Universidad Carlos III de Madrid

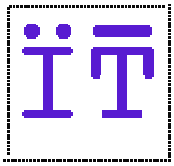
Ingeniería de Telecomunicación

Proyecto Fin de Carrera

Estudio de la Movilidad en Redes de Siguiente Generación

Cristina Rodríguez Gallego

Diciembre de 2009



Universidad Carlos III de Madrid

Ingeniería de Telecomunicación

Proyecto Fin de Carrera

Estudio de la Movilidad en Redes de Siguiente Generación

Autora: Cristina Rodríguez Gallego

Tutor: Dr. José Ignacio Moreno Novella

Diciembre de 2009

Departamento de Ingeniería Telemática

PROYECTO FIN DE CARRERA

Departamento de Ingeniería Telemática

Universidad Carlos III de Madrid

Título: Estudio de la Movilidad en Redes de Siguiente Generación

Autor: Cristina Rodríguez Gallego

Tutor: Dr. José Ignacio Moreno Novella

La lectura y defensa del presente proyecto fin de carrera se realizó el día 14 de Diciembre de 2009 bajo el tribunal:

Presidente: Carlos García Rubio

Vocal: Fernando García Fernández

Secretario: Iván Vidal Fernández

Habiendo obtenido la calificación de:

Presidente **Vocal** **Secretario**

Dedicado a mis padres y hermana: Paqui, Eleuterio y Beatriz.

AGRADECIMIENTOS

En primer lugar me gustaría darle las gracias a mi familia, por el apoyo y la comprensión que me prestan cada día. Sin su ayuda no habría sido posible alcanzar cada una de las metas que me he ido marcando durante estos años, ni tampoco me vería capaz de poder alcanzar las siguientes. Siempre me han recordado y recuerdan día tras día lo importante que es la confianza y el afán de superación de uno mismo, sin olvidar nunca el respeto hacia los que me rodean.

También quiero agradecer a mi tutor, José Ignacio Moreno, toda la ayuda prestada y sus numerosos consejos, tanto durante mi estancia en Berlín, como en Madrid, mostrándose siempre paciente y dispuesto ayudarme en todo momento.

Por supuesto, darle las gracias a todos mis amigos y compañeros de la universidad, con los que he compartido muchas vivencias y me han ayudado a alcanzar esta meta que, en ocasiones, parecía imposible alcanzar.

Y por último y no menos importante, quiero darle las gracias a José, por su paciencia y su apoyo incondicional.

RESUMEN

El continuo avance de las redes de telecomunicaciones nos proporciona cada vez más facilidades en todos los ámbitos de nuestra vida. En este caso, nos hemos centrado en el estudio de la movilidad en Redes de Siguiente Generación.

Una parte del presente proyecto se ha realizado en colaboración con Deutsche Telekom AG, durante una estancia de seis meses trabajando como colaboradora en sus laboratorios con emplazamiento en Berlín.

El principal objetivo de este proyecto ha sido realizar un estudio sobre los diferentes estándares y tecnologías que facilitan la movilidad en Redes de Siguiente Generación. Por ello, en la primera parte se han estudiado los diferentes grupos de trabajo centrados en este aspecto, así como se ha recabado información sobre productos y soluciones disponibles en el mercado, para obtener una visión global de la situación actual.

Como se puede comprobar más adelante, esta primera parte es la más extensa de todo el documento. Esto se debe a que es, probablemente, la parte más importante del trabajo, ya que contiene el estudio de los mecanismos que más tarde nos servirán para dar una solución teórica a los distintos escenarios que se plantean.

En la segunda parte del proyecto, nos hemos centrado en desarrollar varios escenarios de interés en sistemas de Redes de Siguiente Generación y aportar, de forma posterior, posibles soluciones teóricas.

Para finalizar, se han expuesto las conclusiones extraídas como resultado del trabajo y los aspectos que se podrán tratar sobre el mismo en un futuro próximo.

Tabla de contenido

Índice de figuras

Índice de tablas

CAPÍTULO 1

INTRODUCCIÓN Y OBJETIVOS

1.1 Motivación

Si nos detenemos a analizar el cambio que ha experimentado tanto la sociedad como la forma de vida en las últimas décadas, nos daremos cuenta de que el avance de las comunicaciones ha sido uno de los principales detonantes.

De hecho, en los últimos años las comunicaciones inalámbricas han experimentado un crecimiento sin precedentes, ganando más y más popularidad conforme sus prestaciones aumentan y se desarrollan nuevas aplicaciones para este tipo de redes.

Las redes inalámbricas permiten a sus usuarios acceder a la información y a los recursos disponibles en tiempo real y sin necesidad de estar físicamente conectados mediante un cable a un determinado lugar. Lo que es más, uno de los objetivos principales que condujo al desarrollo de las redes inalámbricas, fue facilitar a los usuarios un sistema de comunicaciones más flexible, permitiéndoles elegir dónde comunicarse.

El siguiente reto que se planteó fue la evolución de la infraestructura de redes de telecomunicación y acceso telefónico para lograr la congruencia de los nuevos servicios multimedia (voz, datos, video, etc.) permitiendo así a los usuarios comunicarse mientras cambiaban de localización, sin que las prestaciones de sus comunicaciones se vieran alteradas. Es en este punto donde surge el concepto de Redes de Siguiente Generación, o redes NGN (Next Generation Network).

Según la ITU-T, una Red de Siguiente Generación es una red basada en la transmisión de paquetes capaz de proveer servicios integrados, incluyendo los tradicionales telefónicos, y capaz de explotar al máximo el ancho de banda del canal haciendo uso de las tecnologías de calidad de servicio de modo que el transporte sea totalmente independiente de la infraestructura de red utilizada. Además, ofrece acceso libre para usuarios de diferentes compañías telefónicas y apoya la movilidad que permite acceso multipunto a los usuarios.

Desde el punto de vista más práctico, las Redes de Siguiente Generación suponen tres cambios fundamentales en la arquitectura de red tradicional que han de ser evaluados de forma independiente.

Respecto al núcleo de red, NGN supone la consolidación de varias redes de transporte construidas históricamente a partir de diferentes servicios individuales. También implica la migración del servicio de voz desde la tradicional arquitectura conmutada (PSTN) a la nueva VoIP, además de la sustitución de las redes tradicionales como X.25 o Frame Relay. Esto supone incluso una migración para el usuario tradicional hacia un nuevo servicio como es el IP VPN o la transformación técnica de las redes tradicionales.

Respecto a las redes de acceso, las Redes de Siguiente Generación suponen la migración del canal tradicional dual de voz y datos asociado a las redes xDSL hacia instalaciones convergentes en las que las DSLAMs integren puertos de voz o VoIP, permitiendo de esta forma dejar atrás las actuales redes conmutadas que multiplexan voz y datos por diferentes canales.

Respecto a las redes cableadas, la convergencia NGN implica la migración de la tasa constante de flujo de bits a estándares CableLabs PacketCable que suministren servicios VoIP y SIP. Ambos servicios funcionan sobre DOCSIS como estándar para el cableado.

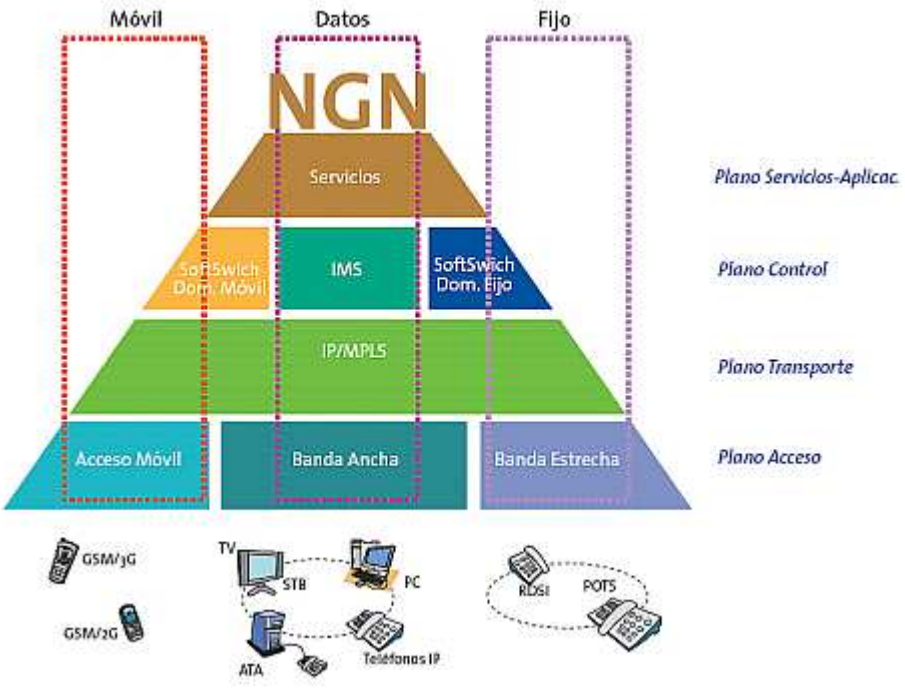


Figura 1: Conjunto de elementos funcionales que configuran el plano de control del modelo de referencia NGN

En las Redes de Siguiente Generación existe una separación bien definida entre la red de transporte y los servicios que corren por encima de esa red. Esto quiere decir que siempre que un proveedor telefónico desee habilitar un nuevo servicio, puede hacerlo fácilmente definiéndolo desde la capa de servicio directamente sin tener en cuenta la capa de transporte. Como se ha dicho, los servicios

proporcionados serán independientes de la infraestructura de red. La tendencia actual es que estos servicios, incluyendo la voz, se inclinen hacia la independencia de red y normalmente residan en los dispositivos de usuario (teléfono, PC, receptores TDT,...) [1]

Una vez presentado el entorno que motivó la realización de este estudio, presentamos los objetivos marcados dentro del mismo en el siguiente punto.

1.2 Objetivos

En la presente memoria se expone el trabajo de investigación realizado durante la estancia Erasmus-Placement en Deutsche Telekom AG Laboratories. Dicho trabajo se llevó a cabo durante un periodo de seis meses en la ciudad de Berlín, entre los meses de abril y octubre de 2009.

El objetivo general del proyecto es realizar un estudio sobre la movilidad en Redes de Siguiente Generación, estudiando los mecanismos actualmente disponibles y los que están en desarrollo, para poder dar solución a los escenarios posteriormente planteados.

Debido a que el trabajo se desarrolló en Berlín bajo un programa internacional, el estudio tuvo que realizarse en inglés. Por ello, y para no desvirtuar los documentos resultado de las tareas de investigación, se incluyen en la memoria en la versión original.

Por otra parte, los objetivos del estudio están recogidos dentro del programa de prácticas denominado Extended Mobility (ExMob), y se detallan a continuación:

- Análisis del Estado del Arte en Tecnologías Móviles
- Identificación de escenarios
- Propuesta de soluciones para los distintos escenarios
- Discusión de casos de uso y otras colaboraciones con Fixed-Mobile Convergence Alliance (FMCA)
- Preparación de informes y publicaciones
- Presentación final de actividades

En este punto nos detendremos para explicar brevemente en qué consiste Fixed-Mobile Convergence Alliance.

Fixed-Mobile Convergence Alliance se formó a mediados del año 2004, como una organización global sin ánimo de lucro. Dicha alianza trabaja con sus miembros para proporcionar una plataforma común de aprendizaje, para facilitar el desarrollo y la disponibilidad de productos de convergencia fáciles de usar y de gran calidad para los clientes del presente y del futuro. FMCA fue incorporada como una asociación sin ánimo de lucro bajo la ley de Nueva York en agosto de 2006.

La Alianza se beneficia de una creciente comunidad de miembros formada por los veinte operadores de telecomunicaciones líderes a escala global, la mayoría de los cuales son operadores propietarios de redes tanto fijas como móviles.

Vendor Affiliation Programme también pone de manifiesto que los operadores pueden trabajar estrechamente con los miembros asociados, que son todos ellos proveedores de telecomunicaciones.

La alianza fue fundada por seis compañías: British Telecom, NTT, Rogers Wireless, Brasil Telecom, Korea Telecom y Swisscom. El propósito de esta alianza es fomentar la integración *seamless* de los servicios telefónicos móviles y fijos. Es lo que se denomina como convergencia tecnológica.

Su sede global de operadores líderes, representa a más de 500 millones de clientes, o un tercio de los usuarios de telecomunicaciones del mundo, y colabora con proveedores miembro hacia el desarrollo y la disponibilidad de productos y servicios de convergencia en áreas tales como dispositivos, puntos de acceso y home gateways, roaming y aplicaciones innovadoras.

Para lograr sus metas, la FMCA ha desarrollado estrechas relaciones con organizaciones de desarrollo, especificación y certificación de estándares (Standards Development, Specification & Certification Organizations, SDO/Fora), incluyendo Wi-Fi Alliance, Wireless Broadband Alliance, Home Gateway Initiative y 3GPP. La FMCA contribuye activamente hacia la difusión de los estándares existentes y emergentes, que son relevantes para los requerimientos de los productos y servicios de FMCA.

Sin embargo, debe ser resaltado que la FMCA no es una organización de desarrollo de estándares. Por ello, la alianza no está orientada a la creación de estándares pero sí a acelerar la adopción de las tecnologías de convergencia.

1.3 Fases de realización

En este apartado se explican las diferentes tareas y objetivos parciales que se han desarrollado para la consecución de los objetivos explicados en el apartado anterior.

En primer lugar, y debido a que, fundamentalmente, el trabajo planteado se basa en un estudio teórico sobre la movilidad en redes de siguiente generación, se ha considerado imprescindible realizar un estudio exhaustivo sobre los diferentes grupos de trabajo centrados en nuestro tema de interés.

Una vez finalizado este primer estudio, se procedió a la búsqueda de proyectos, soluciones y productos de diferentes organismos, proveedores y operadores, que resolvieran aspectos apoyados en la movilidad de usuario en Redes de Siguiente Generación.

La tercera fase está comprendida por la elaboración de cuatro casos de uso basados en escenarios de interés en sistemas de Redes de Siguiente Generación. Dichos casos de uso tuvieron que ser planteados y redactados en primer lugar. Una vez planteados se procedió a su publicación en la *Wiki* de Fixed-Mobile Convergente Alliance (http://usecases.thefmca.com), para su posterior discusión con los diferentes miembros que componen la alianza. Una vez discutidos y modificados cuando procediera, se pasó al planteamiento de una solución teórica para cada uno de ellos.

Tras la realización de estas tareas, se prepararon una serie de informes conteniendo la información recabada durante el estudio y los casos de uso con sus soluciones propuestas.

Por último, se preparó una presentación final resumiendo el trabajo realizado durante el periodo de prácticas.

1.4 Estructura de la memoria

El **primer capítulo** de la memoria consiste en una introducción, donde se exponen las motivaciones y los objetivos que conducen a la realización del presente proyecto. Además, se explican las diferentes partes de las que se compone el documento.

El **segundo capítulo** contiene un estudio de todos los estándares y grupos de trabajo cuyo fundamento se basa en el desarrollo de la movilidad tanto de red como de usuario en Redes de Siguiente Generación. Una vez expuesto dicho estudio, se explican los proyectos, productos y soluciones que han sido desarrollados por diferentes instituciones, así como proveedores y operadores de telefonía móvil.

Como se puede comprobar más adelante, este capítulo es el más extenso de todo el documento. Esto se debe a que es, probablemente, la parte más importante del trabajo, ya que contiene el estudio de los mecanismos que de forma posterior nos servirán para dar una solución teórica a los distintos escenarios que se plantean.

El siguiente capítulo, el **capítulo tercero**, contiene la descripción de los casos de uso que se han elaborado para resolver situaciones relacionadas con la movilidad en Redes de Siguiente Generación. Estos escenarios son planteados tras la realización del estudio previo sobre los mecanismos existentes, para proponer, en una etapa posterior, una serie de soluciones teóricas para cada uno de ellos.

Por otra parte, es en el **cuarto capítulo** donde se exponen las conclusiones que derivan de la realización del estudio y las posibles líneas de trabajo futuras que pueden desarrollarse a partir de este proyecto.

El **apéndice A** es el que contiene el presupuesto del proyecto. Es aquí donde se puede ver un diagrama de Gantt que describe el tiempo dedicado a la realización de cada una de las fases, así como los recursos utilizados. Por otra parte, aparecen los costes de personal, de material y los totales que suponen el desarrollo del proyecto.

Para finalizar, el **apéndice B** muestra el procedimiento a seguir para cada tipo de handover empleando el estándar IEEE 802.21, así como una serie de ejemplos de handover entre diferentes tecnologías como 802.11 y 802.16.

CAPÍTULO 2

ESTADO DEL ARTE

2.1 Introduction

Accelerated by the success of cellular technologies, mobility has changed the way people communicate. As Internet access becomes more and more ubiquitous, demands for mobility are not restricted to single terminals anymore. It is also needed to support the movement of a complete network that changes its point of attachment to the fixed infrastructure, maintaining the sessions of every device of the network: what is known as network mobility in IP networks. In this scenario, the mobile network has at least a (mobile) router that connects to the fixed infrastructure, and the devices of the mobile network connect to the exterior through this mobile router.

Support of the roaming of networks that move as a whole is required in order to enable the transparent provision of Internet access in mobile platforms, such as the following:

- Public transportation systems: These systems would let passengers in trains, planes, ships, etc. access the Internet from terminals onboard (for example, laptops, cellular phones, Personal Digital Assistants, and so on) through a mobile router located at the transport vehicle that connects to the fixed infrastructure.
- Personal networks: Electronic devices carried by people, such as PDAs, photo cameras, etc. would connect through a cellular phone acting as the mobile router of the personal network.
- Vehicular scenarios: Future cars will benefit from having Internet connectivity, not only to enhance safety (for example, by using sensors that could control multiple aspects of the vehicle operation, interacting with the environment and communicating with the Internet), but also to provide personal communication, entertainment, and Internet-based services to passengers.

However, IP networks were not designed for mobile environments. In both IPv4 and IPv6, IP addresses play two different roles. On the one hand, they are

locators that specify, based on a routing system, how to reach the node that is using that address. The routing system keeps information about how to reach different sets of addresses that have a common network prefix. This address aggregation in the routing system satisfies scalability requirements. On the other hand, IP addresses are also part of the endpoint identifiers of a communication, and upper layers use the identifiers of the peers of a communication to identify them. For example, the Transmission Control Protocol (TCP), which is used to support most of the Internet applications, uses the IP address as part of the TCP connection identifier.

This dual role played by IP addresses imposes some restrictions on mobility, because when a terminal moves from one network (IP subnet) to another, we would like to maintain the IP address of the node that moves (associated to one of its network interfaces) in order not to change the identifier that upper layers are using in their ongoing sessions. However, we also would like to change the IP address to make it topologically correct in the new location of the terminal, allowing in this way the routing system to reach the terminal.

Protocols such as the Dynamic Host Configuration Protocol (DHCP) facilitated the portability of terminals by enabling the dynamic acquisition of IP configuration information without involving manual intervention. However, this automation is not enough to achieve real and transparent mobility because it requires the restarting of ongoing transport sessions after the point of attachment changes. The IETF has studied the problem of terminal mobility in IP networks for a long time, and IP –layer solutions exist for both IPv4 (Mobile IPv4 [8]) and IPv6 (Mobile IPv6 [30]) that enable the movement of terminals without stopping their ongoing sessions.

If we focus on IPv6 networks, Mobile IPv6 does not support, as it is now defined, the movement of complete networks. One way of achieving the transparent mobility of all the nodes of a network moving together (for example, in a plane) could be enabling host mobility support in all of them, so they independently manage their mobility. However, this approach has the following drawbacks:

- Host mobility support is required in all the nodes of the network. This support might not be possible, for example, because of the limited capacities of the nodes (such as in sensors or embedded devices) or because it is not possible to update the software in some older devices. By having a single entity (the mobile router) that manages the mobility of the complete network, nodes of the network do not require any special mobility software to benefit from the transparent mobility support provided by the (mobile) router.
- The signalling exchanged because of the roaming of the network is limited to a single node sending only one message (avoiding "storms" of signalling messages every time the network moves).
- Nodes of the network must be able to attach to the access technology available to connect to the Internet. This requirement might mean that all the nodes of the network should have Universal Mobile Telecommunications Service (UMTS) or WiMAX interfaces, for example. On the other hand, by putting this requirement on a single node (the mobile router), nodes of the network can gain access to the Internet through the

mobile router, using cheaper and widely available access technologies (for example, wireless LAN or Bluetooth).[2]

2.2 IETF Working Groups and Mobility Protocols

2.2.1 DNA: Detection Network Attachment

2.2.1.1 Description of Working Group

When an IPv6 node detects or suspects that its underlying link layer (L2) connectivity has or may have undergone a change, it needs to check whether its IP layer (L3) addressing and routing configurations are still valid or have changed.

In the case that the L3 connectivity has changed, the node needs to reconfigure and may need to initiate mobility procedures, such as sending Mobile IP binding updates. Changes in an L2 connection do not necessarily mean that there has been change in L3 connectivity.

For the purposes of detecting network attachment, an L3 link is defined as the topological range within which IP packets may be sent without resorting to forwarding. In other words, a link is the range where a given IP configuration is valid.

In IPv6, the IP layer configuration information includes the set of valid unicast addresses[RFC 2462, RFC 3315], the Duplicate Address Detection (DAD) status of the addresses (RFC 2462), valid routing prefixes (RFC 2461), set of default routers (RFC 2461), neighbour and destination caches (RFC 2461), multicast listener (MLD) state (RFC 2710). The current IPv6 stateless and stateful auto configuration procedures may take a fairly long time due to delays associated with Router Discovery and Duplicate Address Detection.

The main goal of this WG is to develop mechanisms that reduce or avoid such delays, in cases where they are not necessary. For example if an interface comes back up after having been down momentarily, it can be quicker to verify that one is still attached to the same link than rerunning the full reconfiguration as if one were connecting to a new L3 link and had no previous configuration information cached.

In some wireless technologies, the link layer state and events may not give an accurate indication of whether or not the IP addressing configuration and routability have changed. For example, a host may be able to see a base station but still be unable to deliver or receive IP packets within the L3 link. Moreover, a hardware indication that a radio link is up does not necessarily mean that all link layer configuration, such as authentication or virtual LAN connectivity has been completed. Therefore detecting network attachment requires not only change detection but IP layer connectivity testing.

The purpose of the DNA working group is to define standards track and BCP documents that allow hosts to detect their IP layer configuration and connectivity status quickly, proposing some optimization to the current specifications that would allow a host to reconfigure its IPv6 layer faster than today.

The group will define a set of goals for detecting network attachment, describing existing issues and important properties of potential solutions.

The working group will describe best current practice for nodes making use of existing information for detecting network attachment.

The working group will define a set of extensions to the current IPv6 configuration protocols (RFC 2461, 2462, possibly RFC 3315) that allow the nodes to discover whether L3 configuration or connectivity may have changed more reliably and easily than today.

Initiation of L3 link change detection procedures can be achieved either through reception (or lack of reception) of messages at the IP layer or through indications from other layers. The working group will produce an informational document that contains a catalogue of the indications currently available from a subset of wireless link layer technologies.

The DNA WG will not define new procedures or APIs related to link layers.

Documents:

- Define goals for detecting network attachment in IPv6 (Informational).
- Specify recommendations for detecting network attachment and L3 link change in IPv6 networks (BCP).
- Define a protocol extension for detecting network attachment and L3 link change in IPv6 networks more reliably and easily (Standards Track).
- Document existing link layer (L2) information which is useful to start detecting network attachment (Informational).

2.2.1.2 Goals and milestones

The goals and milestones of this Working Group are shown in a table as follows:

Detection Network Attachment Working Group	
Done	Submit to IESG Goals for Detecting Network Attachment in IPv6
Done	Submit to IESG Existing Link Layer Hints Catalogue
October 2008	Submit 'Tentative options for link-layer addresses' to IESG as Standards Track
November 2008	Submit 'Detecting Network Attachment in IPv6' to IESG as Informational
January 2009	Submit 'Simple procedures for Detecting Network Attachment in IPv6' to IESG as Standards Track
March 2009	Submit 'Fast Router Discovery with Link-Layer Support' to IESG as Informational

Tabla 1: DNA WG Goals and milestones

2.2.1.3 Internet drafts

- Tentative Options for Link-Layer Addresses in IPv6 Neighbour Discovery [4]

- Simple procedures for Detecting Network Attachment in IPv6 [5]

2.2.1.4 Requests For Comments

- Goals of Detecting Network Attachment in IPv6 (RFC 4135) [6]
- Link-layer Event Notifications for Detecting Network Attachments [7]

2.2.2 MIP4: Mobility for IP version 4 Working Group

2.2.2.1 Description of Working Group

IP mobility support for IPv4 nodes (hosts and routers) is specified in RFC3344. RFC 3344 mobility allows a node to continue using its "permanent" home address as it moves around the Internet. The Mobile IP protocols support transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings. Besides the basic Mobile IPv4 (MIPv4) protocols, several other drafts deal with concerns such as optimization, security, extensions, AAA support, and deployment issues.

MIPv4 is currently being deployed on a wide basis (e.g., in cdma2000 networks). The scope of the deployment is on a fairly large scale and accordingly, the MIP4 WG will focus on deployment issues and on addressing known deficiencies and shortcomings in the protocol that have come up as a result of deployment experience. Specifically, the working group will complete the work items to facilitate interactions with AAA environments, interactions with enterprise environments when MIPv4 is used therein, and updating existing protocol specifications in accordance with deployment needs and advancing those protocols that are on the standards track.

Work expected to be done by the MIP4 WG as proposed by its charter is as follows:

1. MIPv4 has been a proposed standard for several years. It has been adopted by other standard development organizations and has been deployed commercially. One of the next steps for the WG is to advance the protocol to draft standard status. As part of advancing base Mobile IP specs to DS, the MIPv4 NAI RFC (2794) will be revised to reflect implementation experience.
2. Work items that are pending from the previous Mobile IP WG, which will be completed by the MIP4 WG, are:
   - completion of the MIB for the revised base Mobile IP specification (2006bis)
   - regional registration draft.
3. The MIP4 WG will also complete the work on MIPv4 interactions in VPN scenarios. This work will involve identifying the requirements and a solution development for MIPv4 operation in the presence of IPsec VPNs.
4. Additionally, a proposal has been made for how MO BIKE could work together with MIPv4. This proposal does not describe any new protocol, but formulates a best current practice for deploying MOBIKE together with MIPv4. The working group will adopt and complete his document.

5. Some issues have been raised with respect to RFC3519. These will be identified and addressed as appropriate, through errata, revision of RFC 3519, and/or supplemental documents as needed.
6. It has been proposed that the FMIP protocol, which has been standardised for MIPv6 in the MIPSHOP working group, should also be published as an experimental protocol for MIPv4. A draft for this exists. The working group will take up and carry this work forward to publication.
7. An extension to carry generic strings in the Registration Reply message has been proposed. The purpose is to supply supplemental human-readable information intended to the MN user. The working group will complete the specification and applicability statement of such an extension.
8. RADIUS attributes for MIP4. A set of RADIUS attributes has been proposed for MIPv4.

   The working group will first produce a requirements specification, describing how the work differs from the requirements in RFC 2977 and the functionality provided by RFC 4004 (the MIPv4 Diameter App). The reason why this first step is required is that RFC 3127 shows that full RFC 2977 functionality can't be provided by even a considerably extended RADIUS, so we need to match the requirements to what can be done within RADIUS.

   Provided the requirements work finds approval with ADs and RADEXT WG, the workgroup will complete the specification of MIPv4 RADIUS attributes, solicit feedback from the RADEXT WG, adjust, and submit this for publication. Note that the work may require extensions to the RADIUS attribute space which will be handled outside the MIP4 WG.
9. MIPv4 Extension for Configuration Options.

   Several drafts have proposed extensions to help improve configuration of MIPv4 clients. The latest proposal is for a general configuration option extension which could carry information such as e.g., DNS address and DHCP server address. The working group will take on and complete one proposal for a configuration option extension.
10. Dual-stack Support

    There have been several proposals for how to enable an IPv6 connection over a network that supports Mobile IPv4. A protocol enhancement to MIPv4 would allow for IPv6 support in a region where Mobile IPv4 has already been implemented and deployed. This would allow a dual stack mobile node to maintain IPv6 connectivity when using MIPv4. The solution would therefore be applicable only to networks that are not deploying Mobile IPv6.

    The working group will take on and complete one proposal for IPv6 over Mobile IPv4. This work is restricted to a small protocol extension similar to current Mobile IPv4 functionality. Support for advanced Mobile IPv6 functionality is strictly outside the scope.

    A problem statement covering both Mobile IPv4 and IPv6 dual-stack issues is expected to come out of MIP6 WG, and will not be developed in MIP4 WG.

11. MIPv4 Moving Network Support

    The Network Mobility (NEMO) working group deals with the problem of mobility of a whole network, such as might exist inside a vehicle, train, or airplane. The NEMO working group has developed draft specifications for both IPv6 and IPv4 mobile networks. However, it has been recognized that the IPv4 version of the protocol can be viewed as an extension of the basic Mobile IPv4 protocol, and there is good reason to do this extension in the MIP4 working group. The working group will take on the MIPv4 network mobility internet draft and progress it along the standards track. In addition, the working group will take up extensions to the basic MIPv4 moving network support in the areas of dynamic prefix assignment and foreign agent support.

12. Asynchronous Notification Mechanism

    In some situations, there is a need for Mobile IPv4 entities, such as the home agent, foreign agent and mobile node to send and receive asynchronous notification events related to the operation of the MIPv4 protocol. A couple of examples of such events are registration revocation from a home agent to a foreign agent in order to terminate the service (to release resources and end charging), and notification of pending HA shutdown and indication of alternative serving HA, from a HA to the mobile node.

The base Mobile IP Specification [RFC3344] does not have a provision for this. A new MIPv4 message pair which would support asynchronous notifications and a notification model describing how to use these messages has been proposed. The working group will take on the existing MIPv4 notification message draft as a starting point, review and update it as needed, and progress it as a standards track document. In addition, the working group will also consider defining specific usages of the notification message based on the examples in the current document.

2.2.2.2 Goals and milestones

The goals and milestones of this Working Group are shown in a table as follows:

Mobility for IPv4 Working Group	
Done	AAA Keys for MIPv4 to IESG
Done	MIPv4 VPN interaction problem statement to IESG
Done	Low latency handover to experimental
Done	Experimental MIPv4 message and extensions draft to IESG
Done	Dynamic Home Agent assignment protocol solution to IESG
Done	Dynamic Home Agent assignment protocol solution to IESG
Done	Revised MIPv4 Challenge/Response (3012bis) to IESG
Done	Regional registration document to IESG

Done	Generic Strings for MIPv4 (Proposed Standard) to the IESG
Done	MIPv4 MOBIKE interaction (BCP) to the IESG
Done	MIPv4 RADIUS Extensions Requirements to the IESG
Done	MIPv4 Extension for Configuration Options (Proposed Standard) to the IESG
Done	FMIPv4 (Experimental) to the IESG
Done	MIPv4 VPN interaction (BCP) to the IESG
Done	Base MIPv4 Mobile Network Support (Draft Standard) to IESG

Tabla 2: MIPv4 WG Goals and milestones

2.2.2.3 Internet drafts

- The Definitions of Managed Objects for IP Mobility Support using SMIv2, revised [9]
- Generic Notification Message for Mobile IPv4 [10]
- The Definitions of Managed Objects for Mobile IP UDP Tunnelling [11]

2.2.2.4 Requests For Comments

- Mobile IPv4 Extension for AAA Network Access Identifiers (RFC 3846) [12]
- Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4 (RFC 3957) [13]
- Experimental Message, Extension and Error Codes for Mobile IPv4 (RFC 4064) [14]
- Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways (RFC 4093) [15]
- Mobile IPv4 Dynamic Home Agent Assignment (RFC 4433) [16]
- Foreign Agent Error Extension for Mobile IPv4 (RFC 4636) [17]
- Mobile IPv4 Challenge/Response Extensions (Revised) (RFC 4721) [18]
- Mobile IPv4 Regional Registration (RFC 4857) [19]
- Mobile IPv4 Message String Extension (RFC 4917) [20]
- Low-Latency Handoffs in Mobile IPv4 (RFC 4881) [21]
- Mobile IPv4 RADIUS requirements (RFC 5030) [22]
- Mobile IPv4 Fast Handovers (RFC 4988) [23]
- Network Mobility (NEMO) Extensions for Mobile IPv4 (RFC 5177) [24]
- Mobile IPv4 Traversal across IPsec-Based VPN Gateways (RFC 5265) [25]

- Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE) (RFC 5266) [26]
- Dual-Stack Mobile IPv4 (RFC 5454) [27]

2.2.3 MIP6: Mobility for IPv6 Working Group

2.2.3.1 Description of Working Group

Mobile IPv6 (MIP6) specifies routing support which permits an IPv6 host to continue using its home address as it moves around the Internet, enabling continuity of sessions. Mobile IPv6 supports transparency above the IP layer, including maintenance of active transport level sessions. The base specifications for Mobile IPv6 consist of:

- RFC 3775
- RFC 3776

The primary goal of the MIP6 working group will be to enhance base IPv6 mobility by continuing work on developments that are required for wide-scale deployments. Additionally the working group will ensure that any issues identified by implementation and interoperability experience are addressed, and that the base specifications are maintained. The group will also produce informational documentation, such as design rationale documents or description of specific issues within the protocol.

Deployment considerations call for work to reduce per-mobile node configuration and enrolment effort, solutions to enable dual-stack operation, mechanisms to support high-availabity home agents, and ways to employ Mobile IPv6 in the presence of firewalls.

Work items related to base specification maintenance include:

- Create and maintain an issue list that is generated on the basis of implementation and interoperability experience. Address specific issues with specific updates or revisions of the base specification. One specific area of concern that should be analyzed and addressed relates to multilink subnets.

This work item relates only to corrections and clarifications. The working group shall not revisit design decisions or change the protocol.

- Update RFC 3776 to specify the usage of IKEv2 for the establishment of the IPsec SA between the MN and HA. This work also provides a way for a mobile node to change its home address or employ multiple home addresses as needed.

- Update the IANA considerations of RFC 3775 to allow extensions for experimental purposes as well passing of optional vendor-specific information.

Work items related to large scale deployment include:

- Bootstrapping Mobile IPv6: A bootstrapping mechanism is intended to be used when the device is turned on the very first time and activates Mobile IPv6, or periodically such as when powering on. The WG should investigate and define the scope before solving the problem.

Work on the problem statement and the solutions needed for various deployment scenarios. Work with other WGs such as DHC for defining the options needed for bootstrapping.

- Capture the AAA requirements needed for bootstrapping and deployment, and work with the Radext and DiME WGs on the solutions.

- A Solution for MIP6 session continuity for dual stack hosts which attach to IPv4 access networks. Additionally provide a mechanism for carrying IPv4 packets via the Home agent for MIP6 capable dual-stack hosts. This work will be done in collaboration with the NEMO WG.

- A protocol based solution for enhancing the reliability of home agents and a method to force a host to switch home agents.

- A mechanism to force an MN to switch the HA that is currently serving it. This is required in deployments where the HA may need to be taken offline for maintenance.

- Work on solutions to deal with firewalls and the problems that firewalls cause as identified in RFC 4487.

Work items related to informational documentation include:

- Produce a problem statement relating to location privacy and the use of Mobile IPv6. Work with the IRTF MOBOPTS RG on developing the solution.

- Produce a design rationale that documents the historical thinking behind the introduction of an alternative security mechanism, the Authentication Protocol (RFC 4285).

It should be noted that some of the features that are directly related to Mobile IPv6 are being worked on in the MONAMI6, MIPSHOP, and NEMO working groups. The specific extensions from these groups are out of scope for the MIP6 working group. In particular, all optimizations are out of scope. However, MIP6 may assist these groups when they use features listed above and have requirements on them.

2.2.3.2 Goals and milestones

Mobility for IPv6 Working Group	
Done	Submit I-D ‘Issues with firewall problem statement’ to IESG
Done	Submit I-D 'MIPv6 MIB' to IESG
Done	Submit I-D 'Extensions to Socket Advanced API for MIPv6' to IESG
Done	Submit I-D 'Alternate Route Optimization (Pre-config Key) scheme' to IESG
Done	Submit Bootstrapping problem statement to IESG
Done	Submit I-D 'Authentication Option for MIPv6' to IESG
Done	Submit I-D 'Identification Option for MIPv6' to IESG

Done	Submit I-D 'MIPv6 operation with IKEV2 and the revised IPsec Architecture to IESG
Done	Submit Problem statement and Solution to Mobile IPv6 transition between v4/v6 networks to IESG
Done	Submit I-D 'Mobility management for Dual stack mobile nodes: A Problem Statement' to IESG for publication as Informational
Done	Submit I-D 'Address Location Privacy and Mobile IPv6 Problem Statement' to IESG for publication as Informational.
Done	Submit I-D 'Bootstrapping solution for split Scenario' to IESG for publication as a Proposed Standard.
April 2007	Submit I-D 'Motivation for Authentication I-D' to IESG for publication as Informational.
Done	Submit I-D 'Bootstrapping solution for Integrated Scenario' to IESG for publication as a Proposed Standard.
July 2007	Submit I-D 'DHCP Options for Home Information Discovery in MIPv6' for publication as a proposed standard.
July 2007	Submit I-D 'Mobility Header Home Agent Switch Message' to IESG for publication as a Proposed Standard.
August 2007	Submit I-D 'Goals for AAA HA Interface' to IESG for publication as Informational.
September 2007	Submit I-D 'Home agent reliability' to IESG for publication as a Proposed Standard.
September 2007	Submit I-D 'Mobile IPv6 Dual-Stack Operation' to IESG for publication as a Proposed Standard.
October 2007	Submit I-D 'Mobile IPv6 Vendor Specific Option' to IESG for publication as a Proposed Standard.
December 2007	Submit I-D 'Mobile IPv6 Experimental Allocations' to IESG for publication as a Proposed Standard
December 2007	Submit the I-D 'RADIUS Mobile IPv6 Support' to IESG for publication as a proposed standard.
February 2008	Submit I-D 'Mobile IPv6 Operation with Firewalls' to IESG for publication as Informational.
February 2008	Submit I-D(s) related to specific updates and corrections of RFC 3775 to IESG for

publication as Proposed Standard.

Tabla 3: MIP6 WG Goals and milestones

2.2.3.3 Internet drafts

There are no Internet Drafts currently available.

2.2.3.4 Requests For Comments

- Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents (RFC 3776) updated by RFC 4877 [29]
- Mobility Support in IPv6 (RFC 3775) [30]
- Mobile Node Identifier Option for Mobile IPv6 (MIPv6) (RFC 4283) [31]
- Mobile IP version 6 Route Optimization Security Design Background (RFC 4225) [32]
- Authentication Protocol for Mobile IPv6 (RFC 4285) [33]
- Mobile IPv6 Management Information Base (RFC 4295) [34]
- Mobile IPv6 and Firewalls: Problem Statement (RFC 4487) [35]
- Securing Mobile IPv6 Route Optimization Using a Static Shared Key (RFC 4449) [36]
- Extension to Sockets API for Mobile IPv6 (RFC 4584) [37]
- Problem Statement for bootstrapping Mobile IPv6 (RFC 4640) [38]
- Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture (RFC 4877) updates RFC 3776 [39]
- IP Address Location Privacy and Mobile IPv6: Problem Statement (RFC 4882) [40]
- Problem Statement: Dual Stack Mobility (RFC 4977) [41]
- Mobile IPv6 bootstrapping in split scenario (RFC 5026) [42]
- Mobile IPv6 Experimental Messages (RFC 5096) [43]
- Mobile IPv6 Vendor Specific Option (RFC 5094) [44]

2.2.4 MIPSHOP: Mobility for IP. Performance, Signaling and Handoff Optimization

2.2.4.1 Description of Working Group

Mobile IPv6 enables IPv6 mobile nodes to continue a session using a given "home address" in spite of changes in its point of attachment to the network. These changes may cause delay, packet loss, and also represent signaling overhead traffic on the network. The MIPSHOP WG has so far worked on two technologies to address these issues. Hierarchical Mobile IPv6 (HMIPv6) reduces the amount and latency of signaling between a MN, its Home Agent and one or more correspondent nodes. Mobile IPv6 Fast Handovers (FMIPv6) reduces packet loss

by providing fast IP connectivity as soon as the mobile node establishes a new point of attachment at a new link.

The MIPSHOP WG will continue to work on HMIPv6 and FMIPv6, and the necessary extensions to improve these protocols. The MIPSHOP WG will also identify missing components that are required for deploying these protocols and standardize the necessary extensions. The WG will also address using these protocols to provide fast handovers for network-based mobility management protocols like Proxy Mobile IPv6.

The IEEE 802.21 Media Independent Handover (MIH) working group aims at providing services to assist with handoffs between heterogeneous link-layer technologies, and across IP subnet boundaries. MIH services can be delivered through link-layer specific solutions and/or through a "layer 3 or above" protocol. MIPSHOP will define the delivery of information for MIH services for this latter case. A L3 based mechanism to identify a valid information server is also required. The MIPSHOP will work on developing a protocol for transport of MIH services information and mechanisms for discovering the MIH server. Security for the transport of MIH information will also be addressed.

The MOBOPTS Research Group in the IRTF is chartered to work on optimizations related to Mobile IPv6 and IP handoffs among other things. The MIPSHOP WG will take mature proposals from the MOBOPTS group and standardize them in the IETF on a case-by-case basis.

The MIPSHOP WG will also consider and standardize optimizations for the Mobile IPv6 protocol and IP mobility in general.

Scope of MIPSHOP:

The working group will work on:

1. FMIPv6 Mobile Node - Access Router security using the AAA infrastructure.

   Currently MIPSHOP has produced a standards track protocol for setting up security between the mobile node and access router for security FMIPv6 signaling messages. However, the protocol depends on SeND (Secure Neighbor Discovery) to be available on the mobile node and the access router. An alternate mechanism that leverages the AAA infrastructure would be useful. Many target systems where FMIPv6 is likely to be used use a AAA infrastructure to authenticate and authorize network access. The working group will work on an Informational document describing how the AAA infrastructure could be used for setting up security associations between the mobile node and the access router.

2. Prefix Management for point-to-point links with FMIPv6.

   Using FMIPv6 over point-to-points like requires some additional considerations with respect to managing and allocating prefixes for the mobile node on these point-to-point links. Therefore the WG will work on an Informational document to address the issues.

3. Handover optimizations when Proxy Mobile IPv6 is used for handovers.

   Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol where a node in the access network, called the Mobile Access Gateway (MAG) handles mobility on behalf of the mobile node. It has been

proposed to use FMIPv6 to optimize the handover in terms of reducing the packet loss and transferring relevant context from the old MAG to the new MAG. The working group will also work on other optimizations like the use of a transient binding cache entry for improving a PMIPv6-based handover.

4. Work on protocols and extensions for transporting information related to IEEE 802.21:

   The work includes the layer 3 protocol for transporting MIH related information and DHCP and DNS extensions for discovering the information servers.

2.2.4.2 Goals and milestones

MIPSHOP Working Group	
Done	Working Group Last Call on draft-ietf-mipshop-hmip-xx.txt
Done	Working Group Last Call on draft-ietf-mipshop-lmm-requirements-XX.txt
Done	Working Group Last Call on draft-ietf-mipshop-lmm-requirements-XX.txt
Done	Discuss Last Call comments and security analyses at IETF 58
Done	Submit draft draft-ietf-mipshop-lmm-requirements-XX.txt to IESG for consideration of publication as Informational
Done	Submit draft-ietf-mipshop-fmipv6-xx.txt to IESG for consideration of publication as Experimental
Done	Submit draft-ietf-mipshop-hmip-xx.txt to IESG for consideration of publication as Experimental
Done	Working Group Last Call on draft-ietf-mipshop-80211fh-xx.txt for Informational
Done	Submit draft-ietf-mipshop-80211fh-xx.txt to IESG for consideration of publication as Informational
Done	Working Group Last Call on draft-ietf-mipshop-cga-cba-XX.txt
Done	Working Group Last Call on draft-ietf-mipshop-mis-ps
Done	Submit draft-ietf-mipshop-cga-cba to IESG for publication as Proposed Standard
Done	Working Group Last Call on draft-ietf-mipshop-fmipv6-rfc4068bis
Done	Working Group Last Call on draft-ietf-mipshop-handover-key-send
Done	Submit draft-ietf-mipshop-mis-ps to IESG for publication as Informational RFC

Done	Working Group Last Call on draft-ietf-mipshop-rfc4041bis
Done	Working Group Last Call on draft-ietf-mipshop-3gfh
Done	Working Group Last Call on draft-ietf-mipshop-fh80216e
Done	Submit draft-ietf-mipshop-fmipv6-rfc4068bis to IESG for publication as Proposed Standard
Done	Submit draft-ietf-mipshop-handover-key-send to IESG for publication as Proposed Standard
Done	Submit draft-ietf-mipshop-3gfh to IESG for publication as Informational RFC
Done	Submit draft-ietf-mipshop-fh80216e to IESG for publication as Informational RFC
Done	Working Group Last Call on draft-ietf-mipshop-mih-support
Done	Submit draft-ietf-mipshop-mih-support to IESG for publication as Proposed Standard
Done	Working Group Last Call on draft-ietf-mipshop-mos-dns-discovery
Done	Working Group Last Call on draft-ietf-mipshop-mos-dhcp-options
Done	Submit draft-ietf-mipshop-mos-dhcp-options to the IESG for publication as Proposed Standard
May 2009	Working Group Last Call on draft-ietf-mipshop-pfmipv6
June 2009	Working Group Last Call on draft-ietf-mipshop-transient-bce-pmipv6
June 2009	Submit draft-ietf-mipshop-pfmipv6 to the IESG for publication as Proposed Standard
July 2009	Submit draft-ietf-mipshop-transient-bce-pmipv6 to the IESG for publication as Experimental
August 2009	Working group last call on draft-ietf-mipshop-fmipv6-ptp
September 2009	Submit draft-ietf-mipshop-fmipv6-ptp to the IESG for publication as Informational

Tabla 4: MIPSHOP WG Goals and milestones

2.2.4.3 Internet drafts

- IEEE 802.21 Mobility Services Framework Design (MSFD) [46]
- Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Services (MoS) Discovery [47]
- Locating IEEE 802.21 Mobility Servers using DNS [48]
- Fast Handovers for Proxy Mobile IPv6 [49]

- Transient Binding for Proxy Mobile IPv6 [50]
- Mobile IPv6 Fast Handovers [51]

2.2.4.4 Requests For Comments

- Mobile IPv6 Fast Handovers for 802.11 Networks (RFC 4260) [52]
- Enhanced Route Optimization for Mobile IPv6 (RFC 4866) [53]
- Mobility Services Transport: Problem Statement (RFC 5164) [54]
- Mobile IPv6 Fast Handovers over IEEE 802.16e Networks (RFC 5270) [55]
- Mobile IPv6 Fast Handovers for 3G CDMA Networks (RFC 5271) [56]
- Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND) (RFC 5269) [57]
- Mobile IPv6 Fast Handovers (RFC 5268) obsoletes RFC 4068 [58]
- Hierarchical Mobile IPv6 Mobility Management (RFC 5380) obsoletes RFC 4140 [59]

2.2.5 NEMO: Network Mobility

2.2.5.1 Description of Working Group

The NEMO Working Group is concerned with managing the mobility of an entire network, which changes its point of attachment to the Internet and thus its reachability in the network topology. The mobile network includes one or more mobile routers (MRs) which connect the rest of the mobile network to the global Internet.

For the purposes of this working group, a mobile network is a leaf network; it does not carry transit traffic. Nonetheless, it could be multihomed, either with a single MR that has multiple attachments to the Internet, or by using multiple MRs that attach the mobile network to the Internet.

For the basic NEMO support case, none of the nodes behind the MR need be aware of the network's mobility; thus, the network's movement is completely transparent to the nodes inside the mobile network. This design consideration was made to accommodate nodes inside the network that are not generally aware of mobility.

Basic network mobility support is described in RFC 3963. This RFC contains NEMO Basic Support, which is a protocol based on Mobile IPv6 (RFC 3775, 3776) that enables network mobility in an IPv6 network.

The working group is tasked with continuing to evolve RFC 3963 to correct errors and maintain the specification. In addition, the group works in co-operation with the MIP6 WG to design a mechanism to allow mixed IPv4/IPv6 networks to be used.

At this point, the working group is concerned with solving deployment issues of NEMO, primarily relating to the identified needs of the automotive and aviation communities. The group will gather requirements from those builders and users, and then solve the route optimization issues necessary for optimized deployments.

Among the deployments that have issues which may be solved by NEMO Route Optimization feature(s), we have identified three cases that have a likelihood of requirements gathering and an Optimization solution. These are called the Aviation case, the Automotive case, and the Personal Mobile Router (consumer electronics) case, though the actual technical problems are characterized by the type of movements and environments more than by the specific industry using the technology. The group will explore these cases to gather requirements and, if those requirements match the capability of a NEMO RO solution space, proceed with solving the open issues.

The WG will:

- Finish working group documents that are currently in process, and submit for RFC. This includes prefix delegation protocol mechanisms, a multihoming problem statement, and a MIB for NEMO Basic Support.

- Gather requirements for NEMO Route Optimization in deployment scenarios:

1. Airline and spacecraft community, who are deploying NEMO for control systems, as well as Internet connectivity and entertainment systems. This use case is characterized by fast (~ 1000 km/h) moving objects over large distances (across continents). The main technical problem is that tunneling-based solutions imply a roundtrip to another continent and that BGP based solutions imply significant churn in the global Internet routing table.
2. Automotive industry, who are deploying NEMO for in-car communication, entertainment, and data gathering, possible control systems use, and communication to roadside devices. This use case is characterized by moderately fast (~ 100-300 km/h) moving objects that employ local or cellular networks for connectivity.
3. Personal Mobile Routers, which are consumer devices that allow the user to bring a NEMO network with the user while mobile, and communicate with peer NEMO networks/MNNs.

After gathering the requirements for these types of deployments, the working group will evaluate what type of route optimization needs to be performed (if any), and formulate a solution to those problems.

If no requirements for those scenarios can be collected by the deadline, it will be assumed that the work is premature, and that type of deployment will be dropped from the list of use cases currently addressed by NEMO.

The group will only consider airline and spacecraft solutions that combine tunneling solutions for small movements with either federated tunnel servers or slowly changing end host prefixes.

The group will only consider personal mobile router requirements about optimized routes to another mobile router belonging to the same operator.

The group will only consider automotive industry requirements to allow MR-attached hosts to directly access the network where MR has attached to.

Work on automotive and personal mobile router solutions requires rechartering.

The WG will not:

- consider routing issues inside the mobile network. Existing routing protocols (including MANET protocols) can be used to solve these problems.

- consider general route optimization, multihoming, or other problems that are not related to the deployment and maintenance of NEMO networks.

- consider or rely on the results of general routing architecture, Internet architecture, or identifier-locator split issues that are discussed in separate, long term efforts elsewhere in the IETF.

- consider solutions that require changes from correspondent nodes in the general Internet.

The working group will endeavor to separate research issues, and refer them to the IRTF as appropriate.

2.2.5.2 Goals and milestones

Network Mobility Working Group	
Done	Submit terminology and requirements documents (for Basic support).
Done	Submit NEMO Basic Support to IESG
Done	Submit NEMO Basic Support to IESG
Done	Submit WG draft -00 on Multihoming Problem Statement
Done	Submit WG draft -00 on NEMO Basic Support Usages
Done	Submit WG draft -00 on Prefix Delegation for NEMO
Done	Submit WG draft -00 on MIB for NEMO Basic Support
Done	Submit WG draft -00 on Analysis of the Solution Space for Route Optimization
Done	Submit Terminology as Informational to IESG
Done	Submit Goals and Requirements as Informational to IESG
May 2007	Submit the final doc on MIB for NEMO Basic Support to the IESG, for Proposed Standard
Done	Submit the final doc Multihoming Problem Statement to the IESG, for Informational
Done	Submit the final doc on Prefix Delegation for NEMO to the IESG, for Proposed Standard
July 2007	Submit -00 draft on Route Optimization Needs for Aircraft and Spacecraft Deployments
July 2007	Submit -00 draft on Route Optimization Needs for Automobile and Highway Deployments
July 2007	Submit -00 draft on Route Optimization needs for Personal Mobile Router
September 2007	Submit -00 draft for solution to aircraft/spacecraft problem

	aircraft/spacecraft problem
Novemeber 2007	Submit final doc on Route Optimization Needs for Aircraft and Spacecraft Deployments, for Informational
November 2007	Submit final doc on Route Optimization Needs for Automobile and Highway Deployments, for Informational
November 2007	Submit final doc on Route Optimization needs for Personal Mobile Router, for Informational
December 2007	Determine how to proceed with remaining automotive/Personal Mobile Router solutions
December 2007	Recharter to work on the remaining automotive/Personal Mobile Router solutions
January 2008	Submit final doc for solution to aircraft/spacecraft problem to the IESG, for Proposed Standard

Tabla 5: NEMO WG Goals and milestones

2.2.5.3 Internet drafts

There are no current Internet drafts available.

2.2.5.4 Request For Comments

- Network Mobility (NEMO) Basic Support Protocol (RFC 3963) [61]
- Network Mobility Route Optimization Solution Space Analysis (RFC 4889) [62]
- Network Mobility Route Optimization Problem Statement (RFC 4888) [63]
- Network Mobility Home Network Models (RFC 4887) [64]
- Network Mobility Support Goals and Requirements (RFC 4886) [65]
- Network Mobility Support Terminology (RFC 4885) [66]
- Analysis of Multihoming in Network Mobility Support (RFC 4980) [67]

2.2.6 NETLMM: Network-based Localized Mobility Management

2.2.6.1 Description of Working Group

The IETF has defined both local and global mobility management protocols that are intended to handle IP mobility for nodes. All IP mobility management protocols defined thus far require the involvement of the mobile node in order to accomplish mobility. This working group is tasked with defining a network-based local mobility management protocol, where local IP mobility is handled without involvement from the mobile node. The idea is that the mobile node may move across multiple access routers without encountering a change in its IP address, thereby hiding the mobility from the IP layer and above.

As part of the first phase of efforts in this working group, a protocol for such network-based local mobility has been developed.

This protocol, Proxy Mobile IPv6 (PMIPv6), has been developed based on Mobile IPv6, after considering other alternative approaches. With this protocol, unmodified IP nodes may change access routers without having to change the IP address on an interface, within a given administrative domain. This is accomplished by having Mobile Access Gateways (MAGs), often part of the access routers in a network, send binding updates on behalf of mobile nodes attached to them, to a Local Mobility Anchor (LMA). The LMA manages the mobility of the mobile nodes across the MAGs within a given PMIPv6 domain.

The PMIPv6 protocol is being adopted as part of several wide-area wireless network (e.g., 3GPP, 3GPP2, WiMAX) and local area network environments. The current charter of this working group involves specification of some necessary features that make the deployment of this protocol feasible in these various environments.

As part of this effort, it is essential to support mobility for IPv4 end nodes. Some means of dealing with overlapping private IPv4 addresses of mobile nodes and supporting separation of flows between the MAG and LMA is also required. Further, given that local and global mobility management protocols are likely to be deployed in some combination in various environments, it is necessary to clearly define the interactions between PMIPv6 and MIPv6. Interactions with AAA protocols such as RADIUS and Diameter may be required for authorization or provisioning purposes.

When multiple LMAs are present, an automated LMA discovery mechanism may be needed to facilitate deployment. The above items are in scope of the current charter.

The MAG and LMA are considered to be IPv6 capable for all efforts of this protocol. Also, all features defined must work with unmodified IP nodes. Specifying any changes to mobile nodes is out of scope of the current charter. Handoff and route optimizations are also out of scope. There is, however, considerable interest in optimization work, for instance, and a future recharter of this working group is likely to address this in some manner.

NETLMM WG Deliverables:

1. Interface between a PMIPv6 MAG and MN: This interface will define the interaction between a regular IP node and a MAG that will be used to trigger various mobility management actions on the MAG. This is necessary for the MAG to properly trigger binding updates to the LMA and create appropriate mobility management state.
2. IPv4 Support for PMIPv6: This will define the support for IPv4 nodes in PMIPv6. This will also define the protocol operation over an IPv4 transport between the MAG and LMA, by employing protocol extensions already developed in the MEXT WG.
3. Interactions between Mobile IPv6 and Proxy Mobile IPv6: This will highlight the interactions required between these protocols in various methods of co-existence of these in a system, with a view to documenting the best practices to be used. The scenarios considered will include a hierarchical model of local and global mobility management using PMIPv6 and MIPv6 respectively, a

fixed mode of the two with some nodes supporting MIPv6 and others not, and the use of MIPv6 upon movement of nodes outside a PMIPv6 domain.

4. GRE Keying option for PMIPv6: This will define a mechanism using GRE keys to support separation of flows between a MAG and LMA.
5. RADIUS support for PMIPv6: This will define the interactions between RADIUS and PMIPv6 to support policy provisioning and authorization.
6. Automatic LMA discovery: This will define the ability for MAGs to automatically discover and use an LMA within a PMIPv6 domain. The scope of this effort may include specifying the use of DNS or DHCP based LMA discovery or LMA discovery using policy information retrieved via AAA protocols.
7. MIB for PMIPv6: This will define the MIB for the protocol for interoperability purposes.
8. PMIPv6 path management and failure detection: This will define an extension to the PMIPv6 protocol allowing PMIPv6 peers to verify bidirectional reachability with their peer, detect failure of their peer, and signal their own failure to their peer.

2.2.6.2 Goals and milestones

NETLMM Working Group	
Done	Charter Working Group.
Done	Working Group Last Call on Problem Statement and Requirements documents
Done	Discuss Last Call comments on Problem Statement and Requirements documents.
Done	Submit Problem Statement and Requirements documents to IESG for publication as Informational RFCs
Done	Working Group Last Call on Threat Model documents. Submit Threat Model document to SAAG for review
Done	Working Group Last Call on Threat Model document
Done	IETF 66, Discuss Last Call comments on Threat Model document
Done	Submit Threat Model document to IESG for publication as an Informational RFC
Done	Main protocol decision completed
Done	Initial version of the Protocol draft submitted
Done	Working Group Last Call on Mobile Node to Access Router document
August 2008	Initial version of the PMIP6-MIP6 Interactions document for publication as Proposed Standard

August 2008	Working Group Last Call on the IPv4 support document
August 2008	Initial version of GRE keying document
August 2008	Working Group Last Call on MAG-MN Interface document
October 2008	Initial version of RADIUS support document
October 2008	Submit IPv4 support and MAG-MN Interface documents for AD review
October 2008	Initial version of path management document
November 2008	Working Group Last Call on the PMIP6-MIP6 Interactions document
November 2008	Working Group Last Call on GRE Keying document
November 2008	Initial version of LMA Discovery document
November 2008	Initial version of the MIB document
December 2008	Working Group Last Call on path management document
January 2009	Submit PMIP6-MIP6 Interactions document for AD review
January 2009	Submit GRE Keying document for AD review
January 2009	Working Group Last Call on RADIUS support document
January 2009	Submit path management document for AD review
March 2009	Submit RADIUS support document for AD review
March 2009	Working Group Last Call on LMA Discovery document
March 2009	Working Group Last Call on the MIB document
May 2009	Submit LMA Discovery document for AD review
May 2009	Submit the MIB document for AD review
July 2009	Re-charter

Tabla 6: NETLMM WG Goals and milestones

2.2.6.3 Internet drafts

- IPv4 Support for Proxy Mobile IPv6 [69]
- GRE Key Option for Proxy Mobile IPv6 [70]
- Heartbeat Mechanism for Proxy Mobile IPv6 [71]
- Interactions between PMIPv6 and MIPv6: scenarios and related issues [72]
- LMA Discovery for Proxy Mobile IPv6 [73]

2.2.6.4 Requests For Comments

- Security Threats to Network-Based Localized Mobility Management (NETLMM) (RFC 4832) [74]
- Goals for Network-based Localized Mobility Management (NETLMM) (RFC 4831) [75]
- Problem Statement for Network-based Localized Mobility Management (NETLMM) (RFC 4830) [76]
- Proxy Mobile IPv6 (RFC 5213) [77]

2.2.7 HIP: Host Identity Protocol

2.2.7.1 Description of Working Group

The Host Identity Protocol (HIP) provides a method of separating the end-point identifier and locator roles of IP addresses. It introduces a new Host Identity (HI) name space, based on public keys. The public keys are typically, but not necessarily, self generated.

The specifications for the architecture and protocol details for these mechanisms consist of:

- HIP Architecture (RFC 4423)
- Host Identity Protocol (RFC 5201)

There are several publicly known interoperating implementations, some of which are open source.

Currently, the HIP base protocol works well with any pair of co-operating end-hosts. However, to be more useful and more widely deployable, HIP needs some support from the existing infrastructure, including the DNS, and a new piece of infrastructure, called the HIP rendezvous server.

At this point, the missing elements for running such wide-scale experiments are a NAT transversal solution, a description on the interactions between legacy (i.e., HIP unaware) applications and HIP, and a native API for HIP. Additionally, the working group will specify, also in Experimental RFCs, how to build HIP-based overlays. HIP-based overlays have received a lot of attention in different fora and are seen as a key area for HIP experimentation where the benefits HIP brings may be most relevant.

Note that even though the specifications are chartered for Experimental, it is understood that their quality and security properties should match the standards track requirements. The main purpose for producing Experimental documents instead of standards track ones are the unknown effects that the mechanisms may have on applications and on the Internet at large.

In parallel to this working group, there is an IRTF Research Group with a broader scope that includes efforts both on developing the more forward looking aspects of the HIP architecture and on exploring the effects that HIP may have on the applications and the Internet.

The following are charter items for the working group:

- Specify how legacy (i.e., HIP unaware) applications can be made to work with HIP.
- Specify a solution for HIP to traverse legacy (i.e., HIP unaware) NATs. This solution will be based on existing NAT traversal mechanisms such as ICE (Interactive Connectivity Establishment).
- Specify a native HIP socket API.
- Specify a framework to build HIP-based overlays. This framework will describe how HIP can perform some of the tasks needed to build an overlay and how technologies developed somewhere else (e.g., a peer protocol developed in the P2PSIP WG) can complement HIP by performing the tasks HIP was not designed to perform.
- Specify how to generate ORCHIDs from other node identifiers including both cryptographic ones (leading to cryptographic delegation) and non-cryptographic ones (e.g., identifiers defined by a peer protocol).
- Specify how to carry certificates in the base exchange. This was removed from the base HIP specification so that the mechanism is specified in a stand-alone spec.
- Specify how to carry upper-layer data over specified HIP packets. These include some of the existing HIP packets and possibly new HIP packets (e.g., a HIP packet that occurs outside a HIP base exchange).

2.2.7.2 Goals and milestones

The goals and milestones of this Working Group are shown in a table as follows:

Host Identity Protocol Working Group	
Done	First version of the HIP basic mobility and multi-homing mechanism specification.
Done	First version of the HIP DNS resource record(s) specification.
Done	First version of the HIP basic rendezvous mechanism specification.
Done	WGLC on the HIP architecture specification
Done	Submit the HIP architecture specification to the IESG
Done	WG LC on the base protocol specification
Done	WG LC on the ESP usage specification.
Done	WG LC the HIP registration extensions specification

Done	WGLC the HIP DNS resource record(s) specification
Done	WG LC on the basic HIP rendezvous mechanism specification.
Done	Submit the ESP usage specification to the IESG for Experimental
Done	Submit the base protocol specification to the IESG for Experimental
Done	WG LC on the HIP basic mobility and multi-homing specification.
Done	Submit the HIP registration extensions specification for Experimental
Done	Submit the HIP DNS resource record(s) specification to the IESG for Experimental.
Done	Submit the HIP basic mobility and multihoming specification to the IESG for Experimental
Done	Submit the basic HIP rendezvous mechanism specification to the IESG for Experimental.
Done	WGLC Legacy Application Interworking specification
Done	Submit the Legacy Application Interworking specification to the IESG
December 2008	WGLC Legacy NAT traversal specification
February 2009	WGLC Native API specification
February 2009	Submit the Legacy NAT traversal specification to the IESG
April 2009	Submit Native API specification to the IESG
April 2009	WGLC Framework for HIP overlays specification
April 2009	WGLC ORCHID generation specification
April 2009	WGLC Certs in HIP base exchange specification
April 2009	WGLC Upper-layer data transport in HIP
July 2009	Recharter or close the WG
July 2009	Submit Framework for HIP overlays specification to the IESG
July 2009	Submit ORCHID generation specification to the IESG
July 2009	Submit Certs in HIP base exchange specification to the IESG
July 2009	Submit Upper-layer data transport in HIP to the IESG

Tabla 7: HIP WG Goals and milestones

2.2.7.3 Internet drafts

- Basic HIP Extensions for Traversal of Network Address Translators [79]
- Basic Socket Interface Extensions for Host Identity Protocol (HIP) [80]
- HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking Environment [81]

2.2.7.4 Requests For Comments

- Host Identity Protocol (HIP) Architecture (RFC 4423) [82]
- Host Identity Protocol (RFC 5201) [83]
- Host Identity Protocol (HIP) Domain Name System (DNS) Extensions (RFC 5205) [84]
- Host Identity Protocol (HIP) Registration Extension (RFC 5203) [85]
- Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP) (RFC 5202) [86]
- Host Identity Protocol (HIP) Rendezvous Extension (RFC 5204) [87]
- End-Host Mobility and Multihoming with the Host Identity Protocol (RFC 5206) [88]
- Using the Host Identity Protocol with Legacy Applications (RFC 5338) [89]

2.2.8 MEXT: Mobility Extensions for IPv6

2.2.8.1 Description of Working Group

Mobile IPv6 specifies routing support which permits an IPv6 host to continue using its home address as it moves around the Internet, enabling continuity of sessions. Mobile IPv6 supports transparency above the IP layer, including maintenance of active transport level sessions. In addition, network mobility (NEMO) mechanisms built on top of Mobile IPv6 allow managing the mobility of an entire network, as it changes its point of attachment to the Internet. The base specifications consist of:

- RFC 3775 (Mobile IPv6)
- RFC 3963 (NEMO)
- RFC 4877 (Mobile IPv6 Operation with IKEv2)

The MEXT Working Group continues the work of the former MIP6, NEMO, and MONAMI6 Working Groups.

The primary goal of MEXT will be to:

a) enhance base IPv6 mobility by continuing work on developments that are required for wide-scale deployments and specific deployment scenarios.

b) Additionally, the working group will ensure that any issues identified by implementation and interoperability experience are addressed, and that the base specifications are maintained.

c) The group will also produce informational documentation, such as design rationale documents or description of specific issues within the protocol.

Deployment considerations call for:

a) solutions to enable dual-stack operation,

b) mechanisms to support high-availability home agents,

c) allowing the use of multiple interfaces in mobile nodes,

d) ways to employ Mobile IPv6 in the presence of firewalls,

e) address the specific needs of automotive and aviation communities for route optimization in network mobility,

f) support for AAA is needed as a continuation of earlier work on bootstrapping,

g) revocation of binding,

h) generic notification message format and

i) extended DSMIP home network support.

Work items related to large scale deployment include:

a) A Solution for Mobile IPv6 and NEMO session continuity for dual stack hosts which attach to IPv4 access networks. Additionally provide a mechanism for carrying IPv4 packets via the Home agent for Mobile IPv6 or NEMO capable dual-stack hosts.

b) A protocol based solution for enhancing the reliability of home agents and a method to force a host/router to switch home agents.

A mechanism to force an MN to switch the HA that is currently serving it. This is required in deployments where the HA needs to be taken offline for maintenance.

c) Use of multiple interfaces.

Today, the protocols do not provide support for simultaneous differentiated use of multiple access technologies. Several proposals exist for such support, and some of them have been implemented and tested.

When a mobile host/router uses multiple network interfaces simultaneously, or when multiple prefixes are available on a single network interface, the mobile host/router would end up with multiple Care-of Addresses (CoAs). In addition, the Home Agent might be attached to multiple network interfaces, or to a single network interface with multiple prefixes, hence resulting in the option to use multiple IP addresses for the Home Agent. This could result in the possibility of using a multitude of bi-directional tunnels between pairs of {Home Agent address, CoA} and a number of associated issues: establishment, selection and modification of multiple simultaneous tunnels.

The objective of the WG is to produce a clear problem statement and to produce standard track specifications to the problems associated with the simultaneous use of multiple addresses for either mobile hosts using Mobile IPv6 or mobile routers using NEMO Basic Support and their variants (FMIPv6, HMIPv6, etc). Where the effects of having multiple prefixes on a single interface is identical to the effects of having multiple interfaces each with a single prefix, the WG will consider a generalized approach to cater for multiple prefixes available to a mobile host/router.

The WG uses existing tunneling mechanisms defined for Mobile IPv6. The involved nodes need to select which tunnel instance to use when multiple ones are available due to multiple addresses on either end. But the WG does not plan to define a new mechanism for this, but rather document how to use existing mechanisms based upon preferences or policies. In particular, the WG will consider that a tunnel is alive as long as packets can be exchanged with the corresponding peer. In addition, local information, such as interface up/down events, or other failure detection mechanisms can be used to quickly detect failure of tunnel(s).

Deliverables related to this include:

- A document explaining the motivations for a node using multiple interfaces and the scenarios where it may end up with multiple global addresses on its interfaces [Informational]
- An analysis document explaining what are the limitations for mobile hosts using multiple simultaneous Care-of Addresses and Home Agent addresses using Mobile IPv6, whether issues are specific to Mobile IPv6 or not [Informational].
- A protocol extension to support the registration of multiple Care-of Addresses at a given Home Agent address [Standard Track].
- A "Flow/binding policies exchange" solution for an exchange of policies from the mobile host/router to the Home Agent and from the Home Agent to the mobile host/router influencing the choice of the Care-of Address and Home Agent address. The solution involves two specifications, one for the policy format and another for its transport [both Standard Track].

d) Work on solutions to deal with firewalls and the problems that firewalls cause as identified in RFC 4487.

e) Route optimization of network mobility.

Three use cases have been identified for this. These are called the Aviation case, the Automotive case, and the Personal Mobile Router (consumer electronics) case, though the actual technical problems are characterized by the type of movements and environments more than by the specific industry using the technology. The group will explore these cases to gather requirements and proceed with solving the open issues.

1. Airline and spacecraft community, who are deploying NEMO for control systems, as well as Internet connectivity and entertainment systems. This use case is characterized by fast (~ 1000 km/h) moving objects over large distances (across continents). The main technical problem is

that tunneling-based solutions imply a roundtrip to another continent and that BGP based solutions imply significant churn in the global Internet routing table.

2. Automotive industry who are deploying NEMO for in-car communication, entertainment, and data gathering, possible control systems use, and communication to roadside devices. This use case is characterized by moderately fast (~ 100-300 km/h) moving objects that employ local or cellular networks for connectivity.
3. Personal Mobile Routers, which are consumer devices that allow the user to bring a NEMO network with the user while mobile, and communicate with peer NEMO Basic Support nodes and nodes served by them.

After gathering the requirements for these types of deployments, the working group will evaluate what type of route optimization needs to be performed (if any), and formulate a solution to those problems.

If no requirements for those scenarios can be collected by the deadline, it will be assumed that the work is premature, and that type of deployment will be dropped from the WG.

The group will only consider airline and spacecraft solutions that combine tunneling solutions for small movements with either federated tunnel servers or slowly changing end host prefixes. The group will only consider personal mobile router requirements about optimized routes to another mobile router belonging to the same operator. The group will only consider automotive industry requirements to allow MR-attached hosts to directly access the network where MR has attached to. Work on automotive and personal mobile router solutions requires rechartering.

The WG will not consider extensions to routing protocols. The group will not consider general multi-homing problems that are not related to the deployment and maintenance of Mobile IPv6 or NEMO Basic Support protocols. The group will also not consider general route optimization, or other problems that are not related to the deployment and maintenance of NEMO Basic Support protocols. Similarly, the group will not consider or rely on the results of general routing architecture, Internet architecture, or identifier-locator split issues that are discussed in separate, long term efforts elsewhere in the IETF. Finally, the group will not consider solutions that require changes from correspondent nodes in the general Internet.

f) Bootstrapping mechanisms developed earlier in the MIP6 WG require AAA support for Mobile IPv6. Part of this work is already being done in the DIME WG, but the MEXT WG is chartered to complete a design for RADIUS.

g) Binding Revocation for IP Mobility: Define a binding revocation mechanism for Mobile IPv6 and its extensions. This mechanism can be used by any entity involved in the base Mobile IPv6 protocol or one of its extensions to request its corresponding entity to terminate either one, multiple or all binding cache entries.

h) Generic Notification Message for Mobile IPv6: A proposal for defining generic notification framework that can be used by the mobility entities for sending and receiving asynchronous notification messages was proposed and the same was adopted by the WG.

i) Extended DSMIPv6 Home Network Support: DSMIPv6 assumes the home network to be dual stack providing simultaneous IPv6 and IPv4 network access. It is proposed to extend DSMIPv6 to support home networks which provides IPv4, or IPv6 respectively, direct network access only, but where virtual IPv6 home network connectivity, or virtual IPv4 home network connectivity respectively, may be obtained by tunneling to the HA. The latter shall be obtained by DSMIPv6 operation using the v4HoA address as Care-of-address for the v6HoA address, and vice versa, the v6HoA address as care-of-address for the v4HoA address.

Work items related to base specification maintenance include:

a) Create and maintain issue lists that are generated on the basis of implementation and interoperability experience. Address specific issues with specific updates or revisions of the base specification. One specific area of concern that should be analyzed and addressed relates to multilink subnets.

   This work item relates only to corrections and clarifications. The working group shall not revisit design decisions or change the protocol.

b) Update the IANA considerations of RFC 3775 to allow extensions for experimental purposes as well passing of optional vendor-specific information.

c) Finish working group documents that are currently in process, and submit for RFC. This includes prefix delegation protocol mechanism for network mobility, and a MIB for NEMO Basic Support.

Work items related to informational documentation include:

a) Produce a design rationale that documents the historical thinking behind the introduction of an alternative security mechanism, the Authentication Protocol (RFC 4285).

b) Virtual Home Link configuration for Mobile IPv6: A proposal has been made on Mobile IPv6 home link configuration on virtual links. The proposal does not describe any new protocol, but provides the operational and configuration details and additionally provides implementation guidance for achieving this configuration.

The group employs IPsec and IKE as a security mechanism. The group shall refrain, however, from making generic extensions to these protocols. Any proposed extension must be reviewed by the INT and SEC ADs before it can be accepted as a part of a work item.

2.2.8.2 Goals and milestones

MEXT Working Group	
Done	Submit I-D ‘Mobile IPv6 Vendor Specific Option’ to IESG for publication as a Proposed Standard.
December 2007	Submit I-D ‘Mobile IPv6 Dual-Stack Operation’ to IESG for publication as a Proposed Standard.
December 2007	Submit I-D ‘Motivation for Authentication I-D’ to IESG for publication as Informational.
December 2007	Submit Multiple CoA Registration to IESG.
Done	Submit I-D ‘Mobile IPv6 Experimental Allocations’ to IESG for publication as a Proposed Standard.
Februrary 2008	Submit I-D 'Goals for AAA HA Interface' to IESG for publication as Informational.
February 2008	Submit -00 draft on Route Optimization needs for Personal Mobile Router.
February 2008	Submit -00 draft on Route Optimization Needs for Automobile and Highway Deployments
February 2008	Submit -00 draft on Route Optimization Needs for Aircraft and Spacecraft Deployments
March 2008	Submit the final doc on Prefix Delegation for NEMO to the IESG, for Proposed Standard
Done	Submit I-D 'Mobility Header Home Agent Switch Message' to IESG for publication as a Proposed Standard
May 2008	Submit final doc on Route Optimization needs for Personal Mobile Router, for Informational
May 2008	Submit final doc on Route Optimization Needs for Automobile and Highway Deployments, for Informational
May 2008	Submit final doc on Route Optimization Needs for Aircraft and Spacecraft Deployments, for Informational
May 2008	Submit -00 draft for solution to aircraft/spacecraft problem
June 2008	Determine how to proceed with remaining automotive/Personal Mobile Router solutions
June 2008	Submit the I-D 'RADIUS Mobile IPv6 Support' to IESG for publication as a proposed standard
June 2008	Submit 00 draft on Binding Revocation
July 2008	Submit Analysis of the use of Multiple Simultaneous Care-of Addresses and Home Agent addresses, for Informational

August 2008	Submit I-D 'Mobile IPv6 Operation with Firewalls' to IESG for publication as Informational.
August 2008	Submit the final doc on MIB for NEMO Basic Support to the IESG, for Proposed Standard
October 2008	Submit Flow/binding policy transport to IESG, for Proposed Standard
October 2008	Submit Flow/binding policy format to IESG, for Proposed Standard
October 2008	Submit draft on Binding Revocation to IESG
October 2008	Submit 00 draft on Generic Notification
November 2008	Submit final doc for solution to aircraft/spacecraft problem to the IESG, for Proposed Standard
November 2008	Recharter to work on the remaining automotive/Personal Mobile Router solutions
December 2008	Submit I-D(s) related to specific updates and corrections of RFC 3775 to IESG for publication as Proposed Standard.
December 2008	Submit I-D 'Home agent reliability' to IESG for publication as a Proposed Standard.
December 2008	Submit 00 draft on Extended DSMIPv6 Home Network support
December 2008	Submit 00 draft on Virtual Home link configuration
January 2009	Submit draft on Generic Notification to IESG
March 2009	Submit draft on Virtual Home link configuration to IESG
May 2009	Submit draft on Extended DSMIPv6 Home Network support to IESG

Tabla 8: MEXT WG Goals and milestones

2.2.8.3 Internet drafts

- Multiple Care-of Addresses Registration [91]
- NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks [92]
- AAA Goals for Mobile IPv6 [93]
- Mobile IPv6 Support for Dual Stack Hosts and Routers [94]
- Automotive Industry Requirements for NEMO Route Optimization [95]
- Flow Bindings in Mobile IPv6 and Nemo Basic Support [96]
- Mobility Support in IPv6 [97]

- DHCPv6 Prefix Delegation for NEMO [98]
- Binding Revocation for IPv6 Mobility [99]
- Guidelines for firewall administrators regarding MIPv6 traffic [100]
- Guidelines for firewall vendors regarding MIPv6 traffic [101]

2.2.8.4 Requests For Comments

- Network Mobility (NEMO) Management Information Base [102]

2.2.9 NETEXT: Network-based Mobility Extensions

2.2.9.1 Description of Working Group

Proxy Mobile IPv6, specified in RFC 5213, is a network-based mobility protocol. It uses a Mobile Access Gateway (MAG) and a Local Mobility Anchor (LMA) to allow hosts to move around within a domain while keeping their address or address prefix stable. Proxy Mobile IPv6 has been incorporated into a number of products and deployments are starting.

Certain deployment considerations, including localized routing and bulk refresh of lifetime are already emerging.

The working group will focus on the following topics relevant for network-based mobility:

Localized Routing: a specification for routing traffic between the MAG(s) without involving the LMA. That is, allow the MAG to route traffic between hosts from one MAG to another, without being tunnelled all the way to the LMA. This reduces latency and backhaul load. Applications such as voice can benefit from the reduced latency.

Bulk Refresh: a specification of improving the signaling load for binding lifetime refresh. The current specifications call for the handling of each mobility session independent of each other. When a large number of hosts are served by a single MAG, a periodic refresh of the binding lifetimes can lead to a signaling storm. The purpose of the Bulk Refresh feature is to construct a protocol feature that allows such refreshes to occur on a per-MAG basis.

LMA Redirection: a specification for allowing an LMA to redirect a MAG to another LMA. This is primarily needed as a way to perform load balancing. This functionality is complementary to implementation techniques that allow distributed MAG implementations to move tasks around without a visible impact at the protocol level, and the initial LMA discovery work in the NETLMM WG. An applicability statement describing the situations where the new functionality is or is not applicable has to be included in the specification.

The work in this charter is entirely internal to the network and does not affect hosts in any way (except perhaps through impacting packet forwarding capacity visible to the hosts).

The proposed activity will be complementary to the existing IETF Working Groups, notably the NETLMM and MEXT WGs. The NETEXT working group will also act as the primary forum where new extensions on top of the Proxy

Mobile IPv6 protocol can be developed. The addition of such new extensions to the working group involves addition of the extension to this charter through the normal rechartering process.

This initial charter excludes a number of possible work items that were discussed in the March 2009 BOF. The working group should continue the discussion about a possible update of its charter and principles under which the new work items must operate under. The completion of the work items in the initial charter is not a requirement for the rechartering to become possible.

2.2.9.2 Goals and milestones

NETEXT Working Group	
May 2009	WG chartered
July 2009	Initial WG draft on Bulk Refresh
July 2009	Decision on the inclusion of possible additional work items
September 2009	Initial WG draft on LMA Redirection
November 2009	Initial WG draft on Route Optimization
December 2009	Submit Bulk Refresh to IESG for publication as a Proposed Standard RFC
January 2010	Submit LMA Redirection to IESG for publication as a Proposed Standard RFC
April 2010	Submit Route Optimization to IESG for publication as a Proposed Standard RFC

Tabla 9: NETEXT WG Goals and milestones

2.2.9.3 Internet drafts

There are no current Internet Drafts available.

2.2.9.4 Requests For Comments

There are no Requests For Comments published.

2.2.10 SIP: Session Initiation Protocol

2.2.10.1 Introduction

There are many applications of the Internet that require the creation and management of a session, where a session is considered an exchange of data between an association of participants. The implementation of these applications is complicated by the practices of participants: users may move between endpoints they may be addressable by multiple names, and they may communicate in several different media – sometimes simultaneously. Numerous protocols have been authored that carry various forms of real-time multimedia session data such as

voice, video, or text messages. The Session Initiation Protocol (SIP) works in concert with these protocols by enabling Internet endpoints (called user agents) to discover one another and to agree on a characterization of a session they would like to share. For locating prospective session participants, and for other functions, SIP enables the creation of an infrastructure of network hosts (called proxy servers) to which user agents can send registrations, invitations to sessions, and other requests. SIP is an agile, general-purpose tool for creating, modifying, and terminating sessions that works independently of underlying transport protocols and without dependency on the type of session that is being established.

2.2.10.2 Overview of SIP functionality

SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP transparently supports name mapping and redirection services, which supports personal mobility – users can maintain a single externally visible identifier regardless of their network location.

SIP supports five facets of establishing and terminating multimedia communications:

User location: determination of the end system to be used for communication;

User availability: determination of the willingness of the called party to engage in communications;

User capabilities: determination of the media and media parameters to be used;

Session setup: “ringing”, establishment of session parameters at both called and calling party;

Session management: including transfer and termination of sessions, modifying session parameters, and invoking services.

SIP is not a vertically integrated communications system. SIP is rather a component that can be used with other IETF protocols to build a complete multimedia architecture. Typically, these architectures will include protocols such as the Real-time Transport Protocol (RTP) for transporting real-time data and providing QoS feedback, the Real-Time streaming protocol (RTSP) for controlling delivery of streaming media, the Media Gateway Control Protocol (MEGACO) for controlling gateways to the Public Switched Telephone Network (PSTN), and the Session Description Protocol (SDP) for describing multimedia sessions. Therefore, SIP should be used in conjunction with other protocols in order to provide complete services to the users. However, the basic functionality and operation of SIP does not depend on any of these protocols.

SIP does not provide services. Rather, SIP provides primitives that can be used to implement different services. For example, SIP can locate a user and deliver an opaque object to his current location. If this primitive is used to deliver a session description written in SDP, for instance, the endpoints can agree on the parameters of a session. If the same primitive is used to deliver a photo of the caller as well as

the session description, a "caller ID" service can be easily implemented. As this example shows, a single primitive is typically used to provide several different services.

SIP does not offer conference control services such as floor control or voting and does not prescribe how a conference is to be managed. SIP can be used to initiate a session that uses some other conference control protocol. Since SIP messages and the sessions they establish can pass through entirely different networks, SIP cannot, and does not, provide any kind of network resource reservation capabilities.

The nature of the services provided make security particularly important. To that end, SIP provides a suite of security services, which include denial-of-service prevention, authentication (both user to user and proxy to user), integrity protection, and encryption and privacy services.

SIP works with both IPv4 and IPv6. [122]

2.2.10.3 Modifying an Existing Session

A successful INVITE request (see Section 13 [122]) establishes both a dialog between two user agents and a session using the offer-answer model. Section 12 [122] explains how to modify an existing dialog using a target refresh request (for example, changing the remote target URI of the dialog). This section describes how to modify the actual session. This modification can involve changing addresses or ports, adding a media stream, deleting a media stream, and so on. This is accomplished by sending a new INVITE request within the same dialog that established the session. An INVITE request sent within an existing dialog is known as a re-INVITE.

Note that a single re-INVITE can modify the dialog and the parameters of the session at the same time.

Either the caller or callee can modify an existing session.

The behavior of a UA on detection of media failure is a matter of local policy. However, automated generation of re-INVITE or BYE is NOT RECOMMENDED to avoid flooding the network with traffic when there is congestion. In any case, if these messages are sent automatically, they SHOULD be sent after some randomized interval.

Note that the paragraph above refers to automatically generated BYEs and re-INVITEs. If the user hangs up upon media failure, the UA would send a BYE request as usual.

UAC Behavior

The same offer-answer model that applies to session descriptions in INVITEs (Section 13.2.1[122]) applies to re-INVITEs. As a result, a UAC that wants to add a media stream, for example, will create a new offer that contains this media stream, and send that in an INVITE request to its peer. It is important to note that the full description of the session, not just the change, is sent. This supports stateless session processing in various elements, and supports failover and recovery capabilities. Of course, a UAC MAY send a re-INVITE with no session

description, in which case the first reliable non-failure response to the re-INVITE will contain the offer (in this specification, that is a 2xx response).

If the session description format has the capability for version numbers, the offerer SHOULD indicate that the version of the session description has changed.

The To, From, Call-ID, CSeq, and Request-URI of a re-INVITE are set following the same rules as for regular requests within an existing dialog, described in Section 12[122].

A UAC MAY choose not to add an Alert-Info header field or a body with Content-Disposition "alert" to re-INVITEs because UASs do not typically alert the user upon reception of a re-INVITE.

Unlike an INVITE, which can fork, a re-INVITE will never fork, and therefore, only ever generate a single final response. The reason a re-INVITE will never fork is that the Request-URI identifies the target as the UA instance it established the dialog with, rather than identifying an address-of-record for the user.

Note that a UAC MUST NOT initiate a new INVITE transaction within a dialog while another INVITE transaction is in progress in either direction.

1. If there is an ongoing INVITE client transaction, the TU MUST wait until the transaction reaches the completed or terminated state before initiating the new INVITE.

2. If there is an ongoing INVITE server transaction, the TU MUST wait until the transaction reaches the confirmed or terminated state before initiating the new INVITE.

However, a UA MAY initiate a regular transaction while an INVITE transaction is in progress. A UA MAY also initiate an INVITE transaction while a regular transaction is in progress. If a UA receives a non-2xx final response to a re-INVITE, the session parameters MUST remain unchanged, as if no re-INVITE had been issued.

Note that, as stated in Section 12.2.1.2 [122], if the non-2xx final response is a 481 (Call/Transaction Does Not Exist), or a 408 (Request Timeout), or no response at all is received for the re-INVITE (that is, a timeout is returned by the INVITE client transaction), the UAC will terminate the dialog.

If a UAC receives a 491 response to a re-INVITE, it SHOULD start a timer with a value T chosen as follows:

1. If the UAC is the owner of the Call-ID of the dialog ID (meaning it generated the value), T has a randomly chosen value between 2.1 and 4 seconds in units of 10 ms.

2. If the UAC is not the owner of the Call-ID of the dialog ID, T has a randomly chosen value of between 0 and 2 seconds in units of 10 ms.

When the timer fires, the UAC SHOULD attempt the re-INVITE once more, if it still desires for that session modification to take place. For example, if the call was already hung up with a BYE, the re-INVITE would not take place.

The rules for transmitting a re-INVITE and for generating an ACK for a 2xx response to re-INVITE are the same as for the initial INVITE (Section 13.2.1[122]).

UAS Behavior

Section 13.3.1 [122] describes the procedure for distinguishing incoming re-INVITEs from incoming initial INVITEs and handling a re-INVITE for an existing dialog.

A UAS that receives a second INVITE before it sends the final response to a first INVITE with a lower CSeq sequence number on the same dialog MUST return a 500 (Server Internal Error) response to the second INVITE and MUST include a Retry-After header field with a randomly chosen value of between 0 and 10 seconds.

A UAS that receives an INVITE on a dialog while an INVITE it had sent on that dialog is in progress MUST return a 491 (Request Pending) response to the received INVITE.

If a UA receives a re-INVITE for an existing dialog, it MUST check any version identifiers in the session description or, if there are no version identifiers, the content of the session description to see if it has changed. If the session description has changed, the UAS MUST adjust the session parameters accordingly, possibly after asking the user for confirmation.

Versioning of the session description can be used to accommodate the capabilities of new arrivals to a conference, add or delete media, or change from a unicast to a multicast conference.

If the new session description is not acceptable, the UAS can reject it by returning a 488 (Not Acceptable Here) response for the re-INVITE. This response SHOULD include a Warning header field.

If a UAS generates a 2xx response and never receives an ACK, it SHOULD generate a BYE to terminate the dialog.

A UAS MAY choose not to generate 180 (Ringing) responses for a re-INVITE because UACs do not typically render this information to the user. For the same reason, UASs MAY choose not to use an Alert-Info header field or a body with Content-Disposition "alert" in responses to a re-INVITE.

A UAS providing an offer in a 2xx (because the INVITE did not contain an offer) SHOULD construct the offer as if the UAS were making a brand new call, subject to the constraints of sending an offer that updates an existing session, as described in [129] in the case of SDP.

Specifically, this means that it SHOULD include as many media formats and media types that the UA is willing to support. The UAS MUST ensure that the session description overlaps with its previous session description in media formats, transports, or other parameters that require support from the peer. This is to avoid the need for the peer to reject the session description. If, however, it is unacceptable to the UAC, the UAC SHOULD generate an answer with a valid session description, and then send a BYE to terminate the session.

2.3 IEEE 802.21 Media Independent Handover Services

2.3.1 Overview

2.3.1.1 Scope

This standard defines extensible IEEE 802 media access independent mechanisms that enable the optimization of handover between heterogeneous IEEE 802 networks and facilitates handover between IEEE 802 networks and cellular networks.

2.3.1.2 Purpose

The purpose is to improve the user experience of mobile devices by facilitating handover between 802 networks whether or not they are of different media types, including both wired and wireless, where handover is not otherwise defined; and to make it possible for mobile devices to perform seamless handover where the network environment supports it. These mechanisms are also usable for handovers between 802 networks and non 802 networks.

2.3.1.3 General

This standard provides link layer intelligence and other related network information to upper layers to optimize handovers between heterogeneous networks. This includes media types specified by Third Generation (3G) Partnership Project (3GPP), 3G Partnership Project 2 (3GPP2), and both wired and wireless media in the IEEE 802 family of standards. In this standard, unless otherwise noted, media refers to method/mode of accessing a telecommunication system (e.g., cable, radio, satellite), as opposed to sensory aspects of communication (e.g., audio, video).

The following items are not within the scope of this standard:

- Intra-technology handover (except for handovers across extended service sets (ESSs) in case of IEEE 802.11);
- Handover policy;
- Security mechanisms;
- Enhancements specific to particular link layer technologies that are required to support this standard; they will be carried out by those respective link-layer technology standards;
- Higher layer (layer 3 and above) enhancements that are required to support this standard.

The purpose of this standard is to enhance the experience of mobile users by facilitating handovers between heterogeneous networks. The standard addresses the support of handovers for both mobile and stationary users. For mobile users, handovers can occur when wireless link conditions change due to the users' movement. For the stationary user, handovers become imminent when the surrounding network environment changes, making one network more attractive than another.

This standard supports another important aspect of optimized handover - link adaptation. A user can choose an application that requires a higher data rate than available on the current link, necessitating a link adaptation to provide the higher rate, or necessitating a handover if the higher rate is unavailable on the current link.

In all such cases service continuity should be maintained to the extent possible during handover. As an example, when making a network transition during a phone call the handover procedures should be executed in such a way that any perceptible interruption to the conversation will be minimized.

This standard supports cooperative use of information available at the mobile node and within the network infrastructure. The mobile node is well-placed to detect available networks. The network infrastructure is well-suited to store overall network information, such as neighborhood cell lists, location of mobile nodes, and higher layer service availability. Both the mobile node and the network make decisions about connectivity. In general, both the mobile node and the network points of attachment (such as base stations and access points) can be multi-modal (i.e., capable of supporting multiple radio standards and simultaneously supporting connections on more than one radio interface).

The overall network can include a mixture of cells of drastically different sizes, such as those from IEEE 802.15, IEEE 802.11, IEEE 802.16, 3GPP, and 3GPP2, with overlapping coverage. The handover process can be initiated by measurement reports and triggers supplied by the link layers on the mobile node. The measurement reports can include metrics such as signal quality, synchronization time differences, and transmission error rates. Specifically the standard consists of the following elements:

a) A framework that enables service continuity while a mobile node (MN) transitions between heterogeneous link-layer technologies. The framework relies on the presence of a mobility management protocol stack within the network elements that support the handover. The framework presents media independent handover (MIH) reference models for different link layer technologies.

b) A set of handover-enabling functions within the protocol stacks of the network elements and a new entity created therein called the MIH Function (MIHF).

c) A media independent handover Service Access Point (called the MIH_SAP) and associated primitives are defined to provide MIH Users with access to the services of the MIHF. The MIHF provides the following services:

    i. The Media Independent Event service that detects changes in link layer properties and initiates appropriate events (triggers) from both local and remote interfaces.

    ii. The Media Independent Command service provides a set of commands for the MIH Users to control link properties that are relevant to handover and switch between links if required.

    iii. The Media Independent Information service provides the information about different networks and their services thus

enabling more effective handover decision to be made across heterogeneous networks.

d) The definition of new link layer service access points (SAPs) and associated primitives for each link-layer technology. The new primitives help the MIHF collect link information and control link behavior during handovers. If applicable, the new SAPs are recommended as amendments to the standards for the respective link-layer technology.

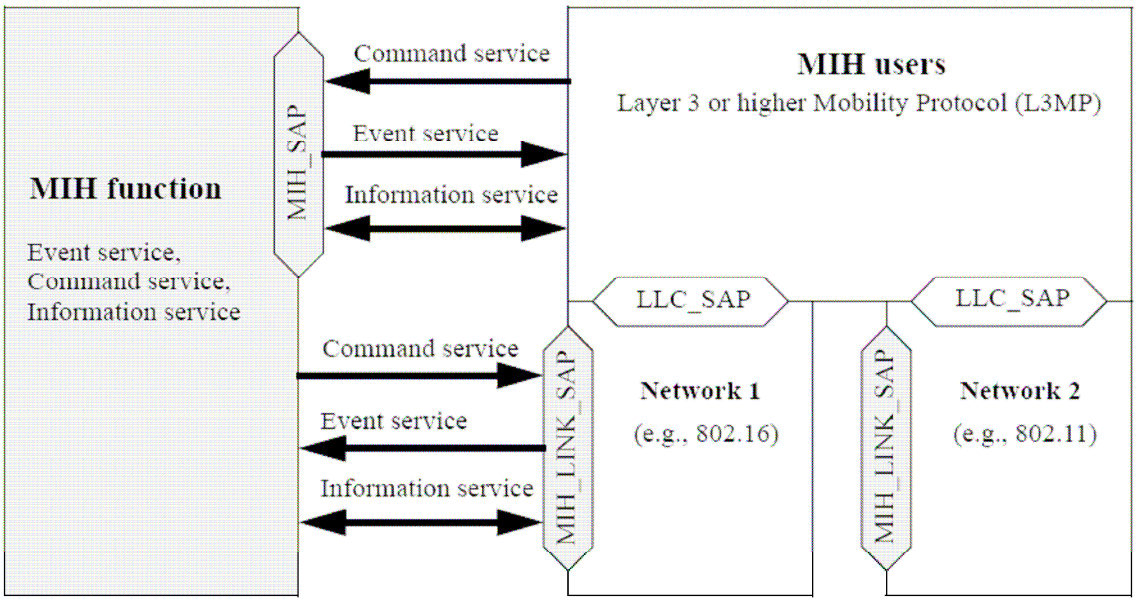


Figura 2: MIH services and their initiation

Figura 2 shows the placement of the MIHF within the protocol stack of a multiple interfaced MN or network entity. The MIHF provides services to the MIH Users through a single media independent interface (the MIH service access point) and obtains services from the lower layers through a variety of media dependent interfaces (media-specific SAPs).

2.3.1.4 Assumptions

The following assumptions have been made in the development of this standard:

a) The MN is capable of supporting multiple link-layer technologies, such as wireless, wired, or mixed;

b) The MIHF is a logical entity, whose definition is independent of its deployment location on the MN or in the network;

c) The MIHF, regardless of whether it is located on the MN or in the network, receives and transmits information about the configuration and condition of access networks around the MN. This information originates at different layers of the protocol stack within the MN or at various network elements.

   i. When the information originates at a remote network element, the MIHF on the local network element obtains it through MIH

message exchanges with a peer MIHF instance that resides in the remote network element.

ii. When the information originates at lower layers of the protocol stack within an MN or network entity, the MIHF on that entity obtains it locally through the service primitives of the SAPs that define the interface of the MIHF with the lower layers.

2.3.1.5 Media independence

The intent of this standard is to provide generic link layer intelligence independent of the specifics of mobile nodes or radio networks. As such this standard is intended to provide a generic interface between the link layer users in the mobility-management protocol stack and existing media-specific link layers, such as those specified by 3GPP, 3GPP2 and the IEEE 802 family of standards.

This standard defines SAPs and primitives that provide generic link layer intelligence. Individual media-specific technologies thereafter need to enhance their media-specific SAPs and primitives to satisfy the generic abstractions of this standard. Suitable amendments are required to existing link layer (medium access control (MAC)/ physical layer (PHY)) standards of different media-specific technologies such as IEEE Std 802.3, IEEE Std 802.11, IEEE Std 802.16, 3GPP, and 3GPP2 to satisfy the requirements of generic link layer intelligence identified by this standard.

2.3.2 General architecture

2.3.2.1 Introduction

2.3.2.1.1 General

This standard supports different handover methods. Such methods are generally classified as “hard” or “soft”, depending on whether the handover procedure is “break-before-make” or “make-before-break” with respect to the data transport facilities that support the exchange of data packets between the MN and the network.

Handover decision making involves cooperative use of both MN and network infrastructure. Handover control, handover policies and other algorithms involved in handover decision making are generally handled by communication system elements that do not fall within the scope of this standard. However, it is beneficial to describe certain aspects of the overall handover procedure so that the role and purpose of the MIH services in the handover process are clear. The following subclauses give an overview of how the different factors that affect handovers are addressed within this standard.

2.3.2.1.2 Service continuity

Service continuity is defined as the continuation of the service during and after the handover while minimizing aspects such as data loss and duration of loss of connectivity during the handover without requiring any user intervention. The change of access network need not be noticeable to the end user. However, irrespective of that, there should be no need for the user to re-establish the service. There can be a change in service quality as a consequence of the transition between different networks due to the varying capabilities and characteristics of

the access networks. For example if the quality of service (QoS) supported by the new access network is unacceptable, higher layer entities can decide not to handover or terminate the current session after the handover based on applicable policies. This standard specifies essential elements that enable service continuity.

2.3.2.1.3 Application class

Various applications have different tolerance characteristics for delay and data loss. Application aware handover decisions can be possible by making a provision for such characteristics. For example, when a network transition due to impending handover is made during the pause phase of a conversation in an active voice call, the perceptible interruption in the service is minimized.

2.3.2.1.4 Quality of service

The quality of the service (QoS) experienced by an application depends on the accuracy, speed, and availability of the information transfer in the communication channel. This standard provides support for fulfilling application QoS requirements during handover.

There are two aspects of QoS to consider in the context of IEEE 802.21. Firstly, there is the QoS experienced by an application during a handover. Secondly, there is the QoS considered as part of a handover decision. This standard includes mechanisms that support both aspects of QoS towards enabling seamless mobility; however the MIHF alone cannot guarantee seamless mobility. Depending on the QoS requirements of the end-to-end application, seamless mobility implies minimizing the handover latency and packet loss so as to minimize the end-to-end delay and the loss of transmitted information. Seamless mobility also implies the timely assessment of network conditions, such as the monitoring of packet loss on the current link and signal strength from both current and target networks, in order to optimize the handover decision and its execution.

The MIH QoS model (see Annex B [123]) defines parameters that are used to set the requirements and assess the performance of packet transfers between a source and its destinations. When used in threshold-setting commands (such as MIH_Link_Configure_Thresholds), these parameters describe the QoS requirements of the MIH User. On the other hand, when used in parameter-reporting events (such as MIH_Link_Parameters_Report) and parameter-extraction commands (such as MIH_Link_Get_Parameters), they characterize current network conditions. Therefore, depending on their usage these parameters can represent either static QoS requirements or dynamic network measurements.

2.3.2.1.5 Network discovery

This standard defines the information that helps in network discovery and specifies the means by which such information can be obtained and be made available to the MIH Users. The network information includes information about link type, link identifier, link availability, link quality, etc.

2.3.2.1.6 Network selection

Network selection is the process by which an MN or a network entity selects a network (possibly out of many available) to establish network-layer connectivity. The selection is based on various criteria such as required QoS, cost, user preferences, or the network operator's policies. This standard specifies means by

which such information can be made available to the MIH Users to enable effective network selection.

2.3.2.1.7 Power management

This standard allows the MN to discover different types of wireless networks (e.g., 802.11, 802.16 and 3GPP networks), avoiding powering-up of multiple radios and/or excessive scanning at the radios. Thus this standard minimizes power consumed by mobile devices in the discovery of potential handover candidates. Specific power management mechanisms deployed are dependent on individual link-layer technologies and the potential power management benefits from this standard only extends to the discovery of wireless networks.

2.3.2.1.8 Handover policy

The primary role of the MIHF is to facilitate handovers and provide intelligence to the network selector entity. The MIHF aids the network selector entity with the help of the Event Service, Command Service, and Information Service. The network selector entity and the handover policies that control handovers are out-side the scope of this standard.

2.3.2.2 General design principles

2.3.2.2.1 MIHF design principles

This standard is based on the following general design principles.

a) MIHF is a logical entity that facilitates handover decision making. MIH Users make handover decisions based on inputs from the MIHF.

b) MIHF provides abstracted services to higher layers. The service primitives defined by this interface are based on the technology-specific protocol entities of the different access networks. The MIHF communicates with the lower layers of the mobility-management protocol stack through technology-specific interfaces.

c) Higher layer mobility management protocols specify handover signaling mechanisms for vertical handovers. Additionally, different access network technologies have defined handover signaling mechanisms to facilitate horizontal handover. The definition of such handover signaling mechanisms is outside the scope of this standard except in the case of handovers across ESSs in 802.11.

   The role of this standard is to serve as a handover facilitating service and to maximize the efficiency of such handovers by providing appropriate link layer intelligence and network information.

d) The standard provides support for remote events. Events are advisory in nature. The decision whether to cause a handover or not based on these events is outside the scope of this standard.

e) The standard supports transparent operation with legacy equipment. IEEE 802.21 standard compatible equipment should be able to co-exist with legacy equipment.

2.3.2.2.2 QoS design principles

In the context of this standard it is assumed that applications communicate via a communication channel that is considered to be composed of several connected segments, each under a possibly different but cooperative administrative authority. Examples of such channels (e.g., for internet protocol (IP) traffic) have been detailed in International Telecommunications Union (ITU) - Telecommunication Standardization Sector (ITU-T) Recommendation Y.1540. It is generally accepted that, based on the required accuracy of information transfer, applications can be grouped into a small number of behavioral sets (ITU-T recommendation Y.1540) called Class of Service (CoS). Support for differentiation via Classes of Service is pervasive in many of the IEEE 802 based standards (IEEE Std 802.11, IEEE Std 802.1q, IEEE Std 802.16, etc.). It is assumed that the classes of service definitions used within this standard conform to ITU-T recommendation Y.1540.

2.3.2.3 MIHF service overview

2.3.2.3.1 General

This standard defines services that comprise the MIHF service; these services facilitate handovers between heterogeneous access links.

a) A Media Independent Event Service (MIES) that provides event classification, event filtering and event reporting corresponding to dynamic changes in link characteristics, link status, and link quality.

b) A Media Independent Command Service (MICS) that enables MIH Users to manage and control link behavior relevant to handovers and mobility.

c) A Media Independent Information Service (MIIS) that provides details on the characteristics and services provided by the serving and neighboring networks. The information enables effective system access and effective handover decisions.

The MIHF provides asynchronous and synchronous services through well-defined SAPs for link layers and MIH Users. In the case of a system with multiple network interfaces of arbitrary type, the MIH Users use the Event Service, Command Service and Information Service provided by MIHF to manage, determine, and control the state of the underlying interfaces.

These services provided by MIHF help the MIH Users in maintaining service continuity, service adaptation to varying quality of service, battery life conservation, network discovery, and link selection. In a system containing heterogeneous network interfaces of IEEE 802 types and cellular (3GPP, 3GPP2) types, the MIHF helps the MIH Users to implement effective procedures to couple services across heterogeneous network interfaces. MIH Users utilize services provided by the MIHF across different entities to query resources required for a handover operation between heterogeneous networks.

MIH Services in mobile nodes facilitate seamless handovers between heterogeneous networks. MIH Services are used by MIH Users such as a mobility management protocol (e.g., Mobile IP). Other mobility management protocols (in addition to Mobile IP) and even other MIH Users are not precluded from making use of MIH Services.

2.3.2.3.2 Media independent event service

General

Events indicate changes in state and transmission behavior of the physical, data link and logical link layers, or predict state changes of these layers. The Event Service is also used to indicate management actions or command status on the part of the network or some management entity.

Event origination

Events originate from the MIHF (MIH Events) or any lower layer (Link Events) within the protocol stack of an MN or network node.

Event destination

The destination of an event is the MIHF or any upper layer entity. The recipient of the event is located within the node that originated the event or within a remote node. The destination of an event is established with a subscription mechanism that enables an MN or network node to subscribe its interest in particular event types.

Event service flow

In the case of local events, messages often propagate from the lower layers (e.g., PHY, MAC) to the MIHF and from MIHF to any upper layer. In case of remote events, messages propagate from the MIHF in one protocol stack to the MIHF in the peer protocol stack. One of the protocol stacks can be present in an MN while the other can be present in a fixed network entity. This network entity is the point of attachment or any node not directly connected to the other protocol stack.

Event service use cases and functions

The event service is used to detect the need for handovers. For example, an indication that the link will cease to carry MAC service data units (SDUs) at some point in the near future is used by MIH Users to prepare a new point of attachment ahead of the current point of attachment ceasing to carry frames. This has the potential to reduce the time needed to handover between attachment points. Events carry additional context data such as a layer 2 (MAC and/or LLC) (L2) identifier or L3 identifier. A Link_Up event can also carry a new IP address acquisition indication that informs the upper layers of the need to initiate a layer 3 handover.

2.3.2.3.3 Media independent command service

General

The command service enables higher layers to control the physical, data link, and logical link layers (also known as “lower layers”). The higher layers control the reconfiguration or selection of an appropriate link through a set of handover commands. If an MIHF supports the command service, all MIH commands are mandatory in nature. When an MIHF receives a command, it is always expected to execute the command.

Command origination

Commands are invoked by MIH Users (MIH Commands), as well as by the MIHF itself (Link Commands).

Command destination

The destination of a command is the MIHF or any lower layer. The recipient of a command is located within the protocol stack that originated the command, or within a remote protocol stack.

Command service flow

In the case of local commands, messages often propagate from the MIH Users (e.g., policy engine) to the MIHF and then from MIHF to lower layers. In the case of remote commands, messages propagate from MIH Users via MIHF in one protocol stack to the MIHF in a peer protocol stack (with the use of the MIH Protocol). One of the protocol stacks can be present in an MN while the other can be present in a fixed network entity. This network entity is either a point of attachment or any node not directly connected to the other protocol stack.

Command service use cases and functions

The commands generally carry the upper layer decisions to the lower layers on the local device entity or at the remote entity. For example the command service can be used by the policy engine of an entity in the network to request an MN to switch between links (remote command to lower layers on MN protocol stack).

This standard facilitates both mobile-initiated and network-initiated handovers. Handovers are initiated by changes in the wireless environment that leads to the selection of a network that supports a different access technology other than the serving network.

During network selection, the MN and the network need to exchange information about available candidate networks and select the best network. The network selection policy engine can select a different network than the current one, which can necessitate an inter-technology handover. Network selection and handover initiation are outside the scope of mobility management protocols such as mobile IP (MIP) and session initiation protocol (SIP). Once a new network has been selected and handover has been initiated, mobility management protocols handle packet routing aspects such as address update and transfer of packet delivery to the new network.

This standard supports a set of media independent commands that help with network selection under different conditions. These commands allow both the MN and the network to initiate handovers and exchange information about available networks and negotiate the best available network under different conditions. Please refer to the flow diagrams in Apéndice B for more information. These commands do not affect packet routing aspects and can be used in conjunction with other mobility management protocols such as MIP and SIP to perform inter-technology handovers.

2.3.2.3.4 Media independent information service

The Media Independent Information Service (MIIS) provides a framework and corresponding mechanisms by which an MIHF entity can discover and obtain network information existing within a geographical area to facilitate the handovers.

The neighboring network information discovered and obtained by this framework and mechanisms can also be used in conjunction with user and network

operator policies for optimum initial network selection and access (attachment), or network re-selection in idle mode.

MIIS primarily provides a set of information elements (IEs), the information structure and its representation, and a query/response type of mechanism (pull mode) for information transfer. The information can also include inter-technology handover policies. The definition of such policies is outside the scope of this standard. MIIS also supports a push mode wherein the information can be pushed to the MN by the operator. The information can be present in an information server from where the MIHF in the MN accesses it. The definition of the information server is outside the scope of this standard. In other cases information can be present locally in the MN, and can be learned by the MN or pre-provisioned, or both. The definition of and indexing of such a local database, as well as the regime for maintaining it or accessing it, are outside the scope of this standard.

The information is made available via both lower and higher layers. Information is made available at L2 through both a secure and a non-secure port. Information available through the non-secure port allows a network selection decision to be made before incurring the overhead of authentication and the establishment of a secure L2 connection with the network.

In certain scenarios information cannot be accessed at L2, or the information available at L2 is not sufficient to make an intelligent handover decision. In such cases information can be accessed via higher layers. Hence this standard enables both L2 and L3 transport options for information access. The selected transport option is expected to provide security, such as data integrity and data confidentiality, for the information access.

MIIS typically provides static link layer parameters such as channel information, the MAC address and security information of a point of attachment (PoA). Information about available higher layer services in a network can also help in more effective handover decision making before the MN actually attaches to any particular network.

The information provided by MIIS conforms to the structure and semantics specified within this standard. MIIS specifies a common (or media independent) way of representing this information across different technologies by using a standardized format such as extensible mark-up language (XML) or binary encoding. A structure of information is defined as a schema.

MIIS provides the ability to access information about all networks in a geographical area from any single L2 network, depending on how the IEEE 802.21 MIIS service is implemented. MIIS either relies on existing access media specific transports and security mechanisms or L3 transport and L3 security mechanisms to provide access to the information. How this information is developed and deployed in a given network is outside the scope of the standard. Typically, in a heterogeneous network composed of multiple media types, the network selector or higher layer mobility management will collect information from different media types and assemble a consolidated view to facilitate its inter-media handover decision.

Some networks such as the cellular networks already have an existing means of detecting a list of neighborhood base stations within the vicinity of an area via the broadcast control channel. Some IEEE standards define similar means and support

MNs in detecting a list of neighborhood access points within the vicinity of an area via either beaconing or via the broadcast of MAC management messages. MIIS defines a unified mechanism to the higher layer entities to provide handover candidate information in a heterogeneous network environment by a given geographical location. However, the algorithm for deciding what information to provide is out of scope. In the larger view, the objective is to help the higher layer mobility protocol to acquire a global view of the heterogeneous networks to effect seamless handover across these networks.

2.3.2.4 Media independent handover reference framework

2.3.2.4.1 General

The following subclause describes the key points with regards to communication between different MIHF entities in the MN and the network.

2.3.2.4.2 MIHF communication model

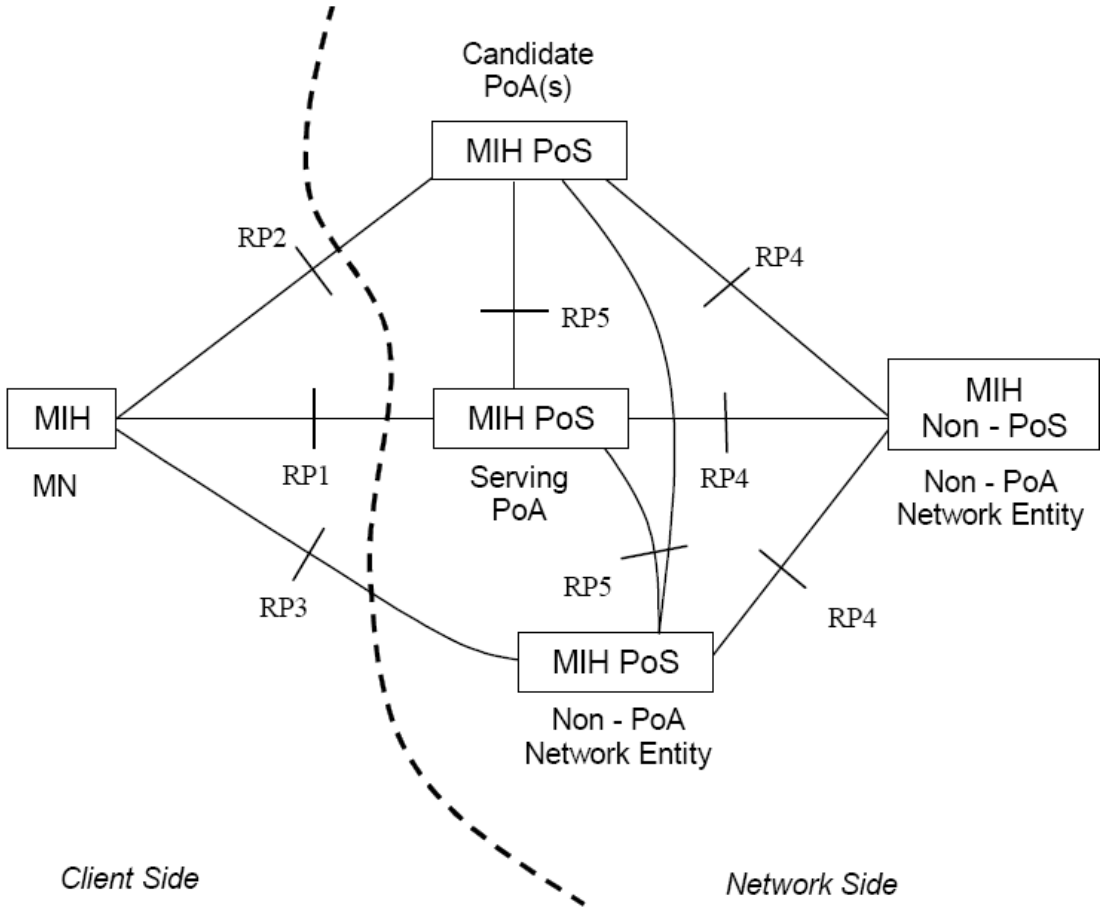


Figura 3: MIHF communication model

MIH Functions communicate with each other for various purposes. The MN exchanges MIH information with its MIH Point of Service. The MIHF in any Network Entity becomes an MIH point of service (PoS) when it communicates directly with an MN-based MIHF. When an MIHF in a Network Entity does not have a direct connection to the MN, it does not act as an MIH PoS for that particular MN. However the same MIH Network Entity can still act as MIH PoS for a different MN.

An MN can have multiple L2 interfaces. However MIHF communication need not take place on all L2 interfaces of an MIH-capable MN. As an example, on an MIH-capable MN with three L2 interfaces, namely IEEE 802.11, IEEE 802.16, and IEEE 802.3, the IEEE 802.3 interface might be used only for system administration and maintenance operations, while the IEEE 802.11 and IEEE 802.16 interfaces might engage in the provisioning of MIHF services. The MN can use L2 transport for exchanging MIH information with an MIH PoS that resides in the same Network Entity as its Network PoA. The MN can use L3 transport for exchanging MIH information with an MIH PoS that does not reside in the same Network Entity as its Network PoA. The framework supports use of either L2 or L3 mechanisms for communication among MIH network entities.

Figura 3 shows the MIHF communication model. The model shows MIHFs in different roles and the communication relationships amongst them. The communication relationship shown in Figura 3 applies only to MIHFs. It is important to note that each of the communication relationships in the communication model does not imply a particular transport mechanism. Rather, a communication relationship only intends to show that passing MIHF related information is possible between the two different MIHFs. Moreover, each communication relationship shown in the diagram encompasses different types of interfaces, different transport mechanisms used (e.g., L2, L3), and different MIHF service related content being passed (e.g., MIIS, MICS, or MIES).

The communication model assigns different roles to the MIHF depending on its position in the system.

a) MIHF on the MN

b) MIH PoS on the Network Entity that includes the serving PoA of the MN

c) MIH PoS on the Network Entity that includes a candidate PoA for the MN

d) MIH PoS on a Network Entity that does not include a PoA for the MN

e) MIH non-PoS on a Network Entity that does not include a PoA for the MN

The communication model also identifies the following reference points between different instances of MIHFs.

- **Reference point RP1:** Reference point RP1 refers to MIHF procedures between the MIHF on the MN and the MIH PoS on the Network Entity of its serving PoA. RP1 encompasses communication interfaces over both L2 and L3 and above. MIHF content passed over RP1 are related to MIIS, MIES, or MICS.
- **Reference point RP2:** Reference point RP2 refers to MIHF procedures between the MIHF on the MN and the MIH PoS on the Network Entity of a candidate PoA. RP2 encompasses communication interfaces over both L2 and L3 and above. MIHF content passed over RP2 are related to MIIS, MIES, or MICS.
- **Reference point RP3:** Reference point RP3 refers to MIHF procedures between the MIHF on the MN and the MIH PoS on a non-PoA Network Entity. RP3 encompasses communication interfaces over L3 and above and possibly L2 transport protocols like Ethernet bridging, or multi-

protocol label switching (MPLS). MIHF content passed over RP3 are related to MIIS, MIES, or MICS.

- **Reference point RP4:** Reference point RP4 refers to MIHF procedures between an MIH PoS in a Network Entity and an MIH non-PoS instance in another Network Entity. RP4 encompasses communication interfaces over L3 and above. MIHF content passed over RP4 are related to MIIS, MIES, or MICS.
- **Reference point RP5:** Reference point RP5 refers to MIHF procedures between two MIH PoS instances in different Network Entities. RP5 encompasses communication interfaces over L3 and above. MIHF content passed over RP5 are related to MIIS, MIES, or MICS. All reference point definitions are within the scope of this standard. Annex D[123] provides a mapping of various MIH messages to the reference points.

2.3.2.4.3 A deployment example for the MIH services

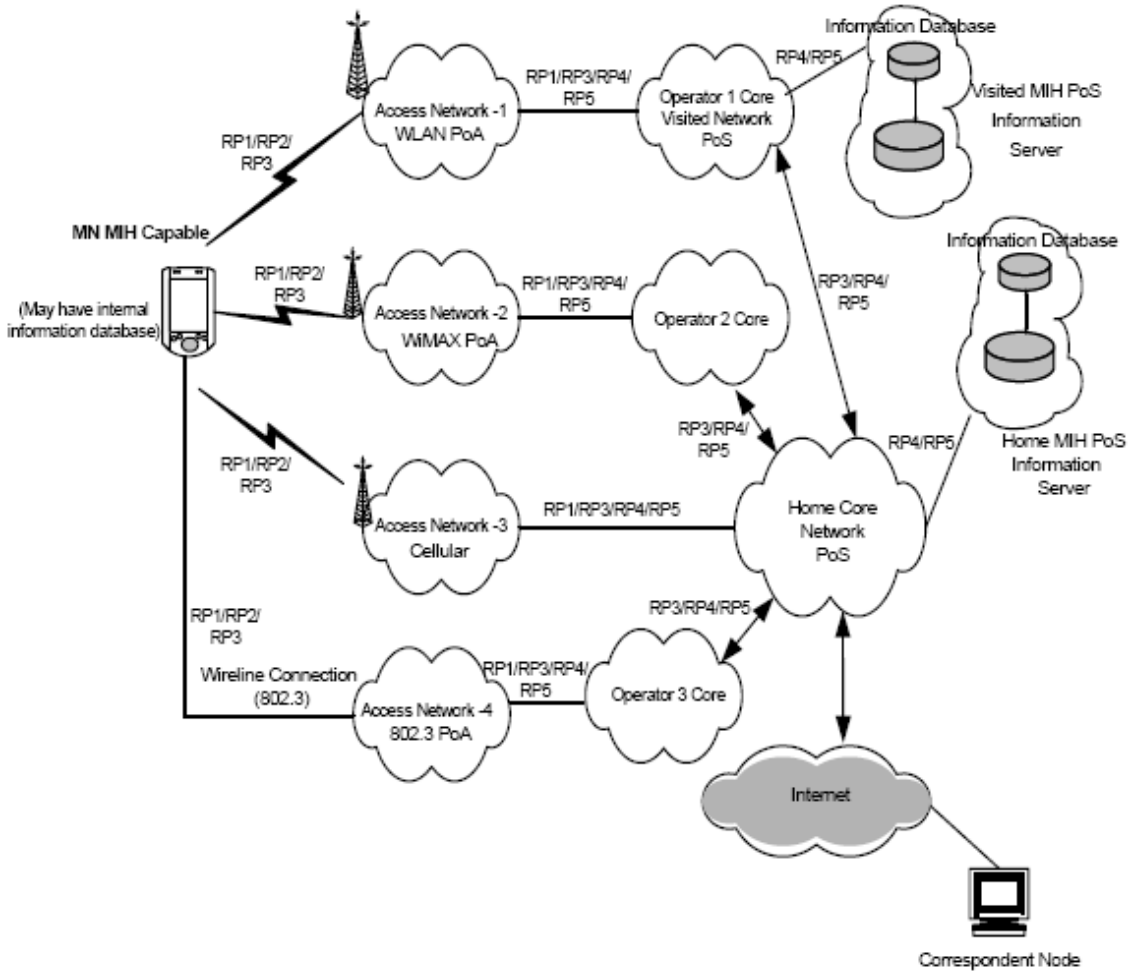


Figura 4: Example of network model with MIH services

A network model including MIH services is shown in Figura 4 to better illustrate the MIH Reference Points. Moving from left to right, the model includes an MIH-capable mobile node (MN, far left) that supports multiple wired and wireless access technologies. The model assumes that the serving network either operates multiple link-layer technologies or allows its user to roam into other networks when a service level agreement (SLA) in support of inter-working has been established.

The model illustrates access networks that are connected in some loose, serial way to a given core network (i.e., Core Operator 1, 2, or 3). Also depicted is an access network that is more tightly coupled (Access Network3). Not depicted in Figura 4, an access network can also connect to a core network via the Internet. Each Core Operator network (1, 2, or 3) might represent a service provider, corporate intranet provider, or just another part of the visited or home access. In this depicted model the provisioning provider is operating Access Network-3, which couples the terminal to the core (labeled Home Core Network) via RP1. At any given point in time, the subscriber's serving network can be the home subscriber network or a visited network.

The network providers offer MIH services in their access networks (Access Network-1 to 4) in order to facilitate heterogeneous handovers into their networks. Each access technology either advertises its MIH capability or responds to MIH service discovery. Each service provider for these access networks allows access to one or more MIH Points of Service (PoS) node(s). These PoS nodes provide some or all of the MIH services as determined during the MIH capabilities discovery. The PoS location varies based on the operator deployment scenario and the technology-specific MIH architecture.

An MIH PoS resides next to, or is co-located with, the point of attachment (PoA) node in the access network (e.g., Access Network 1, 2, 4). Alternatively the PoS can reside deeper inside the access or core networks (e.g., Access Network 3). As shown in Figura 4, the MIH entity in the MN can communicate with MIH network entities using reference points RP1, RP2, or RP3 over any of the available access network. If the PoA in the serving access network has a co-located MIHF, the RP1 reference point terminates at the PoA that is also the PoS (MN to Access Network 1, 2, 4 of the model can all be RP1). In that case an RP3 reference point would be terminated at any non-PoA (illustrated by MN connectivity to Access Networks 1, 2, 4). MIH events originate at both sides of an active RP1 link. The MN is typically the first node to react to these events.

The interaction of visited and home subscriber networks could be either for control and management purposes or for data transport purposes. It is also possible that due to roaming or SLA agreements, the home subscriber network allows the MN to access the public Internet directly through a visited network. As illustrated, two MIH network entities communicate with each other via RP4 or RP5 reference points. The MIH capable PoA communicate with other MIH network entities via RP4 and RP5 reference points. The MIH capable MN have MIH communication with other PoA in the candidate access networks via RP2 reference point to obtain Information Services about the candidate network.

With regard to the MIH Information Service, visited providers can offer access to their information server located in an MIH PoS node (upper far right). The operator provides the MIIS to mobile nodes so they can obtain pertinent

information including, but not limited to, new roaming lists, costs, provider identification information, provider services, priorities and any other information that would enable the selection and utilization of these services. As illustrated, it is possible for the MN to be pre-provisioned with MIIS data by its provider. It is also possible for the MN to obtain MIH Information Services from any access network of its service provider or from visited networks that maintain SLA agreements with the MN's service provider. MIIS can also be available from another overlapping or nearby visited network, using that network's MIIS point of service. The serving network utilizes RP4 and RP5 interfaces to access other MIH entities. As an example, in Figura 4 the home subscriber network accesses its own MIH information server or core operator 1 (visited network) MIH information server.

2.3.2.5 MIHF reference models for link-layer technologies

The MIHF provides asynchronous and synchronous services through well-defined Service Access Points for MIH Users. The following subclauses describe the reference models for various link-layer technologies with MIH functionality.

2.3.2.5.1 IEEE 802 architectural considerations

The MIH reference models for different IEEE 802 technologies and the general MIH framework is designed to be consistent with the IEEE 802 Architecture for different link layer technologies. The MIH Function is a management entity that obtains link layer information from lower layers of different protocol stacks and also from other remote nodes. The MIH Function co-ordinates handover decision making with other peer MIH Functions in the network.

The MIH Protocol provides the capability for transferring MIH messages between peer MIH Function entities at L2 or at L3. These messages transfer information about different available networks and also provide network switching and handover capability across different networks. The MIH protocol encompasses IEEE 802 technologies such as IEEE 802.11 and IEEE 802.16 and also other non IEEE 802 technologies such as those specified by 3GPP and 3GPP2 standards. In this sense the MIH Protocol has different scope and functionality than the Link Layer Discovery Protocol (LLDP) as specified by the IEEE Std 802.1AB[130].

2.3.2.5.2 General MIHF reference model and SAPs

Figura 5 illustrates the position of the MIHF in a protocol stack and the interaction of the MIHF with other elements of the system. All exchanges between the MIHF and other functional entities occur through service primitives, grouped in Service Access Points (SAPs).

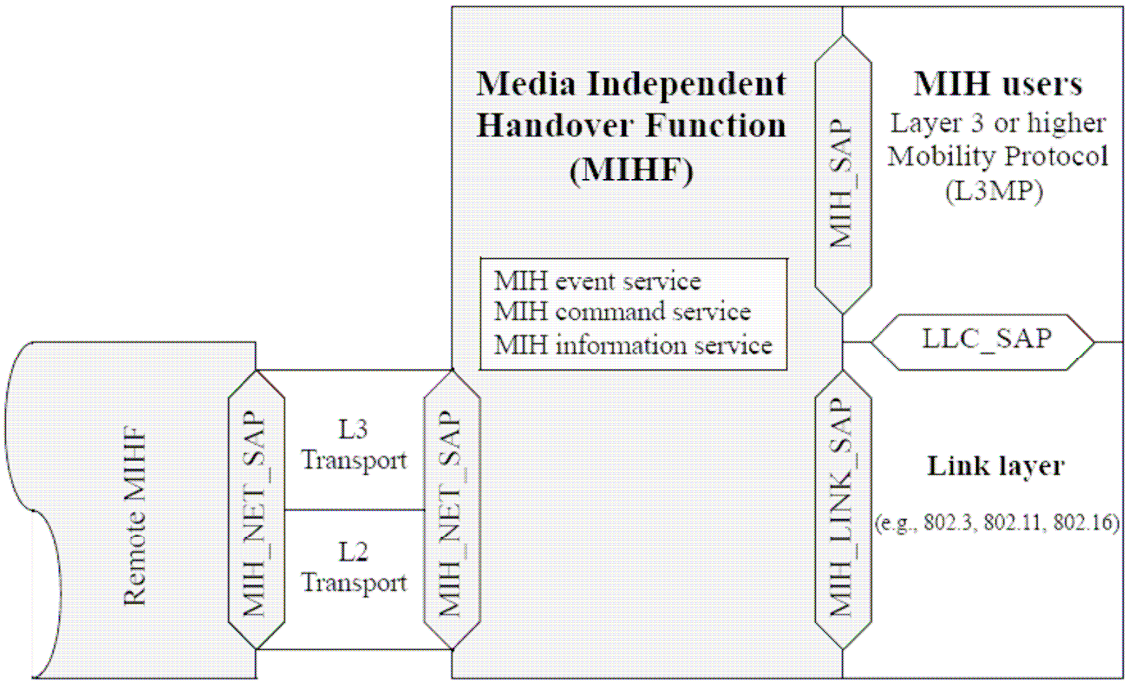


Figura 5: General MIHF reference model and SAPs

The media agnostic General MIH Reference Model includes the following SAPs:

a) MIH_SAP: Media independent interface of MIHF with the upper layers of the protocol stack.

b) MIH_LINK_SAP: Abstract media dependent interface of MIHF with the lower layers of the media-specific protocol stacks.

c) MIH_NET_SAP: Abstract media dependent interface of MIHF that provides transport services over the data plane on the local node, supporting the exchange of MIH information and messages with the remote MIHF. For all transport services over L2, the MIH_NET_SAP uses the primitives specified by the MIH_LINK_SAP.

In the media-specific reference models, the media independent SAP (MIH_SAP) always maintains the same name and same set of primitives. The media dependent SAP (which is a technology specific instantiation of the MIH_LINK_SAP), assumes media-specific names and sets of primitives, often reusing names and primitives that already exist in the respective media-specific existing lower-layer SAPs. Primitives defined in MIH_LINK_SAP result in amendments to media-specific SAPs due to additional functionality being defined for interfacing with the MIHF. All communications of the MIHF with the lower layers of media-specific protocol stacks take place through media-specific instantiations of MIH_LINK_SAP.

The message exchanges between peer MIHF instances, in particular the type of transport that they use, are sensitive to several factors, such as the nature of the network nodes that contain the peer MIHF instances (whether or not one of the two is an MN or a PoA), the nature of the access network (whether IEEE 802 or 3G cellular), and the availability of MIH capabilities at the PoA.

Figura 6 presents a summary of the types of relationships that can exist between the MIHF and other functional components in the same network node.

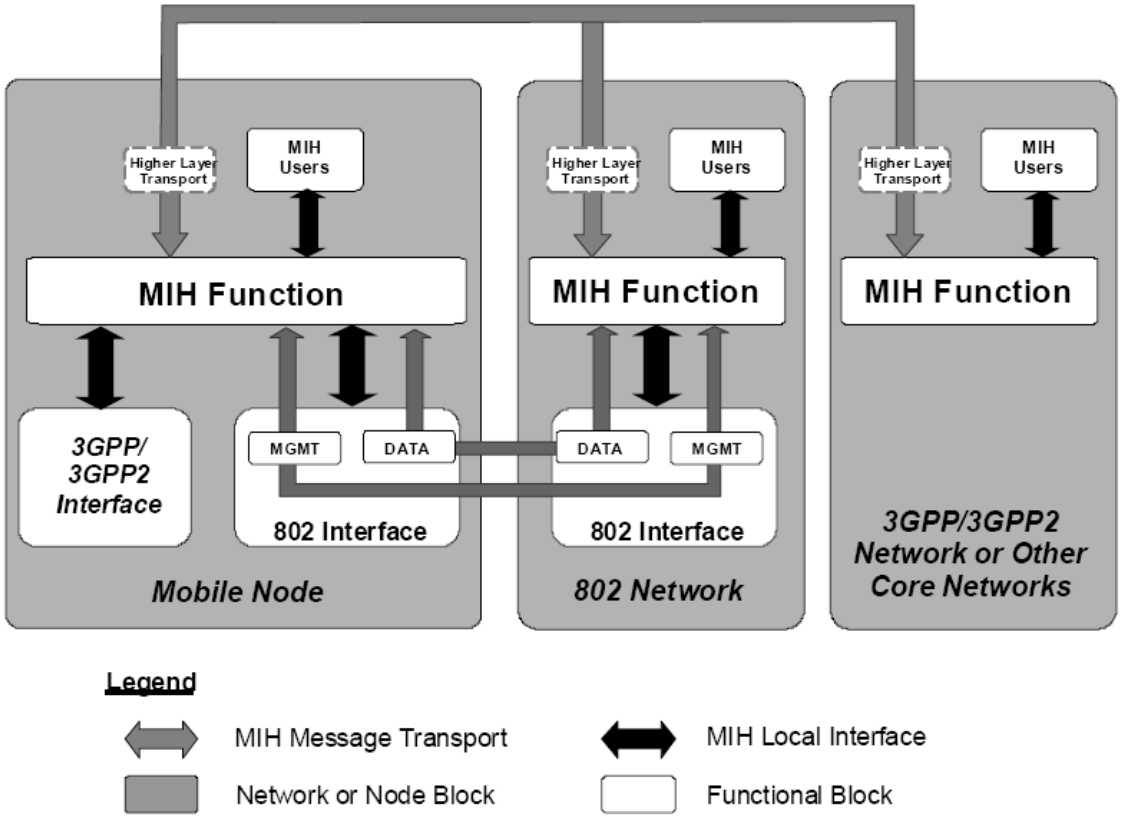


Figura 6: Types of MIHF relationship

The general MIH reference model in Figura 5 enables a simple representation of the broad variety of MIHF relationships shown in Figura 6. In the model, a mobility-management protocol stack is logically identified within each network node that includes an MIHF instance. The provided abstraction makes it easy to isolate and represent the MIH relationships with all pre-existing functional entities within the same network node. Such relationships are both internal (with functional entities that, just like the MIHF, share the logical inclusion in the mobility-management protocol) and external (with functional entities that belong to other planes).

Figura 6 shows how an MIH-enabled MN communicates with an MIH-enabled network. The grey arrows show the MIH signaling over the network, whereas the black arrows show local interactions between the MIHF and lower and higher layers in the same network or node block. For a more detailed view of local interactions, please refer to technology-specific reference models and Service Access Point in the following subclauses.

When connected to an IEEE 802 network, an MN directly uses L2 for exchanging MIH signaling, as the peer MIHF can be embedded in a PoA. The MN does this for certain IEEE 802 networks even before being authenticated with the network. However, the MN can also use L3 for exchanging MIH signaling, for example in cases where the peer MIHF is not located in the PoA, but deeper in the network.

When connected to a 3GPP or 3GPP2 network, an MN uses L3 transport to conduct MIH signaling.

2.3.2.5.3 MIHF reference model for IEEE 802.3

The MIHF reference model for IEEE 802.3 is illustrated in Figura 7. The transport of MIHF services is supported over the data plane by use of existing primitives defined by the logical link control service access point (LSAP). There are no amendments specified in IEEE Std 802.3 to support any link services defined over the MIH_LINK_SAP in this specification.

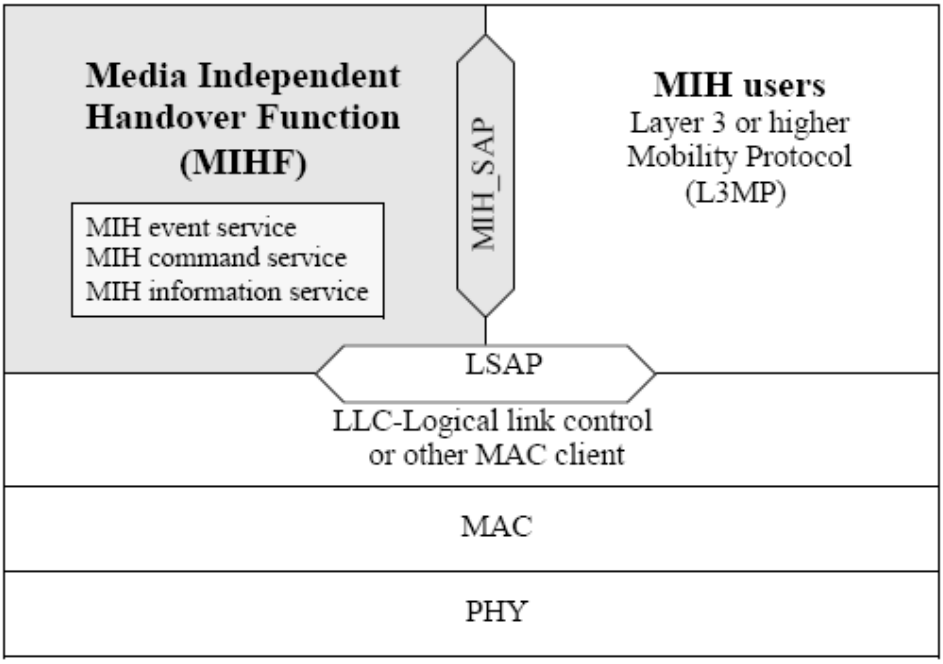


Figura 7: MIHF reference model for IEEE 802.3

2.3.2.5.4 MIHF reference model for IEEE 802.11

Figura 8 shows the MIHF reference model for IEEE 802.11. The payload of MIHF services over IEEE 802.11 is carried either in the data frames by using existing primitives defined by the LSAP or by using primitives defined by the MAC State Generic Convergence Function (MSGCF) service access point (SAP) (MSGCF_SAP). The MSGCF has access to all management primitives and provides services to higher layers.

It should be noted that sending MIHF payload over the LSAP is allowed only after successful authentication and association of the station to the access point (AP). Moreover, before the station has authenticated and associated with the AP, only MIH Information Service and MIH Capability Discovery messages can be transported over the MSGCF_SAP. The MIH_SAP specifies the interface of the MIHF with MIH Users.

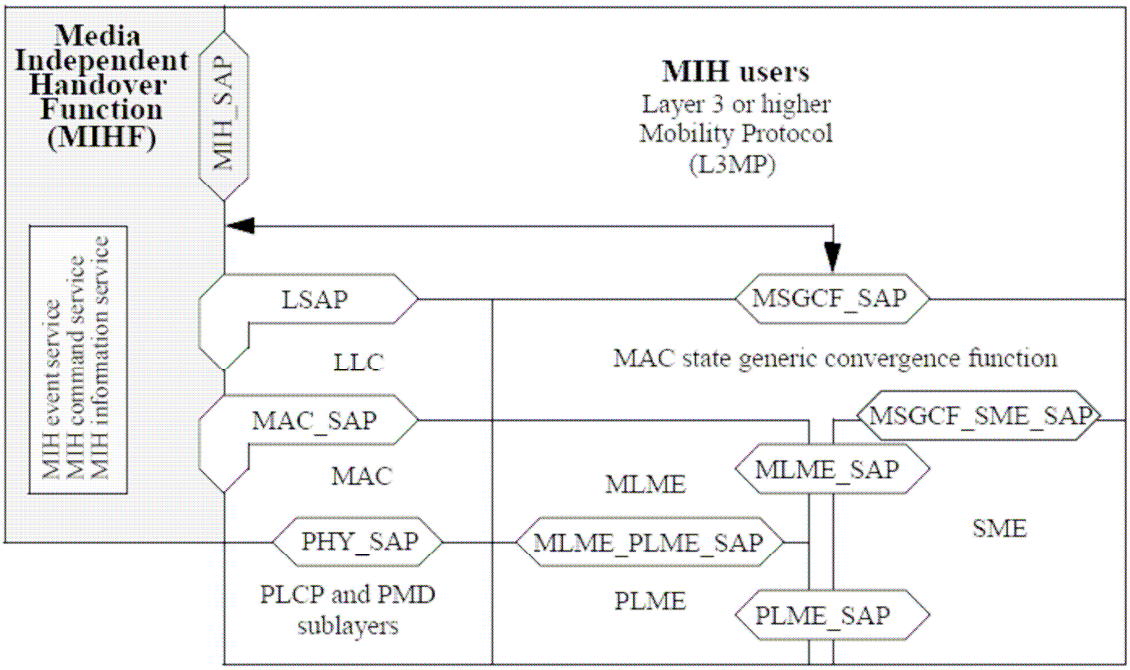


Figura 8: MIHF reference model for IEEE 802.11

2.3.2.5.5 MIHF reference model for IEEE 802.16

Figura 9 shows the MIHF for IEEE 802.16 based systems. The Management SAP (M_SAP) and Control SAP (C_SAP) are common between the MIHF and Network Control and Management System (NCMS).

The M_SAP specifies the interface between the MIHF and the management plane and allows MIHF payload to be encapsulated in management messages (such as MOB_MIH-MSG defined in [125]). The primitives specified by M_SAP are used by an MN to transfer packets to a base station (BS), both before and after it has completed the network entry procedures. The C_SAP specifies the interface between the MIHF and control plane. M_SAP and C_SAP also transport MIH messages to peer MIHF entities. The Convergence Sub-layer SAP (CS_SAP) is used to transfer packets from higher layer protocol entities after appropriate connections have been established with the network.

The MIH_SAP specifies the interface of the MIHF with other higher layer entities such as transport layer, handover policy engine, and layer 3 mobility protocol.

In the below model, C_SAP and M_SAP provide link services defined by MIH_LINK_SAP, C_SAP provides services before network entry, while CS_SAP provides services over the data plane after network entry.

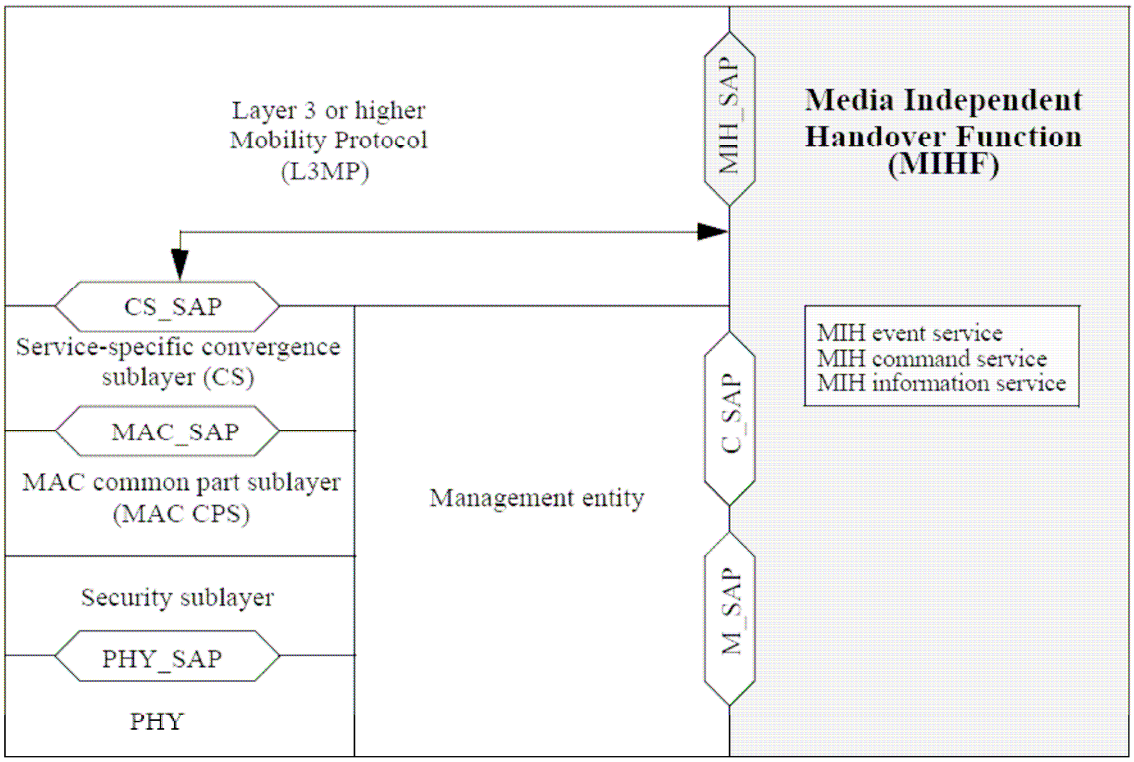


Figura 9: MIHF reference model for IEEE 802.16

2.3.2.5.6 MIHF reference model for 3GPP

Figura 10 illustrates the interaction between the MIHF and the 3GPP based systems. The MIHF services are specified by the MIH_3GLINK_SAP. However no new primitives or protocols need to be defined in the 3GPP specification for accessing these services. The MIHF services are mapped to existing 3GPP signaling functions (see Table E.3 in Annex E [123]). The architectural placement of the MIHF is also decided by the 3GPP standard. Figura 10 is for illustrative purposes only and should not constrain implementations.

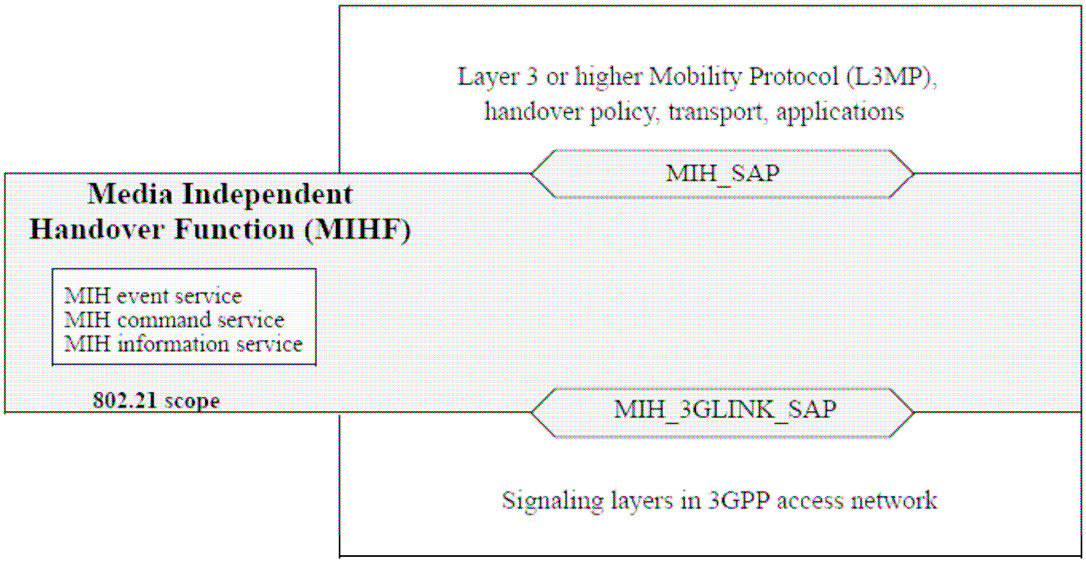


Figura 10: MIHF reference model for 3GPP systems

2.3.2.5.7 MIHF reference model for 3GPP2

Figura 11 illustrates the interaction between IEEE 802.21 services and 3GPP2 based systems. IEEE 802.21 services are accessed through the MIH_3GLINK_SAP. However note that no new primitives or protocols need to be defined within the 3GPP2 specification. Instead, a mapping between IEEE 802.21 Link Layer primitives and 3GPP2 primitives as defined in Internet Engineering Task Force (IETF) request for comment (RFC) 1661 and 3GPP2 C.S0004-D is already established. Primitive information available from Upper Layer Signaling and Point-to-Point Protocol (PPP) can be directly used by mapping LAC SAP and PPP SAP primitives to IEEE 802.21 service primitives in order to generate an event.

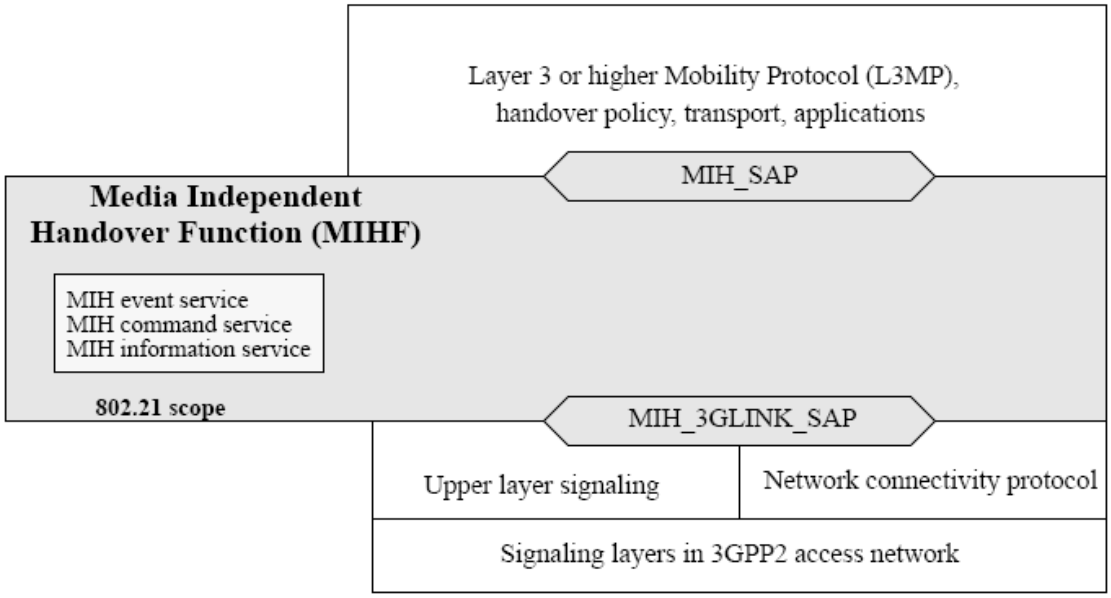


Figura 11: MIHF reference model for 3GPP2 systems

This mapping is illustrated in Table E.3 [123], which provides an example of how 3GPP and 3GPP2 primitives can be mapped to IEEE 802.21 primitives. For example, events received from the Upper Layer Signaling through the LAC layer SAP such as “L2.Condition.Notification” can be mapped and generated through the MIH_3GLINK_SAP as a Link_Up, Link_Down, or Link_Going_Down. Likewise, events generated at the PPP SAP within the PPP layer, such as LCP-Link-Up or IPCP_LINK_OPEN, could be mapped and generated through the MIH_3GLINK_SAP as a Link_Up event. It is noteworthy that there will be no direct communication between the 3GPP2 PHY and MAC layers with the MIHF. The architectural placement of any MIHF is left to 3GPP2. Figura 11 is for illustrative purposes only and should not constrain implementations.

2.3.3 MIHF services

The MIHF provides the Media Independent Event Service, the Media Independent Command Service, and the Media Independent Information Service that facilitate handovers across heterogeneous networks. In this clause a general description of these services is provided.

2.3.3.1 Media Independent Event Service

In general, handovers can be initiated either by the MN or by the network. Events relevant to handover originate from MAC, PHY or MIHF at the MN, at the network PoA, or at the PoS. Thus, the source of these events is either local or remote entity. A transport protocol is needed for supporting remote events. Security is another important consideration in such transport protocols.

Multiple higher layer entities can be interested in these events at the same time. Thus these events can have multiple destinations. Higher layer entities can subscribe to receive event notifications from a particular event source. The MIHF can help in dispatching these events to multiple destinations.

These events are treated as discrete events. As such there is no general event state machine. Event notifications are generated asynchronously. Thus, all MIH Users and MIHFs that want to receive event notifications need to subscribe to particular events.

From the recipient's perspective these events are mostly “advisory” in nature and not “mandatory”. The recipient is not obligated to act on these events. Layer 3 and above entities need to deal with reliability and robustness issues associated with these events. Higher layer protocols and other entities can take a more cautious approach when events originate remotely as opposed to when they originate locally. These events can also be used for horizontal handovers.

The Event Service is broadly divided into two categories, Link Events and MIH Events. Both Link and MIH Events traverse from a lower to a higher layer. Link Events are defined as events that originate from event source entities below the MIHF and terminate at the MIHF. Entities generating Link Events include, but are not limited to, various IEEE 802-defined, 3GPP-defined, and 3GPP2-defined interfaces. Within the MIHF, Link Events propagate further, with or without additional processing, to MIH Users that have subscribed for the specific events. MIH events are defined as events that originate from within the MIHF, or they are Link Events that are propagated by the MIHF to the MIH Users. This relationship is shown in Figura 12.

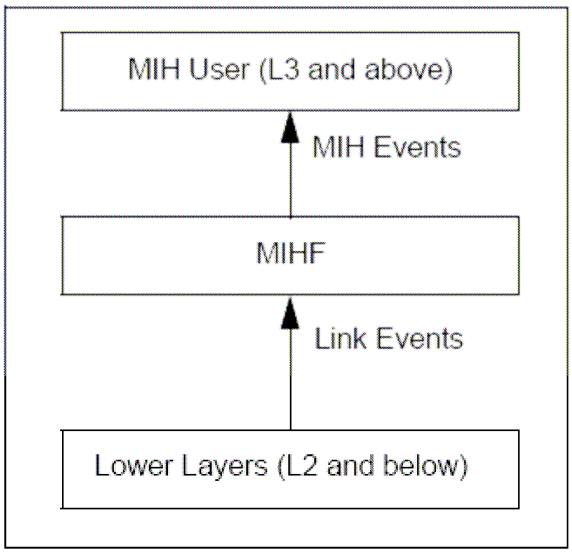


Figura 12: Link events and MIH events

An event can be local or remote; a local event is one that propagates across different layers within the local protocol stack of an MIH entity, while a remote event is one that traverses across the network medium from one MIH entity to another MIH entity.

All Link Events are local in nature and propagate from the local lower layer to the local MIHF. MIH Events are local or remote. A remote MIH Event traverses the medium from a remote MIHF to the local MIHF and is then dispatched to local MIH Users that have subscribed to this remote event, as shown in Figura 13.

A Link Event that is received by the MIHF can also be sent to a remote MIH entity as a remote MIH Event.

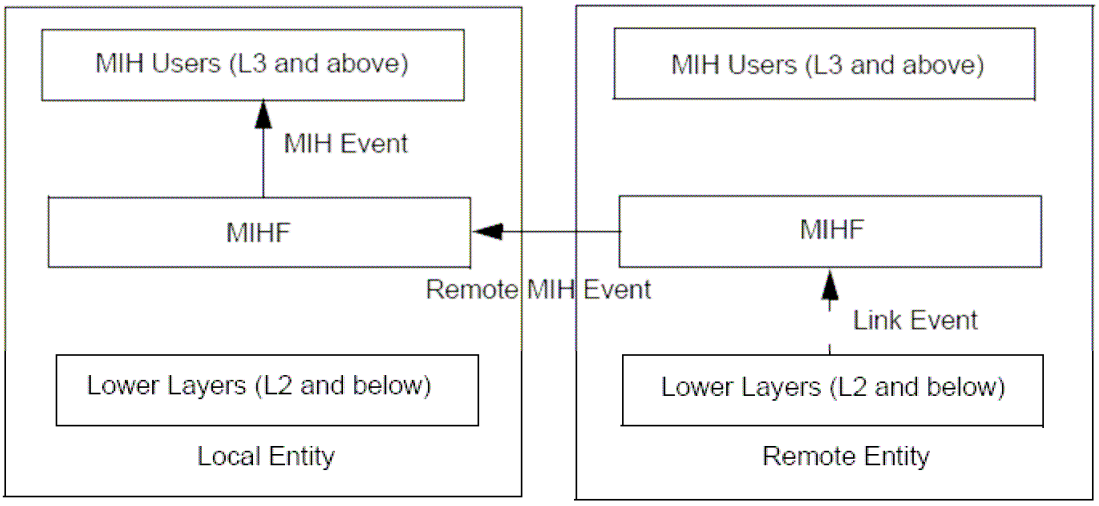


Figura 13: Remote MIH events

2.3.3.2 Media Independent Command Service

Media Independent Command Service (MICS) refers to the commands sent from MIH Users to the lower layers in the reference model. MIH Users utilizes command services to determine the status of links and/or control the multi-mode device for optimal performance. Command services also enable MIH Users to facilitate optimal handover policies. For example, the network initiates and control handovers to balance the load of two different access networks.

The link status varies with time and MN mobility. Information provided by MICS is dynamic information composed of link parameters such as signal strength and link speed, whereas information provided by MIIS is less dynamic or static in nature and is composed of parameters such as network operators and higher layer service information. MICS and MIIS information could be used in combination by the MN/network to facilitate the handover.

A number of commands are defined in this standard to allow the MIH Users to configure, control, and retrieve information from the lower layers including MAC, Radio Resource Management, and PHY. The commands are classified into two categories: MIH Commands and Link Commands. Figura 14 shows link commands and MIH commands.

The receipt of certain MIH command requests can cause event indications to be generated. The receipt of MIH command requests indicates a future state change in one of the link layers in the local node. These indications notify subscribed MIH Users of impending link state changes. This allows MIH Users to be better prepared to take appropriate action.

Link Commands originate from the MIHF and are directed to the lower layers. These commands mainly control the behavior of the lower layer entities. Link Commands are local only. Whenever applicable this standard encourages use of existing media-specific link commands for interaction with specific access networks. New link commands, if required, are defined as recommendations to different link layer technology standards. It is to be noted that although Link Commands originate from the MIHF, these commands are executed on behalf of the MIH Users.

The MIH commands are generated by the MIH Users and sent to the MIHF. MIH commands can be local or remote. Local MIH commands are sent by MIH Users to the MIHF in the local protocol stack.

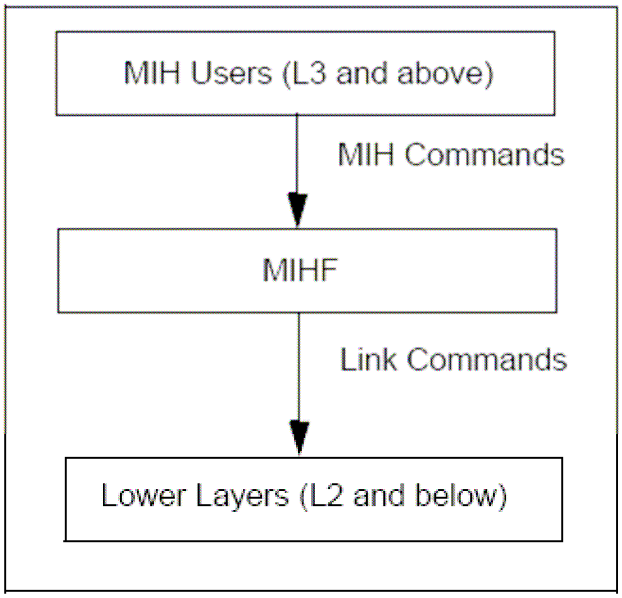


Figura 14: Link commands and MIH commands

Remote MIH commands are sent by MIH Users to the MIHF in a peer protocol stack. A remote MIH command delivered to a peer MIHF is executed by the lower-layers under the peer MIHF as a link command; or is executed by the peer MIHF itself as an MIH command (as if the MIH command came from an MIH User of the peer MIHF); or is executed by an MIH User of the peer MIHF in response to the corresponding indication. Often, an MIH indication to a remote MIH User results from the execution of the MIH command by the peer MIHF. Figura 15 shows remote MIH commands.

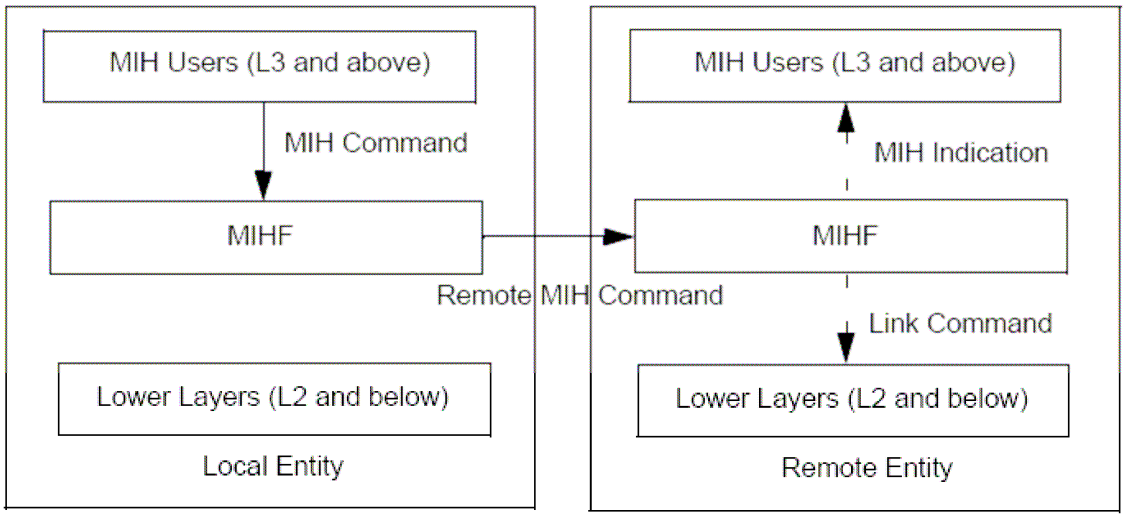


Figura 15: Remote MIH command

2.3.3.3 Media Independent Information Service

2.3.3.3.1 Introduction

Media Independent Information Service (MIIS) provides a framework by which an MIHF, residing in the MN or in the network, discovers and obtain network information within a geographical area to facilitate network selection and handovers. The objective is to acquire a global view of all the heterogeneous networks relevant to the MN in the area to facilitate seamless roaming across these networks.

Media Independent Information Service includes support for various Information Elements (IEs). Information Elements provide information that is essential for a network selector to make intelligent handover decisions.

Depending on the type of mobility, support for different types of information elements is required for performing handovers. MIIS provides the capability for obtaining information about lower layers such as neighbor maps and other link layer parameters, as well as information about available higher layer services such as Internet connectivity.

MIIS provides a generic mechanism to allow a service provider and a mobile user to exchange information on different handover candidate access networks. The handover candidate information includes different access technologies such as IEEE 802 networks, 3GPP networks and 3GPP2 networks. The MIIS also allows this collective information to be accessed from any single network. For example, by using an IEEE 802.11 access network the MN gets information not only about all other IEEE 802 based networks in a particular region but also about 3GPP and 3GPP2 networks. Similarly by using a 3GPP2 interface, the MN gets access to information about all IEEE 802 and 3GPP networks in a given region. This capability allows the MN to use its currently active access network and inquire about other available access networks in a geographical region. Thus an MN is freed from the burden of powering up each of its individual radios and establishing network connectivity for the purpose of retrieving heterogeneous network information. MIIS enables this functionality across all available access networks

by providing a uniform way to retrieve heterogeneous network information in any geographical area.

The main goal behind the Information Service is to allow MN and network entities to discover information that influences the selection of appropriate networks during handovers. This information is intended to be primarily used by a policy engine entity that can make effective handover decisions based on this information. This Information Service provides mostly static information, although network configuration changes are also accounted for. Other dynamic information about different access networks, such as current available resource levels, state parameters, and dynamic statistics should be obtained directly from the respective access networks. Some of the key motivations behind the Information Service are as follows:

a) Provide information about the availability of access networks in a geographical area. Further, this information could be retrieved using any wireless network, for example, information about a nearby Wi-Fi hotspot could be obtained using a global system for mobile communication (GSM), CDMA, or any other cellular network, whether by means of request/response signaling, or by means of information that is specifically or implicitly broadcast over those cellular networks. Alternatively, this information could be maintained in an internal database on the MN.

b) Provide static link layer information parameters that helps the mobile nodes in selecting the appropriate access network. For example knowledge of whether security and QoS are supported on a particular access network influences the decision to select such an access network during handovers.

c) Provide information about capabilities of different PoAs in neighbor reports to aid in configuring the radios optimally (to the extent possible) for connecting to available or selected access networks. For example knowing about supported channels by different PoAs helps in configuring the channels optimally as opposed to scanning or beaconing and then finding out this information. Dynamic link layer parameters have to be obtained or selected based on direct interaction with the access networks.

d) Provide an indication of higher layer services supported by different access networks and core networks that can aid in making handover decisions. Such information is not available directly from the MAC sublayer or PHY of specific access networks, but can be provided as part of the Information Service. For example, classification of different networks into categories, such as public, enterprise, home, and others, influences a handover decision. These higher layer services information is more vendor specific in nature.

2.3.3.3.2 Access information service before authentication

It is important to note that, with certain access networks an MN should be able to obtain IEEE 802.21 related information elements before the MN is authenticated with the PoA. These information elements are used by the handover policy

function to determine if the PoA can be selected. In order to enable the information query before authentication, individual link technologies provide an L2 or media-specific transport or a protocol message exchange that makes this MIIS query exchange possible between the user equipment (MN) and a certain MIHF in the network. It should be noted that the pre-authentication query facility is provided only for MIH information query and cannot be used for carrying other MIH protocol services except MIHF capability discovery query using MIH_Capability_Discover embedded into media specific management frames. Additionally, any MIHF within the network can request for the set of information elements from a peer MIHF located in the same or a different network using the MIH protocol.

Allowing access of information service before authentication carries certain security risks such as denial-of-service attacks and exposure of information to unauthorized MNs. In such scenarios the information service provider limits the scope of information accessible to an unauthenticated MN.

After authentication and attachment to a certain PoA, the MIH protocol is used for information retrieval by use of data frames specific to that media technology.

2.3.3.3.3 Restricting query response size

When sending an information query request, the MIIS client provides a maximum response size to limit the query response message size. A request can contain multiple queries. If the request contains multiple queries, they will be in the order of significance to the client. In case the query results exceed the maximum response size, the least significant query results will be removed from the response. The MIIS server has its own maximum response size limit configured that is smaller than the one specified by the MIIS client request. In this case the response message returns results in the order of significance to the client up to that limit.

2.3.3.3.4 Information elements

The Information Service elements are classified into three groups:

a) General Information and Access Network Specific Information: These information elements give a general overview of the different networks providing coverage within an area. For example, a list of available networks and their associated operators, roaming agreements between different operators, cost of connecting to the network and network security and quality of service capabilities.

b) PoA Specific Information: These information elements provide information about different PoAs for each of the available access networks. These IEs include PoA addressing information, PoA location, data rates supported, the type of PHY and MAC layers and any channel parameters to optimize link layer connectivity. This also includes higher layer services and individual capabilities of different PoAs.

c) Other information that is access network specific, service specific, or vendor/network specific.

In certain access network deployments, some PoA properties (e.g., data rate, IP configuration methods, capabilities) are common for all PoAs within that access

network. In such a case the common PoA properties are represented as IEs as part of the access network property information.

As an example, Figura 16 shows the layout of different Information Elements and the neighbor map of different networks in a geographical area. Multiple operators can be providing support for a particular network. Thus support for IEEE 802.11 network is provided by both Operator_1 and Operator_2. A single operator can provide support for multiple networks. Thus Operator_1 provides support for IEEE 802.11 and universal mobile telecommunications system (UMTS) networks while Operator_3 provides support for IEEE 802.16 and UMTS networks. The General Network Information Elements are specified for each network supported by an operator. Thus in the case of Operator_1, General Network Information is specified for both IEEE 802.11 and UMTS networks, while in the case of Operator_2 it is specified only for an IEEE 802.11 network.

For each network supported by an operator there is a list of supported PoAs. For each PoA the PoA Information Elements are specified. Figura 16 shows this information representation and tree hierarchy for different networks.

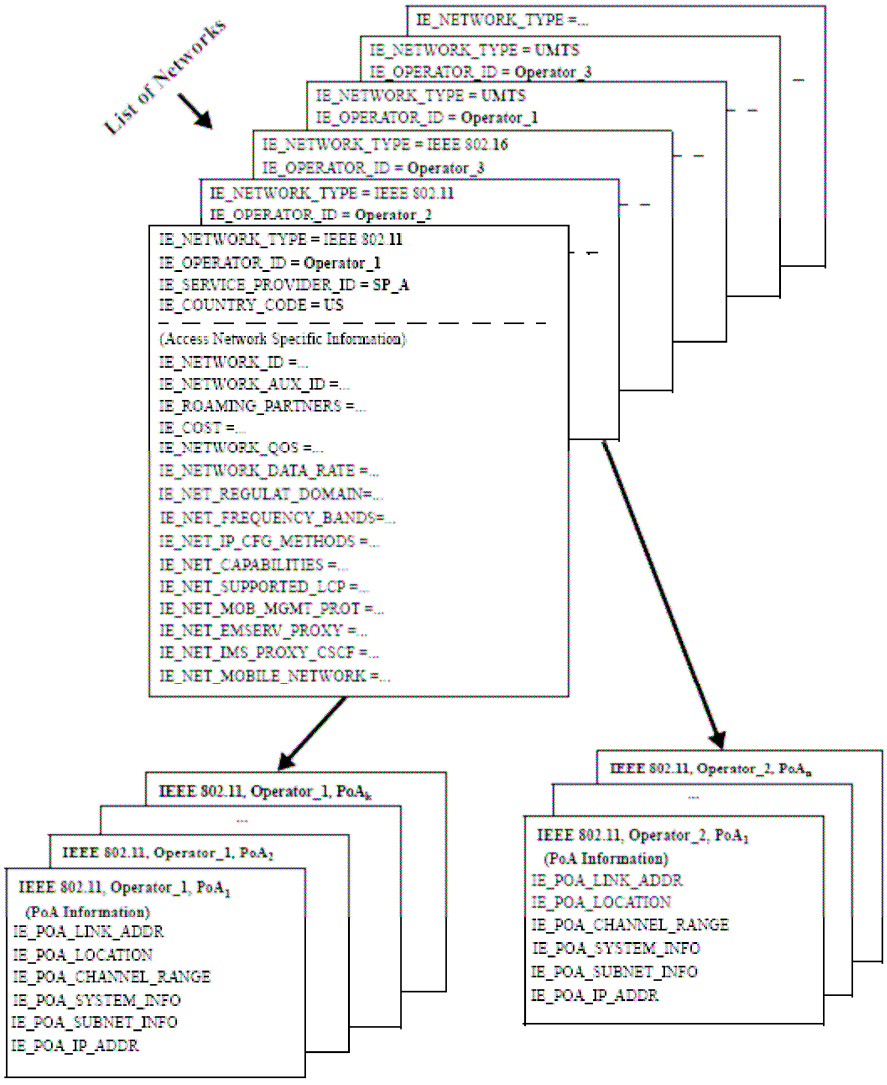


Figura 16: Depicting a list of neighboring networks with information elements

2.4 Current Solutions

2.4.1 Daidalos: Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services

The objective of Daidalos is to develop and demonstrate an open architecture based on a common network protocol (IPv6) that becomes a significant step towards approaching the Daidalos vision.

The overall Daidalos objectives are to:

- Design, prototype and validate the necessary infrastructure and components for efficient distribution of services over diverse network technologies beyond 3G.
- Integrate complementary network technologies to provide pervasive and user-centred access to these services.
- Develop an optimized signalling system for communication and management support in these networks.
- Demonstrate the results of the work through strong focus on user-centred and scenario-based development of technology.

Four technical work packages have been defined (WP1-4) in order to achieve this objective, and a 5th (WP5) for integration activities. [103]

Daidalos is an Integrated Project in the Thematic Priority “Information Society Technologies” of EU Framework Programme 6 for Research and Development, which is currently finished and it consisted of two phases, described separately as follows.

2.4.1.1 Daidalos I

Daidalos is about radically improving the usability of European telecommunication technologies by integrating mobile and broadcast communications.

Following a user-centred scenario-based approach, Daidalos will deliver ubiquitous end-to-end services across heterogeneous technologies.

Motivation

Mobility has become a central aspect of the lives of European citizens – in business, education, and leisure. This trend has been followed by an increased usage and diversity of multimedia communications, as the increased success of cellular phones with embedded cameras illustrates. In order to keep up with the resulting new communications needs, it becomes necessary to re-think existing network paradigms. Future networks should be able to support multiple business models with quite extreme company strategies – from network operators, service providers, broadcast companies, or cellular operators. These companies will function on a mixed competition-cooperation environment, where individuality will be required to surpass competition, but cooperation will be essential to improve the network value. Daidalos innovations will make real these trends even to telecommunication companies with different purposes and business models,

allowing their smooth interoperation and providing an opportunity for new service developments. Furthermore, the resort to open technologies will support end-user centric service developments, such as peer-to-peer technologies.

Due to rapid technological and societal changes, there has been a bewildering proliferation of technologies and services for mobile users. This has created a complex communications environment for both users and network operators. For efficient interoperation, these novel network environments will need to integrate quality-of-service capabilities in mobile heterogeneous environments, under a common authentication, authorization, accounting, auditing and charging (A4C) framework, and provide a secure communication environment. The integration of all these technologies represents a major multi-disciplinary research effort undertaken in Daidalos.

Vision and goals

The Daidalos project aims at working towards an environment, where mobility is fully established through scalable and seamless integration of a complementary range of heterogeneous technologies and concepts, and providing the framework of integrating multiple existing technological, service and business paradigms. Daidalos is also committed to use open interfaces and technologies according to a vision of a future user-centric, fully-networked society. This environment will enable mobile users to enjoy a diverse range of personalized services – seamlessly supported by the underlying technology and transparently provided through pervasive interfaces. In Daidalos, information will reach the user through an "always best-connected" approach, taking in consideration network availability, user preferences and user/service contracts. Daidalos will develop and demonstrate an open architecture based on a common network protocol (IPv6), which in its iterations will increasingly approach the Daidalos vision.

Scenarios

The Daidalos approach is being detailed through a scenario-based design concept. A scenario is a real-life, user-centric description of communication-based activities, which we use in an iterative process to further refine the requirements for system and architecture design.

Two major scenarios are currently under consideration: the Daidalos Mobile University scenario and the Daidalos Automotive scenario. Together, both scenarios are highly representative for a broad variety of education, entertainment and business scenarios in the mobile world.

Mobile University

Key vision: Students, studying abroad, have access to their personal set of services and can dynamically discover local services and devices.

Building blocks

- Organization of daily life at the university (friends, appointments and reservations, classes, projects, exams, entertainment)
- Locating people and devices, checking availability, discovering local services
- Searching for best / cheapest available infrastructure
- Personal broadcasting, e.g. of classes and speeches

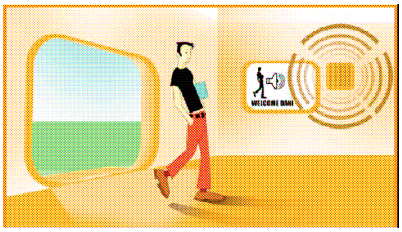


Figura 17: Dani arriving for the lectures

Automobile Mobility

Key vision: Mobility supporting services in and around the vehicle with aspects of personal multimedia, ad-hoc mobile networking and session mobility.

Building blocks

- Access to personal information and services inside and outside the vehicle.
- Locating and detecting presence.
- Service and content adaptation based on QoS across network and operator boundaries.
- Session mobility between terminals (incl. vehicles), and across organizational and operational domains.
- Broadcast services for entertainment, inter-vehicle safety, and regional traffic information services.

Figura 18: Presence detection for automobile mobility applications

Technical approach

The overall architecture design is based on multiple requirements, including the user point of view, business models for operators and content/application providers, and technical requirements.

This architecture and the overall design choices for the project are passed to the technical activities that will develop and implement the required components for the Daidalos architecture. All these components will be later delivered to an integration activity, which will instantiate proof-of-concept designs. With the

feedback from these instantiations, new refinements will be promoted at the architecture level.

Architecture

The Daidalos architecture introduces in an Internet-centric manner pervasive personalized services and mobility enabled broadcast. It is based on IPv6-technologies, and addresses mobility, authentication, authorization, accounting, auditing, charging (A4C), security and QoS issues. The architecture is access technology independent, and specific support for broadcast media is being developed. In reality, broadcast media and broadcast services are separated in this architecture, and different combinations of these two different concepts can be supported.

The generic service provider/consumer implemented allows a flexible and optimizable architecture. The federation concept is being used not only to exchange variable details of user data, but also to implement a variable set of operator related information. Thus, although well defined interfaces exist at the service platform level, multiple service platforms can be integrated in several aspects, reducing implementation costs and providing for better service provision and network management.

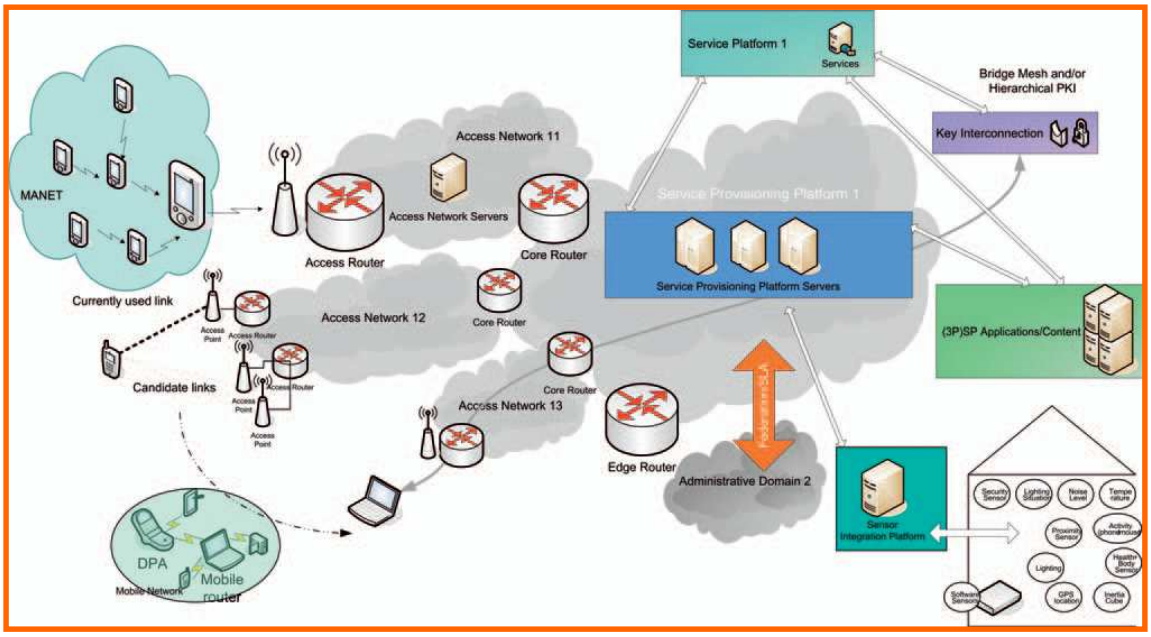


Figura 19: The Daidalos architecture introduces pervasive personalized services and mobility enabled broadcast

Business models

Daidalos explores business models oriented towards future communication operators' needs, both mobile and broadcast-based. These operators may have very different scales: national operators, small communities, application providers, etc. but will all use the same basic technologies.

The basic assumptions are:

- Traditional operators outsource OSS or service provision

- 3rd Party service providers supported with variable QoS over open APIs
- Intelligence at the network VS multimode-terminals
- Converged mobile/media operators under EU licence
- End-user/communities as service provider
- Dis-integration of network functionality is enabling service providers[104]

2.4.1.2 Daidalos II

Daidalos II is the second phase of the Integrated Project Daidalos (2003 - 2008).

Daidalos II continues research on Beyond 3G architectural concepts and components with an operator-driven perspective.

Among the new research topics and innovations are:

- Federation in diversified and fragmented markets
- Context-aware mobility management, localized mobility, multihoming, QoS
- Cross-layer context and identity management
- Tools, APIs and deployment schemes for pervasive applications.

Motivation

The project addresses the fact that mobility has become a central aspect of our lives in business, education, and leisure. It deals with rapid technological and societal changes with proliferating technologies and services that have resulted in complex and confusing communications environments for users and network operators.

By rethinking fundamental technology and business issues, Daidalos targets usable and manageable communication infrastructures for the future. The goal is a seamless, pervasive access to content and services via heterogeneous networks that supports user preferences and context. The project will use a user-centred, scenario-based and operator-driven approach to effectively cover user and business needs. The Daidalos project aims at working towards an environment, where mobility is fully established through scalable and seamless integration of a complementary range of heterogeneous technologies and concepts, and providing the framework of integrating multiple existing technological, service and business paradigms.

Daidalos is also committed to use open interfaces and technologies according to a vision of a future user-centric, fully networked society. This environment will enable mobile users to enjoy a diverse range of personalised services – seamlessly supported by the underlying technology and transparently provided through pervasive interfaces. In Daidalos, information will reach the user through an “always best-connected” approach, taking into consideration network availability, user preferences and user/service contracts. Daidalos will develop and demonstrate an open architecture based on a common network protocol (IPv6), which in its iterations will increasingly approach the Daidalos vision.

Key guiding concepts

Daidalos will be guided by five key concepts:

- MARQS (Mobility Management, AAA [Authentication, Authorisation and Accounting], Resource Management, QoS and Security), supporting functional integration for end-to-end services across heterogeneous technologies.
- VID (Virtual Identity), which separates the user from a device, thereby enables flexibility as well as privacy and personalization.
- USP (Ubiquitous and Seamless Pervasiveness), enabling pervasiveness across personal and embedded devices, and allowing adaptation to changing contexts, movement and user requests.
- SIB (Seamless Integration of Broadcast), which integrates broadcast at both the technology level, such as DVB-S/T/H, and at the services level, such as TV, carousels and data-cast.
- Federation, which will enable network operators and service providers to offer and receive services, allowing players to enter and leave the field in a dynamic business environment.

Daidalos brings together several domains and will follow a strictly methodological approach on modelling, testing, and integration cycles with feedback loops via early integration.

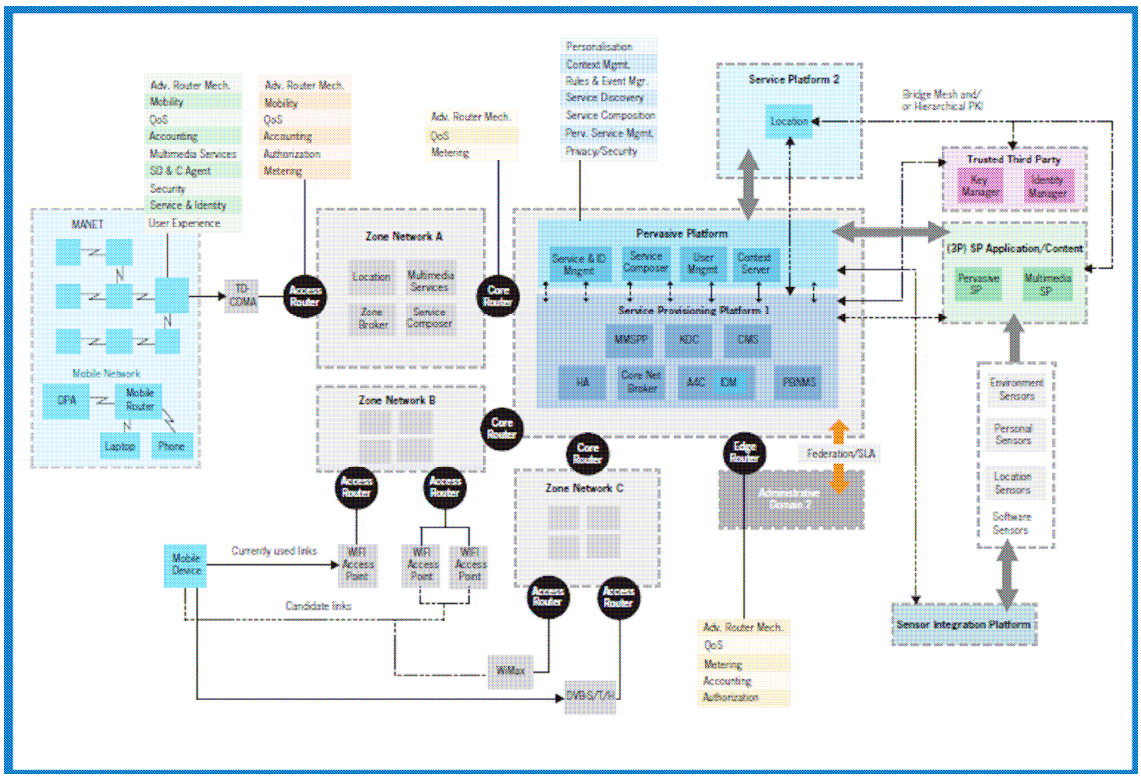


Figura 20: Daidalos – Global network architecture

Technical approach

The Daidalos II project is structured in four technical work packages, representing the different network and service layers to be researched. In addition, there is a work package dedicated to integration, and a work package dealing with project management, dissemination, standardisation, and training.

Global architecture

The main objective of this work package is to technically align the other work packages, in order to ensure consistency in architecture, consistency of technical direction in relation to the five key concepts, maximisation of impacts on standards, monitoring, and adhering to business needs.

Integration of heterogeneous networks

This work package is dedicated to the specification and implementation of an integrated pure-IP network for mobile communication. Daidalos II aims at achieving an efficient and scalable integration of heterogeneous access network technologies, including cellular, satellite, broadcast, wired networks, wireless networks and sensor networks.

Context-aware network service provisioning

This work package addresses network operation and service provisioning. The planned architecture will be context-aware, flexible, scalable, robust, and optimised. This will allow for the provisioning of creative, attractive and more stringent services, whilst supporting new business models.

Enabling pervasive services

This work package focuses on developing an enabling platform for providing services in a pervasive way. Particular emphasis is put on user-centred, flexible and adaptable service management; ontologies and models for open service value chains. In addition, Daidalos will explore user behaviour and usage of this knowledge for service provisioning, tools and methodologies for pervasive service engineering as well as privacy and security issues related to pervasive computing.

Proof of Daidalos II concepts

Work package 5 will provide the main validation and verification effort of Daidalos II. This work will be based on the work done in work packages 1 to 4.

Qualitative and quantitative measurements will be provided to gather information from expert groups and end-user evaluation. This will be used to get feedback on the application of the global architecture in the selected scenarios and produce an overall evaluation of the Daidalos II system. [105]

2.4.2 Vendors

2.4.2.1 Alcatel Lucent

Mobile technology has rapidly entered the workplace, meaning employees enjoy more flexibility to work on the move. However, for many enterprises, the uptake of mobile working has been almost entirely spontaneous and unsystematic. Alcatel Lucent ensures that mobile technologies have a positive impact on business performance by helping companies adopt an effective mobile strategy: supporting users, building networks and maintaining mobile security.

Supporting your users

For equipping users with tools that allow them to connect to the right people and knowledge when they need to, wherever they are.

- On-site mobility solutions: Roaming workers need to remain accessible and have access the information they need when moving around the office. With these mobility solutions, employees and executives can connect to the network and receive calls, wherever they are in the office building. The components and features of this solution are the following: Mobile desktop environment, advanced mobile telephony and Mobility for fixed-line users.
- Off-site mobility solutions: Being on the road often means sacrificing connectivity and spending precious time catching up with activities in the office. Off-site mobility solutions give off-site employees the tools they need to manage their communications simply and easily and enable them to take a proactive approach to core business. For example, we provide advanced telephony and remote network access for off-site workers so they can always access relevant information and the right people in real time, wherever they happen to be. The components and features of this solution are the following: Advanced mobile telephony, One number service, Voice messaging and Business/personal modes.
- Dual-mode solution: Employees who work both on site and outside the company require flexible communications that they can use in any location, without any fuss. For example, workers' portable phones connect to the enterprise communication system when on campus; moving off-site, they can continue their conversation with a switch of a button as they move toward public cellular network coverage. As a result, mobile workers have a convenient and productive way to manage their communications and organizations benefit from cost-effective enterprise mobility. The components and features of this solution are: Advanced mobile telephony and One number service.
- Remote working: Geographical distance is no longer a reason to be isolated. This solution allows remote employees to interact with colleagues and customers as though they were sitting in the same office. With reliable, secure network integration, remote workers have access to the same information and communication services as central office workers. The components and features of this solution are the following: Remote connection to IP server, Web-based applications, One number service, Internal extension number, Telephony features, Guarantee lowest cost calls, Contact center extension and Converged voice and data applications.

Building your network

For taking an end-to-end view of mobility and consider how your network interacts with new mobile devices and applications.

- Mobility infrastructure solutions: Whether they work at headquarters, on the road or in a remote office, employees need secure access to identical services on your network. To support your mobile employees, we help you define and install a secure and efficient mobility infrastructure. We offer a wide portfolio based on IP/LAN/WLAN, DECT and/or GSM, which is adaptable to your needs.

Mobility products

- Omni Access Wireless LAN: Alcatel-Lucent's next generation WLAN solution is a highly scalable, comprehensive set of mobile LAN products

that automatically identify and authenticate users as they connect to the network. Once user identity is established, it enables "follow-me" privileges, security and services - something no other enterprise system provides today. This sophisticated technology gives corporations the power to manage and secure people rather than ports.

- Alcatel-Lucent Advanced Cellular Extension (ACE): is an application which turns any smart mobile phone into an extension of the communication server, without extra hardware, infrastructure changes, or dedicated link involved. The full suite of communication tools is made available on the leading-edge mobile platforms via two components:
  - **A server application**, hosted on the Alcatel-Lucent OmniPCX Communication Server, provides corporate telephony services to authorized mobile devices.
  - **A client application**, hosted on the smart mobile device, provides a menu-driven interface to access Alcatel-Lucent OmniPCX Communication Server features.

  Microsoft Windows Mobile, Nokia Phones and Blackberry are the mobile platforms with Cellular Extensions. [106]

2.4.2.2 Nokia/Nokia Siemens Networks

Demand for convergence is evident. Users want convenient quadruple play access to personalized voice, data and video/TV services, supported by mobility over any access network. From an operator or service provider perspective the challenge is to meet this requirement with long-term profitable business.

Nokia Siemens Networks provides a customer optimized end-to-end solution, complete with business and technology consulting, deployment services, hosting and other managed services. We work closely with operators and service providers to reach their goals and our combined breadth includes the most comprehensive offering of mobile and fixed soft switching, cable solutions, applications and IMS based solutions.

Fixed-Mobile Convergence Solution

The long-term profitability of fixed and mobile businesses is predicated on the delivery of a wide range of user-centric services that can be self-provisioned and personalized. To do this the industry must provide a simple and convenient user experience combined with complementary access and cost effective solutions.

There is broad agreement within the industry on standards based initiatives such as IMS and the need for fast service creation and deployment. Use of these services must be intuitive and deliver a unified user experience across the different fixed and mobile access networks. Success in the emerging FMC environment will be determined by user acceptance, not networking technology, although IP, VoIP and SIP are important enablers.

We are in a communications-centric era. This equates to a huge market for smarter, tailored services and an unprecedented opportunity for network operators and service providers. We have the technology to create and deploy virtually any

service for which there is an appetite. However, the size of the market, combined with factors such as broadband access and location-agnostic delivery, allows new players entry, resulting in new business models and the arrival of xVNOs.

As an operator you need to decrease complexity, launch new services and continuously ensure cost efficient operation. Nokia Siemens Networks can help you with these FMC challenges, now and into the future.

1. Decrease complexity in your network

   We provide a clear and flexible evolution path towards converged, access-agnostic networks with service integration and interoperability across domains and devices. You benefit from CAPEX and OPEX savings with common IP based transport networks, and centralized OSS and BSS. And, dissolve the complexities of network islands and achieve synergies and cost optimization by deploying the same services across all domains.

2. Launch new services effectively and differentiate your offering to meet end user needs

   Retain customers and increase revenues with attractive, easy to use services and service bundles accessible through any access network or device. Differentiate with unique service offerings such as quadruple-play services based on standard service enablers and attractive applications created by our developer and partner programs. Take advantage of all available service opportunities and stay in control of your subscribers using IMS.

3. Take advantage of our end-to-end solutions and ensure cost efficient operations

   We work with you to deliver an optimized end-to-end FMC solution tailored to your needs. We provide a smooth and cost efficient convergence evolution, including a cost effective migration to an all-IP network, based on your existing assets. [107]

2.4.2.3 Huawei

The Internet has grown to be a key component of everyday life for many people. Having to restrict the use of the Internet to when they are at home or the office has become a major obstacle to fulfilling the promise of the Internet. Full, high-speed access from mobile handsets opens up new revenue sources, but only if the underlying network is built to support existing and emerging standards.

Mobile Broadband Solution

The rapid development of mobile broadband services is changing people's life style and also bringing in opportunities for innovations in services and benefits to operators. Meanwhile, the implementation of various high–speed wireless technology, is witnessing a growing pressure on the bandwidth of the current network. Besides, operators also need to increase OPEX to build more core networks to meet the requirements of the continuous network architecture evolution. Due to the lack of refined management of the bandwidth resources, the profit for operators is only minimal. The important question, today, therefore, is on how operators can establish a smooth broadband channel and transfer to refined operation to benefit from new services.

Solution

Adopting packet core network with broadband, intelligence and convergence as its core, Huawei mobile broadband solution features super high broadband, high performance content charging and convergent 2G/3G/WiMAX/WLAN networks. This innovative solution is 10–15 times greater in volume compared with the traditional equipment, and can provide single user experience of Kbps class to Mbps class service improvement.

The Huawei intelligent packet domain solution fulfils the precise content resolution and charging without affecting the capacity and volume of equipment.

Considering the investment protection and network evolution, the Huawei convergence solution based on 3GPP standard supports various wireless access technologies simultaneously, such as GRPS, UMTS, WiMAX and WiFi.

Currently, the Huawei GRPS/UMTS packet domain solution is being widely used in over 70 countries worldwide. Huawei is successfully working with 18 TOP 50 operators such as China Mobile, China Unicom, T–Mobile, KPN, AIS, Etisalat, MTN, MTS, VimpelCom, Meqafon, and STC. [108]

2.4.2.4 Cisco

Cisco has delivered a practical approach to Business Mobility: Cisco 3300 Series Mobility Services Engine.

The innovative Cisco 3300 Series Mobility Services Engine is an appliance solution that transforms existing wireless LANs into mobility networks. The platform is a combination of hardware and software that:

- Simplifies provisioning and management of mobility services.
- Offers scalable and reliable multidevice, multinetwork application delivery.
- Facilitates a broad partner ecosystem mobile applications development.

The platform is extensible to support a variety of mobility services in a modular fashion.

The Cisco 3300 Series Mobility Services Engine abstracts applications and services from the underlying control network to optimize performance and reliability while reducing the operational complexities associated with business mobility. This architecture unifies application delivery across Wi-Fi, Ethernet, WiMAX, and cellular networks while preserving security and manageability.

The Cisco 3300 Series Mobility Services Engine supports:

- An open API based on Simple Object Access Protocol (SOAP) and XML for third-party application development.
- Scalable, simultaneous delivery of multiple mobility services.
- Centralized or distributed configuration for all network topologies

The centrally managed and provisioned Cisco 3300 Series Mobility Services Engine software suite includes Cisco Context-Aware Software, Cisco Mobile Intelligent Roaming, and Cisco Adaptive Wireless IPS. [109]

Some information more about the Cisco Mobility Services Architecture can be found at [110].

2.4.3 Operators

2.4.3.1 British Telecom (BT)

BT – Enterprise Mobile Services

BT Enterprise Mobile Services combine mobile voice, data and email options – designed specifically for large organisations – together with a complete range of management information and support solutions.

BT can help you control the management and cost of your mobile communications infrastructure. Our broad portfolio of devices, including BlackBerrys and Windows Mobile smart phones, ensures users get the best technology available. And with access to voice, email, data and corporate applications, your mobile employees can easily stay in touch – no matter where they are.

Our powerful analytical applications provide an accurate insight into usage and costs, so you can control expenditure. And by consolidating your contracts and invoices with one dedicated provider, you'll be able to manage all your mobile communications more efficiently. [111]

2.4.3.2 France Telecom/Orange

Checking your schedule while waiting to board the plane; connecting easily and securely to your company intranet from a client's office; emailing an important document form home; receiving alerts and being reachable at all times: all this is possible with single, consistent, one-click experience through **Business Everywhere**.

You will now be able to work together more effectively in all situations with collaborative, communications and contractibility services. More than 850,000 business users already use it worldwide.

This solution is broadly used in the France Telecom Group and has made it possible for us to reduce our greenhouse gas emissions as well as our transportation costs while improving individual and group productivity.

Business Everywhere gives your mobile employees a safe, simple and coherent way to connect around the world with superior coverage and support from Orange Business Services. Your mobile employees will enjoy an easy access to the Internet and corporate networks using virtually any network technology and a variety of devices as if they were at the office.

Benefits:

- Flexible solution: Our mobility design and integration teams work with you to help to simplify the process and provide the most effective mobility solution. Our teams offer a development, deployment, management and maintenance of your complete mobility solutions, available on a truly global scale.

- Safe: Give your mobile employees a fully secured way to connect around the world with the superior support from Orange Business Services and a seamless managed solution (IPSec or SSL gateways, manage user authentication, compatible with our fleet management solutions: Secure My Device, smart phone management).
- Easy to use: Uses only one click to connect with the same password, no matter which access technology you use or what country you are in, with a global phonebook. Our coverage of around 150 countries includes the largest dial coverage, worldwide Wi-Fi with more than 110,000 hotspots, broadband and 3G+/3G/EDGE /GPRS coverage.
- Cost control: Flat-fee unlimited pricing model (3G mobile data bundles) includes simple contract terms.
- Centralized solution for IT managers: Online reporting, trainings, global support for your IT manager and a 24/7 help desk for end users. [112]

2.4.3.3 Vodafone

Built-in mobile broadband

Built-in 3G

The Built-in mobile Broadband laptop will provide secure, high speed access to the Internet, intranet, email and customer's business applications without the need for a separate connectivity device.

Stay connected throughout the world with mobile broadband, 3G, GPRS and HSDPA coverage in over 100 countries.

There are a range of laptops and notebooks for you to use from leading manufacturers such as Dell, HP and Lenovo.

What this product can do for you:

- Simplified User Experience: Integrating the wireless module and SIM and pre-loading the Vodafone dashboard software into the laptop or notebook will provide you with a simplified user experience in comparison to the Mobile Connect Card.
- Ideal for any employees that rely on their email and the internet to stay in touch with work, Built-in mobile Broadband uses the extensive Vodafone network to provide mobile connectivity wherever your people are working.
- Everything your employees need to access email and office data or connect to the internet is already installed on their laptop – including SIM card, software and an antenna built into the screen.
- Instead of having to find a WiFi hotspot, your employees will be able to use their laptops anywhere on the Vodafone footprint and access mobile Broadband, 3G, GPRS and HSDPA.
- Connectivity enables you to operate far more efficiently in a demanding, fast paced world. When connectivity becomes immediate, easy, reliable and fast wherever you are, it starts to make real business sense. [113]

Gobi enabled laptop

Gobi is a mobile internet module that is embedded into your laptop and provides secure, high speed access to the internet, from anywhere in the world, without the need for external data hardware. The Gobi wireless embedded module allows our customers to travel from the USA to anywhere else in the World, accessing the internet via their laptop without having to carry additional hardware. This leverages Vodafone's GSM network footprint outside the USA.

In addition, Vodafone Global Enterprise customers will be able to roam from Europe and the rest of the world into the USA via standard GSM networks without reconfiguration.

This gives multi-national organisations the confidence to standardise on Gobi's wireless module as a mobile internet access technology across worldwide laptop deployments, thus reducing both your internal support requirements and ongoing maintenance costs.

There are a range of laptops for you to use from leading manufacturers such as HP, Dell, and Lenovo. HP is the only vendor who is standardising on the Gobi module in laptops in both the USA and Europe.

What can this product do for you?:

- Standardise on a single embedded laptop module for worldwide deployment
- Seamless international roaming between the USA and the rest of the world
- Predictable billing through a single consolidated domestic and roaming invoice
- Reduced IT procurement, qualification, support and management costs
- Increased productivity by removing complexity of external cards
- Optimised performance through higher connections speeds and battery life
- Easy asset tracking or data protection on a lost or stolen laptop via the GPS functionality – one device for all locations
- Hassle-free management of software updates [114]

2.4.3.4 Telefónica

Telefónica offers in Spain Facilidad Movilidad. It consists of a flat rate for Internet connection that allows you to connect to the Internet at every location in Spain you are.

One of the following three different possibilities can be chosen:

- Facilidad Movilidad Tarifa Plana Internet Reducido: It provides an unlimited Internet access from Monday to Friday from 6pm to 8am, and Saturday and Sunday 24h. [115]
- Facilidad Movilidad Tarifa Plana Internet 24h: unlimited Internet access from Monday to Sunday 24h. [116]

- Facilidad Movilidad Tarifa Plana Internet Horario Comercial: unlimited access to the Internet from Monday to Friday, from 9 am to 2 pm and from 4 pm to 10 pm. [117]

2.4.3.5 Swisscom

Swisscom has developed several business mobility solutions: Corporate Access CAA/CNA and Mobile Unlimited.

With **Corporate Application Access (CAA)** your company-specific applications go mobile. Corporate Application Access ensures that your mobile devices can communicate with the servers in the corporate network. The data traffic makes use of the Internet, with Corporate Application Access ensuring optimised connection management with public Internet addresses. The Managed Firewall ensures that you are protected against attacks from the Internet.

With **Corporate Network Access (CNA)** your LAN goes mobile. You are able to access your corporate LAN network at any time and to use a guaranteed bandwidth for your data. You can exchange data between your corporate network and mobile devices, as if the latter were an integral part of your network. [118]

Send e-mails and surf with high speed while en route: Switzerland is a hotspot with Mobile Unlimited.

Mobile Unlimited gives you the freedom to work wherever you want. Whether at home, in the office, en route or at your holiday home – you're automatically connected to the internet or to your corporate network via high speed. [119]

CAPÍTULO 3

ESCENARIOS DE INTERÉS EN SISTEMAS DE NGN

En esta sección se presentan los cuatro casos de uso que fueron propuestos tras realizar el estudio sobre la movilidad en Redes de Siguiente Generación. La elección de los escenarios se basó en posibles situaciones que no se habían resuelto hasta la fecha. Tras la elaboración, fueron publicados en colaboración con Fixed-Mobile Convergence Alliance y posteriormente discutidos en conferencias telefónicas internacionales.

Como trabajo posterior a la elaboración y publicación de los casos de uso, se ha realizado un estudio de las posibles soluciones para implementarlos, así como la aplicación parcial o total de soluciones disponibles en la actualidad.

3.1 Media Independent Handover: Seamless handover and service adaptation (I)

3.1.1 Use Case description

Remarks: Transfer a VoIP video call from fixed access to in-house WiFi network and afterwards session transfer to wide area network taking into account service adaptation.

Status: open.

Use case title: MIH: Seamless handover and service adaptation.

Customer type: Consumer.

Customer trend (consumer): Simplicity, Being always in touch, Wireless broadband, Snacking entertainment anytime, Integration of devices and user identities.

Customer trend (business): Mobile use of business applications, customer service seen as key differentiator, managing more and more information.

Date of publication: 9th April 2009.

Customer need: Customer requires flexibility of service usage while changing locations (e.g. in the house) or going abroad. Besides session should continue seamlessly without losing connection, picture frames, etc., and the transfer should be as easy as possible: one click or even automatically using sensors or context information. Service adaptation should be supported based on availability of networks, network resources, and devices (e.g. splitting audio & video stream) too.

Other considerations: Customer may already own a "home hub" which provides several access technologies and services such as - WiFi, Fixed access (xDSL), IPTV, and VoIP capabilities within the home environment.

Detailed service description:

A user has a VoIP video call at a fixed IPTV set at home connected via xDSL. He/she wants to leave the house. Therefore, a transfer of the current video call has to be made to his/her mobile device using the in-house WiFi network. The session will be reduced to an audio conference only, because he/she wants to drive with his/her car afterwards and a video call on the mobile device while walking does not make sense.

While being in the car the session (audio call) will be transferred to a wide area network (WAN), such as UMTS (data transfer mode, VoIP client on the UMTS-device). In-house (fixed and wireless) & WAN being operated by one telecommunication operator and will host also other services. The handover is controlled by the network operator and triggered by context information of the user/customer management by the network operator (profile) and by network resource management and network context information (IEEE 802.21 information). Currently WiMAX is not considered as a home access technology.

Portfolio category: Fixed telephony, Mobile telephony, Broadband, Mobile Data.

Live service: No – but future

Market success: Probably

Customer benefits: Always best served (connection & service)

3.1.2 Use Case publication

The picture below shows the first use case published on the FMCA Wiki (http://usecases.thefmca.com).

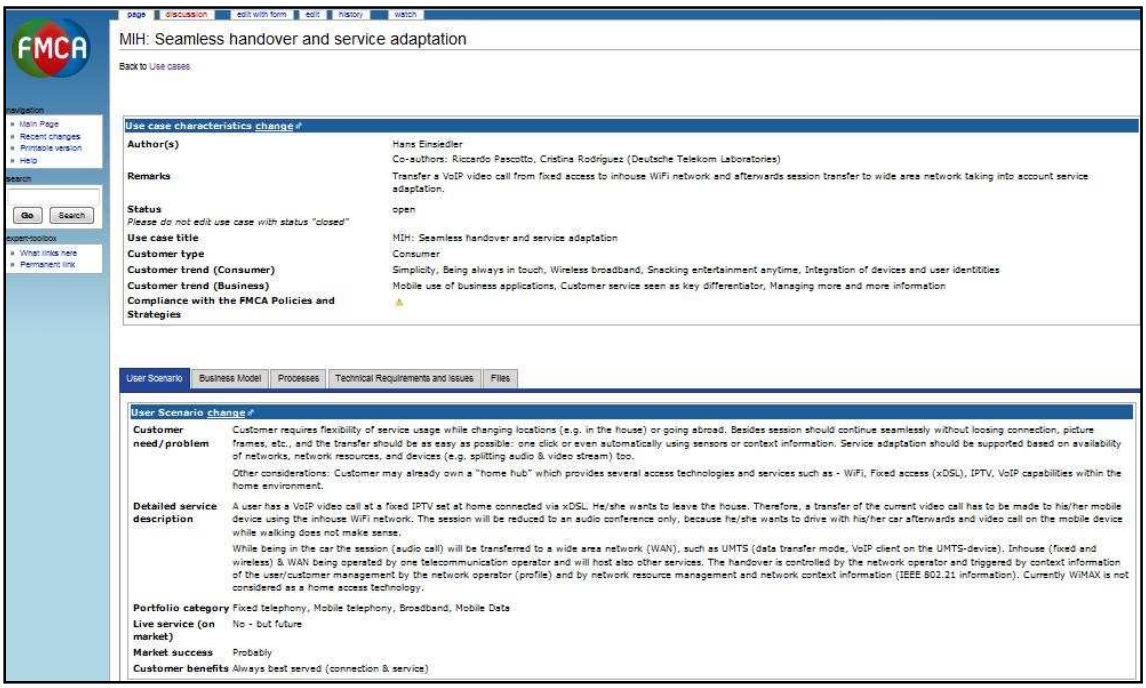


Figura 21: Use Case 1 published on the FMCA-Wiki

3.1.3 Use Case solution

While the user is at home, a conventional communication between both end users is made. In other words, a TCP/UDP connection is established, because a fixed line is used (xDSL).

Figura 22: Use Case 1 scenario

But, when the user leaves the house, a first handover is required. The connection from the IPTV set at home from the fixed line, has to be transferred to the user's mobile device using the in-house WiFi network. Since the user is having a video call it is necessary to enable continuity of sessions, and taking into account service adaptation, because the session has to be reduced to an audio conference only.

In order to transfer the session completely from the IPTV set to the mobile device, the following steps must be followed:

1) The mobile device must be discovered by the IPTV set. To discover it, the Service Location Protocol (SLP) is used. The diagram below shows how the different entities involved act:

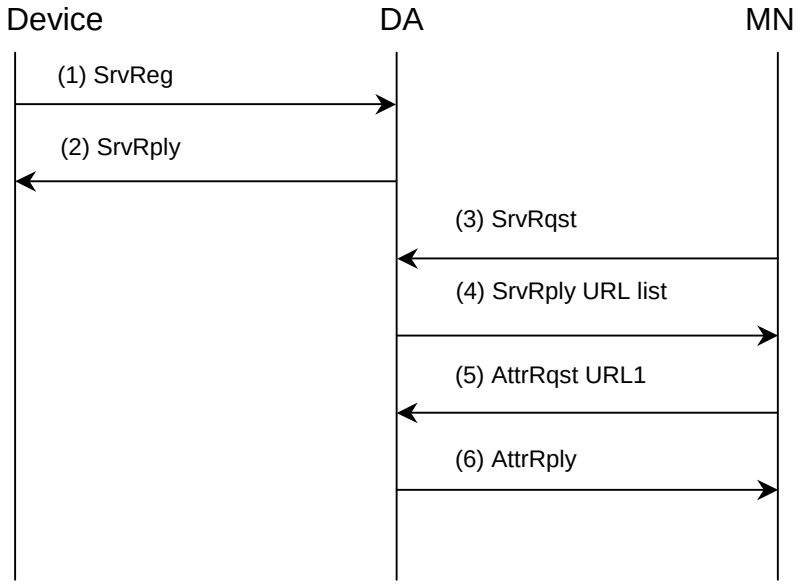


Figura 23: SLP protocol flow to discover devices

2) Once the mobile device has been discovered, the session must be transferred to it. To do it, the IPTV set uses Session Initiation Protocol (SIP)[122] Session Mobility. Two different modes are possible for session transfer, Mobile Node Control (MNC) mode and Session Handoff (SH) mode. Since the session must be completely transferred, the Session Handoff mode is used. The diagram below shows the protocol flow:

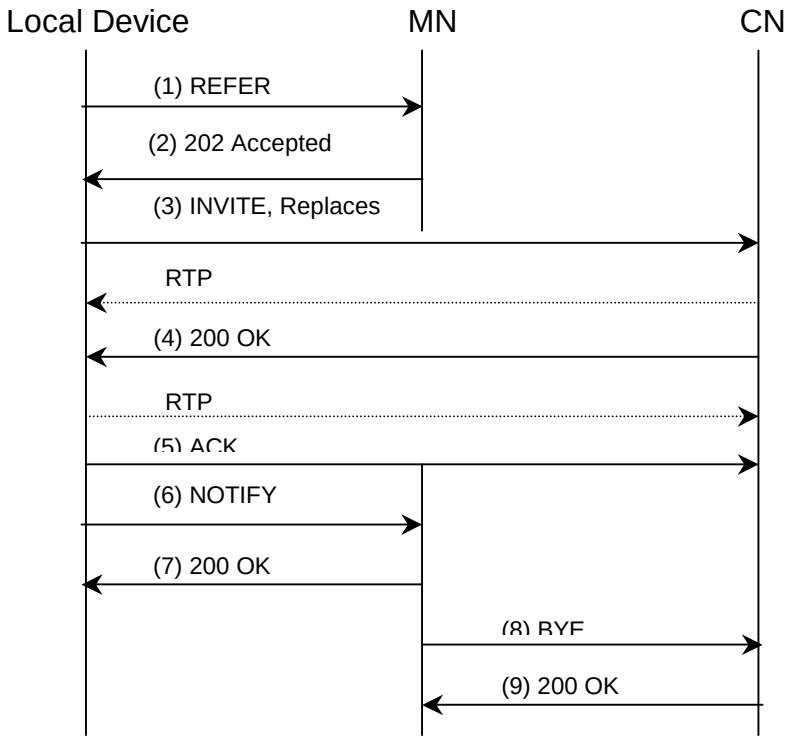


Figura 24: SIP protocol flow to transfer the session

The other factor to consider is how to split the session into audio conference only. Since SIP is rather a component that can be used with other IETF protocols to build a complete multimedia architecture, for describing multimedia sessions, Session Description Protocol (SDP) [124] should be used.

To transfer the session into audio conference only, a SIP re-INVITE request should be sent, but with SDP media parameters. Note that a re-INVITE is an INVITE request within the same dialog that established the session.

Since the user wants to transfer into audio conference only, the parameter of video should be suppressed, but the rest of parameters should be maintained and sent once again, as follows:

First INVITE request:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via:SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 356
```

(Alice's SDP)
v=0
o=alice 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/Alice/sdp.03.ps
e=alice@atlanta.com
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait

Re-INVITE request:

INVITE sip:bob@biloxi.com SIP/2.0
Via:SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 331
(Alice's SDP)
v=1 (1)
o=alice 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/Alice/sdp.03.ps
e=alice@atlanta.com
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696

```
a=recvonly
m=audio 49170 RTP/AVP 0
m=application 32416 udp wb
a=orient:portrait
```

(1)If the session description format has the capability for version numbers, the offerer should indicate that the version of the session description has changed.

The description of the SDP parameters is shown below:

```
Session description. Optional items are marked with a `*'.
    v=  (protocol version)
    o=  (owner/creator and session identifier).
    s=  (session name)
    i=* (session information)
    u=* (URI of description)
    e=* (email address)
    p=* (phone number)
    c=* (connection information - not required if included in all media)
    b=* (bandwidth information)
    One or more time descriptions (see below)
    z=* (time zone adjustments)
    k=* (encryption key)
    a=* (zero or more session attribute lines)
    Zero or more media descriptions (see below)
Time description
    t=  (time the session is active)
    r=* (zero or more repeat times)
Media description
    m=  (media name and transport address)
    i=* (media title)
    c=* (connection information - optional if included at session-level)
    b=* (bandwidth information)
    k=* (encryption key)
    a=* (zero or more media attribute lines)
```

The Network Mobility (NEMO) Basic Support protocol enables Mobile Networks to attach to different points in the Internet. The protocol is an extension of Mobile IPv6 and allows session continuity for every node in the Mobile Network as the network moves. It also allows every node in the Mobile Network to

be reachable while moving around. The Mobile Router, which connects the network to the Internet, runs the NEMO Basic Support protocol with its Home Agent. The protocol is designed so that network mobility is transparent to the nodes inside the Mobile Network.

Because of the explained before, NEMO protocol could be used to provide terminal mobility, considering the terminal as a mobile router and the IPTV set as a Home Agent. If we consider the mobile device as a mobile router attached in a first step to its Home Agent, other devices can be used at the same time, considering the terminal as their mobile router where they are attached.

Since in the use case nothing about the terminal as a mobile router is specified, then Mobile IPv6 could be used. Both alternatives are valid, because NEMO is an extension of Mobile IPv6, as explained before.

In a second step, the connection has to be transferred to a Wide Area Network, such UMTS, while the user is in the car. Then, when the connection to the Home Agent is almost lost, the mobile device handovers to another router and it uses NEMO protocol to inform its Home Agent that it is leaving the home link, and providing it its Care-of address.

The mobile node acts the same way when changing routers because of lost of coverage while travelling in the car.

During the process IEEE MIH 802.21 is used under the mobility protocol, but there is a problem: Seamless handover and service adaptation use case is partially addressed by network initiated handover with the assumption that the call information and user location is accessible by the network. The application switching from Video conference to Audio conference is a software application and is not supported by 802.21. The network may utilize the MIH information stored in the IS server. For this use case, we assume that the IS server is implemented on the PoS. [126]

3.2 Media Independent Handover: Seamless handover and service adaptation (II)

3.2.1 Use Case description

Remarks: Transfer a VoIP audio call from wide area network (Hotzone based on e.g. WiFi, WiMAX, or LTE) to a video call at airport WiFi network taking into account service adaptation.

Status: open.

Use case title: MIH: Seamless handover and service adaptation (II)

Customer type: Corporate consumer, Small and Medium Enterprises (SME), Consumer.

Customer trend (consumer): Using services seamlessly independent of the device or network used, simplicity, being always in touch, integration of devices and user identities.

Customer trend (business): Use case to be used for business customers as well.

Date of publication: 12th May 2009

Customer need: More and more workers spend the day in their car or travelling everywhere and they require flexibility of service usage while changing locations. Besides, session should continue seamlessly without losing connection, picture frames, etc., and the transfer should be as easy as possible. Service adaptation should be supported based on availability of networks and devices (e.g. splitting audio & video stream) too.

Detailed service description:

A user has an audio call in his/her car terminal while he/she is driving to the airport. The car terminal is connected to a hotzone (LTE, WiMAX, WiFi). When the hotzone coverage is lost, the car terminal handovers to another hotzone. When the user arrives to the airport, he/she gets out of the car and then, the audio call transfers from the car terminal to his/her mobile device. Once he/she is at the airport the mobile device is connected to the airport's WiFi. He/She turns on his/her laptop and the audio call transfers to a video call from the mobile device to the laptop – still connected to WiFi.

Portfolio category: Mobile telephony, Broadband, Mobile Data, Entertainment and TV.

Live service: No – but future

Market success: Probably

Customer benefits: Always best served (connection & service).

3.2.2 Use Case publication

The following picture shows the second use case published on the FMCA Wiki (http://usecases.thefmca.com).

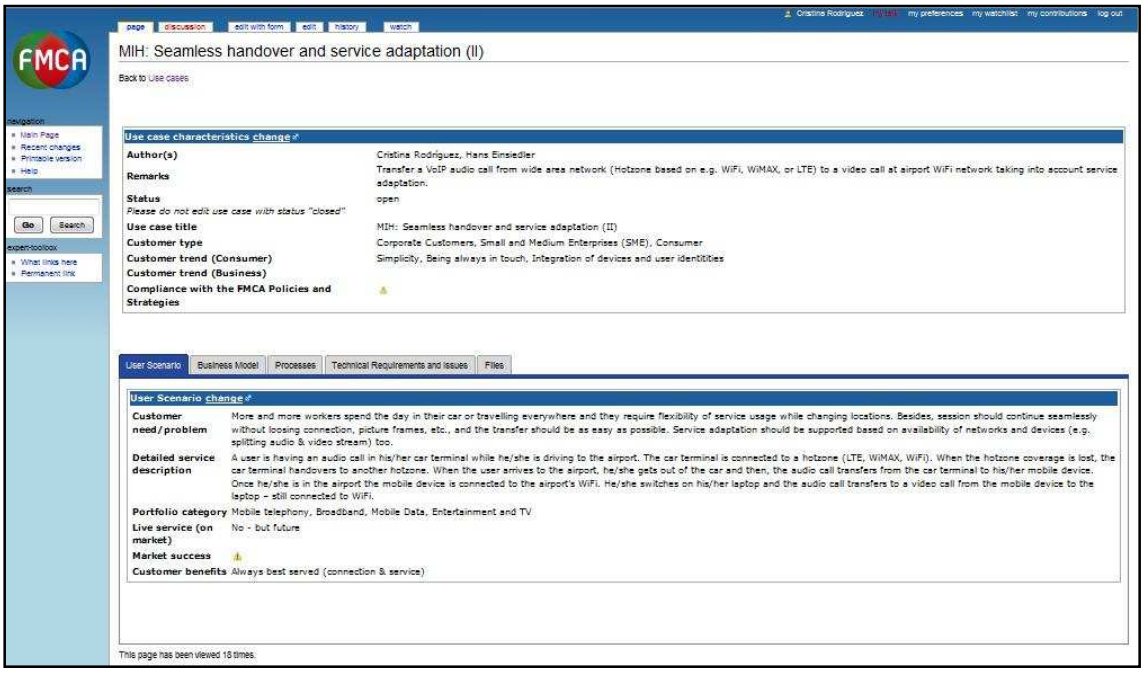


Figura 25: Use Case 2 published on FMCA-Wiki

3.2.3 Use Case solution

Figura 26: Use Case 2 scenario

While the user is in the car, the car terminal handovers from one hotzone to another using NEMO protocol. To transfer the connection from the car terminal to the user's mobile device, the following steps must be followed:

1) The mobile device must be discovered by the car terminal. To discover it, the Service Location Protocol (SLP) is used. The diagram below shows how the different entities involved act:

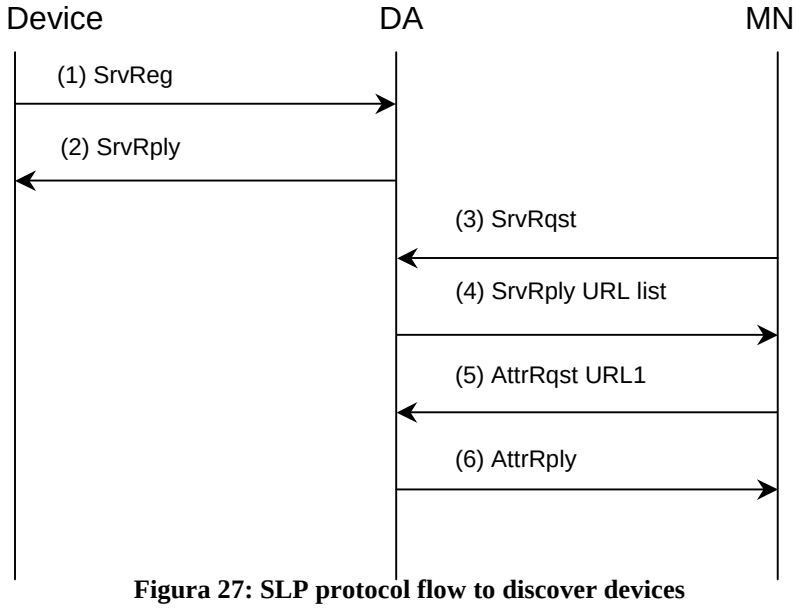


Figura 27: SLP protocol flow to discover devices

2) Once the mobile device has been discovered, the session must be transferred to it. To do it, the car terminal uses Session Initiation Protocol (SIP) Session Mobility. Two different modes are possible for session transfer, Mobile Node Control (MNC) mode and Session Handoff (SH) mode. Since the session must be completely transferred, the Session Handoff mode is used. The diagram below shows the protocol flow:

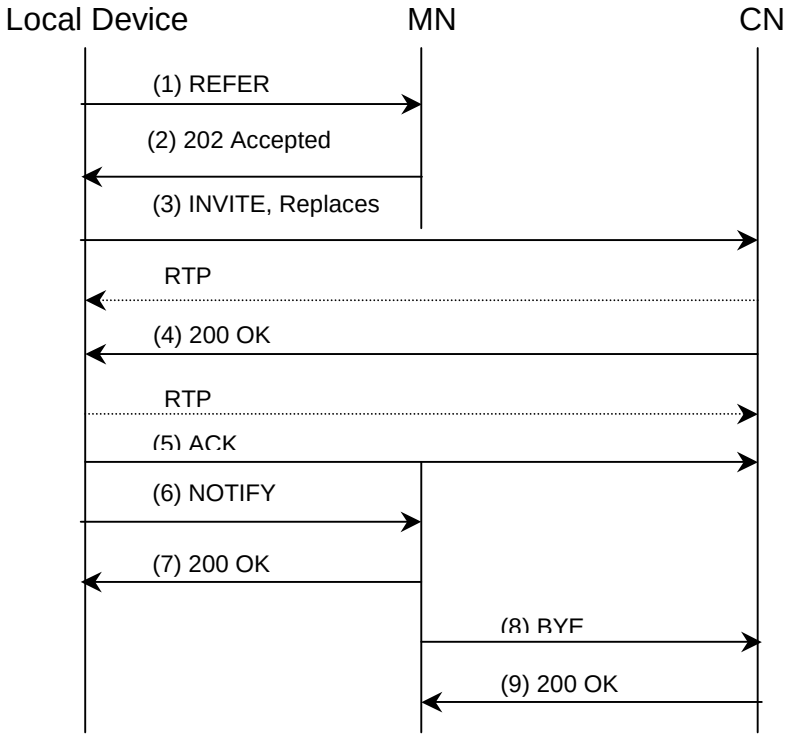


Figura 28: SIP protocol flow to transfer the session

To transfer the connection from the mobile device to the laptop, the same procedure explained before is done.

To transfer the audio conference into a video conference, SIP with SDP should be used. The actual session should be modified adding a media stream (video, in this case). So, as in the first use case, a re-INVITE request should be sent:

First INVITE request:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via:SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 331
(Alice's SDP)
v=0
o=alice 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/Alice/sdp.03.ps
e=alice@atlanta.com
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=application 32416 udp wb
a=orient:portrait
```

Re-INVITE request:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via:SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
```

Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 356
(Alice's SDP)
v=1 (2)
o=alice 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/Alice/sdp.03.ps
e=alice@atlanta.com
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait

(2) If the session description format has the capability for version numbers, the offerer should indicate that the version of the session description has changed.

As in the first use case, IEEE MIH 802.21 is used under the mobility protocol to obtain information about the different networks that are available, and to handover between different technologies.

3.3 Media Independent Handover: Seamless handover, service adaptation, administrative domain handover (III)

3.3.1 Use Case description

Remarks: Mobility or handover between a cellular technology (LTE or UMTS-HSPA) – which is managed by an operator – and Wireless LAN of a home network.

Status: open

Use case title: MIH: Seamless handover, service adaptation, administrative domain handover (III)

Customer type: Corporate consumer, Small and Medium Enterprises (SME), Consumer.

Customer trend (consumer): Simplicity, being always in touch, Wireless broadband, snacking entertainment anytime, integration of devices and user identities.

Customer trend (business): Use case to be used for business customers as well.

Date of publication: 19th May 2009

Customer need: More and more users want to snack entertainment everywhere at anytime, using a portable device or not. Because of that, a handover between a cellular technology and Wireless LAN of a home network is needed.

Detailed service description:

A user, who is a passenger in a car, has a video conference on his/her portable device (e.g. laptop, PDA, mobile phone) connected to a LTE or UMTS-HSPA. He/she arrives home and wants to continue the video conference on his/her IPTV set at home.

When the IPTV set is detected, the connection transfers from the portable device using the in-house Wireless LAN network, which is not managed by an operator. The home network is under full control of the user. Apart from the hand-over between devices, an inter-domain hand-over occurs from the cellular provider to the home-network supported by the fixed line operator.

The scenario covers two interesting points: the technical implementation of the hand-over and the administrative domain and business logic related topics.

Portfolio category: Mobile telephony, Broadband, Mobile Data, Entertainment and TV.

Live service: No – but future

Market success: Probably.

Customer benefits: Always best served (connection & service).

3.3.2 Use Case publication

The following picture shows the second use case published on the FMCA Wiki (http://usecases.thefmca.com).

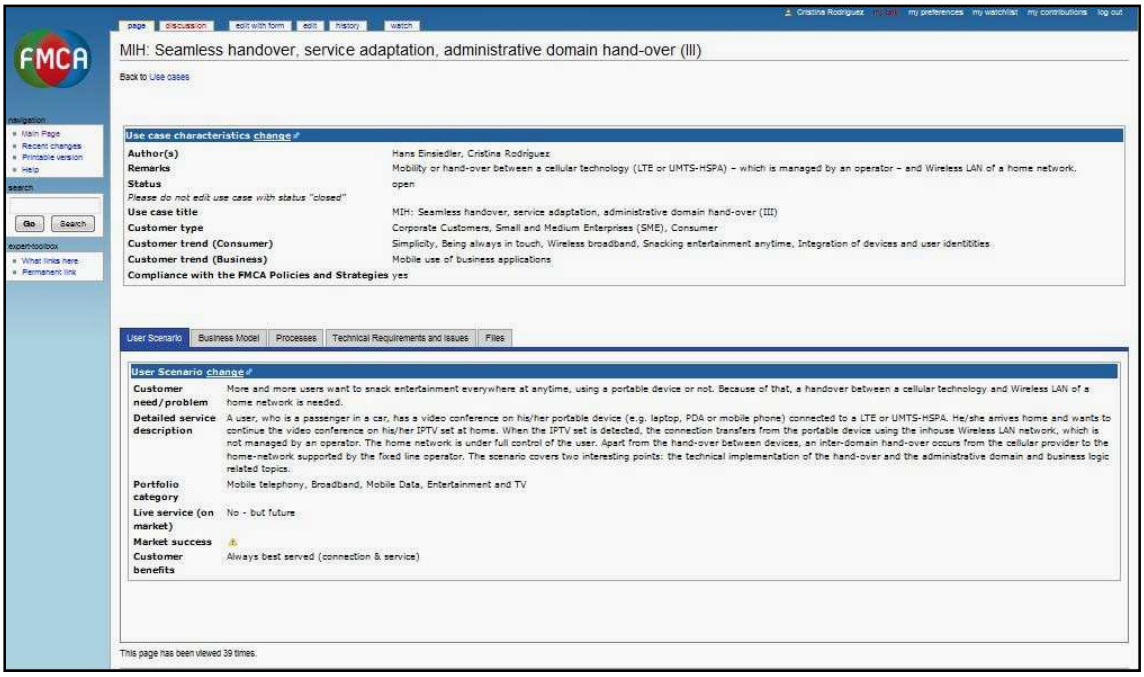


Figura 29: Use Case 3 published on FMCA-Wiki

3.3.3 Use Case solution

Figura 30: Use Case 3 scenario

The picture above shows the scenario of this use case.

To solve this use case, the “Multi-Access Network Mobility Solution” provided by Stoke could be used.

Multi-Access Network Mobility Solution (Stoke)

Introduction

As mobile broadband operators embrace multiple wireless access networks to economically deliver broadband services and content over a wider range of locations and circumstances, subscribers will come to expect broad-band coverage as ubiquitous, ignoring the wireless access network they are using at any given time. Given these expectations, MNOs are working to provide intelligent, automatic switching between supported access networks as part of the standard data services bundle.

Stoke delivers secure Multi-Access Network Mobility solutions today and has worked with partner technology vendors to develop a complete solution ecosystem to ease trials, integration and deployments. The Stoke mobility solution employs the Stoke Session Exchange (SSX) with MOBIKE to create a session mobility anchor for managing network hand-over of subscribers transitioning from one wireless access network to another. With little-to-no impact to existing network infrastructures, the Stoke solution enables mobile operators to deliver services over the most efficient and cost effective wireless technology available, and it frees subscribers from the hassle of manually (re)connecting to services as the connected network changes.

Stoke's mobility solution is deployed in the WiMAX core network allowing subscribers to move between the WiMAX, UMTS, and Wi-Fi networks while maintaining session continuity and without requiring additional network elements in either the Wi-Fi or 3G networks.

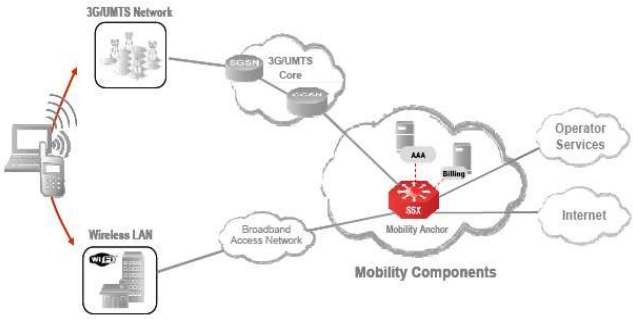


Figura 31: Stoke's mobility solution scenario example

A Multi-Access Network Mobility solution requires several ecosystem components to deploy including:

- Multi-radio mobile device with radio resource manager
- Client software supporting standard mobile infrastructure connectivity and mobility anchor element
- An IP-based AAA server for mobility services authorization

- A Stoke Session Exchange for mobility anchor functions including subscriber location management, traffic routing, and billing [127]

Stoke Session Exchange 3000 overview. Benefits summary.

Feature	Benefits
Multiple Access Technologies, Multiple Access Methods	Delivering broad support of access technologies in a single, multi-function device offers a leveraged Capex investment and ensures a long service life.
Multi-Function, Multi-Purpose	Enables operators to reduce overall network device count and network complexity, driving efficiency into network operations
Operationally Efficient	Requiring only two processing blade types (line card and management card), and consuming under 1200 watts of power fully loaded, the SSX reduces operations
Compact, Modular, High-Density	Enables operators to smoothly scale services from 8,000 to 240,000 active subscribers within a single 5RU footprint.
Multimedia Optimized	Latency under 50 µseconds and line rate support for small packet sizes ensures smooth video and voice services delivery.
Optimal Scalability	Subscribers, services and throughput scale linearly. Operators are not forced to trade off capacity in one functional area in order to access capacity in another.
Application Aware	Awareness of the applications within subscriber sessions enables operations including charging, QoS, and policy enforcement. Embedded in the mobile broadband access gateway relieves pressure on mobile core elements.
Flexible Traffic Classification	Comprehensive traffic classification allows easy bundling of mashups of applications, and flexible service classes support uniform treatment of the "subscriber service"

Tabla 10: Stoke Session Exchange 3000 benefits summary

Stoke OS

As mobile operators move toward providing high speed, media rich services to mass markets, new platforms and new operating systems are needed with the right underlying architecture and feature set to ensure ongoing service differentiation, rapid time to revenue, operational efficiency, and high availability.

StokeOS provides a powerful operating system and a rich set of tools for IP service enablement. Optimized for IP session management, Stoke OS supports the latest features to enable advanced multimedia services, improve operator visibility into network traffic with application awareness, ensure subscriber security and protect network resources, and deliver intelligent mobility network wide.

In addition, StokeOS is optimized for availability, with individual, dynamically restartable, processes running in protected memory on top of a hardened microkernel. Stoke developed middleware features advanced self-monitoring and self correcting capabilities as well as state check pointing and replication to ensure session persistence even through failures of essential system components. StokeOS also features self protecting capabilities to mitigate the impact of DoS attacks on the SSX.

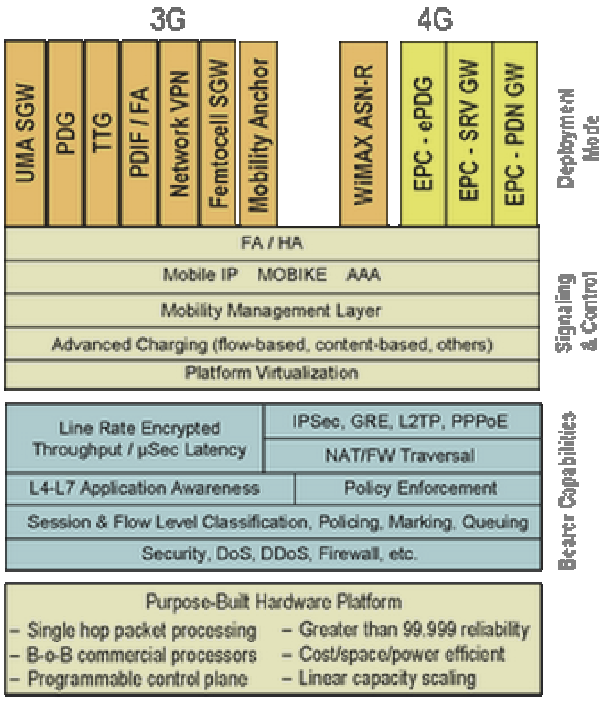


Figura 32: StokeOS includes a broad range of functions and supports a variety of access gateway roles (note color coding of the "Deployment Mode" level; orange indicates roles available today, yellow indicates planned).

StokeOS Feature Highlights

Session Management

The mobile broadband opportunity is forcing new requirements on carrier edge networks. In addition to managing much higher data rates and volumes, along with longer active session durations, Stoke delivers a wide range of IP session management capabilities including:

- Multiple access technology support
- Scalable session security
- Optimal multimedia session delivery
- Application awareness and control
- QOS and policy enforcement
- Flexible service definition and charging
- Mobility: Session continuity over multiple networks

Each function above is required to deliver an exceptional mobile broadband Internet experience. These functions ensure secure multimedia sessions over multiple access networks including support, control, and properly monetized in-house and over-the-top applications while providing seamless mobility for subscribers moving between access points and access networks.

Policy Enforcement

With key session management features in place, the StokeOS, together with the SSX-3000 enables operators to enforce subscriber and network wide policies to keep control of network use, ensure proper billing for services, and meet service level agreements. StokeOS supports DIAMETER and RADIUS, common protocols for retrieving policy information from PCRF functions and/or AAA servers. StokeOS applies access, charging, QoS, and use policies to individual sessions.

Policy enforcement functions are tightly coupled with Stoke application awareness capabilities to enable fine grained policy definition and application. For example, combining these capabilities combined enables operators to implement creative application accounting and charging solutions for home grown or partner content services.

Virtualization

StokeOS provides the foundation for provisioning, delivery, and charging for the next generation of multimedia services. Virtualization of the chassis provides a simple and efficient means of aligning the network with a broad range of market-driven retail and wholesale service models.

A context is a virtual router configured within the SSX, and the SSX can support up to 250 virtual routers or contexts – a single SSX chassis can be configured to appear as many separate logical routers. Every context runs routing protocols and has its own addressing domain, routing table, interface table, ARP table, and host table so address spaces can overlap. Because contexts behave as autonomous routers they can also be privately addressed, supporting multiple MVNOs and/or Enterprise customers.

Stoke OS Specifications	
Session Management	
Tunnel & Session Support	IPSec, PPP / PPPoE, DHCP
AAA Capabilities	RADIUS authentication (RFC 2865) RADIUS accounting (RFC 2866) RADIUS extensions (RFC 2869) RADIUS Change of Authorization (RFC 3576)
IP Address Assignment	Static, Internal address pool IPSec mode-config (draft-dukes-ike-mode-cfg-02.txt) IKEv2 Configuration Payload (CP)
Routing	OSPFv2 (RFC 2328) BGP4 (RFC 1771, 1997) RIPv2 (RFC 2453)
Virtualization	Up to 250 Contexts (virtual routers)
Mobility	Mobile IP (RFC 3344) MOBIKE (RFC 4555)
Traffic Management	
Traffic Classification	Payload inspection for application aware flow classification Static payload filter definitions with regular expressions Stateful packet classification L2/L3/L4 header based classification
QoS	802.1p, IP SA/DA, UDP/TCP port, protocol, ToS, DSCP DSCP-to-ToS Mapping Session and flow level marking, policing, queuing Deficit Round Robin scheduling Session and flow level RED
Reporting / Accounting	Call Detail Records 9ASN.1, CSV, TLV, XML upload formats) Session and flow level records Time and volume based
Mobile Network Standars Compliance	
Wireless LAN Interworking	3GPP system to WLAN Interworking; System Description (TS 23.234) 3GPP system to WLAN Interworking; Stage 3 (TS 29.234) 3GPP 3G Security; WLAN interworking security (TS 33.234) 3GPP2 Wireless LAN (WLAN) Interworking - List of Parts (X.S0028)
UMA	3GPP Generic access to the A/Gb interface (UMA Protocols) (TS 43.318)

IP Security	3GPP Network domain security; IP network layer security (TS 33.210)
Session Security	
IKE	IKEv1 and IKEv2 (Main mode, agressive mode, quick mode)
Authentication	PSK, digital certificate
Diffie-Hellman Groups	1,2,5 (RFC 2409, 3526)
Encryption Algorithms	DES-CBC (RFC 2405) 3DES-CBC (RFC 2451) AES-CBC (RFC 3602) AES-XBC-PRF-128 (RFC 3664) AES-XCBC-MAC-96 (RFC 3566) AES-128-CTR (RFC 3686)
HMAC Algorithms	HMAC-MD5-96 (RFC 2403) & HMAC-SHA-1-96 (RFC 2404)
Secondary Authentication:	XAUTH (IKEv1) (draft-beaulieu-ike-xauth-02.txt) EAP (IKEv2)
Client Configuration	MODECFG (IKEv1) Configuration payload (IKEv2)
Other IKE/IPSec Features	Rekeying Traffic Selector Negotiation of NAT Traversal (RFCs 3947) UDP encapsulation of IPSec ESP Packets (IKEv2) Liveness Detection (RFC 3948) Dead Peer Detection (IKEv2) Stateless cookies (IKEv2) MOBIKE (IKEv2)
Access Control List (ACL)	Static and Dynamic ACLs
Administration and Management	
System Management	Command Line Interface (CLI) - console and telnet Syslog (RFC 3164) SNMP v1 / v2c / v3 Comprehensive MIB Support
System Administration	Privilege-based administrator and operator user-types External administrator database via RADIUS Local administrator database
Enterprise MIBs	IPSEC MIB IPV4 EXTENSION IPV4 INTERFACE IPV4 PREFIX LIST IPV4 STATIC ROUTES SNMP RESEARCH SR AGENT INFO STOKE ENVMON STOKE PRODUCTS

	STOKE SMI STOKE SYSTEM TGT ADDRESS MASK USM TARGET TAG
Standard MIBs	ENTITY Interface IP FORWARD IP IPV6 IPV6 TCP IPV6 UDP OSPF RADIUS ACC CLIENT RADIUS AUTH CLIENT RADIUS DYNAUTH SERVER RFC1213 RFC1213 SMI RMON SNMP COMMUNITY SNMP FRAMEWORK SNMP MPD SNMP NOTIFICATION SNMP USM AES SNMP USM DH OBJECTS SNMP VIEW BASED ACM SNMPV2 SNMPV2 TM SNMPV2 USEC TCP MIB TRANSPORT ADDRESS UDP
Traps	Documentation Available on Request
Alarms	Documentation Available on Request

Tabla 11: Stoke OS Specifications

3.4 Media Independent Handover: QoS of available resources announcement through IEEE 802.21 Media Independent Information Service (MIIS)

3.4.1 Use Case description

Remarks: Common QoS resource control independent of the access technology and announcement of available resources trough IEEE802.21 Media Independent Information Service (MIIS). MIIS parameters can be used in a control system to manage multiple different access technology in the same operator domain.

Status: open

Use case title: MIH: QoS of available resources announcement through IEEE 802.21 Media Independent Information Service (MIIS).

Customer type: Corporate consumer, Small and Medium Enterprises (SME), Consumer.

Customer trend (consumer): Simplicity, being always in touch, Wireless broadband, snacking entertainment anytime, integration of devices and user identities.

Customer trend (business): Use case to be used for business customers as well.

Date of publication: 8th June 2009

Customer need: Nowadays, users desire to be always best connected wherever they are with certain QoS. Therefore, to provide QoS information while announcing the available resources through IEEE 802.21 Media Independent Service is required.

Detailed service description:

A user has a videoconference on his/her portable device (e.g. laptop, PDA or mobile phone) connected to a LTE or UMTS-HSPA while travelling (e.g, by train or by car). Then, while the user is on the way, the portable device loses coverage and a handover to another network has to be made. For this some information (availability of other access networks, situation of the cells, QoS situation, etc.) should be available to the terminal; therefore the IEEE 802.21 Media Independent Information Service can be used. Through this service the available bandwidth and the overload of the cell can be announced to potential connecting terminals. Depending on these parameters the user, the terminal or even the operator can decide to do a hand-over to a new cell.

Portfolio category: Mobile telephony, Broadband, Mobile Data, Entertainment, and TV.

Live service: No – but future

Market success: Probably.

Customer benefits: Always best served (connection & service).

3.4.2 Use Case publication

The following picture shows the second use case published on the FMCA Wiki (http://usecases.thefmca.com).

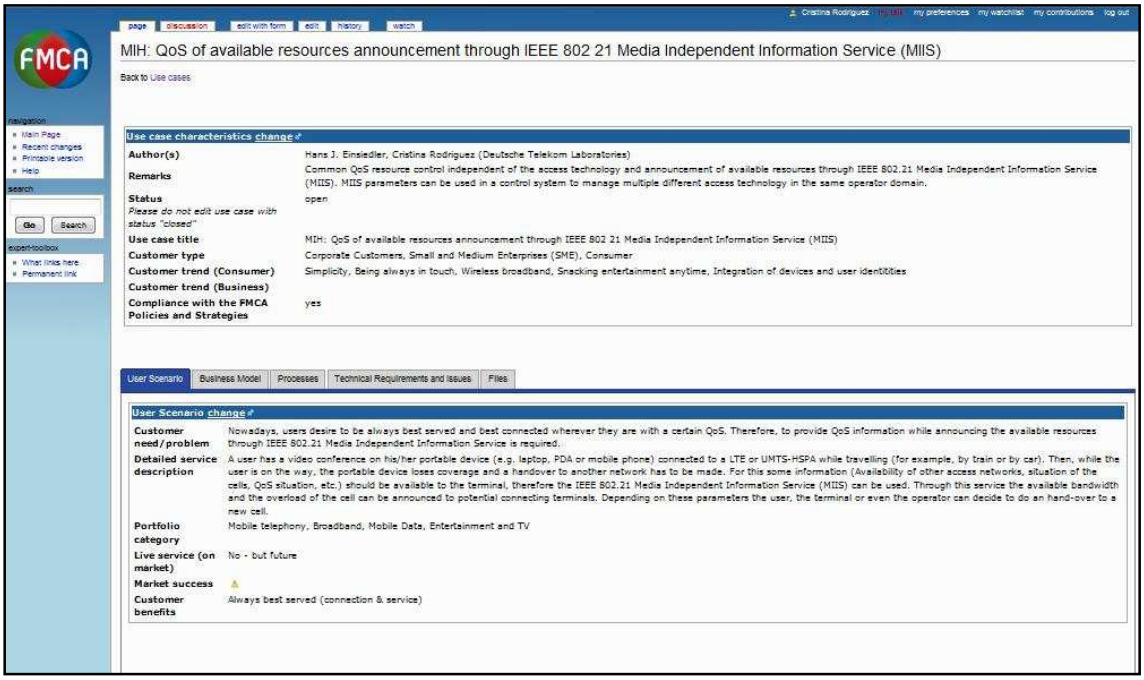


Figura 33: Use Case 4 published on FMCA-Wiki

3.4.3 Use Case solution

Regarding IEEE 802.21 MIH Protocol, several parameters of QoS, as “Minimum packet transmission delay” or “Packet Loss rate”, and the mechanisms to announce them are defined. However, neither the available bandwidth nor the overload of the cell, are defined yet.

Because of that, it could be an option to define these parameters and after that, to use the mechanisms already defined in IEEE 802.21 MIH Protocol, to solve this use case.

With these new parameters defined, the procedure would be the explained below:

MN was registered to PoS1 through Com3 via Link1. When test starts, PoS1 asks MN for providing a list of candidate networks. Once PoS1 receives the list of candidate networks from MN, it indicates MN about its choice of target point of attachment which is PoA2. Once attached to PoA2, the MN deregisters from PoS1 and detaches drom PoA1. [128]

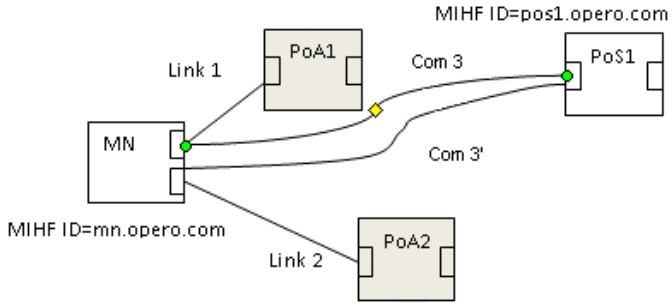


Figura 34: Use Case 4 scenario

The steps followed are:

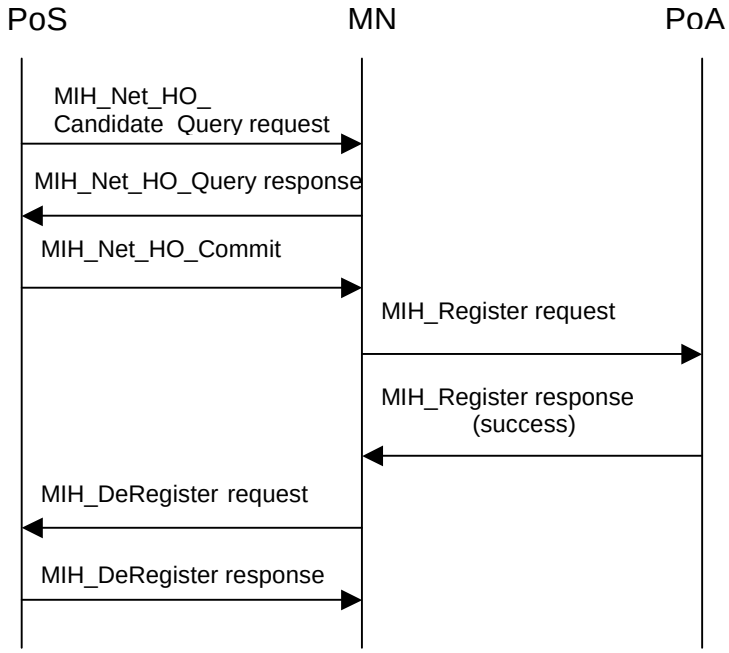


Figura 35: MIH protocol flow

1. PoS1 sends MIH_Net_HO_Candidate_Query request message to MN through Com3 via Link 1 (PDU14)
2. MN responds with MIH_Net_HO_Query response message to PoS1 through Com3 (PDU15)
3. PoS1 sends MIH_Net_HO_Commit request message to MN through Com3 (PDU22)
4. MN attaches to PoA2 and establishes Link2.
5. MN establishes Com3' (PDU35-36)
6. MN deregistered from PoS1 (PDU37-38)
7. MN disconnects from PoA1 and break Link1.

CAPÍTULO 4

CONCLUSIONES Y TRABAJOS FUTUROS

En este capítulo se expondrán las conclusiones a las que se han llegado tras la elaboración de este proyecto, y se comentarán los posibles trabajos futuros que se podrían realizar a partir de él.

4.1 Conclusiones

Este proyecto contiene parte del trabajo desarrollado en Deutsche Telekom AG Laboratories durante el programa de prácticas Extended Mobility, donde se ha tenido la oportunidad de trabajar en tareas de investigación sobre tecnologías que, a nivel personal, eran desconocidas. También se me ha brindado la oportunidad de verme inmersa en un entorno empresarial real, además de internacional, y poder colaborar con grandes expertos.

Si recuperamos los objetivos planteados al inicio de dicho programa, podemos ver que se han desarrollado todos y cada uno de ellos.

En primer lugar, se ha realizado un estudio sobre la movilidad en Redes de Siguiente Generación, estudiando cada uno de los grupos de trabajo que se centran en estos aspectos. Además, mediante la búsqueda de proyectos, proveedores y operadores, hemos accedido a las soluciones y productos de movilidad que ofrecen los mismos actualmente, para hacernos así una idea general de 1os problemas que resuelven.

Uno de los problemas principales que se encontró en esta parte del trabajo fue que muchos de los documentos que se consultaron podían no ser una versión definitiva y estar sujetos a cambios, ya que las tecnologías y mecanismos sobre los que se estaba realizando el estudio son relativamente novedosas. También por este mismo motivo fue difícil encontrar una amplia oferta de productos y/o servicios, y además la mayor parte de proveedores y operadores que ofertaban algún tipo de producto de esta índole no proporcionaba información técnica relevante sobre el mismo, sino que se limitaba a una descripción cualitativa de las características.

Tras la realización de este estudio que comprende la mayor parte del trabajo desarrollado durante la estancia, se procedió a la elaboración de cuatro casos de uso. Mediante conferencias telefónicas internacionales se pusieron en común estos casos de uso junto con los propuestos por otros miembros de Fixed-Mobile Convergence Alliance. En estas conferencias todos los miembros planteaban sus dudas respecto a los diferentes casos de uso, así como sus observaciones y consejos de mejora.

Una vez puesto todo en común se procedió a la elaboración de posibles soluciones teóricas. Un aspecto que quedaría por resolver, sería la puesta en común de las soluciones propuestas, obteniendo así *feedback* de los distintos miembros, pudiendo llegar a mejores soluciones, más realistas y más eficientes.La siguiente tarea a abordar era la realización de los documentos que contenían tanto el estudio realizado sobre la movilidad en redes de siguiente generación, como los casos de uso y las soluciones teóricas propuestas.

Otro aspecto a resaltar es que, a pesar de que combinando los mecanismos aportados por IEEE 802.21 con los diferentes protocolos de movilidad, podemos realizar los handovers entre las distintas tecnologías existentes, queda por resolver el algoritmo de decisión de qué información proporcionar para cada tipo de red. Este aspecto queda sujeto a las diferentes implementaciones, así como qué parámetros evaluar para realizar un handover eficiente.

4.2 Trabajos futuros

A pesar del trabajo realizado durante la estancia, queda todavía un largo camino por recorrer en aspectos de movilidad en Redes de Siguiente Generación, y varios de los hitos de este camino se exponen en este punto.

En primer lugar, se haría necesario una evaluación de las soluciones teóricas planteadas para los distintos casos de uso, donde analizar deficiencias y proponer mejoras.

Una vez que esas soluciones hubiesen sido, de alguna manera, validadas, se podría abordar la realización de simulaciones de las mismas para analizar de una forma más práctica su validez y la posibilidad de implementarlas.

Si los resultados de las simulaciones fueran favorables, se podría proceder a la implementación de las soluciones en maquetas reales, donde se podría ver de una manera más real su funcionamiento y solventar posibles deficiencias.

Como punto final, si todos los aspectos anteriores han resultado favorables y aptos para la realización, se podría plantear una manera de llevarlo a la práctica e implantarlo en entornos controlados para continuar realizando baterías de pruebas.

Uno de los aspectos a resolver para poder trasladar al “mundo real” las soluciones a los distintos escenarios propuestos, sería llegar a un acuerdo entre operadores para facilitar *handovers* entre sus redes, ya que en un entorno real es bastante complicado encontrarnos con una situación en las que las distintas redes sean propiedad de un mismo operador.

Sin embargo, cada una de estos trabajos futuros propuestos no formaban parte de los objetivos iniciales del programa y, debido a limitaciones de tiempo, no se ha podido llevar a cabo ninguno de ellos, aunque sería deseable poder realizar al menos los dos primeros.

APÉNDICE A

PRESUPUESTO

En el presente proyecto se ha realizado un estudio sobre las tecnologías actuales disponibles para llevar a cabo el desarrollo de nuevos escenarios y casos de uso en lo que a la movilidad de usuario y red se refiere.

Para ello, en primer lugar fue necesario realzar un estudio sobre la filosofía y las capacidades de las distintas tecnologías existentes, así como en desarrollo. Se estudiaron y analizaron las diferentes posibilidades que nos brindaban cada uno de los estándares, qué problemas resolvían y cuáles no.

En función de los resultados obtenidos, se aplicaron diversas soluciones teóricas a los distintos casos de uso propuestos, que posteriormente fueron publicados y discutidos con los miembros que componen Fixed-Mobile Convergence Alliance.

En esta sección se muestra detalladamente el coste total de la ejecución del proyecto. Para calcular dicho coste, se ha dividido el proyecto en diferentes tareas que representan las distintas fases de desarrollo del mismo, así como su evolución en el tiempo.

Para cada una de las tareas individuales, se detallará toda la información relevante, y se representarán todas las tareas de forma conjunta en un diagrama de Gantt. Por último, se calculará el coste total del proyecto.

A.1 Descomposición en tareas

El proyecto se compone de diversas tareas, las cuales a su vez, están divididas en subtareas. En este mismo apartado se aportará información detallada para cada una de las tareas y subtareas, como la descripción de la misma, los objetivos, las relaciones de dependencia con otras tareas y/o subtareas, la duración y el esfuerzo asociado a cada una de ellas. El cálculo del esfuerzo se ha basado en una jornada de 8 horas/día y 20 días/mes.

A continuación se indican las tareas en las que se ha dividido el proyecto:

- **Tarea A:** Documentación y análisis del estado del arte.
- **Tarea B:** Elaboración de casos de uso.
- **Tarea C:** Preparación y publicación de documentos.
- **Tarea D:** Documentación y realización de la memoria del proyecto.

A.1.1 Tarea A: Documentación y análisis del estado del arte

Subtarea A.1: Estudio de los grupos de trabajo relacionados con aspectos de movilidad de red y usuario

Descripción: En primer lugar se realizó el estudio de los grupos de trabajo que están relacionados con los aspectos de movilidad de red y de usuario. A través del conocimiento de estos grupos de trabajo, se accedió a los protocolos y mecanismos desarrollados y/o en desarrollo para implementar la movilidad en Redes de Siguiente Generación. Por otra parte, se realizó un estudio de IEEE 802.21 Media Independent Handover Services.

Objetivos:

- Familiarizarse con los grupos de trabajo existentes involucrados en el estudio y desarrollo de mecanismos y protocolos para la implementación de la movilidad de red y usuario en redes de siguiente generación.
- Estudio de IEEE 802.21 Media Independent Handover Services.
- Redacción de un documento inicial, resumiendo toda la información relevante sobre los grupos de trabajo estudiados.

Dependencias: Esta subtarea es la inicial del proyecto.

Duración: Ocho semanas.

Esfuerzo: Ingeniero, 0.7 personas-día.

Subtarea A.2: Búsqueda de proyectos de investigación y desarrollo, operadores y fabricantes

Descripción: En esta subtarea se realizó un estudio sobre los proyectos de investigación y desarrollo que aportaran una solución relacionada con la movilidad de red, así como operadores y fabricantes que ofrecieran productos y/o soluciones personalizadas.

Objetivos:

- Búsqueda de proyectos desarrollados relacionados con la movilidad en Redes de Siguiente Generación.
- Búsqueda y estudio de las soluciones y/o productos ofrecidos por operadores de telefonía.
- Búsqueda y estudio de productos ofrecidos por fabricantes.
- Redacción de un documento conteniendo la información recabada en esta subtarea.

Dependencias: Esta subtarea comenzará después de haber finalizado la subtarea A.1.

Duración: Dos semanas.

Esfuerzo: Ingeniero, 0.7 personas-día.

A.1.2 Tarea B: Elaboración de casos de uso

Subtarea B.1: Planteamiento de casos de uso

Descripción: Una vez realizado el estudio de los grupos de trabajo y soluciones existentes relacionadas con la movilidad tanto de red como de usuario, se procede al planteamiento de cuatro casos de uso.

Objetivos:

- Estudio de la necesidad de los usuarios en relación con las comunicaciones móviles.
- Descripción de los distintos casos de uso.
- Publicación de los casos de uso en colaboración para Fixed-Mobile Convergence Alliance.

Dependencias: Esta subtarea comienza después de finalización de la subtarea A.2.

Duración: Dos semanas.

Esfuerzo: Ingeniero, 0.6 personas-día.

Subtarea B.2: Discusión de casos de uso

Descripción: Una vez realizada la publicación de los casos de uso en la Wiki de Fixed-Mobile Convergence Alliance, se procede a la discusión de la viabilidad de los mismos.

Objetivos:

- Discusión de los casos de uso junto con Fixed-Mobile Convergence Alliance mediante conferencias telefónicas.
- En caso de ser necesario modificaciones, se realizan sobre los casos de uso.

Dependencias: Esta subtarea comienza después de finalización de la subtarea B.1.

Duración: Una semana.

Esfuerzo: Ingeniero, 0.4 personas-día.

Subtarea B.3: Planteamiento de soluciones teóricas

Descripción: Una vez publicados y revisados los diferentes casos de uso, se procede al planteamiento de una solución teórica.

Objetivos:

- Planteamiento de soluciones teóricas para los casos de uso.
- Análisis de posibles problemas que quedan sin resolver.
- Redacción de un documento conteniendo la información recabada en esta subtarea.

Dependencias: Esta tarea comienza después de finalización de la subtarea B.2.

Duración: Dos semanas.

Esfuerzo: Ingeniero, 0.7 personas-día

A.1.3 Tarea C: Preparación y publicación de documentos

Descripción: Esta tarea consiste en la recopilación de todo el material utilizado durante las tareas anteriores para la preparación de los documentos pertinentes.

Objetivos:

- Publicación de un documento final conteniendo la totalidad del estudio teórico realizado: estado del arte, productos y soluciones.
- Publicación de un segundo documento con los casos de uso desarrollados y sus posibles soluciones teóricas planteadas.

Dependencias: Esta tarea comienza después de finalización de la tarea B.3.

Duración: Dos semanas.

Esfuerzo: Ingeniero, 0.7 personas-día

A.1.4 Tarea D: Documentación y realización de la memoria del proyecto

Descripción: En esta tarea se procederá a redactar la memoria final del proyecto, comentando los aspectos más relevantes de la realización del mismo. Para la realización de esta memoria se utilizarán todos los documentos generados durante el proyecto.

Objetivos:

- Presentación final del estudio realizado durante la estancia en Deutsche Telekom AG Laboratories.
- Presentación final de los casos de uso y las soluciones teóricas aportadas.

Dependencias: Esta tarea comienza después de finalización de la tarea C.

Duración: Tres semanas.

Esfuerzo: Ingeniero, 0.9 personas-día.

A continuación se presenta en forma de tabla la información sobre el tiempo empleado en cada tarea.

Tareas	Duración (semanas)	Esfuerzo (personas-día)	Total (horas)
A. Documentación y análisis del estado del arte			
A.1. Estudio de los grupos de trabajo relacionados con aspectos de movilidad de red y usuario			
♦ Ingeniero	8	0.7	224
A.2. Búsqueda de proyectos de investigación y desarrollo, operadores y fabricantes			
♦ Ingeniero	3	0.7	84
Total Tarea A			**308**
B. Elaboración de casos de uso			
B.1. Planteamiento de casos de uso			
♦ Ingeniero	2	0.6	48
B.2. Discusión de casos de uso			
♦ Ingeniero	1	0.4	16
B.3. Planteamiento de soluciones teóricas			
♦ Ingeniero	3	0.7	84
Total Tarea B			**148**
C. Preparación y realización de documentos			
♦ Ingeniero	2	0.7	56
Total Tarea C			**56**
D. Documentación y realización de la memoria del proyecto			
♦ Ingeniero	3	0.9	108
Total Tarea D			**108**
Total proyecto			**620**

A.2 Diagrama de Gantt

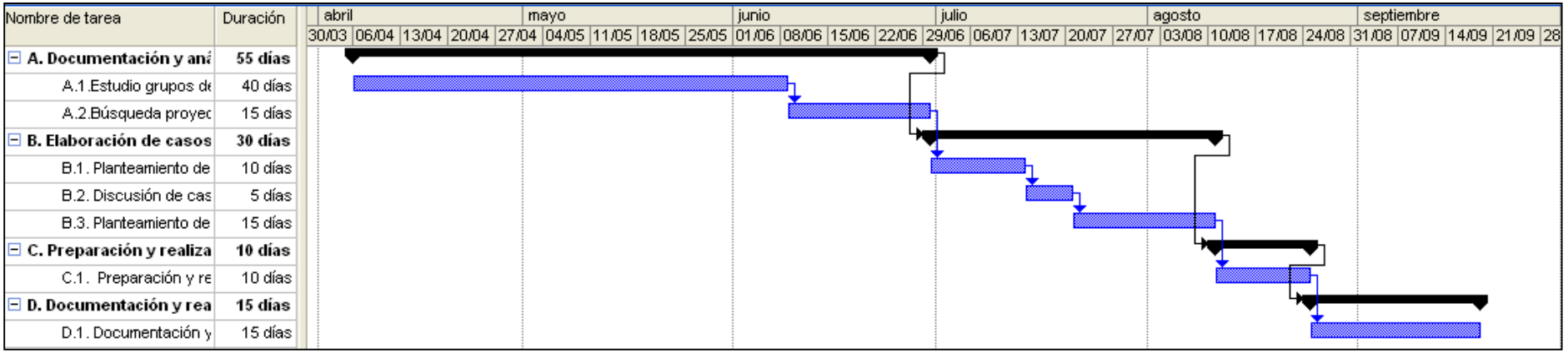


Figura 36: Diagrama de Gantt

En el diagrama de Gantt que se muestra en la figura anterior, se puede ver la relación existente entre las tareas. Cabe destacar que la escala temporal que aparece es aproximada y no real. Es decir, el tiempo empleado para desempeñar las tareas es el mostrado, pero las fechas no son las exactas, debido a que durante la estancia en Deutsche Telekom AG Laboratories, se llevaron a cabo también otras tareas que en el presente diagrama no aparecen, debido a que no son relevantes en relación con el tema del proyecto.

A.3 Costes del proyecto

En esta sección se muestra el coste del proyecto estimado. Tal y como se puede observar a continuación, el coste está desglosado en coste de personal y de material.

Concepto	Cantidad	Coste unitario	Importe
Costes de personal			
Ingeniero Superior de Telecomunicaciones	620 horas	60 €/hora	37200 €
Total costes personal			**37200 €**
Costes de material			
Ordenador portátil	1 unidad	1100 €	1100 €
Conexión a Internet	6 meses	36 €/mes	216 €
Total costes material			**1316 €**
Total proyecto			**38516 €**

El presupuesto total del proyecto asciende a **treinta y ocho mil quinientos dieciséis euros**.

APÉNDICE B

PROCEDIMIENTOS HANDOVER IEEE 802.21

B.1 Mobile-initiated handover procedure

The Mobile-initiated handover procedure operates as follows (see Figura 37, Figura 38, Figura 39, and Figura 40):

1) The Mobile Node is connected to the serving network via the current PoS and it has access to the MIH Information Server.

2) The Mobile Node queries information about neighboring networks by sending an MIH_Get_Information request message to the Information Server. The Information Server responds with an MIH_Get_Information response message. This information is attempted as soon as the Mobile Node is first attached to the network.

3) The Mobile Node triggers a mobile-initiated handover by sending an MIH_MN_HO_Candidate_Query request message to the Serving PoS. This request contains the information of potential candidate networks.

4) The Serving PoS queries the availability of resources at the candidate networks by sending an MIH_N2N_HO_Query_Resources request message to one or multiple Candidate PoSs.

5) The Candidate PoSs respond with an MIH_N2N_HO_Query_Resources response message and the Serving PoS notifies the Mobile Node of the resulting resource availability at the candidate networks through an MIH_MN_HO_Candidate_Query response message.

6) The Mobile Node decides on the target of the handover and notifies the Serving PoS of the decided target network information by sending the MIH_MN_HO_Commit request message. Also, the Mobile Node commits a link switch to the target network interface by invoking the MIH_Link_Actions.request primitive.

7) The Serving PoS sends the MIH_N2N_HO_Commit request message to the Target PoS to request resource preparation at the target network. The Target

PoS responds the result of the resource preparation by an MIH_N2N_HO_Commit response message.

8) The new layer 2 connection is established and a certain mobility management protocol procedures are carried out between the Mobile Node and the target network.

9) The Mobile Node sends an MIH_MN_HO_Complete request message to the Target PoS. The Target PoS sends an MIH_N2N_HO_Complete request message to the previous Serving PoS to release resource, which was allocated to the Mobile Node. After identifying that resource is successfully released, the Target PoS sends an MIH_MN_HO_Complete response message to the Mobile Node.

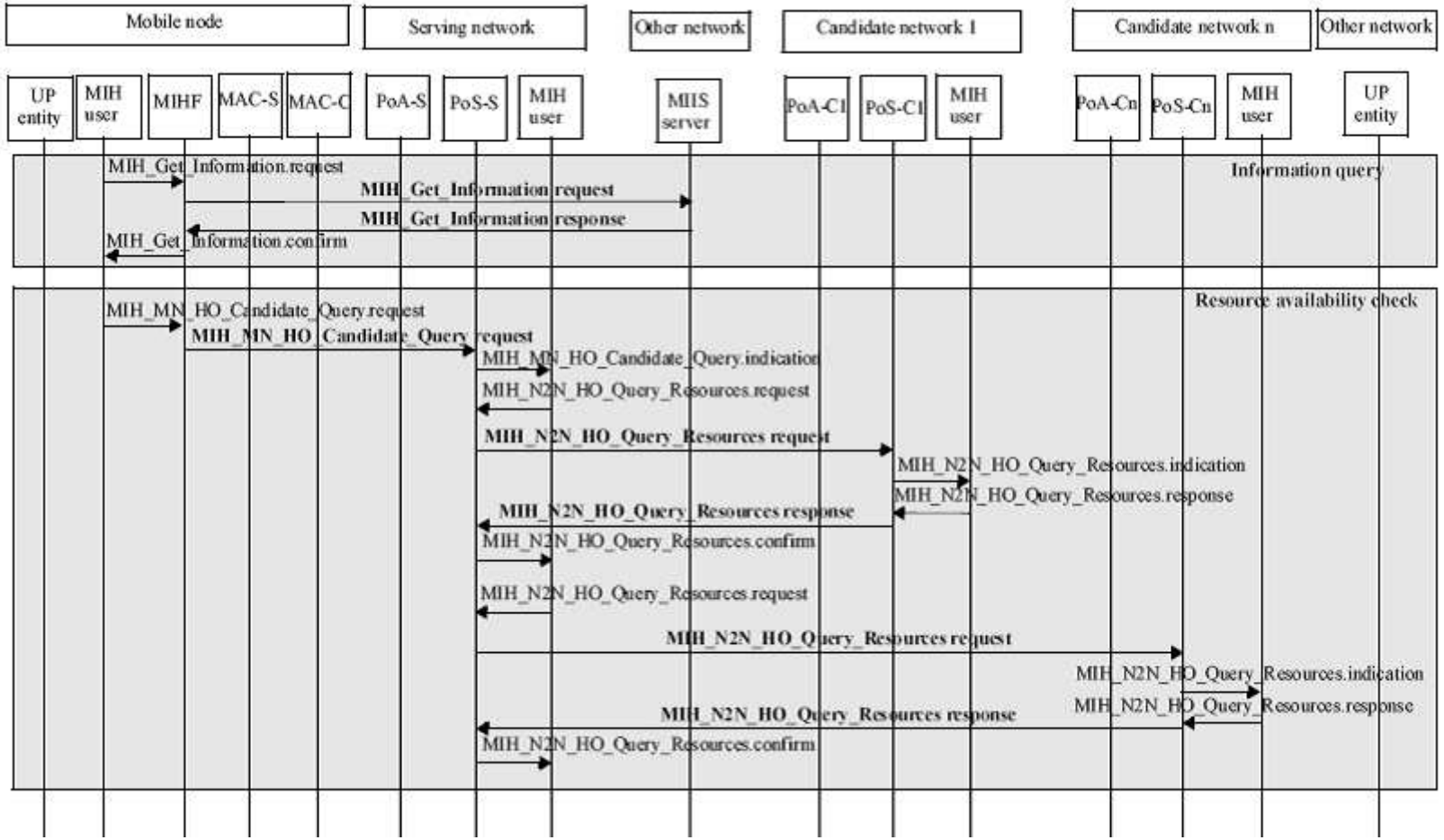


Figura 37: Mobile-initiated handover procedure

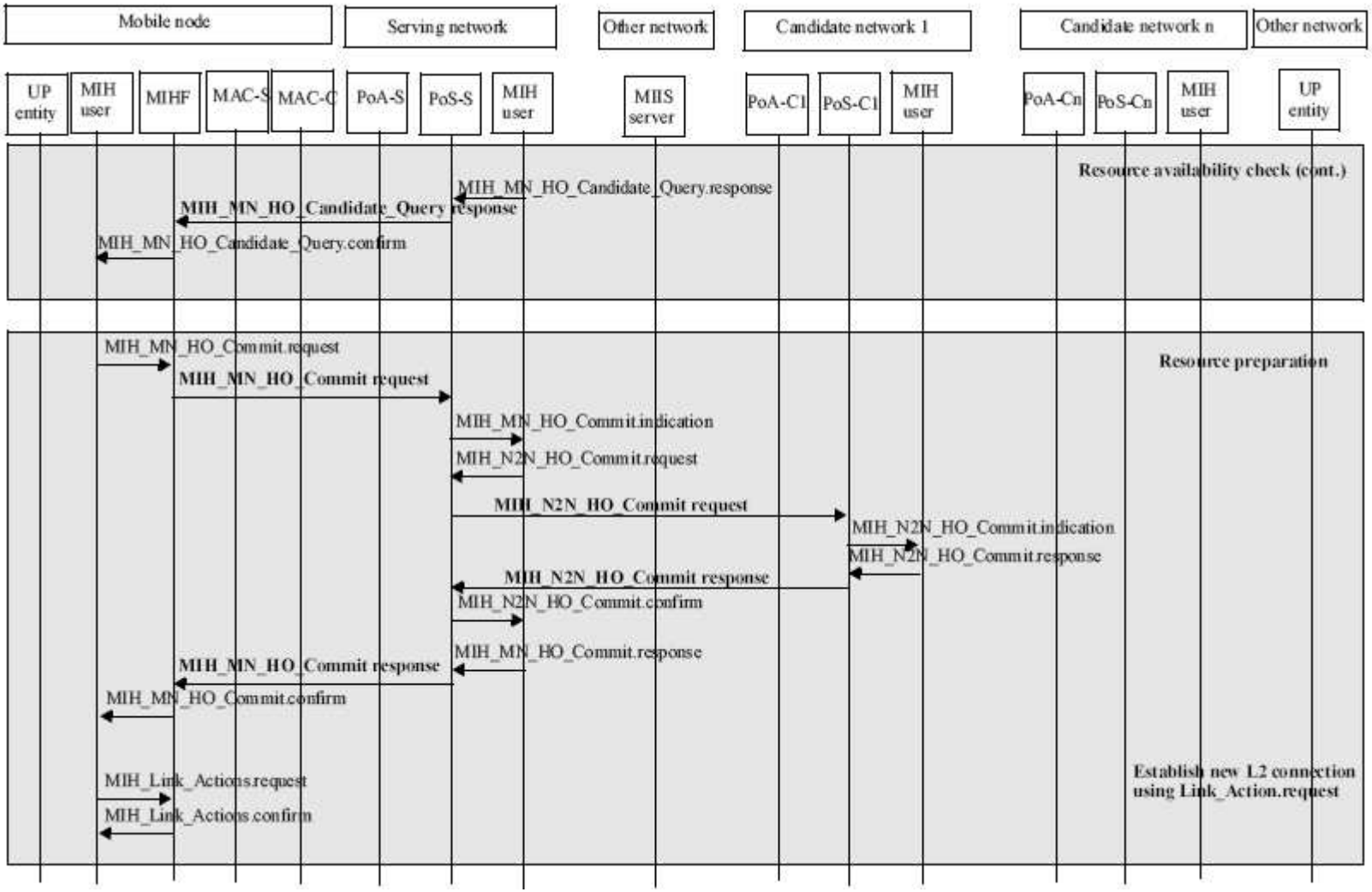


Figura 38: Mobile-initiated handover procedure (cont.)

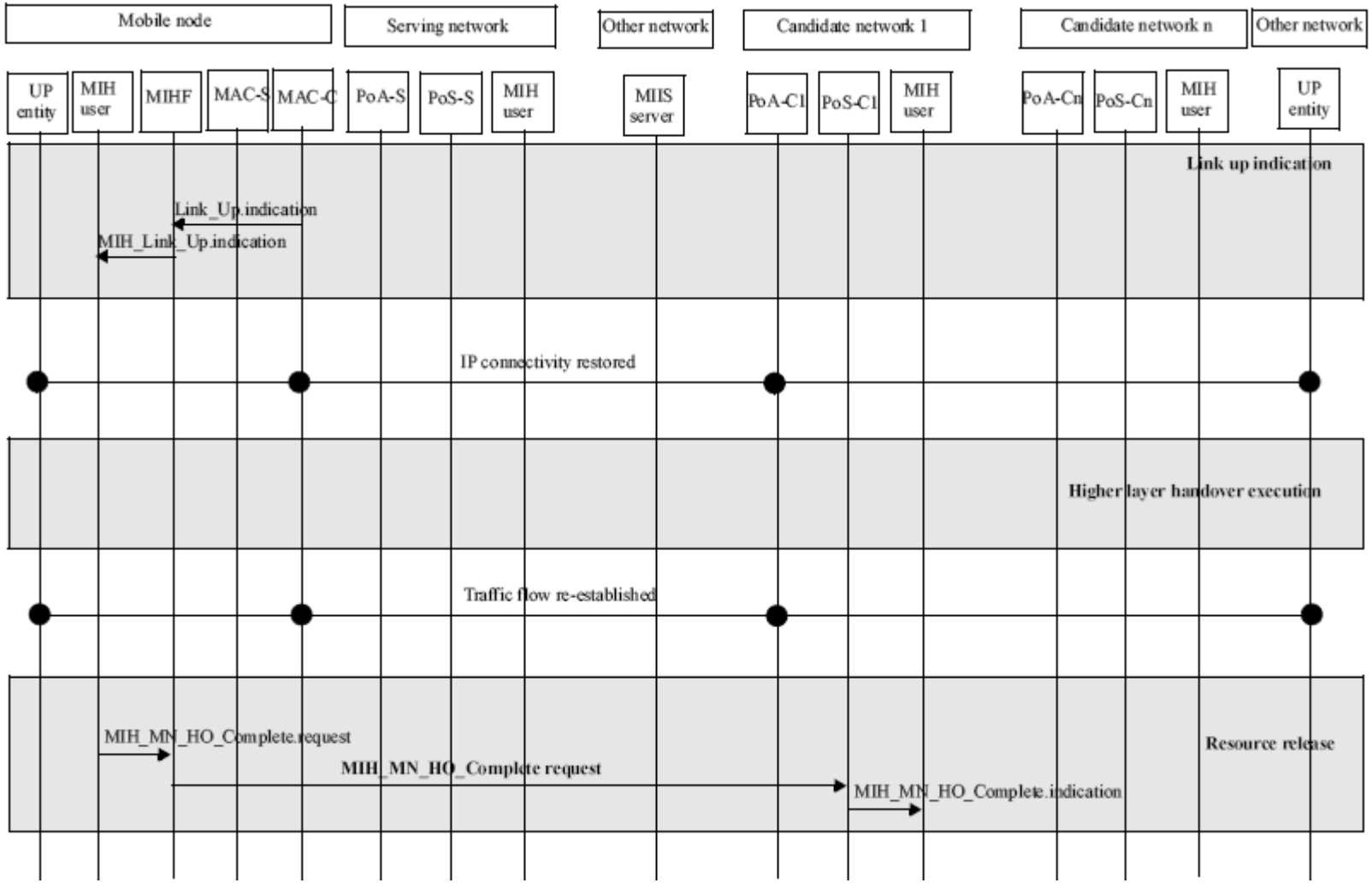


Figura 39: Mobile-initiated handover procedure (cont.)

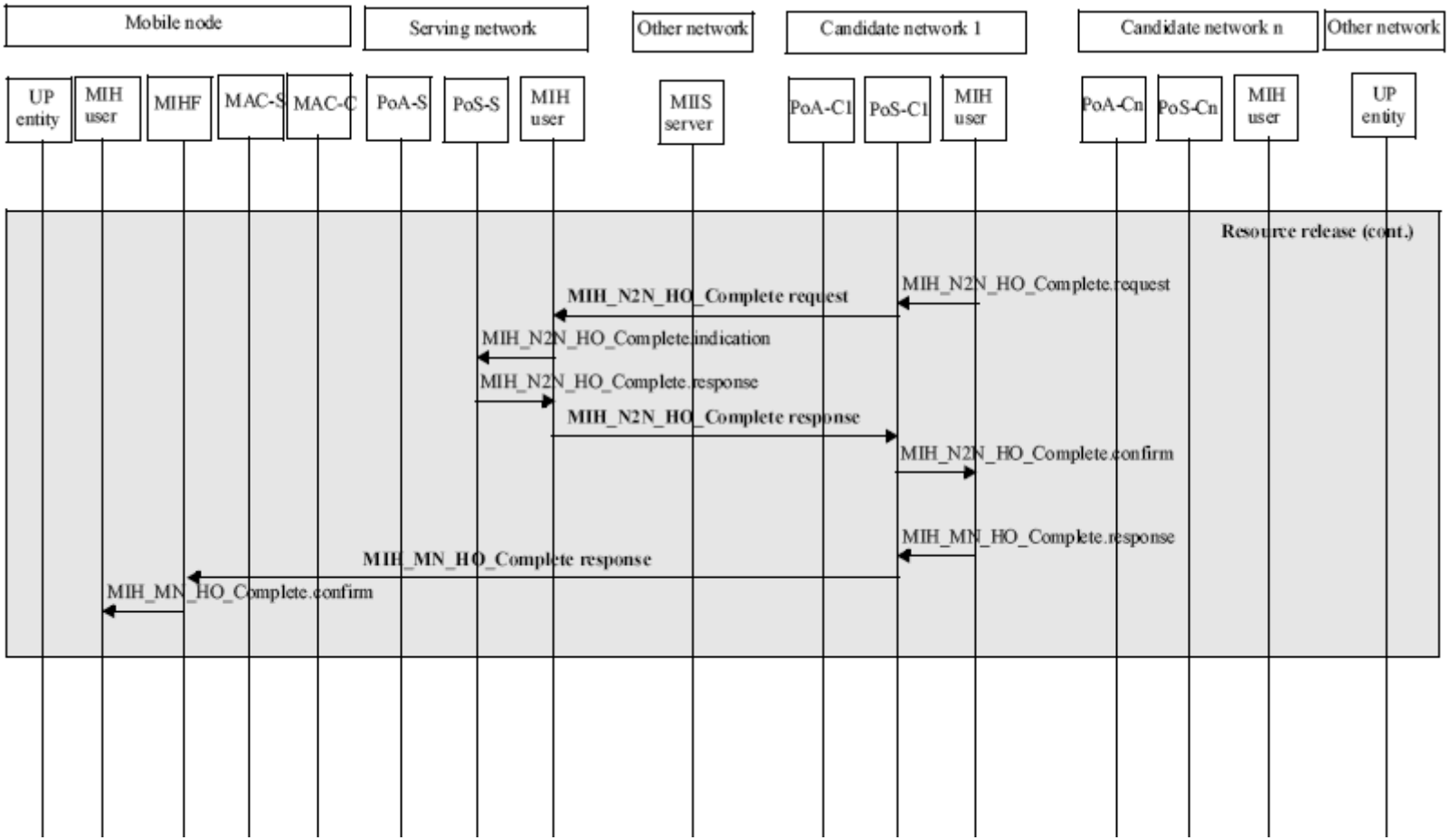


Figura 40: Mobile-initiated handover procedure (cont.)

B.2 Network-initiated handover procedure

The Network-initiated handover procedure operates as follows (see Figura 41, Figura 42, Figura 43, and Figura 44):

1) The Serving PoS sends an MIH_Get_Information request message to the Information Server to get neighboring network information and the Information Server responds by sending an MIH_Get_Information response message.

2) The Serving PoS triggers a network-initiated handover by sending an MIH_Net_HO_Candidate_Query request message to the Mobile Node. The MN responds through an MIH_Net_HO_Candidate_Query response message, which contains the Mobile Node's acknowledgement about the handover and its preferred link and PoS lists.

3) The Serving PoS sends an MIH_N2N_HO_Query_Resources request message to one or more Candidate PoSs to check the availability of the resource at candidate networks. The Candidate PoS responds by sending an MIH_N2N_HO_Query_Resources response message to the Serving PoS.

4) The Serving PoS decides the target of the handover based on the available resource status at candidate networks.

5) The Serving PoS sends an MIH_N2N_HO_Commit request message to the Target PoS to prepare resource at the target network. The Target PoS responds the result of the resource preparation by sending an MIH_N2N_HO_Commit response message.

6) After identifying that resource is successfully prepared, the Serving PoS commands the Mobile Node to commit handover towards the specified network type and PoA through an MIH_Net_HO_Commit request message.

7) The new layer 2 connection is established and the Mobile Node sends an MIH_Net_HO_Commit response message to the Serving PoS.

8) After higher layer handover execution, the Mobile Node sends an MIH_MN_HO_Complete request message to the Target PoS. The Target PoS sends an MIH_N2N_HO_Complete request message to the previous Serving PoS to release resource, which was allocated to the Mobile Node. After identifying that resource is successfully released, the Target PoS sends an MIH_MN_HO_Complete response message to the Mobile Node.

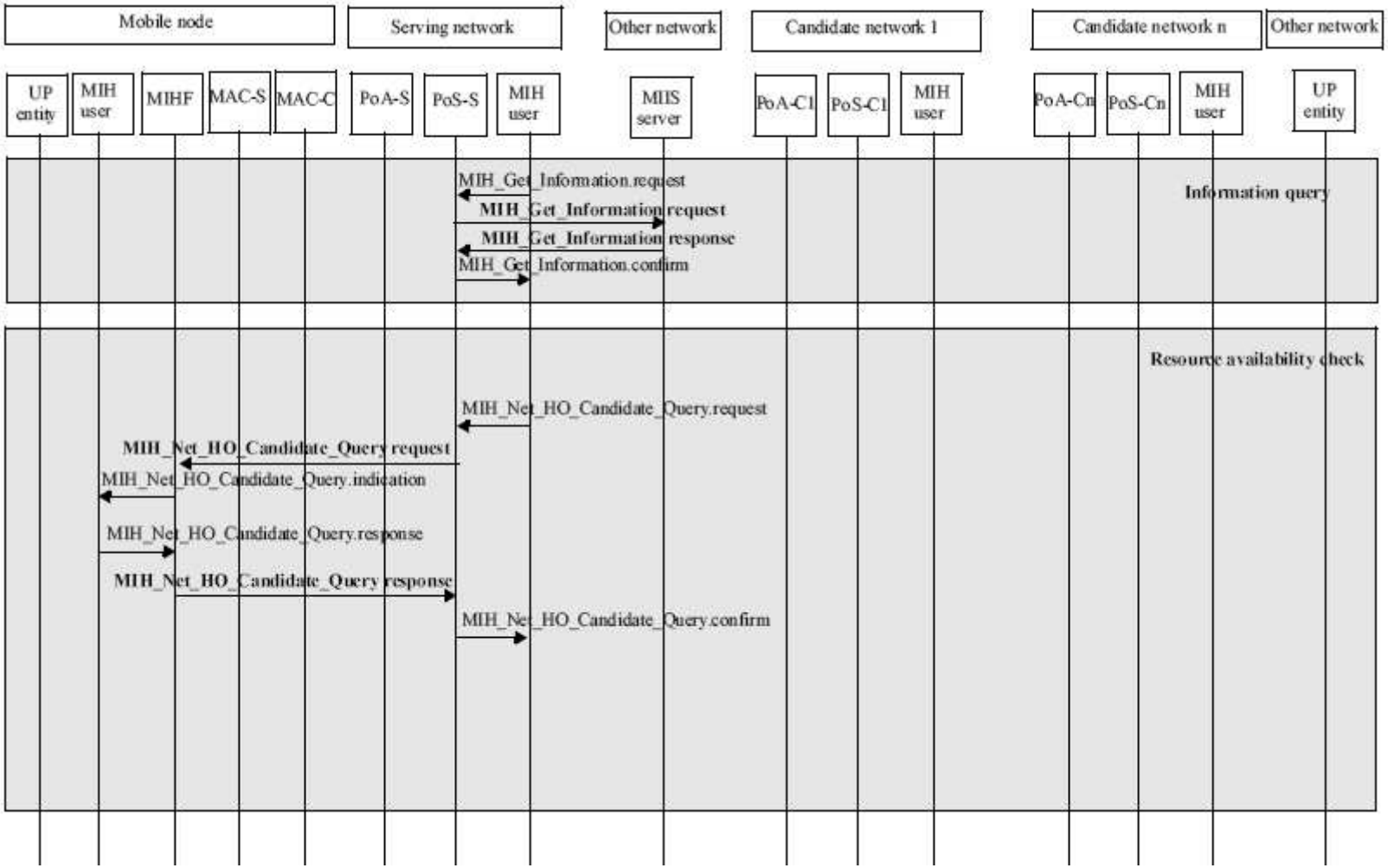


Figura 41: Network-initiated handover procedure

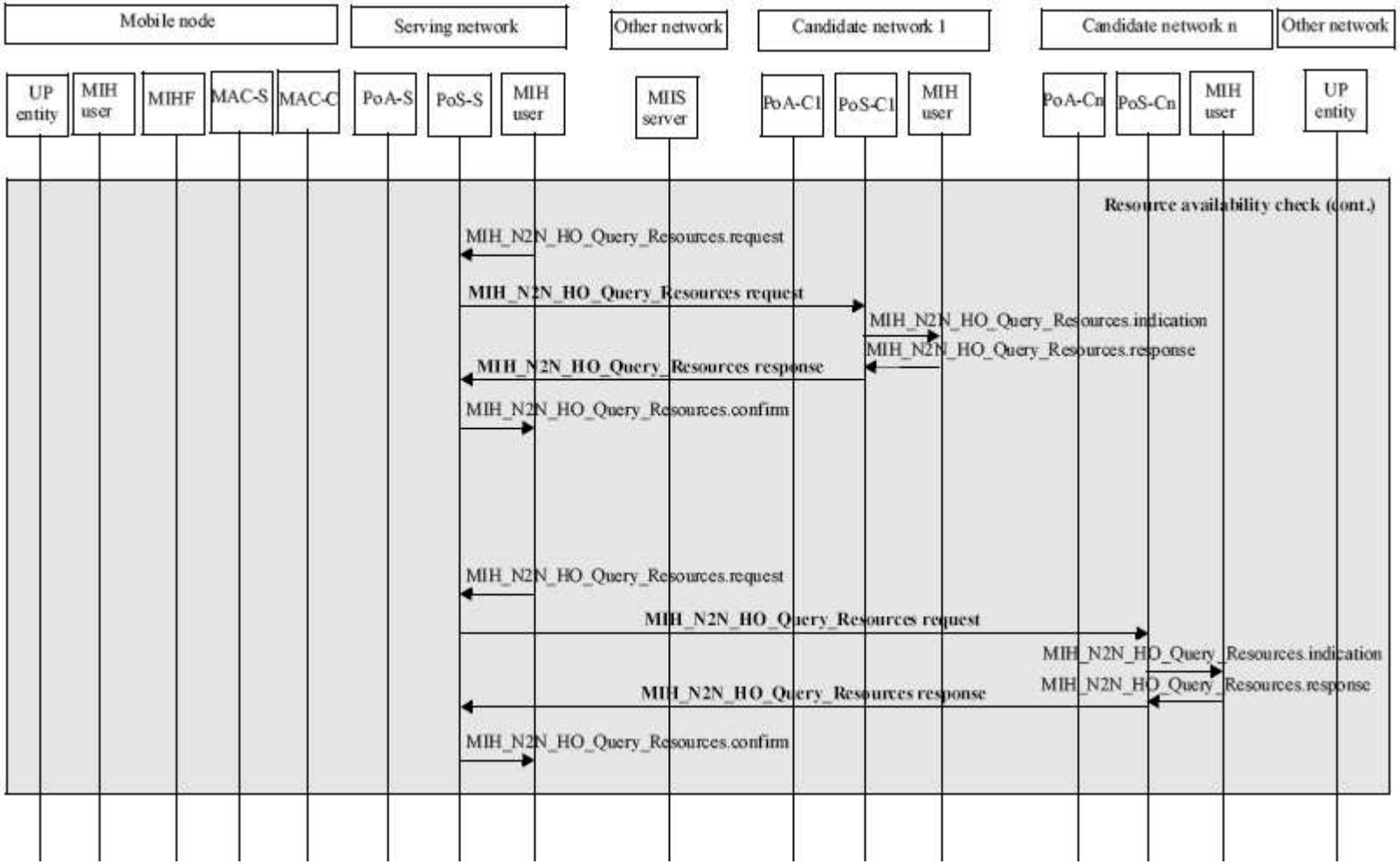


Figura 42: Network-initiated handover procedure (cont.)

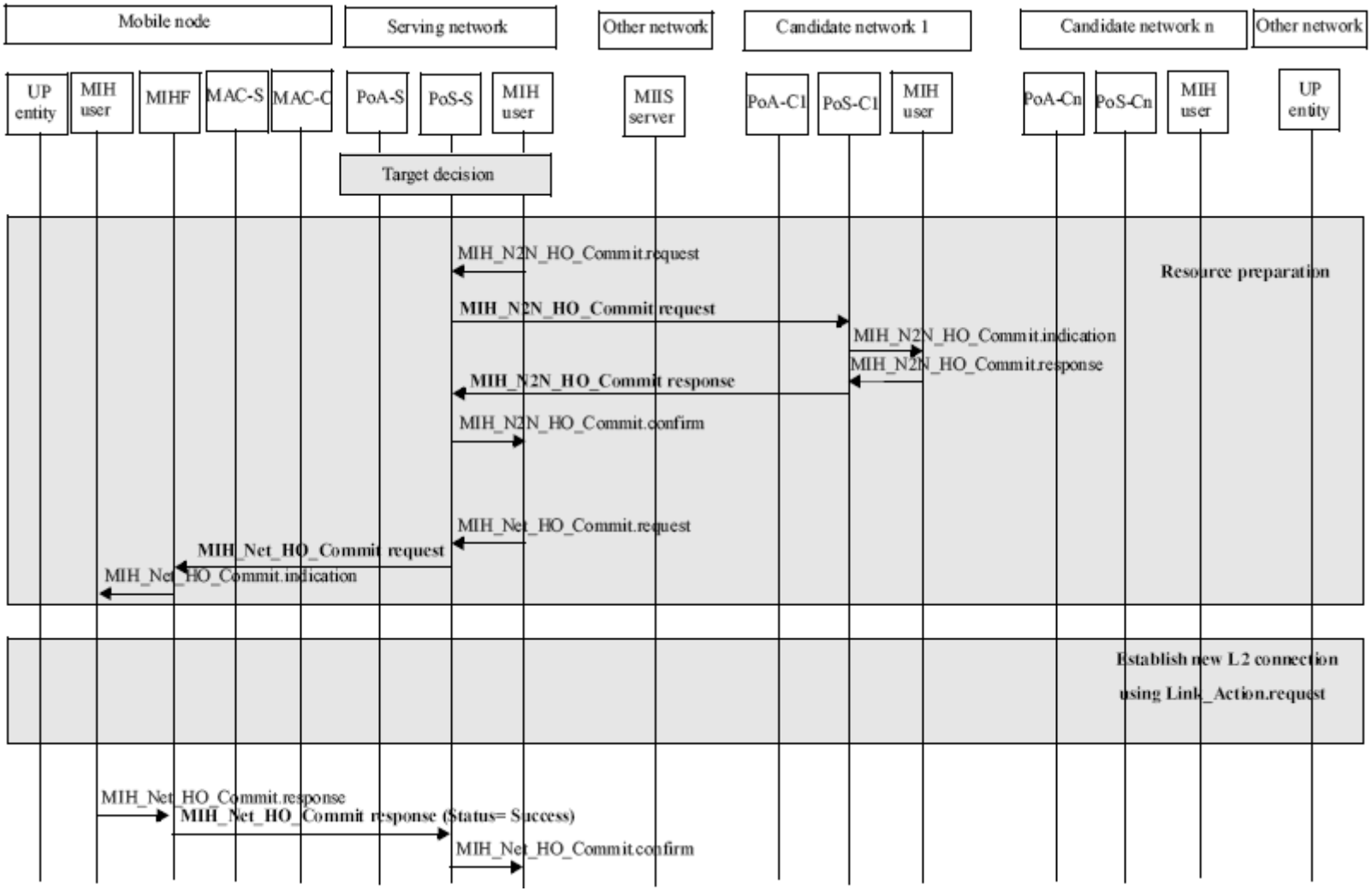


Figura 43: Network-inititated handover procedure (cont.)

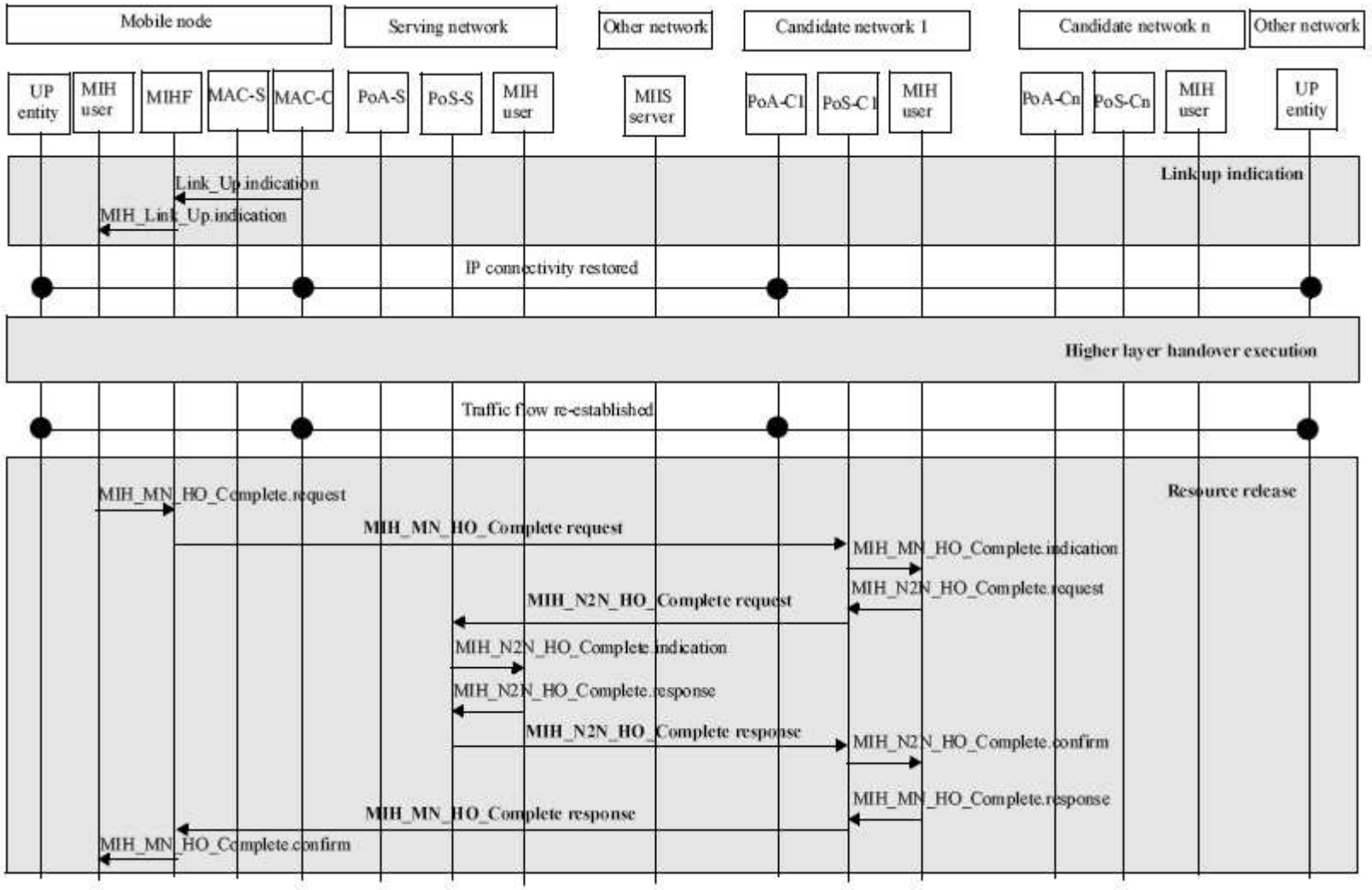


Figura 44: Network-inititated handover procedures (cont.)

B.3 Example handover flow chart between 802.11 and 802.16

Figura 45, Figura 46, Figura 47, and Figura 48 show a handover flow chart between the 802.11 the 802.16 network. This is an example of dual radio handover procedure wherein both the radios involved in handover can transmit and receive at the same time. The handover procedure operates as follows:

1) The Mobile Node is connected to the 802.11 network and receives the 802.11 link measurement through the MIH_Link_Parameters_Report.indication and acquires the neighboring network information the MIH_Get_Information.confirm.

2) When the Link_Going_Down event happens on the current 802.11 network, the Mobile Node performs the MIH_Link_Actions.request to scan the link status of the candidate networks. The mobile node discovers the 802.16 network and can acquire the candidate 802.16 network's DL_MAP, UL_MAP, DCD and parameters.

3) The Mobile Node identifies the resource availability status of the candidate network by sending MIH_MN_HO_Candidate_Query message to the Serving PoS. When the Serving PoS receives MIH_MN_HO_Candidate_Query request message from the Mobile Node, it retrieves resource information from target network by sending MIH_N2N_HO_Query_Resources message to the PoSs on the candidate networks.

4) Based on resource availability and other selection criteria the 802.16 network is selected as the target the handover and the Mobile Node sends MIH_MN_HO_Commit request message to the Serving PoS notify the decided target network information. The Serving PoS reserves the resource at the target network through MIH_N2N_HO_Commit messages.

5) The Mobile Node commits a link switch to the 802.16 interface and the new layer 2 connection for target 802.16 network is established. The Mobile IP procedures are carried out between the Mobile and the 802.16 network. As a result of that, the active sessions are now shifted over to the 802.16 network.

6) The Mobile Node sends the MIH_MN_HO_Complete request message to the Serving PoS on the 802.16 network and that Serving PoS exchanges the MIH_N2N_HO_Complete messages with the previous PoS the 802.11 network to release the resource that was reserved for the Mobile Node on that network.

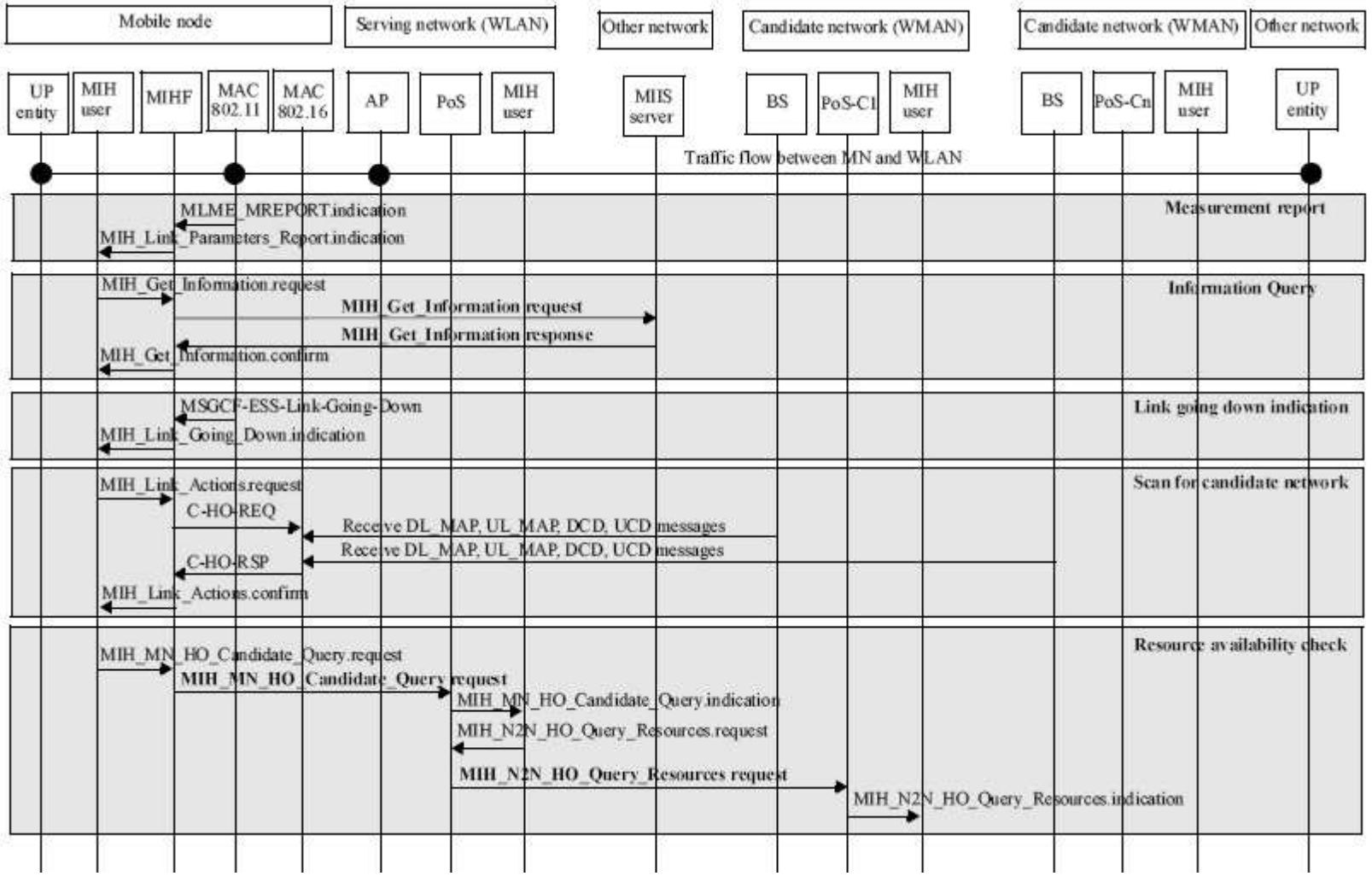


Figura 45: Example handover flow chart between 802.11 and 802.16

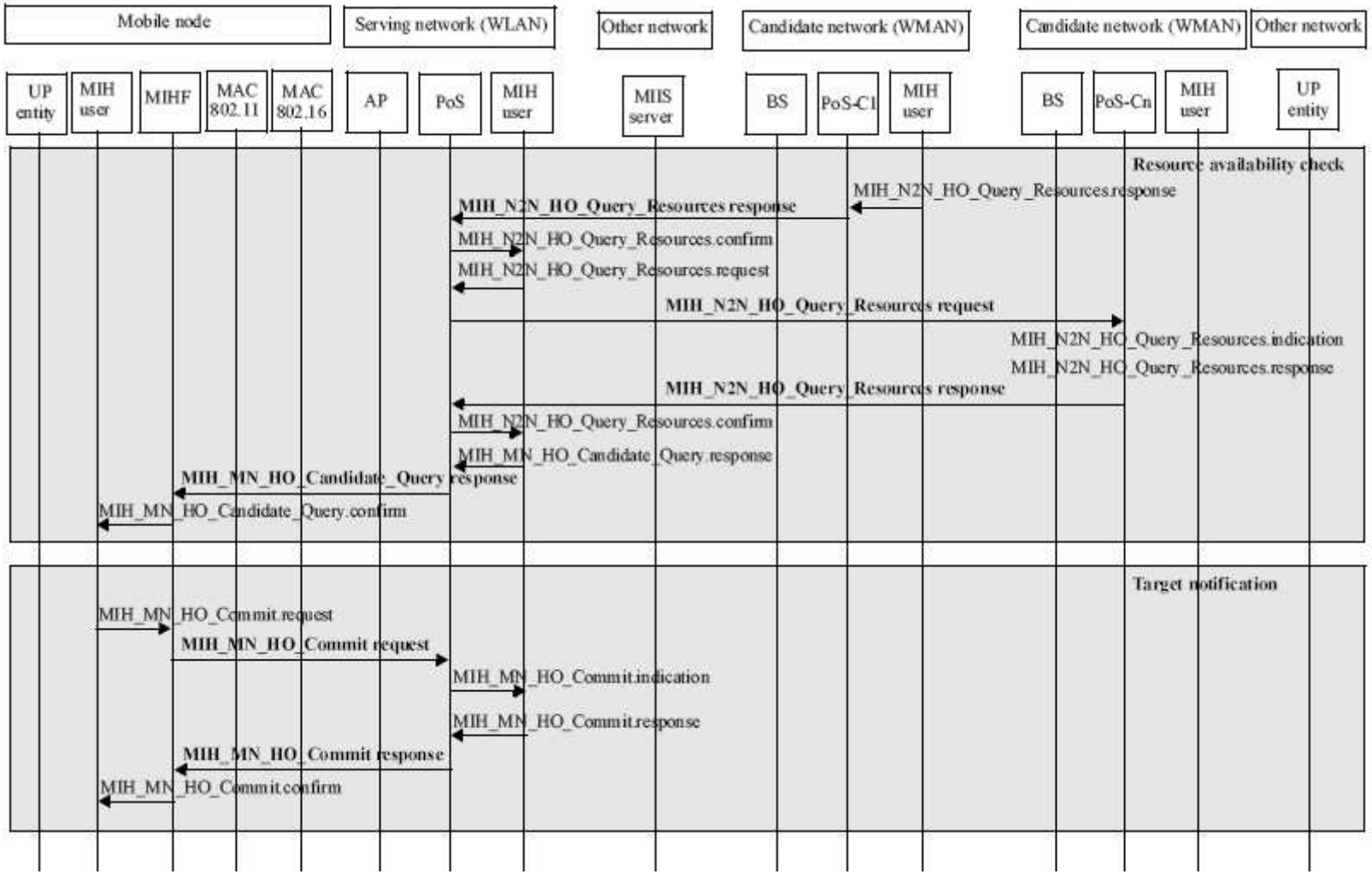


Figura 46: Example handover flow chart between 802.11 and 802.16 (cont.)

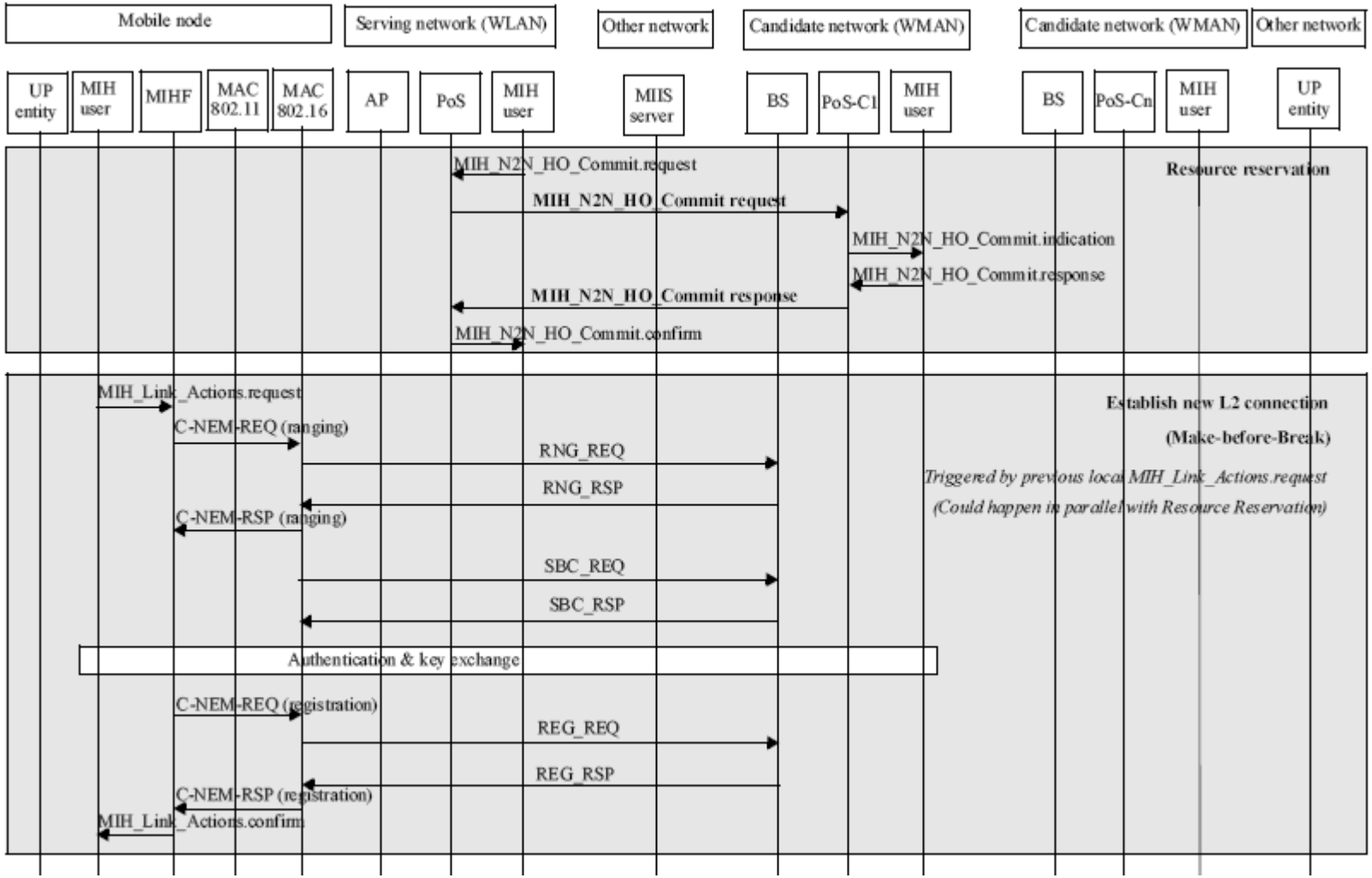


Figura 47: Example handover flow chart between 802.11 and 802.16 (cont.)

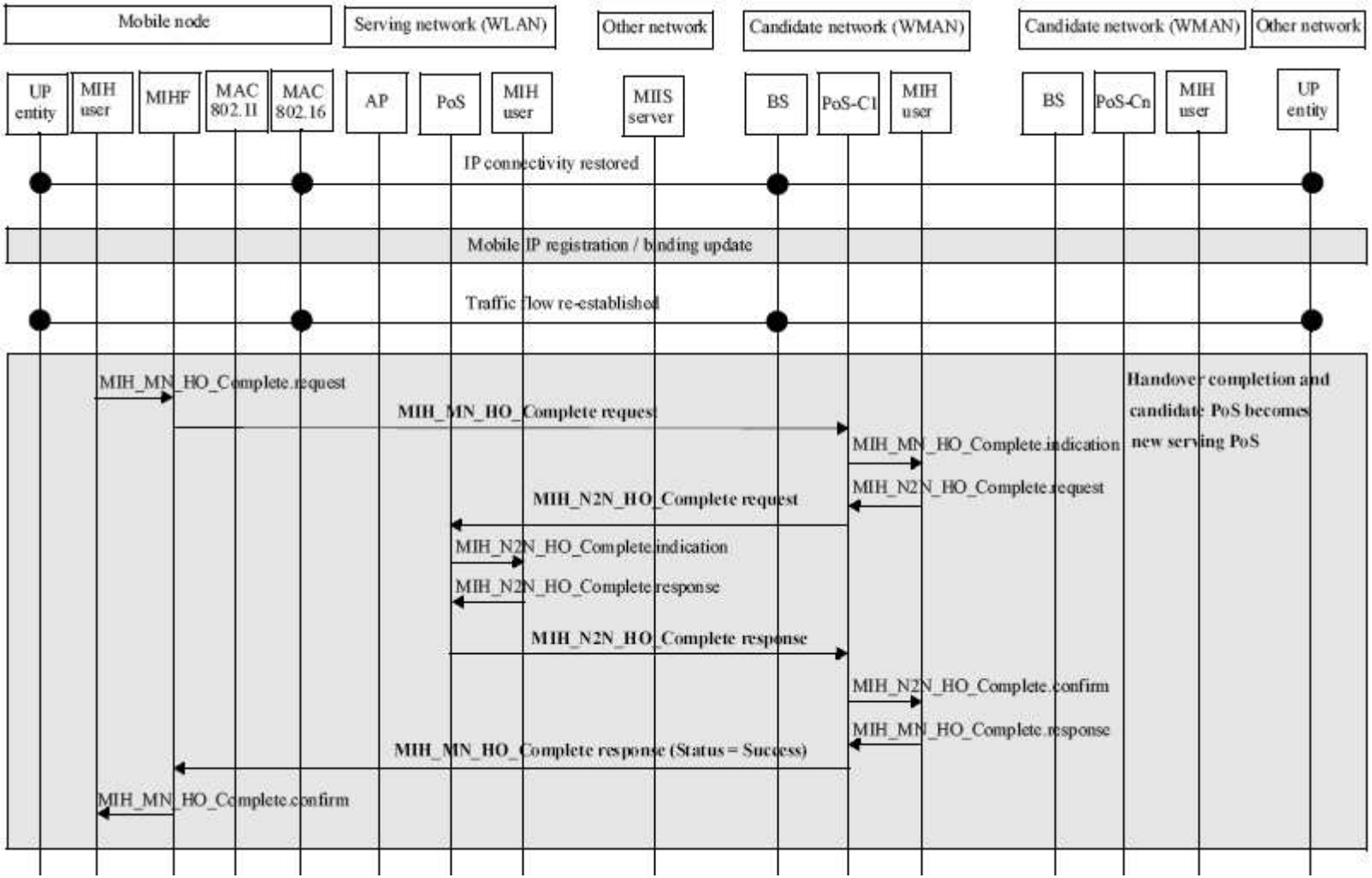


Figura 48: Example handover flow chart between 802.11 and 802.16 (cont.)

B.4 Example handover flow chart for Proxy Mobile IPv6

B.4.1 Network-initiated handover procedures

Figura 49 and Figura 50 show a network-initiated handover flow chart for Proxy Mobile IPv6 (PMIPv6), which is currently under standardization for supporting a local mobility in IETF NetLMM Working Group (Although the Proxy Mobile IP is under standardization, its overall flow is already defined. The following handover flow refers to the overall flow). The handover flow operates as follows:

1) The MN receives packets through both the Mobile Access Gateway (MAG) 1 located in the serving network and the Local Mobility Anchor (LMA), which are primary components of the PMIPv6.

2) The Serving PoS queries the Information Server to get information about available neighboring networks.

3) The Serving PoS triggers a network-initiated handover by sending the MIH_Net_HO_Candidate_Query request message to the MN. The MN responds with the MIH_Net_HO_Candidate_Query response message, which contains MN's acknowledgement about the handover initiation and its preferred link and PoS lists.

4) The Serving PoS sends the MIH_N2N_HO_Query_Resource request messages to different Candidate PoSs (can be more than one) to query the availability of the resource at candidate networks. The Candidate PoSs respond by sending the MIH_N2N_HO_Query_Resource response message to the Serving PoS. The Serving PoS decides on the handover target based on the resource availability information of candidate networks informed by the MIH_N2N_HO_Query_Resource response message.

5) The Serving PoS informs the decided Target PoS (i.e., Candidate Network 1 in the

6) Figura 49, where MAG2 is located) of the handover commitment and requests the Target PoS to prepare resources for the incoming MN through sending the MIH_N2N_HO_Commit request message. The Target PoS replies to the result of the handover commitment and resource preparation by sending an MIH_N2N_HO_Commit response message. (Upon receiving the MIH_N2N_HO_Commit request message, the PMIPv6 client in the Target PoS queries the incoming MN's profile to an AAA server and sends a Proxy Binding Update in order to register the location of the MN in advance. The PMIPv6 client in the Target PoS buffers the packets received from the LMA until the MN attaches to the Target PoS.)

7) The Serving PoS requests the MN to perform handover to the decided Target PoS by sending the MIH_Net_HO_Commit request message. The MN replies with the result of the handover commitment by sending an MIH_Net_HO_Commit response message.

8) Upon detecting the MN's detachment, the PMIPv6 client in the Serving PoS terminates its current binding of the MN via sending a Proxy Binding Update with Lifetime set to 0 and requests the LMA to buffer packets destined for the MN.

9) Once the MN establishes Layer 2 connection to the Target PoS, the PMIPv6 client in the Target PoS registers the current MN's location to the LMA by sending a Proxy Binding Update message. The LMA updates its Binding Cache Entry with the Proxy Binding Update message and then replies with a Proxy Binding Acknowledgement message. The LMA forwards the buffered packets.

10) After receiving the Proxy Binding Acknowledgement message, the PMIPv6 client sends a Router Advertisement message to the MN. The Router Advertisement is constructed with the MN's information obtained from the policy server and the LMA. It can be solicited by a Router Solicitation message from the MN or periodically transmitted. The MN configures IP addresses on its interface, which is currently used to connect to the Target PoS, with the received Router Advertisement message. Once the PMIPv6 procedures are completed, the MN receives packets through both MAG 2 and LMA.

11) After the PMIPv6 execution, the Target PoS sends the MIH_N2N_HO_Complete request message to the previous Serving PoS. The previous Serving PoS responds to the message with an MIH_N2N_HO_Complete response message.

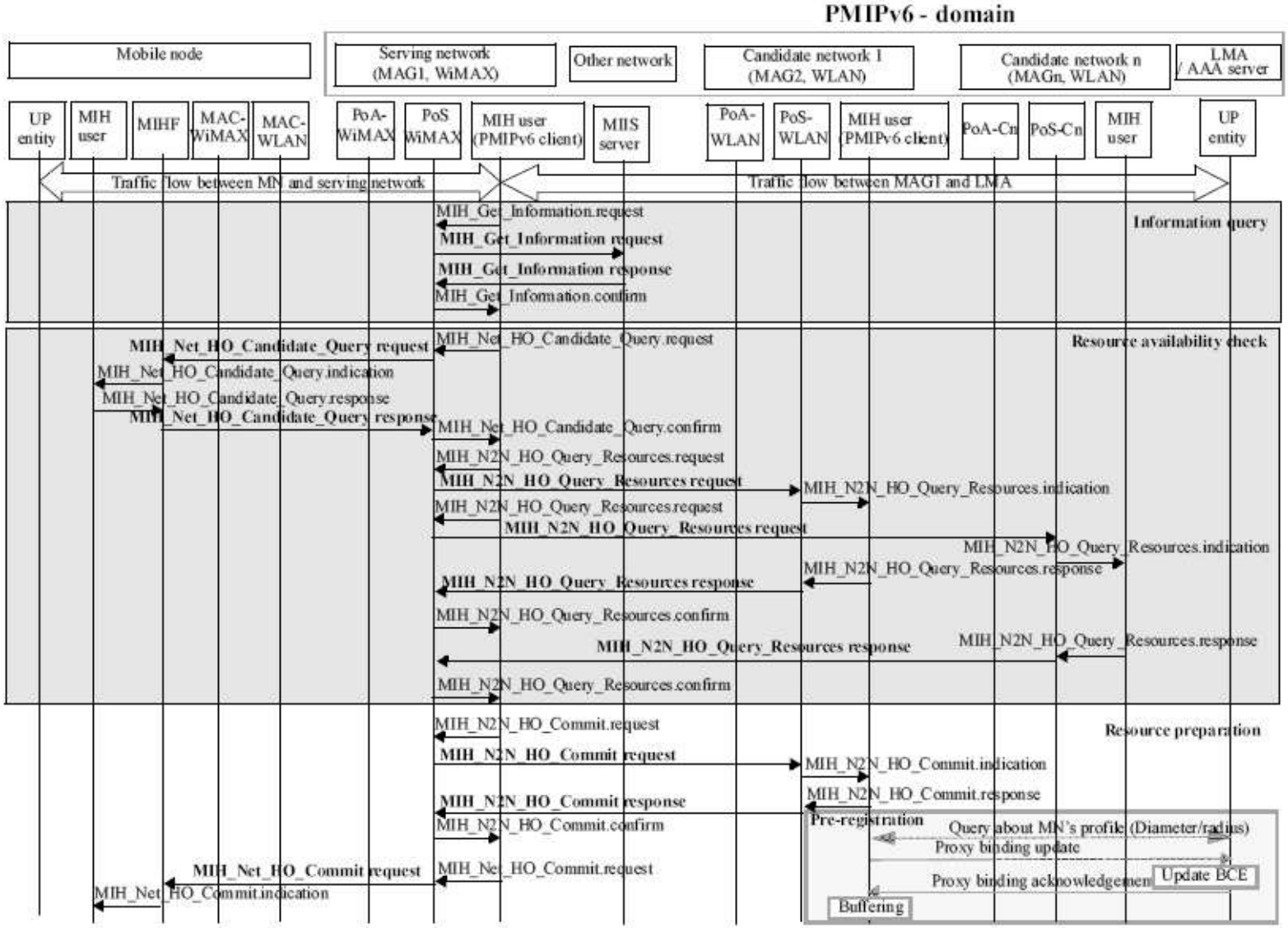


Figura 49: Network-initiated handover procedure. PMIPv6

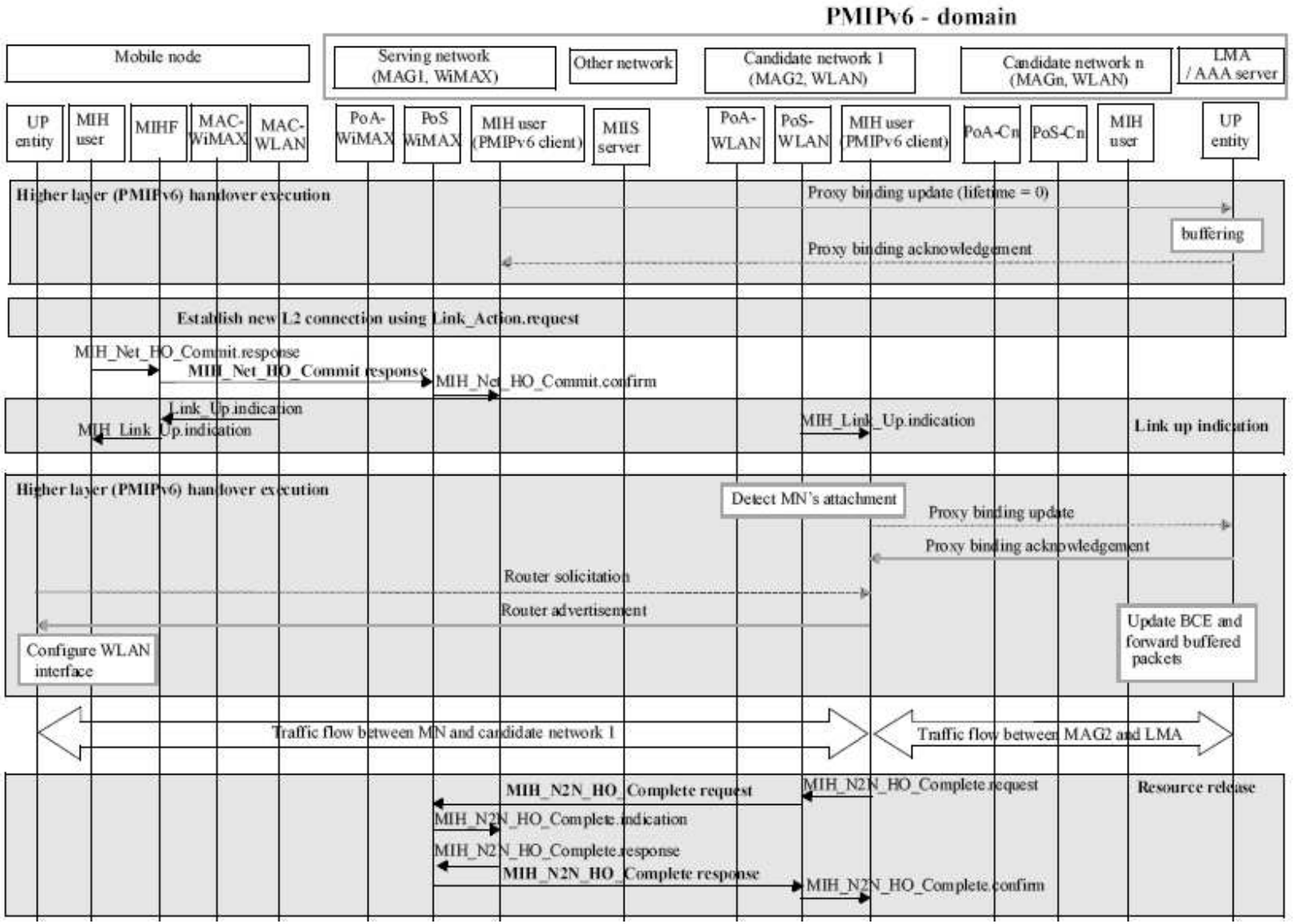


Figura 50: Network-initiated handover procedure. PMIPv6 (cont.)

B.4.2 Mobile-initiated handover procedures

Figura 51 and Figura 52 show a mobile-initiated handover flow chart for Proxy Mobile IPv6 (PMIPv6), which is currently under standardization for supporting a local mobility in IETF NetLMM Working Group (Although the Proxy Mobile IP is under standardization, its overall flow is already defined. Following handover flow refers to the overall flow). The handover flow operates as follows:

1) MN receives packets through both Mobile Access Gateway (MAG) 1 located in the serving network and Local Mobility Anchor (LMA), which are primary components of the PMIPv6.

2) The MN queries the Information Server to get information about available neighboring networks. This information query can be attempted as soon as the MN attaches to a new serving network or periodically for refreshing the information.

3) MN sends the MIH_MN_HO_Candidate_Query request message to the Serving PoS for triggering a mobile-initiated handover. This message contains requirements for potential candidate networks.

4) The Serving PoS sends the MIH_N2N_HO_Query_Resource request messages to the informed Candidate PoSs (can be more than one) in order to query the availability of the resource at the candidate networks. The Candidate PoS responds by sending the MIH_N2N_HO_Query_Resource response message to the Serving PoS. The Serving PoS in turn sends MIH_MN_HO_Candidate_Query response message to the MN. Finally, the MN decides the handover target based on the result of query about resource availability at the candidate networks.

5) The MN sends the MIH_MN_HO_Commit request message to notify the Serving PoS of the decided target network information. The Serving PoS reserves the resource at the target network through MIH_N2N_HO_Commit messages. Upon receiving the MIH_N2N_HO_Commit request message, PMIPv6 client as MIH User in the target PoS queries the incoming MN's profile to a policy store such as AAA server. As a result, the Target PoS obtains MN's information for PMIP processes in advance. (Upon receiving the MIH_N2N_HO_Commit request message, PMIPv6 client in the Target PoS queries the incoming MN's profile to an AAA server and sends Proxy Binding Update in order to register the location of the MN in advance. The PMIPv6 client in the Target PoS also buffers the packets received from LMA until the MN attaches to the Target PoS.)

6) The Target PoS replies to the Serving PoS with the result of the resource preparation by sending MIH_N2N_HO_Commit response message.

7) The MN performs handover to the specified network type and PoA by the MIH_Link_Actions.request primitive. Upon detecting MN's detachment, the PMIPv6 client in the Serving PoS terminates its current binding of the MN via sending Proxy Binding Update with Lifetime set to 0 and requests LMA to buffer packets destined for the MN.

8) Once the MN establishes the layer 2 connection to the Target PoS, PMIPv6 client as MIH User in the Target PoS registers the current MN's location to LMA by sending a Proxy Binding Update message. The LMA updates its Binding Cache Entry with the Proxy Binding Update message and then replies with Proxy Binding Acknowledgement message. The LMA also forwards the buffered packets.

9) After receiving the Proxy Binding Acknowledgement message, the PMIPv6 client sends a Router Advertisement message to the MN. The Router Advertisement is constructed with the MN's information obtained from the policy server and LMA. It can be solicited by a Router Solicitation message from the MN or periodically transmitted. MN configures IP addresses on its interface, which is currently used to connect to the Target PoS, with the received Router Advertisement message. Once the PMIPv6 procedures are completed, the MN receives packets through both MAG 2 and LMA

10) After the PMIPv6 execution, the Target PoS sends the MIH_N2N_HO_Complete request message to the previous Serving PoS. The previous Serving PoS responds to the message with an MIH_N2N_HO_Complete response message.

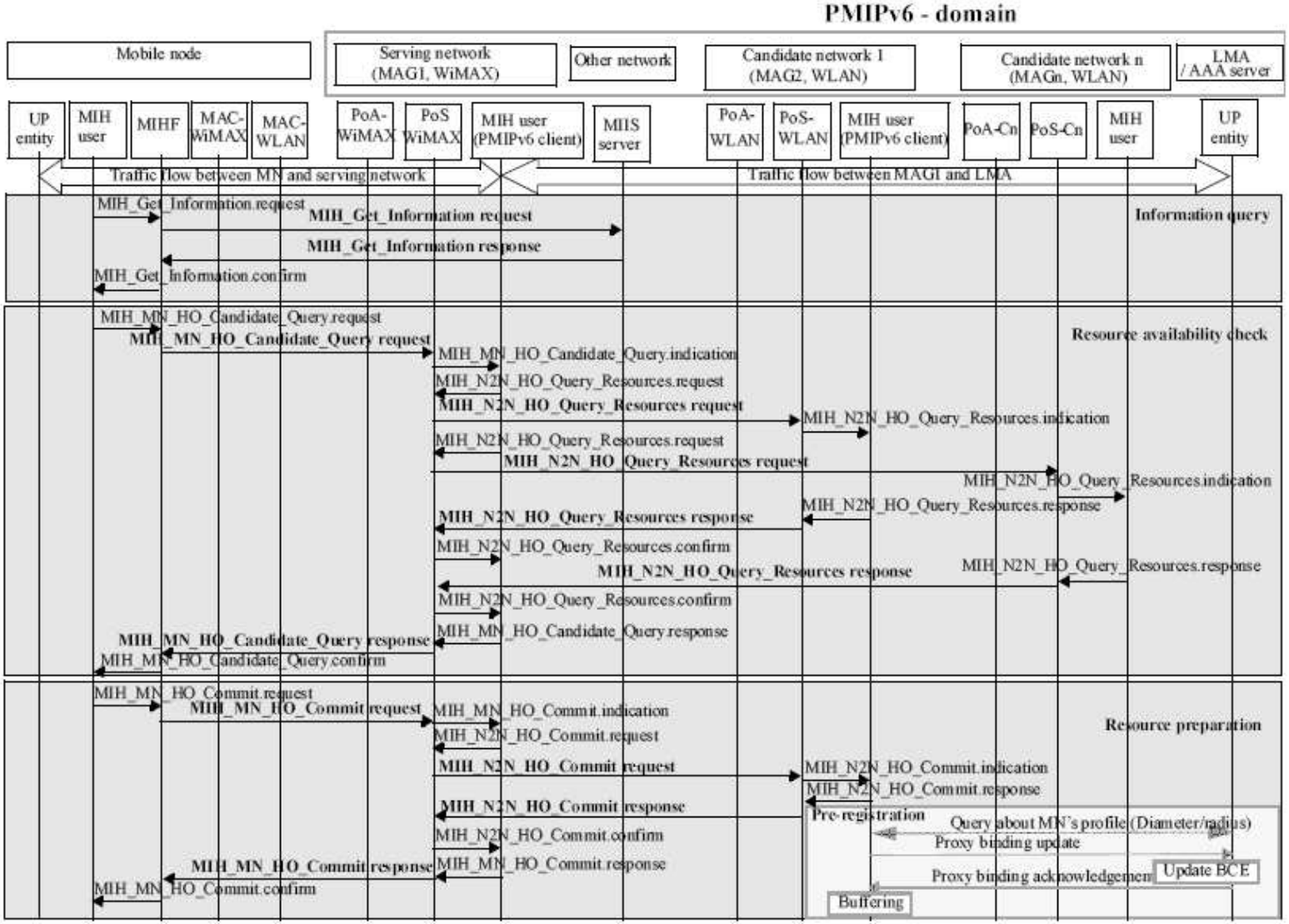


Figura 51: Mobile-initiated handover procedure. MIPv6

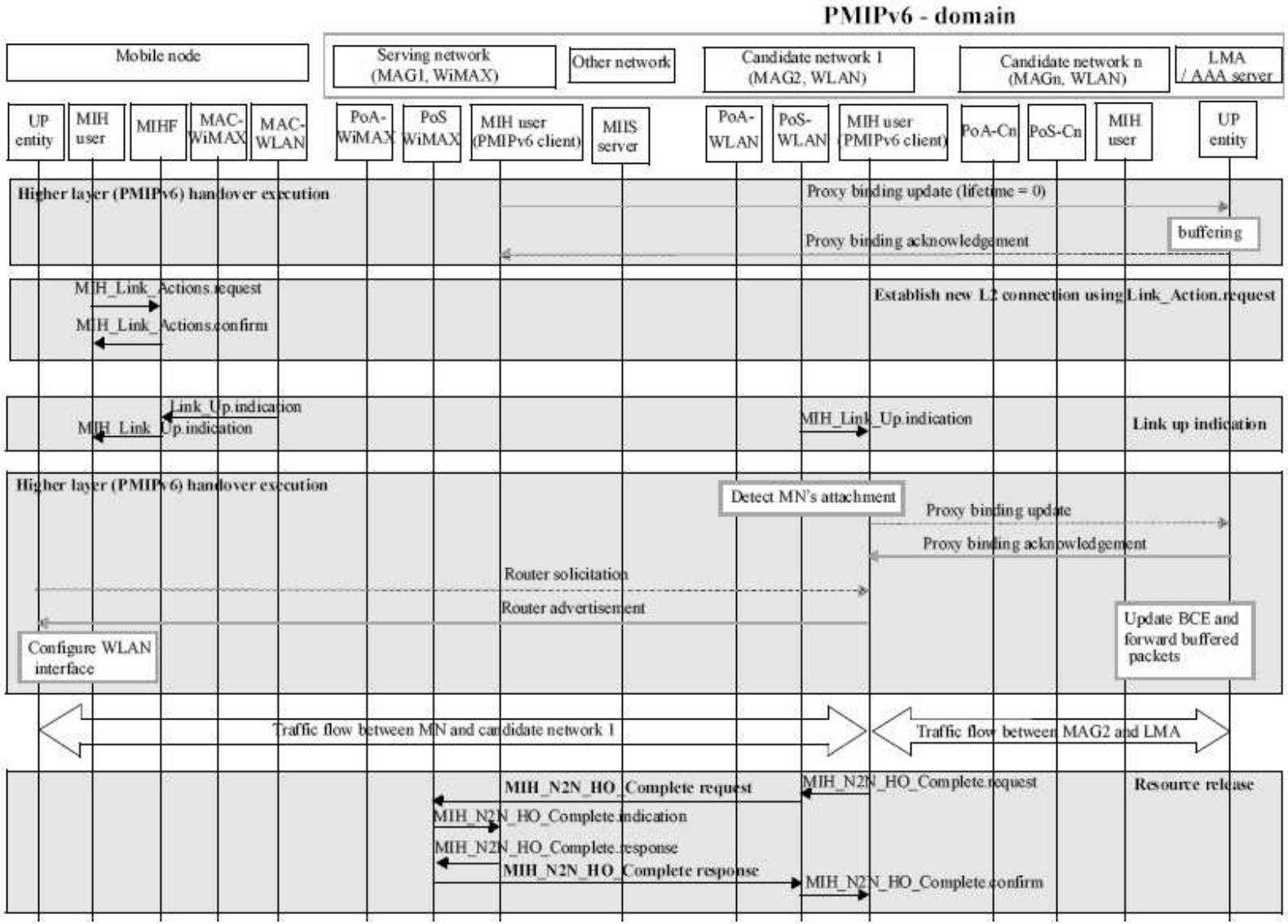


Figura 52: Mobile-initiated handover procedure. MIPv6 (cont.)

B.4.3 Mobile-initiated handover for break before make case

Figura 53 and Figura 54 show a mobile-initiated handover flow chart for Proxy Mobile IPv6 (PMIPv6). In this case the MN looses its connectivity with the serving PoA before the target PoA can be notified of the MN's decision to handover. However, the MN discovers the target PoA, establishes connectivity with the target PoA and then the target PoA notifies the serving PoA of the handover completion. PMIPv6 signaling is then completed and the packets are then forwarded to the MN's new location. The handover flow operates as follows:

1) The MN receives packets through both Mobile Access Gateway (MAG) 1 located in the serving network and Local Mobility Anchor (LMA), which are primary components of the PMIPv6.

2) The MN queries the Information Server to get information about available neighboring networks. This information query can be attempted as soon as the MN attaches to a new serving network or periodically for refreshing the information.

3) The MN sends the MIH_MN_HO_Candidate_Query request message to the Serving PoS for triggering a mobile-initiated handover. This message contains requirements for potential candidate networks.

4) The Serving PoS sends the MIH_N2N_HO_Query_Resource request messages to the informed Candidate PoSs (can be more than one) in order to query the availability of the resource at the candidate networks. The Candidate PoS responds by sending the MIH_N2N_HO_Query_Resource response message to the Serving PoS. The Serving PoS in turn sends MIH_MN_HO_Candidate_Query response message to the MN. Finally, the MN decides on the handover target based on the result of query about resource availability at the candidate networks.

5) The MN unexpectedly looses connectivity with the serving PoS. Upon detecting MN's detachment, PMIPv6 client in the Serving PoS terminates a current binding of the MN via sending a Proxy Binding Update with Lifetime set to 0 and requests the LMA to buffer packets destined for the MN.

6) The loss of the link connectivity triggers an MIH_Link_Down event on the MN. Later the MN receives an MIH_Link_Up event when the WLAN L2 connection is established.

7) Once the MN establishes the layer 2 connection to the Target PoS, the PMIPv6 client as an MIH User in the Target PoS registers the current MN's location to the LMA by sending a Proxy Binding Update message. The LMA updates its Binding Cache Entry with the Proxy Binding Update message and then replies with Proxy Binding Acknowledgement message.

8) After receiving the Proxy Binding Acknowledgement message, the PMIPv6 client sends a Router Advertisement message to the MN. The Router Advertisement is constructed with the MN's information obtained from the policy server and LMA. It can be solicited by a Router Solicitation message from the MN or periodically transmitted. The MN configures IP addresses

on its interface, which is currently used to connect to the Target PoS, with the received Router Advertisement message. Once the PMIPv6 procedures are completed, the MN receives packets through both MAG 2 and LMA.

9) After the PMIPv6 execution, the Target PoS sends the MIH_N2N_HO_Complete request message to the previous Serving PoS. The previous Serving PoS responds to the message with MIH_N2N_HO_Complete response message.

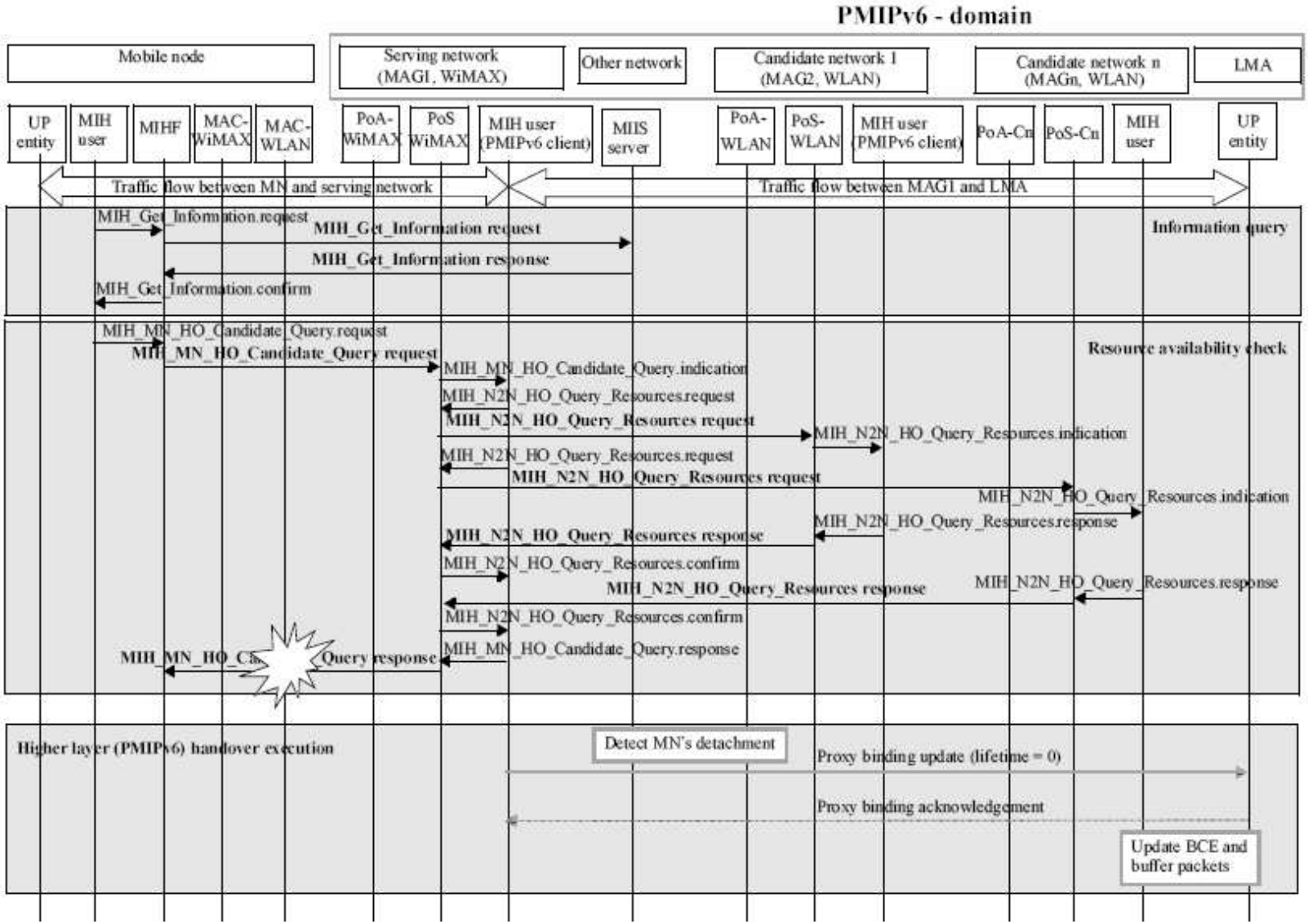


Figura 53: Mobile-initiated handover for break before make case

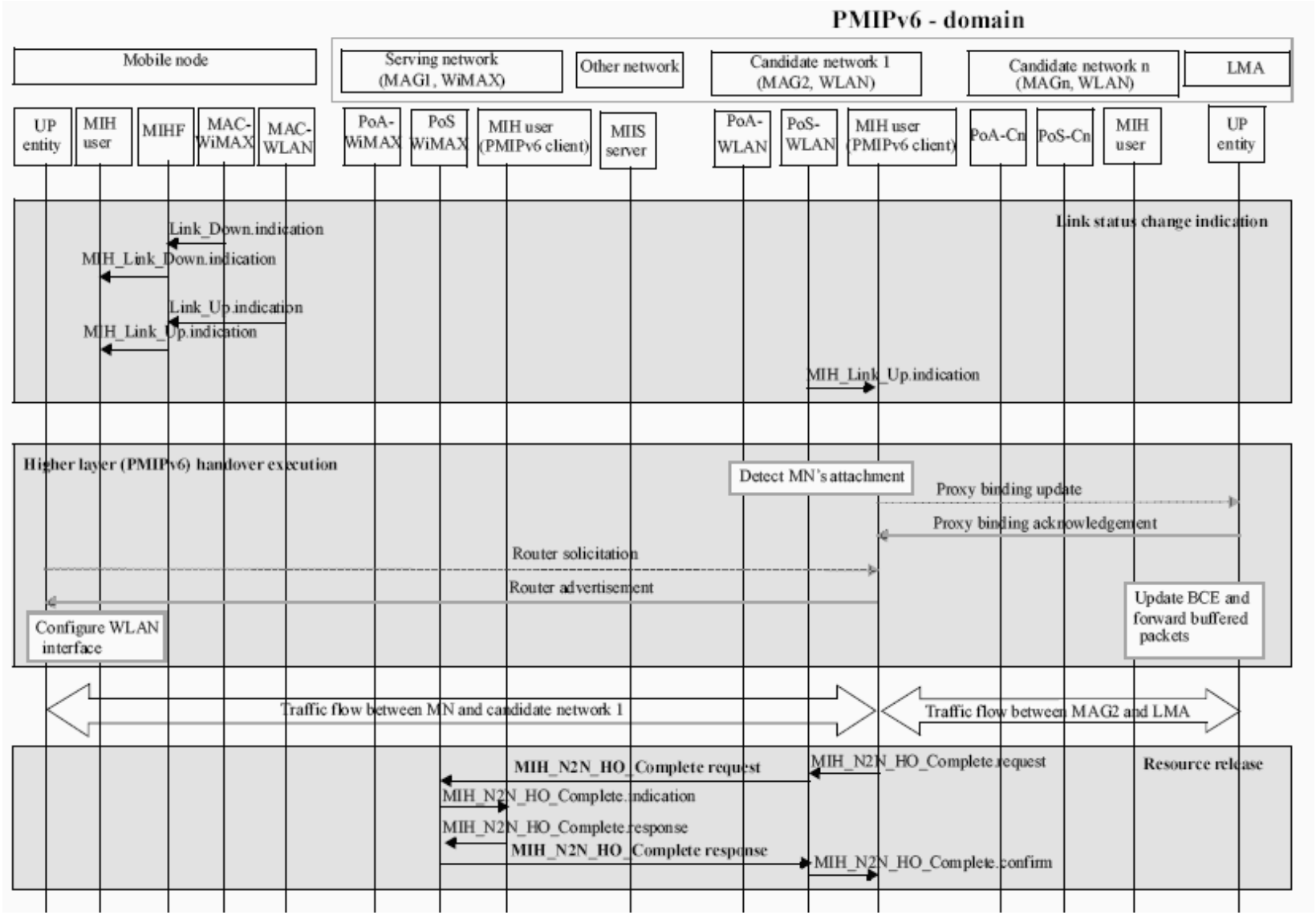


Figura 54: Mobile-initiated handover for break before make case (cont.)

B.5 Network selection in 802.11 (WLAN) using 802.21

Figura 55 shows the general topology of an 802.11 (WLAN) network operating with an 802.21 MIIS. The steps in network selection as shown in Figura 56 are as follows:

1) Pre-configuration: The AP is pre-configured with advertising protocol identifier (APID) of choice and is pre-configured to use 802.21 MIIS. The AP discovers the MIIS through a variety of different mechanisms that are outside the scope of specification. The maximum length of response messages from MIIS is also set. The AP communicates with MIIS at L2 or at L3 using a protocol defined elsewhere.

2) Discover AP/Access Network Capabilities: The AP sends out a beacon with Interworking set in the extended capabilities information element and APID set to GAS (Generic Advertisement Service). The STA discovers access network capabilities by listening to beacons or it could also send a probe request and discover access network capabilities through the probe response.

3) Query list of subscription service provider networks (SSPNs): The STA sends out a query asking for a list of available SSPNs. The query is defined using an 802.21 specific MIH frame. The MIH frame is then relayed by the AP to the MIIS. Meanwhile the AP sends out the initial GAS response to the STA with initial delay (comeback delay).

4) GAS response: The MIIS interprets the query and retrieves the response either from local or remote repository. It then packs the response in an appropriate MIH frame and sends it to the AP. Subsequently when the STA sends the GAS comeback request to the AP, the AP responds with the available information in the MIH frame. The STA then retrieves the information out of the MIH frame and obtains the answer to the query.

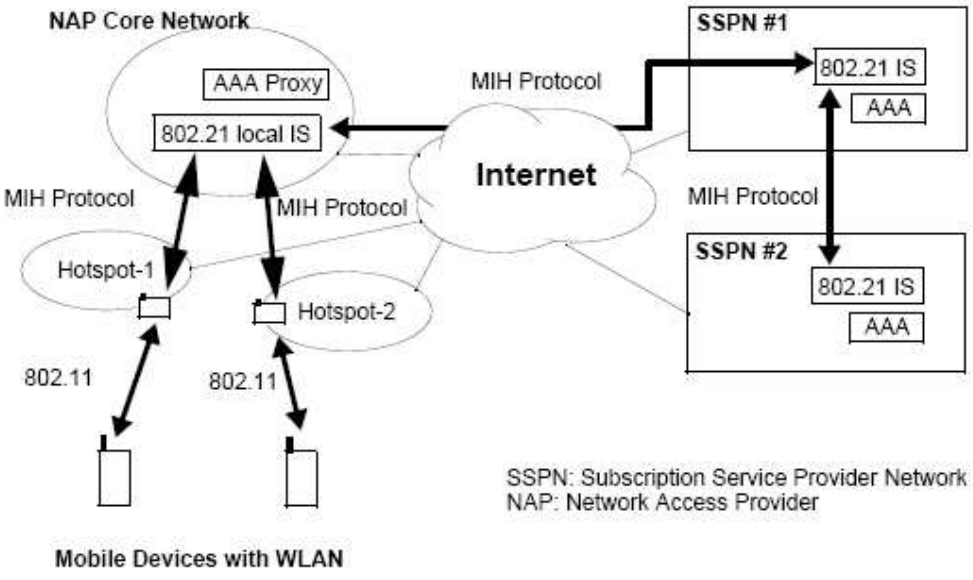


Figura 55: Network selection in WLAN with 802.11 and 802.21

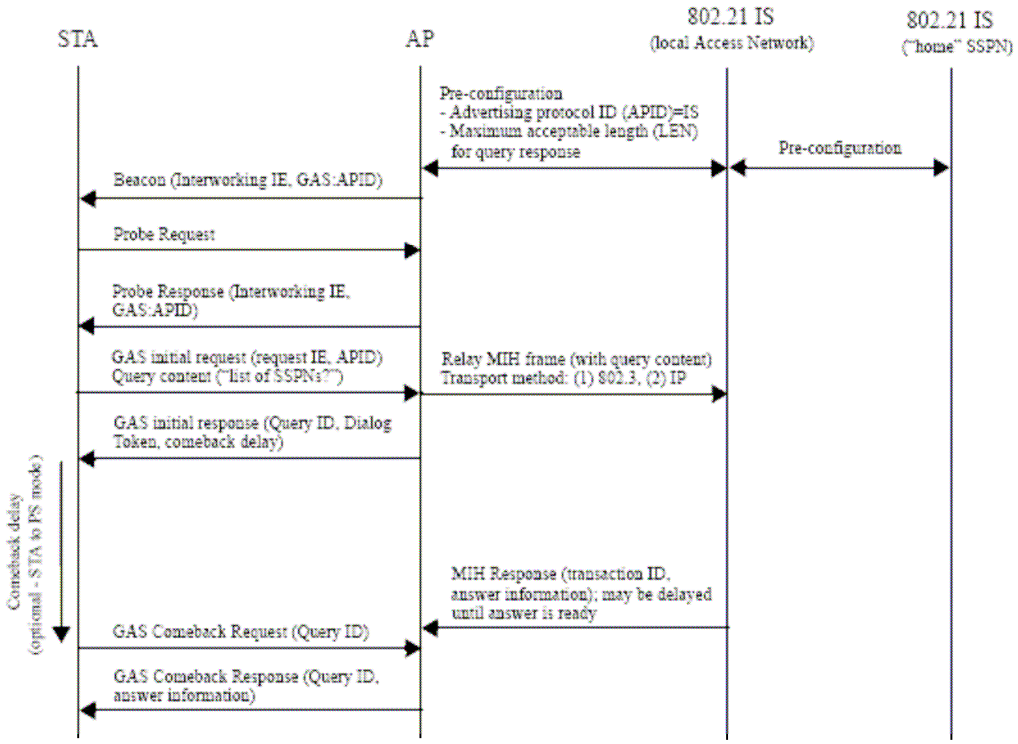


Figura 56: Use case: query SSPN list

Listado de acrónimos y abreviaturas

2G	Second Generation
3G	Third Generation
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
A4C	Authentication, Authorization, Accounting, Auditing, Charging
AAA	Authentication, Authorization, and Accounting
ANDSF	Access Network Discovery and Selection Function
BCP	Business Continuity Plan
BSS	Business Support System
C_SAP	Control Service Access Point
CoS	Class of Service
DAD	Duplicate Address Detection
DAIDALOS	Daidalos: Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimized personal Services
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DNA	Detection Network Attachment
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DSLAM	Digital Subscriber Line Access Multiplexer
DSMIP	Dual Stack Mobile IP
E-UTRAN	Evolved UTRAN
EPC	Evolved Packet Core
ESS	Extended Service Set
FMC	Fixed-Mobile Convergence
FMCA	Fixed-Mobile Convergence Alliance
FMIPv6	Fast Handovers for Mobile IPv6
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communication
HA	Home Agent
HIP	Host Identity Protocol
HMIPv6	Hierarchical Mobile IPv6
HSDPA	High-Speed Downlink Packet Access
HSPA	High Speed Packet Access

IANA	Internet Assignment Numbers Authority
ICE	Interactive Connectivity Establishment
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	IP Television
IS	Information Server
ITU-T	International Telecommunication Union-Telecommunication
L2	Layer 2 (MAC and or LLC)
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LMA	Local Mobility Anchor
LSAP	Logical link control Service Access Point
LTE	Long Term Evolution
M_SAP	Management Service Access Point
MAC	Medium Access Control
MAG	Mobile Access Gateway
MARQS	Mobility Management, AAA, Resource Management, QoS and Security
MEGACO	Media Gateway Control Protocol
MEXT	Mobility Extensions for IPv6
MIB	Management Information Base
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MIP4	Mobility for IPv4
MIP6	Mobility for IPv6
MIPSHOP	Mobility for IP:Performance, Signaling and Handoff Optimization
MLME	MAC Layer Management Entity
MME	Mobility Management Entity
MN	Mobile Node
MNO	Mobile Network Operator
MR	Mobile Router
MSGCF	MAC State Generic Convergence Function
NAT	Network Address Translation
NCMS	Network Control and Management System

NEMO	Network Mobility
NETLMM	Network-based Localized Mobility Management
NGN	Next Generation Network
OSS	Operational Support System
PDA	Personal Digital Assistant
PHY	Physical Layer
PLME	Physical Layer Management Entity
PMIPv6	Proxy Mobile IPv6
PoA	Point of Attachment
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
RTP	Real-time Transport Protocol
RTSP	Real-time Streaming Protocol
SAP	Service Access Point
SDP	Session Description Protocol
SDU	Service Data Unit
SeND	Secure Neighbor Discovery
SIB	Seamless Integration of Broadcast
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SME	Station Management Entity
SMIv2	Structure of Management Information version 2
SOAP	Simple Object Access Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication Service
UTRAN	UMTS Terrestrial Radio Access Network
USP	Ubiquitous and Seamless Pervasiveness
VID	Virtual Identity
VNO	Virtual Network Operator
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group
WLAN	Wireless Local Area Network
XML	eXtensible Mark-up Language

Referencias

[1] Wikipedia, Redes de Siguiente Generación, http://es.wikipedia.org/wiki/Red_de_siguiente_generaci%C3%B3n

[2] Carlos J. Bernardos, Ignacio Soto and María Calderón, "IPv6 Network Mobility", http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_102/102_ipv6.html

[3] Detecting Network Attachment (DNA) Working Group, http://www.ietf.org/html.charters/dna-charter.html

[4] DNA Working Group, "Tentative Options for Link-Layer Addresses in IPv6 Neighbour Discovery" http://www.ietf.org/internet-drafts/draft-ietf-dna-tentative-02.txt

[5] DNA Working Group, "Simple procedures for Detecting Network Attachment in IPv6" http://www.ietf.org/internet-drafts/draft-ietf-dna-simple-06.txt

[6] DNA Working Group, "Goals of Detecting Network Attachment in IPv6" http://www.ietf.org/rfc/rfc4135.txt

[7] DNA Working Group, "Link-layer Event Notifications for Detecting Network Attachments" http://www.ietf.org/rfc/rfc4957.txt

[8] Mobility for IPv4 (MIP4) Working Group, http://www.ietf.org/html.charters/mip4-charter.html

[9] MIP4 Working Group, "The Definitions of Managed Objects for IP Mobility Support using SMIv2, revised "http://www.ietf.org/internet-drafts/draft-ietf-mip4-rfc2006bis-06.txt

[10] MIP4 Working Group, "Generic Notification Message for Mobile IPv4" http://www.ietf.org/internet-drafts/draft-ietf-mip4-generic-notification-message-08.txt

[11] MIP4 Working Group, "The Definitions of Managed Objects for Mobile IP UDP Tunneling" http://www.ietf.org/internet-drafts/draft-ietf-mip4-udptunnel-mib-02.txt

[12] MIP4 Working Group, "Mobile IPv4 Extension for AAA Network Access Identifiers" http://www.ietf.org/rfc/rfc3846.txt

[13] MIP4 Working Group, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4"http://www.ietf.org/rfc/rfc3957.txt

[14] MIP4 Working Group, "Experimental Message, Extension and Error Codes for Mobile IPv4" http://www.ietf.org/rfc/rfc4064.txt

[15] MIP4 Working Group, "Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways" http://www.ietf.org/rfc/rfc4093.txt

[16] MIP4 Working Group, "Mobile IPv4 Dynamic Home Agent Assignment" http://www.ietf.org/rfc/rfc4433.txt

[17] MIP4 Working Group, "Foreign Agent Error Extension for Mobile IPv4" http://www.ietf.org/rfc/rfc4636.txt

[18] MIP4 Working Group, “Mobile IPv4 Challenge/Response Extensions” http://www.ietf.org/rfc/rfc4721.txt

[19] MIP4 Working Group, “Mobile IPv4 Regional Registration” http://www.ietf.org/rfc/rfc4857.txt

[20] MIP4 Working Group, “Mobile IPv4 Message String Extension” http://www.ietf.org/rfc/rfc4917.txt

[21] MIP4 Working Group, “Low-Latency Handoffs in Mobile IPv4” http://www.ietf.org/rfc/rfc4881.txt

[22] MIP4 Working Group, “Mobile IPv4 RADIUS requirements” http://www.ietf.org/rfc/rfc5030.txt

[23] MIP4 Working Group, “Mobile IPv4 Fast Handovers” http://www.ietf.org/rfc/rfc4988.txt

[24] MIP4 Working Group, “Network Mobility (NEMO) Extensions for Mobile IPv4” http://www.ietf.org/rfc/rfc5177.txt

[25] MIP4 Working Group, “Mobile IPv4 Traversal across IPsec-Based VPN Gateways” http://www.ietf.org/rfc/rfc5265.txt

[26] MIP4 Working Group, “Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)” http://www.ietf.org/rfc/rfc5266.txt

[27] MIP4 Working Group, “Dual-Stack Mobile IPv4” http://www.ietf.org/rfc/rfc5454.txt

[28] Mobility for IPv6 (MIP6) Working Group, http://www.ietf.org/html.charters/OLD/mip6-charter.html

[29] MIP6 Working Group, “Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents” http://www.ietf.org/rfc/rfc3776.txt

[30] MIP6 Working Group, “Mobility Support in IPv6” http://www.ietf.org/rfc/rfc3775.txt

[31] MIP6 Working Group, “Mobile Node Identifier Option for Mobile IPv6 (MIPv6)” http://www.ietf.org/rfc/rfc4283.txt

[32] MIP6 Working Group, “Mobile IP version 6 Route Optimization Security Design Background” http://www.ietf.org/rfc/rfc4225.txt

[33] MIP6 Working Group, “Authentication Protocol for Mobile IPv6” http://www.ietf.org/rfc/rfc4285.txt

[34] MIP6 Working Group, “Mobile IPv6 Management Information Base” http://www.ietf.org/rfc/rfc4295.txt

[35] MIP6 Working Group, “Mobile IPv6 and Firewalls: Problem Statement” http://www.ietf.org/rfc/rfc4487.txt

[36] MIP6 Working Group, “Securing Mobile IPv6 Route Optimization Using a Static Shared Key” http://www.ietf.org/rfc/rfc4449.txt

[37] MIP6 Working Group, “Extension to Sockets API for Mobile IPv6” http://www.ietf.org/rfc/rfc4584.txt

[38] MIP6 Working Group, “Problem Statement for bootstrapping Mobile IPv6” http://www.ietf.org/rfc/rfc4640.txt

[39] MIP6 Working Group, “Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture” http://www.ietf.org/rfc/rfc4877.txt

[40] MIP6 Working Group, “IP Address Location Privacy and Mobile IPv6: Problem Statement” http://www.ietf.org/rfc/rfc4882.txt

[41] MIP6 Working Group, “Problem Statement: Dual Stack Mobility” http://www.ietf.org/rfc/rfc4977.txt

[42] MIP6 Working Group, “Mobile IPv6 bootstrapping in split scenario” http://www.ietf.org/rfc/rfc5026.txt

[43] MIP6 Working Group, “Mobile IPv6 Experimental Messages” http://www.ietf.org/rfc/rfc5096.txt

[44] MIP6 Working Group, “Mobile IPv6 Vendor Specific Option” http://www.ietf.org/rfc/rfc5094.txt

[45] Mobility for IP: Performance, Signaling and Handoff Optimization (MIPSHOP) Working Group, http://www.ietf.org/html.charters/mipshop-charter.html

[46] MIPSHOP Working Group, “IEEE 802.21 Mobility Services Framework Design (MSFD)” http://www.ietf.org/internet-drafts/draft-ietf-mipshop-mstp-solution-12.txt

[47] MIPSHOP Working Group, “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Services (MoS) Discovery” http://www.ietf.org/internet-drafts/draft-ietf-mipshop-mos-dhcp-options-14.txt

[48] MIPSHOP Working Group, “Locating IEEE 802.21 Mobility Servers using DNS” http://www.ietf.org/internet-drafts/draft-ietf-mipshop-mos-dns-discovery-05.txt

[49] MIPSHOP Working Group, “Fast Handovers for Proxy Mobile IPv6” http://www.ietf.org/internet-drafts/draft-ietf-mipshop-pfmipv6-04.txt

[50] MIPSHOP Working Group, “Transient Binding for Proxy Mobile IPv6” http://www.ietf.org/internet-drafts/draft-ietf-mipshop-transient-bce-pmipv6-02.txt

[51] MIPSHOP Working Group, “Mobile IPv6 Fast Handovers” http://www.ietf.org/internet-drafts/draft-ietf-mipshop-rfc5268bis-01.txt

[52] MIPSHOP Working Group, “Mobile IPv6 Fast Handovers for 802.11 Networks” http://www.ietf.org/rfc/rfc4260.txt

[53] MIPSHOP Working Group, “Enhanced Route Optimization for Mobile IPv6” http://www.ietf.org/rfc/rfc4866.txt

[54] MIPSHOP Working Group, “Mobility Services Transport: Problem Statement” http://www.ietf.org/rfc/rfc5164.txt

[55] MIPSHOP Working Group, “Mobile IPv6 Fast Handovers over IEEE 802.16e Networks” http://www.ietf.org/rfc/rfc5270.txt

[56] MIPSHOP Working Group, “Mobile IPv6 Fast Handovers for 3G CDMA Networks” http://www.ietf.org/rfc/rfc5271.txt

[57] MIPSHOP Working Group, “Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND) ” http://www.ietf.org/rfc/rfc5269.txt

[58] MIPSHOP Working Group, “Mobile IPv6 Fast Handovers (RFC 5268)” http://www.ietf.org/rfc/rfc4068.txt

[59] MIPSHOP Working Group, “Hierarchical Mobile IPv6 Mobility Management (RFC 5380) obsoletes RFC 4140” http://www.ietf.org/rfc/rfc4140.txt

[60] Network Mobility Working Group, http://www.ietf.org/html.charters/OLD/nemo-charter.html

[61] NEMO Working Group, “Network Mobility (NEMO) Basic Support Protocol (RFC 3963)” http://www.ietf.org/rfc/rfc3963.txt

[62] NEMO Working Group, “Network Mobility Route Optimization Solution Space Analysis (RFC 4889)” http://www.ietf.org/rfc/rfc4889.txt

[63] NEMO Working Group, “Network Mobility Route Optimization Problem Statement (RFC 4888)” http://www.ietf.org/rfc/rfc4888.txt

[64] NEMO Working Group, “Network Mobility Home Network Models (RFC 4887)” http://www.ietf.org/rfc/rfc4887.txt

[65] NEMO Working Group, “Network Mobility Support Goals and Requirements (RFC 4886)” http://www.ietf.org/rfc/rfc4886.txt

[66] NEMO Working Group, “Network Mobility Support Terminology (RFC 4885)” http://www.ietf.org/rfc/rfc4885.txt

[67] NEMO Working Group, “Analysis of Multihoming in Network Mobility Support (RFC 4980)” http://www.ietf.org/rfc/rfc4980.txt

[68] Network- Based Localized Mobility Management Working Group, http://www.ietf.org/html.charters/netlmm-charter.html

[69] NETLMM Working Group, “IPv4 Support for Proxy Mobile IPv6”, http://www.ietf.org/internet-drafts/draft-ietf-netlmm-pmip6-ipv4-support-12.txt

[70] NETLMM Working Group, “GRE Key Option for Proxy Mobile IPv6”, http://www.ietf.org/internet-drafts/draft-ietf-netlmm-grekey-option-09.txt

[71] NETLMM Working Group, “Heartbeat Mechanism for Proxy Mobile IPv6” http://www.ietf.org/internet-drafts/draft-ietf-netlmm-pmipv6-heartbeat-07.txt

[72] NETLMM Working Group, “Interactions between PMIPv6 and MIPv6: scenarios and related issues” http://www.ietf.org/internet-drafts/draft-ietf-netlmm-mip-interactions-04.txt

[73] NETLMM Working Group, “LMA Discovery for Proxy Mobile IPv6” http://www.ietf.org/internet-drafts/draft-ietf-netlmm-lma-discovery-00.txt

[74] NETLMM Working Group, “Security Threats to Network-Based Localized Mobility Management (NETLMM) (RFC 4832)” http://www.ietf.org/rfc/rfc4832.txt

[75] NETLMM Working Group, “Goals for Network-based Localized Mobility Management (NETLMM) (RFC 4831)” http://www.ietf.org/rfc/rfc4831.txt

[76] NETLMM Working Group, “Problem Statement for Network-based Localized Mobility Management (NETLMM) (RFC 4830)” http://www.ietf.org/rfc/rfc4830.txt

[77] NETLMM Working Group, “Proxy Mobile IPv6 (RFC 5213)” http://www.ietf.org/rfc/rfc5213.txt

[78] Host Identity Protocol Working Group, http://www.ietf.org/html.charters/hip-charter.html

[79] HIP Working Group, “Basic HIP Extensions for Traversal of Network Address Translators” http://www.ietf.org/internet-drafts/draft-ietf-hip-nat-traversal-06.txt

[80] HIP Working Group, “Basic Socket Interface Extensions for Host Identity Protocol (HIP)” http://www.ietf.org/internet-drafts/draft-ietf-hip-native-api-06.txt

[81] HIP Working Group, “HIP BONE: Host Identity Protocol (HIP) Based Overlay Networking Environment” http://www.ietf.org/internet-drafts/draft-ietf-hip-bone-01.txt

[82] HIP Working Group, “Host Identity Protocol (HIP) Architecture (RFC 4423)” http://www.ietf.org/rfc/rfc4423.txt

[83] HIP Working Group, “Host Identity Protocol (RFC 5201)” http://www.ietf.org/rfc/rfc5201.txt

[84] HIP Working Group, “Host Identity Protocol (HIP) Domain Name System (DNS) Extensions (RFC 5205)” http://www.ietf.org/rfc/rfc5205.txt

[85] HIP Working Group, “Host Identity Protocol (HIP) Registration Extension (RFC 5203)” http://www.ietf.org/rfc/rfc5203.txt

[86] HIP Working Group, “Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP) (RFC 5202)” http://www.ietf.org/rfc/rfc5202.txt

[87] HIP Working Group, “Host Identity Protocol (HIP) Rendezvous Extension (RFC 5204)” http://www.ietf.org/rfc/rfc5204.txt

[88] HIP Working Group, “End-Host Mobility and Multihoming with the Host Identity Protocol (RFC 5206)” http://www.ietf.org/rfc/rfc5206.txt

[89] HIP Working Group, “Using the Host Identity Protocol with Legacy Applications (RFC 5338)” http://www.ietf.org/rfc/rfc5338.txt

[90] Mobility Extensions for Mobile IPv6 http://www.ietf.org/html.charters/mext-charter.html

[91] MEXT Working Group, “Multiple Care-of Addresses Registration” http://www.ietf.org/internet-drafts/draft-ietf-monami6-multiplecoa-14.txt

[92] MEXT Working Group, “NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks” http://www.ietf.org/internet-drafts/draft-ietf-mext-aero-reqs-03.txt

[93] MEXT Working Group, “AAA Goals for Mobile IPv6” http://www.ietf.org/internet-drafts/draft-ietf-mext-aaa-ha-goals-01.txt

[94] MEXT Working Group, “Mobile IPv6 Support for Dual Stack Hosts and Routers” http://www.ietf.org/internet-drafts/draft-ietf-mext-nemo-v4traversal-10.txt

[95] MEXT Working Group, “Automotive Industry Requirements for NEMO Route Optimization” http://www.ietf.org/internet-drafts/draft-ietf-mext-nemo-ro-automotive-req-02.txt

[96] MEXT Working Group, “Flow Bindings in Mobile IPv6 and Nemo Basic Support” http://www.ietf.org/internet-drafts/draft-ietf-mext-flow-binding-02.txt

[97] MEXT Working Group, “Mobility Support in IPv6” http://www.ietf.org/internet-drafts/draft-ietf-mext-rfc3775bis-03.txt

[98] MEXT Working Group, “DHCPv6 Prefix Delegation for NEMO“http://www.ietf.org/internet-drafts/draft-ietf-mext-nemo-pd-02.txt

[99] MEXT Working Group, “Binding Revocation for IPv6 Mobility” http://www.ietf.org/internet-drafts/draft-ietf-mext-binding-revocation-06.txt

[100] MEXT Working Group, “Guidelines for firewall administrators regarding MIPv6 traffic” http://www.ietf.org/internet-drafts/draft-ietf-mext-firewall-admin-01.txt

[101] MEXT Working Group, “Guidelines for firewall vendors regarding MIPv6 traffic” http://www.ietf.org/internet-drafts/draft-ietf-mext-firewall-vendor-01.txt

[102] MEXT Working Group, “Network Mobility (NEMO) Management Information Base “, http://www.ietf.org/rfc/rfc5488.txt

[103] FP6 Integrated Project DAIDALOS, http://www.ist-daidalos.org/default.htm

[104] Daidalos I, http://www.ist-daidalos.org/daten/publications/flyer/Daidalos_I_Flyer .pdf, June 2004.

[105] Daidalos II, http://www.ist-daidalos.org/daten/publications/flyer/Daidalos_II_ Flyer.pdf, October 2006.

[106] Alcate-Lucent, “Alcatel-Lucent Mobility Solutions”, http://enterprise.alcatel-lucent.com/?solution=Mobility&page=Homepage.

[107] Nokia Siemens Networks, “Nokia Siemens Networks Fixed-Mobile Convergence. Executive Summary”, http://www.nokiasiemensnetworks.com/NR/rdonlyres/A5BCF461-5270-41E9-87BB-0501DE210A4F/3000/FMC_ executive_summary1.pdf

[108] Huawei, “Internet mobility solutions. Mobile Broadband solution”, http://www.huawei.com/core_network/internet_mobility _solutions/mobile_broadband_solution.do?card=0

[109] Cisco, “Cisco 3300 Series Mobility Services Engine”,http://www.cisco.com/en/US/products/ps9742/index.html

[110] Cisco, “Cisco Mobility Services Architecture”, http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/white_paper_c11-478162_ns348_Networking_Solutions_White_Paper.html

[111] British Telecom, “Enterprise Mobile Services”, http://globalservices.bt.com/LeafAction.do?Record=Enterprise_mobile_services_solutions_ gbl_en-gb&Context=Products

[112] France Telecom Group, “Business Everywhere”, http://www.orange-business.com/en/mnc2/mobility/mobile_information/ business_everywhere/index.html

[113] Vodafone, “Built-in mobile broadband. Buit-in 3G”, http://enterprise.vodafone.com/global/product_solutions/data_connectivity/ builtin_3g/builtin/builtin.jsp

[114] Vodafone, “Built-in mobile broadband. Gobi enabled laptops”, http://enterprise.vodafone.com/global/product_solutions/ data_connectivity/builtin_3g/gobi/gobi.jsp

[115] Telefónica, “Facilidad Movilidad. Movilidad para Tarifa Plana Horario Reducido Telefónica Net”, http://www.telefonica.es/on/onTOFichaProducto/0,,v_segmento%2BAHOG%2Bv_idioma%2Bes%2Bv_segest%2BAHOG%2Bv_pagina%2BLI4%2Bv_producto%2B19140%2BdsCatPrimerNivel%2BINTERNET%2Bv_proceede%2Bhome,00.html

[116] Telefónica, “Facilidad Movilidad. Movilidad para Tarifa Plana 24H Telefónica Net”, http://www.telefonica.es/on/onTOFichaProducto/0,,v_segmento%2BAHOG%2Bv_idioma%2Bes%2Bv_segest%2BAHOG%2Bv_pagina%2BLI4%2Bv_producto%2B24300%2BdsCatPrimerNivel%2BINTERNET%2Bv_proceede%2Bhome,00.html

[117] Telefónica, “Facilidad Movilidad. Movilidad para Tarifa Plana Horario Comercial Telefónica Net”, http://www.telefonica.es/on/onTOFichaProducto/0,,v_segmento%2BAHOG%2Bv_idioma%2Bes%2Bv_segest%2BAHOG%2Bv_pagina%2BLI4%2Bv_producto%2B25780%2BdsCatPrimerNivel%2BINTERNET%2Bv_proceede%2Bhome,00.html

[118] Swisscom, “Swisscom Corporate Access CAA/CNA”, http://www.swisscom.ch/solutions/en/index/product/corporate_access.htm.

[119] Swisscom, “Swisscom Mobile Unlimited”, http://www.swisscom.ch/solutions/en/index/product/mobile-unlimited.htm

[120] Stoke, “Multi-Access Network Mobility Solution Brief”, October 2008, http://www.stoke.com/Solutions/mobile_anchor.asp

[121] IEEE Computer Society, “Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services”, September 2008.

[122] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, “SIP: Session Initiation Protocol”, RFC 3261, June 2002.

[123] IEEE P802.21/D14 Draft Standard for Local and Metropolitan Area Networks: Media Independent Handover Services

[124] Handley, M. and V. Jacobson, “SDP: Session Description Protocol”, RFC 2327, April 1998.

[125] IEEE P802.16g™-2007, IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment 3: Management Plane Procedures and Services.

[126] Stoke, “Stoke OS”, http://www.stoke.com/products/StokeOS.asp#specs

[127] Stoke, “Multi-Access Network Mobility”, http://www.stoke.com/Solutions/mobile_anchor.asp

[128] Cheng, Alice Y., Das, Subir, Ohba, Yosihiro, and Zuniga, Juan Carlos, “IEEE 802.21 MIH Protocol Test Cases”, August 2009.

[129] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with SDP", RFC 3264, June 2002.

[130] IEEE 802.1AB™-2005, IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery.