Network Working Group
Internet-Draft
Expires: March 12, 2007

K. Chowdhury
Starent Networks
A. Singh
Motorola

September 8, 2006

Network Based Layer 3 Connectivity and Mobility Management for IPv6 draft-chowdhury-netmip6-01.txt

Status of this Memo

Copyright Notice

Abstract

The layer 3 connection and mobility management is essential in providing seamless access to services and enhanced user experience in a mobile and nomadic envoirnment. This document defines a mechanism via which service providers can deploy a managed layer 3 connectivity and mobility management scheme that is entirely based on the capabilities in the Network.

Table of Contents

1. Introduction and Scope

Network based L3 mobility management allows any mobile node to connect to a mobile wireless network and maintain it's L3 connectivity while crossing link boundaries. This type of mobility management solution does not necessarily require any Mobile IPv6 implementation in the mobile node. Rather, the L3 mobility is handled entirely in the network via a Mobile IPv6 function in a network node such as an Access Router (AR).

In a typical mobile wireless network the inter base station handoffs (often called L2 handoffs) are handled by local mobility management protocols. There are various flavors of such protocols deployed today. When the mobile node incurs handoff to a base station that is attached to an Access Router in a different link than the current one, the L3 mobility management procedure is invoked by the mobile node to re-register the new Care-of Address with the Home Agent. However, if the mobile node does not have Mobile IPv6 implementation it's L3 will break and the session will terminate abnormally. If the mobile node has Mobile IPv6 implementation, there are solutions to handle inter AR handoffs via techniques like Fast MIPv6 [RFC4068]. The solution offers early establishment of the link with the new AR albeit requiring number of messages exchanged over the air and still requiring the mobile node to re-register with the Home Agent even if the mobile user is in the middle of a real time conversation. The requirement of additional messaging over the air to manage handoff that can be easily managed by the network nodes is a problem that this document addresses.

There are other reasons why network based IPv6 mobility makes perfect sense. For example, the network operators are deploying more than one access technology for the wireless data users. These wireless technologies are being developed in different standerdization organizations such as 3GPP2, WiMAX forum, 3GPP etc. The standards developed by these organizations do impose some level of requirements on the MN's. However it becomes impractical to assume uniform capabilities acorss MNs of different access technologies. Ideally the operator's core IP network should be able handle any type of MN regardless of Mobile IPv6 capabiliy and use of client based Mobile IPv6 in the MN. For this reason, Mobile IPv6 is being considered for deployment in various standerdazation organisations.

The solution provided in this document allows any mobile node to connect to the network and be mobile without Mobile IPv6 in the mobile node and without losing its L3 connectivity or having to perform additional signaling to maintain L3 connectivity during handoffs.

2. Terminology & Definitions

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].

The definitions of some new terms that are used in this document:

SAR: Serving Access Router

TAR: Target Access Router

3. Solution Overview

The solution has two aspects. The first aspect deals with the network connection setup. The second aspect deals with the L3 mobility management.

3.1 Network Connection Setup for IPv6

The mobile node connects to the mobile wireless network via any access technology e.g. CDMA, GPRS, 802.11, 802.16e etc. After establishing L2 connection with the network, the mobile node initiates L3 establishment by requesting an IPv6 address from the network. There are various ways the mobile node can request for an IPv6 address e.g. IPv6CP [RFC2472], IPv6 stateless address autoconf [RFC2462], and DHCPv6 [RFC3315].

The following message sequence diagram shows the network connectivity procedure.

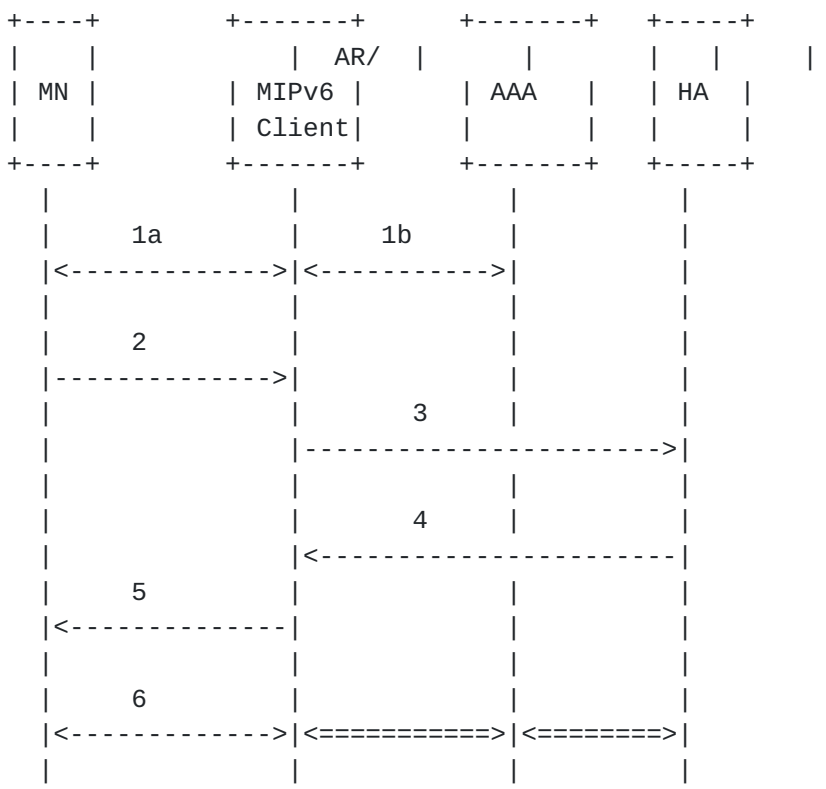


Figure 1. Network Connection Setup for IPv6 with MIPv6 Function in the AR.

Description of the steps:

1a. MN and the NAS performs L2 establishment with the base station (not shown) and performs access authentication/authorization. During this phase, the MN may run CHAP or PAP if PPP is used or EAP over foo if PPP is not used. The AR acts as the NAS in this phase.

1b. The NAS exchanges AAA messages with the AAA infrastructure to perform authentication and authorization of the MN. As part of this step, the AAA server may download some information about the MN (e.g. user's profile, handset type, assigned home agent address, and other capabilities of the MN) if needed.

2. The MN sends an IPv6CP config request to the NAS/AR in case of PPP to configure the IID. Subsequently, the MN sends an Router Solicitation to request an IPv6 address prefix. If DHCPv6 is used, the DHCPv6 client in the MN sends a DHCP SOLICIT or REQUEST message. It is assumed in this document that the AR has a DHCPv6 proxy/server function.

3. Triggered by step 2 the MIPv6 Client in the AR (Net-MIPv6) sends a Mobile IPv6 Binding Update (BU) to the Home Agent. The Home Agent's address if either received at step 1b from the Home AAA or it is provisioned in a out of band way at the AR. The BU contains the Care-of Address (CoA) of the AR. The HoA field is set to ALL-ZERO-ONES-ADDRESS if not already assigned by the AAA at step 1b. It is assumed that the AR and the HA either has an IPsec SA setup to protect the BU and the AR and the HA uses auth protocol [RFC4285] based security. These security aspects are to be defined in more details either in the current document or in some other document.

4. The home agent registers the MN's session and assigns an HoA. The home agent returns the HoA in the BA.

5. The AR/NAS sends an RA with IPv6 address prefix with the prefix of the HoA to the MN. If DHCPv6 was used at step 2, the AR/ DHCP-proxy/server sends back a DHCP Reply with the IPv6 address set to the received HoA.

6. At this step, the MN's IPv6 stack is ready to receive or send IPv6 packets. If DHCPv6 is used, the regular DHCPv6 messages are exchanged and the MN's IPv6 stack is configured with the assigned IPv6 address.

3.2 Network Connection Setup for IPv4

The network based connectivity and mobility management protocol defined in this document can be used to support IPv4 MNs as well. The mobile node connects to the mobile wireless network via any access technology e.g. CDMA, GPRS, 802.11, 802.16e etc. After establishing L2 connection with the network, the mobile node initiates L3 establishment by requesting an IPv4 address from the network. There are various ways the mobile node can request an IPv4 address e.g. IPCP [RFC1332], or DHCP [RFC2132].

The following message sequence diagram shows the network connectivity procedure.

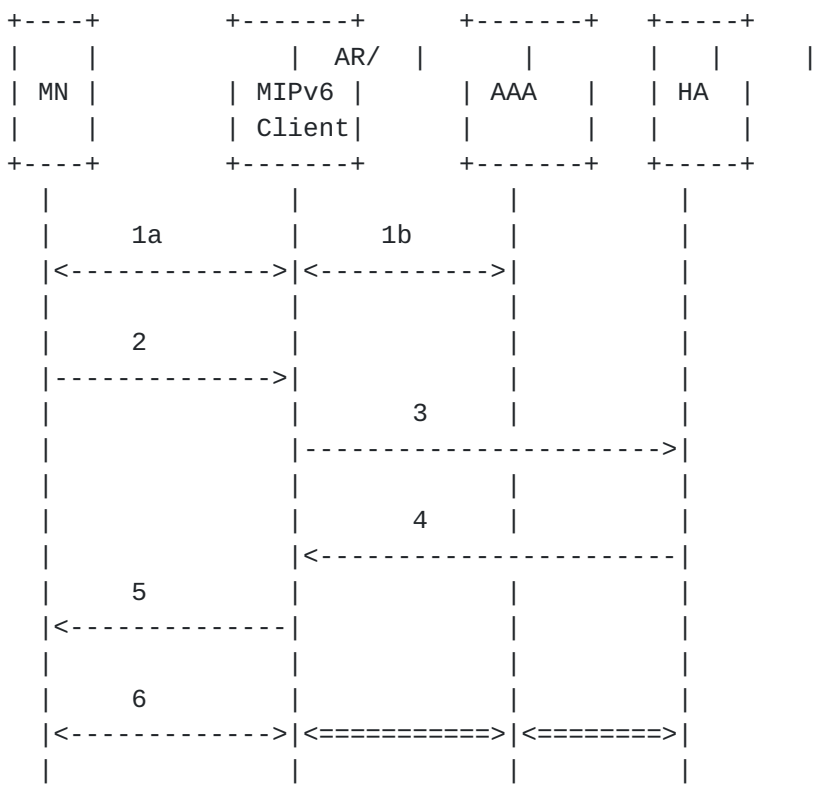


Figure 1. Network Connection Setup for IPv4 with MIPv6 Function in the AR.

Description of the steps:

1a. MN and the NAS performs L2 establishment with the base station (not shown) and performs access authentication/authorization. During this phase, the MN may run CHAP or PAP if PPP is used or EAP over foo if PPP is not used. The AR acts as the NAS in this phase.

1b. The NAS exchanges AAA messages with the AAA infrastructure to perform authentication and authorization of the MN. As part of this step, the AAA server may download some information about the MN (e.g. user's profile, handset type, assigned home agent address, and other capabilities of the MN) if needed.

2. The MN sends an IPCP config request to the NAS/AR in case of PPP to configure the IPv4 address. If DHCP is used, the DHCP client in the MN sends a DHCP DISCOVER message. It is assumed in this document that the AR has a DHCP proxy/server function.

3. Triggered by step 2 the MIPv6 Client in the AR (Net-MIPv6) sends

a Mobile IPv6 Binding Update (BU) to the Home Agent. The Home Agent's address if either received at step 1b from the Home AAA or it is provisioned in a out of band way at the AR. The BU contains the Care-of Address (CoA) of the AR. The HoA field is set to ALL-ZERO-ONES-ADDRESS. The BU contains the IPv4 home address option [DSMIPv6] with IPv4 home address field set to 0.0.0.0 and P-bit not set. It is assumed that the AR and the HA either has an IPsec SA setup to protect the BU and the AR and the HA uses auth protocol [RFC4285] based security. These security aspects are to be defined in more details either in the current document or in some other document.

4. The home agent registers the MN's session and assigns an IPv4 HoA. The home agent returns the IPv4 HoA in IPv4 home address option in the BA.

5. The AR/NAS sends an IPCP configure-NACK with IPv4 address to the MN. If DHCP was used at step 2, the AR/DHCP-proxy/server sends back a DHCP OFFER with the IPv4 address set to the received IPv4 HoA.

6. At this step, the MN's IPv4 stack is ready to receive or send IPv4 packets. If DHCP is used, the regular DHCP messages are exchanged and the MN's IPv4 stack is configured with the assigned IPv4 address.

3.3 Inter AR Handoff

After connecting to the access network, the MN may incur inter AR handoff due to mobility. This poses the challenge of keeping the L3 connection for the MN intact due to possible change in the link.

The following message sequence diagram shows how the network connectivity can be maintained across an inter AR handoff.

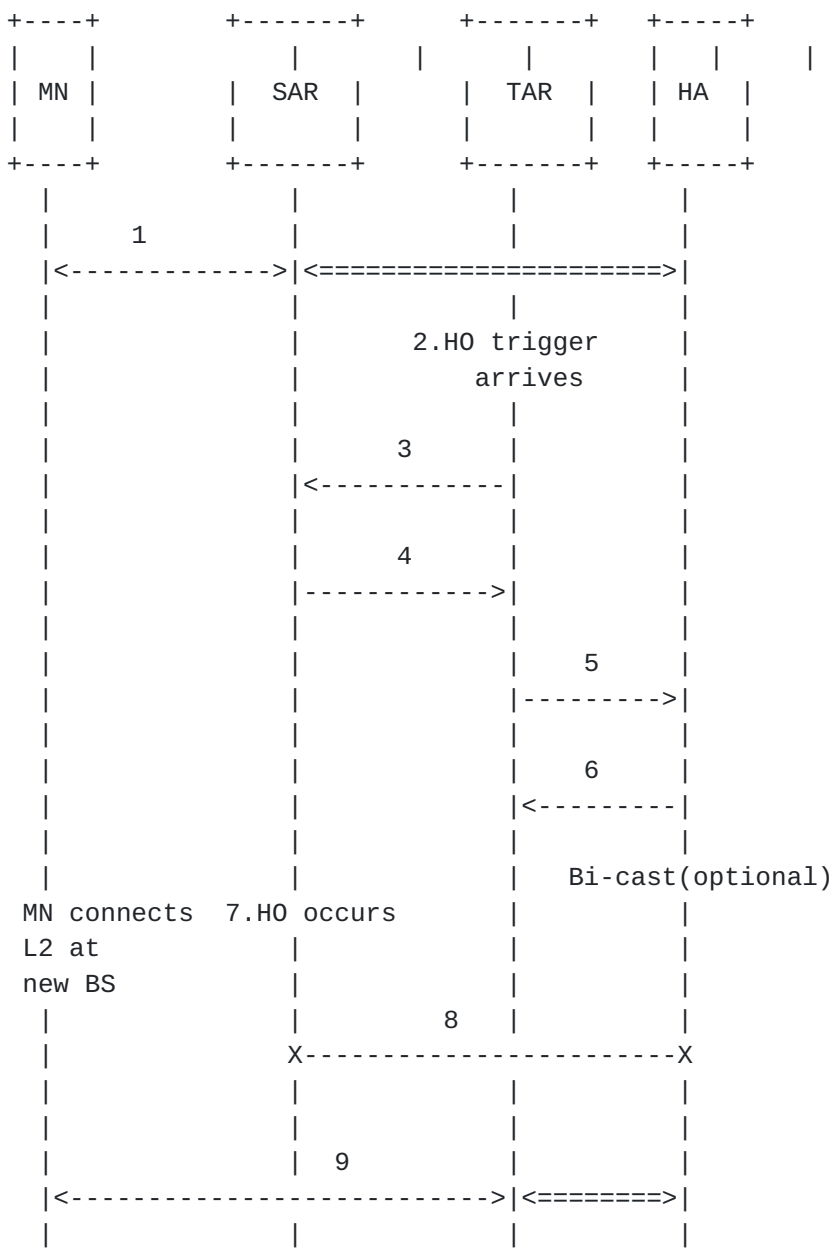


Figure 1. Inter AR Mobility Management with MIPv6 Client in the AR.

Description of the steps:

1. MN is connected at the Serving AR (SAR) and it is sending/ receiving data via SAR. The HA has a tunnel established with the SAR.

2. The MN moves into an area of a target Base Station (not shown in

the figure) that is connected to a target AR (TAR). The target BS sends a HO indication message (out of scope of this document) to the target AR. This message contains the address of the SAR and the MN identifier (NAI) among other parameters.

3. Based on the trigger at step 2, the TAR sends a HO Request message to the SAR to fetch the relevant context for the MN. The ICMPv6 HO Request message is defined in the following section of this document. Note that the TAR and the SAR share a security association. The HO Request message can be protected with an IPsec authentication header using the security association between the ARs.

4. Upon receiving the HO Request message the SAR validates it by checking it's security association with the TAR. if the validation succeeds, the SAR sends all the state information (context) for the identified MN to the TAR in a ICMPv6 HO Response message.

5. The Mobile IPv6 Client in the TAR sends a Binding Update to the HA with its' CoA (CoA of the TAR) and sets the HoA to the HoA of the MN which is received as part of the state information at step 4.

6. Upon receiving the BU from the TAR, the HA updates it's BCE with the new CoA and an HoA to the MN and returns the HoA in an RRP. Since the binding/tunnel with the SAR is still not torn down, the HA has an option of bi-casting to both SAR and TAR at this time.

7. At this time, the MN connects L2 with the target BS. The target BS (not shown in the figure for brevity) informs the TAR that the MN has connected to the target system. The Serving BS also detects that the handoff (L2 torn down with the MN) and it informs the SAR about this event.

8. Upon receiving the HO event from the Serving BS, the SAR tears down the tunnel with the HA.

9. The MN continues to receive service (i.e. send/receive data) with the same IPv6 address which is the HoA. The MN is agnostic to the L3 mobility procedures in the network.

4. ICMPv6 Enhancements for Inter AR Interaction

The format of the inter AR messages are defined here:

4.1 HO Request Message

The HO Request message is an inter AR message used for HO notification and request for context transfer. The message is formatted as follows:

IP Fields:

Source Address

The IPv6 address of the TAR.

Destination Address

The IPv6 address of the SAR.

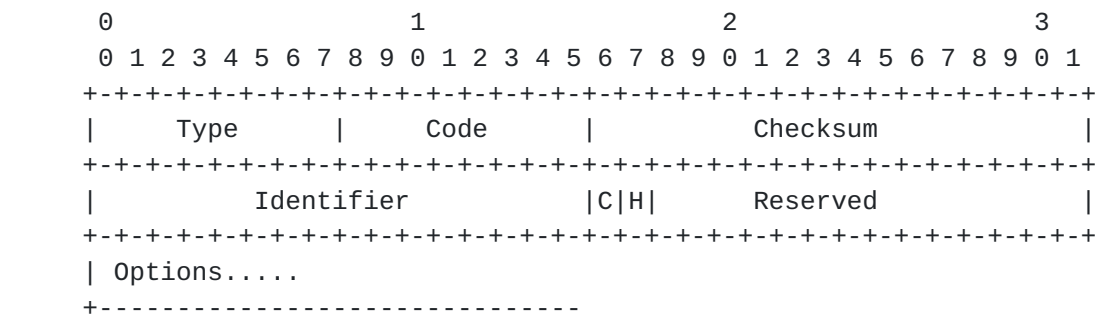
Hop Limit

255, refer to [RFC2461].

Authentication Header

The authentication header SHOULD be used, ref [RFC2402].

The ICMPv6 message has the following fields as shown below.



Type

A 8-bit field indicating the type of the message. To be assigned by IANA.

Code

TBD, to be assigned by IANA.

Checksum

An 16-bit Checksum of the ICMPv6 message.

Identifier

An 16-bit string that the sender uses to match the corresponding response from the receiver.

C-bit

If set, the sender is requesting context transfer for the identified MN.

H-bit

By setting this bit the sender informs the receiver that the reason for this message is a handoff by the identified MN.

Options

This message can carry several options to help identify the proper context in the receiver. The options MUST be encoded as defined in [RFC2461].

An option carrying MN's identity (e.g. NAI) MUST be included in this message.

4.2 HO Response Message

The HO Response message is an inter AR message that is used to respond to an HO Request message. The message is formatted as follows:

IP Fields:

Source Address

The IPv6 address of the SAR.

Destination Address

The IPv6 address of the TAR.

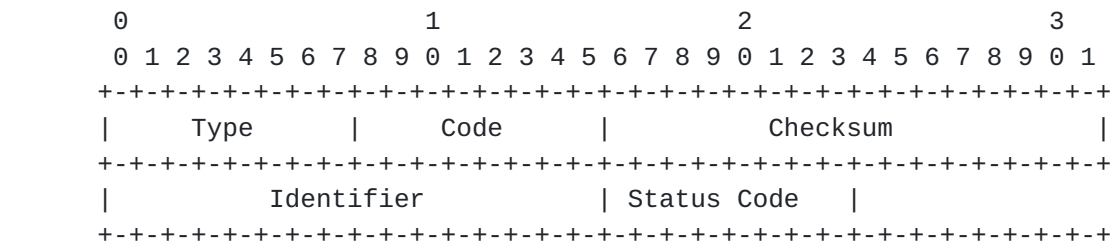
Hop Limit

255, refer to [RFC2461].

Authentication Header

The authentication header SHOULD be used, ref [RFC2402].

The ICMPv6 message has the following fields as shown below.



Type

A 8-bit field indicating the type of the message. To be assigned by IANA.

Code

TBD, to be assigned by IANA.

Checksum

An 16-bit Checksum of the ICMPv6 message.

Identifier

An 16-bit string that is copied from the corresponding field in the HO Request message.

Status Code

The 8-bit Status Code is used by the sender of this message to convey the status of the corresponding request. The following values are defined at this time:

0: Success.

1: Failure, Poorly Formatted Request.

2: Failure, Authentication failed.

3: Failure, Unable to locate Context.

4: Failure, Administratively Prohibited.

All other values are reserved.

5. HMIPv6 Considerations

HMIPv6 [RFC4140] is a MIPv6 (experimental) extension to support localized mobility management. The base HMIPv6 protocol supports mobile controlled mobility management and hence requires MN to be aware of the MN's local CoA, Regional CoA and HoA. The MN manages localized mobility management (e.g., mobility inside a MAP domain) by updating binding between LCoA and RCoA while it moves inside the coverage area of the MAP (Mobility Anchor Point, ref: RFC4140) domain. It performs Global Mobility Management (e.g., inter-MAP mobility) by updating binding between RCoA and HA to Home Agent and CN while it moves from one MAP domain to other. The use of vanilla HMIPv6 enables mobile controlled localized mobility management, but does not enable network controlled mobility management required by some deployments.

5.1 Network Based HMIPv6 Operation

In some special deployment scenarios localized mobility management may be desired. In this document, we are proposing a network controlled mobility management scheme that is based on modified HMIPv6 protocol, Net-HMIPv6. The Net-HMIPv6 protocol re-uses HMIPv6 signaling and HMIPv6 MAP function to enable network controlled localized mobility management. The Net-HMIPv6 protocol introduces a network based MIPv6 Client (NetMIPv6) that is responsible for sending binding updates on behalf of a MN to the MAP. The NetMIPv6 Client performs mobility management signaling on behalf of a MN as long as the MN moves inside the coverage area of a given MAP domain. The NetMIPv6 Client uses link layer specific mechanism to detect movement of a mobile node from one AR to other AR inside a MAP domain. To manage intra-MAP mobility on behalf of MN, the NetMIpv6 Client keeps updating the MAP about the mapping between LCoA and RCoA every time the MN changes its point of attachment from one AR to another inside the same MAP domain. The MIPv6 protocol can be used along with Net-HMIPv6 to provide global mobility management when a MN moves from one MAP to other. The NetMIPv6 Client also acquires local care of address every time a mobile moves from one MAP domain to another. The LCoA is derived using TAR prefix information and RCoA is derived using MAP prefix information. The Net-HMIPv6 solution uses trust model between the NetMIPv6 Client and the MAP in place of end-to-end security model of HMIPv6 as end-to-end security may be difficult to

achieve in this mode of operation. The subsequent revisions of this document will investigate further the end-to-end security model if any that can be used to along with Net-HMIPv6 based solution.

5.2 Net-HMIPv6 and MIPv6 Interaction

The Net-HMIPv6 is able to inter-work with vanilla Mobile Node based MIPv6 protocol (C-MIPv6) [RFC3775]. The C-MIPv6 protocol is used to manage Mobility when a MN moves from one AR to other within a given MAP. To avoid the MN to initiate C-MIPv6 as long it moves from SAR to TAR inside a given MAP domain, the proposed Net-HMIPv6 solution requires that ARs belonging to a given MAP domain to advertise prefix associated with the MAP instead of its own prefix. This is required to prohibit the C-MIPv6 stack in the MN to initiate mobility management signaing over the air when it moves from one AR to another inside a given mobility domain. The advertisement of MAP prefix to the MN ensures that the MN only detects prefix change when it moves away from one MAP to other. If the Client does not have a C-MIPv6 implementation mobility management is entirely performed by the network nodes as described in section 3 of this document, this requirement on the ARs does not apply.

6. Node Requirements

This section describes the requirements for each of the nodes involved.

6.1 Mobile Node Requirements

This solution does not impose any new requirement on the MN. Any MN with an IPv6 stack and DHCPv6 or IPv6CP implementations should work.

6.2 Access Router/NetMIPv6 Client Requirements

the NetMIPv6 Client shall perform the mobility binding creation, modification and deletion functions on behalf of the MN. The NetMIPv6 Client shall support Mobile IPv6 protocol as defined in RFC 3775, and RFC 4285. The user identifier e.g. NAI of the user can be extracted from lower layer protocols, e.g. PPP and MUST be included in client identifier option as defiend in [RFC4283]. The NetMIPv6 client SHALL maintain and update the mobility binding for the MN as long as the MN has an IP session with the AR. The NetMIPv6 client MAY support the IPv4 Home Address Option as defined in [DSMIPv6]. The NetMIPv6 client MAY support the HMIPv6 extentions [RFC4140].

In order to support inter AR HO, the AR SHOULD support HO Request and HO Response messages defined in this document.

6.3 Home Agent Requirements

The HA MUST support the basic Mobile IPv6 operational requirments as defined in RFC 3775, and RFC 4285. The HA shall also support client identifier option as defined in [RFC4283]. The HA MAY support HMIPv6 extenstions. The HA SHOULD support the IPv4 Home Address option as defined in [DSMIPv6].

7. Security Considerations

The HO Request and the HO Response messages SHOULD be protected via IPsec AH. In the absence of such security, the context information of the MN's ongoing session at the SAR may be compromised when sent to a rogue AR.

At the time of L2 establishment, the SAR may receive security keying information for the MN from the Home AAA server that can be used to secure the subsequent BU. The HA should be able to retrieve the corresponding security keying material from the Home AAA server to process the BU and send the BA.

Alternatively, if individual security keying material per MN are not available at the AR and the HA, the AR and the HA SHOULD secure the BU/BA by a common security association that they share.

The support for Route Optimization and the associated security mechanism to protect the return routability signaling is outside the scope of this document. The mechanism proposed in this document allows dynamic HA assignment. Hence the possibility of a inefficient transport due to reverse tunnel can be significantly mitigated.

HMIPv6 supports end-to-end security. However, use of Net-HMIPv6 based approach would require trust between NetMIPv6 Client in the AR and the MAP. Also, it is to be noted that security of HMIPv6 is closely tied to RCoA allocation, hence RCoA need to be allocated in such a way that uniqueness of RCoA allocation is guaranteed otherwise existing HMIPv6 security would break.

8. IANA Considerations

The following ICMPv6 messages need IANA assignment:

HO Request:

Type: TBD-1.

Code: TBD-2.

HO Response:

Type: TBD-3.

Code: TBD-4.

9. Acknowledgements

TBD.

10. Normative References

[DSMIPv6] Soliman et. al., H., "Mobile IPv6 support for dual stack Hosts and Routers", draft-ietf-mip6-nemo-v4traversal-02.txt (work in progress), June 2006.

[RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

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

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2402] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC2472] Haskin, D. and E. Allen, "IP Version 6 over PPP", RFC 2472, December 1998.

[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.

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

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

Authors' Addresses

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

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

Ajoy Singh
Motorola
1421 West Shure Dr.
Arlington Heights, IL 60004
US

Phone: +1 847-632-6941
Email: asingh1@email.mot.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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