to the 'RFC Required' policy described in [RFC5226] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” May 2008.).

The Generic Notification Acknowledgement message, specified in Section 4.2 (Generic Notification Acknowledgment Message), has a Code field. The number space for the Code field values is new, and also specified in Section 4.2 (Generic Notification Acknowledgment Message). The Code number space is structured according to whether the notification was successful, or whether the HA denied the notification, or whether FA denied the notification, or whether MN denied the notification, as follows:

0	Success Code
64-69	Error Codes from the FA
128-133	Error Codes from the HA
192-197	Error Codes from the MN

Approval of new Code values require expert review.

---

7. Security Considerations

TOC

This specification operates with the security constraints and requirements of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). This means that when these message is transmitted between the MN and the HA, MN-HA AE is REQUIRED, when this message is transmitted between the MN and the FA, MN-FA AE is REQUIRED, when this message is transmitted between the FA and the HA, FA-HA AE is REQUIRED. It extends the operations of MN, HA and FA defined in [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) to notify each other about some events. The GNM message defined in the specification could carry information that modifies the mobility bindings. Therefore the message MUST be integrity protected. Replay protection MUST also be guaranteed.
RFC 3344 provides replay protection only for registration requests sent by the MN. There is no mechanism for replay protection for messages initiated by a FA or a HA. The 64-bit Identification field specified in this document (Section 4.1 and 4.2) for the GNM message is used to provide replay protection for the notification messages initiated by the FA or HA.

7.1. Replay Protection for GNM, GNAM messages

TOC

The Identification field is used to let the receiving node verify that a GNM has been freshly generated by the sending node, not replayed by an attacker from some previous registration. Two methods are described in this section: timestamps (REQUIRED) and "nonces" (OPTIONAL). All senders and receivers MUST implement timestamp-based replay protection. These nodes MAY also implement nonce-based replay protection
The style of replay protection in effect between any two peer nodes among MN, FA and HA is part of the mobile security association. A sending node and its receiving node MUST agree on which method of replay protection will be used. The interpretation of the Identification field depends on the method of replay protection as described in the subsequent subsections.

Whatever method is used, the low-order 32 bits of the Identification MUST be copied unchanged from the GNM to the GNAM. The receiver uses those bits (and the sender's source address) to match GNAM with corresponding replies. The receiver MUST verify that the low-order 32 bits of any GNAM are identical to the bits it sent in the GNM.
The Identification in a new GNM MUST NOT be the same as in an immediately preceding GNM, and SHOULD NOT repeat while the same security context is being used between the MN and the HA.

7.1.1. Replay Protection using Timestamps

TOC

The basic principle of timestamp replay protection is that the node generating a message inserts the current time of day, and the node receiving the message checks that this timestamp is sufficiently close to its own time of day. Unless specified differently in the security association between the nodes, a default value of 7 seconds MAY be used to limit the time difference. This value SHOULD be greater than 3 seconds. Obviously the two nodes must have adequately synchronized time-of-day clocks. As with any messages, time synchronization messages may be protected against tampering by an authentication mechanism determined by the security context between the two nodes.
In this document, the timestamps are used, the sender MUST set the Identification field to a 64-bit value formatted as specified by the Network Time Protocol (NTP) [RFC5905] (Mills, D., Martin, J., Burbank, J., and W. Kasch, “Network Time Protocol Version 4: Protocol and Algorithms Specification,” June 2010.). The low-order 32 bits of the NTP format represent fractional seconds . Note, however, that when using timestamps, the 64-bit Identification used in a GNM message from the sender MUST be greater than that used in any previous GNM message, as the receiver uses this field also as a sequence number. Without such a sequence number, it would be possible for a delayed duplicate of an earlier GNM message to arrive at the receiver (within the clock synchronization required by the receiver), and thus be applied out of order, mistakenly altering the sender's current status.
Upon receipt of a GNM message with an authorization-enabling extension, the receiver MUST check the Identification field for validity. In order to be valid, the timestamp contained in the Identification field MUST be close enough to the receiver's time of day clock and the timestamp MUST be greater than all previously accepted timestamps for the requesting sender. Time tolerances and re-synchronization details are specific to a particular mobility security association.
If the timestamp is valid, the receiver copies the entire Identification field into the GNAM it returns the GNAM message to the sender. If the timestamp is not valid, the receiver copies only the low-order 32 bits into the GNAM, and supplies the high-order 32 bits from its own time of day. In this latter case, the receiver MUST reject

the registration by returning Code 69/133/197 (identification mismatch) in the GNAM message.
Furthermore, the receiver MUST verify that the low-order 32 bits of the Identification in the GNAM are identical to those in the rejected GNM attempt, before using the high-order bits for clock re-synchronization.

7.1.2. Replay Protection using Nonces

TOC

The basic principle of nonce replay protection is that node A includes a new random number in every message to node B, and checks that node B returns that same number in its next message to node A. Both messages use an authentication code to protect against alteration by an attacker. At the same time node B can send its own nonces in all messages to node A (to be echoed by node A), so that it too can verify that it is receiving fresh messages.
The receiver may be expected to have resources for computing pseudo-random numbers useful as nonces, according to [RFC4086] (Eastlake, D., Schiller, J., and S. Crocker, “Randomness Requirements for Security,” June 2005.). It inserts a new nonce as the high-order 32 bits of the identification field of every GNAM message. The receiver copies the low-order 32 bits of the Identification from the GNM message into the low-order 32 bits of the Identification in the GNAM message. When the sender receives an authenticated GNAM message from the receiver, it saves the high-order 32 bits of the identification for use as the high-order 32 bits of its next GNM message.
The sender is responsible for generating the low-order 32 bits of the Identification in each GNM message. Ideally it should generate its own random nonces. However it may use any expedient method, including duplication of the random value sent by the receiver. The method chosen is of concern only to the sender , because it is the node that checks for valid values in the GNAM message. The high-order and low-order 32 bits of the identification chosen SHOULD both differ from their previous values. The receiver uses a new high-order value and the sender uses a new low-order value for each registration message.
If a GNM message is rejected because of an invalid nonce, the GNAM always provides the sender with a new nonce to be used in the next registration. Thus the nonce protocol is self- synchronizing.

7.2. Non-authentication Extensions Handling in Foreign Agent

TOC

When the FA is relaying the GNM message between the MN and the HA, and if the FA does not share a mobility security association with the MN or HA, all non-authentication extensions between MN and FA, or FA and HA

are not protected; In this case, all non-authentication extensions should be silently discarded.

8. Acknowledgments

TOC

The author appreciate the efforts of Ahmad Muhanna for his detail reviewing of this document and his many contributions to the text of this document. The author also wants to thank Kent Leung, Peng Yang and Peter McCann et al. for their helping developing this document. Thanks to Alexey Melnikov, Sean Turner, Ralph Droms, Charles E. Perkins, Russ Housley, Magnus Westerlund, Lars Eggert, Dan Romascanu, Tim Polk, Amanda Baber, Sebastian Thalanany, and Joseph Salowey's discussion and comments. Thanks to Jari Arkko for each step of this document.

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3344]	Perkins, C., “IP Mobility Support for IPv4,” RFC 3344, August 2002 (TXT).
[RFC3543]	Glass, S. and M. Chandra, “Registration Revocation in Mobile IPv4,” RFC 3543, August 2003 (TXT).
[RFC4086]	Eastlake, D., Schiller, J., and S. Crocker, “Randomness Requirements for Security,” BCP 106, RFC 4086, June 2005 (TXT).
[RFC4917]	Sastry, V., Leung, K., and A. Patel, “Mobile IPv4 Message String Extension,” RFC 4917, June 2007 (TXT).
[RFC5905]	Mills, D., Martin, J., Burbank, J., and W. Kasch, “Network Time Protocol Version 4: Protocol and Algorithms Specification,” RFC 5905, June 2010 (TXT).

9.2. Informative References

TOC

[RFC5177]	Leung, K., Dommety, G., Narayanan, V., and A. Petrescu, “Network Mobility (NEMO) Extensions for Mobile IPv4,” RFC 5177, April 2008 (TXT).

[RFC5226]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 5226, May 2008 (TXT).

Authors' Addresses

TOC

	Hui Deng
	China Mobile
	53A,Xibianmennei Ave.,
	Xuanwu District,
	Beijing 100053
	China
Email:	denghui02@gmail.com
	Henrik Levkowetz
	Netnod
	Franzengatan 5
	S-104 25, Stockholm
	SWEDEN
Email:	henrik@levkowetz.com
	Vijay Devarapalli
	WiChorus
	3590 North First St
	San Jose, CA
	USA
Email:	dvijay@gmail.com
	Sri Gundavelli
	Cisco Systems
	170 W.Tasman Drive
	San Jose, CA 95134
	USA
Email:	sgundave@cisco.com
	Brian Haley
	Hewlett-Packard Company
	110 Spitbrook Road
	Nashua, NH 03062
	USA
Email:	brian.haley@hp.com