Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 4, 2012

B. Sarikaya
Huawei USA

February 1, 2012

Distributed Mobile IPv6
draft-sarikaya-dmm-dmipv6-00.txt

Abstract

As networks are moving towards flat architectures, a distributed approach is needed to Mobile IPv6. This document defines a distributed mobility management protocol. Protocol is based on Mobile IPv6 and its extensions for multiple care of address registration, flow mobility and dual stack mobile IPv6 with minimum extensions. Control and data plane separation is achieved by separating Home Agent functionalities into the control and data planes.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on August 4, 2012.

Table of Contents

1. Introduction

Mobile IPv6 defines client based mobility support to the mobile nodes and is defined in [RFC6275]. There are several extensions to Mobile IPv6 such as multiple Care-of Address registration for multi-homed mobile nodes [RFC5648], flow mobility [RFC6089] and Dual Stack Mobile IPv6 [RFC5555]. Mobile IPv6 is based on a centralized mobility anchoring architecture.

Centralized mobility anchoring has several drawbacks such as single point of failure, routing in a non optimal route, overloading of the centralized data anchor point due to the data traffic increase, low scalability of the centralized route and context management [I-D.liu-mext-distributed-mobile-ip].

In this document, we define a client based distributed mobility management protocol. The protocol assumes a flat network architecture as shown in Figure 1 [I-D.liu-mext-distributed-mobile-ip]. Access router on each link mobile node visits is expected to have the home agent capabilities. Unlike in Mobile IPv6, mobile node at a given time may be registered with more than one home agent and may be receiving data tunneled from these home agents. Mobile IPv6 used in such a flat architecture removes the need for route optimization which has many flaws such as revealing the mobile nodes location to the outside [I-D.liu-mext-distributed-mobile-ip].

Control and data plane separation is stated as a requirement for the distributed mobility management. Mobile IPv6 control plane is used for registration and handover signaling and for establishing security association, e.g. IPSec SAs. Data plane is used for data transfer from the corresponding nodes (CN) to MN and from MN to CNs. Typically control plane traffic is much ligther than the data plane traffic and thus the control plane can be centralized while distributing the data plane. This separation however requires new signaling between the control and data plane functional entities [I-D.yokota-dmm-scenario].

Client based distributed mobility management protocol is designed based on Mobile IPv6 protocols and its many extensions with a minimum amount of extensions.

Due to the popularity of mobile nodes with multiple interfaces client based distributed mobility management protocol must support multi-homed mobile nodes. In this document, this is achieved by way of using [RFC5648]. Flow mobility among the interfaces need to be supported and this is accomplished using [RFC6089]. Mobile nodes in IPv4 only networks also need to be supported and this is done using

[RFC5555].

Access to a content delivery network (CDN) is done using multicasting. Mobile node operation for multicasting is needed for a client based distributed mobility management protocol. The current trend is that service providers tend to relieve the core network traffic by placing the content closer to the users in the access network in the form of cache or local CDN servers. Multicast support in the client based distributed mobility management protocol is out of scope.

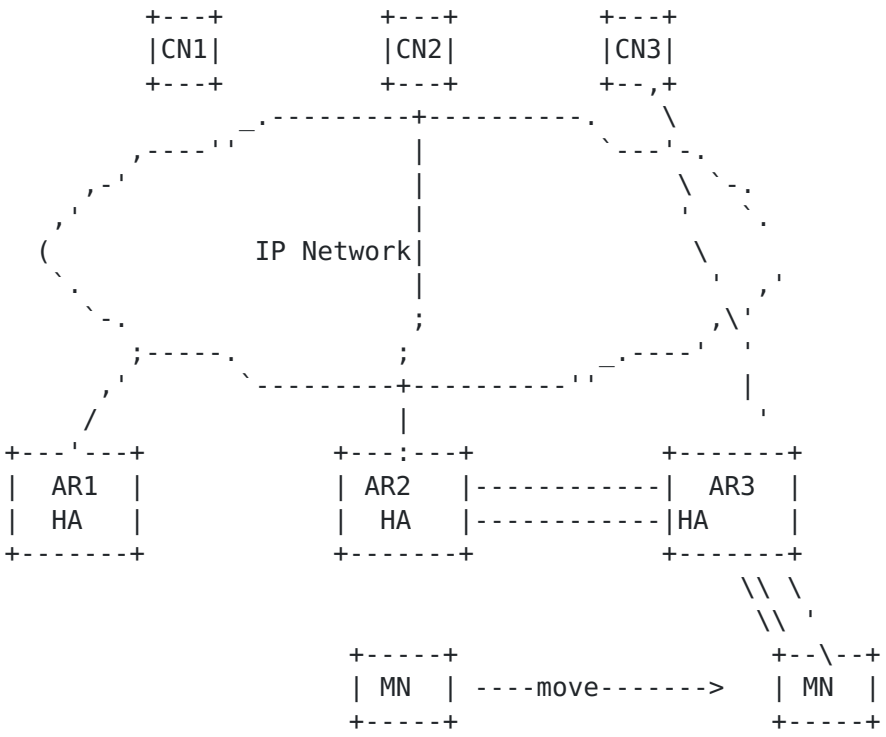

Figure 1: Architecture of Distributed Mobile IPv6 Protocol

2. Terminology

This document uses the terminology defined in [RFC6275].

3. Overview

This section presents an overview of the protocol.

Home agent capable access routers (AR) send router advertisements

(RA) with Home Agent Information Option. Mobile node caches the home agent address when it receives such an RA. Cache entries expire after a timeout period. Only the first entry from MN's home link does not expire.

Mobile node uses a home agent after it moves to another link and if it still has ongoing communication with a correspondent node. MN gets a new Care-of Address (CoA) on the new link and MN sends a Binding Update message to the HA on the previous link to register CoA with HA. Binding Acknowledgement received from HA completes the registration. MN starts to receive the packets over HA-MN link from CN and MN starts to reverse tunnel packets to the CN.

At each link, mobile node goes through bootstrapping if the router advertisement from the access router does not contain Home Agent Information Option. Using [RFC5026] MN either does DNS lookup by home agent name or by service name. MN gets the local domain name during link establishment. This constitutes dynamic assignment of the home agent and [RFC5026] allows such a dynamic assignment as mentioned in Section 5.1.1.

Alternatively, MN can use stateless DHCP for Home Info discovery as in [I-D.ietf-mip6-hiopt]. Dynamic home agent address assignment using DHCP is allowed as mentioned in Section 1.

After the bootstrapping, MN gets a new Care-of Address. MN uses this new address as its new Home Address and registers it in the DNS. HA can register MN's address in the DNS if MN sets DNS Update Mobility Option defined in [RFC5026] and sends it in the binding update to HA. MN sets R bit to zero. The procedure for sending a dynamic DNS update message is specified in [RFC2136]. AAA server could also register MN's new address in the DNS. MN also removes DNS entries with MN's Home Addresses that are no longer used. MN sends BU with DNS Update Mobility Option. MN sets the R flag in the option and sets its old address as the FQDN in the option.

MN uses Cryptographically Generated Addresses if the link is a public multi-access link. Wireless LAN links especially in public hotspots are examples of such links.

4. Correspondent Node Operation

This protocol removes the need for route optimization. Corresponding nodes receive regular IPv6 data packets sent by the mobile nodes and reverse tunneled from the home agent. Also corresponding nodes do not need to be involved in any route optimization message exchanges nor maintaining state, i.e. binding cache.

Correspondent nodes when communicating with the same mobile node may only receive regular IPv6 data packets with no mobility headers. In some cases these packets are directly sent by the mobile node, i.e. when the mobile node is not using its home agent and in some other cases, i.e. when the mobile node starts using a home agent, coming via the home agent.

5. Home Agent Operation

Home agent provides mobility support to the mobile nodes as defined in [RFC6275].

Home agent receiving the DNS Update mobility option MUST process the option as described in Section 6 of [RFC5026]. The dynamic DNS update SHOULD be performed in a secure way. After the DNS update, the home agent MUST send a Binding Acknowledgement message to the Mobile Node, including the DNS Update mobility option with the correct value in the Status field.

Home agent receiving the DNS Update mobility option with R-flag set the Home Agent MUST remove the DNS entry and MUST send Binding Acknowledgement message to the Mobile Node, including the DNS Update mobility option with the correct value in the Status field. Home agent MUST remove the DNS entry upon receiving a deregistration BU from the mobile node. Home agent MAY use the binding cache entry expiration as a trigger to remove the DNS entry.

In this specification route optimization is DISABLED. This means that Home Test Init, Care-of Test Init, Home Test, Care-of Test messages defined in [RFC6275] are not used in this specification.

Home agent MUST support multiple Care-of address registration [RFC5648] and flow mobility for multi homed mobile nodes [RFC6089]. Home agent MUST maintain several flow bindings for a given home address and to direct packets to different care-of addresses according to flow bindings. Home agent MUST keep a flow binding list which is associated with the mobile node with an entry for each flow that is registered.

Dual stack home agent MUST support Dual Stack Mobile IPv6 protocol defined in [RFC5555]. When home agent receives Binding Update message with IPv4 CoA option and IPv4 Home Address option home agent sets a home address and/or prefix, creates a binding cache entry for this mobile node and then sends back a binding acknowledgement message with IPv4 Address Acknowledgement option which includes an IPv4 home address.

6. Mobile Node Operation

Mobile nodes keep a cache of home agent addresses. This cache is called Binding Update List in [RFC6275] and is used for route optimization. In this specification, home agent cache or binding update list is used to keep track of the home agents with which the mobile node is currently registered and not for route optimization.

Mobile node sends periodic binding update messages to each home agent in the home agent cache if the sessions initiated when mobile node was on home agent's link. This keeps the HA-MN tunnel active. Mobile node MAY send a deregistration BU when the sessions initiated with the home agent are no longer active.

If mobile node receives a router advertisement with Home Agent Information option it adds an entry to the home agent cache. Mobile node does not establish a binding with a home agent until it moves to a new link and still has active sessions initiated when on link. On the new link, if a binding update message is not sent the cache entry for this home agent is removed.

On a new link, mobile node does a DNS lookup for a Home Agent address if it is configured with a DNS server address. If the Mobile Node is configured with the Fully Qualified Domain Name of the Home Agent it does DNS lookup by home agent name. Otherwise mobile node does DNS lookup by service name and constructs a request with QNAME set to "_mip6._ipv6.example.com" and QTYPE to SRV.

On a new link, mobile node does home agent address discovery using stateless DHCP if configured. Mobile node as DHCP Client exchanges home network information with DHCP server. Mobile node sends Information-request message including the Home Network Information option. Mobile node indicates its preference about the requested home network with the Id-type in the Home Network Information option. Mobile node MUST set the Id-type to 2 to indicate that the mobile node has no preferred home network. Such a value is needed for bootstrapping on any link. DHCP server returns the Reply message including a Home Network Information option which contains home agent address and home network prefix.

In the registration binding update message mobile node MUST set DNS Update mobility option so that home agent does DNS update on its behalf. Mobile node does not set the flag R in the option. Mobile node sets the MN identity field in DNS Update option with its FQDN and sets its Home Address in the Home Address Option. DNS update is made based on these values.

Mobile node starts to use a home agent after it moves to a new link

and if it still has ongoing communication with a correspondent node. MN registers its care-of address with the home agent. MN changes its communication with the corresponding node: MN starts to receive the packets over HA-MN link from CN and MN starts to reverse tunnel packets to the CN. To the corresponding nodes this change is invisible except for some additional delays the tirangular route may introduce.

6.1. Multiple Interface Operation

When a new interface becomes active such as Wi-Fi the mobile node forms an address and starts using that interface for communication on that link. No home agent is involved. When the mobile node starts to use a home agent any new communication on the new interface MUST use the registered home address. Mobile node MUST register its care-of address with this home agent as described in [RFC5648]. In the Binding Update message, Binding Identifier Mobility option defined in MUST be used. Mobile node MUST assign a BID for this Care-of Address which is unique. Mobile node also MUST assign a BID-PRI for this BID with lower value indicating a higher priority. If the registration is successful mobile node receives a binding acknowledgement with Status set to zero in the Binding Identifier Mobility option.

Multiple Care-of address registration allows flow mobility between interfaces of a mobile node. Mobile node can then move flows by sending BU with flow identification mobility option.

Multiple interfaces and possible use of multiple home address registered with the home agents makes it important for the mobile node to select the correct source address in sending packets.

7. IPv4 Support

In IPv4 only foreign networks mobile node gets an IPv4 care-of address. It registers this address with a dual stack home agent only after moving to a new link and with open sessions with the correspondent nodes. Mobile node includes IPv4 CoA option and IPv4 Home Address option in the binding update message when registering and gets an IPv4 Home Address assigned. Mobile node does a DNS update registering its IPv4 home address on the DNS.

In IPv4 only foreign networks mobile node does stateless DHCP in order to receive the home network information. Mobile node MUST use Home Network Information DHCPv4 option defined in [I-D.xia-mext-hioptv4].

8. Control and Data Plane Separation

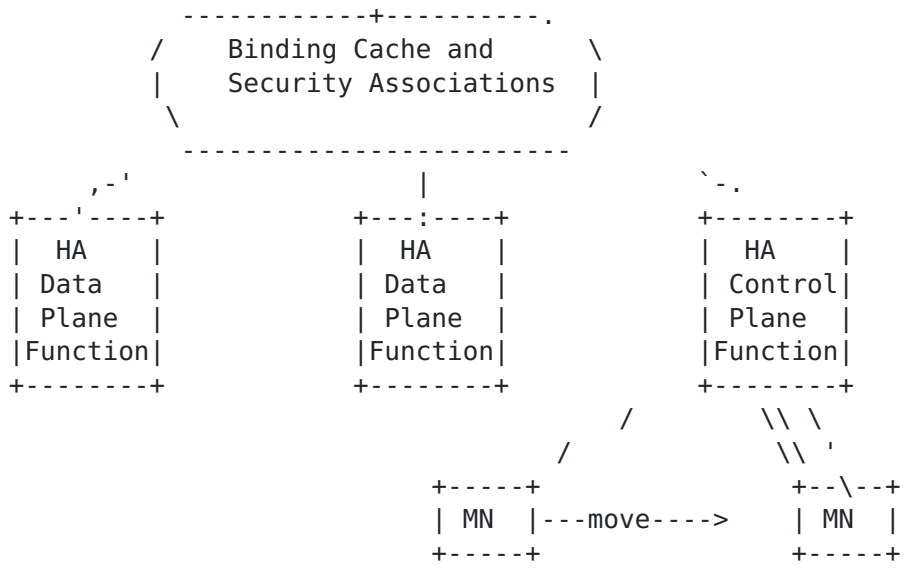

Figure 2: Architecture of Control and Data Planes

Control and data plane separation can be achieved by dividing HA into two functional entities: control plane functional entity and data plane functional entity as shown in Figure 2. These functional entities can be hosted on different physical entities. These two entities must share a common database. The database contains the binding cache and the security association information such as IPSec keys.

MN first communicates with the control plane function to establish security association. Address configuration and binding registration follows. Next MN receives/sends data packets using the data plane function closest to the link MN is attached.

When MN moves MN does handover signaling with the control plane function which updates the binding cache based on this move. Control plane function informs the new data plane function of this binding cache update and then this MN starts to receive and send data to the new data plane function. MN MUST keep HA control plane function address in cache so that it can conduct handover signaling with it.

When MN boots, it goes through authentication and security association establishment. Next MN sends a binding update. MN does these steps with HA control plane function. MN sends Binding Update message to HA control plane function and receives a Binding Acknowledgement message and in this message MN MUST receive HA data plane function address.

HA data plane function address can be provided by HA control plane function to MN in Alternate Home Agent Tunnel Address option defined in [I-D.perkins-mext-hatunaddr] of BA message [RFC6275].

Control and data plane separation does not require protocol extensions except the sharing of binding cache and security associations database. How this sharing can be accomplished is left out of scope with this specification.

9. Authentication for Distributed Mobility Management

Currently, MN and HA create security associations (SA) based on the home address using IKEv2 as the key exchange protocol. When MN moves SAs are reestablished when MN gets a new care-of address. After SA is established, MN and HA use Encapsulating Security Payload (ESP) encapsulation for Binding Updates and Binding Acknowledgements [RFC4877].

IKEv2 enables the use of EAP authentication and provides EAP transport between MN as the peer and HA as the authenticator. EAP authentication is done using one of the EAP methods such as EAP-AKA [RFC4187].

MN is authorized as a valid user using EAP authentication. IKEv2 public key signature authentication with certificates is used to authenticate the home agent and derive keys to be used in exchanging BU/BA securely. MN can use the same identity, e.g. MN-NAI during both EAP and IKEv2 authentication.

On the other hand MN goes through the access authentication when it first connects to the network. A typical access authentication protocol is AKA. MSK derived from this authentication serves as the session key in accessing the air interface.

There is an overlap between the access and user authentications sometimes done using the same protocol, e.g. AKA. Full EAP method execution may take several round trips, some times five or more round trips and slow down the user access to the Internet. This is especially an important consideration in Distributed Mobility Management since MN may connect to several home agents instead of staying anchored at one home agent.

In order to reduce the number of round trips EAP authenticaton can be combined with reauthentication. Reauthentication is EAP method dependent. EAP-AKA reauthentication takes only one round trip [RFC4187]. MN must go through an EAP-AKA reauthentication before when MN was connected to the previous HA. During reauthentication

reauthentication ID is generated. MN MUST use its reauthentication ID during IKEv2 EAP authentication with the new home agent. This ensures that EAP-AKA authentication takes only one round trip. MN continues to use its reauthentication ID in subsequent reauthentication runs with the same HA.

10. Security Considerations

TBD.

11. IANA Considerations

TBD.

12. Acknowledgements

Romain Kuntz provided many comments that has lead to improvements in this document.

13. References

13.1. Normative References

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

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.

[RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G.,

and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

[I-D.ietf-mip6-hiopt]
Jang, H., Yegin, A., Chowdhury, K., and J. Choi, "DHCP Options for Home Information Discovery in MIPv6", draft-ietf-mip6-hiopt-17 (work in progress), May 2008.

[I-D.xia-mext-hioptv4]
Xia, F. and B. Sarikaya, "DHCPv4 Options for Home Information Discovery in Dual Stack MIPv6", draft-xia-mext-hioptv4-04 (work in progress), January 2012.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

13.2. Informative references

[I-D.liu-mext-distributed-mobile-ip]
Liu, D., "Distributed Deployment of Mobile IPv6", draft-liu-mext-distributed-mobile-ip-00 (work in progress), March 2011.

[I-D.yokota-dmm-scenario]
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

[I-D.perkins-mext-hatunaddr]
Perkins, C., "Alternate Tunnel Source Address for Home Agent", draft-perkins-mext-hatunaddr-02 (work in progress), October 2011.

Author's Address

Behcet Sarikaya
Huawei USA
5340 Legacy Dr. Building 175
Plano, TX 75074

Phone: +1 469 277 5839
Email: sarikaya@ieee.org