Network Working Group
Internet-Draft
Expires: April 19, 2006

K. Chowdhury, Editor
Starent Networks
A. Yegin
Samsung

October 16, 2005

MIP6-bootstrapping via DHCPv6 for the Integrated Scenario
draft-ietf-mip6-bootstrapping-integrated-dhc-00.txt

Status of this Memo

Copyright Notice

Abstract

The Mobile IPv6 bootstrapping problem statement describes two main scenarios. In the first scenario (i.e. the split scenario), the mobile node's mobility service is authorized by a different service authorizer than the basic network access authorizer. In the second scenario (i.e. the integrated scenario), the mobile node's mobility service is authorized by the same service authorizer as the basic network access service authorizer. This document defines a method

for home agent information discovery based on DHCPv6 for the integrated scenario.

Table of Contents

1. Introduction and Scope

The Mobile IPv6 protocol [RFC3775] requires the mobile node to have knowledge of its Home Address, the home agent address and the cryptographic materials for establishing an IPsec security association with the home agent prior to performing home registration. The mechanism via which the mobile node obtains these information is called Mobile IPv6 bootstrapping. In order to allow a flexible deployment model for Mobile IPv6, it is desirable to define a bootstrapping mechanism for the mobile node to acquire these parameters dynamically. The [BOOT-PS] describes the problem statement for Mobile IPv6 bootstrapping. It also defines two bootstrapping scenarios based on the relationship between the entity that authenticates and authorizes the mobile node for network access (i.e., the Access Service Authorizer) and the entity that authenticates and authorizes the mobile node for mobility service (i.e., the Mobility Service Authorizer). The scenario in which the Access Service Authorizer is not the Mobility Service Authorizer is called the "Split" scenario. The bootstrapping solution for split scenario is defined in [BOOT-SPLIT]. The scenario in which the Access Service Authorizer is also the Mobility Service Authorizer is called the "Integrated" scenario. This document defines a bootstrapping solution using DHCPv6 for the Integrated scenario.

[BOOT-SPLIT] identifies four different components of the bootstrapping problem: home agent address discovery, HoA assignment, IPsec Security Association setup and Authentication and Authorization with the MSA. This document defines a mechanism for home agent address discovery. For the rest of components, please refer to [BOOT-SPLIT].

In the integrated scenario, the bootstrapping of the home agent information can be performed via DHCPv6. DHCPv6 is designed for configuration management and it is being deployed by operators to handle their configuration management needs in their networks.

2. Terminology

The keywords "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].

General mobility terminology can be found in [RFC3753]. The following additional terms, as defined in [BOOT-PS], are used in this document:

Access Service Authorizer (ASA):
: A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

Access Service Provider (ASP):
: A network operator that provides direct IP packet forwarding to and from the mobile node.

Mobility Service Authorizer (MSA):
: A service provider that authorizes Mobile IPv6 service.

Mobility Service Provider (MSP):
: A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and authorized to obtain the Mobile IPv6 service.

Split scenario:
: A scenario where the mobility service and the network access

service are authorized by different entities.

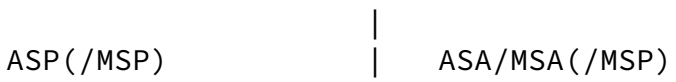
Integrated Scenario:
A scenario where the mobility service and the network access service are authorized by the same entity.

3. Solution Overview

3.1 Logical Diagram of the Integrated Scenario

In the integrated scenario the mobile node may use the security credentials for network access to bootstrap Mobile IPv6. As such, it is assumed that the access service authorizer is mobility service aware. This allows for Mobile IPv6 bootstrapping at the time of access authentication and authorization. Also, the mechanism defined in this document requires the NAS to support Mobile IPv6 specific AAA attributes and a collocated DHCP relay agent.

The following diagram shows the network elements and layout in the integrated scenario:



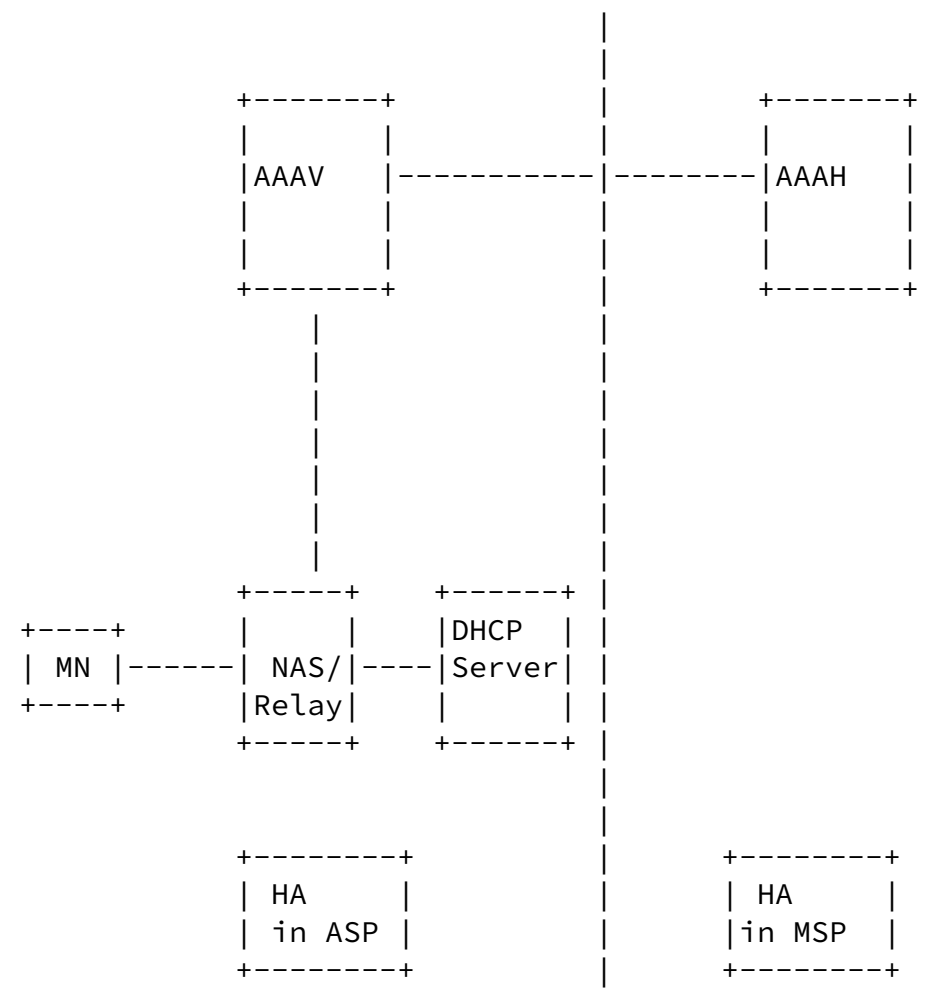


Figure 1. Integrated Scenario, Network Diagram with DHCP

Figure 1 shows the AAA infrastructure with a AAA client (NAS), a AAA proxy in the visited network and a AAA server in the home network. The user's home network authorizes the mobile node for network access and also for mobility services. Note that a home agent for usage with the mobile node might be selected in the access service provider's network or alternatively in the mobility service provider's network.

The mobile node interacts with the DHCP Server via the Relay Agent

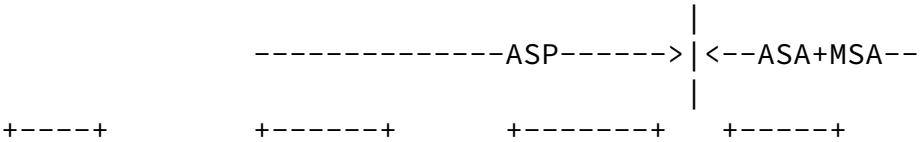
(ideally collocated with the NAS) after the network access authentication as part of the mobile node configuration procedure.

3.2 Bootstrapping Message Sequence, Success Case

In the success case, the mobile node is able to acquire the home agent address via a DHCPv6 query. The message flows for home agent allocation in the ASP and the MSP are illustrated below. Since, in the integrated scenario, the ASA and the MSA are the same, it can be safely assumed that the AAAH used for network access authentication (ASA) has access to the same database as the AAAH used for the mobility service authentication (MSA). Hence, the same AAAH can authorize the mobile node for network access and mobility service at the same time.

3.2.1 Home Agent allocation in the MSP

This section describes a scenario where the home agent is allocated in the mobile node's home MSP network. in order to provide the mobile node with information about the assigned home agent the AAAH conveys the assigned home agent's information to the NAS via AAA protocol.



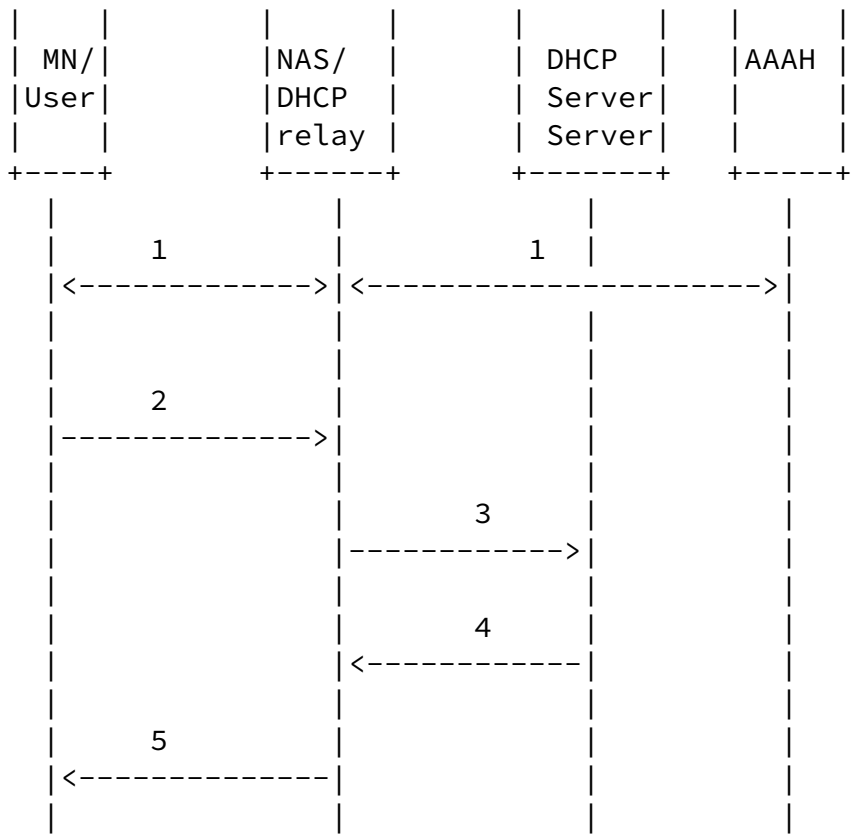


Figure 2. The home agent allocation in the home MSP

Figure 2 shows the message sequence for home agent allocation in the home MSP.

(1) The mobile node executes the network access authentication procedure (e.g., IEEE 802.11i/802.1X) and thereby interacts with the NAS. The NAS is in the ASP and it interacts with the AAAH, which is in the ASA/MSA, to authenticate the mobile node. In the process of authorizing the mobile node the AAAH verifies in the AAA profile that the mobile node is allowed to use Mobile IPv6 service. The AAAH assigns a home agent in the home MSP and returns this information to the NAS.

(2) The mobile node sends a DHCPv6 Information Request message [RFC3315] to the All_DHCP_Relay_Agents_and_Servers multicast address. In this message the mobile node (DHCP client) SHALL include the Option Code for Home Network Identifier Option [HAOPT] in the OPTION_ORO, Home Network Identifier Option with id-type set to 1 and the Home Network Identifier field set to the network realm of the

home MSP [HAOPT]. The mobile node SHALL also include the OPTION_CLIENTID to identify itself to the DHCP server.

(3) The Relay Agent intercepts the Information Request from the mobile node and forwards it to the DHCP server. The Relay Agent also includes the received home agent information from the AAAH in the OPTION_MIP6-RELAY-Option (see section 3.5).

(4) The DHCP server identifies the client by looking at the DUID for the client in the OPTION_CLIENTID. The DHCP server also determines that the mobile node is requesting home agent information in the MSP by looking at the Home Network Identifier Option (id-type 1). The DHCP server determines that the home agent is allocated by the AAAH by looking at the MIP6 home agent sub-option in the OPTION_MIP6-RELAY-Option. The DHCP server extracts the allocated home agent information from the OPTION_MIP6-RELAY-Option and includes it in the Home Network Information Option [HAOPT] in the Reply Message.

(5) The Relay Agent relays the Reply Message from the DHCP server to the mobile node. At this point, the mobile node has the home agent information that it requested.

3.2.2 Home Agent allocation in the ASP

This section describes a scenario where the mobile node requests for home agent allocation in the ASP by setting the id-type field to zero in the Home Network Identifier Option in the DHCPv6 request message. In this scenario, the ASP becomes the MSP for the duration of the network access authentication session.

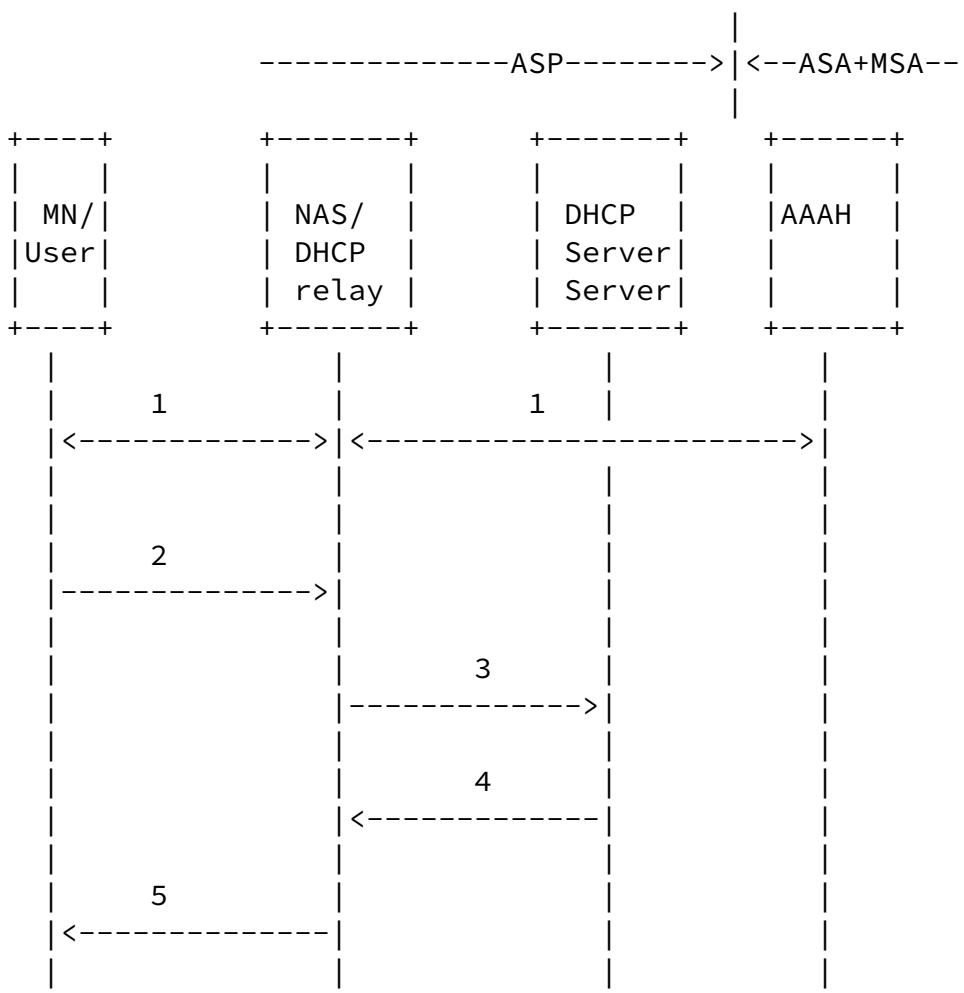


Figure 3. The home agent allocation in the ASP

Figure 3 shows the message sequence for home agent allocation in the ASP.

(1) The mobile node executes the network access authentication procedure (e.g., IEEE 802.11i/802.1X) and thereby interacts with the NAS. The NAS is in the ASP and it interacts with the AAAH, which is in the ASA/MSA, to authenticate the mobile node. In the process of authorizing the mobile node the AAAH verifies in the AAA profile that the mobile node is allowed to use Mobile IPv6 services. The AAAH assigns a home agent in the home MSP and returns this information to

the NAS. Note that the AAAH is not aware of the fact that the mobile node will rather request for a home agent allocation in the ASP. Therefore the assigned home agent may not be used by the mobile node. This leaves the location of the mobility anchor point decision to the mobile node.

(2) The mobile node sends a DHCPv6 Information Request message [RFC3315] to the All_DHCP_Relay_Agents_and_Servers multicast address.

In this message the mobile node (DHCP client) SHALL include the Option Code for Home Network Identifier Option [HAOPT] in the OPTION_ORO, Home Network Identifier Option with id-type set to 0. The mobile node SHALL also include the OPTION_CLIENTID to identify itself to the DHCP server.

(3) The Relay Agent intercepts the Information Request from the mobile node and forwards it to the DHCP server. The Relay Agent (which is the NAS) also includes the received AAA AVP from the AAAH in the OPTION_MIP6-RELAY-Option.

(4) The DHCP server identifies the client by looking at the DUID for the client in the OPTION_CLIENTID. The DHCP server also determines that the mobile node is requesting home agent information in the ASP by looking at the Home Network Identifier Option (id-type 0). If configured to do so, the DHCP server allocates an home agent from its configured list of home agents and includes it in the Home Network Information Option [HAOPT] in the Reply Message. Note that in this case, the DHCP server does not use the received information in the OPTION_MIP6-RELAY-Option.

(5) The Relay Agent relays the Reply Message from the DHCP server to the mobile node. At this point, the mobile node has the home agent information that it requested.

3.3 Bootstrapping Message Sequence: Fallback case

In the fallback case, the mobile node is not able to acquire the home agent information via DHCPv6. The mobile node performs DNS queries to discover the home agent address as defined in [BOOT-SPLIT]. To perform DNS based home agent discovery, the mobile node needs to know the DNS server address. How the mobile node knows the DNS server address is outside the scope of this document.

3.4 HoA and IKEv2 SA Bootstrapping in the Integrated Scenario

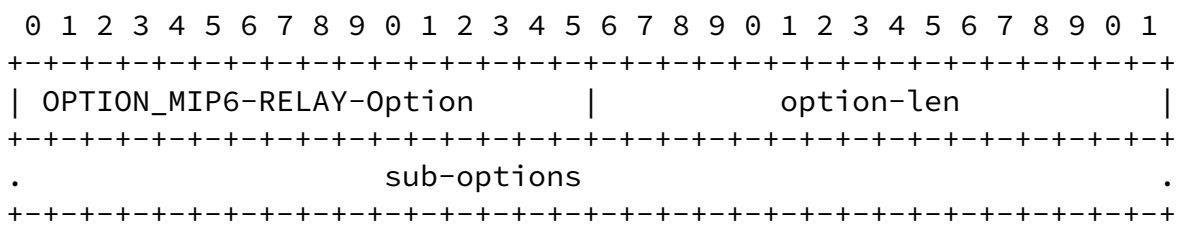
In the integrated scenario, the HoA, IPsec Security Associations setup, and Authentication and Authorization with the MSA are bootstrapped via the same mechanism as described in the bootstrapping solution for split scenario [BOOT-SPLIT].

3.5 DHCPv6 options

The following DHCP options are used in this solution to carry the home agent information from the DHCP relay agent to the DHCP serever:

3.5.1 DHC Relay Agent Option to carry Mobile IPv6 parameters

This option carries the RADIUS or Diameter attributes that are received at the NAS from the AAAH. The DHCP relay agent sends this option to the DHCP server in the Relay-Forward message.



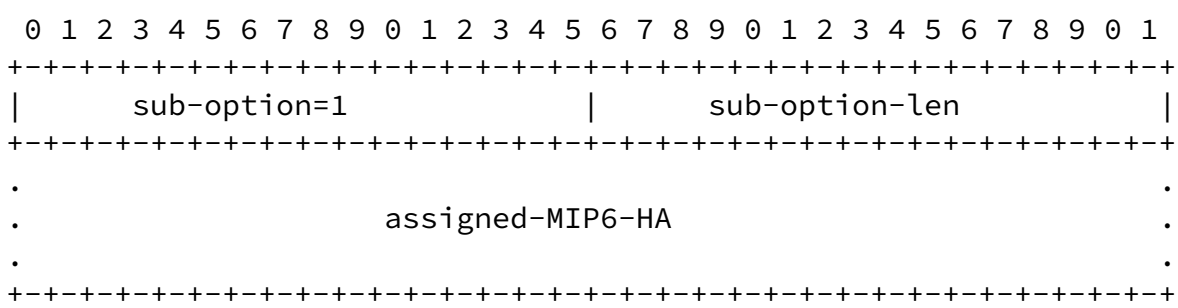
option-code OPTION_MIP6-RELAY-Option (TBD-1 by IANA).

option-len Length of OPTION_MIP6-RELAY-Option.

sub-options A series of sub-options carrying MIP6 bootstrap information. The values are:
1 - MIP6 home agent.
other values are reserved.

3.5.2 MIP6 home agent sub-option

This sub-option carries the assigned home agent information to the DHCP server.



sub-option-code	MIP6 home agent (1).
option-len	Length of assigned home agent field.
assigned-MIP6-HA	IPv6 address or FQDN of the assigned home agent.

The following DHCP options are used in this solution to carry the home agent information and home agent bootstrap request information between the mobile node and the DHCP server:

Home Network Information Option [HAOPT].

Home Network Identifier Option [HAOPT].

The following DHCP options are requried in this solution for normal DHCP operation:

Option Request Option [RFC3315].

Client Identifier Option [RFC3315].

Relay Message Option [RFC3315].

Interface-Id Option [RFC3315].

3.6 Mobile Node Behavior

If configured to do so, the mobile node MUST first try to perform home agent discovery using DHCPv6. In order to acquire the home agent information, the mobile node SHALL send an Information Request to the All_DHCP_Relay_Agents_and_Servers multicast address. In this message the mobile node (DHCP client) SHALL include the Option Code for Home Network Identifier Option [HAOPT] in the OPTION_ORO, Home Network Identifier Option with id-type set to either 1 or 0. The mobile node SHALL also include the OPTION_CLIENTID [RFC3315] to identify itself to the DHCP server.

Upon receiving the Reply message from the DHCP server, the mobile node SHALL check for the requested configuration options. Here are the possible scenarios:

Home Network info Option	mobile node Action
hninfo-type 0,1,2	Use home agent address
hninfo-type 0,1	Use home agent address
hninfo-type 0	Use home agent address
hninfo-type 1,2	Use home agent address

hninfo-type 1	Use home agent address
hninfo-type 0,2	Use home agent address
hninfo-type 2	Use HA-FQDN, ref [BOOT-SPLIT] for DNS based home agent discovery.
No	Ref [BOOT-SPLIT] for DNS based home agent discovery.

The mobile node MAY request for local home agent assignment by including the Home Network Identifier Option [HAOPT] in the Information Request message and by setting the id-type to 0.

If the mobile node wants to discover an home agent in a particular MSP, the mobile node SHALL request for home agent assignment in that MSP by including the Home Network Identifier Option [HAOPT] in the Information Request message. In this option the mobile node SHALL set the id-type to 1 and the Home Network Identifier field to the network realm of the MSP.

3.7 NAS, DHCP Relay Agent Behavior

The NAS and the DHCP relay agent are assumed to be collocated in this solution. The NAS communicates with the mobile node during the network access authentication and interacts with the AAAH (via the AAAV) using either Diameter NASREQ [RFC4005] or RADIUS [MIP6-RADIUS] [Editor's note: The Diameter AVPs need to be defined].

Upon receiving the MIP6 related RADIUS or Diameter attributes returned by the AAAH, the NAS passes the information to the collocated DHCP Relay Agent.

Upon receiving the Information Request from the mobile node, the DHCP relay agent MUST forward the message to the DHCP server as per [RFC3315]. The relay agent SHALL use the OPTION_CLIENTID to identify the mobile node (user). This is required to check whether there are some additional information for the user that need to be appended

while relaying the information request message to the DHCP server. If the relay agent determines that the NAS has passed home agent information for this mobile node, the relay agent MUST include the received home agent information in the OPTION_MIP6-RELAY-Option and include this option in the Relay-Forward message. The relay agent MAY include the Interface-Id Option [RFC3315] in the Relay-Forward message.

Upon receiving the Reply message from the DHCPv6 server, the relay agent SHALL follow the guidelines defined in [RFC3315] to forward the message to the mobile node.

3.8 DHCP Server Behavior

The DHCP server MUST follow the following logic to process Information Request from the mobile node:

Information Request message includes:

a. OPTION_MIP6-RELAY-Option, OPTION_ORO and Home Network Identifier Option with id-type 1 (home agent assignment request in the home MSP), Interface-Id Option, Client Identifier Option.

The DHCP server MUST extract the assigned home agent information from the OPTION_MIP6-RELAY-Option and include it in the Home Network Information Option of the Reply message.

b. OPTION_MIP6-RELAY-Option, OPTION_ORO and Home Network Identifier Option with id-type 0 (home agent assignment request in the ASP), Interface-Id Option, Client Identifier Option.

If the DHCP server is configured with information about a local home agent, select a home agent address or FQDN for the home agent from locally provisioned configuration and include it in the Home Network Information Option of the Reply message.

If the DHCP server is not configured with information about a local home agent, but it received the assigned home agent info in the OPTION_MIP6-RELAY-Option, then it MUST extract the assigned home agent info from this option and MUST include it in the Home Network Information Option of the Reply message.

If the DHCP server is not configured with information about a local

home agent, and no OPTION_MIP6-RELAY-Option is received, then it MAY return any other option in the Reply message that is requested. In this case no home agent is assigned to the mobile node.

In all cases, in the Reply message the DHCP server MUST return the Interface-Id Option as received in the Information Request. The DHCP server SHOULD use the Client Identifier Option to identify the mobile node.

4. Security Considerations

The transport of the assigned home agent information via the AAA infrastructure (i.e., from the AAA server to the AAA client) to the NAS is subject to the standard RADIUS and Diameter security considerations. No new security considerations are imposed by the usage of this document. The security mechanisms provided by [RFC2865] and [RFC3588] are applicable and provide adequate security for this purpose.

The communication between the NAS/DHCP relay agent to the DHCP server must be authenticated, integrity and replay protected. Deployments MAY either rely on lower-layer security, (i.e., physical or link layer security), or rely on security mechanisms specifically defined for DHCPv6, such as [RELAY-IPSEC] or [RFC4030].

The communication between the DHCP client and the DHCP server for the exchange of home agent information is security sensitive and requires authentication, integrity and replay protection. Either lower-layer security (such as link layer security established as part of the network access authentication protocol run) or DHCP security [RFC3118] can be used. The latter approach is only applicable in non-roaming environments due to the limited applicability of the DHCP security mechanisms. An adversary that is able to modify home agent information can force the mobile node to use a different home agent than intended by the MSA. However, this type of attack can be detected by the security mechanism between the mobile node and the home agent.

Overall, the home agent information carried by the AAA protocols and DHCP does not impose any new security concerns for the transport protocols.

5. IANA Considerations

The following DHCP option code MUST be assigned by IANA:

option-code for OPTION_MIP6-RELAY-Option: TBD-1.

6. Acknowledgements

TBD.

7. Contributors

This contribution is a joint effort of the bootstrapping solution design team of the MIP6 WG. The contributors include Gerardo Giaretta, Basavaraj Patil, Alpesh Patel, Jari Arkko, James Kempf, Gopal Dommety, Alper Yegin, Junghoon Jee, Vijay Devarapalli, Kuntal Chowdhury, Julien Bournelle, and Hannes Tschofenig.

The design team members can be reached at:

Gerardo Giaretta gerardo.giaretta@tilab.com

Basavaraj Patil basavaraj.patil@nokia.com

Alpesh Patel alpesh@cisco.com

Jari Arkko jari.arkko@kolumbus.fi

James Kempf kempf@docomolabs-usa.com

Gopal Dommety gdommety@cisco.com

Alper Yegin alper.yegin@samsung.com

Junghoon Jee jhjee@etri.re.kr

Vijay Devarapalli vijayd@iprg.nokia.com

Kuntal Chowdhury kchowdhury@starentnetworks.com

Julien Bournelle julien.bournelle@int-evry.fr

Hannes Tschofenig hannes.tschofenig@siemens.com

8. References

8.1 Normative References

[BOOT-PS] Patel et. al., A., "Problem Statement for bootstrapping Mobile IPv6.", draft-ietf-mip6-bootstrap-ps-03.txt (work in progress), July 2005.

[HAOPT] Hee Jang et. al., A., "DHCP Option for Home Agent Discovery in MIPv6.", draft-jang-dhc-haopt-01.txt (work in progress), April 2005.

[MIP6-RADIUS] Chowdhury et. al., K., "RADIUS Mobile IPv6 Support.",

draft-chowdhury-mip6-radius-00.txt (work in progress), October 2005.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3118] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4030] Stapp, M. and T. Lemon, "The Authentication Suboption for

the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option", RFC 4030, March 2005.

8.2 Informative References

[BOOT-SPLIT]
Giaretta et. al., A., "Mobile IPv6 bootstrapping in split

scenario.", draft-ietf-mip6-bootstrapping-split-00.txt (work in progress), June 2005.

[RELAY-IPSEC]
Droms, R., "Authentication of DHCP Relay Agent Options Using IPsec.", draft-ietf-dhc-relay-agent-ipsec-02.txt (work in progress), May 2005.

Authors' Addresses

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US

Phone: +1 214-550-1416
Email: kchowdhury@starentnetworks.com

Alper Yegin
Samsung
Email: alper.yegin@yegin.org

Intellectual Property Statement

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

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.