

Network Working Group
Internet-Draft
Expires: January 6, 2008

V. Narayanan
Qualcomm, Inc.
D. Thaler
Microsoft
M. Bagnulo
Huawei Lab at UC3M
H. Soliman
Elevate Technologies
July 5, 2007

IP Mobility and Multi-homing Interactions and Architectural
Considerations
draft-vidya-ip-mobility-multihoming-interactions-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 6, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

A number of protocols have been defined at the IETF to handle IP mobility and multi-homing - each of the defined protocols satisfies a

different set of requirements - however, there is an overlap on some of the requirements and features among many of these protocols. In practice, a combination of the protocols are likely to be deployed in a system. There are various such combinations plausible, but some combinations are more realistic than others. This document analyzes the overall mobility and multi-homing architecture and highlights some key points to consider while deploying an architecture consisting of one or more of these protocols. The protocols considered in scope for this document include Mobile IPv4 (MIPv4), Mobile IPv6 (MIPv6), Hierarchical Mobile IPv6 (HMIPv6), Fast Mobile IPv6 (FMIPv6), Network-based Local Mobility Management (NetLMM), MOBIKE, Host Identity Protocol (HIP), and Shim6.

Table of Contents

1.	Introduction	4
2.	Terminology	4
3.	IP Mobility and Multi-homing - Relative Analysis	7
4.	Protocol Sub-classes	10
4.1.	Node-based Mobility and Multihoming	10
4.1.1.	Mobile IP	10
4.1.2.	Hierarchical Mobile IP	11
4.1.3.	Fast Mobile IP	12
4.1.4.	MOBIKE	12
4.1.5.	SHIM6	12
4.1.6.	HIP	13
4.2.	Network-based Mobility	14
5.	Mobility Architectures	15
5.1.	Architectural Entities	15
5.2.	Protocol Stacks	18
6.	Protocol Interactions, Usage Models and Architectural Implications	20
6.1.	Multi-Level Node-based Mobility and Multihoming	20
6.1.1.	MIP, HMIP, and FMIP	21
6.1.2.	MIP and MOBIKE	25
6.1.3.	MIP and SHIM6	27
6.1.4.	MIP and HIP	27
6.1.5.	SHIM6 and MOBIKE	27
6.1.6.	SHIM6 and HIP	27
6.1.7.	HIP and MOBIKE	27
6.1.8.	MIP, SHIM6 and HIP	27
6.2.	Node-based and Network-based Mobility	28
6.2.1.	Security Implications	29
6.2.2.	Multihoming Implications	30
6.2.3.	Network-based mobility for non-MIP nodes	32
6.2.4.	Other Analysis	32
7.	Security Considerations	33
8.	IANA Considerations	33
9.	References	33

Authors' Addresses	35
Intellectual Property and Copyright Statements	37

[1.](#) Introduction

Over the years, several protocols have been defined at the IETF to handle changes to IP addresses of endpoints in a seamless fashion and preserving communications established using a given IP address across changes in the IP points of attachment. Essentially, all of the proposed mechanisms provide IP address permanence at some level to layers above. Some protocols go beyond support for just single-interfaced endpoints and allow multi-homing and IP address permanence to applications on infrastructure sites, servers, gateways, etc. "Permanence" as used here is typically bound by some length of time and hence is not quite permanent in the literal sense. The idea is for the IP address, as observed by layers above IP, to stay constant within that duration, even if the endpoint changed its IP point of attachment or added an interface within that time. The existing documents on these protocols provide sufficient details for the individual protocol operation itself, but do not touch on architectural aspects. In practice, a combination of the protocols are likely to be deployed in an architecture. There are various such combinations plausible, but some combinations are more realistic than others. Also, various considerations come into play while defining an overall architecture that encompasses IP mobility and multi-homing. Often, a network may need to support a variety of such protocols to satisfy the varying needs of the different nodes that attach to it. Also, a given node would often support multiple such protocols for various reasons.

This document analyzes the overall mobility architecture and highlights some key points to consider while deploying an

architecture consisting of one or more of these protocols. The protocols considered in scope for this document include Mobile IPv4 (MIPv4), Mobile IPv6 (MIPv6), Hierarchical Mobile IPv6 (HMIPv6), Fast Mobile IPv6 (FMIPv6), Proxy Mobile IPv6 (PMIPv6), MOBIKE, Host Identity Protocol (HIP), and Shim6.

2. 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 [[1](#)].

This document follows the terminology that has been defined in the normative references included in this document. In addition, the following terminology is used in this draft.

IP Mobility

IP mobility refers to changes in the IP point of attachment of a node. As a consequence of this change, a node may obtain a different (topologically meaningful) address. The result is that a mobile node or network, as it moves, may obtain different topologically meaningful IP addresses that it can use for IP-based communications. Some protocols allow the nodes to maintain the same IP address as they move across different IP points of attachment.

IP Mobility Protocol

An IP mobility protocol provides transparency to layers above IP from the changes in the IP addresses resulting from IP mobility. In particular, such protocols allow nodes to continue IP communications independent of the current IP point of attachment and to preserve established communications across any corresponding IP address changes. A key element of an IP mobility protocol is to detect movement and do what is needed to allow communication continuity.

IP Multi-addressing

A node or a network is multi-addressed when it simultaneously has multiple topologically meaningful addresses or prefixes. Note that nodes and networks can be multi-addressed even if they only have a single network attachment point. This is typically true for IPv6 nodes for example, since interfaces can have both link-local and global addresses.

IP Multi-homing

A network is multihomed when it has multiple network (not necessarily physical) attachment points. From an IP perspective, these multiple attachment points typically imply that the node or network is also multi-addressed. There are some exceptions, however, (e.g., with Provider Independent (PI) addressing), where multihoming does not translate to having a meaningful address/prefix from each of the providers. Similarly, a node is multihomed when it has multiple network interfaces

IP Multi-addressing Protocol

An IP multi-addressing protocol provides transparency to upper layers from changes in the IP address actually used to exchange packets by presenting a constant IP address. A key element of an IP multi-addressing protocol is to detect the reachability status

of the different addresses and do what is needed to allow communication continuity.

Node-based Mobility

Node-based mobility is defined as an IP mobility mechanism where the mobility management signaling is performed by the node requiring mobility itself. Mobile nodes include end hosts and routers that may be mobile.

Network-based Mobility

Network-based mobility is defined as an IP mobility mechanism where the mobility management signaling is performed by a network entity on behalf of the node requiring mobility itself.

Local Mobility

For the purpose of this document, local mobility is defined as mobility within a given domain. Local mobility protocols allow at least one IP address of a node to remain constant within the local domain. Continuity of sessions using that IP address in the local domain is a goal for these protocols. The term "domain" is quite loosely used to indicate a region within which it is practical to expect end-to-end security associations between the mobility signaling endpoints. Typically, this is limited to a single administrative domain. Depending on the protocol used, this may mean mobility within an access technology or may also involve inter-technology handoffs.

Global Mobility

For the purpose of this document, global mobility is defined as mobility within a larger geographic area. Typically, this includes mobility across heterogeneous technologies and inter-administrative domains. Global mobility protocols allow at least one IP address of a node to remain constant across any handoffs. Continuity of sessions using that IP address across handoffs is a goal for these protocols.

Global Roaming

This term is used to refer to the availability of a set of services to a node from anywhere, at any time. Maintenance of IP address or session continuity is not a goal for this. This term encompasses the cases of a node roaming world-wide and accessing a set of services from anywhere.

Correspondent Node

Any entity that communicates with a mobile node is referred to as a correspondent node.

Access Router

An Access Router is defined as the first hop IP router for a

mobile node at its point of attachment. This entity typically serves as the default router for the mobile node.

Access Network

An access network is typically the edge network to which a mobile node attaches. An access network typically comprises of one or more physical and link layer attachment points, as well as one or more access routers.

[3.](#) IP Mobility and Multi-homing - Relative Analysis

IP mobility and multi-homing are closely related in one sense and somewhat different in another sense. Protocols that handle IP mobility and multi-homing can be used together in a competing or complementary fashion. All IP mobility protocols support basic host multi-homing or multi-addressing functions. There are protocols that further support site multi-homing, that can be leveraged for mobility to a certain extent. A system looking at using the various available components should look at the scope of each and the requirements at hand to see how best to fit these together. This section provides an analysis on the relative scope and requirements handled by each suite of protocols.

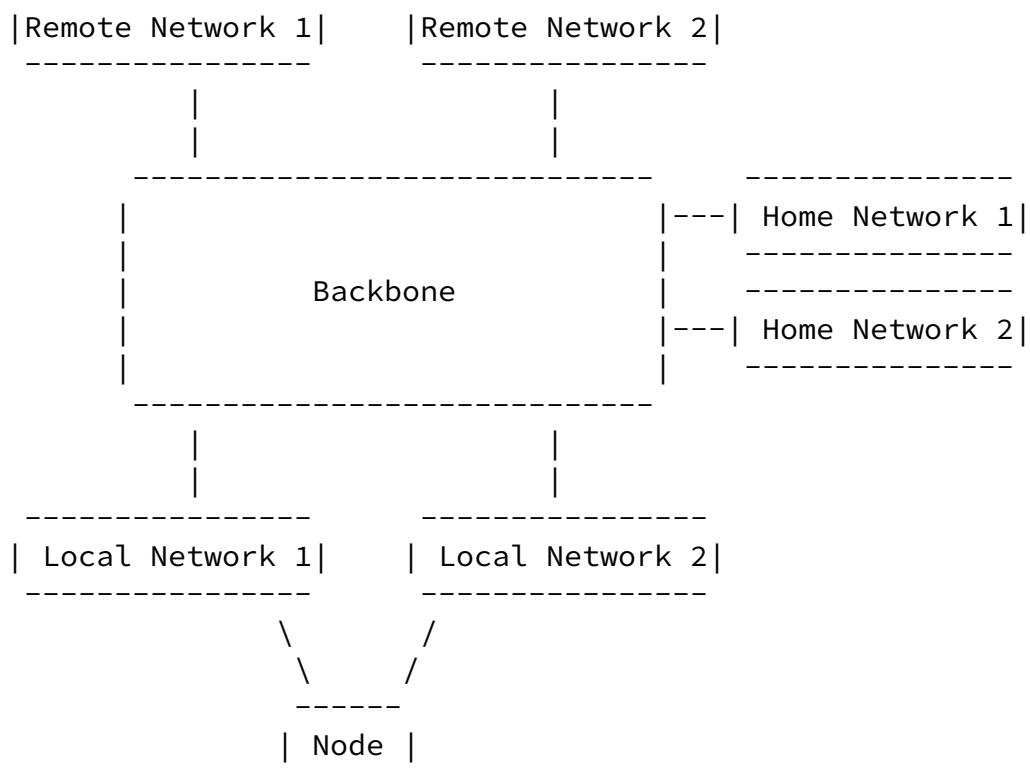


Figure 1: End Node and Multi-Network Associations

Figure 1 shows a multi-network setup with local networks, remote networks and home networks, all inter-connected in some fashion. The main idea is that these networks can communicate via a backbone of some form. There are three classes of networks illustrated here:

Local Networks

A local network is an access network to which a node is attached at any given time. The node may or may not have a long term association with that network. The local network often defines the actual IP point of attachment of a node and may change over time.

Home Networks

A home network is one with which a node has a long term association (this is not to be confused with the "home network" in the context of Mobile IP or related protocols). While that is certainly one example of a home network, the various provider networks in the SHIM6 context may also be home networks from an association point of view. Networks with which a node has a VPN relationship may also fall under this category.

Remote Networks

A remote network is one with which a node has no association. A remote network may become a local network at some point of time. A node with certain local and home networks may communicate with any of the networks. For generality, everything except the local and home networks may be viewed as a remote network.

Given all the networks, there are several mobility, multihoming, and multi-addressing relations that can be drawn from here.

Note that the nodes within a multihomed network will be exposed to multiple prefixes and they will then configure multiple global topologically meaningful addresses. The result is that nodes within a multihomed network are multi-addressed, as are nodes which are themselves multihomed. Even if the former type of nodes access the Internet through a single interface, the use of different addresses implies different paths (because each address is associated to a different point of attachment of the multihomed network to the Internet). Both types of nodes encounter similar problems and also benefit from a multi-addressing support protocol.

The multihoming aspects may vary due to mobility or due to network unreachability. The former may cause more frequent changes in the multihoming state than the latter. Also, a node may be multihomed both in the local and home networks. For instance, a mobile node with cellular and WLAN accesses may be associated with two ISPs or with an ISP and an enterprise network. The local multihoming situation may change relatively frequently based on the rate of mobility of the node, while the multihoming situation with multiple home networks may remain fairly stable.

Correspondent nodes may be located in the local, home, or remote networks. While it is technically feasible for communication with the correspondent node to happen using any of the IP addresses owned by the node, there may be some practical considerations with respect to making IP address changes known to the correspondent nodes and its impact to applications in use. Using DNS updates or SIP Re-invite like mechanisms, IP address changes can be made visible to the correspondent nodes. For some applications, such transitions may be seamless enough, while it may not be the case for some other applications.

The alternative to DNS updates or SIP Re-invites and affecting applications with IP address changes and reachability issues is to provide an unchanging address to the applications and handle actual

IP address changes at a lower layer. This is the approach taken by IP mobility and multihoming protocols, although in different ways.

IP mobility protocols achieve this property via tunneling mechanisms. A centralized entity keeps track of the current location of the mobile node, so that data can be appropriately forwarded to the node. IP multihoming protocols like SHIM6 achieve this property via a shim layer between the IP and transport layers that perform address translation, thereby avoiding tunnels.

IP mobility protocols developed at the IETF thus far are scoped to solve both mobility and multihoming in the context of a single home network. In other words, local multihoming (attachment to multiple local networks) is handled by extensions to Mobile IP, for instance. Some rudimentary local multihoming is also feasible by the basic Mobile IP class of protocols without extensions. This provides seamlessness to the applications using the address of the end node associated with one home network for communication.

IP multihoming protocols developed at the IETF thus far are scoped to solving site multihoming in the context of one or more local and/or home networks. The main difficulty that multi-addressed nodes face when managing their multiple addresses, is that the reachability status of the addresses may vary during the lifetime of a communication (e.g. because of outages) and it may be required to use a different address for continuing an established communication, since the original one has become unreachable. While address unavailability and additions may be caused by mobility, solving node mobility is not a goal of the protocol.

[Section 6.1.3](#) provides details on how IP mobility and multihoming protocols can be architecturally combined.

[4.](#) Protocol Sub-classes

[4.1.](#) Node-based Mobility and Multihoming

[4.1.1.](#) Mobile IP

Mobile IP (v4 and v6) provides a mechanism by which a node can maintain the same IP address as it changes its IP point of

attachment. This is enabled by having a Home Address which is on the prefix of a Home Agent and a Care-of-Address which is the topologically correct local address at the point of attachment. The Home Agent maintains the mapping between the Home Address and the Care-of-Address. The Mobile Node is responsible for updating the binding between the Home Address and Care-of-Address at the Home Agent. All packets sent to the Home Address of the mobile node will be received by the Home Agent and tunneled or forwarded to the mobile node at its Care-of-Address. The packets sent from the mobile node

may be sent directly or reverse tunneled through the Home Agent.

Mobile IPv4 (MIPv4) additionally provides a mode of operation with a Foreign Agent in the local network. The Foreign Agent makes conservation of IP space possible by allowing multiple mobile nodes on its link to share the same Care-of-Address. The Care-of-Address in this case is the IP address of the Foreign Agent. The Mobile IP tunnel in this case terminates at the Foreign Agent and the Foreign Agent forwards packets to the mobile node based on the Home Address in the packets.

Mobile IPv6 (MIPv6) additionally provides the capability of route optimization. Here, the mobile node may provide the Home Address-Care-of-Address binding to a correspondent node (CN) so that the CN sends packets directly to the Care-of-Address bypassing the Home Agent.

Mobile routers may be supported using Network Mobility (NEMO), where, in addition to a Home Address, a prefix owned by the node is also bound to the Care-of-Address at the Home Agent or CN.

Multi-homing for the Care-of-Addresses may be supported in MIPv6 using extensions being defined in [2]. This allows multiple Care-of-Addresses for an mobile node to be bound to a given Home Address. There are extensions being proposed to use multiple Care-of-Addresses simultaneously based on flow mapping information - [2], for instance. One Care-of-Address is registered as a primary Care-of-Address and is used by default. Multiple Care-of-Addresses are also supported in MIPv4 (simultaneous bindings), although data is duplicated to every Care-of-Address registered [3].

[4.1.2.](#) Hierarchical Mobile IP

Hierarchical Mobile IPv6 (HMIPv6) [4] provides a means of local mobility management for mobile nodes. Essentially, it is a variant of MIP6 that provides more efficient mobility within a local domain. In this case, the mobile node obtains a Regional Care-of-Address (RCoA) in the prefix of a Mobility Anchor Point (MAP) and a Local Care-of-Address (LCoA) which is the topologically correct IP address at the point of attachment. The mobile node is responsible for updating the binding between the LCoA and RCoA at the MAP. HMIPv6 may be used independent of the use of MIP6. This results in a deterministic delay for routing updates due to the MN's movement, when compared to the variation in delays when relying on updating the HA (which can be anywhere on the Internet). HMIPv6 also reduces the number of binding updates sent as a result of movement to one.

A similar concept for Mobile IPv4, regional registration, has been

proposed [5]. In Regional Registration, a Generic Foreign Agent is used in place of the MAP to hide the local mobility from the Home Agent. Unlike HMIPv6, regional registration relies on the presence of Mobile IP as a higher level mobility management protocol in the system.

In general, all the extensions defined for MIP6 may be used with HMIPv6 as well. Hence, NEMO and multiple Care-of-Address binding would also be supported in HMIPv6. Similarly, MIP4 extensions may be used with regional registration mechanisms as well.

4.1.3. Fast Mobile IP

Fast Mobile IP (v4 and v6) provides a means of local mobility management at the edge for mobile nodes. FMIP is designed to provide temporary mobility management across Access Routers for faster and low latency handoffs. Here, a previous Care-of-Address (pCoA) is bound to a new Care-of-Address (nCoA) at the previous Access Router (pAR), after the mobile node has left the pAR and attached itself to a new Access Router (nAR). Effectively, data is tunneled from the pAR to the mobile node at its nCoA

FMIPv4 also supports the Foreign Agents, in keeping with MIP4. In addition to FMIPv4, some low latency extensions to MIP4 have also been proposed in [6].

[4.1.4.](#) MOBIKE

MOBIKE provides mobility and multi-homing capabilities to IKEv2. When IKEv2 is used to create IPsec Security Associations between a node and a VPN gateway, the node may change its IP point of attachment, causing a change to the IP address which was used in IKEv2. Further, the node and the VPN gateway may be multi-homed with multiple IP addresses. MOBIKE allows a node to update its IP address on the IKE SA and correspondingly change the IPsec tunnel outer addresses. Hence, a node may change IP addresses without having to re-establish the IKE and IPsec SAs. Packets sent to the tunnel inner address of the node are tunneled to the appropriate outer address.

Since IKEv2 is defined in an IP version agnostic manner, MOBIKE also applies equally to IPv4 and IPv6.

[4.1.5.](#) SHIM6

In order to preserve global routing system scalability, the Site Multi-homing by IPv6 Intermediation (Shim6) approach proposes that multihomed sites obtain multiple globally routable prefixes, one from each of their ISPs. In this configuration, each prefix assigned to a

multihomed site can be aggregated into the prefix of the correspondent ISP, eliminating the contribution of multihomed sites to the global routing table. The result is that interfaces within multihomed sites will configure one address per prefix that is available in the site. In this setup, each address is reachable as long the corresponding path is working, so in order to preserve established communications through outages, it may be necessary to change the address used for exchanging packets during the lifetime of the communication. This is achieved using the Shim6 protocol.

The Shim6 protocol provides a means by which two nodes with more than one IP address pair can change the address used to exchange packets during the lifetime of a communication without impacting the applications. Shim6 introduces the concept of an Upper Layer Identifier (ULID), and allows the IP address chosen by applications to persist, while using different addresses (called locators) to actually exchange packets below IP, based on their reachability status. A shim sub-layer located within the IP layer, between the IP

endpoint sub-layer (handling fragmentation and IPSec functions among others) and the IP forwarding sublayer provides this transparency. The ULIDs used by Shim6 are in the form of an IPv6 address and contain cryptographic information that is used to secure the binding between the ULID and its locator set. The Shim6 architecture has two main components. The Shim6 protocol that is used to create and manage the Shim6 context between the endpoints containing ULID pair and locator set information for the peers. The other component is the failure detection and alternative path exploration protocol (called REAP), that allows the peers to detect failures along the currently used path and explore alternative locator pairs to divert the communication through.

4.1.6. HIP

The Host Identity Protocol (HIP) [[RFC4423](#)] is a new architecture that separates the identity and the locator functions currently performed by the IP address in the Internet architecture. It does so by creating a new namespace for the identity of the network layer endpoints. The new identity namespace is cryptographic in nature, since the Host Identities (HI) are public keys that are associated to the hosts they represent. In order to be backward compatible with current transport and application layers, the HIP architecture does not impose the direct usage of the HI by the upper layers, but provides a compact representation of the Host Identities, namely the Host Identity Tag, which are 128 bits long hashes of the actual HI. The result is that transport and application layer communications are bound to the HI/HIT while the actual packets are routed at the IP layer using routable IP addresses. The HIP sub-layer located in the IP layer securely performs the translation between the host identity

and the routable locators.

The HIP architecture provides built-in security features. Essentially, HIP can be seen as a key exchange protocol, through which the keys associated to the HI/HITs are negotiated prior to the beginning of the communication. Actual data packets are carried encapsulated with ESP protection. So, the HIP architecture naturally provides the means to establish secure communication channels between the peers. Moreover, since the endpoint identity space is cryptographic in nature, the HIP architecture intrinsically provides the means to prove identity ownership without requiring any

additional infrastructure. Such capability enables alternative means to support mobility and multihoming, as described in [7]. Essentially, mobility and multihoming support for the HIP protocol relies on conveying alternative locator information in HIP signaling messages called UPDATE messages. Such UPDATE messages are protected using the trust acquired while the initial HIP key exchange. In order to support simultaneous movement and initial contact after movement, the HIP architecture relies on Rendez-Vous server defined in [8].

[4.2.](#) Network-based Mobility

Network-based mobility provides a means of mobility management for nodes without involving the nodes themselves in the signaling. This is done by making IP mobility transparent to the nodes. Network-based Local Mobility Management (NetLMM) is essentially a concept of providing local mobility using network-based mobility management protocols. Here, a Mobility Access Gateway (MAG), often located at the Access Router (AR), updates a Local Mobility Agent (LMA) with the location of a mobile node. A mobile node acquires an IP address in the NetLMM domain, which remains the same as long as the mobile node remains within that domain. Hence, the changes in the IP point of attachment do not cause IP address changes.

By definition, NetLMM allows an IP prefix to span multiple links. By assigning a unique prefix for every mobile node and by employing virtual point-to-point link semantics for link local behavior, it is possible to avoid the issues of multi-link subnets [9] in NetLMM.

Also, by definition, NetLMM provides mobility for a given IP address or prefix of a node. If a node is multi-addressed, mobility for each address or prefix will be handled separately in the NetLMM domain. While it is feasible to identify the multiple IP addresses or prefixes as belonging to the same node using other identifiers, it is not possible to provide transparency of such addresses to correspondent nodes or applications.

[5.](#) Mobility Architectures

This section provides an overall picture of all the elements involved in an overall mobility architecture. It also provides a description

of where the various IP mobility functions fit in the stack relative to other protocols.

[5.1.](#) Architectural Entities

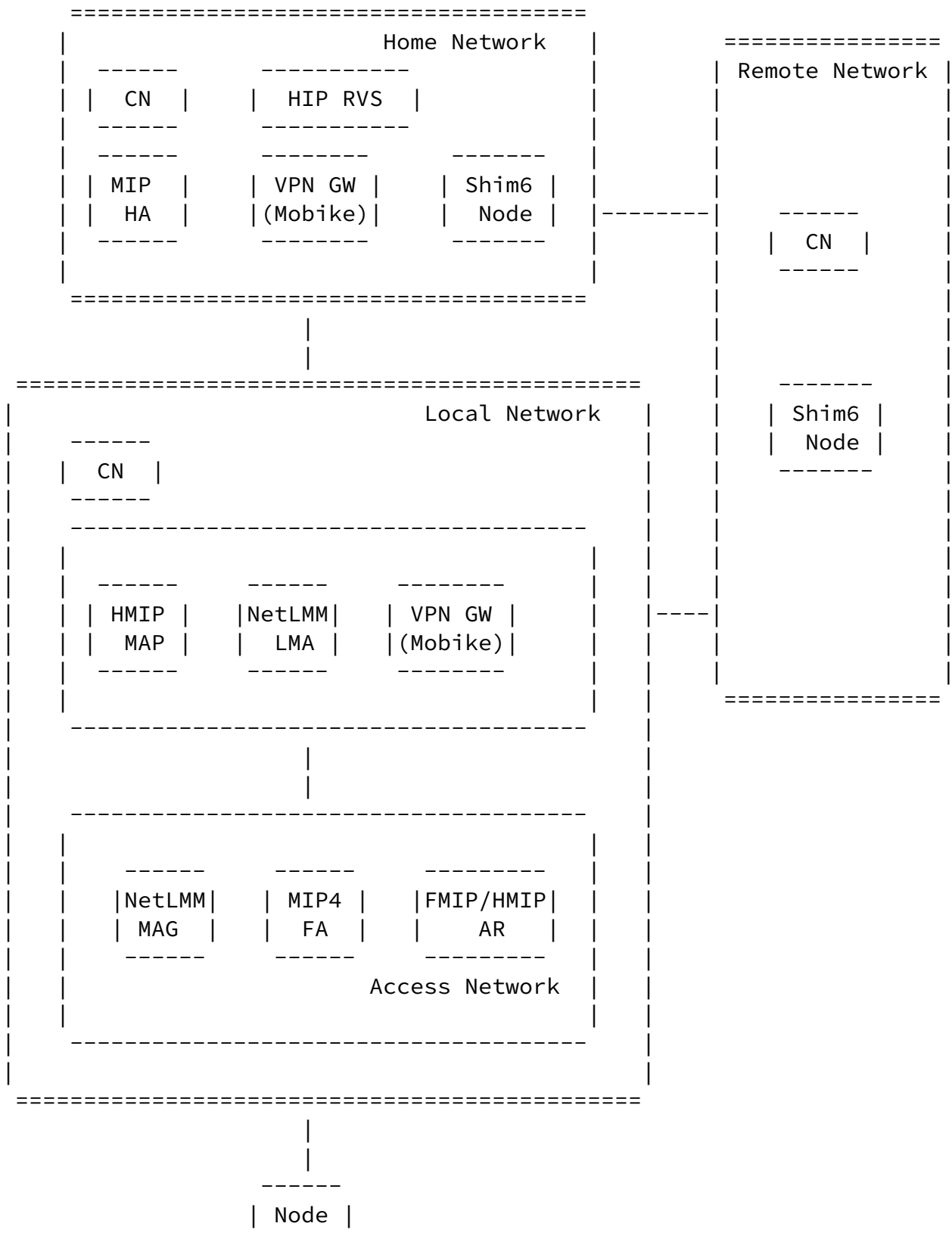


Figure 2: Architectural Entities in IP Mobility and Multi-homing

Figure 2 shows a potential network architecture with various components of IP mobility management entities. The figure follows the local, home and remote network models shown in Figure 1. As shown, a part of the local network may be the edge or access network to which a node attaches. The access network typically consists of the first hop IP routers that nodes can attach to. The access network also provides the physical point of attachment (wired or wireless access with L1/L2 points of attachment such as access points) for the nodes. Depending on the system, there may or may not be mobility management elements in the local network. Also, depending on the system, there may not be a home network at all. For completeness, the figure shows the possible IP mobility management entities. All the elements shown are logical elements and some of them may be physically collocated in a system.

As shown in the figure, the Mobility Access Gateway, the Foreign Agent, and the Access Router are all functions residing on the MN's first hop router. The MAG is responsible for playing the role of a network-based mobility client. The Foreign Agent provides MIP4 services and the Access Router plays a role for FMIP and HMIP. In FMIP, the Access Router is responsible for assisting the MN in predicting the handover, in addition to handling of edge tunnels upon handoff of a node and in HMIP, the Access Router is responsible for advertising the MAP in the IPv6 Router Advertisements. While all these elements can technically co-exist in the same access network and in the same physical box, there are some considerations that need to be taken into account when these do co-exist. Such considerations are outlined in [Section 6](#).

When the local network supports mobility management, there may be other entities such as a Mobility Anchor Point (MAP), a Local Mobility Agent (LMA), a VPN gateway supporting MOBIKE, or even a Home Agent present in the local network. One or more of these may serve a node from a mobility management perspective. Some of these interact with some of the elements in the access network to support IP mobility for the end node. As in the case of the access network elements, one or more of these logical functions may be present in the local network and may be collocated in the same physical entity. Some interactions are studied in [Section 6](#).

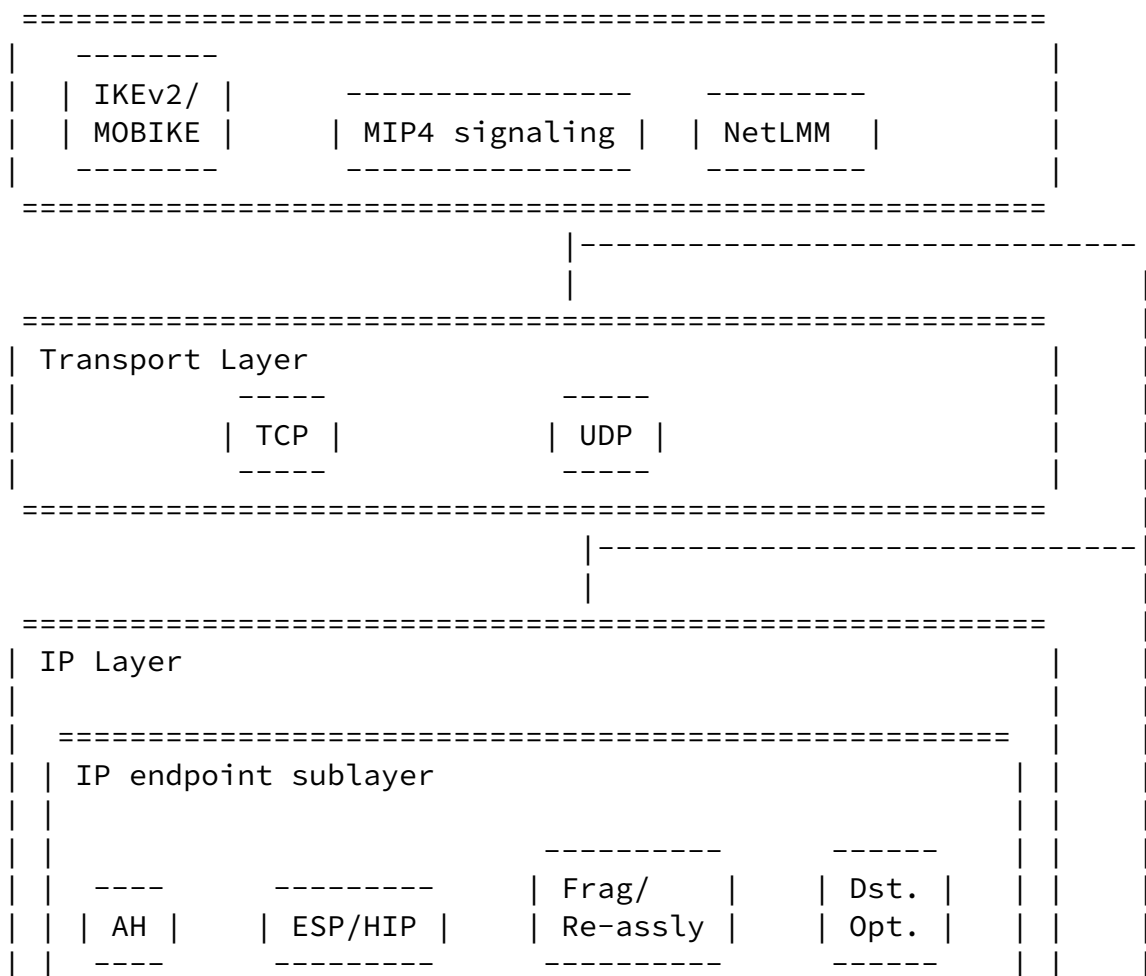
When involved in mobility management, a home network may host a Home Agent or a VPN Gateway supporting MOBIKE. Local mobility management entities may be present in a home network, where the home network is also a local network. Note that the sub-divisions of local, home and remote network, etc. are with respect to the end node - for e.g., a network that is remote for one node may be a local network for a different node.

The end node itself may be multi-homed in a couple of different ways - it may have multiple addresses from the home or local network. The node may have multiple interfaces that attach to different access networks within the same or different local network. Further, the node may also have connectivity to multiple home networks, as discussed in [Section 3](#) - for instance, it may be served by different Home Agents or VPN Gateways for access to specific services in each home network. The node may use Shim6 for multi-homing - it may correspond with other Shim6 nodes in other networks. Even though a Shim6 node is shown separately in the home and remote networks, any of the other entities may also be Shim6 capable.

One aspect not indicated in the figure is connectivity to the "Internet" or other networks. It can be assumed that any of the networks provide connectivity to the Internet. The home network can also be expected to provide connectivity to other networks that offer some services to the end node.

[5.2.](#) Protocol Stacks

With so many IP mobility management protocols, all potentially solving slightly different problems, it is interesting to see how these fit together in the stack. The following figure shows the stack diagram for the protocols discussed in this document.



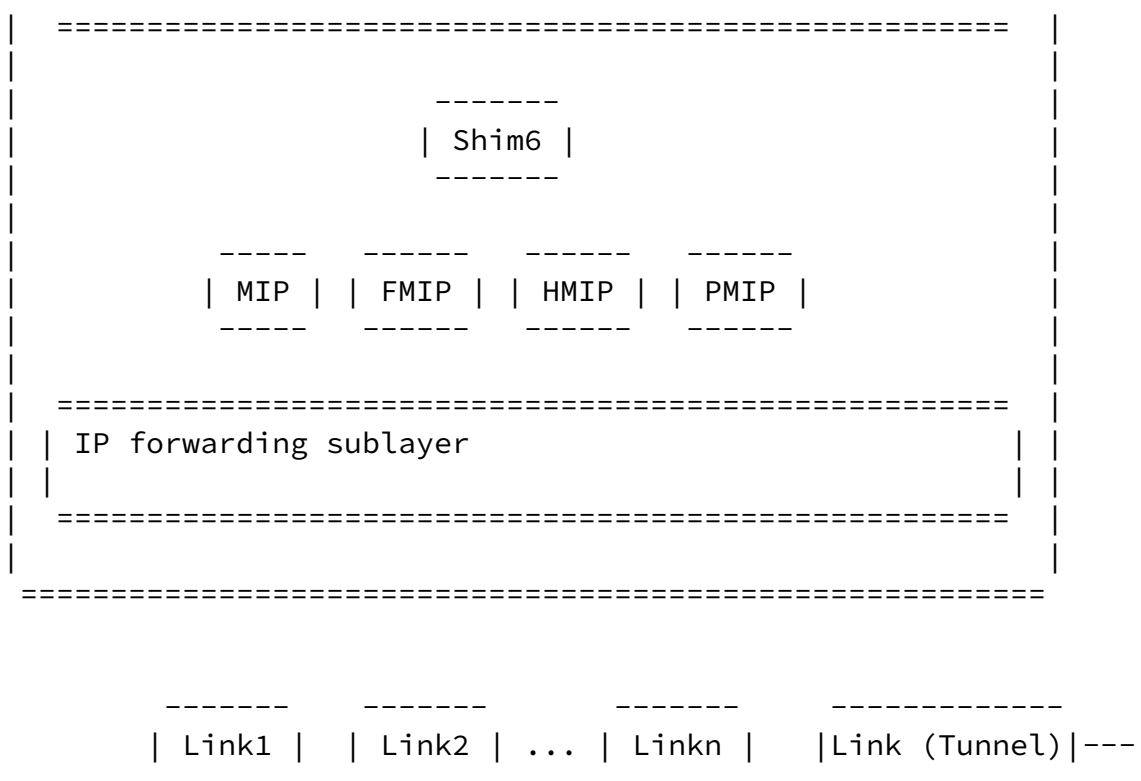


Figure 3: Stack Diagram

Figure 3 above shows a stack diagram of how the various IP mobility and multihoming components fit in a stack with respect to some other layers. A node may have various link layers as indicated. The IP layer is indicated in three parts. One is the IP forwarding sublayer that sits right above the link layer. In many of these protocols, there may be IP-in-IP tunneling. This is indicated in the figure by "Link (Tunnel)" - this layer would essentially wrap around the IP layer as a loopback, as shown. Typically, IP addressing is done on a per-link basis. Any virtual interfaces/links are assumed to still be a separate link. The Shim6 layer has two possible locations in the stack - it may be above or below the "Mobile IP family" of protocols. Since the Mobile IP family of protocols (MIP, FMIP, HMIP, PMIP) involve mapping between two IP addresses, Shim6 can be invoked as a multi-homing solution for either of those addresses. More about this interaction will be described in [Section 6.1.3](#) below.

The figure shows MIP generically at the IP layer and MIP4

specifically over the transport layer. MIP4 signaling runs over UDP, while the MIP4 data tunnel is an IP-in-IP tunnel. For sake of completeness, the figure shows MIP4 signaling also over UDP, for the signaling portion.

The IPsec components (AH and ESP) may either be part of the tunnel (shown as a link) or the actual IP layer above the MIP family of protocols when IP-in-IP encapsulation (with reverse tunneling) is used for the MIP data path. This depends on which address is used for IPsec purposes. However, it should be noted that MIP6 is operated with Route Optimization, the IPsec components are always above the MIP components in the header. IKEv2 (and by definition, MOBIKE) run over UDP. IKEv2/MOBIKE is the signaling mechanism that ultimately affects the IPsec tunnel endpoints - hence, as in the case of MIP4, it is only the signaling that is layered over a transport protocol.

AH and ESP may also be used in transport or tunnel mode and hence may be part of the tunnel or the regular IP layer. All of the elements shown are optional elements and the existence of any of this depends on the protocols used in the system.

[6.](#) Protocol Interactions, Usage Models and Architectural Implications

[6.1.](#) Multi-Level Node-based Mobility and Multihoming

This section is intended to discuss the various viable combinations of node-based mobility and multihoming protocols and also point out

any problematic combinations. This is a work in progress and is expected to be more detailed in later versions.

[6.1.1.](#) MIP, HMIP, and FMIP

Depending on the mobility needs of a system, one or more of these protocols may be deployed. Typically, this is a two level mobility management mechanism, with additional edge mobility. However, multiple modes of combining FMIP and HMIP are also feasible. A few different modes of using these protocols together is explained below. It should be noted that it is feasible to run any of these modes with just a subset of these three protocols. It should further be noted

that while this section focuses on the v6 versions of these protocols, similar combinations are also feasible with the v4 versions of the same – there may be additional modes of interest with MIP4, given the Foreign Agent mode of operation; however, that is left for further study. Alternatively, the same result can be obtained for both MIPv4 and MIPv6 using one version of MIP. This can be done using Dual Stack MIP v4 or v6 as presented in [10] and [11].

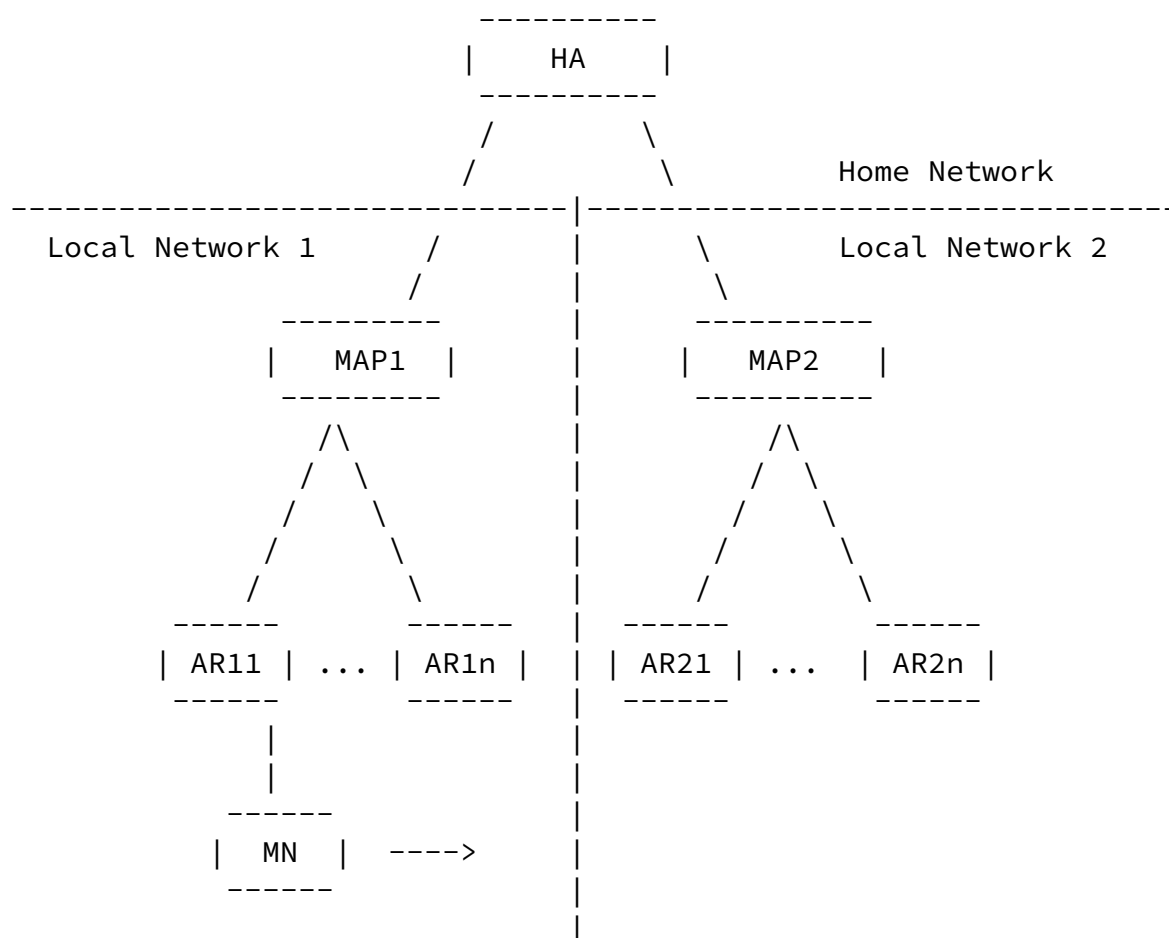


Figure 4: MIP, HMIP, and FMIP

Figure 4 shows an architecture with a MIP Home Agent, an HMIP MAP and Access Routers that perform FMIP operation. Upon first entering the network, the mobile node obtains an IP address on the prefix served

by an Access Router. Using the MAP advertised by the Access Router, the mobile node may perform an HMIP registration, using that IP address as its Local Care-of-Address (LCoA) and an IP address obtained in the MAP's prefix as its Regional Care-of-Address (RCoA). The mobile node may further obtain a Home Address from the Home Agent and use that for mobility across MAPs. In this case, the HMIP RCoA is registered as the MIP6 Care-of-Address of the mobile node. In the presence of a Home Address, the mobile node would typically use this address for application connectivity. However, there may be certain other considerations in choosing the right address for communication. More on that in [Section 6.1.1.3](#).

The combination of HMIP and FMIP may also be done in a few different ways. When the mobile node moves from one Access Router to another, it may use FMIP for faster handoffs. FMIP may be used within a MAP or across MAPs between Access Routers. It is also feasible to use FMIP on the previous MAP, when the mobile node moves across MAP boundaries. This would often be more efficient in such border cases than setting up the FMIP session between the Access Routers. In a tree topology, it may always be more efficient to allow the MAP to perform FMIP services. In these cases, the "PAR (Previous Access Router)" functionality of FMIP is performed by the MAP. When the mobile node moves across Access Routers within a MAP, the FMIP tunnel is set up with the previous and new LCoAs as the FMIP PCoA and NCoA respectively. When the mobile node moves across MAPs and uses FMIP on the MAP, the previous and new RCoAs are treated as the FMIP PCoA and NCoA respectively.

The FMIP tunnel is viewed as a temporary, short-lived tunnel used to help mobile nodes receive packets while waiting for the HMIP or MIP registration to complete. When FMIP is not in use, such a two-level mobility management mechanism leads to two IP tunnels on every data packet. For the period where FMIP is also in use, every packet is tunneled thrice. For a packet sent from the mobile node, this tunneling results in something as shown in Figure 5. The figure shows source and destination addresses of each IP header present in the packet. The original packet is sourced using the Home Address to a correspondent node. This is first encapsulated in the Mobile IP tunnel, followed by the HMIP tunnel and finally followed by the FMIP tunnel. For a packet received by the mobile node from a CN, the tunneling is similar in the reverse direction.

+-----+	+-----+	+-----+	+-----+	+-----+
S=NCoA	S=LCoA(=PCoA)	S=CoA(=RCoA)	S=HoA	Payload
D=PAR	D=MAP	D=HA	D=CN	
+-----+	+-----+	+-----+	+-----+	+-----+

Figure 5: Packet Tunneling with MIP, HMIP, and FMIP

A simple superimposition of all protocols (i.e. when the three protocols are in use) would lead the mobile node to perform signaling for FMIP and HMIP upon handoff within a given local network and for FMIP, HMIP and MIP upon handoff across local networks. However, there are other modes of integration that would not result in such inefficiency. For instance, HMIP and FMIP can be combined such that binding updates are only sent to the MAP, while FMIP is used to anticipate the movement of the mobile node. This would eliminate the tunnel between the old and new AR.

[6.1.1.1](#). Security Implications

In this model, the mobile node is responsible for all of the signaling. Each protocol requires a specific security association that is tied with the address for which the binding needs to be created. This ensures that the mobile node cannot redirect traffic meant for some other node. When all the three protocols are in use, this implies that the mobile node may share a Security Association with the PAR tied to the PCoA, which is also the HMIP LCoA, a Security Association with the MAP tied to the RCoA (which is also the MIP Care-of-Address), and a Security Association with the Home Agent tied to the Home Address. Depending on the choice of security protocol used by each of these mobility management protocols, these security associations may be IPsec security associations or something else. However, as mentioned above the security association between the MN and any AR can be eliminated in this configuration.

[6.1.1.2](#). Multihoming Implications

The mobile node may be attached to multiple Access Routers, thereby having multiple LCoAs. The mobile node may register multiple LCoAs with the MAP in that case. Further, the mobile node may actually be attached to multiple MAPs (if there are overlapping MAP regions as described in [Section 6.1.1.3](#)), in which case, it possesses multiple RCoAs. The mobile node may then use MIP to register multiple Care-of-Addresses (each RCoA would be registered as a MIP Care-of-Address) with the Home Agent.

Multihoming with connectivity to multiple Home Agents is discussed in [Section 6.1.3](#).

[6.1.1.3](#). Other Analysis

It is important to look at system requirements before determining whether all the protocols are needed. For many practical needs of mobile nodes, it is possible that only a subset of these protocols are needed. For instance, both FMIP and HMIP address the latency involved in MIP registrations - FMIP allows reception of packets at new location before the registration with the Home Agent completes. HMIP ensures that the MIP registrations need not be that frequent - hence, the latency really comes into play only upon crossing MAP boundaries. If something like FMIP is needed for fast handoff purposes anyway, HMIP may not be needed as an intermediate level of mobility management. Depending on the location of the MAP and the kind of interconnectivity that is present between the Access Routers, it may also be the case that the latency involved in HMIP registrations and FMIP tunnel setup are comparable. In such cases, it may be feasible to avoid the use of FMIP in the system.

The use of HMIP permits a not-so-transient local address (RCoA) that can be used for communication. When there is no need for a really long-lived IP address, it may not be necessary to have a global mobility management mechanism. This basically allows the data path latency to be lower, since the MAP is meant to be geographically closer to the mobile node. When Route Optimization is used for MIP, this data path latency is not an issue. However, even when Route Optimization is used, HMIP is useful to ensure that frequent registrations with the correspondent node are not needed. Registrations with the correspondent node will need to be modified only upon handoff to a new MAP. In reality, the local network regions managed by MAPs is likely to be overlapping, in which case, make-before-break HMIP transitions can be made. This is especially feasible with HMIP, since there is no requirement on trust relationships between the Access Routers and the MAP. Once the mobile node possesses a security association with the MAP, it can register any LCoA with it. The overlapping MAP boundaries may be indicative of a geographically closer MAP, implying a MAP transition for more optimal communication. Such an overlap provides the mobile node the opportunity to bootstrap the HMIP session with the new MAP before switching the data path to it. However, this places a requirement on the mobile node to be able to handle multiple HMIP sessions simultaneously for a short period of time. It must be noted that an overlap is harder for inter-administrative domains, since

even though there is no trust relationship requirement between the Access Routers and the MAPs, the Access Routers are required to advertise the presence of the MAPs to the mobile nodes.

When the three protocols are all used, the mobile node has several IP addresses to choose from for communication purposes. For really

long-lived connections, it is always better to use the most permanent IP address - this would be the Home Address of the mobile node. However, the mobile node may be running some latency sensitive applications that are not necessarily long-lived. Voice over IP is one such application. In those cases, tunneling all the data packets through the Home Agent may introduce unacceptable latency for the application. When Route Optimization is used, it is feasible to avoid such tunneling - however, route optimization support may not be available and it may also be considered expensive in some cases. For such cases, it would be an option to use the HMIP RCoA as the IP address for applications. Especially in situations of overlapping HMIP coverage as discussed above, the transition from one HMIP RCoA to another may be made seamlessly via SIP Re-Invite messages for the purposes of applications such as VoIP. Such a transition would be needed when the application persists while the mobile node is moving across MAP boundaries. It is also feasible to continue keeping the association with the old MAP until the end of the application, if it was going to only be short-lived.

[6.1.2.](#) MIP and MOBIKE

One method of combining MIP and MOBIKE is described for MIP4 in [\[12\]](#). In that model, MIP is used for mobility inside a given secure network, while MOBIKE with a VPN gateway is used for mobility outside the secure network. The general goal there is to allow enterprise mobile devices to keep the same IP address while roaming in and out of the enterprise network. There are other possible combinations as well.

There is the question of the usefulness of MOBIKE when MIP6 is employed. MIP6 inherently provides a means of updating the IKE endpoint IP address when the mobile node registers a new Care-of-Address for itself. This functionality is supported by indicating the need for dynamic key management in the MIP6 binding update sent by the mobile node with a new Care-of-Address. This is functionality

that would be duplicated by MOBIKE if both protocols were to be used in conjunction. By using a MIP6 Home Agent as also a VPN gateway, it is then feasible to just use MIP6 for mobility and still provide protected access. However, in addition to allowing changes to the local IP address of the initiator (typically the MIP6 mobile node), MOBIKE also allows the responder (typically the MIP6 Home Agent) to be multihomed and change the IP address used in a security association – this is not functionality supported by MIP6. Hence, depending on the requirements, it may make sense to run MIP6 and MOBIKE together or not in a given system.

Further, if the goal is to provide support for mobile devices roaming in and out of enterprise networks, it is likely that both protocols

are needed, unless detection of protected vs. unprotected network can happen through other means. This is due to the fact that in the MIP6-only mode, the Home Agent is made reachable from inside and outside the protected network. Hence, if the policy to use IPsec for data traffic only applies when the client is outside the protected network, the client must be able to securely determine whether it is attached to the protected network or not. If not, an impersonating element in the access network will successfully cause the mobile node to send sensitive data without any protection. In the model described in [12], the Home Agent is not reachable from an external network and hence, that provides a rather secure means of ensuring that unprotected data exchange does not occur while the MN is attached to an untrusted network.

Future revisions of this document will address this kind of combination in greater detail.

[6.1.2.1](#). Security Implications

As in the case of multi-level node-based IP mobility management, this mechanism also requires the mobile node to possess appropriate security associations with the Home Agent and the VPN gateway performing MOBIKE. The security association for MIP must be tied to the home address, while the IPsec selectors for the security association created or modified using MOBIKE will depend on the type of protection that is intended using that SA.

Additionally, the security of the internal IP addressing semantics of

a protected network may be important to consider while designing a solution that requires both VPNs and mobility support. For example, the VPN gateway, in many networks, is the only reachable device from an unprotected network. If a MIP6 Home Agent was made reachable from an external network, it may be exposed to additional threats than the case where the Home Agent is "behind" the VPN gateway and only accessible from the protected network. Also, another consideration while deciding to choose between a MIP6-only with data protection and a combined MIP6-MOBIKE solution with separate VPN gateway and Home Agent, is ensuring the ability to securely detect the connectivity to an untrusted network to avoid sending unprotected sensitive data over the untrusted network. An alternative would be to always require that data be sent in a protected manner, irrespective of the location of the mobile node. However, that adds a lot of load on the Home Agent/VPN Gateway device to process a lot more protected traffic and is often unnecessary.

[6.1.3.](#) MIP and SHIM6

As described in [Section 3](#), MIP and SHIM6 can either be deployed in a complementary or competing fashion. The mobile node may be multi-addressed in the local networks by virtue of either the local network being multi-homed or attaching to multiple local networks. In such cases, if MIP is employed to handle mobility, it is easier for the local multi-addressing to be handled as part of mobility. In other words, the mobile node may register multiple Care-of-Addresses tied to the same Home Address with the HA. The mobile node may then use any Care-of-Address to send or receive data.

However, when the mobile node is multi-addressed with IP addresses from multiple home networks, even if MIP is used in each home network, it only ties each Home Address with one or more of the Care-of-Addresses that the mobile node possesses. So, while multiple Home Addresses can each be bound to multiple (same or different) Care-of-Addresses, MIP does not facilitate tying the Home Addresses itself together. This is due to the fact that MIP requires a central entity (Home Agent) for address mappings and each such entity can only handle IP addresses belonging to it. SHIM6 is a potential solution

to handle such multihoming. Using SHIM6, both Home Addresses can be tied together by providing a common ULID to a correspondent node. Hence, the correspondent nodes may reach the mobile node via either Home Addresses, and this helps to ensure reachability even when one of the home networks is down. Some of this concept is covered in [13]. Future revisions of this document will provide more details.

[6.1.4.](#) MIP and HIP

TBD

[6.1.5.](#) SHIM6 and MOBIKE

TBD

[6.1.6.](#) SHIM6 and HIP

TBD

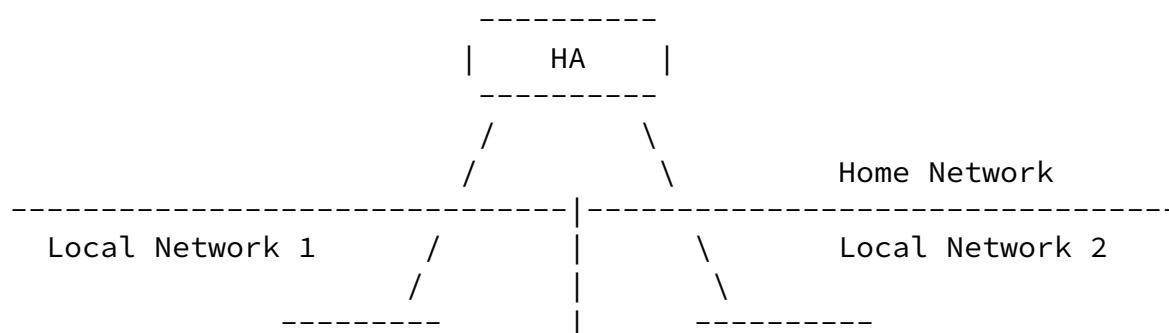
[6.1.7.](#) HIP and MOBIKE

TBD

[6.1.8.](#) MIP, SHIM6 and HIP

TBD

[6.2.](#) Node-based and Network-based Mobility



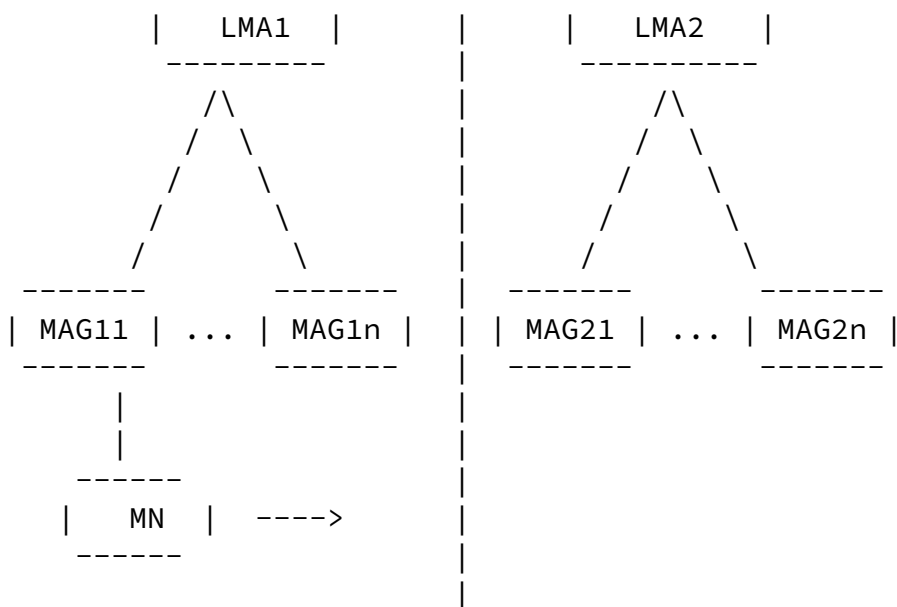


Figure 6: MIP and NETLMM

This section describes how node-based global mobility and network-based local mobility can co-exist in an architecture. Figure 6 shows an architecture that has a MIP Home Agent as part of the home network and network-based mobility entities, LMA and MAG in the local network. Network-based mobility discussions in this section apply equally to solutions described in [14], [15], and [16]. The term NetLMM is used to refer to any of these solutions in a generic manner.

Figure 6 shows the architectural entities involved in the two protocols. While this is architecturally similar to the MIP/HMIP overlay described in [Section 6.1.1](#), there are some significant

differences arising due to the fact that the local mobility here happens without mobile node involvement.

Conceptually, there are similarities between this model and the MIP/HMIP overlay model. The MAP and LMA are equivalent in function and scope – the LMA keeps track of the mobility of the mobile node within the local network. However, an important difference is that local

mobility is achieved here by preserving the same local address for the mobile node within the local network, as described in [Section 4.2](#). The mobile node may register such a local address anchored at the LMA as its Care-of-Address with the Home Agent - MIP updates are then only necessary when the mobile node associates with a new LMA.

As in the case of the MIP/HMIP overlay, it is feasible to have one of the local networks as the Mobile IP home network of the mobile node. In such a case, the LMA and Home Agent for a given mobile node would be collocated in that local network and the mobile node would be "home" from a MIP perspective while attached to that network. MIP operation is then only needed when the mobile node is not attached to that network. However, this model has some security implications that are worth noting and those are captured in [Section 6.2.1](#). In addition to the security implications, this model may also lead to some race conditions which are analyzed in [Section 6.2.4](#).

As the mobile node moves within a local network, its current location will be updated at the LMA by the appropriate MAG. A separate protocol between the mobile node and the MAG may be employed to detect the attachment of an mobile node to a MAG. Alternately, some technologies may allow mobile node movement detection at the network and trigger a context transfer between MAGs to provide the necessary information to complete the new location registration.

[6.2.1](#). Security Implications

The node-based mobility here is handled by the mobile node and Home Agent and the network-based mobility is handled by the MAG and LMA. The mobile node needs to possess a security association with the Home Agent tied to its Home Address for MIP operation, as is normally the case. For the NetLMM operation, there must be a Security Association between the MAG and the LMA. This security association provides the needed data origin authentication. However, it does not guarantee the attachment of the mobile node with that particular MAG. Without mobile node involvement or some authorization checks involving an entity such as a AAA server, it is not feasible to provide any guarantees about the actual presence of the mobile node at that MAG. Hence, a malfunctioning or compromised MAG would be able to redirect traffic meant for that mobile node by creating an incorrect binding

at the LMA. However, such a threat can be limited in scope by ensuring that a MAG is only capable of updating bindings for addresses that are valid in that local domain. This requires appropriate prefix partitioning and verification of the address claimed by the LMA for the mobile node against the prefix it is authorized to serve. In such a case, the MAG would be unable to redirect traffic of an mobile node that is not within its local network.

An additional security implication is when one of the local networks is considered to be the MIP home network, making the local address acquired by the mobile node in that network its MIP Home Address. In this case, while the mobile node is within that domain, the security risks are analogous to what has been described so far. However, it is feasible for a MAG to redirect traffic belonging to a mobile node even when the mobile node is no longer in that local network. Even if the redirection is not successful in some cases, it is capable of leading to ambiguity in mobile node's current location at the LMA/Home Agent. This is due to the fact that the MAG and the mobile node are both authorized to perform updates corresponding to the same IP address. This would basically result in the security guarantees of MIP being affected by the use of NetLMM. Such a threat may be mitigated by requiring the LMA to reject any updates to the mobile node's local address (which is the same as the Home Address in this case) by a MAG when there is an existing binding for that address created by the mobile node. However, this leads to some undesirable inter-dependencies between the two protocols and also may lead to less than ideal mobility management, as described in [Section 6.2.4](#).

[6.2.2](#). Multihoming Implications

Unlike the HMIP case, multi-homing at the local networks level cannot be handled by the NetLMM class of solutions. For instance, the mobile node may be multihomed by virtue of attachment to two MAGs within the same LMA or under different LMAs. An IP node will obtain a distinct global IP address on each of its interfaces (physical or virtual) – hence, if the mobile node is attached to two MAGs at any given time, it will acquire separate IP addresses.

NetLMM provides mobility to each IP address and by itself, has no means of tying the multiple IP addresses to the same mobile node. Hence, mobility for these IP addresses will be handled independently by default. However, certain technologies may have the capability to identify (say, via L2 mapping) that a given set of IP addresses belong to the same mobile node. In such a case, it is feasible for this to be known at the LMA. However, even so, it is not feasible for these IP addresses to be associated with any per-packet identifier. Unlike the ULID in SHIM6 or RCoA in HMIP, NetLMM does

not have anything available for the mobile and correspondent nodes to use for communication.

Extracting from the above, in terms of data flow, these addresses are practically independent and the ability to correlate multiple IP addresses belonging to the same mobile node at the LMA is of little use. In other words, it is unlike the case where the correspondent nodes pick one IP address of the mobile node to get the data to the LMA, with multiple possible paths available to the mobile node from there. In this case, the correspondent node and the mobile node need to pick a particular mobile node address to correspond with. Note that when MIP is used, this correspondent node may actually be the Home Agent. Hence, when the mobile node has multiple IP addresses, the decision of picking an address to correspond with is still left to the application and not handled by NetLMM.

Extending this analysis to multihoming for mobile nodes with multi-radio capabilities, it is not even feasible for the network to provide any correlation between IP addresses of the mobile node, given that there is no common L2 identifier. With involvement on the mobile node's part, it may be feasible to obtain an access agnostic identity to correlate with the multiple IP addresses. However, that would be defeating one of the motivations of having network-based mobility transparent to the mobile node.

It is conceivable that the same global IP address is assigned to the mobile node for multiple interfaces - however, that requires a fundamental change to the functioning of regular IP nodes. Further, it also places restrictions on the simultaneous use of such multiple interfaces. It also requires intelligence below the IP layer to pick the correct interface for different packets sent with the same IP address, which would typically not be needed.

The above analysis leads to the following conclusions.

- o Without an out-of-band mechanism, it is not feasible for the MAG or LMA to correlate multiple IP addresses as belonging to the same mobile node.
- o Even with such correlation, there is no means of presenting a single IP address to applications with multiple paths over the network. Hence, applications are exposed to multiple IP addresses by default.

- o Providing the same global IP address to multiple interfaces would require undesirable changes to mobile nodes and places restrictions on simultaneous use of the interfaces.

By this analysis, it appears that network-based mobility management is not well-suited to handle any kind of multi-homing of a mobile node. The mobile node is in the best position to determine the availability and connection capabilities of its various interfaces and hence, multi-addressing and multi-homing is best handled using node-based mobility management.

[6.2.3.](#) Network-based mobility for non-MIP nodes

We have analyzed the co-existence of node and network-based mobility for a given mobile node for two-level mobility management thus far. The other model is where network-based mobility is only intended for nodes that are incapable of mobility management on their own, such as legacy mobile devices. In that case, a given network must support network-based mobility for such devices and let other mobile nodes handle their own mobility. In the NetLMM class of solutions, the entire local network is made to appear as having the same IP prefix - this is achieved by advertising the same prefix to the mobile node as it moves within the local network. By virtue of such a protocol, it is not feasible to differentiate between MIP-capable and non-MIP-capable endpoints using functionality provided in the protocol itself. Such detection is only feasible via some out-of-band mechanism. In some systems, it may be feasible for the network to know the capabilities of the nodes that attach to it. If the network is aware of the capabilities, it would be feasible to present an unchanging IP address or prefix throughout the local network only to devices that need network-based mobility.

[6.2.4.](#) Other Analysis

This section provides additional analysis on the scenario where network-based local mobility is used on the mobile node's home network to make the entire local network appear to the mobile node as its Mobile IP home network. [Section 6.2.1](#) describes the security implications of the model and shows that it is essential to ensure that a network-based mobility binding for the mobile node's Home

Address is only accepted when there is no current binding for that address created by the mobile node itself. That will ensure that the MIP security guarantees are still available to the mobile node. However, that may lead to a less than ideal mobility solution for the mobile node. It is possible that a registration from the network node arrives at the entity serving as the LMA/Home Agent before the mobile node has a chance to de-register with the Home Agent. In that case, such a registration will be rejected until the mobile node is successfully de-registered from a MIP perspective and its binding is removed at the Home Agent. This may result in undesirable handoff latency for the mobile node, when the mobile node is moving in and out of its home network.

This further introduces the need for some inter-dependency between the node and network-based mobility protocols. Specifically, the NetLMM solution must be able to detect the presence of a MIP binding for a given IP address before accepting a certain registration for an mobile node. When the NetLMM solution used is PMIP, this may be less painful - nevertheless, it is still undesirable behavior.

Overall, systems evaluating such an approach must take such shortcomings into account before using it. The use of this approach allows data exchange in this extended home network without additional tunnel overhead (as MIP6 would have) between the mobile node and the Access Router. It is important to evaluate the need for this, along with the other solutions such as header compression (say, RoHC) that may be deployed in the system. RoHC, for instance handles two IP headers as easily as it does one - hence, if RoHC is needed anyway, the tradeoffs of using this approach may not be worth it.

[7.](#) Security Considerations

For security considerations on the protocols described in this document, please refer to the appropriate protocol documents. For the architectural combinations described here, security implications have been discussed in the corresponding sections. Future revisions of this document will have a more comprehensive security analysis.

[8.](#) IANA Considerations

This document has no actions for IANA.

9. References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Soliman, H., "Flow Bindings in Mobile IPv6 and Nemo Basic Support", [draft-soliman-monami6-flow-binding-04](#) (work in progress), March 2007.
- [3] Perkins, C., "IP Mobility Support for IPv4", [RFC 3344](#), August 2002.
- [4] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", [RFC 4140](#), August 2005.

Narayanan, et al.

Expires January 6, 2008

[Page 33]

Internet-Draft IP Mobility and Multi-homing Interactions

July 2007

- [5] Fogelstroem, E., Jonsson, A., and C. Perkins, "Mobile IPv4 Regional Registration", [RFC 4857](#), June 2007.
- [6] El Malki, K., "Low-Latency Handoffs in Mobile IPv4", [RFC 4881](#), June 2007.
- [7] Henderson, T., "End-Host Mobility and Multihoming with the Host Identity Protocol", [draft-ietf-hip-mm-05](#) (work in progress), March 2007.
- [8] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", [draft-ietf-hip-rvs-05](#) (work in progress), June 2006.
- [9] Thaler, D., "Multilink Subnet Issues", [draft-iab-multilink-subnet-issues-03](#) (work in progress), January 2007.
- [10] Tsirtsis, G., "Dual Stack Mobile IPv4", [draft-ietf-mip4-dsmipv4-02](#) (work in progress), May 2007.
- [11] Soliman, H., "Mobile IPv6 support for dual stack Hosts and

- Routers (DSMIPv6)", [draft-ietf-mip6-nemo-v4traversal-04](#) (work in progress), March 2007.
- [12] Devarapalli, V. and P. Eronen, "Secure Connectivity and Mobility using Mobile IPv4 and MOBIKE", [draft-ietf-mip4-mobike-connectivity-03](#) (work in progress), March 2007.
 - [13] Bagnulo, M. and J. Abley, "Applicability Statement for the Level 3 Multihoming Shim Protocol (Shim6)", [draft-ietf-shim6-applicability-02](#) (work in progress), October 2006.
 - [14] Gundavelli, S., "Proxy Mobile IPv6", [draft-sgundave-mip6-proxymip6-02](#) (work in progress), March 2007.
 - [15] Bedekar, A., "A Protocol for Network-based Localized Mobility Management", [draft-singh-netlmm-protocol-02](#) (work in progress), March 2007.
 - [16] Giaretta, G., "The NetLMM Protocol", [draft-giaretta-netlmm-dt-protocol-02](#) (work in progress), October 2006.
 - [17] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in

- IPv6", [RFC 3775](#), June 2004.
- [18] Koodli, R., "Fast Handovers for Mobile IPv6", [RFC 4068](#), July 2005.
 - [19] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", [RFC 4555](#), June 2006.
 - [20] Bagnulo, M. and E. Nordmark, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", [draft-ietf-shim6-proto-08](#) (work in progress), April 2007.
 - [21] Koodli, R. and C. Perkins, "Mobile IPv4 Fast Handovers", [draft-ietf-mip4-fmipv4-07](#) (work in progress), May 2007.

- [22] Kempf, J., "Problem Statement for Network-based Localized Mobility Management", [draft-ietf-netlmm-nohost-ps-05](#) (work in progress), September 2006.
- [23] Wakikawa, R., "Multiple Care-of Addresses Registration", [draft-ietf-monami6-multiplecoa-02](#) (work in progress), March 2007.

Authors' Addresses

Vidya Narayanan
Qualcomm, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Email: vidyan@qualcomm.com

Dave Thaler
Microsoft
One Microsoft Way
Redmond, WA
USA

Email: dthaler@microsoft.com

Marcelo Bagnulo
Huawei Lab at UC3M

Email: marcelo@it.uc3m.es

Hesham Soliman
Elevate Technologies

Email: Hesham@elevatemobile.com

Narayanan, et al. Expires January 6, 2008 [Page 36]

Internet-Draft IP Mobility and Multi-homing Interactions July 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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