Network Working Group
Request for Comments: 4988
Category: Experimental

R. Koodli
C. Perkins
Nokia Siemens Networks

October 2007

Mobile IPv4 Fast Handovers

Status of This Memo

This memo defines an Experimental Protocol for the Internet community. It does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Abstract

This document adapts the Mobile IPv6 Fast Handovers to improve delay and packet loss resulting from Mobile IPv4 handover operations. Specifically, this document addresses movement detection, IP address configuration, and location update latencies during a handover. For reducing the IP address configuration latency, the document proposes that the new Care-of Address is always made to be the new access router's IP address.

Table of Contents

1. Introduction

This document adapts the fast handover specification [rfc4068] to IPv4 networks. The fast handover protocol specified in this document is particularly interesting for operation over links such as IEEE 802 wireless links. Fast handovers are not typically needed for wired media due to the relatively large delays attributable to establishing new connections in today's wired networks. Mobile IPv4 [rfc3344] registration messages are reused (with new type numbers) in this document to enable faster implementation using existing Mobile IPv4 software. This document does not require link-layer triggers for protocol operation, but performance will typically be enhanced by using the appropriate triggers when they are available. This document assumes that the reader is familiar with the basic operation and terminology of Mobile IPv4 [rfc3344] and Fast Handovers for Mobile IPv6 [rfc4068].

The active agents that enable continued packet delivery to a mobile node (MN) are the access routers on the networks that the mobile node connects to. Handover means that the mobile node changes its network connection, and we consider the scenario in which this change means change in access routers. The mobile node utilizes the access routers as default routers in the normal sense, but also as partners in mobility management. Thus, when the mobile node moves to a new network, it processes handover-related signaling in order to identify and develop a relationship with a new access router. In this document, we call the previous access router PAR and the new access router NAR, consistent with the terminology in [rfc4068]. Unless otherwise mentioned, a PAR is also a Previous Foreign Agent (PFA) and a NAR is also a New Foreign Agent (NFA).

On a particular network, a mobile node may obtain its IP address via DHCP [rfc2131] (i.e., Co-located Care-of Address) or use the Foreign Agent CoA. During a handover, the new CoA (NCoA) is always made to be that of NAR. This allows a mobile node to receive and send packets using its previous CoA (PCoA), so that delays resulting from IP configuration (such as DHCP address acquisition delay) subsequent to attaching to the new link are disengaged from affecting the existing sessions.

Unlike in Mobile IPv6, a Mobile IPv4 host may rely on its Foreign Agent to provide a Care-of Address. Using the protocol specified in this document, the binding at the PAR is always established between the on-link address the mobile node is using and a new CoA that it can use on the NAR's link. When FA-CoA is used, the on-link address is the MN's home address, not the FA-CoA itself, which needs to be

bound to the NCoA. So, when we say "a binding is established between PCoA and NCoA", it is actually the home address of the mobile node that is bound to the NCoA in the FA-CoA mode.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Terminology

The terminology used in this document in based on [rfc4068] and [rfc3344]. We provide some definitions below for convenience.

Mobile Node (MN): A Mobile IPv4 host.

Access Point (AP): A Layer 2 device connected to an IP subnet that offers wireless connectivity to an MN. An Access Point Identifier (AP-ID) refers to the AP's L2 address. Sometimes, AP-ID is also referred to as a Base Station Subsystem ID (BSSID).

Access Router (AR): The MN's default router.

Previous Access Router (PAR): The MN's default router prior to its handover.

New Access Router (NAR): The MN's default router subsequent to its handover.

Previous CoA (PCoA): The IP address of the MN valid on PAR's subnet.

New CoA (NCoA): The MN's Care-of Address valid on NAR's subnet.

Handover: A process of terminating existing connectivity and obtaining new IP connectivity.

(AP-ID, AR-Info) tuple: Contains an access router's L2 and IP addresses, and the prefix valid on the interface to which the Access Point (identified by AP-ID) is attached. The triplet [Router's L2 address, Router's IP address, Prefix] is called "AR-Info".

3. Factors Affecting Handover

Both link-layer operations and IP-layer procedures affect the perceived handover performance. However, the overall performance is also (always) a function of specific implementation of the technology as well as the system configuration. This document only specifies IP layer protocol operations. The purpose of this section is to provide an illustration of events that affect handover performance, but it is purely informative.

The IP-layer handover delay and packet loss are influenced by latencies due to movement detection, IP address configuration, and the Mobile IP registration procedure. Movement detection latency comes from the need to reliably detect movement to a new subnet. This is a function of the frequency of router advertisements as well as default agent reachability. IP address configuration latency depends on the particular IP CoA being used. If co-located mode with DHCP is used, the latency is quite likely going to be higher and potentially unacceptable for real-time applications such as Voice over IP. Finally, the Mobile IP registration procedure introduces a round-trip of delay between the Mobile Node and its Home Agent over the Internet. This delay is incurred after the mobile node performs movement detection and IP configuration.

Underlying the IP operations are link-layer procedures. These are technology-specific. For instance, in IEEE 802.11, the handover operation typically involves scanning access points over all available channels, selecting a suitable access point, and associating with it. It may also involve performing access control operations such as those specified in IEEE 802.1X [ieee-802.1x]. These delays contribute to the handover performance. See [fh-ccr] and Chapters 20 and 22 in [mi-book]. Optimizations are being proposed for standardization in IEEE; for instance, see [ieee-802.11r] and [ieee-802.21]. Together with appropriate implementation techniques, these optimizations can provide the required level of delay support at the link-layer for real-time applications.

4. Protocol

4.1. Overview

The design of the protocol is the same as for Mobile IPv6 [rfc4068]. Readers should consult [rfc4068] for details; here we provide a summary.

The protocol avoids the delay due to movement detection and IP configuration and disengages Mobile IP registration delay from the time-critical path. The protocol provides the surrounding network neighborhood information so that a mobile node can determine whether it is moving to a new subnet even before the handover. The information provided and the signaling exchanged between the local mobility agents allow the mobile node to send and receive packets immediately after handover. In order to disengage the Mobile IP registration latency, the protocol provides routing support for the continued use of a mobile node's previous CoA.

After a mobile node obtains its IPv4 Care-of Address, it builds a neighborhood access point and subnet map using the Router Solicitation for Proxy Advertisement (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages. The mobile node may scan for access points (APs) based on the configuration policy in operation for its wireless network interface. If a scan detects a new AP, the mobile node resolves the corresponding AP Identifier to subnet information using the RtSolPr and PrRtAdv messages mentioned above.

At some point, the mobile node decides to undergo handover. It sends a Fast Binding Update (FBU) message to PAR from the previous link or from the new link. An FBU message enables creation of a binding between the mobile node's previous CoA and the new CoA.

The coordination between the access routers is done by way of the Handover Initiate (HI) and Handover Acknowledge (HAck) messages defined in [rfc4068]. After these signals have been exchanged between the previous and new access routers (PAR and NAR), data arriving at PAR will be tunneled to NAR for delivery to the newly arrived mobile node. The purpose of HI is to securely deliver the routing parameters for establishing this tunnel. The tunnel is created by the access routers in response to the delivery of the FBU from the mobile node.

4.2. Operation

In response to a handover trigger or indication, the mobile node sends a Fast Binding Update message to the Previous Access Router (PAR) (see Section 5.1). Depending on the Mobile IP mode of operation, the source IP address is either the Home Address (in FA CoA mode) or co-located CoA (in CCoA mode). The FBU message SHOULD (when possible) be sent while the mobile node is still connected to PAR. When sent in this "predictive" mode, the fields in the FBU MUST be set as follows:

The Home Address field is either the Home Address or the co-located CoA whenever the mobile node has a co-located CoA.

The Home Agent field is set to PAR's IP address.

The Care-of Address field is the NAR's IP address (as discovered via a PrRtAdv message).

The fields in the IP header MUST be set as follows:

The Destination IP address is PAR's IP address.

The Source IP address is either the Home Address or the co-located CoA whenever the mobile node has a co-located CoA.

As a result of processing the FBU, PAR creates a binding between the address given by the mobile node in the Home Address field and NAR's IP address in its routing table. The PAR sends an FBack message (see Section 5.2) as a response to the mobile node.

The timeline for the predictive mode of operation (adapted from [rfc4068]) is shown in Figure 1.

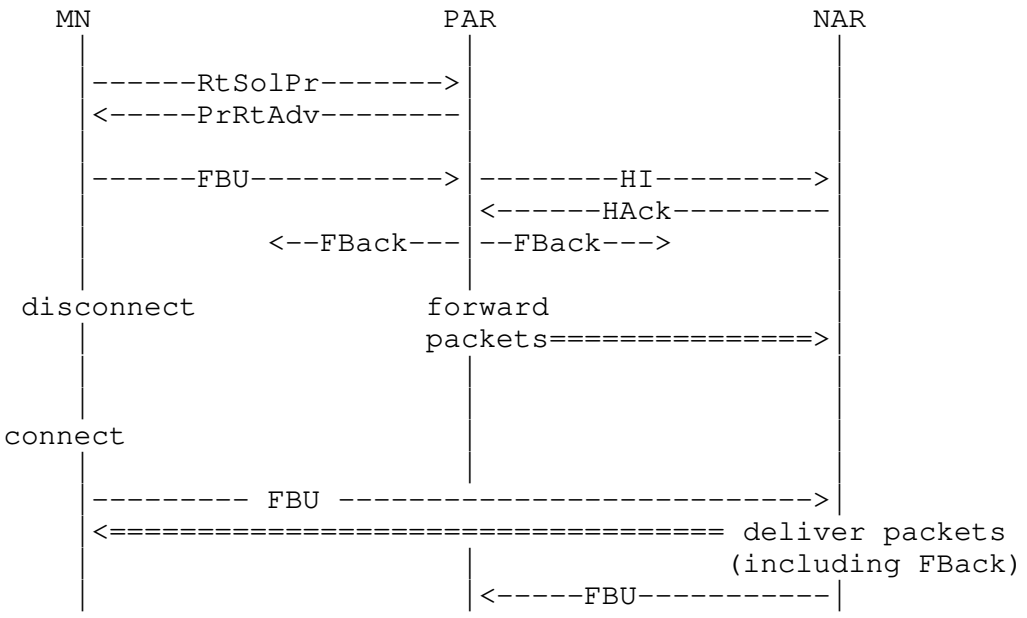

Figure 1: Predictive Fast Handover

The mobile node sends the FBU, regardless of its previous transmission, when attachment to a new link is detected. This minimally allows NAR to detect the mobile node's attachment, but also the retransmission of FBU when an FBack has not been received yet. When sent in this "reactive" mode, the Destination IP address in the IP header MUST be NAR's IP address; the rest of the fields in the FBU are the same as in the "predictive" case.

When NAR receives FBU, it may already have processed the HI message and created a host route entry for the mobile node, using either the home address or the co-located care-of address as provided by PAR. In that case, NAR SHOULD immediately forward arriving and buffered packets as well as the FBAck message. In any case, NAR MUST forward the contents of the FBU message, starting from the Type field, to PAR; the Source and Destination IP addresses in the new packet now contain the IP addresses of NAR and PAR, respectively.

The reactive mode of operation (adapted from [rfc4068]) is illustrated in Figure 2. Even though the Figure does not show the HI and HAck messages illustrated in Figure 1, these messages could already have been exchanged (in the case when the PAR has already processed the FBU sent from the previous link); if not, the PAR sends a HI message to the NAR. The FBack packet is forwarded by the NAR to the MN along with the data packets.

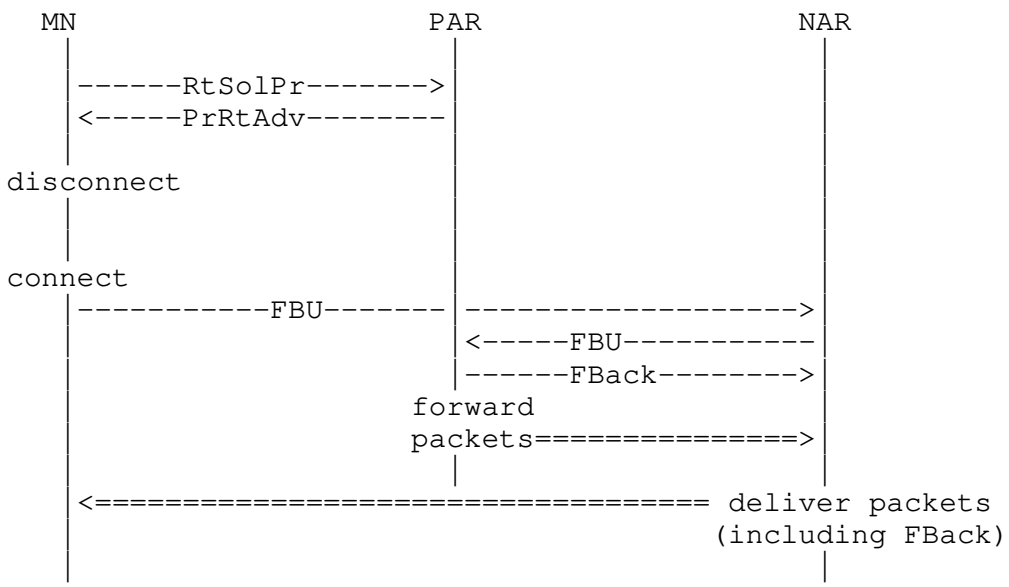

Figure 2: Reactive Fast Handover

The Handover Initiate (HI) and Handover Acknowledge (HAck) messages serve to establish a bidirectional tunnel between the routers to support packet forwarding for PCoA. The tunnel itself is established as a response to the FBU message. The PAR sends the HI message with Code = 0 when it receives FBU with source IP address set to PCoA. The PAR sends HI with Code = 1 when it receives FBU with source IP address not set to PCoA (i.e., when received from NAR). This allows NAR to disambiguate HI message processing sent as a response to predictive and reactive modes of operation. If NAR receives a HI message with Code = 1, and it has already set up a host route entry and a reverse tunnel for PCoA, it SHOULD still respond with a HAck message, using an appropriate Code value defined in Section 5.6.

The protocol provides an option for NAR to return NCoA for use by the mobile node. When NAR can provide an NCoA for exclusive use of the mobile node, the address is supplied in the HAck message. The PAR includes this NCoA in FBack. Exactly how NAR manages the address pool from which it supplies NCoA is not specified in this document. Nevertheless, the MN should be prepared to use this address instead of performing DHCP or similar operations to obtain an IPv4 address.

Even though the mobile node can obtain this NCoA from the NAR, it is unaware of the address at the time it sends an FBU. Hence, it binds PCoA to NAR's IP address as before.

5. Message Formats

This section specifies the formats for messages used in this protocol. The Code values below are the same as those in [rfc4068], and do not require any assignment from IANA.

5.1. Fast Binding Update (FBU)

The FBU format is bitwise identical to the Registration Request format in [rfc3344]. The same destination port number, 434, is used, but the FBU and FBAck messages in this specification have new message type numbers.

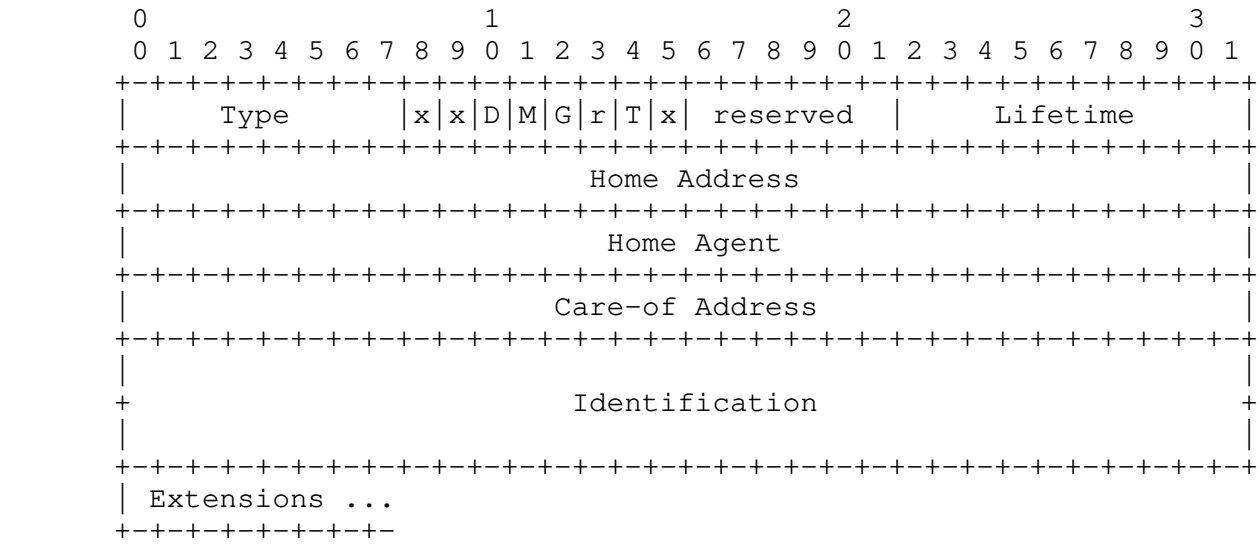

Figure 3: Fast Binding Update (FBU) Message

IP Fields:

Source address: The interface address from which the message is sent. Either PCoA (co-located or Home Address), or NAR's IP address (when forwarded from NAR to PAR).

Destination Address: The IP address of the Previous Access Router (PAR) or the New Access Router (NAR).

Source Port: variable

Destination port: 434

Message Fields:

Type: 20

Flags: See [rfc3344]. The 'S' and 'B' flags in [rfc3344] are sent as zero, and ignored on reception.

reserved: Sent as zero, ignored on reception

Lifetime: The number of seconds remaining before the binding expires. This value MUST NOT exceed 10 seconds.

Home Address: MUST be either the co-located CoA or the Home Address itself (in FA-CoA mode)

Home Agent: The Previous Access Router's global IP address

Care-of Address: The New Access Router's global IP address. Even when a New CoA is provided to the MN (see Section 5.4), NAR's IP address MUST be used for this field.

Identification: a 64-bit number used for matching an FBU with FBack. Identical to usage in [rfc3344]

Extensions: MUST contain the MN-PAR Authentication Extension (see Section 8)

The MN-PAR Authentication Extension is the Generalized Mobile IP Authentication Extension in [rfc4721] with a new Subtype for MN-PAR Authentication. The Authenticator field in the Generalized Mobile IP Authentication Extension is calculated using a shared key between the MN and the PAR. However, the key distribution itself is beyond the scope of this document, and is assumed to be performed by other means (for example, using [rfc3957]).

5.2. Fast Binding Acknowledgment (FBAck)

The FBAck format is bitwise identical to the Registration Reply format in [rfc3344].

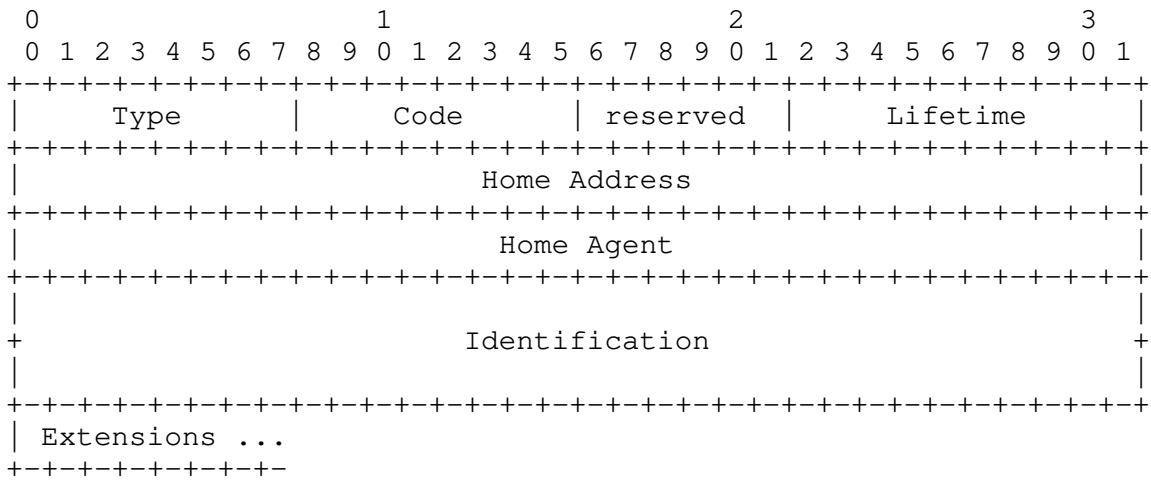

Figure 4: Fast Binding Acknowledgment (FBAck)

IP Fields:

Message Source address: Typically copied from the destination address of the FBU message

Destination Address: Copied from the Source IP address in FBU message

Source Port: variable

Destination port: Copied from the source port in FBU message

Message Fields:

Type: 21

Code: Indicates the result of processing FBU message.

0: FBU Accepted
1: FBU Accepted, NCoA supplied
128: FBU Not Accepted, reason unspecified
129: Administratively prohibited
130: Insufficient resources

reserved: Sent as zero, ignored on reception

Lifetime: The granted number of seconds remaining before binding expires.

Home Address: either the co-located CoA or the Home Address itself (in FA-Coa mode)

Home Agent: The Previous Access Router's global IP address

Identification: a 64-bit number used for matching FBU. Copied from the field in FBU for which this FBack is a reply.

Extensions: The MN-PAR Authentication extension MUST be present (see Section 8). In addition, a New IPv4 Address Option, with Option-Code 2, MUST be present when NAR supplies the NCoA (see Section 6.2).

5.3. Router Solicitation for Proxy Advertisement (RtSolPr)

Mobile Nodes send Router Solicitation for Proxy Advertisement in order to prompt routers for Proxy Router Advertisements. All the link-layer address options have the format defined in Section 6.1. The message format and processing rules are identical to those defined in [rfc4068].

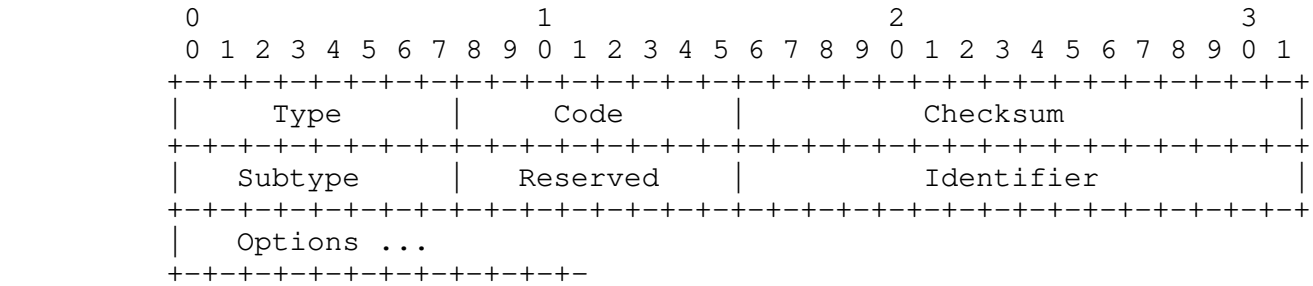

Figure 5: Router Solicitation for Proxy Advertisement (RtSolPr) Message

IP Fields:

Source Address: An IP address assigned to the sending interface

Destination Address: The address of the Access Router or the all routers multicast address.

Time-to-Live: At least 1. See [rfc1256].

ICMP Fields:

Type: 41. See Section 3 in [rfc4065].

Code: 0

Checksum: The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum and the Reserved fields are set to 0. See [rfc1256].

Subtype: 6

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

Identifier: MUST be set by the sender so that replies can be matched to this Solicitation.

Valid Options:

New Access Point Link-layer Address: The link-layer address or identification of the access point for which the MN requests routing advertisement information. It MUST be included in all RtSolPr messages. More than one such address or identifier can be present. This field can also be a wildcard address (see Section 6.1).

5.4. Proxy Router Advertisement (PrRtAdv)

Access routers send out a Proxy Router Advertisement message gratuitously if the handover is network-initiated or as a response to RtSolPr message from a mobile node, providing the link-layer address, IP address, and subnet prefixes of neighboring access routers. All the link-layer address options have the format defined in Section 6.1.

The message format and processing rules are identical to those defined in [rfc4068].

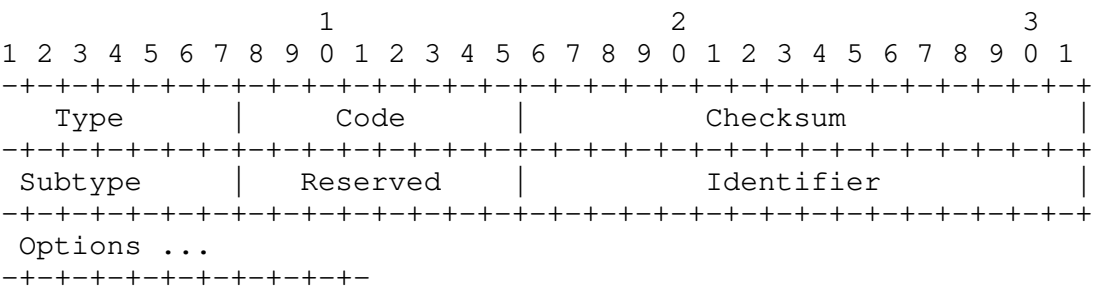

Figure 6: Proxy Router Advertisement (PrRtAdv) Message

IP Fields:

Source Address: An IP address assigned to the sending interface

Destination Address: The Source Address of an invoking Router Solicitation for Proxy Advertisement or the address of the node the Access Router is instructing to handover.

Time-to-Live: At least 1. See [rfc1256].

ICMP Fields:

Type: 41. See Section 3 in [rfc4065].

Code 0, 1, 2, 3, or 4. See below.

Checksum: The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum and the Reserved fields are set to 0. See [rfc1256].

Subtype: 7

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

Identifier: Copied from Router Solicitation for Proxy Advertisement or set to Zero if unsolicited.

Valid Options in the following order:

New Access Point Link-layer Address: The link-layer address (LLA) or identification of the access point. When there is no wildcard in RtSolPr, this is copied from the LLA (for which the router is supplying the [AP-ID, AR-Info] tuple) present in

RtSolPr. When a wildcard is present in RtSolPr, PAR uses its neighborhood information to populate this field. This option MUST be present.

New Router's Link-layer Address: The link-layer address of the Access Router for which this message is proxied. This option MUST be included when Code is 0 or 1.

New Router's IP Address: The IP address of NAR. This option MUST be included when Code is 0 or 1.

New Router Prefix Information Option: The number of leading bits that define the network number of the corresponding Router's IP Address option (see above).

New CoA Option: MAY be present, typically when PrRtAdv is sent unsolicited. PAR MAY compute new CoA by communicating with the NAR or by means not specified in this document. In any case, the MN should be prepared to use this address instead of performing DHCP or similar operations to obtain an IPv4 address. Even when it uses the New CoA provided, the MN MUST bind its current on-link address (PCoA) to that of NAR in the FBU message.

A PrRtAdv with Code 0 means that the MN should use the [AP-ID, AR-Info] tuple present in the options above. In this case, the Option-Code field (see Section 6.1) in the New AP LLA option is 1, reflecting the LLA of the access point for which the rest of the options are related, and the Option-Code for the New Router's LLA option is 3. Multiple tuples may be present.

A PrRtAdv with Code 1 means that the message is sent unsolicited. If a New IPv4 option (see Figure 10) is present following the New Router Prefix Information option (see Section 6.3), the MN SHOULD use the supplied NCoA and send the FBU immediately or else stand to lose service. This message acts as a network-initiated handover trigger. The Option-Code field (see Section 6.1) in the New AP LLA option in this case is 1 reflecting the LLA of the access point for which the rest of the options are related.

A Proxy Router Advertisement with Code 2 means that no new router information is present. The LLA option contains an Option-Code value that indicates a specific reason (see Section 6.1).

A Proxy Router Advertisement with Code 3 means that new router information is only present for a subset of access points requested. The Option-Code values in the LLA option distinguish different outcomes (see Section 6.1).

A Proxy Router Advertisement with Code 4 means that the subnet information regarding neighboring access points is sent unsolicited, but the message is not a handover trigger, unlike when the message is sent with Code 1. Multiple tuples may be present.

When a wildcard AP identifier is supplied in the RtSolPr message, the PrRtAdv message should include all available [Access Point Identifier, Link-Layer Address option, Prefix Information Option] tuples corresponding to the PAR's neighborhood.

The New CoA option may also be used when the PrRtAdv is sent as a response to a RtSolPr message. However, the solicited RtSolPr and PrRtAdv exchange for neighborhood discovery is logically decoupled from the actual handover phase involving the FBU and FBack messages (above) as well as HI and HAck messages (see below). This means the access routers have to carefully manage the supplied address due to the relative scarcity of addresses in IPv4.

5.5. Handover Initiate (HI)

The Handover Initiate (HI) is an ICMP message sent by an Access Router (typically PAR) to another Access Router (typically NAR) to initiate the process of a mobile node's handover.

The message format and processing rules are identical to those defined in [rfc4068].

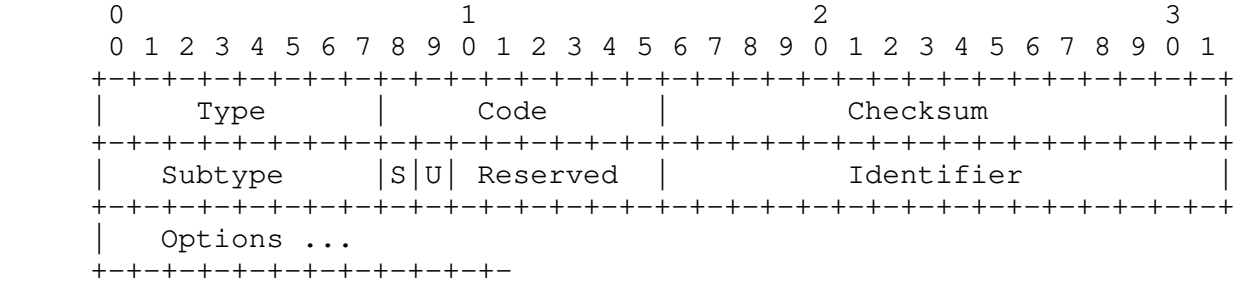

Figure 7: Handover Initiate (HI) Message

IP Fields:

Source Address: The IP address of the PAR

Destination Address: The IP address of the NAR

Time-to-Live: At least 1. See [rfc1256].

ICMP Fields:

Type: 41. See Section 3 in [rfc4065].

Code: 0 or 1. See below

Checksum: The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum and the Reserved fields are set to 0. See [rfc1256].

Subtype: 8

S: Assigned address configuration flag. When set, this message requests a new CoA to be returned by the destination. May be set when Code = 0. MUST be 0 when Code = 1.

U: Buffer flag. When set, the destination SHOULD buffer any packets towards the node indicated in the options of this message. Used when Code = 0, SHOULD be set to 0 when Code = 1.

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

Identifier: MUST be set by the sender so replies can be matched to this message.

Valid Options:

Link-layer address of MN: The link-layer address of the MN that is undergoing handover to the destination (i.e., NAR). This option MUST be included so that the destination can recognize the MN.

Previous Care-of Address: The IP address used by the MN while attached to the originating router. This option MUST be included so that a host route can be established on the NAR.

New Care-of Address: This option MAY be present when the MN wishes to use a new IP address when connected to the destination. When the 'S' bit is set, NAR MAY provide this address in HAck, in which case the MN should be prepared to use this address instead of performing DHCP or similar operations to obtain an IPv4 address.

PAR uses Code = 0 when it processes the FBU received with PCoA as source IP address. PAR uses Code = 1 when the FBU is received with NAR's IP address as the source IP address.

5.6. Handover Acknowledge (HAck)

The Handover Acknowledgment message is a new ICMP message that MUST be sent (typically by NAR to PAR) as a reply to the Handover Initiate (HI) (see Section 5.5) message.

The message format and processing rules are identical to those defined in [rfc4068].

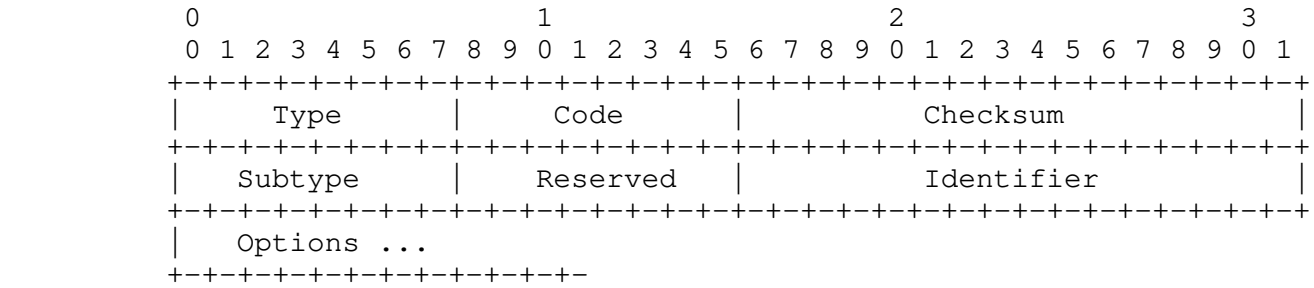

Figure 8: Handover Acknowledge (HAck) Message

IP Fields:

Source Address: Copied from the destination address of the Handover Initiate Message to which this message is a response.

Destination Address: Copied from the source address of the Handover Initiate Message to which this message is a response.

Time-to-Live: At least 1. See [rfc1256].

ICMP Fields:

Type: 41. See Section 3 in [rfc4065].

Code:

0: Handover Accepted
1: Handover Accepted, NCoA not valid
2: Handover Accepted, NCoA in use
3: Handover Accepted, NCoA assigned (used in Assigned addressing)
4: Handover Accepted, NCoA not assigned
128: Handover Not Accepted, reason unspecified
129: Administratively prohibited
130: Insufficient resources

Checksum: The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP Type. For computing the checksum, the Checksum and the Reserved fields are set to 0. See [rfc1256].

Subtype: 9

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

Identifier: Copied from the corresponding field in the Handover Initiate message this message is in response to.

Valid Options:

New Care-of Address: If the 'S' flag in the HI message is set, this option MUST be used to provide NCoA the MN should use when connected to this router. This option MAY be included even when 'S' bit is not set, e.g., Code 2 above. The MN should be prepared to use this address instead of performing DHCP or similar operations to obtain an IPv4 address.

The Code 0 is the expected average case of a handover being accepted and the routing support provided for the use of PCoA. The rest of the Code values pertain to the use of NCoA (which is common in [rfc4068]). Code values 1 and 2 are for cases when the MN proposes an NCoA and the NAR provides a response. Code 3 is when the NAR provides NCoA (which could be the same as that proposed by the MN). Code 4 is when the NAR does not provide NCoA, but instead provides routing support for PCoA.

6. Option Formats

The options in this section are specified as extensions for the HI and HAck messages, as well as for the PrRtSol and PrRtAdv messages. The Option-Code values below are the same as those in [rfc4068], and do not require any assignment from IANA.

6.1. Link-Layer Address Option Format

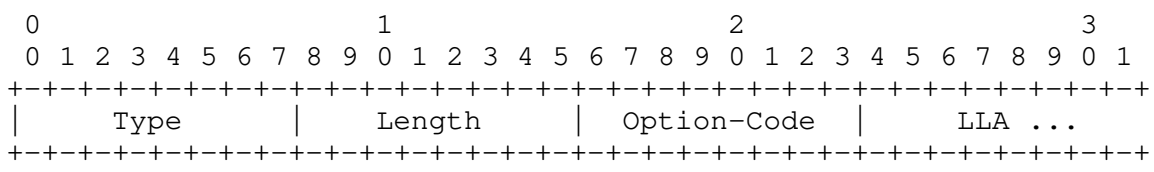

Figure 9: Link-Layer Address Option Format

Fields:

Type: 20

Option-Code:

0: Wildcard requesting resolution for all nearby access points
1: Link-Layer Address of the New Access Point
2: Link-Layer Address of the MN
3: Link-Layer Address of the NAR
4: Link-Layer Address of the source of the RtSolPr or PrRtAdv message
5: The access point identified by the LLA belongs to the current interface of the router
6: No prefix information available for the access point identified by the LLA
7: No fast handovers support available for the access point identified by the LLA

Length: The length of the option (including the Type, Length and Option-Code fields) in units of 8 octets.

Link-Layer Address: The variable-length link-layer address. The content and format of this field (including byte and bit ordering) depends on the specific link-layer in use.

There is no length field for the LLA itself. Implementations MUST determine the length of the LLA based on the specific link technology where the protocol is run. The total size of the LLA option itself MUST be a multiple of 8 octets. Hence, padding may be necessary depending on the size of the LLA used. In such a case, the padN option [rfc2460] MUST be used. As an example, when the LLA is 6 bytes (meaning 7 bytes of padding is necessary to bring the LLA option length to 2), the padN option will have a length field of 5 and 5 bytes of zero-valued octets (see [rfc2460]).

6.2. New IPv4 Address Option Format

This option is used to provide the new router's IPv4 address or the NCoA in PrRtAdv, as well as PCoA and NCoA in HI and HAck messages.

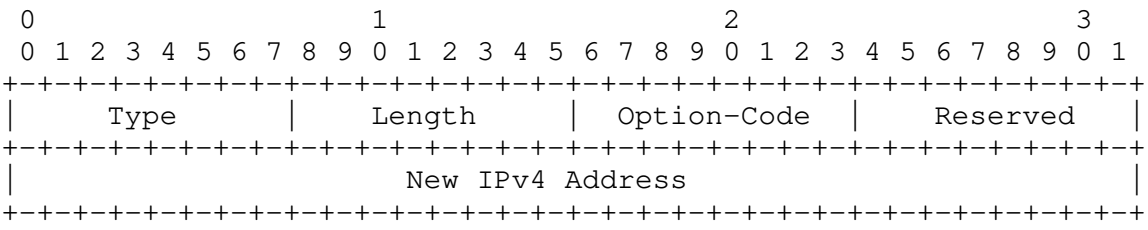

Figure 10: New IPv4 Address Option Format

Fields:

Type: 21

Length: The length of the option (including the Type, Length and Option-Code fields) in units of 8 octets.

Option-Code:

1: Previous CoA
2: New CoA
3: NAR's IP Address

Reserved: Set to zero.

New IPv4 Address: NAR's IPv4 address or the NCoA assigned by NAR.

6.3. New Router Prefix Information Option

This option is used in the PrRtAdv message.

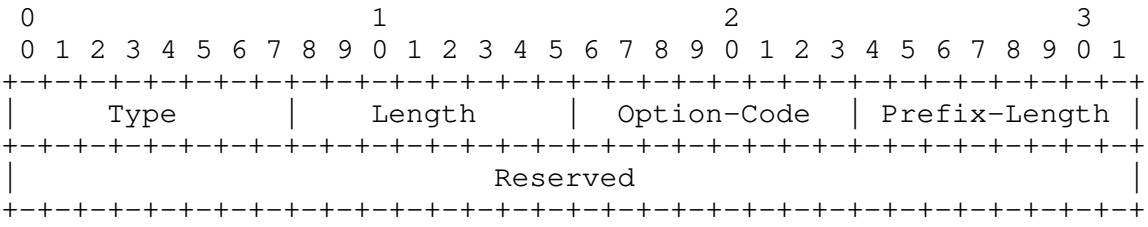

Figure 11: New Router Prefix Information Option Format

Fields:

Type: 22

Length: The length of the option (including the Type, Length and Option-Code fields) in units of 8 octets.

Option-Code: 0

Prefix-Length The number of leading bits that define the network number of the corresponding Router's IP Address option.

Reserved: Set to zero.

7. Security Considerations

As outlined in [rfc4068], the following vulnerabilities are identified and the solutions mentioned.

Insecure FBU:

Failure to protect the FBU message could result in packets meant for an address being stolen or redirected to some unsuspecting node. This concern is similar to that in Mobile Node and Home Agent relationship.

Hence, the FBU and FBack messages MUST be protected using a security association shared between a mobile node and its access router. In particular, the MN-PAR Authentication Extension MUST be present in each of these messages. This document does not specify how the security association is established between an MN and the AR/FA.

Secure FBU, malicious or inadvertent redirection:

Even if the MN-PAR authentication extension is present in an FBU, an MN may inadvertently or maliciously attempt to bind its PCoA to an unintended address on NAR's link, and cause traffic flooding to an unsuspecting node.

This vulnerability is avoided by always binding the PCoA to the NAR's IP address, even when the NAR supplies an NCoA to use for the MN. It is still possible to jam NAR's buffer with redirected traffic. However, the handover state corresponding to the MN's PCoA has a finite lifetime, and can be configured to be a few multiples of the anticipated handover latency. Hence, the extent of this vulnerability is small. It is possible to trace the culprit MN with an established security association at the access router.

Communication between the access routers:

The access routers communicate using HI and HAck messages in order to establish a temporary routing path for the MN undergoing handover. This message exchange needs to be secured to ensure routing updates take place as intended.

The HI and HAck messages need to be secured using a preexisting security association between the access routers to ensure at least message integrity and authentication, and SHOULD also include encryption. IPsec ESP SHOULD be used.

8. IANA Considerations

The IANA assignments made for messages, extensions, and options specified in this document are described in the following paragraphs.

This document defines two new messages that use the Mobile IPv4 control message format [rfc3344]. These message details are as follows:

Type	Description	Reference
20	FBU	Section 5.1
21	FBAck	Section 5.2

This document defines four new experimental ICMP messages that use the ICMP Type 41 for IPv4. See Section 3 in [rfc4065]. The new messages specified in this document have been assigned Subtypes from the registry in [rfc4065]:

Subtype	Description	Reference
6	RtSolPr	Section 5.3
7	PrRtAdv	Section 5.4
8	HI	Section 5.5
9	HAck	Section 5.6

This document defines three new options that have been assigned Types from the Mobile IP Extensions for ICMP Router Discovery messages [rfc3344]. These options are as follows:

Type	Description	Reference
20	LLA	Section 6.1
21	New IPv4 Address	Section 6.2
22	NAR Prefix Info	Section 6.3

The MN-PAR Authentication Extension described in Sections 5.1 and 5.2 is a Generalized Mobile IP Authentication Extension defined in Section 5 of [rfc4721]. The MN-PAR Authentication has been assigned a Subtype from the registry specified in [rfc4721]. The Extension details are as follows:

Subtype	Description	Reference
4	MN-PAR Auth Extension	Section 5.1

9. Acknowledgments

Thanks to all those who expressed interest in having a Fast Handovers for Mobile IPv4 protocol along the lines of [rfc4068]. Thanks to Vijay Devarapalli, Kent Leung, and Domagoj Premec for their review and input. Kumar Viswanath and Uday Mohan implemented an early version of this protocol. Many thanks to Alex Petrescu for his thorough review that improved this document. Thanks to Pete McCann for the proofreading, and to Jari Arkko for the review, which have helped improve this document. Thanks to Francis Dupont and Hannes Tschofenig for the GEN-ART and TSV-DIR reviews.

Sending FBU from the new link (i.e., reactive mode) is similar to using the extension defined in [mip4-ro]; however, this document also addresses movement detection and router discovery latencies.

10. References

10.1. Normative References

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

[rfc1256] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[rfc2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[rfc3344] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[rfc4065] Kempf, J., "Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations", RFC 4065, July 2005.

[rfc4068] Koodli, R., Ed., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[rfc4721] Perkins, C., Calhoun, P., and J. Bharatia, "Mobile IPv4 Challenge/Response Extensions (Revised)", RFC 4721, January 2007.

10.2. Informative References

[fh-ccr] R. Koodli and C. E. Perkins, "Fast Handovers and Context Transfers in Mobile Networks", ACM Computer Communications Review Special Issue on Wireless Extensions to the Internet, October 2001.

[ieee-802.11r] IEEE, "IEEE Standard for Local and Metropolitan Area Networks: Fast Roaming/Fast BSS Transition, IEEE Std 802.11r", September 2006.

[ieee-802.1x] IEEE, "IEEE Standards for Local and Metropolitan Area Networks: Port-based Network Access Control, IEEE Std 802.1X-2001", June 2001.

[ieee-802.21] The IEEE 802.21 group, http://www.ieee802.org/21.

[mi-book] R. Koodli and C. E. Perkins, "Mobile Internetworking with IPv6: Concepts, Principles and Practices", John Wiley & Sons, June 2007.

[mip4-ro] Perkins, C. and D. Johnson, "Route Optimization in Mobile IP", Work in Progress, September 2001.

[rfc2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[rfc3957] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

Authors' Addresses

Rajeev Koodli
Nokia Siemens Networks
313 Fairchild Driive
Mountain View, CA 94043
USA

EMail: rajeev.koodli@nokia.com

Charles Perkins
Nokia Siemens Networks
313 Fairchild Driive
Mountain View, CA 94043
USA

EMail: charles.perkins@nokia.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

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.

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.

Intellectual Property

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.