

Mipshop Working Group
Internet Draft
Intended status: Standards Track
Expires: January 14, 2009

F. Z. Yousaf
C. Wietfeld
Communication Networks Institute,
Dortmund University of Technology,
Germany.
July 14, 2008

Proactive Bindings for FMIPv6
draft-yousaf-ietf-mipshop-pbfmipv6-01.txt

Status of this Memo

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

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

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

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

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

This Internet-Draft will expire on January 14, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

Usually in FMIPv6, the MN will start the binding process with its home agent and the correspondent nodes after it has attached to NAR. Till the binding is completed, the mobile node continues to receive packets via a reverse tunnel established between PAR and NAR. The duration of this tunnel will depend on the time it takes for the mobile node to complete its binding, till which time the tunnel will

continue to consume buffer and processing resources related to maintaining the tunnel and forwarding packets through this tunnel in both PAR and NAR.

This document specifies an extension to FMIPv6 to enhance its performance, in terms of resource management, by reducing the duration of the tunnel existence. This is achieved by enabling the NAR to act as a proxy for the MN for FMIPv6 handover. Additional message(s) and message options along with modifications to existing FMIPv6 messages and message options and definitions of new messages and message options to achieve the desired functionality is also described in this document.

Table of Contents

1. Requirement notations	3
2. Introduction.....	3
3. Terminology.....	4
4. Protocol Overview.....	6
4.1. Handover Latency in Fast Mobile IPv6.....	6
4.2. Open Issues in FMIPv6.....	7
4.3. Proactive Bindings for FMIPv6 Operation Summary.....	8
4.4. Advantages.....	8
5. Proactive Bindings for FMIPv6 Protocol Details.....	9
5.1. Processing of Proxy Binding Acknowledgement (PrBack) Message.....	11
6. Message Formats.....	13
6.1. New Proactive Binding Acknowledgement (PrBack) Message...13	13
6.2. Modified Inter-Access Router Messages	15
6.2.1. modified Handover Initiate (HI) Message Format	15
6.2.2. Modified Handover Acknowledgement (HACK).....	16
6.3. Modified Mobility Header Messages.....	17
6.3.1. Fast Binding Update (FBU).....	17
6.3.2. Fast Binding Acknowledgement.....	18
6.4. Modified Option.....	20
6.4.1. IP Address Option.....	20
6.5. New Options.....	21
6.5.1. Binding Destination Option.....	21
6.5.2. Anchor Home Address Option.....	22
6.5.3. Binding Update Information Option.....	23
7. Security Considerations	25
8. IANA Considerations.....	25
9. Acknowledgments.....	26
10. Normative References.....	27
Intellectual Property Statement.....	27

Disclaimer of Validity.....[28](#)

[1.](#) Requirements notation

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 [\[1\]](#).

[2.](#) Introduction

In MIPv6 [\[2\]](#) a Mobile Node (MN) is said to have undergone handover when the Home Agent (HA) and Correspondent Node(s) (CN(s)), upon receiving respective Binding Update (BU) from the MN, successfully create bindings between the MN's Home Address (HoA) and the Care-of Address (CoA) pertaining to the MN new point of attachment and the MN receives Binding Acknowledgements (BAs) from the HA and CN(s) in response to the corresponding BUs.

MIPv6 is composed of several delay incurring sub-processes such as Movement Detection, CoA auto-configuration, performing Duplicate Address Detection (DAD) [\[4\]](#) on the newly configured CoA, CoA registration (both with the HA and the CN(s)) and Route Optimization, contributing to the overall handover latency, making MIPv6 unsuitable for real-time communication sessions/streams and for fast moving users undergoing frequent handovers, resulting in packet losses and in worst cases, connection/session timeouts.

FMIPv6 is proposed in [\[3\]](#) which aims at reducing the "handover latency" and related "packet losses" by performing operations such as movement detection and new CoA configuration (including DAD for the newly formed Address) in advance, i.e., while the MN is connected to Previous/Present Access Router (PAR) and before it connected to the New/Next Access Router (NAR)(as in predictive handover mode), by creating a reverse tunnel between NAR and PAR to reduce packet losses, but it does not address the latency that occurs due to process of CoA registration with both the HA and the CN(s).

The FMIPv6 protocol also does not specify as to when, how and under what conditions should this bi-directional PAR-NAR tunnel be torn down and how to reduce its duration for resource preservation in both PAR and NAR related to tunneling overhead.

This specification addresses these issues by proposing a mechanism of "proactively" carrying out in advance the MN's CoA registration

process (home registration and correspondent registration) to further optimize the base FMIPv6 protocol.

3. Terminology

This document refers to [2] and [3] for terminology. The following terms and abbreviations are additionally used in this document.

The reference network is illustrated in Figure 1.

Proxy New Access Router (PrNAR):

The NAR which will act as a proxy on behalf of the MN by proactively carrying out Home and Correspondent Registration on behalf of the MN.

Proxy Binding Update List (PrBUL):

The PrNAR will create and maintain a Proxy Binding Update List on behalf of the MN when carrying out proactive bindings with the HA and CN(s).

Proxy Binding Acknowledgement (PrBAck):

The PrNAR will transmit this message after it successfully creates bindings with the HA and the CN(s).

Anchor Home Network (AHN):

The network domain where the address assigned/configured to/by the MN is considered to be the home address (HoA) and not a care-of address (CoA). The access router of the AHN to which the mobile node is connected to is the HA of the MN.

Surrogate Home Network (SHN):

The network domain where the MN is currently attached and the address assigned/configured to/by the mobile node is considered to be the care-of address and not a home address (or Anchor Home Address).

Anchor Home Address (AHOA):

The address of the MN configured/assigned at the AHN.

Surrogate Home Address (SHoA):

The address of the MN configured/assigned at the SHN. Same as the PCoA (or current CoA).

Anchor Home Network Information (AHNI):

Constitutes the IPv6 address of the MN's home agent in the AHN and the Anchor Home Address (AHOA) of the MN in that domain.

Surrogate Home Network Information (SHNI):

Constitutes the IPv6 address of the access router to which the MN is attached and the CoA assigned/configured to/by the MN in the SHN, also termed as the Surrogate Home Address (SHoA).

Prospective Care-of Address (PCoA):

The NAR compatible address auto-configured by the MN while it is connected to PAR but before it is assigned.

New Care-of Address (NCoA):

The address assigned to the MN after successful DAD operation by NAR.

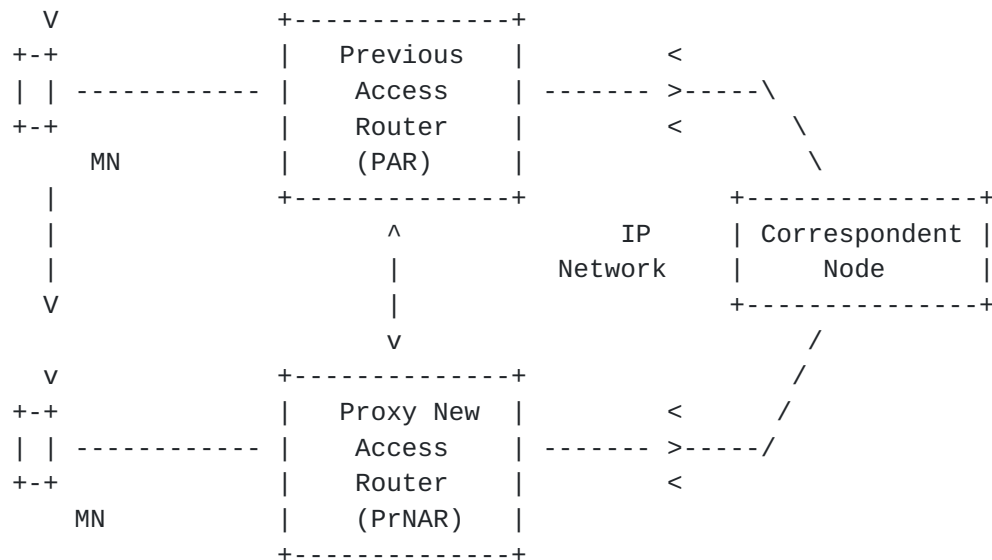


Figure 1 : Reference Scenario for Handover

4. Protocol Overview

4.1. Handover Latency in Fast MIPv6

When a MN moves to a new subnet, it has to establish connection to the NAR of the new subnet and successfully register its NCoA by creating bindings with the CN(s) and the HA before it can start receiving regular traffic from its CN(s) via a direct route, i.e., through a process called route optimization [2].

When the MN moves into a new subnet it has to perform the following tasks before it can resume connection with the CN(s).

1. Movement detection
2. Neighbor (router/AR) prefix discovery
3. NCoA configuration
4. DAD performed by the NAR and confirming the validity of the NCoA.
5. CoA registry

6. Home registration and correspondent registration of this NCoA using BU and BA including the regular Return Routability procedure.

After the successful completion of the above six tasks, the MN becomes IP-capable on the new link and the MN is said to have undergone handover, whereas the total "handover latency" is the sum of the latencies incurred by each of the above six processes.

During this period of handover, the MN is practically disconnected from the HA and the CN(s), this period of disconnection can also be termed as a "blackout" period, and all the packets communicated between the MN and CN(s) are expected to be delayed, lost or in worst cases (in case of TCP timeouts) service disconnection.

The degree of packet loss or packet delay is a function of the overall handover latency, and hence is not suitable for fast moving users and /or using real time applications, such as video conferencing.

FMIPv6 [3] aims at reducing the handover latency by performing the above five steps in advance while the MN is still connected to PAR, i.e., before the MN travel towards and establishes a L2 connection to the NAR (termed as predictive handover mode), or after it has established a L2 connection with the NAR (termed as reactive handover mode).

FMIPv6 also reduces/eliminates the packet loss during the connection blackout time, by establishing a bi-directional tunnel between PAR and NAR. During this blackout period, the traffic from the CN(s) gets delivered to NAR via the PAR through the tunnel where the packets get buffered. When the MN connects to the NAR, all the buffered packets at the NAR and subsequent packets arriving from the CN(s) will get delivered to the MN via the PAR through the PAR-NAR tunnel. The MN after connecting to the NAR will start the MIPv6 binding process [2] with the HA and the CN(s), after the successful completion of which the PAR-NAR tunnel gets torn down and all subsequent communication between the MN and the CN(s) will take place via the NAR.

4.2. Open Issues in FMIPv6

The current FMIPv6 specification [3] does not provide any signaling exchange to inform the PAR that it can stop forwarding packets and/or the tunnel can be released.

Also the duration of the tunnel existence between PAR and NAR is critical in terms of resource management and routing efficiency and this can potentially contribute towards the following:

- o Buffer space/resource commitment in both NAR and PAR, which may not scale well in case of an increase in the number of prospective MNs (or when a large number of MNs belonging to the same PAR migrate to the same NAR), a situation typical on a congested highway.
- o Duration of tunnel existence will potentially contribute towards packet jitter and delay, which may not favor real time communication sessions and applications.
- o Increased processing due to tunneling and de-tunneling of packets at both PAR and NAR and then reverse tunneling of packets during the time when the MN is establishing bindings with its HA and CN(s).
- o Possibility of in-efficient routing between MN and respective CN(s) till the tunnel is released and new efficient/shortest path routes between the CN(s) and NAR is calculated by the network.
- o In case of high probability of error on the MN-PAR wireless link, the tunnel between PAR and NAR may exist of a longer duration.

Thus controlling and minimizing the duration of the tunnel between PAR and NAR holds the key to a better performance of FMIPv6 protocol both in terms of handover latency and efficient management of resources.

4.3. Proactive Binding for FMIPv6 (PB-FMIPv6) Operation Summary

In FMIPv6 [3], the tunnel between PAR and NAR exists till the handover is complete. The handover is said to be complete only when the MN successfully registers its New Care of Address (NCoA) with its corresponding HA and CN(s).

The idea behind PB-FMIPv6 is that the registration of the NCoA with its CN(s) and HA is done in advance and in parallel to when the MN is in the process of disconnecting from PAR, connecting to NAR and announcing its presence to NAR by sending Unsolicited Neighbor Advertisement (UNA) message to NAR.

The motivation behind this approach is based on the fact that the NAR becomes aware of the NCoA of the MN as early as it receives a Handover Initiate (HI) message from PAR, after which it has every

possibility of proxying for MN and hence proactively perform the requisite bindings on its behalf, while the MN is in the process of moving away from PAR and entering the new subnet and establishing connection with the NAR.

It is expected, depending on the speed of the MN, that by the time the MN sends the UNA message to NAR, the NCoA will already be or in the process of getting registered with the HA and the CN(s), afterwards which the tunnel gets released immediately. In essence, PB-FMIPv6 performs the MIPv6 registration process in parallel to the MN's process of moving away from PAR and entering the new subnet and establishing connection with the NAR thereby achieving timing efficiency, which in turn will contribute towards the reduction in PAR - NAR tunnel existence duration and offsetting all the issues related to the extended duration of the PAR-NAR tunnel as outlined in [section 4.2](#).

[4.4](#). Advantages

The reduction in tunnel duration by the proposed mechanism of PB-FMIPv6 is expected to account for the following advantages:

- o Resource preservation in case of early release of tunnel
- o Resource available for other potential fast moving MNs into the domain
- o Early registration of MN's NCoA with the HA and the CN(s) before/shortly after the MN arrives in the new domain.
- o Reduction in processing due to tunneling, de-tunneling and reverse tunneling of packets.
- o Considerable load reduction on ARs due to reduction in buffer and tunnel maintenance.
- o Fully integrated into the present scheme of MIPv6 networks.
- o Zero probability of binding messages to be lost over error prone wireless links.
- o No added complexity to existing network infrastructure and/or topology.
- o Reduction in handover latency.

5. Proactive Binding for FMIPv6 (PB-FMIPv6) Protocol Details

In PB-FMIPv6, the NAR is replaced by Proxy-NAR (PrNAR), which is NAR acting as a proxy and performing proactive bindings on behalf of the MN. The protocol operation is shown in figure 2.

The protocol operation of the PB-FMIPv6 is similar to that of the base FMIPv6 protocol in which the MN, upon detecting one or more L2 ID during its scan operations or upon receiving some link level trigger, will send a RtSolPr message to its access router in order to resolve one or more AP identifiers to subnet-specific information. In response, the PAR will send a PrRtrAdv towards the MN containing one or more [AP-ID, AR-Info] tuples [3].

The MN, based on some network selection criteria, auto-configures a prospective-CoA (PCoA) pertaining to a specific new subnet that it wishes to handover its connection to, and sends a FBU to PAR instructing the PAR to request the PrNAR to proxy on behalf of the MN. The MN will send the FBU with the P-flag set, indicating the MN's request to perform PB-FMIPv6 operation. The FBU will carry the address of the MN's HA in the AHN and the address(es) of the CN(s) in the new Binding Destination Option (see [section 6.5.1](#)) and carry the AHOA of the MN in the new Anchor Home Address Option (see [section 6.5.2](#)). The information carried by these two new options will also convey the complete AHNI profile.

The PAR, upon receiving FBU with the P-flag set will send the HI message towards the PrNAR with the P-flag set. The HI message, with the P-flag set, besides carrying the prescribed FMIPv6 options [3] MUST also be appended with an array of IP Address Option carrying the following addresses:

1. The AHOA of the MN MUST be included with the Code-Option value set to 4. This address will be subsequently used in the Home Address Destination Option of the BU messages [2] sent by the PrNAR on behalf of the MN. This address is obtained from the Anchor Home Address Option carried by the received FBU message.
2. The IP address of the MN's HA at the AHN MUST be included with the Option-Code value set to 5. This address will be subsequently used as the destination address of the IP header of the BU message sent by the PrNAR for Home Registration of the MN. This address is obtained from the Binding Destination Option carried by the received FBU message.

3. The IP address of the CN MAY be included (if the MN is in communication with) with the Option-Code value set to 6. This address will be subsequently used as the destination address of the IP header of the BU message sent by the PrNAR for Correspondent Registration of the MN. The HI message MAY carry none or multiple of such options depending on the number of CN the MN is in communication with. This address is obtained from the Binding Destination Option carried by the received FBU message.

The PrNAR upon receiving the HI message with the P-flag set will decide, based on some decision mechanism (such as available resources) but beyond the scope of this document, whether or not to perform proactive bindings on behalf of the MN, and this decision will be conveyed with the P-flag in the HAck message set or unset. In case of the HAck's P-flag unset; normal FMIPv6 process will ensue as specified in [3].

In case the PrNAR has decided to perform proactive bindings for the MN, it will perform DAD on the PCoA and will inform of the NCoA and its ability to proxy for the MN by sending a HAck message back to PAR with its P-flag set.

As soon as the PAR receives a HAck, regardless of the status of the P-Flag, a binding between the PCoA and NCoA will be formed inside PAR and also a tunnel will be established between PAR and PrNAR. At the same time, when NCoA has been confirmed by PrNAR, the PrNAR will proactively initiate MIPv6 home registration and correspondent registration process with the MN's HA located in the AHN and the CN(s). The PrNAR will create and maintain a Proxy-Binding Update List (PrBUL) on behalf of the MN.

In the meantime, the PAR will send an FBAck informing the MN of its NCoA and the decision of the PrNAR, regarding proxying for the MN, embedded in the status field of the FBAck message.

The PrNAR upon receiving BA(s) from the respective HA and the CN(s) will update its PrBUL and will send Proxy Binding Acknowledgement (PrBack) to the PAR, which will also relay it to the MN (if the MN is still on PAR's link). The PrBack message besides indicating to the MN about the successful binding on it's behalf is also used as an implicit signal for the release of PAR-PrNAR tunnel.

All subsequent packets intended for the MN will now reach PrNAR directly and get buffered. As soon as the MN establishes a L2 connection with the PrNAR, it will send an UNA and the PrNAR will

start forwarding all the buffered packets and subsequent packets towards the MN.

The MN upon receiving a PrBack will know that bindings with the HA and CN(s) has been carried out proactively and will send messages with the NCoA as the source address in all subsequent IP transmissions.

If the MN has not yet established a L2 connection with the PrNAR when it receives PrBack, it MUST do so immediately as all transmissions from the CN(s) will now be getting buffered at the PrNAR and any delays on behalf of the MN in establishing connections with the PrNAR can lead to possible delays, buffer overflow and hence packet losses.

5.1. Processing of Proxy Binding Acknowledgment (PrBack) Message

Since the main motivation behind PB-FMIPv6 is the reduction in the NAR-PrNAR tunnel duration, therefore the timing of the PrNAR's signaling for the release of the tunnel is very important.

In principle the tunnel should be released soon after the PrNAR completes the bindings on behalf of the MN and receives the relevant BA(s) from the HA and CN(s). The PrNAR uses the PrBack message as a tunnel release signal and in addition informs the MN about the successful completion of proactive bindings.

The PrNAR will send a PrBack message for every BA it receives, and every PrBack will be appended with the Binding Update Information Option (see [section 6.5.3](#)), which will enable a MN to update the corresponding entries in its local Binding Update List cache. The PrBack corresponding to the last BA will have the tunnel release flag set.

Since the BAs from different target nodes may arrive at PrNAR at different times, therefore a separate PrBack is sent for each BA received and the last PrBack message will contain the tunnel release signal. Hence the tunnel should not be released until the reception of the last BA.

For each BA received, the PrNAR will transmit a PrBack with the NCoA as the destination IP address on both the local wireless link and on the PAR link via the tunnel. This is done to ensure the reception of the PrBack message by the MN in situation where the MN may have moved to the PrNAR link before receiving the PrBack on the PAR's link. The destination address of the outer tunnel packet should be the IP address of the PAR, which upon receiving the PrBack will release the tunnel, depending on the status of the tunnel release flag and

forward the inner packet (with NCoA as the destination address) on the wireless link. The PAR should create a temporary forwarding state for the NCoA only on the wireless interface till the time it receives a tunnel release signal. The MN will continue to update its local BUL entries with the information carried by the PrBack message and upon receiving the PrBack with the tunnel release signal will know that bindings has been completed and it will disconnect from the PAR (if PAR already has not initiated the disconnection of the MN) and will update its local BUL with the information available in the PrBack

If the PrNAR receives UNA from the MN before it has transmitted the last PrBack (i.e., during the scenario in which the MN attaches to PrNAR before the binding process has completed) then the subsequent PrBacks should be sent only on the local wireless link with NCoA as the destination IP address and only the last PrBack, carrying the tunnel release signal should be sent towards PAR as well. This MAY be true for both the predictive and reactive handover modes, but the actual mode of handover depends on the reception of the FBack message as specified in [3]. For reactive handover modes, i.e. when the MN doesn't receive FBack on the PAR's link, the handover may be carried out as per the reactive handover mode specified in [3] and the choice of carrying out PB-FMIPv6 handovers may be optional depending on the error probability on the PrNAR's wireless link.

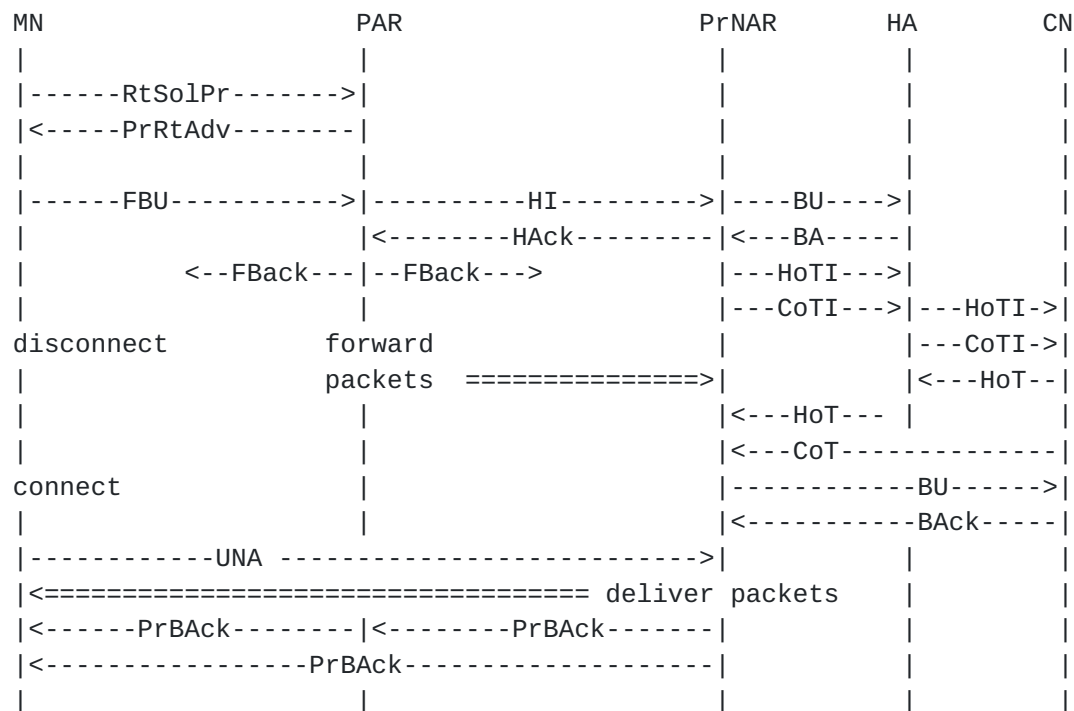


Figure 2 : PB-FMIPv6 Protocol Operation.

6. Message Formats

The PB-FMIPv6 introduces an additional new message called the Proactive Binding Acknowledgement (PrBack) and two new message options namely Binding Destination Option and Anchor Home Address Option besides necessary modifications to the existing FMIPv6 messages and message options.

6.1. New Proactive Binding Acknowledgement (PrBack) Message

The PrNAR will send a PrBack message towards the MN for each BA it receives from the HA and the CN(s). The PrBack not only informs the MN of the successful home and/or correspondent registration but also carries information that is used by the MN to update its local binding update list (BUL). This message is also used as a signal to tear down the PAR-PrNAR tunnel.

The format of the message is shown in figure 3.

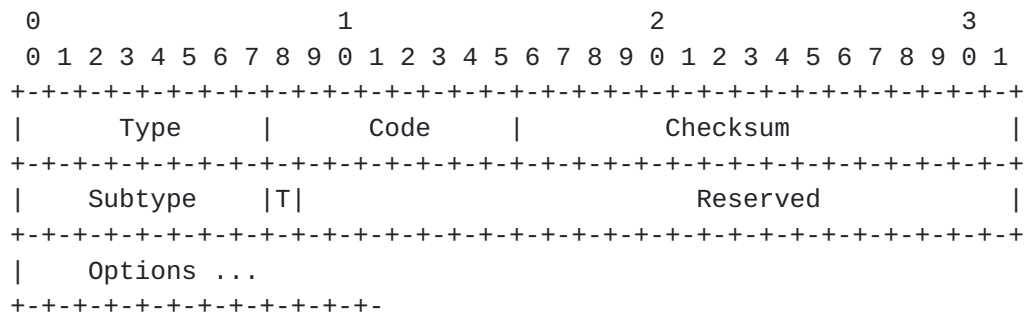


Figure 3 : Proactive Binding Acknowledgement (PrBack) Message

IP Fields:

Source Address

IP address of the PrNAR

Destination Address

The NCoA of the MN.

ICMP Fields:

Type The Experimental Mobility Protocol Type. See [\[5\]](#).Code 0: Home Registration
 1: Correspondent Registration.

Checksum The ICMPv6 checksum.

Subtype 6 (This value is yet to be determined by IANA. See [section 8](#))

'T' Flag Tunnel Release Flag. When set indicates to PAR to release the tunnel.

Reserved MUST be set to zero by the sender and ignored by the receiver.

Valid Options:

Binding Update Information Option

This option MUST be included in the PrBack message. The information carried by this option field is used by the MN to update its corresponding BUL cache entries. For more information see [section 6.5.3](#)

6.2. Modified Inter-Access Router Messages

6.2.1. Modified Handover Initiate (HI) Message Format

PB-FMIPv6 modifies the format of the Handover Initiate [3] by the addition of a single flag bit to indicate that the PAR sending the HI message is requesting a NAR to accept the proxy request for the MN.

The format of the Handover Initiate message is shown in figure 4.

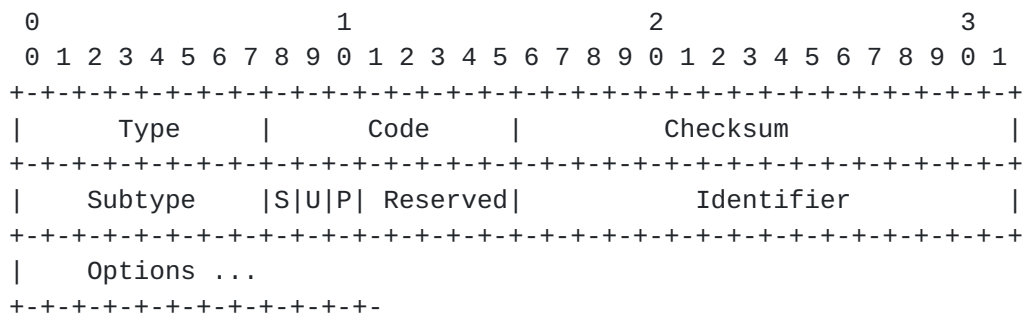


Figure 4 : Handover Initiate (HI) Message

This format represents the following changes over that originally specified for FMIPv6 [3]:

Proxy Flag (P)

When set indicates to the NAR to proxy on behalf of the MN and carry out binding with the HA and the CN(s). When not set indicates normal FMIPv6 operation.

Reserved

Reduced from a 6-bit field to a 5-bit field to account for the addition of the above bit.

Valid Options:

Home Address of the MN at the AHN

The IP address of the MN configured at the Anchor Home Network (AHN) (also termed as AHoA). This option MUST be included, when the P-flag is set, by appending the IP Address option with the Option-code value of 4.

MN's Home Agent Address at the AHN

The IP address of the MN's HA at the Anchor Home Network (AHN). This option MUST be included, when the

P-flag is set, by appending the IP Address option with the Option-code value of 5.

CN Address Option

The IP address of the CN with which, the MN wishes to establish bindings with. This option MAY be included, when the P-flag is set, by appending the IP address option with the Option-code value set to 6. The HI message MAY carry multiple such options.

6.2.2. Modified Handover Acknowledge (HACK)

The format of the Handover Acknowledge (HACK), which is sent as a reply to HI, is modified by the addition of a single flag bit to indicate that the PrNAR has accepted the request and will complete bindings on behalf of the MN.

The format of the Handover Acknowledge message is shown in figure 5.

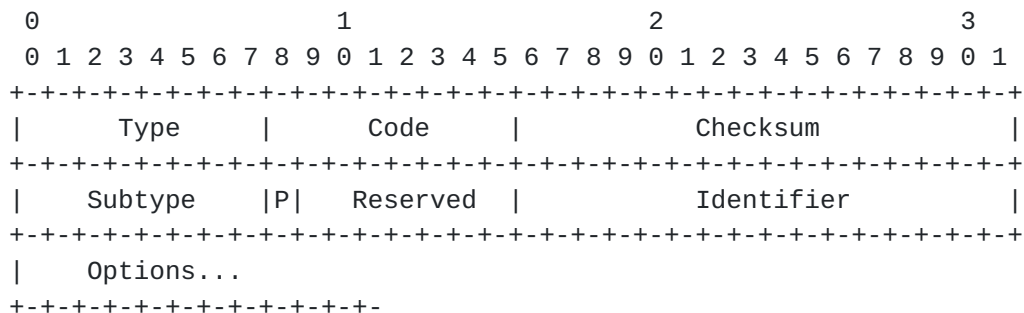


Figure 5 : Handover Acknowledge (HACK) Message

This format represents the following changes over that originally specified for FMIPv6 [3]:

Proxy Acknowledge Flag (P)

When set indicates that the PrNAR has accepted the proxying request of the MN and PrNAR has started the NCoA registration process, and is maintaining a Proxy Binding Update List (PrBUL) cache. When not set indicates that the request can not be fulfilled. The P flag should only be set when the code value is 0, 1, 2, 3 or 4 (for details see [3]). For all other code values, it should be 0.

Reserved

Reduced from a 8-bit field to a 7-bit field to account for the addition of the above bit.

Upon receiving a HI message, the PrNAR MUST respond with a Handover Acknowledge message, with the appropriate value for the code and P-flag. Upon receiving a HI and accepting the MN's proxy request, the PrNAR will create a Proxy Binding Update List (PrBUL), the constitution of which is the same as that of the BUL defined in [2], but with the MN's PAR and/or NAR address as a key to associate the PrBUL contents with the relevant MN(s). This is necessary to handle multiple MN(s) undergoing PB-FMIPv6. The PrNAR will maintain the PrBUL till the MN attaches to it.

6.3. Modified Mobility Header Messages

Mobile IPv6 uses a new IPv6 header type called Mobility Header [2]. The Fast Binding Update, Fast Binding Acknowledgment messages use the Mobility Header. However, PB-FMIPv6 modifies these header messages the relevant details of which are given below.

6.3.1. Fast Binding Update (FBU)

The format of the Fast Binding Update message is modified from the original (see [2]) by the addition of a single flag bit to indicate the MN's request to perform PB-FMIPv6 based handover.

The format of the message is shown in figure 6.

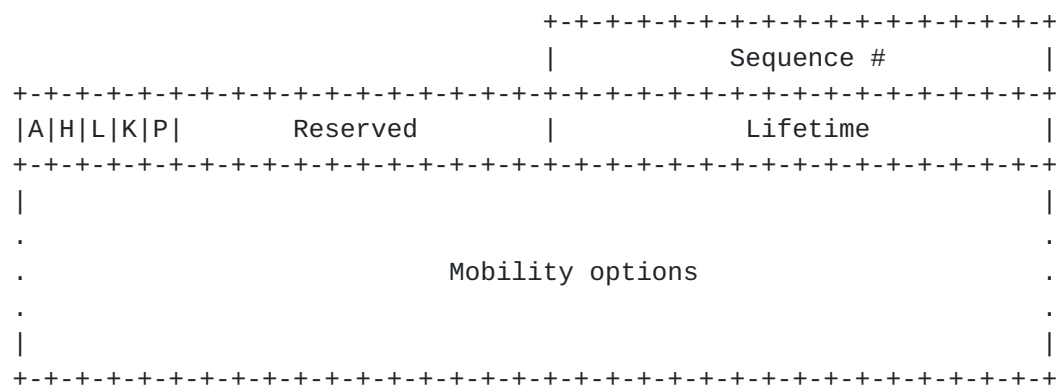


Figure 6 : Fast Binding Update (FBU) Message

This format represents the following changes over that originally specified for FMIPv6 [3]:

Proxy Request Flag (P)

When set indicates that the MN desires to perform PB-FMIPv6 based handover and is a request to the candidate access router (PrNAR in our case) to perform

bindings on its behalf. When not set indicates normal FMIPv6 operation.

Reserved

Reduced from a 12-bit field to a 11-bit field to account for the addition of the above bit.

Valid Options

Binding Destination Option

When the P-flag is set, the FBU must contain one or more binding destination option, which will convey the address(es) to which BUs will be sent. The details about this new option are given in 6.5.1.

Anchor Home Address Option

The FBU MUST contain the Anchor Home Address Option when the P-flag is set. This option will carry the AHOA of the MN which will be used in the Home Address Option of the BU message sent by the NAR on behalf of the MN. The details about this new option are given in 6.5.2.

The combination of the Binding Destination Option and the Anchor Home Address Option provides the complete AHNI profile as well as the destination addresses required by the BU message. The

The other valid options to be used are the same as specified in [3].

6.3.2. Fast Binding Acknowledgment (FBack)

The format of the Fast Binding Acknowledgement message is the same but it modifies the interpretation of the existing status values by defining two new status values indicating the NAR's acceptance/rejection to carry out proactive bindings on behalf of the MN's request. The rules for the Mobility Option is also modified.

The format of the message is shown in figure 7.

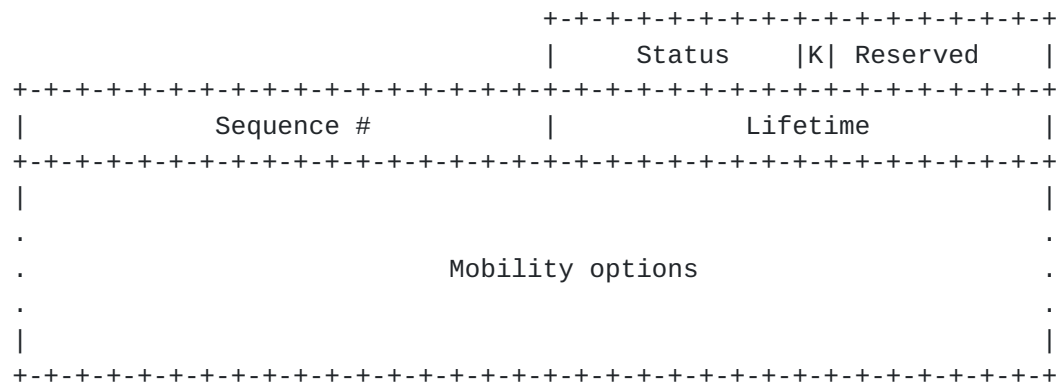


Figure 7 : Fast Binding Acknowledgment (FBack) Message

Status

8-bit unsigned integer indicating the disposition of the Fast Binding Update. Values of the Status field less than 128 indicate that the Binding Update was accepted by the receiving node. The following such Status values are currently defined:

0 Fast Binding Update accepted for normal FMIPv6 operation. PB-FMIPv6 operation not supported

1 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in ``alternate'' CoA and PB-FMIPv6 operation not supported

2 Fast Binding Update accepted and PB-FMIPv6 operation enabled

3 Fast Binding Update accepted but NCoA is invalid. Use NCoA supplied in ``alternate'' CoA and PB-FMIPv6 operation enabled

Values of the Status field greater than or equal to 128 indicate that the Binding Update was rejected by the receiving node. The following such Status values are currently defined:

128 Reason unspecified

129 Administratively prohibited

- 130 Insufficient resources
- 131 Incorrect interface identifier length

Mobility Options

MUST contain Alternate CoA option (see [2]) if Status is 1 or 3. MUST contain the Binding Authorization Data for FMIP (BADF) option as specified in [3].

6.4. Modified Option

PB-FMIPv6 extends the IPv6 Address option by defining additional Option-Codes.

6.4.1. IP Address Option

This option defines new option codes 4, 5 and 6, which is sent in the Handover Initiate message. Option-Codes 4 and 5 convey the Anchor Home Network Information (AHNI) while the Option-Code 6 conveys the address(es) of the CN(s).

The format of the message is shown in figure 8.

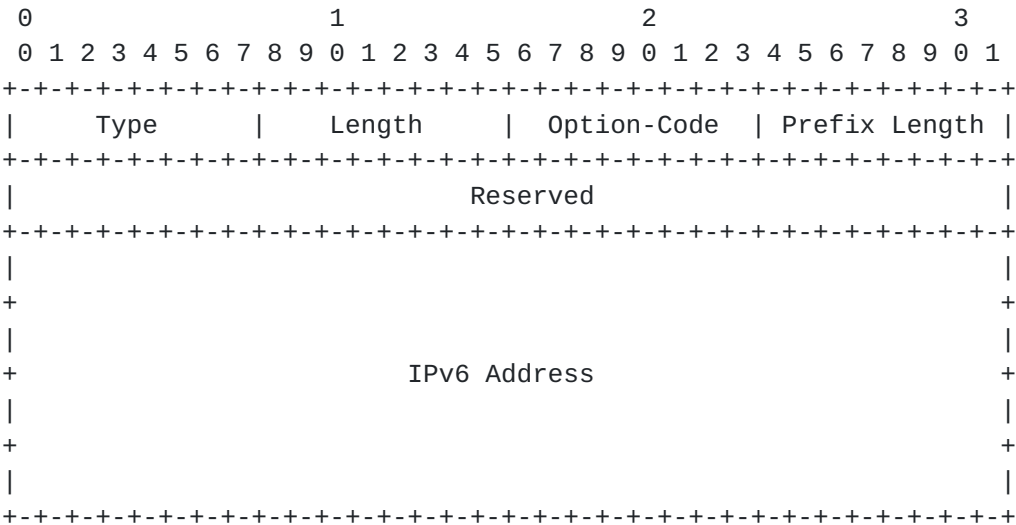


Figure 8 : IPv6 Address Option

- Option-Code
- 1

Old Care-of Address
- 2

New Care-of Address
- 3

NAR's IP address

- 4 MN's IP address at the AHN (AHoA).
- 5 IP address of the MN's home agent at the AHN
- 6 IP address of the CN

Option codes 4, 5 and 6 MUST be included together when the P-Flag in the FBU and HI is set.

6.5. New Options

PB-FMIPv6 defines three new options, two of which namely the Binding Destination Option and Anchor Home Address Option, is carried by the FBU and encoded within the remaining space of the Message Data field of the FBU, using a type-length-value (TLV) format as specified in [2].

The third new option namely, Binding Update Information Option is carried by the PrBAck message (see [section 6.1](#)).

6.5.1. Binding Destination Option

At least one instance of this option MUST be present in the FBU when the P-Flag is set. This option contains the array of address(es), which will be copied into the appropriate options of the HI message, to which the PrNAR will send the bindings to on behalf of the MN. According to normal MIPv6 operations, the MN sends binding updates to the HA and the CN(s) with which a communication session is established. The option type identifies the address to be that of the MN's HA in the AHN or of CN(s). The information contained in the Binding destination option and the Anchor Home Address option (see [section 6.5.2](#)) gives complete AHNI profile, which the PrNAR will use for establishing bindings on behalf of the MN.

The format of the message is shown in figure 9.

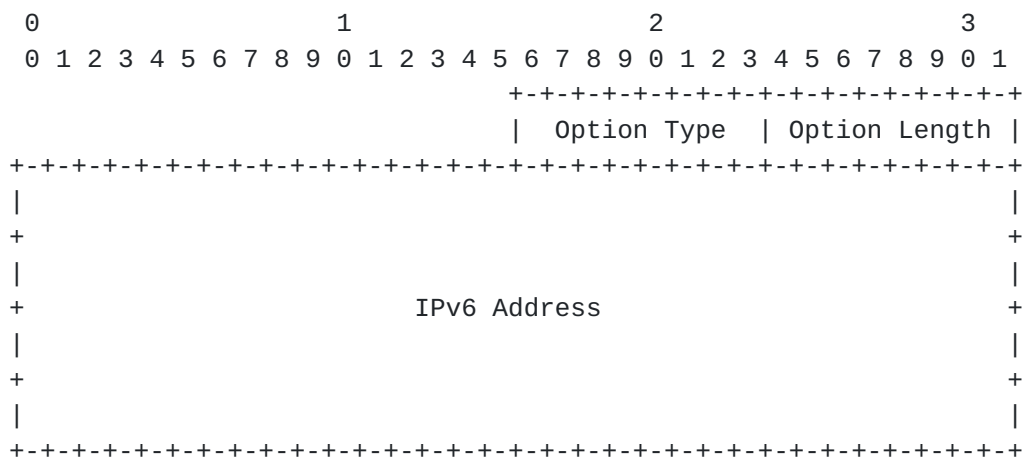


Figure 9 : Binding Destination Option

Option Type

202 = 0xCA* Home Agent address of the MN at the AHN
 203 = 0xCB* CN Address

(* The values for the Option Type field are to be determined by IANA. The values shown here are for experimental purpose. See [section 8](#)).

6.5.2. Anchor Home Address Option

This option MUST be present in the FBU when the P-flag is set. The Home Address option in the FBU carries the MN's PCoA, and adding the Anchor Home Address option enables the information of the MN's AHOA information to be also conveyed.

The format of the message is shown in figure 10.

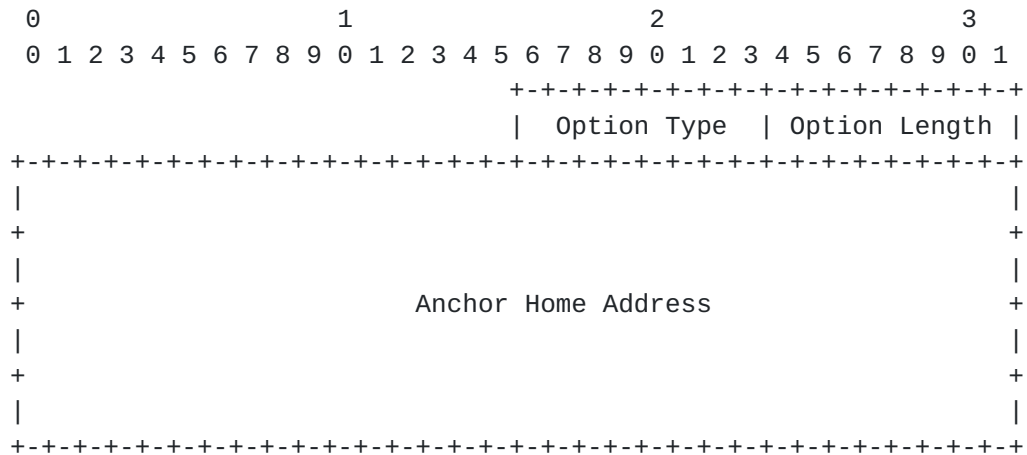


Figure 10 : Anchor Home Address Option

Option Type

204 = 0xCC*

Anchor home address of the MN

(* The values for the Option Type field are to be determined by IANA. The values shown here are for experimental purpose. See [section 8](#)).

6.5.3. Binding Update Information Option

This option MUST be present in the PrBack message and its exact format depends on the code value of the PrBack message.

The format of the message is shown in figure 11.

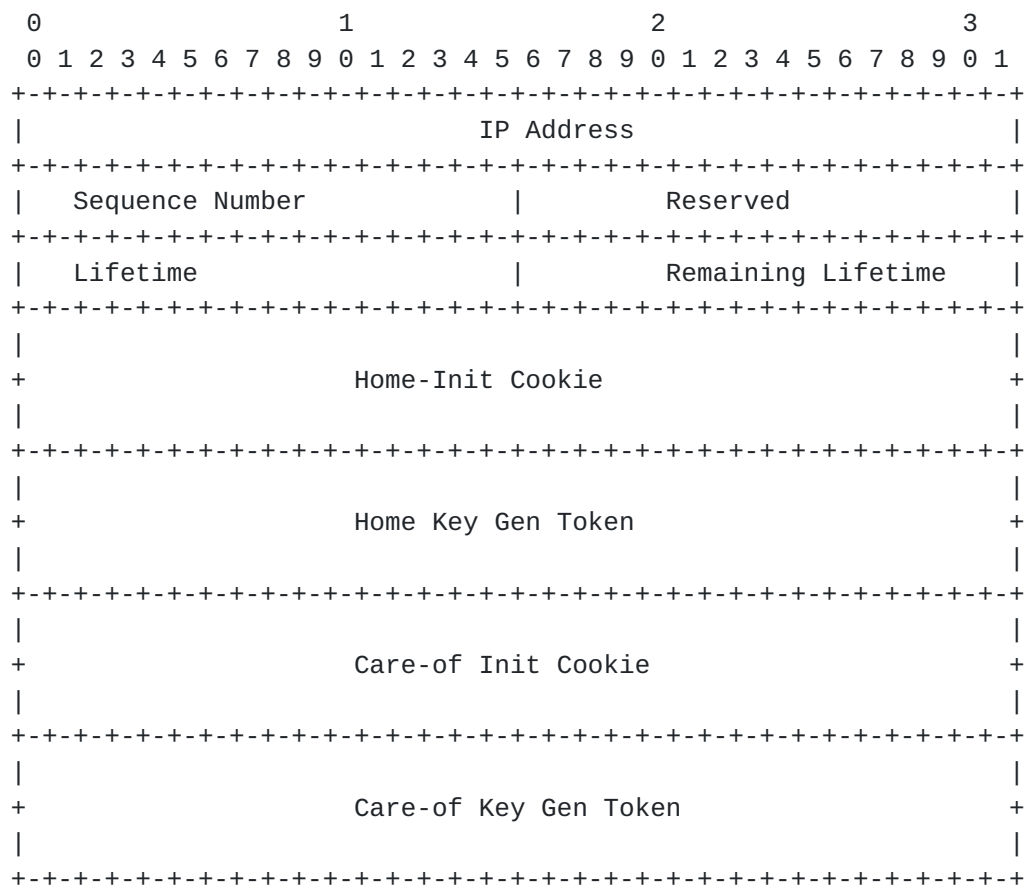


Figure 11: Binding Update Information Option

IP Address	When the Code value in PrBack message is 0, this IP address will be the IP address of the MN's HA in the AHN. When the code value is 1, this IP address will be the IP address of a CN.
Sequence Number	The sequence number of the BU for which the BA was received.
Lifetime	Lifetime of the binding in the destination node
Remaining Lifetime	Remaining lifetime of the binding in the destination node
Home-Init Cookie	It is zero when code value is 0 and should be ignored by the receiver.
Home Key Gen Token	It is zero when code value is 0 and should be ignored by the receiver.

10. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Johnson, D., "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [3] Koodli, R., Ed., "Fast Handover for Mobile IPv6", [RFC 4068](#), July 2005.
- [4] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.
- [5] J. Kempf, "Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations," [RFC 4065](#), Internet Engineering Task Force, June 2004.

Author's Addresses

Faqir Zarrar Yousaf
Communication Networks Institute
University of Dortmund
Building Chemistry,
Otto-Hahn-Str. 6,
D-44227 Dortmund, Germany

Email: faqir.yousaf@tu-dortmund.de

Christian Wietfeld
Communication Networks Institute
University of Dortmund
Building Chemistry,
Otto-Hahn-Str. 6,
D-44227 Dortmund, Germany

Email: christian.wietfeld@tu-dortmund.de

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.

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, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The IETF Trust (2008).

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.

