B.Sc. in Computer Science and Engineering Thesis

Study Of Proxy Mobile IPv6

Submitted by

Lt Sharmin Afroze
201014020

Nusrat Sharmin
201014022

Sazzadur Rahman
200814050

Supervised by

Dr. Md. Shohrab Hossain
Assistant Professor
Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology

Department of Computer Science and Engineering
Military Institute of Science and Technology

CERTIFICATION

This thesis paper titled **"Study of Proxy Mobile IPv6 "**, submitted by the group as mentioned below has been accepted as satisfactory in partial fulfillment of the requirements for the degree B.Sc. in Computer Science and Engineering on December 2013.

Group Members:

Lt Sharmin Afroze
Nusrat Sharmin
Sazzadur Rahman

Supervisor:

———————————-

Dr. Md. Shohrab Hossain
Assistant Professor
Dept of CSE
BUET

CANDIDATE'S DECLARATION

This is to certify that the work presented in this thesis paper is the outcome of the investigation and research carried out by the following students under the supervision of Dr. Md. Shohrab Hossain, Assistant Professor, Dept of CSE, BUET, Dhaka, Bangladesh.

It is also declared that neither this thesis paper nor any part thereof has been submitted anywhere else for the award of any degree, diploma or other qualifications.

———————————-

Lt Sharmin Afroze
201014020

———————————-

Nusrat Sharmin
201014022

———————————-

Sazzadur Rahman
200814050

ACKNOWLEDGEMENT

We are thankful to Almighty Allah for his blessings for the successful completion of our thesis. Our heartiest gratitude, profound indebtedness and deep respect go to our supervisor Dr. Md. Shohrab Hossain, Assistant Professor,Dept of CSE, BUET, Dhaka, Bangladesh, for his constant supervision, affectionate guidance and great encouragement and motivation. His keen interest on the topic and valuable advices throughout the study was of great help in completing thesis.

We are especially grateful to the Department of Computer Science and Engineering (CSE) of Military Institute of Science and Technology (MIST) for providing their all out support during the thesis work.

Finally, we would like to thank our families and our course mates for their appreciable assistance, patience and suggestions during the course of our thesis.

Dhaka
December 2013
.

Lt Sharmin Afroze
Nusrat Sharmin
Sazzadur Rahman

ABSTRACT

A network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) is being actively standardized by the IETF NETLMM working group, and is starting to attract considerable attention among the telecommunication and Internet communities. Unlike the various existing protocols for IP mobility management such as Mobile IPv6 (MIPv6), which are host-based approaches, a network-based approach, PMIPv6 has salient features such as support for unmodified mobile nodes, support for both IPv4 and IPv6, efficient use of wireless link and improved handover performance. In this thesis, we have explained the architecture of PMIPv6 with its detailed signaling diagram. We have compared PMIPv6 with MIPv6 in term of some characteristics and performance aspects and identified some drawbacks of PMIPv6. We have also presented handover latency calculation of MIPv6, HMIPv6 and PMIPv6 based on an analytical model. The results show that PMIPv6 has superior performance to other two protocols(MIPv6 and HMIPv6).

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

ICMPv6	:	Internet Control Message Protocol for IPv6
IPMN	:	Interactive Protocol for Mobile Networking
NETLMM	:	Network-based Localized Mobile Management
IETF	:	Internet Engineering Task Force
AP	:	Access Point
CN	:	Correspondent Node
DAD	:	Duplicate Address Detection
DHCP	:	Dynamic Host Configuration Protocol
IP	:	Internet Protocol
L2	:	Layer 2
LMA	:	Local Mobility Anchor
MAG	:	Mobility Access Gateway
MAP	:	Mobile Access Point
MIPv6	:	Mobile IPv6
MN	:	Mobile Node
NMAG	:	New MAG
PBA	:	Proxy Binding Acknowledgement
PBU	:	Proxy Binding Update
PMAG	:	Previous MAG
RA	:	Router Advertisement
FMIPv6	:	Fast Handover for Mobile IPv6
HACK	:	Handover Acknowledgement
HI	:	Handover Initiate
HMIPv6	:	Hierarchal Mobile IPv6

CHAPTER 1
INTRODUCTION

Technology is progressing in our day to day life. Life has become easier because communication system has developed rapidly for the last few decades. Now-a-days mobile based communication has increased rapidly. Network is one of the major and vital part in mobile based communication. With the rapid growth in the number of mobile subscribers and mobile devices such as cellular phones, personal digital assistants (PDAs), and laptop computers, high-speed Internet access is becoming a primary concern in our lives. Recent advances in various wireless access technologies such as IEEE 802.16d/e and wideband code-division multiple access (WCDMA) and the incessant efforts of several standards bodies such as the Internet Engineering Task Force (IETF), Third Generation Partnership Project (3GPP), and International Telecommunication Union Telecommunication Standardization Sector (ITU-T) appear to increase the possibility of realizing mobile and ubiquitous computing environments. However, many challenges still remain to be solved for achieving such a goal.

The recent fundamental networking trend has focused mostly on realizing all-IP mobile networks. All-IP mobile networks, which are expected to combine the Internet and telecommunication networks tightly together, are networks in which IP is employed from a mobile subscriber to the access points (APs) that connect the wireless networks to the Internet. One of the most important and challenging issues for next-generation all-IP mobile networks is mobility management. Mobility management enables the serving networks to locate a mobile subscribers point of attachment for delivering data packets (i.e., location management) and maintain a mobile subscribers connection as it continues to change its point of attachment (i.e., handover management).

1.1 Problem statement

Mobile IPv6 (MIPv6)[1], which is a host-based mobility management protocol, is one of the most representative efforts and proposed by the IETF as the main protocol for mobility management at the IP layer. However, although MIPv6 is a well-known mature standard for IPv6 mobility, it has some well known problems such as handover latency, packet loss and signaling overhead. Also, the MIPv6 requires protocol stack modification of the Mobile Node (MN) to support IP mobility[2].

A network-based mobility management protocol, which is called the Proxy Mobile IPv6 (PMIPv6), is standardized by the IETF NetLMM WG [3]. Unlike the MIPv6, PMIP6 allows the serving network to control the mobility management on behalf of an MN, thereby eliminating the MN from any mobility-related signaling. PMIPv6 is essentially based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as functionality of Home Agent (HA). However, PMIPv6 is also designed to provide network-based mobility management support to an MN in a topologically localized domain. Therefore, an MN is exempt from participation in any mobility-related signaling, and a proxy mobility agent in the serving network performs mobility-related signaling on behalf of the MN. However, a network-based mobility management protocols, such as PMIPv6, still suffer from handover latency and packet loss during a handover, like MIPv6.

1.2 Objectives and Contributions

The main aim of IP is to continue the mobile communication without any interruption even when the network changes in this environment. PMIPv6 is a protocol which has started to attract considerable attention among the telecommunication and Internet communities.

Unlike the various existing protocols for IP mobility management such as MIPv6, which are host-based approaches, a network-based approach such as PMIPv6 has salient features such as support for unmodified mobile nodes, support for both IPv4 and IPv6, efficient use of wireless link and improved handover performance.

PMIPv6 is expected to expedite the real deployment of IP mobility management. We have done our thesis to analyze PMIPv6. In addition, this thesis provides a comprehensive comparison and summary that addresses the strong and weak points of PMIPv6 against various existing well-known mobilility support protocols such as MIPv6, HMIPv6. And we also discuss about predictive and reactive handover of PMIPv6 and handover analysis between MIPv6, HMIPv6 and PMIPv6.

This thesis is organized as follows. Chapter 2 provides a literature review of some of the related work - MIPv4, MIPv6 and PMIPv6. In Chapter 3, we present the operation, signaling flow of PMIPv6. Chapter 4 provides the comparison between MIPv6 and PMIPv6. We discuss about the handover of PMIPv6 in chapter 5. Finally, we conclude the thesis and discuss possible future works in chapter 6.

CHAPTER 2
LITERATURE REVIEW

2.1 Mobile IP

IP mobility is one of the significant areas of research due to the increased development in the communication area and various technologies involved in the delivery of information from source to destination. Mobile networking refers to the user requirement of roaming while maintaining the ability of having a network communications preferably without service degradation or interruption.

Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile users to move from one network to another while maintaining a permanent IP address.

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. IP, as the primary protocol in the Internet layer of the Internet protocol suite, has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information. Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974; the other being the connection-oriented Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the internet. Its successor is Internet Protocol Version 6 (IPv6). The Internet Protocol is responsible for addressing hosts and for routing datagrams (packets) from a source host to a destination host across one or more IP networks. For this purpose, the Internet Protocol defines the format of packets and provides an addressing system that has two functions: identifying hosts and providing a logical location service. The Mobile IP protocol allows location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the tunnel.

2.1.1 Applications

In many applications (e.g, VPN, VoIP), sudden changes in network connectivity and IP address can cause problems such as interruption during communication, due to sudden changes in network connectivity can be broken, for this reason data can be lost. Mobile IP was designed to support seamless and continuous Internet connectivity. Mobile IP is most often found in wired and wireless environments where users need to carry their mobile devices across multiple LAN subnets. Examples of use are in roaming between overlapping wireless systems, e.g., IP over DVB, WLAN, WiMAX and BWA. Mobile IP is not required within cellular systems such as 3G, to provide transparency when Internet users migrate between cellular towers, since these systems provide their own data link layer handover and roaming mechanisms. However, it is often used in 3G systems to allow seamless IP mobility between different packet data serving node (PDSN) domains.

2.1.2 New Architectural Entities

Mobile IP introduces the following new functional entities:

- **Mobile Node** A host or router that changes its point of attachment from one network or subnetwork to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available.

- **Home Agent** A router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home, and maintains current location information for the mobile node.

- **Foreign Agent**

  A router on a mobile node's visited network which provides routing services to the mobile node while registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes. A mobile node is given a long-term IP address on a home network. This home address is administered in the same way as a *permanent* IP address is provided to a stationary host. When away from its home network, a *care-of address* is associated with the mobile node and reflects the mobile node's current point of attachment. The mobile node uses its home address as the source address of all IP datagrams that it sends, except where otherwise described in this document for datagrams sent for certain mobility management functions.

2.1.3 Terminology

This document frequently uses the following terms:

- **Agent Advertisement:** An advertisement message constructed by attaching a special Extension to a router advertisement message.

- **Care-of Address:** The termination point of a tunnel toward a mobile node, for datagrams forwarded to the mobile node while it is away from home. The protocol can use two different types of care-of address: a *foreign agent care-of address* is an address of a foreign agent with which the mobile node is registered, and a *co-located care-of address* is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

- **Correspondent Node:** A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

- **Foreign Network:** Any network other than the mobile node's Home Network.

- **Home Address:** An IP address that is assigned for an extended period of time to a mobile node. It remains unchanged regardless of where the node is attached to the Internet.

- **Home Network:** A network, possibly virtual, having a network prefix matching that of a mobile node's home address. Note that standard IP routing mechanisms will deliver datagrams destined to a mobile node's Home Address to the mobile node's Home Network.

- **Link :** A facility or medium over which nodes can communicate at the link layer. A link underlies the network layer.

- **Link-Layer Address:**The address used to identify an endpoint of some communication over a physical link. Typically, the Link-Layer address is an interface's Media Access Control (MAC) address.

- **Mobility Agent:** Either a home agent or a foreign agent. Mobility Binding The association of a home address with a care-of address, along with the remaining lifetime of that association.

- **Mobility Security Association:** A collection of security contexts, between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them. Each context indicates an authentication algorithm and mode a secret (a shared key, or appropriate public/private key pair), and a style of replay protection in.

- **Node:** A host or a router.

- **Tunnel :** The path followed by a datagram while it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination.

- **Virtual Network:** A network with no physical instantiation beyond a router (with a physical network interface on another network). The router (e.g., a home agent) generally advertises reachability to the virtual network using conventional routing protocols.

- **Visited Network:**A network other than a mobile node's Home Network, to which the mobile node is currently connected.
- **Visitor List:** The list of mobile nodes visiting a foreign agent.
- **UnicastAddresses:** A unicast address specifies that a packet be sent to a particular interface.
- **MulticastAddresses:** A multicast address is sent to a set of interfaces, typically encompassing multiple nodes.
- **Anycast Addresses:** An anycast address, while identifying multiple interfaces (and typically multiple nodes), is sent only to the interface that's determined to be *nearest* to the sender.

2.1.4 Protocol Overview

The following support services are defined for Mobile IP:

- **Agent Discovery** Home agents and foreign agents may advertise their availability on each link the link to learn if any prospective agents are present.
- **Registration** When the mobile node is away from home, it registers its care-of address with its home agent. Depending on its method of attachment, the mobile node will register either directly with its home agent, or through a foreign agent which forwards the registration to the home agent.

2.1.5 Operational Principles

The goal of IP Mobility is to maintain the TCP connection between a mobile host and a static host while reducing the effects of location changes while the mobile host is moving around, without having to change the underlying TCP/IP protocol. To solve the problem, the RFC allows for a kind of proxy agent to act as a middle-man between a mobile host and a correspondent host.

Two kinds of entities comprise a Mobile IP implementation:

- **Home agent (HA):** The HA stores information about mobile nodes whose permanent home address is in the home agent's network. The HA acts as a router on a MHs home network which tunnels datagrams for delivery to the MH when it is away from home, maintains a location directory (LD) for the MH.

- **Foreign agent (FA):** The FA stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP. If there is no foreign agent in the host network, the mobile device has to take care of getting an address and advertising that address by its own means. The FA acts as a router on a MNs visited network which provides routing services to the MN while registered. FA detunnels and delivers datagrams to the MH that were tunneled by the MNs HA.

  A mobile node has two addresses - *a permanent home address* and *a care-of address (CoA)*, which is associated with the network the mobile node is visiting.The so called Care of Address is a termination point of a tunnel toward a MN, for datagrams forwarded to the MN while it is away from home.

  Foreign agent care-of address: the address of a foreign agent that MH registers with

  Co-located care-of address: an externally obtained local address that a MH gets.

  MNs are responsible for discovering whether it is connected to its home network or has moved to a foreign network. HAs and FAs broadcast their presence on each network to which they are attached. They are not solely responsible for discovery, they only play a part. In [4], specified that MN use agent discovery to locate these entities. When connected to a foreign network, a MN has to determine the foreign agent care-of-address being offered by each foreign agent on the network.

  A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the remote address through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

When acting as transmitter, a mobile node sends packets directly to the other communicating node, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing or *route optimization* (RO) mode. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers check that the source IP address of the mobile host belongs to their subnet or discard the packet otherwise. In Mobile IPv6 (MIPv6), *reverse tunneling* is the default behaviour, with RO being an optional behavior.

2.1.6 Functionality in the Home Network

- The Home Agent (HA) sends agent advertisements, which are extended router advertisements sent with periodically with unicast, broadcast or multicast.

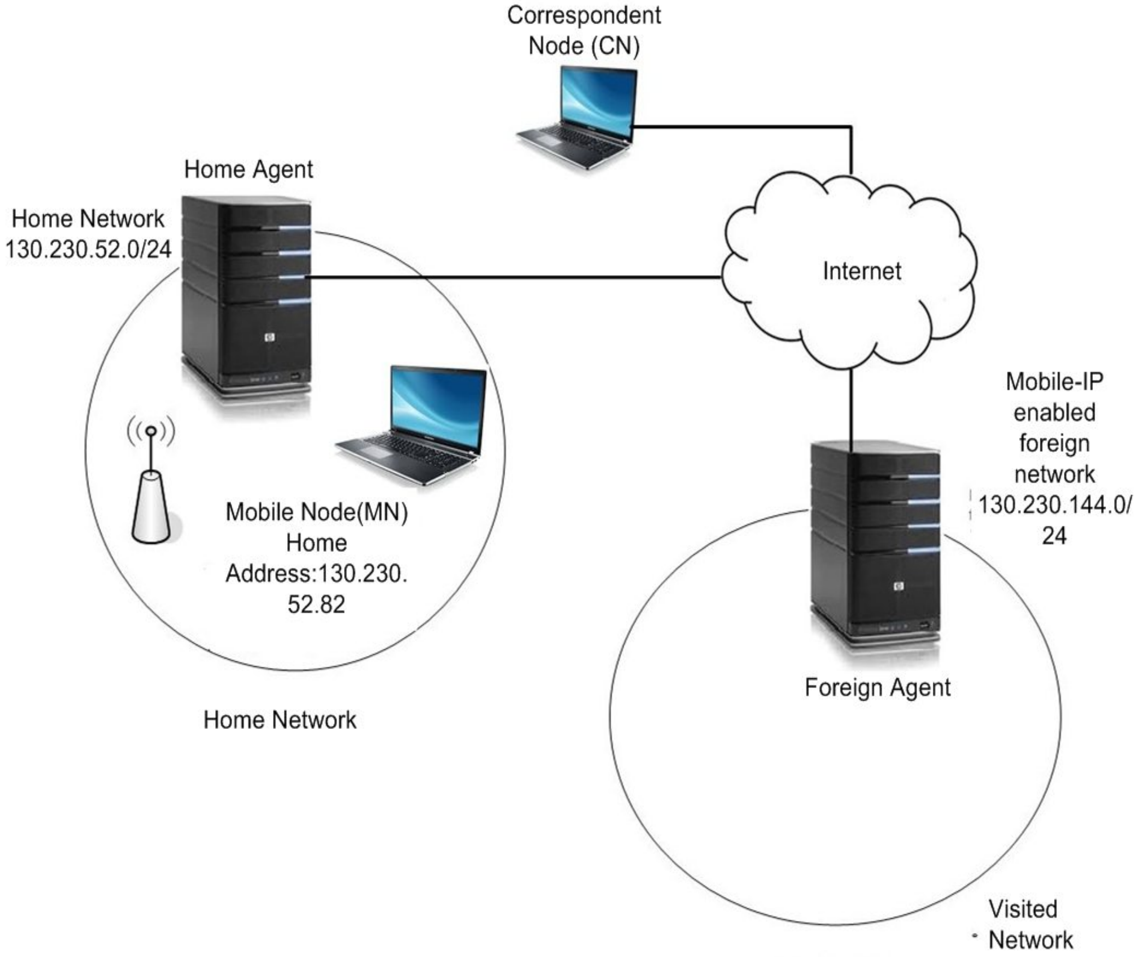

Correspondent Node (CN)
Home Agent
Home Network 130.230.52.0/24
Internet
Mobile-IP enabled foreign network 130.230.144.0/24
Mobile Node(MN) Home Address:130.230.52.82
Foreign Agent
Home Network
Visited Network

Figure 2.1: MN in Home Network

- The agent advertisement contains information such as:
  1. sequence number
  2. lifetime of the registration
  3. flags to indicate if the advertisement was sent by FA or HA
  4. supported IP encapsulations
  5. one or more care of addresses (CoA)
  6. the length of prefixes advertised in the standard part
- The Mobile Node (MN) listens the agent advertisements to determine if it is in its home network or in a foreign network.
- In the home network the MN cancels the home agent registration to ensure normal routing.
- In the Figure 2.1 MN has already started exchanging traffic (using its home address 130.230.52.82) with a correspondent node somewhere in Internet.

2.1.7 Moving to the Foreign Network

- MN leaves the home network, moving to foreign network and receiving a new IP address from the foreign network with DHCP.
- The traffic from Correspondent Node to Mobile Node's home address is still routed to the home network router but no further since no one admits having the MN's home address.
- MN can detect the change of network from various indicators like wireless signal strength, different IP network or FA agent advertisements, these indicators are however such that they vary from implementation to another
- When the MN itself detects the change of network, it sends a router ICMP router solicitation request which triggers the possibly existing Mobile IPv4 agent component (such as FA) to respond with a agent advertisement directed at MN.
- The detected agent advertisement trigger MN to start registration to the home agent (HA)

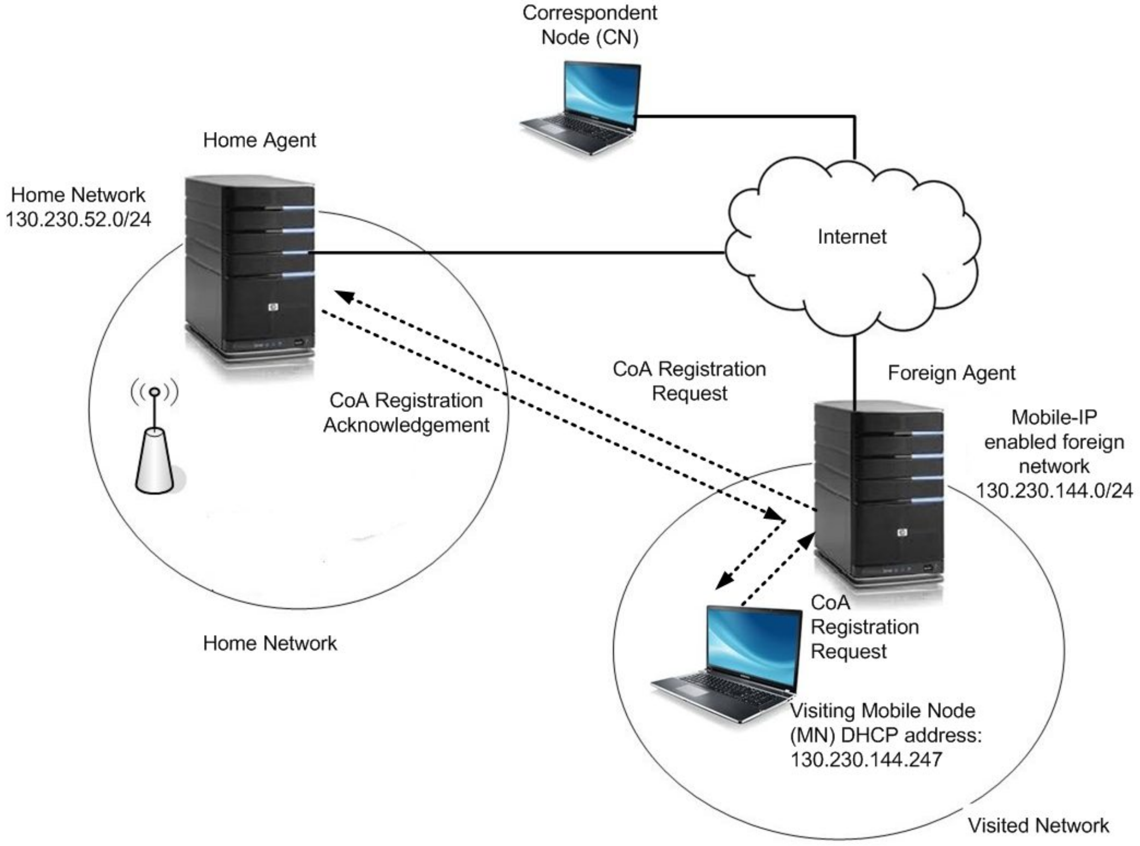

Correspondent Node (CN)
Home Agent
Home Network 130.230.52.0/24
Internet
CoA Registration Request
CoA Registration Acknowledgement
Foreign Agent
Mobile-IP enabled foreign network 130.230.144.0/24
CoA Registration Request
Home Network
Visiting Mobile Node (MN) DHCP address: 130.230.144.247
Visited Network

Figure 2.2: MN Moving to the Foreign Network

2.2 MIPv6

2.2.1 Overview of MIPv6

Mobile IPv6 allows an IPv6 node to arbitrarily change its location on an IPv6 network and still maintain existing connections. When an IPv6 node changes its location, it might also change its link. When an IPv6 node changes its link, its IPv6 address might also change in order to maintain connectivity. There are mechanisms to allow for the change in addresses when moving to a different link, such as stateful and stateless address auto configuration for IPv6. However, when the address changes, the existing connections of the mobile node that is using the address assigned from the previously connected link cannot be maintained and are ungracefully terminated.

The key benefit of Mobile IPv6 is that even though the mobile node changes locations and addresses, the existing connections through which the mobile node is communicating are maintained. To accomplish this, connections to mobile nodes are made with a specific address that is always assigned to the mobile node, and through which the mobile node is always reachable. Mobile IPv6 provides Transport layer connection survivability when a node moves from one link to another by performing address maintenance for mobile nodes at the Internet layer.

2.2.2 Basic terminology

- **Node:** A node is any device that implements IPv6.
- **Router:** A device that forwards packets that are not directed specifically to it.
- **Host:** A node that does not forward packets.
- **Interface:** An interface is the connection to a transmission medium through which packets are sent.
- **Links:** A link is the medium over which packets are carried.
- **Neighbors:** Neighbors are nodes that are connected to the same link.
- **Link MTUs:** A link maximum transmission unit (MTU) is the maximum packet size that can be carried over a given link medium, and is expressed in octets.
- **Link Layer Addresses:** A Link Layer address is the *physical* address of an interface, such as media access control (MAC) addresses for Ethernet links.

2.2.3 Discovery Mechanisms

Neighbor Discovery:

Discovery can be a misleading term, as nodes use discovery mechanisms to both advertise their presence to other nodes on the network and to determine parameters such as node location, router availability, link MTU, and address configuration. Some discovery methods are specific to the physical link type, although in [5] defines general discovery mechanisms. Discovery mechanisms are often implemented as multicasts, and replace IPv4 functionality such as ARP, ICMP router discovery, Internet Group Management Protocol (IGMP), and ICMP redirect.

Router Discovery Mechanisms:

Routers use discovery for a multitude of purposes. Both at regular intervals and in response to router solicitation requests, routers issue router advertisements. These advertisements can include information that informs nodes of Link Layer router addresses, link prefixes (the approximate equivalent to the IPv4 netmask), suggested hop limits, and link MTU.

By advertising its own physical address, each router enables other nodes on the network to ascertain the router's existence. Router advertising of link prefixes allows nodes to determine to which subnet they are attached, and thus to build their internal routing tables. In IPv6, packets are now decremented by hop, rather than by Time-to-Live (TTL) values. By sending suggested hop limits, a router aids nodes in determining whether a destination is reachable by a given path. Additionally, for multicasting to function correctly on a link, all nodes must use the same MTU. Router advertisements enable nodes to configure their packets correctly for the link MTU.

Using Router Advertisement, routers also can be configured for inbound load balancing. A router can have multiple interfaces to a given link. However, these interfaces can be presented as a single interface with multiple bound addresses, and the router can omit the source address in its router advertisement packets. Consequently, hosts wanting to send packets to the router would use a neighbor solicitation request to obtain a router interface's address. The router can then provide different addresses in response to requests from different hosts. All hosts will believe that they are sending packets to a single interface with multiple addresses when, in reality, the router might divide incoming traffic over all connected interfaces.

Host Discovery:

Hosts use discovery mechanisms primarily as an investigative tool, although they will also respond to requests for information regarding their own configuration. Upon initializing, a host might use discovery to query a router as to whether it should configure its address via *stateless* or *stateful* configuration. Stateful autoconfiguration is used to issue host address parameters via Dynamic Host Configuration Protocol (DHCP). As defined in [6], stateless autoconfiguration enables the host to assign itself an address, issue a discovery packet to determine if the address is being used by any other node on the link, and configure remaining link and site parameters based on the information the host received in the router advertisement packet.

When a node wants to communicate with another node, it issues a neighbor solicitation to the solicited node multicast address of the target node requesting its Link Layer address. The source node includes its own Link Layer address in the solicitation packet so that the target node can cache the results and thus does not need to issue its own solicitation. In response, the target node issues a neighbor advertisement listing its own Link Layer address.

When communication between two nodes is actively occurring, each node relies on upper layer protocols to provide confirmation that packets are successfully being sent and received. If this confirmation is not forthcoming, a node uses neighbor unreachability detection to determine if the other node is still functional by sending a unicast neighbor solicitation directly to its partner. If two-way connectivity is not confirmed, the node will stop sending packets to the target.

2.2.4 Mobile IPv6 Components

Figure 2.3 shows the components of Mobile IPv6.

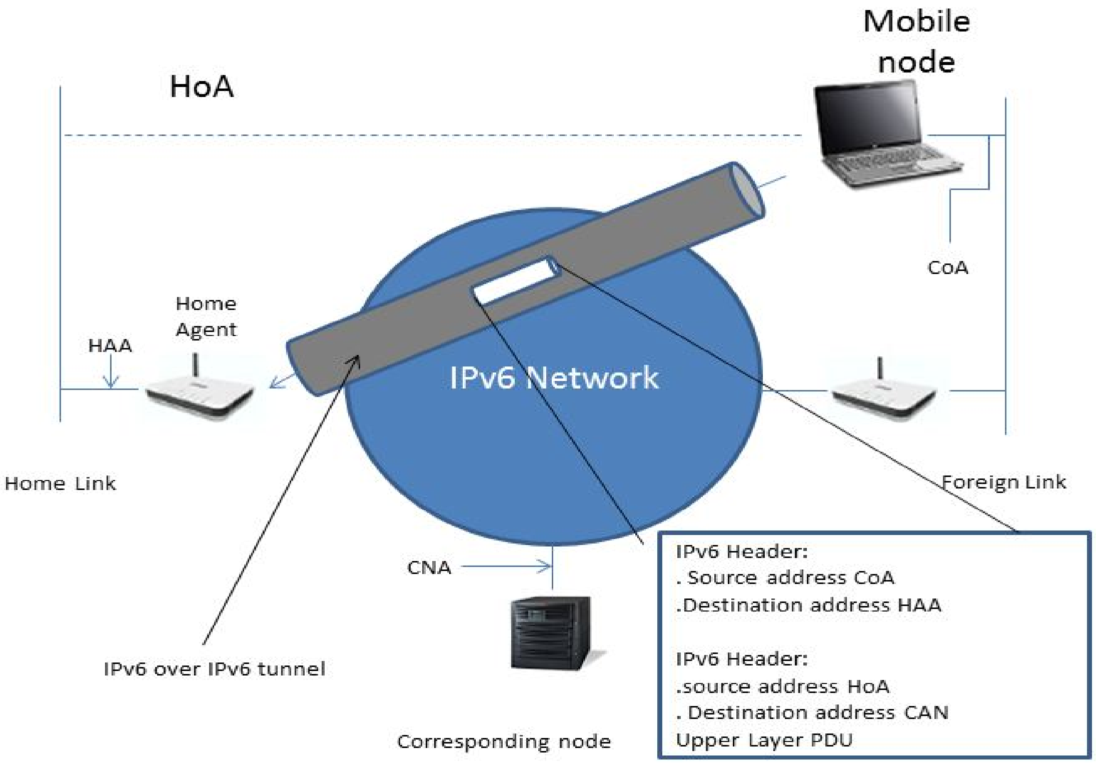


Figure 2.3: Components of Mobile IPv6

The components of Mobile IPv6 are the following:

- **Home Link:** The link that is assigned the home subnet prefix, from which the mobile node obtains its home address. The home agent resides on the home link.
- **Home address:** An address assigned to the mobile node when it is attached to the home link and through which the mobile node is always reachable, regardless of its location on an IPv6 network. If the mobile node is attached to the home link, Mobile IPv6 processes are not used and communication occurs normally. If the mobile node is away from home (not attached to the home link), packets addressed to the mobile node's home address are intercepted by the home agent and tunneled to the mobile node's current location on an IPv6 network. Because the mobile node is always assigned the home address, it is always logically connected to the home link.
- **Home agent:** A router on the home link that maintains registrations of mobile nodes that are away from home and the different addresses that they are currently using. If the mobile node is away from home, it registers its current address with the home agent, which tunnels data sent to the mobile node's home address to the mobile node's current address on an IPv6 network and forwards tunneled data sent by the mobile node. Although the figures in this white paper show the home agent as the router connecting the home link to an IPv6 network, the home agent does not have to serve this function. The home agent can also be a node on the home link that does not perform any forwarding when the mobile node is at home.
- **Mobile node:** An IPv6 node that can change links, and therefore addresses, and maintain reachability using its home address. A mobile node has awareness of its home address and the global address for the link to which it is attached (known as the care-of address), and indicates its home address/care-of address mapping to the home agent and Mobile IPv6-capable nodes with which it is communicating.
- **Foreign link:** A link that is not the mobile node's home link.
- **Care-of address:** An address used by a mobile node while it is attached to a foreign link. For stateless address configuration, the care-of address is a combination of the foreign subnet prefix and an interface ID determined by the mobile node. A mobile

node can be assigned multiple care-of addresses; however, only one care-of address is registered as the primary care-of address with the mobile node's home agent. The association of a home address with a care-of address for a mobile node is known as a binding. Correspondent nodes and home agents keep information on bindings in a binding cache.

- **Correspondent node:** An IPv6 node that communicates with a mobile node. A correspondent node does not have to be Mobile IPv6-capable. If the correspondent node is Mobile IPv6-capable, it can also be a mobile node that is away from home.

2.2.5 Mobile IPv6 Transport Layer Transparency

To achieve Transport layer transparency for the home address while the mobile node is assigned a care-of address, Mobile IPv6-capable nodes use the following:

- When a mobile node that is away from home sends data to a correspondent node, it sends the packets from its care-of address and includes the mobile node's home address in a Home Address option in a Destination Options extension header. When the correspondent node receives the packet, it logically replaces the source address of the packet (the care-of address) with the home address stored in the Home Address option.
- When an Mobile IPv6-capable correspondent node sends data to a mobile node that is away from home, it sends the packets to the care-of address and includes a Type 2 Routing extension header containing a single address, the mobile node's home address. When the mobile node receives the packet, it processes the Type 2 Routing header and logically replaces the destination address of the packet (the care-of address) with the home address from the Type 2 Routing header.

2.2.6 Mobile IPv6 Messages and Options

Mobile IPv6 requires the use of the following messages and message options:

- A new Mobility extension header with a set of Mobile IPv6 messages

- A set of mobility options to include in mobility messages
- A new Home Address option for the Destination Options header
- A new Type 2 Routing header
- New Internet Control Message Protocol for IPv6 (ICMPv6) messages to discover the set of home agents and to obtain the prefix of the home link
- Changes to router discovery messages and options and additional Neighbor Discovery options

2.2.7 Mobility Header and Messages

To facilitate the sending of messages between mobile nodes, correspondent nodes, and home agents for the purposes of managing the set of bindings between home addresses and care-of addresses, the Internet Engineering Task Force (IETF) has defined a new Mobility extension header. This new header can contain one of several defined mobility messages to perform specific functions. Some mobility messages can contain one or more options.

Mobility Header

The new Mobility extension header is dedicated to carrying mobility messages and has the structure as shown in Figure 2.4. Setting the previous header's Next Header field to the value of 135 identifies the Mobility extension header.

Within the Mobility extension header:

- The Payload Protocol field, equivalent to the Next Header field in the IPv6 header, is always set to the value of 59 to indicate that the Mobility header is the last header in the packet
- The MH Type field identifies the specific type of mobility message.
- The Message Data field contains a mobility message.

The following types of mobility messages are defined:

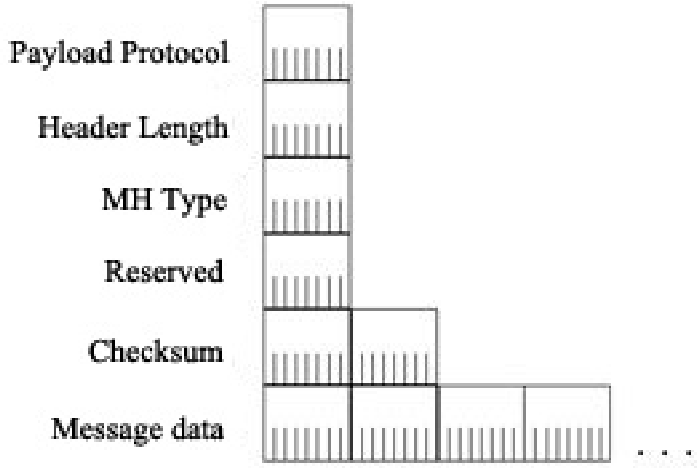


Figure 2.4: Structure of mobility extention header

- **Binding Refresh Request:** Sent by a correspondent node or home agent to request the current binding from a mobile node. If a mobile node receives a binding refresh request, it responds with a binding update. A correspondent node sends a binding refresh request when a binding cache entry is in active use and the lifetime of the binding cache entry approaches expiration. A home agent sends a binding refresh request when the lifetime of its binding cache entry approaches expiration.

- **Home Test Init (HoTI):** Sent by the mobile node during the Return Routability procedure to test the indirect path from a mobile node to a correspondent node via the home agent. For more information, see the *Return Routability Procedure* section of this white paper.

- **Care-of Test Init (CoTI):** Sent by the mobile node during the Return Routability procedure to test the direct path from a mobile node to a correspondent node.

- **Home Test (HoT):** Sent by the correspondent node during the Return Routability procedure to respond to the HoTI message.

- **Care-of Test (CoT):** Sent by the correspondent node during the Return Routability procedure to respond to the CoTI message.

- **Binding Update:** Sent by a mobile IPv6 node that is away from home to update another node with its new care-of address. The Binding Update option is used for the following:

1. To update the home agent with a new primary care-of address. This is known as a home registration binding update. The home agent uses the home address in the Home Address option and the care-of address in an Alternate Care-of Address mobility option to update its Home Address/Primary Care-of Address binding cache entry for the mobile node.
2. To update a Mobile IPv6-capable correspondent node with which the mobile node is actively communicating with a binding that maps the home address of the mobile node to its care-of address. This is known as a correspondent registration binding update. The correspondent node uses the home address in the Home Address option and the source address of the packet to update its Home Address/Care-of Address binding cache entry for the mobile node.

- **Binding Acknowledgement:** Sent by a home agent or a correspondent node to acknowledge the receipt of a Binding Update message. Included in the binding acknowledgement is an indication of how long the node will cache the binding. For home agents, this lifetime indicates how long the home agent will be in service as the home agent for the mobile node.
- **Binding Error:** Sent by a correspondent node to report errors in a binding update.

2.2.8 Type 2 Routing Header

Mobile IPv6-capable correspondent nodes use a new Type 2 Routing header when sending a packet directly to a mobile node that is away from home to indicate the mobile node's home address. Correspondent nodes set the Destination Address field in the IPv6 header to the mobile node's care-of address when performing direct delivery.

Figure 2.5 shows the structure of the new Type 2 Routing header. During the processing of a packet with a Type 2 Routing header, the mobile node replaces the Destination Address field with the value in the Home Address field. The Home Address field in the Type 2 Routing header is the actual destination address of the mobile node to which the packet has been sent (the care-of address stored in the Destination Address field of the IPv6 header is merely an intermediate delivery address).

The Type 2 Routing header is different from the Type 0 Routing header defined in [7]

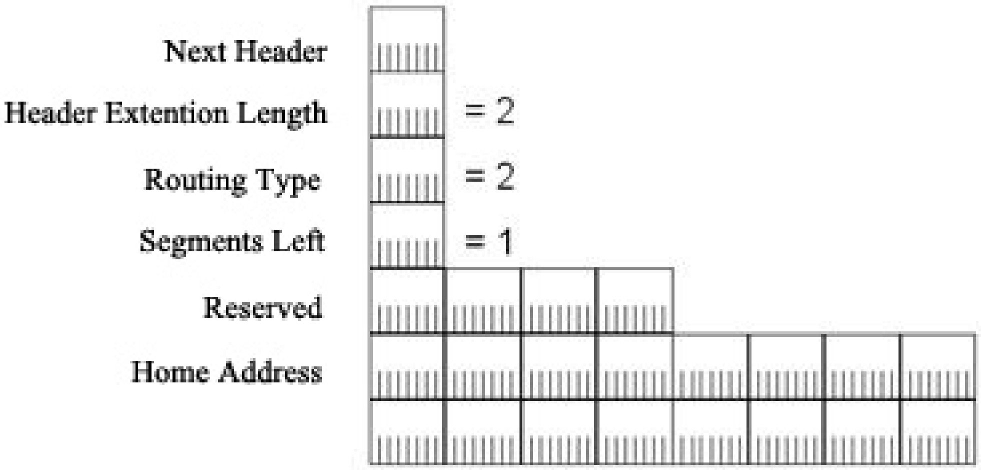


Figure 2.5: Structure of the new Type 2 Routing header

in that it can only store a single address and is only specified for use with Mobile IPv6. The Type 0 Routing header can store multiple addresses and is processed by routers for generalized source routing. Using a different routing type allows firewalls to treat source-routed packets differently from packets sent directly by Mobile IPv6-capable correspondent nodes to mobile nodes that are away from home.

2.2.9 Home Address Option for the Destination Options Header

The Home Address option in the Destination Options extension header in Figure 2.6 is used to indicate the home address of the mobile node and is included in binding updates sent to home agents and packets sent directly to Mobile IPv6-capable correspondent nodes by a mobile node when it is away from home when a binding exists. When a mobile node sends a packet, the source address in the IPv6 header is set to the care-of address. If the source address in the IPv6 header were set to the home address, the router on the foreign link might discard the packet because the source address does not match the prefix of the link on which the mobile node is located. By using the care-of address as the source address in the packet (a topologically correct address on the foreign link), and including the Home Address destination option, the router on the foreign link forwards the packet to its destination. When the packet is received at the destination, the correspondent node processes the Destination Options header and logically replaces the source address of the packet with the address in the Home Address option before passing the payload to the upper layer protocol. To the

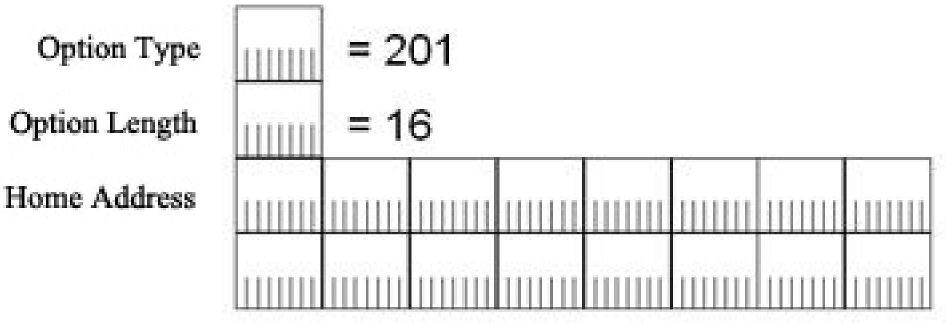


Figure 2.6: Structure of the Home Address destination option

upper layer protocol, the packet was sent from the home address. In contrast to the Home Address field in the Type 2 Routing header, the Home Address field in the Home Address destination option is the actual source address of the mobile node from which the packet was sent (the care-of address stored in the Source Address of the IPv6 header is merely an intermediate address).

2.2.10 ICMPv6 Messages for Mobile IPv6

The mobile node uses the following ICMPv6 messages for dynamic home agent address and home subnet prefix discovery:

- Home Agent Address Discovery Request
- Home Agent Address Discovery Reply
- Mobile Prefix Solicitation
- Mobile Prefix Advertisement

Dynamic home agent address discovery is a process by which the mobile node dynamically discovers the global address of a home agent on the home link. This process is only needed if the mobile node is not already configured with the address of its home agent or if the current home agent becomes unavailable. Home subnet prefix discovery is the process by which a mobile node dynamically discovers the address prefix of its home link. This process is only needed when a mobile node's home address is about to enter the invalid state.

Home Agent Address Discovery Request

The mobile node uses the ICMPv6 Home Agent Address Discovery Request message to begin dynamic home agent address discovery. The ICMPv6 Home Agent Address Discovery Request message is sent to the Mobile IPv6 Home-Agents anycast address that is described in RFC 2526. The Mobile IPv6 Home-Agents anycast is composed of the 64-bit home subnet prefix and the interface ID of ::FEFF:FFFF:FFFF:FFFE. All home agents are automatically configured with this anycast address. The home agent that is topologically closest to the mobile node receives the request message.

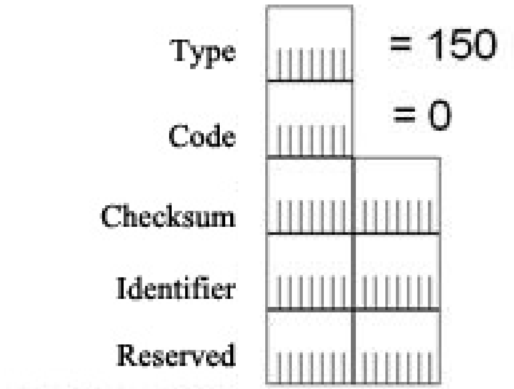


Figure 2.7: Structure of ICMPv6 Home Agent Address Discovery Request message

Figure 2.7 shows the structure of the ICMPv6 Home Agent Address Discovery Request message. In the Home Agent Address Discovery Request message, the Type field is set to 150 and the Code field is set to 0. Following the Checksum field is a 16-bit Identifier field. The value of the Identifier field is chosen by the sending node and copied to the Identifier field of the Home Agent Address Discovery Reply message to match a reply with its request. Following the Identifier field is a 16-bit Reserved field that is set to 0 by the sender.The Home Agent Address Discovery Request message is sent with the source address in the IPv6 header set to the mobile node's care-of address.

Home Agent Address Discovery Reply

The home agent uses the ICMPv6 Home Agent Address Discovery Reply message to complete the dynamic home agent address discovery process by informing the mobile node of the addresses of the home agents on the mobile node's home link.

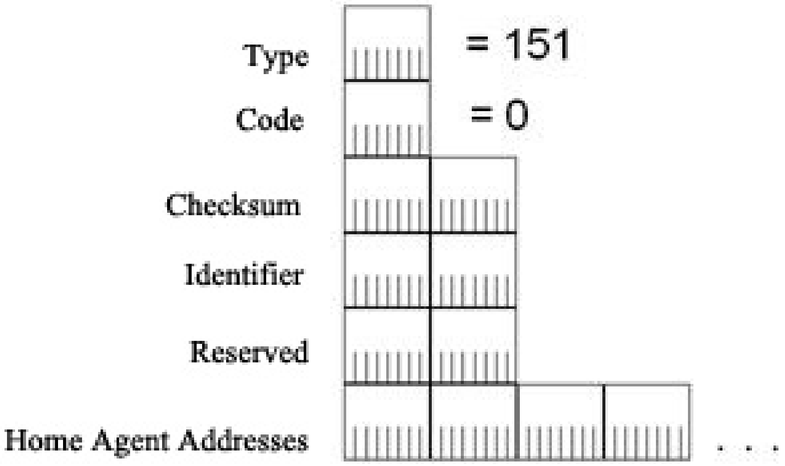


Figure 2.8: Structure of the ICMPv6 Home Agent Address Discovery Reply message

In the Home Agent Address Discovery Reply message, the Type field is set to 151 and the Code field is set to 0. Following the Checksum field is a 16-bit Identifier field. The value of the Identifier field is set to the same value as the Identifier field of the received Home Agent Address Discovery Request message. Following the Identifier field is a 16-bit Reserved field that is set to 0 by the sender, and one or more 128-bit Home Agent Address fields. The Home Agent Address fields contain the global addresses of home agents on the home link in preference order (highest preference first). The Home Agent Address Discovery Reply message is sent with the source address in the IPv6 header set to the global address of the answering home agent, and the destination address set to the mobile node's care-of address. A Type 2 Routing extension header is not included.

Mobile Prefix Solicitation

A mobile node uses the ICMPv6 Mobile Prefix Solicitation message to obtain its home subnet prefix while it is away from home. The response to the ICMPv6 Mobile Prefix Solicitation message is an ICMPv6 Mobile Prefix Advertisement message from the home agent, which contains the home subnet prefix and other configuration information by which the mobile node can update or refresh its home address.

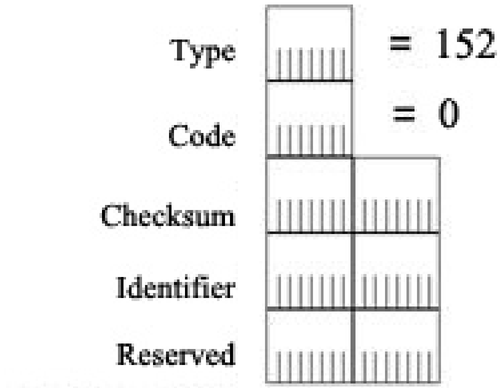


Figure 2.9: Structure of the ICMPv6 Mobile Prefix Solicitation message

Figure 2.9 shows the structure of the ICMPv6 Mobile Prefix Solicitation message The Identifier field is set by the mobile node and used to match a sent Mobile Prefix Solicitation message with its corresponding Mobile Prefix Advertisement message.

Mobile Prefix Advertisement

The home agent uses the ICMPv6 Mobile Prefix Advertisement message to advertise the home subnet prefix and other configuration options to mobile nodes that are away from home, either unsolicited or in response to a received ICMPv6 Mobile Prefix Solicitation message Figure 2.10 shows the structure of the ICMPv6 Mobile Prefix Advertisement message. The Identifier field is set to the value of the Identifier field of a received Mobile Prefix Solicitation message. The Managed Address Configuration, Other Stateful Configuration, and Options fields are the same as the corresponding fields of the Router Advertisement message as defined in RFC 2461, except that RFC 3775 defines the use of the Mobile IPv6-modified Prefix Information option, described in the next section.

2.2.11 Mobile IPv6 Data Structures

The following data structures are needed to facilitate the processes of Mobile IPv6:

- Binding cache
- Binding update list

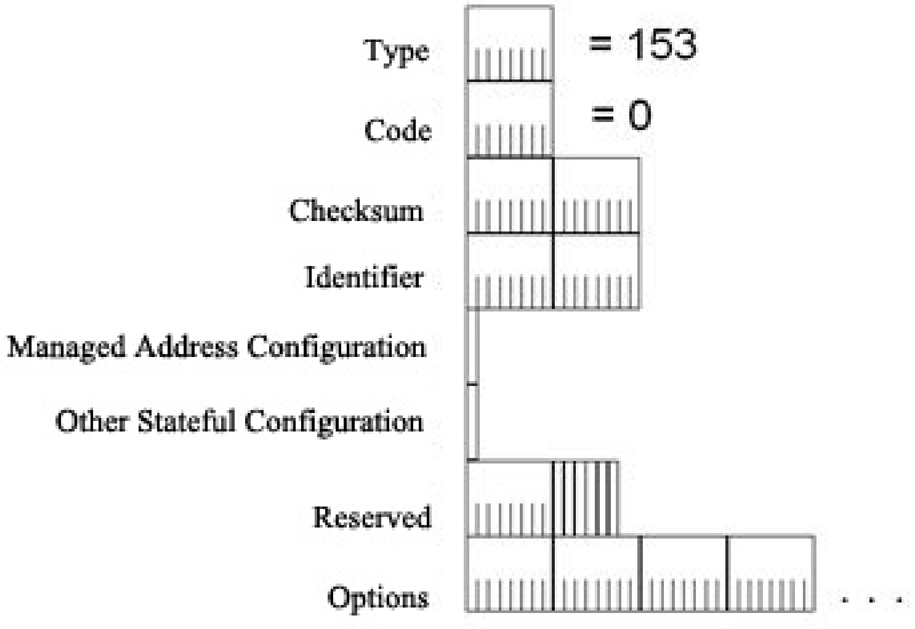


Figure 2.10: Structure of the ICMPv6 Mobile Prefix Advertisement message

- Home agents list

Binding Cache

The binding cache is a table maintained by each correspondent node and home agent that contains the current bindings for mobile nodes. Each binding cache entry contains the following information:

- The home address for the mobile node
- The care-of address for the mobile node
- The lifetime of the binding cache entry.The lifetime is obtained from a Lifetime field of the last Binding Update message that was received for this cache entry.
- A flag indicating whether the binding is a home registration
- The time that the last binding request was sent

The actual implementation details for the binding cache are not specified, as long as the external behavior is consistent with RFC 3775. For example, you could either maintain a separate binding cache or combine the binding cache with the destination cache. If you have a separate binding cache, you could either check it before you check the destination cache or have a pointer from the destination cache entry to the corresponding binding cache entry.

In any case, the information in the binding cache takes precedence over the information in the neighbor cache. For mobile destinations that are away from home, packets should be sent to the mobile node's home address by way of its care-of address. If packets are sent directly to the home address while the mobile node is away from home, the home agent must intercept the packets and tunnel them to the mobile node, lowering the efficiency and performance of the communication between the correspondent node and the mobile node.

Binding Update List

The binding update list is maintained by a mobile node to record the most recent binding updates sent for the home agent and correspondent nodes. A binding update list entry contains:

- The address of the node to which the binding update was sent
- The home address for the binding update
- The care-of address sent in the last binding update
- The value of the Lifetime field in the binding update
- The remaining lifetime of the binding
- The maximum value of the Sequence Number field sent in previous binding updates
- The time that the last binding update was sent
- An indication of whether a retransmission is needed for binding updates sent with the Acknowledge (A) flag set to 1 and when the retransmission is to be sent
- A flag indicating that no future binding updates need to be sent

Home Agents List

Home agents maintain the home agents list and record information about each router from which a Router Advertisement message was received on the home link with the Home Agent (H) flag set to 1. Home agents maintain the home agents list so that they can send the list of home agents to a requesting mobile node away from home during home agent address discovery.

A home agents list entry contains the following:

- The link-local address of the router on the link, obtained from the source address of the received Router Advertisement message
- The global address or addresses of the home agent, obtained from the Prefix field in the Prefix Information options in the Router Advertisement message with the Router Address (R) flag set to 1
- The remaining lifetime of this entry
- The preference for the home agent, obtained from the Home Agent Preference field in the Home Agent Information option

2.2.12 Correspondent Registration

There are two ways in which mobile nodes that are away from home can communicate with correspondent nodes:

- **Directly:** If the correspondent node is Mobile IPv6-capable, then data can be sent directly between the mobile node and the correspondent node. The mobile node sends data directly to the correspondent node using the correspondent node's address and includes the Home Address destination option to indicate its home address. The correspondent node sends data directly to the mobile node's care-of address and includes the Type 2 Routing header to indicate the mobile node's home address.
- **Indirectly:** If the correspondent node is not Mobile IPv6-capable or the registration of the binding for the mobile node with the correspondent node that is Mobile

> IPv6-capable has not yet been completed, then data can be sent indirectly between the mobile node and the correspondent node via the home agent. For traffic from the mobile node to the correspondent node, packets are tunneled to the home agent. The mobile node encapsulates the IPv6 packet sent from the mobile node's home address and to the correspondent node's address with an additional IPv6 header, with the source address of the mobile node's care-of address and the destination address of the home agent's global address. After receiving the packet, the home agent strips the outer IPv6 header and forwards the original IPv6 packet to the correspondent node. For traffic from the correspondent node to the mobile node, the correspondent node sends the packet to the mobile node's home address. When the home agent intercepts the packet, it is encapsulated with an additional IPv6 header, with the source address of the home agent's address and the destination address of the mobile node's care-of address.

In order for direct delivery to occur, the correspondent node with which the mobile node is communicating must be Mobile IPv6-capable and must have a binding cache entry that maps the mobile node's home address to its care-of address. Correspondent nodes that receive packets that contain a Home Address option in a Destination Options header must have a corresponding binding cache entry, otherwise the packet is silently discarded. This behavior provides some protection against malicious users or programs that attempt to impersonate mobile nodes that are away from home.

2.3 IPv6 duplicate address detection

IPv6 duplicate address detection is known as *IPv6 DAD*. When an interface is initialized or reinitialized, it uses autoconfiguration to tentatively associate a link-local address with that interface (the address is not yet assigned to that interface in the traditional sense). At this point, the interface joins the all-nodes and solicited-nodes multicast groups, and sends a neighbor discovery message to these groups. By using the multicast address, the node can determine whether that particular link-local address has been previously assigned, and choose an alternate address.

This eliminates accidentally assigning the same address to two different interfaces on the same link. (It is still possible to create duplicate global-scope addresses for nodes that are not on the same link.)

2.4 Mobile IPv6 Processes

Mobile IPv6 provides a method for a mobile node to determine it is on its home link and message exchanges for the following processes:

Attaching to the Home Link

The method used by a mobile node to determine that it is attached to the home link is not defined in [1]. Once a mobile node determines that it is connected to its home link, it can store the home subnet prefix, home address, and the global address of their home agent. The following methods for configuring home link parameters are based on implementations in development or existence at the time of the writing of this white paper:

- **Manual configuration:** In the simplest case, the home subnet prefix, home address, and the address of the home agent are manually configured, typically through a keyboard-based command, and are permanent until manually changed. These implementations do not support the dynamic discovery of home agents or changes in the home subnet prefix.
- **Pseudo-automatic configuration:** For pseudo-automatic configuration, when an IPv6 node is attached to a link, the user has the option (typically through a button in the user interface of the operating system) to indicate to the IPv6 protocol that the node is now connected to the home link. Based on this indication, the IPv6 protocol stores the home subnet link prefix and home address and listens for additional router advertisements containing the Home Agent (H) flag set to 1. The home agent is the router advertising itself with home agent capabilities and has the highest preference level. Once determined, the IPv6 protocol stores the address of the home agent. These implementations may or may not support the dynamic discovery of home agents or changes in the home subnet prefix.

- **Automatic configuration:** With automatic configuration, the IPv6 node is always listening for router advertisements with the H flag set to 1. Based on additional protocol or operating system parameters, the IPv6 node determines that it is potentially on its home link. Next, it chooses the most preferred home agent and attempts to establish a security relationship with it. If the security relationship with the home agent fails, the IPv6 node must not be on its home link. If the security relationship succeeds, the IPv6 node is on its home link and stores its home subnet prefix, its home address, and the address of its home agent. These implementations may or may not support the dynamic discovery of home agents or changes in the home subnet prefix.

Moving From the Home Link to a Foreign Link

When the mobile node is at home, it autoconfigures its home address through the receipt of a router advertisement, and communication with other nodes occurs normally without the use of Mobile IPv6 functionality.

- **Attaching to the Foreign Link:** When the mobile node attaches to the foreign link, the following occurs:

  1. The mobile node sends a multicast Router Solicitation message on the foreign link. The mobile node might send a router solicitation either because the link layer indicated a media change or because the node received a router advertisement that contains a new prefix. Depending on the Mobile IPv6 implementation, the mobile node sends a router solicitation either from its link-local address (assuming that the link-local address of the mobile node is most likely unique on the foreign link) or from the unspecified address (::) (assuming that the link-local address of the mobile might not be unique on the foreign link).
  2. All routers on the foreign link reply with a Router Advertisement message. Depending on the source address of the Router Solicitation message, the reply is either unicast (because the Router Solicitation was sent from a link-local address) or multicast (because the router solicitation was sent from the unspecified address). Figure 2.11 shows the router advertisement being unicast to the mobile node. The stateless autoconfiguration and registration of solicited node multicast

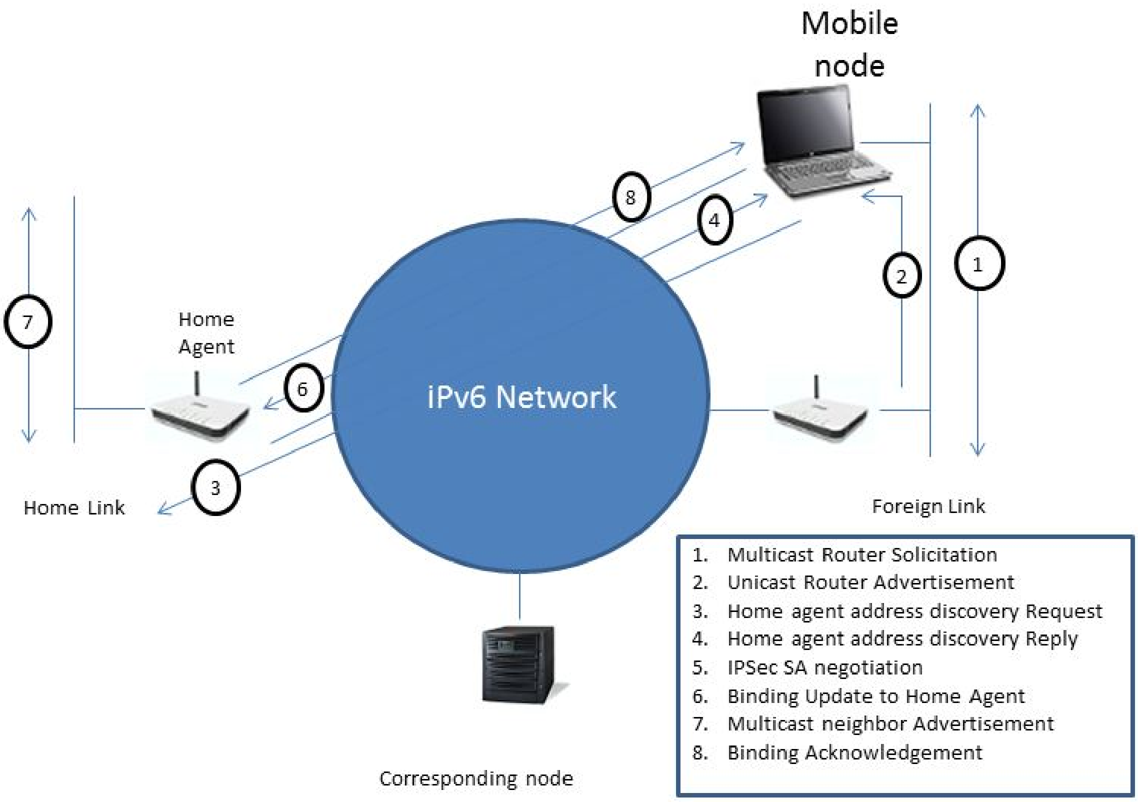

Mobile node
iPv6 Network
Home Agent
Home Link
Foreign Link
Corresponding node
1
2
3
4
6
7
8
1. Multicast Router Solicitation
2. Unicast Router Advertisement
3. Home agent address discovery Request
4. Home agent address discovery Reply
5. IPSec SA negotiation
6. Binding Update to Home Agent
7. Multicast neighbor Advertisement
8. Binding Acknowledgement

Figure 2.11: Mobile node attaching to the first foreign link

addresses on the foreign link introduces some latency in the process of obtaining a valid care-of address.

3. If the mobile node is already configured with the address of its home agent, go to step 5. If not, to determine the address of a home agent on the mobile node's home link, the mobile node uses the home agent discovery process. Mobile nodes do not maintain a list of home agents while connected to the home link. To automatically discover the home agents on the home link, it is sufficient for the mobile node to learn its home subnet prefix. When the mobile node that uses automatic configuration of home agents leaves its home link and moves to the first foreign link, it sends an ICMPv6 Home Agent Address Discovery Request message to the Mobile IPv6 Home Agents anycast address formed from the home subnet prefix.

4. A home agent on the home link that is using the Mobile IPv6 Home Agents anycast address corresponding to the home subnet prefix and is topologically closest to the mobile node receives the ICMPv6 Home Agent Address Discov-

ery Request message. Next, it sends back an ICMPv6 Home Agent Address Discovery Reply message containing the entries in the home agent's home agent list in preference order. Upon receipt of the ICMPv6 Home Agent Address Discovery Reply message, the mobile node selects the first home agent in the list as its home agent.

5. Before the binding update is sent, an IPSec security association (SA) must be created between the mobile node and the home agent. If the mobile node and the home agent support the use of Internet Key Exchange (IKE) for Mobile IPv6, then an IKE negotiation takes place to create SAs for the ESP protection of packets sent between the mobile node and the home agent. The IKE negotiation is not shown in Figure 2.11. If the mobile node and the home agent support the sending of binding updates without IPSec protection or the manual configuration of an IPSec SA, then this step is skipped.

6. To register the primary care-of address with the home agent, the mobile node sends the home agent a binding update. In the binding update, the Home Registration (H) and Acknowledgement (A) flags are set.

7. The home agent receives the binding update and updates its binding cache. To intercept packets destined for the mobile node's home address while the mobile node is away from home, the home agent performs duplicate address detection and proxy ND for the mobile node by answering neighbor solicitations on behalf of the mobile node. Depending on the implementation, the home agent might send an unsolicited multicast Neighbor Advertisement message as if it were the mobile node immediately or only respond to multicast neighbor solicitations for the mobile nodes home address. The duplicate address detection and proxy ND introduces an additional latency in the home registration process.

8. Because the binding update has the A flag set to 1, the home agent responds with a binding acknowledgement.

   This process is shown in Figure 2.11.

Because there are no entries in the binding update list, the mobile node does not send a binding update to all the nodes with which the mobile node was communicating when connected to the home link. The mobile node relies on subsequent data sent on existing connections or the receipt of traffic tunneled via the home agent to initiate correspondent registration with correspondent nodes.

- **A New Correspondent Node Communicates with a Mobile Node:** When a new correspondent node either resumes communication or initiates communication with a mobile node using the mobile node's home address and the mobile node is away from home, the following occurs:

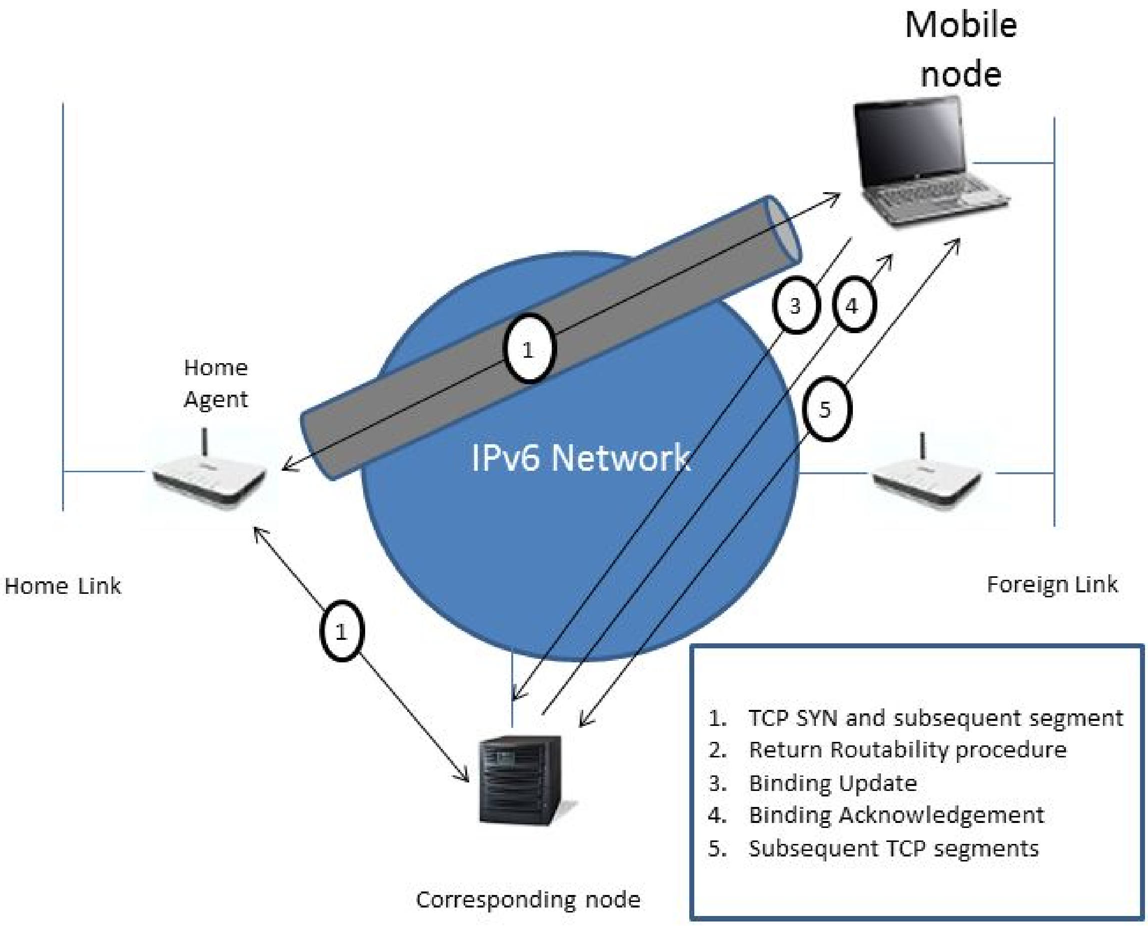

Mobile node
Home Agent
1
3
4
5
IPv6 Network
Home Link
Foreign Link
1
Corresponding node
1. TCP SYN and subsequent segment
2. Return Routability procedure
3. Binding Update
4. Binding Acknowledgement
5. Subsequent TCP segments

Figure 2.12: A new correspondent node communicating with a mobile node

1. The correspondent node begins the TCP connection by sending the initial TCP SYN segment to the mobile node, tunneled via the home agent. Subsequent TCP handshake segments and the initial data communication between the correspondent node and the mobile node are sent using bidirectional tunneling until the correspondent registration is complete (see step 5). This is done so that the application that is attempting to communicate does not have to wait until the correspondent registration is complete before it can begin communicating.

2. The mobile node adds an entry for the correspondent node to its binding update list and initiates the Return Routability procedure
3. After the Return Routability procedure is complete, the mobile node sends the correspondent node a Binding Update message with the A flag set to 1.
4. Upon receipt of the Binding Update message, the correspondent node updates its binding cache and sends back a Binding Acknowledgement message.
5. After the correspondent registration is complete, subsequent TCP segments on the connection are sent directly between the mobile node and the correspondent node.

Because the TCP connection creation occurs separately from the correspondent registration, the subsequent segments in the TCP handshake (the SYN Acknowledge [ACK] and ACK segments) and the ensuing application data sent over the TCP connection are bidirectionally tunneled until the correspondent registration is complete.

This process is shown in Figure 2.12.

- **A Node on the Home Link Communicates with the Mobile Node:** When a node on the home link either resumes or initiates communication with a mobile node using the mobile node's home address and the mobile node is away from home, the following occurs (example assumes a new TCP connection):

1. The node on the home link sends a multicast Neighbor Solicitation message to the solicited node multicast address corresponding to the mobile node's home address.
2. The home agent is acting as an ND proxy for the mobile node. It has registered the solicited node multicast address corresponding to the mobile node's home address as a multicast address to which it is listening. The home agent receives the neighbor solicitation and sends a unicast neighbor advertisement containing the home agent's link-layer address.
3. The initial TCP SYN segment and subsequent TCP segments are sent between the node on the home link and the home agent using each other's link-layer address.

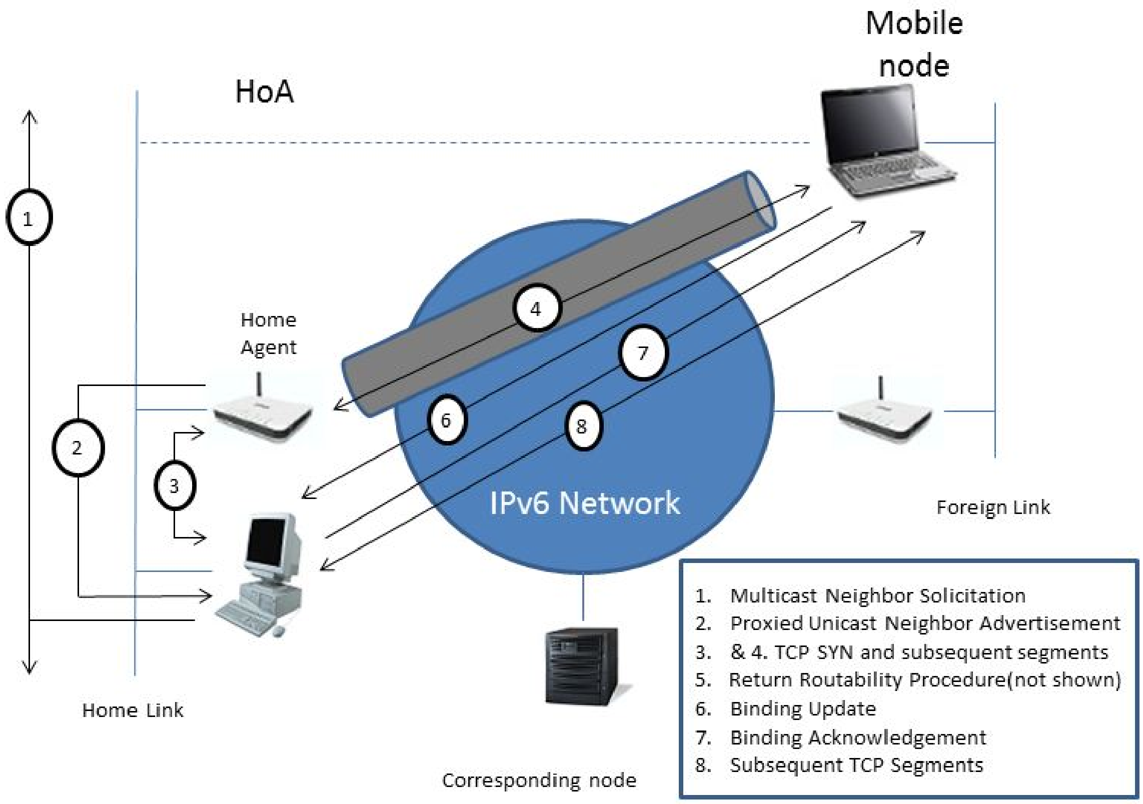

Mobile node
HoA
Home Agent
IPv6 Network
Foreign Link
Home Link
Corresponding node
1
2
3
4
6
7
8
1. Multicast Neighbor Solicitation
2. Proxied Unicast Neighbor Advertisement
3. & 4. TCP SYN and subsequent segments
5. Return Routability Procedure(not shown)
6. Binding Update
7. Binding Acknowledgement
8. Subsequent TCP Segments

Figure 2.13: A node on the home link communicating with the mobile node

4. The TCP segments are tunneled to and from the mobile node. The bidirectional tunneling of TCP segments continues until the correspondent registration is complete (see step 5)

5. Upon receipt of the initial tunneled TCP SYN segment from the home agent, the mobile node performs a Return Routability procedure with the node on the home link

6. The mobile node sends the node on the home link a Binding Update message.

7. The node on the home link sends a Binding Acknowledgement message.

8. After the correspondent registration is complete, subsequent TCP segments on the connection are sent directly between the mobile node and the node on the home link.

This process is shown in Figure 2.13.

- **Mobile Node Changes its Home Address:** To refresh a home address that is approaching the end of its valid lifetime or to receive a new home address following a change in the home subnet prefix, the following process is used:

1. The mobile node sends an ICMPv6 Home Prefix Solicitation message to the home agent.

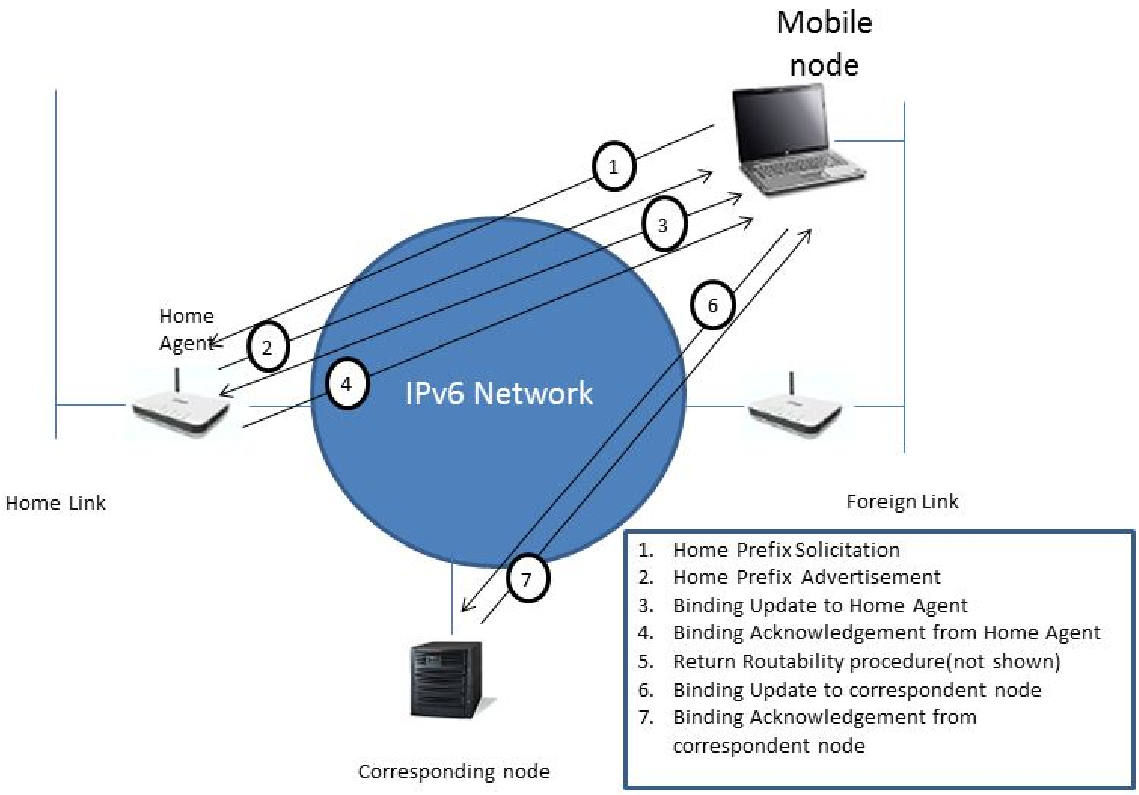

Mobile node
Home Agent
IPv6 Network
Home Link
Foreign Link
Corresponding node
1
2
3
4
6
7
1. Home Prefix Solicitation
2. Home Prefix Advertisement
3. Binding Update to Home Agent
4. Binding Acknowledgement from Home Agent
5. Return Routability procedure(not shown)
6. Binding Update to correspondent node
7. Binding Acknowledgement from correspondent node

Figure 2.14: A mobile node changing its home address

2. The home agent sends back an ICMPv6 Home Prefix Advertisement message. Upon receipt of the Home Prefix Advertisement message, the mobile node examines the Prefix Information option. If there is no change in the home subnet prefix and therefore no change in the home address, the mobile node refreshes the valid and preferred lifetimes of the stateless home address and this process ends.

3. To register the new home address with the home agent, the mobile node sends the home agent a binding update. In the binding update, the Home Registration (H) and Acknowledgement (A) flags are set to 1.

4. The home agent sends a binding acknowledgement.

5. The mobile node must perform a new correspondent registration with each correspondent in its binding update list. Therefore, a Return Routability procedure

is performed (not shown in Figure 2.14) with each correspondent node in the binding update list. Because only the path associated with the home address has changed, only the HoTI and HoT messages are exchanged.

6. After the Return Routability procedure is successful, the mobile node sends a binding update to each correspondent node.
7. Upon the receipt of the binding update, the correspondent node updates its binding cache and sends a binding acknowledgment.

2.5 Hierarchical Mobile IPv6

The Hierarchical Mobile IPv6 (HMIPv6) [8] protocol was the first to introduce [9], prior to PMIPv6, network based mobility management. It is an extension of MIPv6 which introduces a new entity, the Mobility Anchor Point (MAP), to address the handover latency issues of MIPv6. HMIPv6 can be seen mostly as an extension of the MIPv6 protocol: a mobile node is free to choose one or the other, thus allowing it to operate in local or global mobility management scenarios.

To smooth a handover, the mobile node updates its current location with the new MAP entity. This entity is located on the access network, and it will handle the signaling with the HA (located in its home network) and correspondent nodes on behalf of the mobile node. Thus, only one binding message has to be sent to the MAP, instead of having to send bindings to the HA and each correspondent node. Additionally, as the trafic will be tunneled between the mobile node and the MAP, the MAP effectively acts on behalf of the mobile node towards the other entities. Considering that typically a mobile node will use a wireless access technology, which has greater latency and less bandwidth than a wired technology, the nearby MAP can provide a signficant improvement in mobility handover performance. Also, a MAP does no require a permanent HA and home address for the mobile node as it can learn about them through the MAP entity in the access network.

2.5.1 Protocol Extensions

A mobile node learns about MAPs through Router Advertisements and Neighbour Discovery. The MAP option [8] is introduced for this purpose in these messages. A new flag, the M fag, is introduced to the MIPv6 BU message to indicate that a message is a local binding update, which is the message that a mobile node must send to the MAP to update its current location. HMIPv6 requires changes to the mobile node operation and the new MAP entity, whereas all the other entities defined by MIPv6 are left unchanged.

2.5.2 Advantages and Disadvantages

The major advantage of HMIPv6 is the signficant reduction of the mobile node participation in the signaling with the introduction of the MAP entity. The lack of a MAP entity is not a problem for the HMIPv6 since a mobile node can simply fallback to MIPv6. In terms of security the mobile node gains more privacy in relation to the correspondent nodes and HA. The remaining disadvantages are mostly the same as in the MIPv6 protocol with the complexity of the protocol and the required extended modification to the mobile node's IP stack.

2.6 Mobility Mangement

2.6.1 Host-based Mobility Management

In 2.1.5, we discuss about operation of MIPv4 and from Figure 2.1 and 2.2, we observe that

- MN connects to foreign network and gets CoA
- MN sends binding update to HA
- Every traffic destined to the MN will be encapsulated in Ipv6-in-IPv6 tunnel and send to the CoA of MN

So the network involvement in mobility is minimal.Most of mobility functions are operated in MN. So, this mobility type is called Host-based Mobility.

Mobile IP is probably the most widely known IP mobility support protocol. Two versions of Mobile IP have been standardized for supporting host-based mobility on the Internet: MIPv4 and MIPv6. They support the mobility of IP hosts by allowing them to utilize two IP addresses: a home address (HoA) that represents the fixed address of a mobile node (MN) and a careof- address (CoA) that changes with the IP subnet to which an MN is currently attached. In terms of the fundamental architectural aspects, these two mobility support standards follow the same concept. However, there are slight differences with regard to some important details. MIPv6 comprises three components: the MN, the home agent (HA), and the correspondent node (CN). The role of the foreign agent (FA) in MIPv4 was replaced by the access router (AR) in MIPv6.

In addition, although route optimization extensions were proposed for both MIPv4 and MIPv6, they were only standardized for MIPv6. A detailed description of MIPv6 route optimization as well as details of MIPv4 and MIPv6 can be found in [1, 10]. Although MIPv6 is a mature standard for IP mobility support and solves many problems, such as triangle routing, security, and limited IP address space, addressed in MIPv4, it still has some problems such as handover latency, packet loss, and signaling overhead. Besides, the handover latencies associated with MIPv4/v6 do not provide the quality of service (QoS) guarantees required for real-time applications. Therefore, various MIPv6 enhancements such as hierarchical Mobile IPv6 (HMIPv6) [9] and fast handover for Mobile IPv6 (FMIPv6) have been reported over the past years, mainly focused on performance improvement in MIPv6. However, MIPv6 and its various enhancements basically require protocol stack modification of the MN in order to support them. In addition, the requirement for modification of MNs may cause increased complexity on them.

2.6.2 Network-based Mobility Management

In a network-based mobility management approach such as PMIPv6, the serving network handles the mobility management on behalf of the MN. Thus, the MN is not required to participate in any mobility-related signaling. Compared to hostbased mobility management approaches such as MIPv6 and its enhancements, a network-based mobility management approach such as PMIPv6 has the following salient features and advantages.

- **Deployment perspective:**

  Unlike host-based mobility management, network-based mobility management does not require any modification of MNs. The requirement for modification of MNs can be considered one of the primary reasons MIPv6 has not been widely deployed in practice, although several commendable MIPv6 enhancements have been reported over the past years. Therefore, no requirement for modification of MNs is expected to accelerate the practical deployment of PMIPv6. Such an expectation can easily be demonstrated by the fact that in the WLAN switching market, no modification of the software on MNs has been required to support IP mobility, so these unmodified MNs have enabled network service providers to offer services to as many customers as possible [2].

- **Performance perspective:**

  Generally, wireless resources are very scarce. In terms of scalability, efficient use of wireless resources can result in enhancement of network scalability. In hostbased network layer approaches such as MIPv6, the MN is required to participate in mobilityrelated signaling. Thus, a lot of tunneled messages as well as mobility-related signaling messages are exchanged via the wireless links. Considering the explosively increasing number of mobile subscribers, such a problem would cause serious performance degradation. On the contrary, in a network-based network layer approach such as PMIPv6, the serving network controls the mobility management on behalf of the MN, so the tunneling overhead as well as a significant number of mobility-related signaling message exchanges via wireless links can be reduced. Generally, the signaling latency introduced by an MN can be significantly affected by the performance parameters such as wireless channel access delay and wireless transmission delay. The latencies incurred by such performance parameters can be considerable compared to those of the wired link; thus, the signaling latency introduced by the MN could result in increasing handover failures as wireless channel access and wireless transmission delays get larger.

- **Network service provider perspective:**

  From the perspective of a network service provider, it is expected that network-based mobility management would enhance manageability and flexibility by enabling network service providers to ly be expected from legacy cellular systems such as IS-41 and Global System for Mobile Communications (GSM), which can be considered network- based (i.e., network-controlled) systems. Note that PMIPv6 has some resemblance to General Packet Radio Service (GPRS) in that they are both network-based mobility management protocols and have similar functionalities. However, PMIPv6 is an Internet protocol that is not dependent on any access-technology-specific protocol, so it could be used in any IP-based network, while GPRS is an access-technology-specific protocol closely coupled with the signaling protocols used in legacy cellular systems.

CHAPTER 3
PROXY MOBILE IPV6

The main idea of PMIPv6 [3] is that the mobile node is not involved in any IP layer mobility-related signaling. The Mobile Node is a conventional IP device (that is, it runs the standard protocol stack). The purpose of PMIPv6 is to provide mobility to IP devices without their involvement. This provision is achieved by relocating relevant functions for mobility management from the Mobile Node to the network.

3.1 Overview of PMIPv6

The fundamental foundation of PMIPv6 is based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as the HA functionality. However, PMIPv6 is designed to provide network-based mobility management support to an MN in a topologically localized area the Localized Mobility Domain (LMD) or PMIPv6 domain.

Therefore, an MN is exempt from participation in any mobility-related signaling, and the proxy mobility agent in the serving network performs mobility-related signaling on behalf of the MN. Once an MN enters its PMIPv6 domain and performs access authentication, the serving network ensures that the MN is always on its home network and can obtain its HoA on any access network. That is, the serving network assigns a unique home network prefix to each MN, and conceptually this prefix always follows the MN wherever it moves within a PMIPv6 domain. From the perspective of the MN, the entire PMIPv6 domain appears as its home network. Accordingly, it is needless (or impossible) to configure the CoA at the MN.

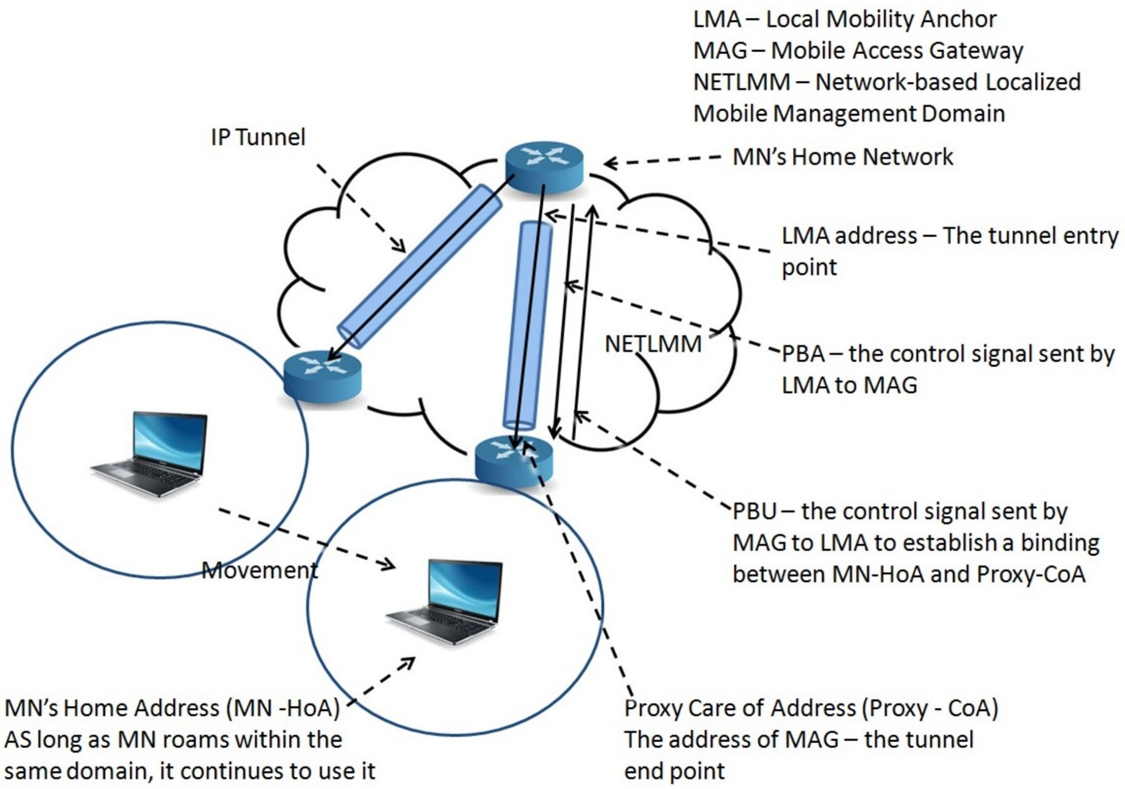

LMA – Local Mobility Anchor
MAG – Mobile Access Gateway
NETLMM – Network-based Localized Mobile Management Domain
IP Tunnel
MN's Home Network
LMA address – The tunnel entry point
NETLMM
PBA – the control signal sent by LMA to MAG
PBU – the control signal sent by MAG to LMA to establish a binding between MN-HoA and Proxy-CoA
Movement
MN's Home Address (MN -HoA) AS long as MN roams within the same domain, it continues to use it
Proxy Care of Address (Proxy - CoA) The address of MAG – the tunnel end point

Figure 3.1: Overview of PMIPv6

The functional entities in the PMIPv6 network architecture (refer to Figure 1) include the following:

- **Mobile Access Gateway (MAG):**

  This entity performs the mobility-related signaling on behalf of the Mobile Nodes attached to its access links. The MAG is usually the access router for the Mobile Node, that is, the first-hop router in the Localized Mobility Management infrastructure. It is responsible for tracking the movements of the Mobile Node in the LMD. An LMD has multiple MAGs. In addition, the MAG establishes a tunnel with the LMA for enabling the MN to use an address from its home network prefix and emulates the MN home network on the access network for each MN.

  It must also emulate the mobile node's home link at the access link. PMIPv6 defines a conceptual data structure, the Binding Update List, for managing the bindings with LMAs on behalf of the mobile nodes. The PMIPv6 Binding Update List is an ex-

Table 3.1: Binding Update List entry extensions

Field	Description
MN identifier	The identifier of mobile node
link layer identifier	The identifier of the mobile node's network interface
list of network prefixes	The network prefixes assigned to the mobile node's network interface
tunnel interface identifier	The tunnel interface identifier of the bidirectional tunnel between the the MAG and LMA
LMA IP address	The IPv6 address of the local mobility anchor serving the attached mobile node
access link interface identifier	The interface identifier of access link
access link interface address	The address of the access link interface

tension of the MIPv6 one. Table 3.1 depicts the extended fields for MIPv6 Binding Update List entry.

Mobile Node Detection

The detection of the mobile node attachment and detachment is specific to the access link technology, thus it is outside of the scope of PMIPv6.

Home Link Emulation

As the mobile node moves from one access point to another, it must continue to detect its home network without a change of L3 attachment. Thus all MAGs must use use the same link-local address for a given mobile node. This also prevents any potential conficts that may arise from the link-local collisions between the mobile node and the MAG. If a link-local address must be generated for the MAG, then it should be the LMA to generate and store this information for the MAG.

Binding Management

The MAG sends a PBU to a LMA when it detects a mobile node attach, detach or a Binding Update List entry lifetime is about to expire. When sending a PBU the corresponding Binding Update List entry must be created or updated, the message must be constructed in the following manner:

1. the proxy and acknowledgeags must be set.
2. the sequence number must be set from the value of the last sent PBU, after being incremented. Or, a Timestamp Mobility Option must be included.
3. the lifetime must be set to a value of zero for de-registrations and greater than zero for registrations.
4. the Mobile Node Identifier Options must be included.
5. one or more Home Network Prefix Option must be included. When a new Binding Update List entry is created and the mobile node does not known the network prefixes from the mobile node's policy profile, the PBU must include only one Home Network Prefix Option with an all zeros network prefix. This indicates to the LMA to allocate the network prefixes.
6. the Handover Option must be included. The handover option data filed must be set to one of value of: 1. for a new mobility session. 2. for an existing mobility session handover between diffierent interfaces of a mobile node. 3. for an existing mobility session handover by the same interface of the mobile node. 4. if the previous reasons cannot be determined. 5. for binding lifetime extension.
7. the Link Layer Identifier option should be included with the mobile node's one, if it's unknown then the option data must be all zeros.
8. the Access Technology Type Option must be included.
9. the Link Local Address Option must be include, unless all MAGs on all access links use the same Link Local Address. If value is unknown, the option value should be all zeros. The message must be retransmitted, with an exponential retransmission time, until a matching PBA is received. Upon receiving the PBA with a success status code, the MAG can set the bi-directional tunnel endpoint and traffic forwarding. If the status code indicates an error the mobile service is not provided to the mobile node.

- **Local Mobility Anchor (LMA):**

  The LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6.

Table 3.2: Binding Update List entry extensions

Field	Description
proxy binding flag	This flags indicates if the entry is a proxy (value = 1) or home (value = 0) registration entry. For PMIPv6, this flag is always 1.
MN identifier	The identifier of registered mobile node. This is obtained from the PBU message.
link layer identifier	The identifier of the mobile node's network interface. This is obtained from the PBU message.
link-local address	The link-local address of the MAG on the mobile node access link. (...)
list of network prefixes	The network prefixes assigned to the mobile node's network interface.
tunnel interface identifier	The tunnel interface identifier of the bidirectional tunnel between the the LMA and the MAG.
access technology type	The technology type, by which the mobile node is currently attached. This is obtained from the PBU message.
64-bit timestamp	The timestamp of the last received PBU message. This field is not used if the sequence number scheme is used, in such case the value should be zero.

The main role of the LMA is to maintain reachability to the MN address while it moves around within a PMIPv6 domain, and the LMA includes a binding cache entry for each currently registered MN. The binding cache entry maintained at the LMA is more extended than that of the HA in MIPv6 with some additional fields such as the MN-Identifier, the MN home network prefix, a flag indicating a proxy registration, and the interface identifier of the bidirectional tunnel between the LMA and MAG. Such information associates an MN with its serving MAG, and enables the relationship between the MAG and LMA to be maintained.

This entity within the core network maintains a collection of routes for each Mobile Node connected to the LMD. The routes point to MAGs managing the links where the Mobile Nodes are currently located. Packets sent or received to or from the Mobile Node are routed through tunnels between the LMA and the corresponding MAG. The LMA is a topological anchor point for the addresses assigned to Mobile Nodes in the LMD, meaning that packets with those addresses as destination are routed to the LMA.

The PMIPv6 extends the Binding Cache conceptual data structure described in MIPv6 with additional fields (table 3.2) which is used to manage the bindings.

Mobility Session

PMIPv6 uses a unique prefix model and not a shared prefix model like MIPv6. From a network perspective, the LMA is a router for the mobile node's traffic. More than one network prefix can be assigned to a given network interface of the mobile node. All prefixes assigned to the same network interface are part of the same mobility session, i.e., a mobility session is managed on a mobile node network interface basis.

Binding Management

When the LMA receives a PBU message from a MAG, the LMA must validate the message by checking the options and match the mobile node policy profile. The source MAG must also be authorized. If the message is not validated, a PBA is sent with an error status code indicating the reason. Figure 3.2 indicates the operation decision to take when a PBU is received:

For new registrations a Binding Cache entry must be created, the tunnel and forwarding must be set. For a registration message with a Network Prefix Option of all zeros, the LMA must allocate prefix(es) for the mobile node.

For a lifetime extension, the Binding Cache entry must be updated. If the extension is a *handoff*, the tunnel and forwarding must be re-set.

For a de-registration, the Binding Cache entry, the tunnel and forwarding must be removed. The Binding Cache entry actual removal is delayed for a given amount of time to provide a wait window for binding registrations.

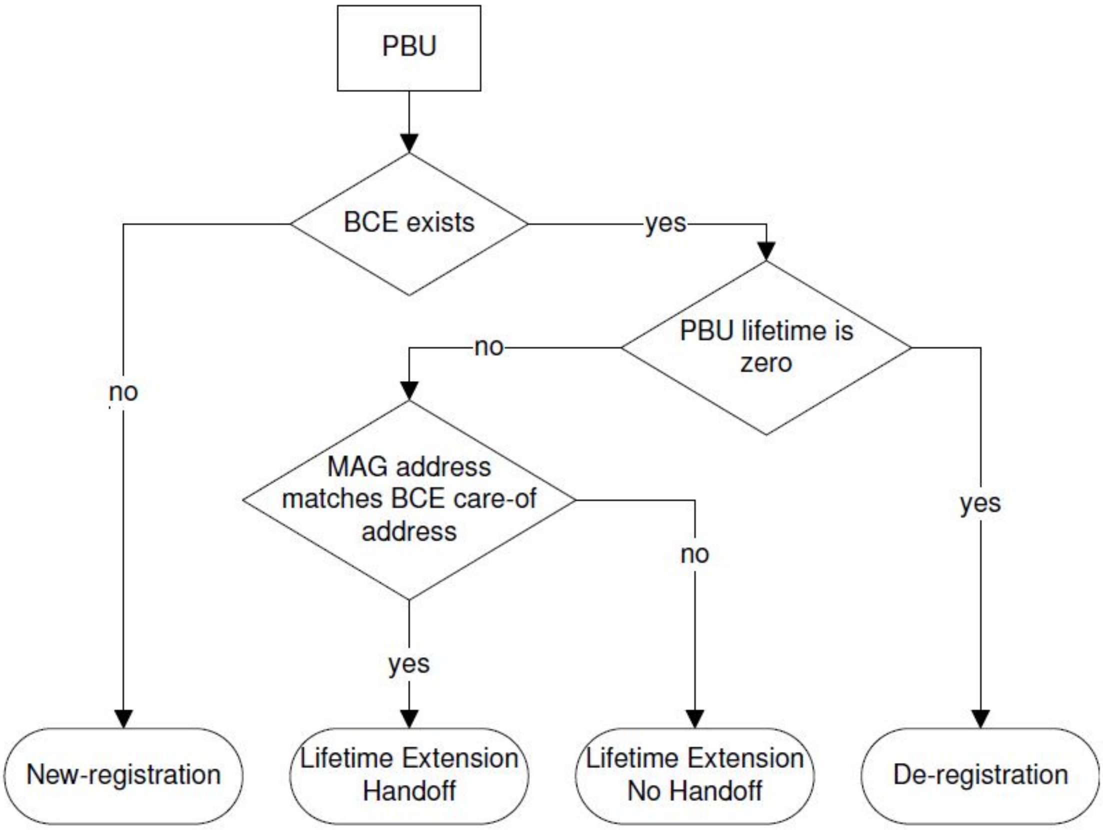

PBU
BCE exists
yes
no
PBU lifetime is zero
no
yes
MAG address matches BCE care-of address
no
yes
New-registration
Lifetime Extension Handoff
Lifetime Extension No Handoff
De-registration

Figure 3.2: Proxy Binding Update message operation decision

After the conclusion of the operation, a reply PBA is sent. When sending a PBA message, Mobility Options are copied from the correspondent PBU, with the exception of the case where the LMA must allocated the prefixes; here the included Network Prefix Option(s) must be the ones allocated by the LMA. The fields in the PBA message header must also be copied from PBU, but lifetime should not be higher than the prefix(es) lifetime. The status code should be set to zero for success or a value of error indication the reason. In the later case, errors may arise from missing Mobility Options. In such case the mobility option is question should be added to the PBA with a value of all zeros.

3.2 The Primary features of PMIPv6

In a network-based approach such as PMIPv6, the serving network controls mobility management on behalf of the MN; thus, the MN is not required to participate in any mobility-related signaling. The design goals the IETF NETLMM working group aims to cover are very extensive. The primary features of such goals are as follows:

1. **Support for unmodified MNs:** Unlike a hostbased approach, a network-based approach should not require any software update for IP mobility support on MNs.

2. **Support for IPv4 and IPv6:** Although the initial design of a network-based approach uses an IPv6 host, it is intended to work with IPv4 or dual-stack hosts as well.

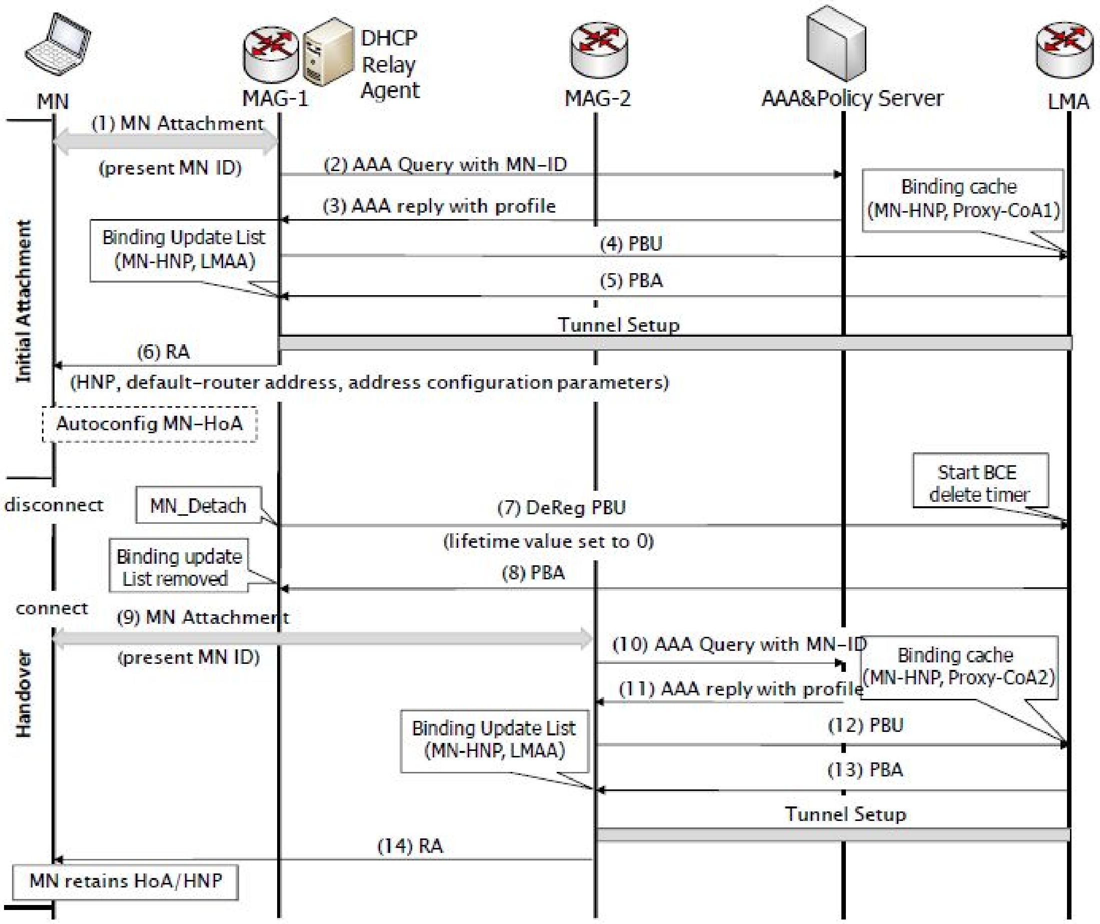
3. **Efficient use of wireless resources:** A networkbased approach should avoid tunneling overhead over a wireless link; hence, it should minimize overhead within the radio access network.

4. **Link technology agnostic:** A network-based approach should not use any wireless-link-specific information for basic routing management, and should support any type of wireless link technology.

5. **Handover performance improvement:** A network- based approach should minimize the time required for handover.

3.3 Signaling Flow of PMIPv6

PMIPv6 is designed to provide a network-based IP mobility management support to an MN in a topologically localized domain, without requiring the participation of the MN in any IP mobility related signaling. The core functional components are used to support mobility in PMIPv6 are the PS, LMA, and MAG. The PS is the entity that manages the MNs authentication and maintains the MNs profile which is a set of parameters configured for a given MN. The LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6. The main role of the LMA is to maintain reachability to the MNs address while the MNmoves around within a PMIPv6 domain. The LMA includes a Binding Cache Entry (BCE) for each currently registered MN. The MAG typically runs on



the Access Router (AR). The main role of the MAG is to detect the MNs movement and sends mobility-related signaling to the MNs LMA on behalf of the MN.

In addition, the MAG establishes a tunnel with the LMA for packet transmission. The MAG ensures that an MN can obtain address from its HNP and move anywhere within the PMIPv6 domain. Therefore, the MN believes it is using the same link obtained with its initial address configuration, even after changing its point of attachment within the network.

Fig. 1 shows the signaling flow of the overall operations in PMIPv6; the steps involved in the initial attachment and handover procedure are described as follows:

1. **Steps 1, 2, and 3:** When a MN initially attaches to MAG-1 in a PMIPv6 domain, the access authentication procedure is performed using an MN-Identifier (MN-ID) via the deployed access security protocols on the access network. After successful access authentication, the MAG-1 obtains the MNs profile, which contains the MN-Identifier, LMA address (LMAA), supported address configuration mode.

2. **Steps 4 and 5:** To update the LMA about the current location of the MN, MAG-1

sends a Proxy Binding Update (PBU) message to the MNs LMA on behalf of the MN. Upon receiving the PBU message, the LMA assigns a MN-HNP and creates a BCE that binds the MN-HNP to a Proxy-CoA which is the address of MAG-1. The LMA also establishes a bidirectional tunnel to MAG-1. The LMA sends a Proxy Binding Acknowledgement (PBA) message including the MN-HNP.

3. **Steps 6:** Upon receiving the PBA message, MAG-1 sets up a tunnel to the LMA and adds a default route over the tunnel to the LMA. It also creates a Binding Update List (BUL) that binds the MN-HNP and LMAA. The MAG-1 then sends Router Advertisement (RA) messages to the MN on the accesslink to advertise the MN-HNP as the hosted on-link-prefix. When the MN receives these RA messages, the MN configures the IP address using either a stateful or stateless address configuration modes. After successfully completing the address configuration procedure, the MN uses this address for packet delivery.

4. **Steps 7 and 8:** When the MN moves to the access network of MAG-2, MAG-1 detects that the MN has moved away from its access link. Therefore, MAG-1 sends a DeReg PBU (DeRegistration PBU) message to the LMA with the lifetime value set to zero for de-registration. Upon receiving the PBU message with a zero lifetime value, the LMA sends a PBA message to MAG-1 and waits for a MinDelayBeforeBCEDelete amount of time, before it deletes the MNs BCE.

5. **Steps 9, 10, and 11:** When MAG-2 detects the attachment of MN, MAG-2 obtains the MN-profile using an MN-ID after successful access authentication. These steps are same with Steps 1, 2, and 3.

6. **Steps 12, 13, and 14:** To update the LMA about the current location of the MN, MAG-2 sends a PBU message to the MNs LMA on behalf of the MN. Within MinDelayBeforeBCEDelete wait period, if the LMA then receives a PBU message for the same MN from the MAG-2 with a lifetime value greater than zero, and if that request is accepted, the Binding Cache entry is not deleted, but rather updated with a new value, which is the address of MAG-2 (Proxy-CoA2). Otherwise the LMA deletes the MNs Binding Cache entry and removes the routing state for the MN-HNP. After updating the BCE, the LMA sends a PBA to MAG-2, MAG-2 then sends RA messages

to the MN with its MN-HNP. Upon receiving the RA message, the MN believes it is still on the home link.

Unlike MIPv6, a tunnel in PMIPv6 is established between the LMA and the MAG, and not the MN. Plus, as the tunnel between the LMA and the MAG is typically a shared tunnel, it can be used for routing traffic streams for different MNs attached to the same MAG. This shared tunnel also reduces the network and signaling overhead. After bidirectional tunnel is successfully set up, all traffic sent from the MN gets routed to its LMA through the tunnel. The LMA forwards the received packet from the CN to the MAG through the tunnel. After receiving the packets, the MAG on the other end of the tunnel removesthe outer header and forwards the packets to the MN.

3.4 Tunneling and Forwarding

A bidirectional tunnel must be used to route the mobile node's traffic between the LMA and the MAG. The tunnel enables mobility because it allows the MAG to be located anywhere. It can be shared for multiple mobile nodes sharing the same MAG and LMA. The details of how tunnels are managed are left to the implementation. The tunnel must use IPv6-in-IPv6 encapsulation or IPv6-in-IPv4 encapsulation [45].

To receive packets sent for the mobile node's network prefixes, the LMA must be able to advertise the specfic route(s) in the routing infrastructure, so that other routers known where to forward the mobile node's traffic. This can be achieve with static routes or routing protocols such as OSPF, BGP and RIP. However, the specifics of this are outside the scope of the PMIPv6 specification.

Finally, the LMA must setup route entries to forward the traffic destined to the mobile node through the bidirectional tunnel. And the MAG must setup route entries to forward the traffic from the tunnel to the mobile node and to forward the traffic from the mobile node to the bidirectional tunnel.

3.5 Mobile Node's Policy Store

A mobile node's policy profile contains the required information to manage the mobile node mobility service. At least the mobile node identfier and LMA address must be part of the policy profile. An optional field for the policy profile is the mobile node prefix(es). The policy profile may also contain other fields that configure other parameters such as: home network prefix(es) lifetime, supported address configuration mechanisms, authorized access link technologies.The policy profiles are stored on a policy store and must be accessible to the MAG and the LMA, the details of this are left to the implementations. It can be defined as [AAA] server - Authentication, Authorization and Accounting.

CHAPTER 4
COMPARISON BETWEEN DIFFERENT PROTOCOLS

4.1 Comparison between MIPv6 and PMIPv6

In this section we qualitatively investigate PMIPv6 based on various evaluation criteria and compare it with various existing well-known mobility support protocols as well as MIPv6. A synopsis of the main characteristics, including the strong and weak points of PMIPv6 compared to the various existing well-known mobility support protocols.

4.1.1 MIPv6 vs PMIPv6

We first compare MIPv6 and PMIPv6 in terms of some high-level characteristics and performance aspects, which are shown in Table.

1. MIPv6 is a host-based solution for handling the global mobility of hosts in IPv6 networks. This means that a host is involved in mobility-related signaling; thus, a modification of the host protocol stack is required for operating MIPv6 (i.e., an MN sends the BU message for location registration).

   In contrast, PMIPv6 provides a network- based solution for handling the localized mobility of hosts in IPv6 networks (i.e., a network entity, the MAG, sends the PBU message for location registration). Therefore, no requirement of the hosts is needed. Moreover, PMIPv6 can also support IPv4 as well as IPv6 by specifying some extensions for supporting the IPv4 tunneling mechanism and specific encapsulation modes.

2. Basically, PMIPv6 attempts to reuse MIPv6 because MIPv6 is a considerably mature protocol with several implementations that have been realized through interoperability testing.

   Thus, the functionality of the LMA in PMIPv6 can be considered as an enhanced HA with additional capabilities.

Table 4.1: Comparison between MIPv6 and PMIPv6

Characteristics	**MIPv6**	**PMIPv6**
Mobility management type	Host-based mobility management	Network-based mobility management
Scope of mobility	Global mobility	Localized mobility
Modification of MN	Yes	No
MN address	HoA or CoA	HoA (alwayes in a LMD)
Functionally correspondent entity	HA	LMA (i.e., HA functionality with additional capabilities)
Topologically correspondent entity	AR	MAG
Location registration message	Binding update message	Proxy binding update message
Acknowledgment message	Binding Acknowlwdgment message	Proxy binding Acknowlwdgment message
Tunneling over wireless link	Required	Not required
Router advertisement type	Broadcast	Unicast
Lookup key in binding cache	HoA	MN identifier
Relation between tunnel and binding cache entry	1:1 relation (i.e., HA-MN tunnel)	1:m relation (i.e., LMA-MAG tunnel)
Addressing model	Shared-prefix model	Per-MN-prefix model
Supported link type	Any type of link	Point-to-point link
Route optimization	Supported	Not supported
Return routability	Required	Not required
Movement detection	Required (performed by RS/RA)	Not required (performed by layer 2)
Duplicate address detection (DAD)	Performed at every subnet movement	Performed only one time (at initial movement into the domain)

3. In MIPv6 a bidirectional tunnel is established between the HA and each MN, whereas a bidirectional tunnel in PMIPv6 is established between the LMA and MAG, not each MN. This is because the MN is not involved in any type of mobility-related signaling.

4. As in MIPv4 , the bidirectional tunnel between the LMA and MAG is typically a shared tunnel, and can be employed for routing traffic streams for different MNs attached to the same MAG. It extends the 1:1 relation between a tunnel and an MNs binding cache entry to a 1:m relation, reflecting the shared nature of the tunnel.

5. MIPv6 employs the shared-prefix model in which multiple MNs in the same subnet are configured with a common IPv6 network prefix. In contrast, PMIPv6 employs the per-MN-prefix model.

6. Hence, a unique home network prefix is assigned to each MN, and no other MN shares this prefix. Therefore, the prefix follows the MN while the MN moves within a PMIPv6 domain, so the network layer movement detection and duplicate address detection (DAD) processes are not required within a PMIPv6 domain (note that for inter-PMIPv6 domain movement, network layer movement detection and DAD are performed).

   In contrast, for MIPv6, movement detection and DAD, which are time-consuming operations that can degrade handover performance significantly, are essential during every subnet movement.

   With regard to some aspects such as movement detection, DAD, and return routability, it can easily be deduced that PMIPv6 is superior to MIPv6.

7. For route optimization, PMIPv6 does not have a corresponding capability. In PMIPv6 an individual RA message should be unicast to the MN because PMIPv6 only supports the per-MN-prefix model.

   However, MIPv6 supports the sharedprefix model; thus, the RA message is broadcast in the same network.

8. The choice of the per-MN-prefix model in PMIPv6 conflicts with the use of a shared link layer (e.g., Ethernet, IEEE 802.11) as the last hop in a PMIPv6 domain. Hence, the type of supported link in PMIPv6 is simply point-to-point

4.2 Drawbacks of PMIPv6

- **No route optimization**

  MIPv6 supports route optimization which allows the CN to send packets directly to the MH, bypassing the HA. To enable route optimization in Mobile IPv6, the MH has to send binding update to the CN. On the other hand, Proxy MIPv6 does not support route optimization; all the CN traffic must go through the LMA which is the topological anchor point of the MH in the localized mobility domain. Therefore, signaling requirement on the LMA can be higher depending on the number of MHs in the LMA-domain, which may results in performance degradtion.

- **Localized mobility management only**

  Proxy Mobile IPv6 is not a global management protocol. Rather it is a localized mobility solution. The MH must be registered to get PMIPv6-support in a PMIP-domain. When the MH moves out of the PMIPv6-domain, it must get mobility support from a global mobility solution, such as, Mobile IPv6. Although PMIPv6 relieves the MN from mobility related signaling causing less signal overhead, the protocol has some significant drawbacks like the protocol suffers from packet loss during handover, It suffers from handover delay or latency which may cause serious distortions in video or sound signal during handover and it is limited to intra-domain handover.

- **Resource restriction**

  Mobility management entities of Proxy Mobile IPv6: LMA, MAG and the MH. The LMA and MAG two key components of PMIP6 are very resource restricted. Thus, overloading these entities may result in complete outage for the whole system.

CHAPTER 5
HANDOVER OF PROXY MIPV6

5.1 Handover

A handover is a process in telecommunications and mobile communications in which a connected cellular call or a data session is transferred from one cell site (base station) to another without disconnecting the session. Cellular services are based on mobility and handover, allowing the user to be moved from one cell site range to another or to be switched to the nearest cell site for better performance.

Handovers are a core element in planning and deploying cellular networks. It allows users to create data sessions or connect phone calls on the move. This process keeps the calls and data sessions connected even if a user moves from one cell site to another

5.1.1 Handover Steps by Layer Basis in PMIPv6

The whole handover procedure can also be divided into two basic steps:

Layer2 Handover

Layer 2 handover can be defined as movement of a MNs point of Layer 2 connection from one wireless access point to another. The layer 2 handoff latency is measured as the time between the first probe request message sent by the mobile node and the arrival of a re-association response message from an access point. Three phases or logical steps can be identified for the layer 2 handoff process: (f1) discovery phase, (f2) re-authentication phase and (f3) reassociation phase.

Layer3 Handover

Layer3 handover process can be defined as movement of an MN between Foreign Agent (FA) or MAGs (in case of PMIPv6) which involves changing the care of address at layer3.

The layer 3 handover is decomposed into creating, verifying and registering a new address. When MN is changing its point of attachment between the MAGs then it requires a new IP address i.e. the new proxy CoA which is the IP address of the new MAG and layer 3 handover is required.

5.1.2 PMIPv6 Handover

PMIPv6 handover is one of the hot issues for research as it results in a significant amount of latency and packets loss. When MN performs a handover from one MAG to another, then the interface setup needs to take place by getting assigned a new prefix and performing optionally the DAD algorithm [11]. This is on top of having MN being authorized again. As a result, multiple IETF drafts were written to improve the efficiency of the handover. Some of the relevant and successful proposals are discussed below.

5.1.3 Fast Handover for Proxy MIPv6

Fast Handover for Proxy MIPv6 (F-PMIPv6), introduced in RFC 5949, performs an efficient handover by reducing the delay and minimizing packet loss without involving the MN in signaling to comply with the main goal of PMIPv6. This protocol is based on establishing a bidirectional tunnel between the Previous MAG (PMAG) that the MN is handing over from and the NMAG that the MN is handing over to and performing context transfer between them. Access Network is composed of Access Point as defined in [RFC 5568] and these are often referred to as base station in cellular networks. Each MAG has an AP therefore AP and MAG are often combine as one entity.

There are two modes of operation for F-PMIPv6: the predictive mode and the reactive mode. In the predictive mode, the bidirectional tunnel between the NMAG and PMAG is established prior to performing a handover. While in the reactive mode, it is established after the MN starts its handover process. In the most severe case when the MN is detached from both old link and new link, the MAGs have to have the capability of buffering the packets for future forwarding. For the predictive mode to work efficiently and to avoid the involvement of MN in the IP mobility signaling, it is required that the MN reports a lower layer information to the Access Network, which in turns, reports this information at short timing to the

PMAG.

1. **Predictive Mode**

   Figure 5.1 shows the message sequencing that happens in the predictive mode. In this mode, the MN detects that it is about to perform a handover. Therefore, it reports some low layer information to the Previous Access Network such as the MN-ID and the new AP identifier to which the MN will move. In some cases, the Previous Access Network can map the AP identifier to the New Access Network but this is an access technology specific.

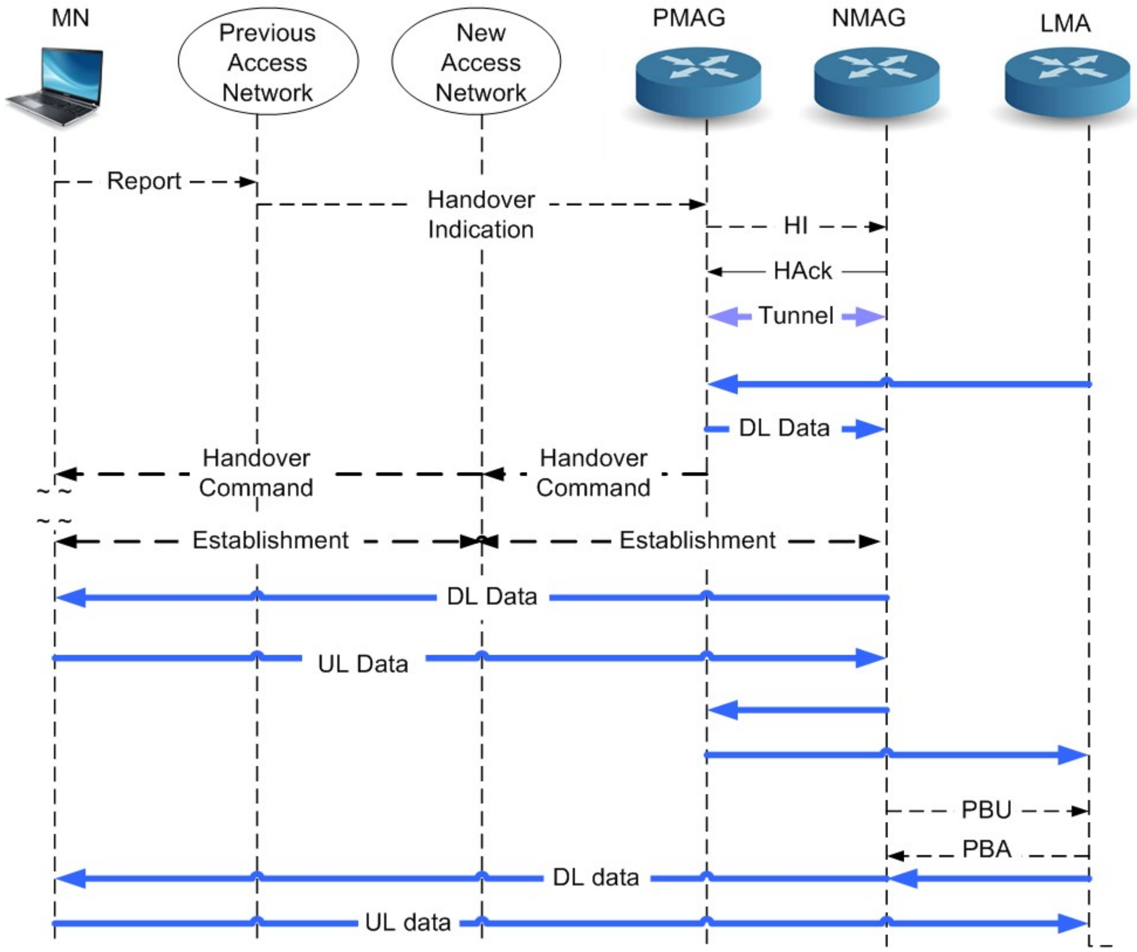


Figure 5.1: Predictive Fast Handover for PMIPv6

New Access Network sends a message to the PMAG informing it of the MN intention of performing a handover along with the MN-ID and the new AP identifier. The PMAG derives the NMAG information from the N-AP identifier and sends a Handover Initiate (HI) message to the NMAG with the Proxy flag (P) set and other relevant information that are related to this protocol. The NMAG sends a Handover

Initiate Acknowledgment (HACK) to the PMAG with the P flag set. As a result, a bidirectional tunnel is established between the PMAG and the NMAG.

Any packet that is destined to the MN and received by the PMAG can be forwarded over the tunnel to the NMAG and buffered till the MN is fully attached and handover is completed. When the handover is completed on the network side, the MN is triggered to perform handover to the new access network. Any packets that are sent from the MN are sent to the NMAG and forwarded to the PMAG before it is sent to the LMA. Once the MN completes the PMIPv6 normal handover procedure (PBU and PBA), the data packets will go through NMAG only and the tunnel is no longer needed.

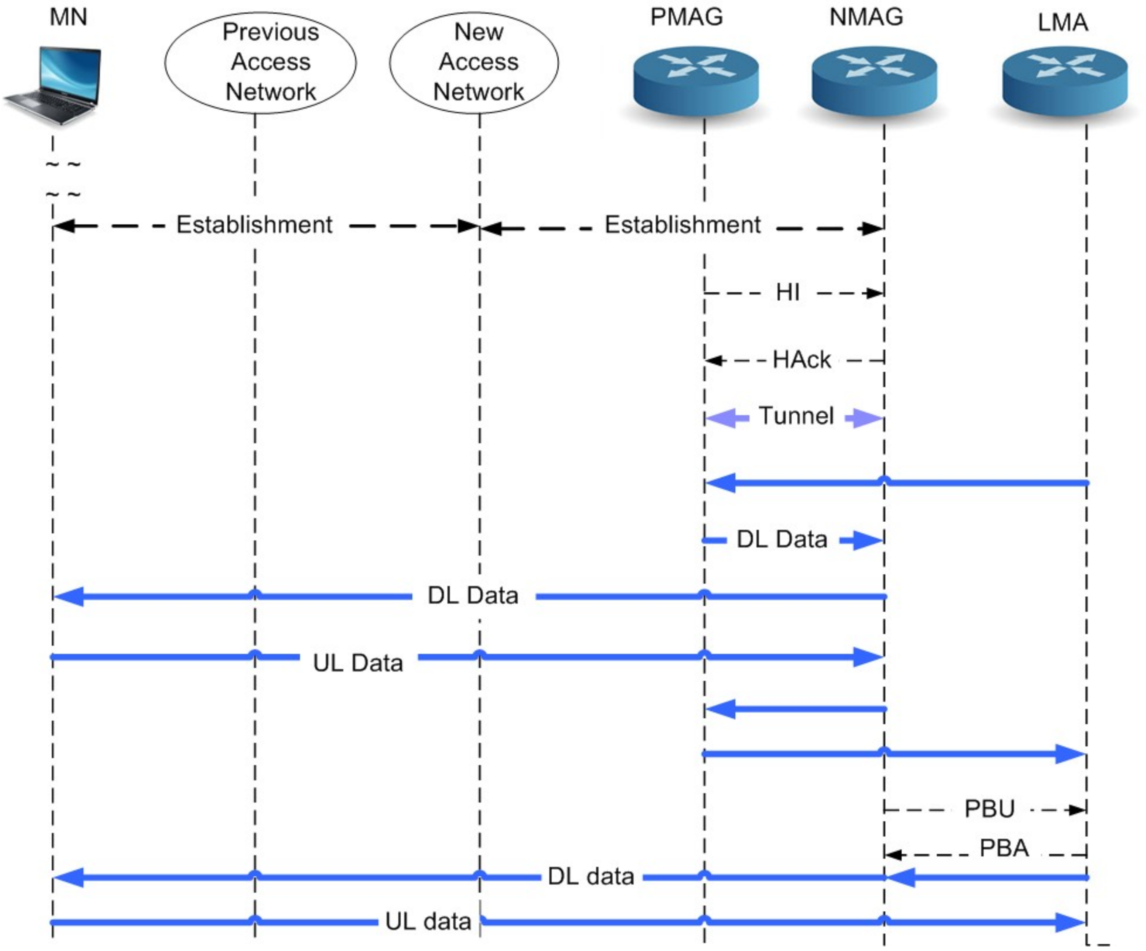


Figure 5.2: Reactive Fast Handover for PMIPv6

2. **Reactive Mode**

In the case of the reactive mode, the tunnel establishment has to come from the NMAG as the AP information is acquired only when the MN moves to the new link. The information can be provided to the NMAG either from the MN on the old link or by a means of communication between the Previous Access Network and the New Access Network. Once this information is acquired, similar procedure to the predictive mode is followed. Figure 5.2 shows this for clarification purposes.

5.2 Handover Analysis

In this section we focus on a quantitative analysis among MIPv6, HMIPv6, and PMIPv6 on handover latency, which is one of the most critical factors in next-generation all-IP mobile networks.

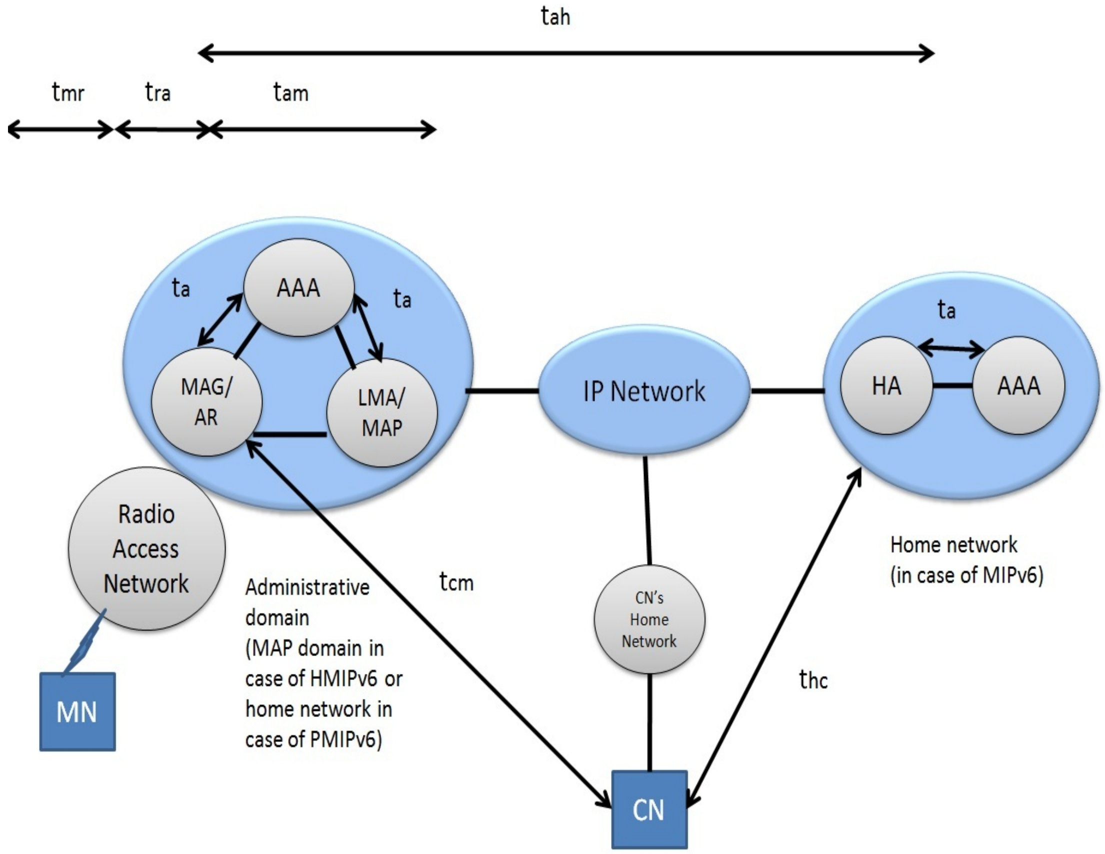

tah
tmr
tra
tam
ta
AAA
ta
MAG/ AR
LMA/ MAP
IP Network
ta
HA
AAA
Radio Access Network
MN
Administrative domain (MAP domain in case of HMIPv6 or home network in case of PMIPv6)
tcm
CN's Home Network
Home network (in case of MIPv6)
thc
CN

Figure 5.3: A simple analytical model for performance analysis

For performance analysis, we consider a simple analytical model shown in Figure 5.3. For simplicity, we make the following assumptions:

Table 5.1: Notations

Notations	Descriptions
t_{mr}	The delay between the MN and AP
t_{ra}	The delay between the AP and MAG/AR
t_{am}	The delay between the MAG/AR and LMA/MAP
t_{ah}	The delay between the AR/MAG and HA
t_{ac}	The delay between the MAG/AR and CN, which is the time required for a packet to be sent between the MAG/AR and the CN, and not via the HA
t_{hc}	The delay between the HA and CN
t_{a}	The delay between the mobility agents and AAA

- For a fair analysis of these protocols under the same network structure, the administrative domain can be applied as follows.

  1. From the perspective of MIPv6, the administrative domain is assumed to be simply a foreign network.
  2. From the perspective of HMIPv6, it is assumed to be a foreign MAP domain.
  3. Similarly, for PMIPv6, it is assumed to be a home network domain because the MN always moves around within a home network regardless of its point of attachment.

- Based on the above assumption, the mobility agents of each protocol follow the mapping scenario shown in Fig. 5.3. For example, if PMIPv6 is considered, the location of the LMA is assumed to be the same as that of the MAP in HMIPv6 because they both have functionalities similar to the HA in MIPv6 within a localized administrative domain.

- For a fair analysis, we assume that the MNs are allowed to access a serving network after the AAA procedure is completed, and these access delays are assumed to be all the same for MIPv6, HMIPv6, and PMIPv6.

- Address configuration is only performed by means of stateless address autoconfiguration, and the time required to combine the network prefix obtained from the RA message to its interface is negligible in the case of address configuration delay.

- All the delays mentioned above are symmetric.
- The delay between the MN and CN is shorter than the sum of the delays between the MN and HA and between the HA and CN.
- For simplicity, router solicitation (RS) messages are not considered here. Thus, only RA messages can affect the movement detection of the MN.

Handover latency calculation

Let, The movement detection delay = T_{MD}

Address configuration delay = T_{DAD}

The delay involved in performing the AAA procedure = T_{AAA}

location registration delay = T_{REG}

Generally, IP handover latency = $T_{MD} + T_{DAD} + T_{AAA} + T_{REG}$

In this thesis, more specifically, handover latency is defined as the time that elapses between the moment the layer 2 handover completes and the moment the MN can receive the first data packet after moving to the new point of attachment.

In order to estimate the movement detection delay, based on the above assumptions, we only consider the delay caused by the reception of an unsolicited RA message without considering an RS message. Therefore, in this case the movement detection delay depends on the period of the RA message. In [1] it is specified that the routers for supporting mobility should be able to be configured with a smaller *MinRtrAdvInterval (= MinInt)* value and *MaxRtrAdvInterval (= MaxInt)* value in order to allow sending unsolicited RA messages more often.

The mean time between unsolicited RA messages can be expressed as *(MinInt + MaxInt)/2*. Therefore, for simplicity, we assume that the mean value of movement detection delay T_{MD} in MIPv6 and HMIPv6 is half of the mean time between unsolicited RA messages, thus, T_{MD} = *(MinInt + MaxInt)/4.*

After an MN detects network layer movement, new prefix information of the network (or subnet) becomes available to the MN. From the prefix information, a new CoA is generated by means of IPv6 stateless (or stateful) address autoconfiguration. In order to verify the uniqueness of this CoA, it performs the DAD process before combining the network prefix to its interface. During this process, the MN cannot use the CoA for communication. Therefore, according to [12], the DAD delay in MIPv6 and HMIPv6 can be simply expressed as TDAD = R D, where R and D denote RetransTimer and DupAddrDetectTransmits specified in [6], respectively.

From the perspective of network service providers, in order to make mobile services feasible in public wireless Internet, AAA functions performed by AAA protocols such as DIAMETER must be implemented. Based on the above assumption, these access delays (T_{AAA}) are all the same; thus, T_{AAA} = 2 x $2t_a = 4t_a$ for the three protocols (i.e., one access is performed between AR/MAG and AAA, the other between HA/MAP/LMA and AAA).

Handover latency of MIPv6

The registration delay in MIPv6 (T_{REG}^{MIPv6}) requires the time equivalent to the sum of the HA registration delay (i.e., $2(t_{mr} + t_{ra} + t_{ah})$) and the CN registration delay (i.e., $2(t_{mr} + t_{ra} + t_{ac})$). Moreover, in order to register with the CN, the delay for return routability (i.e., $2(t_{mr} + t_{ra} + t_{ah} + t_{hc})$) is additionally required prior to the CN registration. Therefore, including all the factors mentioned above, the handover latency in MIPv6 (D_{HO}^{MIPv6}) can be expressed as follows:

$$D_{HO}^{MIPv6} = T_{MD} + T_{DAD} + T_{AAA} + T_{REG}^{MIPv6}$$

$$\text{where } T_{REG}^{MIPv6} = 6(t_{mr} + t_{ra}) + 4t_{ah} + 2(t_{ac} + t_{hc})$$

Handover latency of HMIPv6

Unlike MIPv6, the registration delay in HMIPv6 (T_{REG}^{HMIPv6}) only requires the MAP registration delay (i.e., $2(t_{mr} + t_{ra} + t_{am})$). without the requirement of the CN registration delay within a MAP domain. This is because the MNs movement within a MAP domain is transparent outside of the MAP domain. Therefore, including all the factors mentioned above, the handover latency in HMIPv6 (D_{HO}^{HMIPv6}) within a MAP domain can be expressed as follows:

$$D_{HO}^{HMIPv6} = T_{MD} + T_{DAD} + T_{AAA} + T_{REG}^{HMIPv6}$$

$$\text{where } T_{REG}^{HMIPv6} = 2(t_{mr} + t_{ra} + t_{am})$$

Handover latency of PMIPv6

Unlike MIPv6 and HMIPv6, PMIPv6 does not require movement detection and DAD except when the MN first enters a PMIPv6 domain. In addition, the MNs movement within a PMIPv6 domain is also transparent outside of the PMIPv6 domain because PMIPv6 is a localized mobility management protocol similar to HMIPv6. Therefore, the handover latency in PMIPv6 can be composed of the sum of the AAA access delay (T_{AAA}), the registration delay between the MAG and LMA (T_{REG}^{PMIPv6}), and the packet transmission delay from the MAG to the MN (i.e., $(t_{mr} + t_{ra})$). Finally, the handover latency in PMIPv6 (DHO PMIPv6) within a PMIPv6 domain can be simply expressed as follows:

$$D_{HO}^{PMIPv6} = T_{AAA} + T_{REG}^{PMIPv6} + t_{mr} + t_{ra}$$

$$\text{where } T_{REG}^{PMIPv6} = 2t_{am}$$

From above calculation, we can mention the following results:

- **Influence of Wireless link delay**

  For all of the mobility support protocols, it can be observed that handover latencies increase with the wireless link delay. MIPv6 is most affected by the change in wireless link delay because it requires the largest number of messages (e.g., the message exchanges for the BU or binding acknowledgment (BA) to/from the HA, the return routability procedure, and the BU for the CN) to be exchanged over the wireless link.

  In contrast, PMIPv6 is least affected because the MN is not involved in mobility-related signaling. In particular, it must be noted that the handover latencies of MIPv6 and HMIPv6 based on RFC 2462 are significantly larger than that of PMIPv6. This is because the time required for the DAD2.3 process in MIPv6 and HMIPv6 is considerably larger than the delays caused by other factors that may affect handover latency. As mentioned earlier, the DAD process is very time consuming.

- **Influence of Delay between MN and CN**

  The impact of $(t_{mr} + t_{ra} + t_{ac})$ on handover latency. Since we evaluate handover latency only for intradomain movement, HMIPv6 and PMIPv6 do not require registration to the CN because the MNs movement within a domain is transparent outside the domain. That is, the delay between the MN and CN does not affect the handover latency of each protocol within a domain. However, for MIPv6, the handover latency increases with the delay between the MN and CN. This is because MIPv6 requires registration to both the HA and CN whenever the MN moves across subnets; thus, the increase in the delay between the MN and CN affects the increase in handover latency in MIPv6.

- **Influnce of Movement Detection Delay**

  The impact of T_{MD} on handover latency. As mentioned earlier, in PMIPv6 movement detection does not occur except when the MN moves across a PMIPv6 domain. This is due to the fact that since PMIPv6 only supports the per-MN-prefix model, a unique home network prefix is assigned to each MN. That is, from the perspective of the MN, the entire PMIPv6 domain appears as its home network. In other words, the MN is not related to movement detection delay in intradomain movement. On the contrary, the graphs for MIPv6 and HMIPv6 increase with the same slope as the movement detection delay does. In MIPv6 and HMIPv6, whenever the MN moves across subnets, it configures the different CoAs via stateless (or stateful) address autoconfiguration. Therefore, in MIPv6 and HMIPv6, movement detection should be performed as quickly as possible in order to minimize handover latency and packet loss. Increased movement detection delay results in increased handover latency, and this could cause significant degradation to be experienced by the MNs.

CHAPTER 6
CONCLUSION

Mobile IP is designed to allow mobile users to move from one network to another while maintaining a permanent IP address. IP defines the format of packets and provides an addressing which has two functions: identifying hosts and providing a logical location service. MIPv4 is the dominant protocol of internet. The terminology, the architectural entities and operational principles of MIPv4 have been discussed in this thesis. MIPv6 is the successor of MIPv4. We have discussed the components, messages and options and functional principle of MIPv6 and HMIPv6.

MIPv4 and MIPv6 both are host-based mobility protocols. They require mobile devices to participate in mobility signaling that consumes lots of processing power and memory. On the other hand, PMIPv6 is a network-based mobility protocol and solves this problem by excluding low-end mobile devices from signaling requirement. PMIPv6 also reflects telecommunication operators favor, enabling them to manage and control their networks more efficiently.

In this thesis, we have explained the architecture of PMIPv6 with its detailed signaling diagram. We have compared PMIPv6 with MIPv6 in term of some characteristics and performance aspects and identified some drawbacks of PMIPv6. Then we have explained the handover of PMIPv6 and also discussed about Fast Handover for PMIPv6 with signaling diagram.

We discussed about an analytical model to analyze the handover of PMIPv6. The handover latency calculation has been done on some assumptions such as movement detection delay, address configuration delay etc. Finally the results show that PMIPv6 has better handover performance than MIPv6 and HMIPv6.

The interactions between MIPv6 and PMIPv6 would also be possible. For example, similar to the HMIPv6- MIPv6 interaction, PMIPv6 could be used as a localized mobility management protocol, where as MIPv6 could be used as a global mobility management protocol. Future research will explore cross layering issues (e.g., PMIPv6 over IEEE 802.11 or 802.16e networks) as well as route optimization and fast handover issues in PMIPv6.

REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko, “Mobility support in ipv6,” IETF RFC 3775, JUNE 2004.

[2] J. Kempf, “Goals for network-based localized mobility management (netlmm,” IETF RFC 4831, APRIL 2007.

[3] S. G. (Ed.), V. D. K. Leung, K. Chowdhury, and B. Patil, “Proxy mobile ipv6,” IETF RFC 2008, August 2008.

[4] C. Perkins, “Ip mobility support,” IETF RFC 2002, October 1996.

[5] T. Narten, E. Nordmark, and W. Simpson, “Neighbor discovery for ip version 6 (ipv6),” IETF RFC 2461, December 1998.

[6] S. Thomson and T. Narten, “Ipv6 stateless address autoconfiguration,” IETF RFC 2462, December 1998.

[7] S. Derring and R. Hinden, “Internet protocol, version 6 (ipv6) spcification,” IETF RFC 2460, December 1998.

[8] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, “Hierarchical mobile ipv6 (hmipv6) mobility management,” IETF RFC 5380, OCTOBER 2008.

[9] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, “Hierarchical mobile ipv6 (hmipv6) mobility management,” IETF RFC 4140, MARCH 1999.

[10] C. Perkins, “Ip mobility support for ipv4,” IETF RFC 3344, August 2002.

[11] N. Moore, “Optimistic duplicate address detection,” IETF RFC 4429, APRIL 2006.

[12] Y. Han, J. Choi, and S. Hwang, “Reactive handover optimization in ipv6-based mobile networks,” *IEEE JSAC*, vol. 24, no. 9, p. 175872, Sept 2006.

[13] H. Soliman and G. Giaretta, “Interactions between pmipv6 and mipv6: Scenarios and related issues,” IETF Internet draft, draft-giaretta-netlmm-mip-interactions- 00, APRIL 2007.