

Network Working Group
Request for Comments: 4433
Category: Standards Track

M. Kulkarni
A. Patel
K. Leung
Cisco Systems Inc.
March 2006

Mobile IPv4 Dynamic Home Agent (HA) Assignment

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

Mobile IPv4 (RFC 3344) uses the home agent (HA) to anchor sessions of a roaming mobile node (MN). This document proposes a messaging mechanism for dynamic home agent assignment and HA redirection. The goal is to provide a mechanism to assign an optimal HA for a Mobile IP session while allowing any suitable method for HA selection.

Table of Contents

1. Introduction	3
2. Requirements Terminology	3
3. Problem Statement	5
3.1. Scope	5
3.2. Dynamic Home Agent Discovery in Mobile IPv4	5
3.3. NAI Usage and Dynamic HA Assignment	6
3.4. Dynamic HA Extension	6
3.4.1. Requested HA Extension	7
3.4.2. Redirected HA Extension	7
4. Messaging Mechanism for Dynamic HA Assignment/Redirection	7
4.1. Messaging for Dynamic HA Assignment	7
4.1.1. Example with Message Flow Diagram	8
4.2. Messaging for HA Redirection	10
4.2.1. Example with Message Flow Diagram	12
5. Mobility Agent Considerations	14
5.1. Mobile Node Considerations	14
5.1.1. MN Using FA CoA	14
5.1.2. MN Using Co-Located CoA	15
5.1.3. Refreshing Assigned HA Address on Mobile Node	16
5.2. Foreign Agent Considerations	16
5.3. Home Agent Considerations	17
5.3.1. Assigned Home Agent Considerations	17
6. Requested Home Agent Selection	19
7. Error Values	20
8. IANA Considerations	20
9. Security Considerations	20
10. Backward-Compatibility Considerations	21
11. Acknowledgements	23
12. Normative References	23

1. Introduction

This document adds to the Mobile IP protocol [1], by proposing a messaging mechanism for dynamic home agent assignment and home agent redirection during initial registration. The goal is to assign an optimal HA for a Mobile IP session. The mobile node MUST use the Network Access Identifier (NAI) extension [2] when requesting a dynamically assigned HA.

The MN requests a dynamically assigned HA by setting the HA field in the initial Registration Request to ALL-ZERO-ONE-ADDR (defined in Section 2). If the request is accepted, the HA sends a successful Registration Reply containing the HA's own address. The requested HA can suggest an alternate HA and if so, the Registration Reply is rejected with a new error code REDIRECT-HA-REQ and the alternate HA address is specified in a new extension (Redirected HA Extension).

This document also defines a new Requested HA Extension for use in Registration Requests when the HA field is set to ALL-ZERO-ONE-ADDR. The Requested HA address is a hint to the network about the MN's preferred HA.

The messaging mechanism is defined in this document so that the MN can request and receive a dynamic HA address in Mobile IP messages. However, the mechanism by which the network selects an HA for assignment to the MN is outside the scope of this document. For example, the selection may be made by any network node that receives the Registration Request (or information about the Registration Request), such as a Foreign Agent, AAA server, or home agent. The node that selects the HA may select one based on a number of criteria, including but not limited to HA load-balancing, geographical proximity, administrative policy, etc.

2. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [6].

The Mobile-IP-related terminology described in RFC 3344 [1] is used in this document. In addition, the following terms are used:

ALL-ZERO-ONE-ADDR: IP address 0.0.0.0 or 255.255.255.255. An address of 255.255.255.255 indicates a preference for an HA in the home domain. An address of 0.0.0.0 indicates no preference for home vs. visited domain.

Requested HA: Destination IP address of home agent that the Registration Request is sent to. Must be a unicast IP address. This address can be obtained as described in Section 6.

Note that this specification defines a new "Requested HA Extension" in Section 3.4, which is different from the term "Requested HA".

Assigned HA: The HA that accepts an MN's Registration Request and returns a successful Registration Reply.

Redirected HA: If the registration is rejected with error code REDIRECT-HA-REQ, the HA being referred to is specified in a new extension (Redirected HA Extension).

AAA server: Authentication, Authorization, and Accounting Server.

DNS: Domain Name System.

DHCP: Dynamic Host Configuration Protocol.

MN: Mobile node as defined in Mobile IPv4 [1].

HA: Home agent as defined in Mobile IPv4 [1].

FA: Foreign Agent as defined in Mobile IPv4 [1].

CoA: Care-of Address.

CCoA: Co-located Care-of Address.

MN HoA: Mobile node's home address.

NAI: Network Access Identifier [2].

Src IP: Source IP address of the packet.

Dest IP: Destination IP address of the packet.

RRQ: Registration Request.

3. Problem Statement

The Mobile IPv4 NAI Extension for IPv4 [2] introduced the concept of identifying an MN by the NAI and enabling dynamic home address assignment. When the home address is dynamically assigned, it is desirable to discover the home agent dynamically or inform the MN about an optimal HA to use for a multitude of reasons, such as:

- If the distance between the visited network and the home network of the mobile node is large, the signaling delay for these registrations may be long. In such a case, the MN will be anchored to its distant home agent, resulting in tunneled traffic traveling a long distance between home agent and the mobile node. When a Mobile IP session initiates, if the mobile node can be assigned a home agent that is close to the mobile node it can drastically reduce the latency between the home agent and mobile node.
- In a large-scale Mobile IP deployment, it is cumbersome to provision MNs with multiple HA addresses.
- It is desirable to achieve some form of load balancing between multiple HAs in the network. Dynamic HA assignment and/or HA redirection lets the network select the optimal HA from among a set of HAs and thus achieve load balancing among a group of HAs.
- Local administrative policies.

3.1. Scope

This specification does not address the problem of distributing a security association between the MN and HA, and it can either be statically preconfigured or dynamically distributed using other mechanisms [7].

The document introduces the terms Requested/Assigned/Redirected HA (Section 6). The discovery of candidate HA addresses for insertion into the Redirected HA Extension can be accomplished through various means that are network and/or deployment specific and hence are outside the scope of this specification.

The MN MAY request dynamic HA assignment when it is not aware of any HA address and even when it is aware of at least one HA address.

3.2. Dynamic Home Agent Discovery in Mobile IPv4

Mobile IPv4 [1] specifies the mechanism for discovering the mobile node's home agent using subnet-directed broadcast IP address in the home agent field of the Registration Request. This mechanism was

designed for mobile nodes with a static home address and subnet prefix, anchored on fixed home network. However, using subnet-directed broadcast as the destination IP address of the Registration Request, it is unlikely that the Registration Request will reach the home subnet because routers will drop these packets by default. See CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks [3].

3.3. NAI Usage and Dynamic HA Assignment

The Mobile IPv4 NAI Extension for IPv4 [2] introduced the concept of identifying an MN by the NAI and enabling dynamic home address assignment. This document requires that while using dynamic HA assignment, MN MUST use the NAI and obtain a home address. MN can still suggest a static home address in the Registration Request, but must take the address in the Registration Reply as the home address for the session. This is compatible with the procedures documented in the NAI specification [2].

3.4. Dynamic HA Extension

The Dynamic HA Extension, shown in Figure 1, contains the address of the HA. This is a generic extension and can be used in Registration Request and Reply messages. It is a skippable extension.

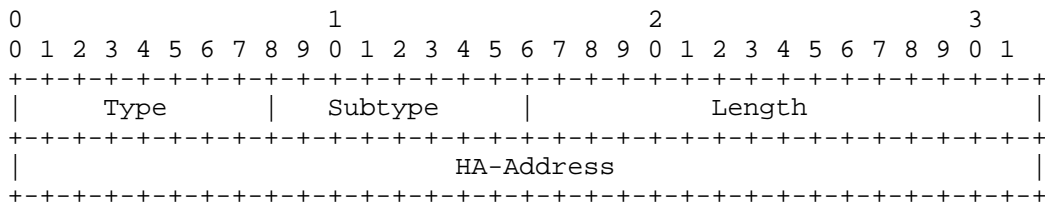


Figure 1: The Dynamic HA Address Extension

- Type DYNAMIC-HA-ADDRESS (skippable) 139 is the type, which specifies the dynamic HA address.
- Subtype Defines the use of this extension as:
 - subtype 1 = Requested HA Extension
 - 2 = Redirected HA Extension
- Length Indicates the length of the extension not including the type, subtype, and length fields. Length is always 4 bytes.
- HA-Address Address of the home agent.

3.4.1. Requested HA Extension

The Requested HA Extension is a Dynamic HA Extension of subtype 1.

The MN may include the Requested HA Extension in the Registration Request as a hint to the network where it wishes to be anchored.

This extension contains the address of the HA. A valid unicast IP address MUST be used as HA address in this extension.

In absence of an FA, the Registration Request is forwarded to this HA. In presence of an FA, the FA MUST forward the Registration Request to the HA address in this extension.

3.4.2. Redirected HA Extension

The Redirected HA Extension is a Dynamic HA Extension of subtype 2.

The Redirected HA Extension contains the address of the HA where the MN should attempt the next registration. The HA receiving a Registration Request can suggest an alternate HA and, if so, the Registration Reply is sent with a new error code REDIRECT-HA-REQ and the alternate HA address is specified in this extension.

The Redirected HA Extension MUST be included in Registration Reply when the reply code is REDIRECT-HA-REQ.

4. Messaging Mechanism for Dynamic HA Assignment/Redirection

This specification presents two alternatives for home agent assignment:

- (a) Dynamic HA assignment (described in Section 4.1) and
- (b) HA redirection (described in Section 4.2).

4.1. Messaging for Dynamic HA Assignment

The following sequence of events occurs when the MN requests dynamic home agent assignment:

1. The MN sets the Home Agent address field in the Registration Request to ALL-ZERO-ONE-ADDR. If the MN is aware of a desired HA address, it can add that address in the Requested HA Extension in the Registration Request. If the HA does not support the Requested HA Extension, see step 2 below.

2. This step is applicable, in lieu of step 1, for an MN that is aware of the HA address and desires dynamic HA assignment. Also, the MN follows this (when aware of a HA address) when it discovers a legacy FA in the path or if the known HA does not support the Requested HA Extension (see Section 10).

The MN sets the Home Agent address field in the Registration Request to the HA address (instead of setting it to ALL-ZERO-ONE-ADDR). The MN also adds the same HA address in the Requested HA Extension in the Registration Request.

3. The MN (if using co-located CoA and registering directly with the HA) or the FA (if the MN is registering via the FA) sends the Registration Request to the "Requested HA". If the Requested HA Extension is present, Requested HA is specified in the "HA Address" of this extension.

Per Section 10, in case of a legacy FA, legacy FA forwards the Registration Request to the address in the HA field of the request (thus, MN uses step 2 above in case of legacy FA instead of step 1).

4. The "Requested HA" is the home agent that processes the Registration Request in accordance with Mobile IPv4 [1] and as per the specification in this document. It creates mobility binding for a successful Registration Request. It also sends a Registration Reply to the MN.
5. The MN obtains an "Assigned HA" address from the HA field in the successful Registration Reply and uses it for the remainder of the session. (Note that the "Assigned HA" will be the same as the "Requested HA".)
6. Subsequent Registration Request messages for renewal are sent to the Assigned HA.

Section 5.3.1 describes the Assigned HA in detail. Some ideas on how to select the Requested HA are briefly covered in Section 6.

4.1.1.1. Example with Message Flow Diagram

Detailed explanation of this alternative is best described with the help of a message flow diagram and description.

Figure 2 shows one specific example of a mobile node using an FA-located Care-of Address (FA CoA) and FA understands the Requested HA Extension per this specification.

Other scenarios such as when the mobile node uses a co-located care of address and presence of a legacy HA or FA are not described below, but the behavior is similar.

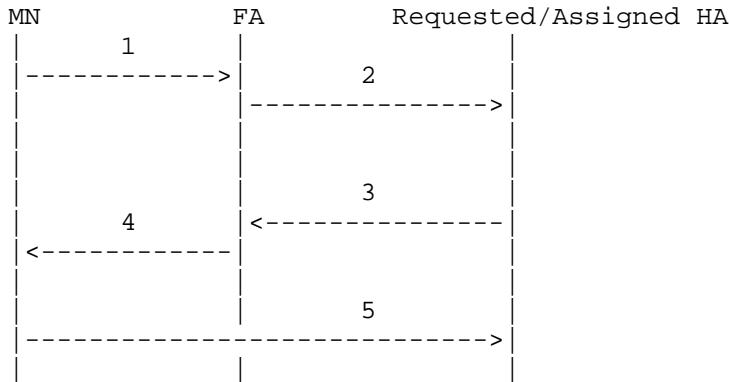


Figure 2: Example Message Flow for Dynamic HA Assignment

1. The MN sets the Home Agent address field in the Registration Request to ALL-ZERO-ONE-ADDR. Since the MN is using FA CoA in this example, it sends the Registration Request to the FA. The Registration Request is formatted as follows:

Src IP=	Dest IP =	MN HoA	HA Address =	CoA =
MN	FA		ALL-ZERO-ONE-ADDR	FA CoA

If the MN is aware of a desired HA address, it can add that address in the Requested HA Extension in Registration Request as a hint. That extension is not shown above.

2. The FA sends the Registration Request to the Requested HA. If the Requested HA Extension is present, Requested HA is the HA address in this extension. If the Requested HA Extension is not present, the FA determines the Requested HA through means outside the scope of this specification. The Registration Request is formatted as follows:

Src IP=	Dest IP =	MN HoA	HA Address =	CoA =
FA	Requested HA		ALL-ZERO-ONE-ADDR	FA CoA

(If MN includes the Requested HA Extension, the FA copies that extension. The FA then forwards the Registration Request, along with the Requested HA Extension, to the HA address specified in Requested HA Extension.)

3. The HA processes the Registration Request in accordance with Mobile IPv4 [1] and the messaging defined in this document. The HA creates mobility binding for successful request and becomes the Assigned HA. The HA then sends a Registration Reply to the FA, which is formatted as follows:

```

+-----+
| Src IP=| Dest IP = | MN HoA | HA Address = | CoA = |
|Assigned| Src IP of |       | Assigned HA  | FA CoA/|
|  HA   | the RRQ   |       |              |        |
+-----+

```

4. The FA relays the Registration Reply to the MN, as follows:

```

+-----+
| Src IP=| Dest IP = | MN HoA | HA Address = | CoA = |
|  FA   |   MN     |       | Assigned HA  | FA CoA/|
+-----+

```

5. The MN obtains the Assigned HA address from the HA field in the successful Registration Reply and uses it for the remainder of the session. The MN sends subsequent Re-Registration or De-Registration Requests for the remainder session directly to the Assigned HA. The Home Agent address field in this Registration Request is set to ALL-ZERO-ONE-ADDR. Note that the Assigned HA is the same as the Requested HA.

4.2. Messaging for HA Redirection

This section describes the events that occur when the Requested HA does not accept the Registration Request and redirects the mobile node to another HA (aka Redirected HA) instead. This behavior is not exhibited by a legacy HA and so is not referred in the description below. In presence of a legacy FA, please refer to Section 4.1 for the specific field in the Registration Request.

1. The MN sets the Home Agent address field in the Registration Request to ALL-ZERO-ONE-ADDR.

2. The MN (if using co-located CoA and registering directly with the HA) or FA (if the MN is registering via the FA) sends the Registration Request to the "Requested HA". If the MN is aware of an HA address, it can add that address in the Requested HA Extension in the Registration Request.
3. When the HA receives the Registration Request, if the HA field is set to ALL-ZERO-ONE-ADDR, the HA may reject the request with Reply code REDIRECT-HA-REQ and suggest an alternate HA.

The HA may reject the request for a number of reasons, which are outside the scope of this specification. If the HA rejects the Request, the HA field in the Reply is set to this HA's address. The IP address of the HA that is the target of the redirection is specified in Redirected HA Extension. The presence of this extension is mandatory when the reply code is set to REDIRECT-HA-REQ. HA sends the Reply to the FA/MN.

4. FA sends the Reply to the MN.
5. If the error code is set to REDIRECT-HA-REQ, the MN obtains the HA address from Redirected HA Extension. The MN then sends a Registration Request to Redirected HA. The MN may choose to add Requested HA Extension in this new Registration Request. If a registration loop occurs (the case when the Redirected HA is an HA that had already directed the MN to register elsewhere), then the MN stops sending any further Registration Request and provides an indication that the loop event was detected. The number of consecutive Redirected HAs remembered by the MN for loop detection is an implementation parameter.

4.2.1. Example with Message Flow Diagram

Figure 3 shows one specific example of a mobile node using FA-located Care-of Address, where the FA is not a legacy FA.

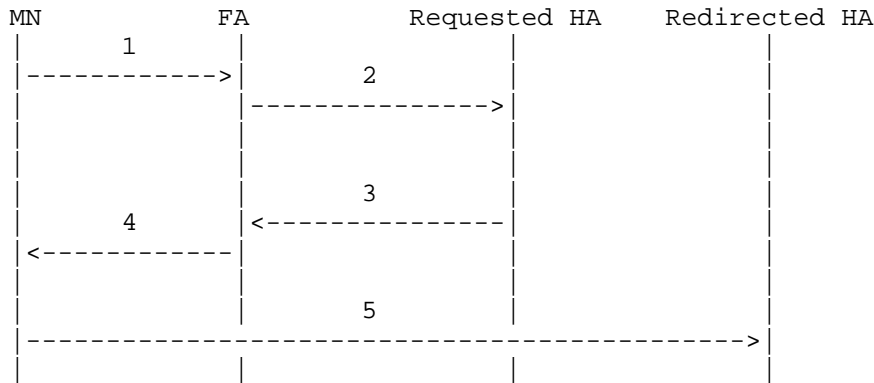


Figure 3: Example Message Flow for HA Redirection

1. The MN sets the Home Agent address field in the Registration Request to ALL-ZERO-ONE-ADDR. Since the MN is using FA CoA in this example, it sends the Registration Request to the FA. The Registration Request is formatted as follows:

Src IP= MN	Dest IP = FA	MN HoA	HA Address = ALL-ZERO-ONE-ADDR	CoA = FA CoA
---------------	-----------------	--------	-----------------------------------	-----------------

If the MN is aware of an HA address, it can add that address in the Requested HA Extension in the Registration Request as a hint. That extension is not shown above.

2. The FA sends the Registration Request to the Requested HA. If Requested HA Extension is present, Requested HA is the HA address in this extension. If the Requested HA Extension is not present, the FA determines the Requested HA through means outside the scope of this specification. The Registration Request is formatted as follows:

Src IP= FA	Dest IP = Requested HA	MN HoA	HA Address = ALL-ZERO-ONE-ADDR	CoA = FA CoA
---------------	---------------------------	--------	-----------------------------------	-----------------

3. The HA processes the Registration Request in accordance with Mobile IPv4 [1] and the messaging defined in this specification. If the registration is successful, but local configuration/administrative policy, etc., directs the HA to refer the MN to another HA, the HA rejects the request with error code REDIRECT-HA-REQ. The HA fills in the address of the Redirected HA in the Redirected HA Extension. The HA then sends Registration Reply reject to the FA, which is formatted as follows:

```

+-----+
| Src IP=| Dest IP = | MN HoA | HA Address = | CoA = |
| FA     | Src IP of |       | HA           | FA CoA |
| HA     | the RRQ   |       |              |        |
+-----+
| Redirected HA Extension ... |
+-----+

```

4. The FA relays the Registration Reply to the MN, as follows:

```

+-----+
| Src IP=| Dest IP = | MN HoA | HA Address = | CoA = |
| FA     | MN       |       | HA           | FA CoA/ |
+-----+
| Redirected HA Extension ... |
+-----+

```

5. If the MN can authenticate the Reply, the MN extracts the HA address from the Redirected HA Extension. The MN then sends a Registration Request to the Redirected HA, unless it has already received a redirection response from that HA while processing the Registration Request. The MN may choose to add Requested HA Extension in this new Registration Request.

5. Mobility Agent Considerations

The following sections describe the behavior of each mobility agent in detail.

5.1. Mobile Node Considerations

The mobile node MUST use the NAI extension for home address assignment when using the messaging mechanism in this document. Since MN uses the NAI extension, the Home Address field is set to 0.0.0.0.

While dynamic HA assignment is in progress and the MN has not successfully anchored at a home agent, the MN MUST set the Home Agent field in the Registration Request to an ALL-ZERO-ONE-ADDR, which is either 255.255.255.255 or 0.0.0.0.

The Registration Request MUST be protected by a valid authenticator as specified in Mobile IPv4 [1] or Mobile IPv4 Challenge/Response Extensions [5]. Configuring security associations is deployment specific and hence outside the scope of this specification. The security associations between an MN and an individual HA may also be dynamically derived during the dynamic HA assignment, based on a shared secret between MN and AAA infrastructure [7].

The mobile node MUST maintain the remaining Mobile IP session with the Assigned HA.

As mentioned in the Security Considerations (Section 9), there is a possibility of more than one HA creating a mobility binding entry for a given MN, if a rogue node in the middle captures the Registration Request and forwards it to other home agents. The MN can mitigate such condition by using a short lifetime (e.g., 5 seconds) in the Registration Request with the Home Agent field set to ALL-ZERO-ONE-ADDR.

The following sections describe MN behavior in FA CoA mode and co-located CoA mode.

5.1.1. MN Using FA CoA

When a mobile node initiates a Mobile IP session requesting dynamic HA assignment, it MUST set the home agent address field in the Registration Request to ALL-ZERO-ONE-ADDR. The destination IP address of the Registration Request is the FA. The FA will determine the Requested HA and forward the Registration Request to the Requested HA. Registration Request processing takes place on the Requested HA as per the specification in this document.

The Registration Request MUST be appropriately authenticated for the HA to validate the Request.

If a successful Registration Reply is received, the MN obtains the Assigned HA from the HA field of Reply. The Assigned HA address will be the same as the Requested HA Extension, if it was included in the Registration Request by the MN.

If a Registration Reply is received with code REDIRECT-HA-REQ, the MN MUST authenticate the Reply based on HA address in HA field of Reply and attempt Registration with the HA address specified in the Redirected HA Extension. The MN MUST put the Redirected HA address as the Requested HA Extension of the new Registration Request.

In some cases, for the first Registration Request the MN may want to hint to the network to be anchored at a specific HA. The MN SHOULD put that address in the HA address of the Requested HA Extension.

5.1.2. MN Using Co-Located CoA

An MN in co-located CoA mode requesting dynamic HA assignment MUST set the home agent address field in the Registration Request to ALL-ZERO-ONE-ADDR. The destination IP address of the Registration Request is the Requested HA. Some ideas on how to select a Requested HA are briefly covered in Section 6.

If a successful Reply is received, the MN obtains the Assigned HA address from the successful Registration Reply. The Assigned HA will be the same as Requested HA to which the Registration Request was sent. The MN MUST cache the Assigned HA address for the length of the Mobile IP session. The mobile node then MUST use this previously cached Assigned HA address as the home agent address in subsequent Re-Registration and De-Registration Request(s). This will make sure that for the duration of the Mobile IP session, the mobile node will always be anchored to the assigned home agent with which it was initially registered.

If a Registration Reply is received with code REDIRECT-HA-REQ, the MN MUST authenticate the Reply based on HA address in HA field of Reply and attempt Registration with the HA address specified in the Redirected HA Extension. The MN MUST put the Redirected HA in the Requested HA Extension of the new Registration Request.

In some cases, for the first Registration Request MN may want to hint to the network to be anchored at a specific HA and the MN SHOULD put that address in the HA address of the Requested HA Extension.

While requesting dynamic HA assignment and registering directly with an HA, the Requested HA Extension MUST be included and MUST contain the address of the HA to which the Registration Request is sent. When using co-located CoA but registering via a legacy FA, the HA field in the Registration Request may be set to Requested HA.

If the Registration Request contains the Requested HA Extension, the HA address in that extension MUST match the destination IP of the Request.

5.1.3. Refreshing Assigned HA Address on Mobile Node

When the Mobile IP session terminates, the mobile node MAY clear the Assigned HA address cached as the home agent address. It MAY request a new HA address for the new Mobile IP session by not including the Requested HA Extension. The advantage of this approach is that the mobile node will be always anchored to an optimal home agent from where it initiated the Mobile IP session.

Alternately, the MN may save the Assigned HA address and use it in the Requested HA Extension along with ALL-ZERO-ONE-ADDR HA address in Registration Request for a new Mobile IP session.

5.2. Foreign Agent Considerations

When the mobile node is using an FA CoA, it always registers via the FA. When the MN is using a co-located CoA, it may register through an FA or it may register directly with an HA, unless the R bit is set in the FA's agent advertisement, in which case it always registers through the FA.

When the FA receives a Registration Request with HA address field set to ALL-ZERO-ONE-ADDR that doesn't contain the Requested HA Extension, the FA obtains the Requested HA address to forward the Registration Request using means outside the scope of this specification. Some ideas on how to select a Requested HA are briefly covered in Section 6.

If the FA cannot obtain the Requested HA to which to forward a Registration Request from the MN, it MUST reject request with error code NONZERO-HA-REQD.

If the MN has included the Requested HA Extension, the FA MUST forward the Registration Request to the address in this extension. If the HA address in this extension is not a routable unicast address, the FA MUST reject the request with error code NONZERO-HA-REQD.

If the Registration Request contains the Requested HA Extension, the FA uses that address as the destination for the relayed Registration Request.

Backward-compatibility issues related to the mobility agents are addressed in Section 10.

5.3. Home Agent Considerations

A home agent can process an incoming Registration Request in one of the following two ways:

1. The MN or FA sends the Registration Request to the Requested HA. The term Requested HA has meaning in the context of a Registration Request message. When the Requested HA successfully processes the Registration Request and creates a binding and sends a Reply with its address, it becomes the Assigned HA. The term Assigned HA is meaningful in the context of a Registration Reply message.
2. A home agent receiving a Registration Request with HA field set to ALL-ZERO-ONE-ADDR MAY reject the request even if successfully authenticated and suggest an alternate HA address in Reply. In such a case, the HA puts its own address in HA field of Reply and sets the Reply code to REDIRECT-HA-REQ and adds the Redirected HA Extension.

If the Registration Request contains the Requested HA Extension, the HA address in that extension must match the destination IP of the Request. If it does not match, the Requested HA MUST reject the Registration Request with error code 136.

5.3.1. Assigned Home Agent Considerations

The HA that processes the incoming Registration Request fully in accordance with Mobile IPv4 [1] and this specification becomes the Assigned HA. The Registration Request terminates at the Assigned HA.

The Assigned HA creates one mobility binding per MN and sends the Registration Reply to the MN by copying its address in the Home Agent field and as the source IP address of the Reply.

The following table summarizes the behavior of the Assigned HA, based on the value of the destination IP address and Home Agent field of the Registration Request.

Dest IP Addr	HA field	Processing at Assigned HA
Unicast (Must be equal to the HA receiving the RRQ)	non-unicast	Mobile IPv4 [1]: There is no change in handling for this case from Mobile IPv4. It is mentioned here for reference only. HA denies the registration with error code 136 and sets HA field to its own IP address in the reply as per Section 3.8.3.2 in [1].
	ALL-ZERO-ONE-ADDR	New Behavior: Accept the RRQ as per this specification. Authenticate the RRQ and create mobility binding if the HA is acting as Assigned HA. Set HA field to its own IP address in the Registration Reply.

OR

New Behavior: If authentication is successful, reject RRQ with a new error code REDIRECT-HA-REQ. HA puts its address in HA address field of Reject. HA suggests an alternate HA to use in the new Redirected HA Extension.

Table 1: Registration Request Handling at Assigned HA

As per the messaging proposed here, the mobile node (or the foreign agent) sends the Registration Request to the Requested HA address, which is a unicast address. Therefore, this document does not specify any new behavior for the case where the HA receives a subnet directed broadcast Registration Request as specified in Section 3.8.2.1 of the Mobile IPv4 specification [1]. Although the Home Agent field in the Registration Request is not a unicast address, the destination IP address is a unicast address. This avoids the problem associated with subnet-directed broadcast destination IP address that may result in multiple HAs responding. Thus, there is no need to deny the registration as stated in Mobile IPv4 [1] Section 3.8.3.2.

When the destination IP address is a unicast address and the Home Agent field is ALL-ZERO-ONE-ADDR, the HA accepts/denies registration and sets the HA field to its own IP address in the reply (i.e., the registration is not rejected with error code 136).

The HA can reject the request with the error code REDIRECT-HA-REQ and suggest an alternate HA. This redirection can be used for load balancing, geographical proximity based on Care-of Address, or other reasons. The HA puts its own address in the HA field of the Registration Reply message and puts the address of the redirected HA in the Redirected HA Extension. If the HA accepts the Request, it sets the HA field in the Registration Reply to its own address.

The Requested HA always performs standard validity checks on the Registration Request. If there is any error, the Registration Request is rejected with error codes specified in Mobile IPv4 [1].

6. Requested Home Agent Selection

When dynamic HA assignment is requested, the MN (or FA in the case of registration via FA) sends the Registration Request to the Requested HA. This address MUST be a unicast IP address. If the MN has included a Requested HA Extension in the Registration Request, the HA address in this extension is the Requested HA.

Some examples of methods by which the MN or the FA may select the Requested HA are briefly described below:

DHCP:

The MN performs DHCP to obtain an IP address on the visited network. The Requested HA is learned from the DHCP Mobile IP Home Agent Option 68 [4]. The MN sends the Registration Request directly to this HA and receives the Assigned HA to be used for the remainder of the Mobile IP session.

AAA:

MN performs challenge/response [5] with the FA. The FA retrieves the Requested HA from the AAA server and forwards the Registration Request directly to this HA. The Assigned HA sends a Registration Reply to the FA, which relays it to the MN. MN uses the Assigned HA for the remainder of the Mobile IP session.

DNS:

In this case, the hostname of the HA is configured on the MN or obtained by some other means, e.g., using a service location protocol. The MN performs DNS lookup on the HA hostname. The DNS infrastructure provides a resource record with information to identify the optimal HA to the MN. The MN sends a Registration Request directly to the HA and receives the Assigned HA to be used for the remainder of the Mobile IP session.

Static configuration:

The HA address is statically configured on the MN. The MN sends the Registration Request to the configured address. The Requested HA may then redirect the MN to a Redirected HA.

7. Error Values

Each entry in the following table contains the name and value for the error code to be returned in a Registration Reply. It also includes the section in which the error code is first mentioned in this document.

Error Name	Value	Section	Description
NONZERO-HA-REQD	90	5.2	Non-zero HA address required in Registration Request.
REDIRECT-HA-REQ	143	5.3	Re-register with redirected HA.

8. IANA Considerations

The code value NONZERO-HA-REQD is a Mobile IP response code [1] taken from the range of values associated with rejection by the foreign agent (i.e., value in the range 64-127).

The code value REDIRECT-HA-REQ is a Mobile IP response code [1] taken from the range of values associated with rejection by the home agent (i.e., value in the range 128-192).

The Dynamic HA Extension is assigned from the range of values associated with skippable extensions at the home agent (i.e., value in the range 128-255).

IANA has recorded the values as defined in Sections 7 and 3.4.

9. Security Considerations

This specification assumes that a security configuration has been preconfigured between the MN and the HA or is configured along with the initial Registration Request/Registration Reply as per [7].

There is a possibility of more than one HA creating a mobility binding entry for a given MN, if a man in the middle captures the Registration Request with the HA field set to ALL-ZERO-ONE-ADDR and forwards it to other HAs. This scenario assumes that the rogue node can find out the addresses of the HAs that are able to authenticate the Registration Request. It also assumes that the rogue node has the capability to store, duplicate, and send packets to the other HAs

within the limited time of the replay window. Otherwise, these HAs will reject the Registration Requests anyway. In addition, this type of attack is only possible when the Requested HA Extension is not included in the registration message. The mobile node can minimize the duration of this condition by using a short lifetime (e.g., 5 seconds) in the Registration Request.

This specification does not change the security model established in Mobile IPv4 [1]. Mobile nodes are often connected to the network via wireless links, which may be more prone to passive eavesdropping or replay attacks. Such an attack might lead to bogus registrations or redirection of traffic or denial of service.

As per the messaging in this document, the Assigned Home Agent will process the incoming Registration Request as per Mobile IPv4 [1]. Hence the Assigned Home Agent will have the same security concerns as those of the home agent in Mobile IPv4 [1]. They are addressed in Section 5, "Security Considerations", of Mobile IPv4 [1].

The Registration Request and Registration Reply messages are protected by a valid authenticator as specified in Mobile IPv4 [1]. Configuring security associations is a deployment-specific issue and is covered by other Mobile IP specifications. There can be many ways of configuring security associations, but this specification does not require any specific way.

An example is where the security association between an MN and an individual HA (Requested or Assigned) is dynamically derived during the registration process based on a shared secret between MN and AAA infrastructure, as defined in [7]. The Registration Request is protected with MN-AAA Authentication Extension, and Registration Reply is protected with MN-HA Authentication Extension. Because the security association is shared between MN and AAA, any dynamically assigned HA in the local domain can proxy authenticate the MN using AAA as per [7].

The Assigned Home Agent authenticates each Registration Request from the mobile node as specified in Mobile IPv4 [1] and/or RFC 3012. The MN also authenticates the Registration Reply from the Assigned HA; thus, the existing trust model in Mobile IPv4 [1] is maintained.

10. Backward-Compatibility Considerations

In this section, we examine concerns that may arise when using this specification in a mixed environment where some nodes implement the specification and others do not. In each of the examples below, we consider the case where one node is a "legacy" node, which does not implement the specification in the context of other nodes that do.

Legacy Home Agent:

Legacy home agents may reject the Registration Request with error code 136 because the Home Agent field is not a unicast address. However, some legacy HA implementations may coincidentally process the Registration Request in accordance with this document, when the HA field in Registration Request is set to ALL-ZERO-ONE-ADDR.

Legacy Foreign Agent:

Legacy foreign agents may forward a Registration Request with home agent field set to ALL-ZERO-ONE-ADDR by setting the destination IP address to ALL-ZERO-ONE-ADDR. This will result in the packet being dropped or incidentally handled by a next-hop HA, adjacent to the FA. The MN may not be aware of the dropped Registration Request and may probably retry registration, thereby increasing the delay in registration.

To reduce the delay in registration, the MN should take the following steps:

1. The MN should send the Registration Request as specified in this specification. In other words, the MN should set the Home Agent field in the Registration Request to ALL-ZERO-ONE-ADDR and also add the Requested HA Extension.
2. If the MN does not receive a Registration Reply within some time and/or after sending a few Registration Requests, it can assume that the Registration Request(s) has been dropped, either by a legacy FA or an incorrect HA. In addition, if the registration is denied with error code 70 (poorly formed Request), the MN can assume that the legacy FA cannot process this message. In either case, the MN should fall back to a recovery mechanism. The MN should quickly send a new Registration Request as mentioned in Section 4.1 step 2. This step will ensure that a legacy FA will forward the Registration Request to the home agent thereby making dynamic HA assignment possible.

Legacy Mobile Node:

An MN that sends a Registration Request to an FA that can do dynamic HA assignment, but does not set the HA field to ALL-ZERO-ONE-ADDR will continue to be registered with its statically configured HA, exactly according to RFC 3344.

11. Acknowledgements

The authors would like to thank Pete McCann for thorough review, suggestions on security considerations, and definition of ALL-ZERO-ONE-ADDR. Thanks to Kuntal Chowdhury for extensive review and comments on this document. Also thanks to Henrik Levkowetz for detailed reviews and suggestions. Thomas Narten highlighted issues for legacy FA considerations. Thanks to Ahmad Muhanna for pointing out scenario of multiple bindings on HAs, documented in the Security Considerations section.

The authors would like to thank Mike Andrews, Madhavi Chandra, and Yoshi Tsuda for their review and suggestions.

12. Normative References

- [1] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.
- [2] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.
- [3] Senie, D., "Changing the Default for Directed Broadcasts in Routers", BCP 34, RFC 2644, August 1999.
- [4] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.
- [5] Perkins, C. and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions", RFC 3012, November 2000.
- [6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [7] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

Authors' Addresses

Milind Kulkarni
Cisco Systems Inc.
170 W. Tasman Drive,
San Jose, CA 95134
USA

Phone: +1 408-527-8382
EMail: mkulkarn@cisco.com

Alpesh Patel
Cisco Systems Inc.
170 W. Tasman Drive,
San Jose, CA 95134
USA

Phone: +1 408-853-9580
EMail: alpesh@cisco.com

Kent Leung
Cisco Systems Inc.
170 W. Tasman Drive,
San Jose, CA 95134
USA

Phone: +1 408-526-5030
EMail: kleung@cisco.com

Full Copyright Statement

Copyright (C) The Internet Society (2006).

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 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.

Acknowledgement

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

