MEDIEVAL
INFSO-ICT-258053

MEDIEVAL

DELIVERABLE D4.1

Light IP Mobility architecture for Video Services: initial architecture

Editor:	Loris Marchetti, TIS
Deliverable nature:	Public
Due date:	June 30th, 2011
Delivery date:	June 30th, 2011; updated October 12th
Version:	1.1
Total number of pages:	84
Reviewed by:	Baruch Altman (LIVEU), Gerald Kunzmann (DOCOMO)
Keywords:	Mobility, Distributed Mobility Management, IEEE 802.21, Anchoring Models, Multihoming, Logical Interface

Abstract

This deliverable provides the description of a novel flat IP mobility architecture. The definition of video aware interfaces between the mobility and the other subsystems of the MEDIEVAL architecture (i.e., wireless access, transport optimisation and video-service control subsystems) is also part of this architectural deliverable.

List of authors

Company	Authors
Telecom Italia	Loris Marchetti, Elena Demaria
ALBLF	Telemaco Melia, Rui Costa
UC3M	Fabio Giust, Carlos Jesús Bernardos Cano
IT	Sérgio Figueiredo, Daniel Corujo
EURECOM	Nguyen Tien-Thinh, Christian Bonnet
PTIN	Pedro Neves, Tiago Cardoso
LIVEU	Baruch Altman

History

Modified by	Date	Version	Comments
TIS	30/6/2011	1.0	Submission
TIS	12/10/2011	1.1	Updated with Appendix I, as requested during the annual audit

Executive Summary

The purpose of this deliverable is to present the MEDIEVAL mobility architecture. As the MEDIEVAL project focuses on mobile operators' networks, the decision has been to incrementally evolve existing network solutions for mobile operators, nowadays based on the 3GPP Evolved Packet System (EPS) architecture.

Within these commercial networks the support of IP mobility is offered "by default" being mobility integral to the network architecture that is based on a core-level anchoring model: the anchor is located in the core network and a given mobile node (MN) is always connected to the same anchor during the lifetime of the session independently of its movements.

This causes the setup and maintenance of several tunnels for each user since mobility must always be guaranteed. On the other hand, the advantage of this model is the fact that it is very flexible and that the host does not need to change anchor (and IP address) for the whole duration of the session.

One of MEDIEVAL project's aims is to evolve from this traditional model trying to see mobility as a service offered only when needed. Moreover, mobility is not only applied to the terminal as a whole but on a per-flow granularity i.e. only to applications that cannot cope with dynamic IP address changes during the communication lifetime.

This new way of considering mobility offers advantages only if it allows the disappearance of mobility tunnels inside the mobile network. In MEDIEVAL architecture this is achieved by moving the anchors from the core level down to the edge. The optimal positioning identified is at the Access Router (AR) level.

The combination of distributing the anchors to the edge and on demand seamless mobility support, nicely fits in scenarios where the Content Delivery Networks (CDN) are deployed with caches closer to the AR (to the edge), thereby avoiding the user's traffic to be tunnelled to the core network.

Another point in favour of this model is when traffic patterns show a high level of inter-users traffic, locally exchanged, and not only directed to the Internet. Also in this case there is a gain in not having the traffic tunnelled to the core network back and forth.

This flat distributed mobility architecture is in line with the Distributed Mobility Management (DMM) concept (currently under investigation in the IETF) and it is assumed that both network-based and host-based mobility solutions/protocols run concurrently in a hybrid network and host-based design.

The access network is organized in Localized Mobility Domains (LMDs) in which a network-based scheme is applied. Users are expected to be roaming within a single LMD most of the time, but, for those cases where this is not possible (e.g., roaming to a network owned by a different operator or to an LMD disjoint with the previous one), a host-based DMM approach is followed. In order to integrate both approaches, so a mobile node can simultaneously have sessions managed by a network-based ("PMIPv6 alike") approach and a host-based ("DSMIPv6 alike") approach, a novel architectural element called Mobile Access Router (MAR) has been introduced. The MAR is a network entity implementing all the functionalities of its counterparts in the standard mobility protocols (DSMIPv6 and PMIPv6), so it is able to play the role of plain access router, home agent, local mobility anchor and mobile access gateway on a per address basis.

Besides designing a dedicated module to carry out the mobility operations, the Mobility architecture also comprises interactions with the other MEDIEVAL subsystems to harmonize the handover process according to the video transport enhancements defined as MEDIEVAL's objectives. For this purpose the mobility subsystem provides the following interfaces for the external communications:

- the interface with the Transport Optimisation subsystem allows to manage network congestion cases and helps to find the best candidate target networks for the handovers (e.g., in terms of availability of content caches located nearby, and network congestion status);
- the interface with the Wireless Access subsystem is used to exchange information with lower layers regarding the radio connectivity and availability of points of attachment;
- the interface with the Video Service Control subsystem triggers content adaptation functions to reduce as much as possible QoS/QoE degradation during the handovers.

Table of Contents

List of Figures

List of Tables

Abbreviations

AFM	Aggregator Flow Manager
A-MAR	Anchoring Mobility Access Router
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
AR	Access Router
BC	Binding Cache
BCE	Binding Cache Entry
BM-SC	Broadcast/Multicast Service Centre
BA	Binding Ack
BU	Binding Update
CDN	Content Delivery Networks
CM	Connection Manager
C-MAR	Candidate Mobility Access Router
CN	Core Network
CoA	Care-of Address
DHCP	Dynamic Host Configuration Protocol
DL	DownLink
DMM	Distributed Mobility Management
DSMIPv6	Dual Stack Mobile IPv6
eMBMS	evolved MBMS
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FM	Flow Manager
GBR:	Guaranteed Bit Rate
HA	Home Agent
HIP	Host Identity Protocol
HO	HandOver
HoA	Home Address
HSS	Home Subscriber Server
IGMP	Internet Group Management Protocol
LMA	Local Mobility Anchor
LMD	Localized Mobility Domain
LTE	Long Term Evolution
MAG	Mobile Access Gateway
MAR	Mobility Access Router

MBMS	Multicast/Broadcast Multimedia Service
MBMS-GW	MBMS GateWay
MEDIEVAL	MultimEDia transport for mobIlE Video AppLications
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIHO	Mobile Initiated Handover
MIIS	Media Independent Information Service
MLD	Multicast Listener Discovery
MIPv6	Mobile IPv6
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MN	Mobile Node
MSC	Message Sequence Chart
MT	Mobile Terminal
MUME	MUlticast Mobility Engine
NEMO	Network Mobility
NIHO	Network Initiated Handover
NME	NEMO Mobility Engine
PBA	Proxy Binding Ack
PBU	Proxy Binding Update
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PIM-SM	Protocol Independent Multicast - Sparse-Mode
PMIPv6	Proxy Mobile IPv6
PoA	Point of Attachment
PoS	Point of Service
PSS	Packet-switched Streaming Service
p-t-m	point-to-multipoint
p-t-p	point-to-point
QCI	Quality of Service (QoS) Class Identifier
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RLC	Radio Link Control
SGW	Serving Gateway

SLAAC	Stateless Address AutoConfiguration
S-MAR	Serving Mobility Access Router
SSM	Source Specific Multicast
T-MAR	Target Mobility Access Router
UE	User Equipment
UL	Uplink
UME	Unicast Mobility Engine
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network

1 Introduction

The purpose of this deliverable is to present the MEDIEVAL mobility architecture as the basis for the subsequent work on mobility in the project itself. A new mobility model is required to address two of the MEDIEVAL main core needs:

1. Optimised for the special requirements of video applications and user experiences and expectations as listed in MEDIEVAL requirements and depicted by the use cases in D1.1[2]; and,
2. Focusing on mobile operator's networks (4G LTE and WiFi)

Starting from the current architecture (Evolved Packet System (EPS)) defined by the 3GPP standardization body, the MEDIEVAL project aims at incrementally evolving the existing functionalities and associated protocol operations and at updating where necessary the network reference model. The current situation, being MEDIEVAL's starting point, is that within these commercial networks the support of IP mobility is based on a core-level anchoring model: the anchor is located in the core network and a given mobile node (MN) is always connected to the same anchor during the lifetime of session independently of its movements. The main advantage of this model is the fact that it is very flexible and that the host does not need to change anchor (and IP address) for the whole session. On the other hand, since the host needs to be connected to a gateway in the core network, a tunnel must be established and maintained.

The main concepts behind/characterizing the MEDIEVAL mobility model are:

1. One of MEDIEVAL project's aims is to evolve from this traditional model trying to move the mobility anchors towards different levels in the network hierarchy, from the core level down to the edge and evaluating the associated benefits and issues, especially when considering deployment of new broadband video services for mobile users.
2. Major effort has been devoted to evolve the mobility architecture towards the Distributed Mobility Management (DMM) concept currently under investigation in the IETF community. The idea is to push the anchors closer to the terminals, ideally at the Access Router (AR) level.
3. A further idea pursued in MEDIEVAL is to enable the IP mobility support (or anchoring) not "by default" but only when the application cannot cope with dynamic IP address changes during the communication lifetime. A further key-feature in the MEDIEVAL architecture is the provisioning of the mobility support at IP-flow granularity, differently from the classical mobility approaches, which offers an "all/nothing" mobility support at IP address granularity.

The combination of distributed anchoring and dynamic mobility support nicely fits with the scenarios where Content Delivery Networks (CDN) are deployed with caches at AR level enabling efficient video delivery to the users.

Another point in favour of this model is when traffic patterns show a high level of inter-user traffic: in this case if users exchange traffic among themselves there are remarkable performance, cost and user experience gains in not having the traffic tunnelled to the core network back and forth.

4. In MEDIEVAL, both network-based and host-based mobility solutions/protocols run concurrently in a hybrid network and host-based design. The mobility management scheme, where necessary, is integrated with Media Independent Handover Services IEEE 802.21, to benefit from a Make-Before-Break for handovers, i.e. the new connection path is established before the previous one is broken. We also discuss the mobility for the bonded-links ("multi-homed") applications.
5. The Mobility subsystem is not a standalone component in the global MEDIEVAL architecture, as it interacts with the other components to harmonize the handover process according to the video transport optimisations. The interactions with the Transport Optimisation subsystem allow managing network congestion cases and help to find the best candidate target networks for the handovers (e.g., in terms of availability of content caches located nearby, and network congestion status). The interface with the Wireless Access subsystem is used to exchange information with lower layers regarding the radio connectivity and availability of points of attachment. In addition, the interaction with the Video Service Control subsystem, triggers content adaptation functions to minimize any QoS/QoE degradation during/as a result of the handovers.

The structure of the deliverable is organized as follows. Section 2 summarizes the key contributions in terms of novelties and basic architectural choices. Section 3 looks at the MEDIEVAL benchmark/referral/baseline/origin model currently defined 3GPP Evolved Packet System architectures, essentially the one based on Release 8, and also presents some advances of interest for MEDIEVAL, introduced in Release 9 and 10 (e.g., support of IP Flow Mobility). Section 4 presents the four different anchoring models, mainly considering the applicability of each to video services and to DMM concept.

Section 5, the core of the deliverable, describes the MEDIEVAL mobility architecture in terms of operations performed by the different subsystems. Note that subsection (5.8) is also devoted to multicast engine operations further specified in D4.2 [5].

Section 6 introduces some of the Message Sequence Charts (MSCs) related to use case two (described in D1.1) with the aim to describe the effective operation of mobility components. Finally, in Section 7 a detailed specification of interfaces is provided.

The architecture described in this deliverable will be subject to future changes, based on feedback and experience gained in the upcoming months with the effective implementation. A final, revised version of the mobility architecture will be described in Deliverable D4.3 [41].

2 Key contributions

The list below represents the contributions offered by the MEDIEVAL project related to the topic dealt by this deliverable. Most of the work done has also been matter of submissions to standardization bodies as IETF and IEEE and scientific publications. In particular, MEDIEVAL's output can be found in the form of standard or draft, in conference proceedings and journal articles.

- The mobility part of the MEDIEVAL general architecture is presented in this deliverable. MEDIEVAL's research team is weighting the impact of deploying the mobility anchors at various levels in the network hierarchy, from the core level down to the edge, thus several efforts are put in describing MEDIEVAL-compliant extensions of Proxy Mobile IPv6 (PMIPv6) [11] (for a centralized approach with the anchors in the core network) and in parallel a complete solution for Distributed Mobility Management (DMM - currently under investigation in the IETF community, [12][13]) whenever the anchors are pushed closer to the terminals.
- Since MEDIEVAL aims at offering the best mobility management scheme according to users' mobility patterns, a further distinction between local and global mobility is done [22]. When dealing with local mobility, a network-based localized mobility management scheme is adopted [24][25], while for global mobility a host-based management like DSMIPv6 [10] is preferred. The combinations of the schemes can be found in [23].
- The mobility management scheme for a centralized approach leverages on PMIPv6 protocol, with the integration of Media Independent Handover Services IEEE 802.21[7], for a Make-Before-Break approach for handovers. Details about an implementation of such approach can be found in [37]. Moreover, PMIPv6 applies for extensions to support flow mobility [26][27], a key-feature in the MEDIEVAL architecture, since mobility support is envisioned to be provided at IP-flow granularity, differently from the classical mobility approaches.
- The distributed mobile architecture was developed starting from [14] and [15] and resulting in [17] for the network-based part, while the host-based part relies on [16] and [18]. These two schemes were then merged into a hybrid network and host-based design representing MEDIEVAL's mobile architecture [19].
- The mobile architecture aims at providing support not only to unicast flows, but also to multicast transmissions, for which a dedicated effort was put in the investigation in order to integrate the two functionalities into the same framework. First, a solution for PMIPv6 was developed, following the guidelines in [29][30][31][33]. A preliminary result was then obtained by using the main concepts elaborated in [32], and the detailed description is presented in MEDIEVAL deliverable D4.2 [5].
- The MEDIEVAL Mobility subsystem interacts with the other components when it is invoked by the Wireless Access [4] and the Transport Optimisation [6] subsystems. In addition, the mobility subsystem interacts with the Video Service Control subsystem [3], for the exchange of QoS parameters. For these purposes, two intelligent modules were designed to interact with the external subsystems and to run the internal mobility engines. The first module is the Flow Manager (FM), residing in the network. It is a MIH user to deal with the handover preparation, but it also uses an API-based scheme to exchange information with the Transport Optimisation subsystem. The second module is the Connection Manager (CM - [20]). It is the MIH user in the terminal, and is responsible for the activation of the mobility client when required and for the configuration of the Logical Interface [21]. In addition the CM handles local host management including cross-layer interactions with the user applications.
- Earlier prototype work was done under the CARMEN project. Part of the prototype has been re-written to adapt to the MEDIEVAL requirements and has been presented in Future Network and Mobile Summit 2011 as a demo stand.

3 Reference technologies

The MEDIEVAL architecture will follow an incremental approach starting from 3GPP architecture and specifically from 3GPP Rel 8 that introduced a change in the network architecture. Extensions and new features added in Rel 9 and 10 will also be considered. The reference architecture is depicted in Figure 1.

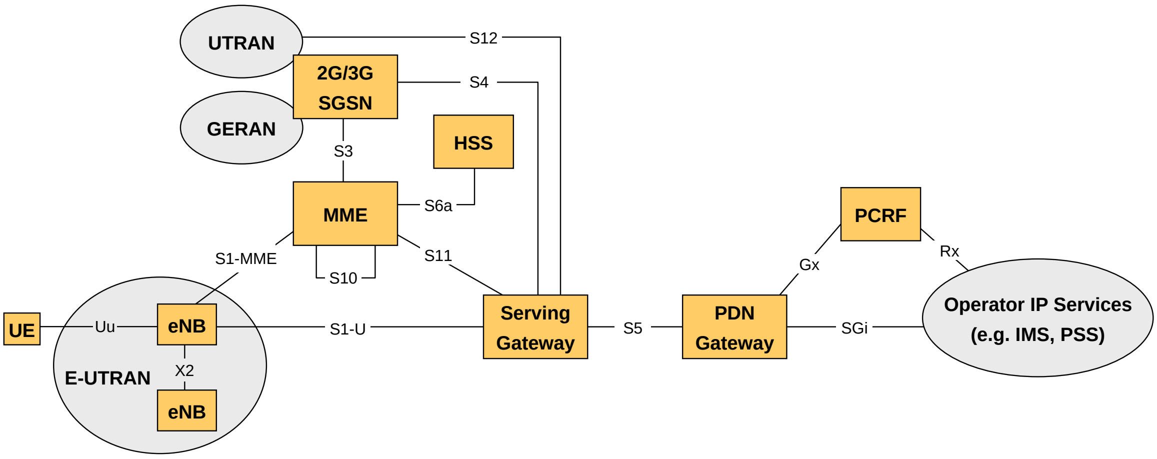

Figure 1: EPS Architecture for unicast communications

The radio access network is based on the LTE Advanced standard and the core network is composed of the following nodes:

- Mobility Management Entity (MME). This node manages the control plane for the UE and in particular ends the Non Access Stratum (NAS) signalling; it manages the UE authentication towards the HSS via the S6a interface (based on Diameter) and intercepts signalling traffic.
- Serving Gateway (SGW). This node anchors 3GPP accesses (GERAN, UTRAN, E-UTRAN) guaranteeing inter-RAT mobility. It can be deployed in conjunction with the PGW or as a standalone node.
- Packet Data Network Gateway (PGW). This node can be seen as the evolution of the GGSN as it offers access to external PDNs, it assigns IP addresses to the UEs and it is the mobility anchor for non-3GPP accesses.
- Home Subscriber Server (HSS). This is the node that stores subscribers' data.
- Policy and Charging Rules Function (PCRF). This is the entity allowing the application of specific service policies such as gating, quality of service and charging on a per user and/or per service base.

In the EPS only packet services are supported and the service model is always-on. Among other innovations, the 3GPP Rel 8 architecture also introduced the possibility to directly use non-3GPP accesses to reach the mobile core network and its services. This is done using mobility protocols specified in IETF and can be based on a network-based mobility solution (see Figure 2) or client-based mobility solution (see Figure 3)

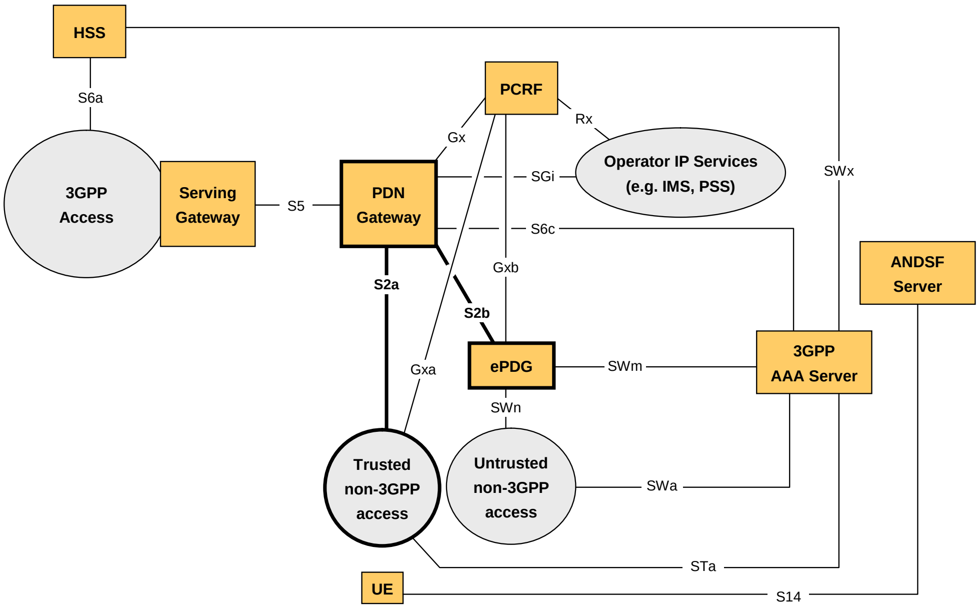

Figure 2: Inter-working with non-3GPP accesses: network-based solution

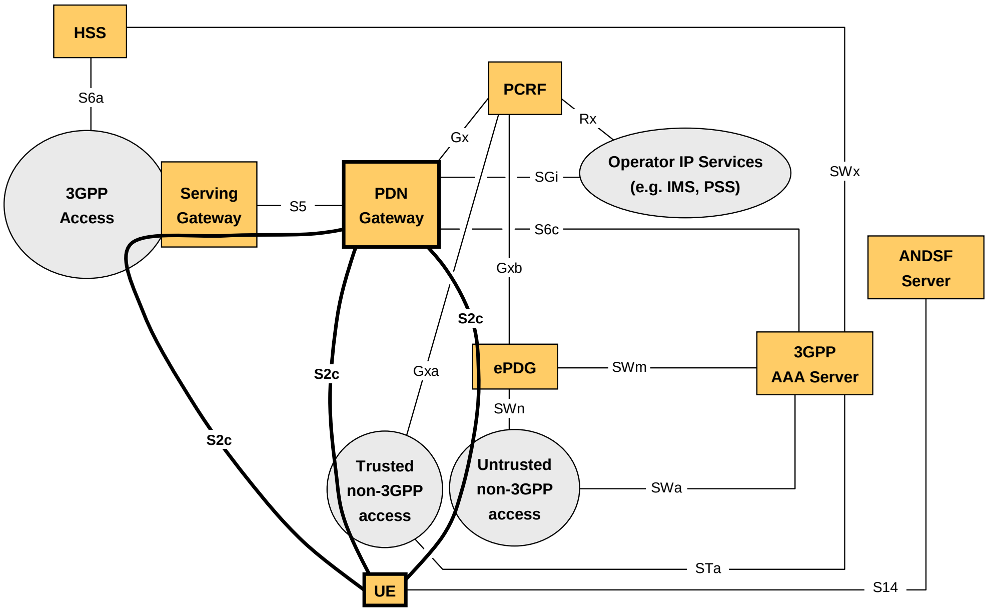

Figure 3: Inter-working with non-3GPP accesses: client-based solution

As reported in the previous pictures for the inter-working with non-3GPP accesses, new protocols have been added to the standard and also new functionalities and network nodes. In particular these new entities have been defined:

- Evolved Packet Data Gateway (ePDG). This is essentially a VPN concentrator used by the UE to establish an IPsec tunnel from a non-3GPP access considered “untrusted” by the operator.
- 3GPP AAA Server. This a network server used for Authentication, Authorization and Accounting functions for users connected through non-3GPP accesses
- Access Network Discovery and Selection Function (ANDSF). This is a server located after the SGi interface (that connects the PGW to the external networks) that provides to the UE information useful for the discovery and selection of access networks in line with the operator’s policies.

The new interfaces added for the inter-working with non-3GPP accesses are:

- Mobility interfaces (S2a, S2b, S2c). S2a and S2b are used to manage mobility for trusted and untrusted accesses in a network-based mode. S2c interface is based on the host-based mobility protocol Dual-Stack Mobile IPv6 (DSMIPv6).
- Interfaces for authentication, authorization and accounting functions (STa, SWa, SWm, SWx, S6c).
- Interfaces for Policy and Charging Control (PCC) between the PCRF and the trusted/untrusted (Gxa, Gxb) accesses.
- SWn interface between the UE and the ePDG.
- S14 interface between the UE and the ANDSF.

Regarding mobility with non-3GPP accesses in Rel 9 and 10 new features have been added to allow the Mobile Node to connect to the same PDN from different accesses simultaneously (MAPCON) and to move flows from one access to another (IP Flow Mobility).

3.1 3GPP architecture evolution

Figure 4 depicts the potential evolutions of the Evolved Packet Core (EPC) architecture currently discussed in 3GPP [REF 23.401]. As compared to Figure 2 we note that the trusted non-3GPP access features a WLAN gateway and that both S2a and S2b reference points do not require the Gxx interfaces. The deployment model suggested by the mobile operators points towards a fully network-based mobility management protocol. Given the specificity of the operators' network, the GPRS Tunnelling Protocol (instead of the IETF standards) has been chosen as the reference protocol. It should also be noted that there is a new trend to consider the WiFi access as trusted, in other words by means of a EAP SIM [1][43] authentication method the UE is granted access over WiFi without requesting the establishment of an IPsec tunnel with the ePDG (SWn reference point).

Along these lines the MEDIEVAL architecture considers the video oriented evolution of the Local Mobility Domain implementing a network-based mobility protocol (RFC 5213) and focuses on the complementarities of the 3GPP and WiFi access technologies.

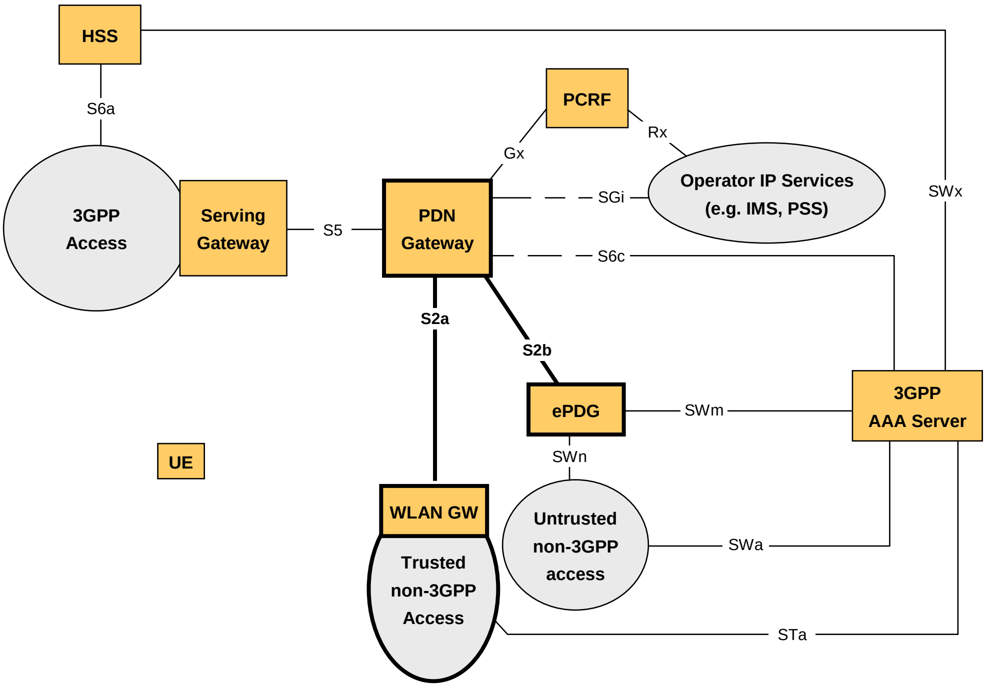

Figure 4: GTP based access for 3GPP and non 3GPP access technologies

As described in Section 2, MEDIEVAL will evolve the localized mobility domain from a centralized approach to a distributed approach. In this view the Serving-GW and the PDN-GW will act as a single box, placed close to mobile users, providing both functionalities at the same time. The new distributed mobility anchors will provide heterogeneous wireless access including LTE advanced and WLAN radios. WLAN is regarded in MEDIEVAL as a trusted access technology. Security considerations and requirements over the existing AAA infrastructure are summarized in Section 3.2.

3.2 Unicast security considerations

The security architecture (as stated in the DoW) has been excluded from the MEDIEVAL project scope, however security considerations and requirements strongly impact the overall design and some considerations can be done even if at a high level. This section briefly introduces some aspects of security regarding unicast traffic (for security considerations related to multicast traffic see D4.2 [1][5]).

The first step in which security is impacted is the attach procedure. The MN must authenticate to the network and different authentication methods must be supported for users that have the SIM/USIM card and also for users that don’t have a mobile device (e.g. PC with only WiFi access). This requirement allows the operator to consider the WiFi access as trusted as reported in Section 3.1. Moreover, these authentication mechanisms allow the terminal to authenticate the network avoiding “rouge” APs and BTSs and protecting against man in the middle attacks.

A second requirement regarding the network access is the possibility to use the same authentication method on both LTE and WiFi accesses. The authentication methods allowed on the network must also offer some mechanisms for fast re-authentication to be used during handovers. Since the MARs in MEDIEVAL architecture can manage PoAs of different technologies (e.g. both LTE and WiFi) this requirement is helpful for reducing handover latency.

Another aspect to take into consideration is the mobility signalling. When using network-based mobility solutions the MN must not send any signalling while when using client-based mobility solutions it must send signalling to the MAR and protect it with proper keys. One requirement that can be derived from the integrated architecture designed for MEDIEVAL is the possibility to use the material generated at the network access authentication to protect the subsequent mobility signalling, thus creating an integrated security architecture for both network access and mobility. To this end the authentication methods allowed on the network must also be able to generate some cryptographic material to be used by other protocols. The way this material is used by other protocols and the methods to send the keys from the AAA server to the right network element must also be defined.

When crossing administrative domains these solutions allow the MN to connect to the mobility anchor provided by his mobility provider only if there are roaming agreements between the two administrative domains so that the authentication can be closed on the home AAA/HSS server. Where it is not possible standard bootstrapping mechanisms (e.g. IKEv2) must be used for the MN to negotiate security associations with the mobility anchor.

3.3 Anchoring models

Mobile networks are based on “anchors” to guarantee session mobility/continuity. Different anchoring models are theoretically possible. In the following subsections four possible models are presented starting from traditional centralized (today deployed solutions) to extreme solutions where the anchor is in the UE.

For each subsection, together with an architecture view, basic features of the models and their differences with respect to the others are presented. Also the applicability of the DMM concept is reported.

The IETF terminology will be used: core-level, AR level, access level, host-level. The different levels of distribution are depicted in the following Figure 5.

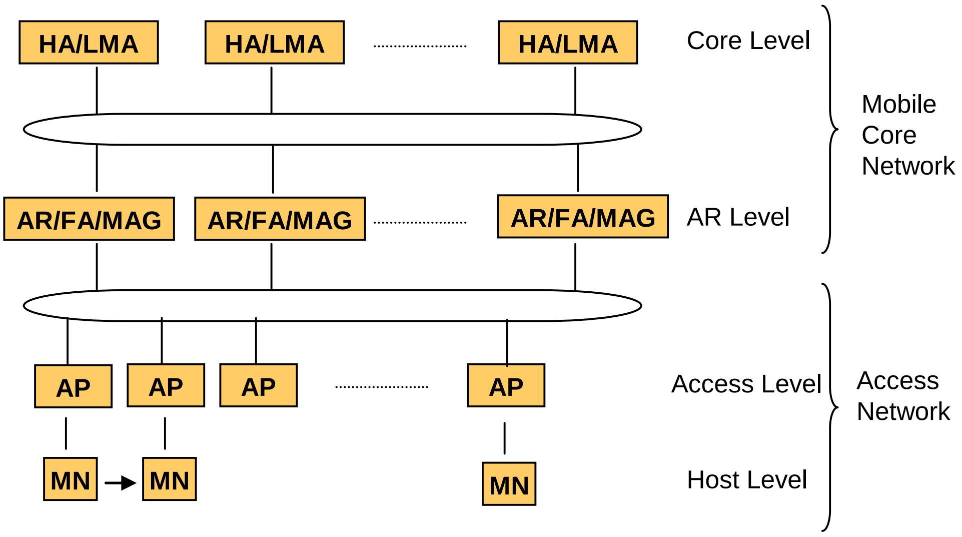

Figure 5: Multiple level of distribution

Following the interests expressed by mobile operators, even if all models are herewith presented, the MEDIEVAL reference architecture, at least at this stage of the project, will only consider the core-level and AR level models.

3.3.1 Core level model (PDN level)

This model is the one adopted in most of commercial mobile networks. The anchor is located in the core network. The MN is always connected to the same anchor during a session independently of its movements.

The main advantage of this model is the fact that it is very flexible and that the host does not need to change anchor (and IP address) for the whole session. On the other hand since the host needs to be connected to a gateway in the core network, a tunnel must be established. This does not allow applying the DMM concept of mobility activated dynamically since plain IP routing cannot be used when the user is not moving: a tunnel is always there. For this reason, even if it is always possible to distribute anchors at the core level there is no clear advantage with respect to the commercial deployment of mobile networks.

Leveraging on the IP Flow Mobility concept (deployed in 3GPP) it is always possible to manage mobility on the basis of single flows but always relaying on the central anchor in case of 3GPP access technologies. In case of non-3GPP accesses (e.g., WiFi) the access can be both registered on the central anchor and used independently for applications that do not need mobility.

3.3.2 Access Router level model

If the UE does not move or if the application does not need session continuity (e.g., it can survive to IP address change), the anchor positioned at the AR level fits well in scenarios where Content Delivery Networks (CDN) are deployed with caches at AR level so that the user's traffic must not be tunnelled to the core network. Another reason to choose this model is when traffic patterns show a high level of inter-user traffic: in this case, if users exchange traffic among themselves, there is a gain in not having the traffic tunnel to the core network and come back.

Also, the deployment of WiFi hotspots can leverage on this architecture to include also non-3GPP accesses into the mobile network. This is due to the fact that also WiFi Access Points can be connected to the Access Router using a CAPWAP model (i.e. the Access Router manages the Access Point as layer 2 nodes in a way similar to the one used for eNodeB in LTE).

This model is the most useful to the deployment of DMM since it allows plain IP routing since the attachment of the Mobile Node and can also facilitate integration of WiFi accesses.

3.3.3 Access level model

This model foresees the mobility anchor on the access node (e.g., eNodeB in case of LTE). The main advantage of this model is the complete distribution of the anchors that reach the last segment of the network allowing to achieve the most optimal routing.

On the contrary, this model has two main drawbacks: the first is the fact that the number of anchors will grow a lot, the second that this model requires the change of access nodes (e.g., eNB or WiFi Access Points): the eNB must become the default gateway for the MN and its mobility anchor thus assigning the IP address to the MN and taking care of more tasks than today. These will increase costs and complexity.

The DMM concept could also be applied to this model since the anchors will be deployed in the edge in a flat architecture.

3.3.4 Host level model

In this model the anchor is located on the host itself. This is a sort of peer-to-peer model where the host directly communicates to the correspondent node its address. This mode of operation corresponds to the route optimization of Mobile IPv6 or to protocols like Host Identity Protocol (HIP) [42].

The main advantage of this model is the routing optimization, i.e., the traffic always follows the best path between the two nodes. On the other hand, the main problem that this model poses is the simultaneous movement of the two hosts and the consequent loss of the Binding Update message. To solve this problem a rendezvous server must be deployed that collects messages when the hosts move.

Since the MN does not have a fixed Home Address, a DNS server dynamically updated must be used to find the current position of the MN itself.

4 Requirements and challenges

Deliverable D1.1 extensively describes the key innovations the MEDIEVAL project is developing and, for easier reading, hereinafter briefly summarized:

1. Design of evolved cross-layer algorithms and mechanisms between the video services and the network layer, dynamically optimizing video services with suitable network support.
2. Design of Quality of Experience-based solutions for mobile video delivery taking the actual user perceived quality into account in traffic management.
3. Design of a mobile CDN concept for efficient media delivery based on intelligent caching and P2P-based video streaming; in contrast to existing solutions this relies on information provided by the network for optimal source (cache) selection.
4. Design of a flat mobility architecture based on a dynamic distributed mobility management concept, including multiple anchoring support. The designed solution will provide mobility services only for those IP flows (and/or applications) that really require IP address continuity.
5. Design of novel mechanisms to optimise video transmission over heterogeneous air interfaces addressing cellular technologies and IEEE 802.11 technologies (including multicast/broadcast audio video streams).
6. Design mechanisms to support video content adaptation and reliability over multiple networks simultaneously (i.e. FEC over multiple connections, SVC layers vs links...).

Innovation one deals with the interfaces between the mobility layer and the overall MEDIEVAL architecture (see reference network model) imposing the following requirements:

R1. The Mobility platform SHALL support cross-layer interaction including wireless access layer, network layer and application layer.

R2. The Mobility platform SHALL support cross-layer interaction among different wireless access systems.

Innovation two deals with the end-to-end QoE approach the project is promoting to provide the required user experience also on non-managed wireless access systems. It is imposing the following requirements:

R3. The Mobility platform SHALL support selective application handover on the most appropriate wireless media.

Innovation three deals with the global design of mobile CDNs imposing the following requirements:

R4. The Mobility platform SHALL support intelligent handover candidate selection based on radio, resource and CDN requirements and availability.

R5. The Mobility platform SHALL enable optimal CDN location while minimizing RTT delays between the source and the destination.

Innovation four deals with the disruptive design of a video-aware flat IP network, imposing the following requirements:

R6. The Mobility platform SHALL support optimised end to end routing.

R7. The Mobility platform SHALL be deployment-friendly (i.e. scalability and reliability in current LTE and WLAN network standards & deployments).

R8. The Mobility platform SHALL support seamless services of selected applications on demand.

R9. The Mobility platform SHALL minimise the signalling overhead over the air and handover frequency.

Innovation number five deals with the use of both unicast and multicast techniques for video delivery imposing the following requirements:

R10. The Mobility platform SHALL support both unicast and multicast schemes for destination node mobility.

R11. The Mobility platform SHALL support both unicast and multicast schemes for source node mobility.

Innovation number six deals with the use of SVC codecs in MEDIEVAL, imposing the following requirements:

R12. The Mobility platform SHALL be able to understand single applications flows and treat them according to selected policies (e.g. multi link vs. single link flow).

4.1 How MEDIEVAL video services map into anchoring models

MEDIEVAL, as described in D1.1, has defined the use of four video services namely Personal Broadcasting (PBS), Mobile TV (MTV), Video on Demand (VoD) and Interactive Video (InV).

In this section we analyse the use of the different anchoring models in the context of each video service.

4.1.1 Core level model

4.1.1.1 PBS service

In this case, the PBS service requires routing of the IP traffic back to the central anchor (P-GW) and distributing the video flows to potentially multiple destinations. Depending on how the PBS is provided, we can derive two different operating models:

- The PBS service is implemented as part of the e-MBMS system: it means that the MN is capable of sending video content to a given unicast address and the service is announced by the e-MBMS platform. The MN is sending unicast packets to the e-MBMS gateway and the MBMS gateway sends multicast packets to the registered users. It should be noted that this method is convenient when the underlying network does not natively support multicast routing.
- The PBS service is implemented as part of the fully fledged multicast solution: in case the network supports multicast routing the MN can send and receive multicast traffic and benefit of seamless mobility support for both senders and receivers. It is clear that this solution requires the network to support multicast routing as specified in deliverable D4.2.

According to the eMBMS deployment model the MBMS GW is integrated in the S-GW, which in the MEDIEVAL architecture maps to the MAR. In case of the core level model packets are tunnelled back to the mobility anchor (P-GW) and subsequently forwarded to their destination. In the core level model the MBMS distribution model seems more appropriate.

4.1.1.2 Mobile TV service

The Mobile TV service is based on the traditional broadcasting distribution model. In the context of the core level model the stream is collected at the P-GW and distributed to n-users requesting the service. Convergence between broadcast methods (e.g., DVB) and e-MBMS methods seems to be the right way forward for a unique and standardised distribution method (also considering the limitations with respect to multicast routing enabled networks).

4.1.1.3 VoD service

The VoD service is delivered as unicast stream and content can be potentially adapted to multiple end devices. From a mobility perspective this is a standard unicast stream with specific per flow policies.

4.1.1.4 INV service

The InV service is a unicast service treated equally to the VoD service.

4.1.2 Access Router level model

4.1.2.1 PBS service

As before, the PBS service can be provided as part of the MBMS platform or as a native multicast service. Intuitively, when the distributed mobility model is achieved at the edge, it seems natural to provide PBS as a native multicast service. When the nodes are communicating in the local domain, no routing deployment issues are foreseen. In case of communication to the Internet, the limited multicast deployment can negatively impact. In case the network has limitations in supporting native multicast routing the e-MBMS GW in charge of the multicast distribution is collocated with the local anchor, thus overcoming the above mentioned issue.

4.1.2.2 Mobile TV service

In the AR level model the Mobile TV service greatly benefits from the multicast solution described in D4.2. In case multicast routing is not supported in the network, the MBMS gateway can still fallback to the unicast solution for inter-MBMS GW communication.

4.1.2.3 VoD service

Being the VOD service a unicast service, there is not impact on the IP distribution model.

4.1.2.4 INV service

Similar considerations to the VoD service apply.

4.1.3 Other anchoring models

The use of access level model and host level model is considered out of scope of the MEDIEVAL approach due to scarce flexibility and increased complexity. In addition, it requires considerable changes to the access and end user devices departing from the original goal of incremental approach.

5 Mobility architecture

5.1 Overview of the mobility architecture

The MEDIEVAL mobility architecture aims at providing always the most efficient mobility support according to the user needs, and for this scope the network-based mobility paradigm has been followed. All the nodes in a network complying with such approach form a Localized Mobility Domain (LMD).

To the MEDIEVAL's extent, an LMD is the part of the network that is able to provide network-based mobility support in a non-centralized (i.e. DMM-compliant) way, and is assumed to be under the administration of the same entity (e.g. a single mobile operator or ISP), which is free to deploy a single LMD covering all or part of its network's nodes, or, on the contrary, multiple disjoint LMDs. In the LMD two nodes are identified:

- **Mobility Access Router (MAR)**. It is the router in the access network acting as the terminals' default gateway. Referring to the EPS and to the anchoring model presented in previous sections, it may be assumed that the S-GW and P-GW are collapsed into the MAR node. Moreover, since MEDIEVAL endows the terminals to exploit (simultaneously or not) different radio interfaces, a MAR should be able to handle non-homogeneous access technologies, i.e. should be connected to LTE eNodeBs and WiFi Access Points. A MAR also implements mobility functions inherited by the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG), defined in PMIPv6, and the Home Agent (HA), defined in DSMIPv6, tuned to follow the DMM approach. In fact a MAR is in charge of assigning IPv6 prefixes to MNs (on a per MN-basis) upon joining its access network, and routing the IP flows established using those prefixes, regardless the MNs are still attached to it or to another MAR in the network. In this fashion, a MAR acts as plain IPv6 router for some flows and as mobility anchor for others. The following terminology will be used to give an insight of the working scheme.
    - Anchor-MAR or A-MAR: the MAR that assigned the IPv6 prefix used in the considered flow.
    - Serving-MAR or S-MAR: the MAR which the MN is currently attached to.
    - Target-MAR or T-MAR: the MAR where the MN attaches after a handover.
    - Candidate-MAR or C-MAR: a MAR that can be selected as T-MAR during the handover process.
- **Mobile Node (MN)**. It is the user terminal, also called User Equipment (UE), according to 3GPP terminology. As long as the MN is roaming within the same LMD, it is involved in the handover preparation and control phases, but not in the signalling related to IP address continuity (see Section 5.6). On the other hand, upon crossing the LMD, the IP mobility task is delegated to the terminal and the client for mobility, running in the terminal, is activated. A terminal is assumed to be multimode, i.e. equipped with a LTE and WiFi radio interface, which can be used alternatively or simultaneously. For this purpose, a MN implements an instance of the Logical Interface concept, to mask the address configuration, such that the same IP address is used by both network cards and seen by upper layers.

Additionally, the MEDIEVAL mobile architecture envisions the support to a NEwork that MOves (NEMO) according to the DMM paradigm. For this purpose the NEMO Basic Support protocol [44] has been considered as a starting point to develop a DMM-alike NEMO support. In this view, the Mobile Router (MR) defined in [44] implements extras functionalities to reflect some features intrinsic of a MAR. Hence the name mobile MAR (mMAR).

- **Mobile MAR (mMAR).** It is a router with the capability of changing its point of attachment to the fixed network, thus travelling across different access networks. It is equipped with an external radio interface that at the IP layer connects to a MAR as an MN does. The internal radio interface serves as access point for the mobile nodes that are joining the mobile network. The mMAR is seen as first IP hop and default gateway by the MNs. Typically a mMAR is installed on vehicles as buses, cars, trains, etc. Its external interface is a long range radio (LTE) and the internal (also referred to the *in-*

vehicle or *on-board* link) is a short range radio (WiFi). A mMAR handles mobility by means of a host-based solution, as described in [18], by which it updates its location and maintains reachability of all the nodes it is carrying on-board. In this sense mobile nodes are passively kept reachable, but they are not totally transparent to mobility as they need to configure a new IPv6 prefix when the mMAR joins a new access network. However, this process is handled by the mMAR that relays the prefixes assigned by the MAR to the MN.

A brief high level description of the DMM-like mechanisms for mobility adopted in MEDIEVAL is given in the following paragraph. A detailed solution for unicast flows is postponed to Section 5.6. Section 5.8 and D4.2 are devoted to multicast flows, while NEMO operations are described in Section 5.9.

The A-MAR and S-MAR are not necessarily two distinct nodes, but it is rather a conceptual separation of services offered to a given IP flow. Indeed, A-MAR and S-MAR residing in the same node means that the MN is attached to the MAR where the flow was started, thus the address configured while connected to that MAR is being used in that flow. In this case the MAR acts as a standard IPv6 router, i.e. without encapsulating packets. On the contrary, if A-MAR and S-MAR reside in different nodes (due to user movement and/or flow mobility), packets need to be tunnelled in order to be routed properly without modifying the endpoint addresses. In particular, packets in downlink are intercepted by the A-MAR, tunnelled to the S-MAR, which decapsulates them, and forwarded to the MN. In uplink direction, the S-MAR realizes that the packets source address does not belong to its prefix pool so it encapsulate them to the corresponding A-MAR, which will decapsulate and forward them to their destination (see figure below).

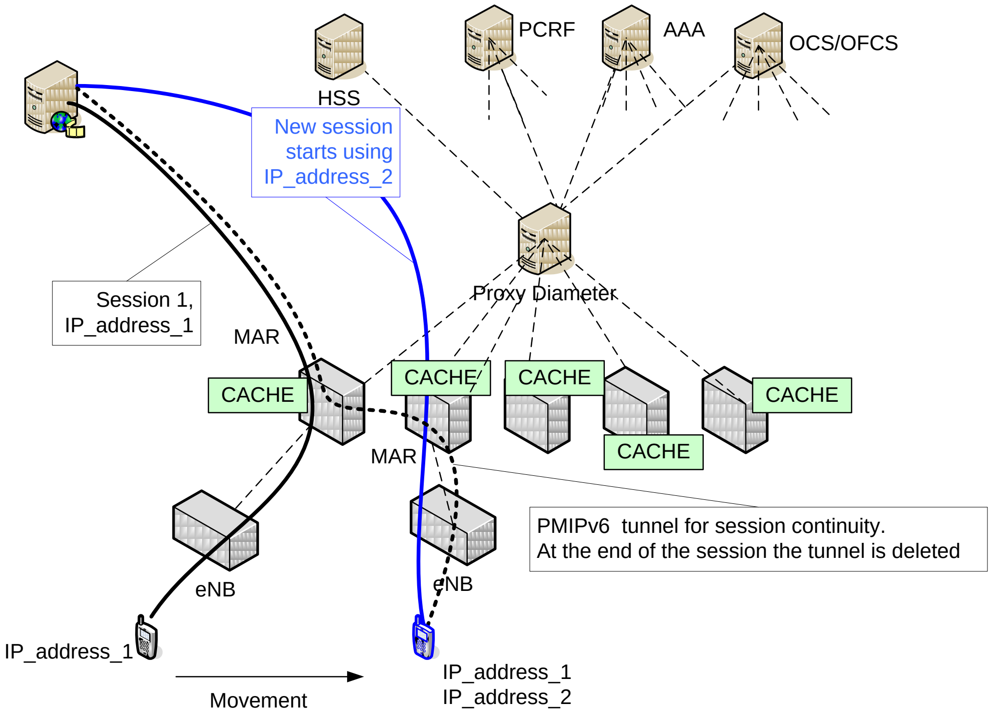

Figure 6: DMM model, basic operation in a single LMD

The conceptual split into Anchoring and Serving MARs is applicable when the MN switches on and roams inside a single LMD. In fact, when crossing the domain boundaries, the MN does not encounter the same mobility support scheme, thus it activates a client for host-based mobility management and all MARs are seen as Home Agents. The mobility client sends a Binding Update message for each prefix it wishes to maintain reachable to the corresponding MARs and when it receives the respective Binding Acknowledgment messages appropriate tunnels are established with the MN's new Care-of Address (CoA) as endpoint. The CoA acquired in the foreign domain can be used by the terminal to start new flows that do not require IP continuity, as IP mobility can only be provided by the DMM host-based support. Thus, it is not recommended to rely on the mobility architecture of the foreign visited network.

In MEDIEVAL, both control and data planes are distributed. Although distributing the data plane requires little intervention to modify current protocols, the control plane needs more efforts to adapt to the DMM scheme. For instance, upon handover and subsequent attachment to a new MAR (S-MAR), the MN should provide to it the IPv6 address of the default router (the A-MAR) configured on the old link (this step is necessary for the S-MAR to be able to contact the A-MAR and setup the tunnel if necessary). This can be achieved through extensions of the Neighbour Discovery protocol or via additional parameters in the DHCP exchange, but, since IEEE 802.21 is extensively used in MEDIEVAL, it can also be exploited for this scope and be part of the control plane. Here follows a list of the entities defined in IEEE 802.21 standard that are used in the MEDIEVAL mobility architecture.

- Point of Service (PoS): network-side MIHF instance that exchanges MIH messages with an MN-based MIHF. The PoS resides in the MAR which includes a PoS for each MIH-enabled MN with which it exchanges MIH messages.
- Point of Access (or attachment): is referred to the entity being the network endpoint of a physical link with the MN. Only LTE eNodeBs and the WiFi access point will be considered.
- Media Independent Information Service (MIIS): provides a framework by which an MIHF, residing in the MN or in the network, discovers and obtains 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. MIIS in the network is generally a PoS-non-PoA.

MARs, mMARs and MNs implement functional building blocks reflecting the internal module’s division into tasks. Following subsections describe in detail the network nodes operations and the modules listed below:

- **Flow Manager (FM).** It resides in the MAR and mMAR; it is a MIH user and it is responsible for the communication with external subsystems as Wireless Access, Transport Optimization and Video Service control. It is able to identify and list the video flows traversing the MAR for which it can activate the IP mobility blocks according to service providers policies.
- **Connection Manager (CM).** It is the FM counterpart residing in the terminal. It is a MIH user too, as it interacts with the Wireless Access subsystem through 802.21 primitives. Also, it exchanges information with the Video Service Control subsystem regarding the QoS/QoE requirements of video streams. It activates the mobility client in the terminal when the localized mobility domain is crossed and the mobility management is delegated to the mobile node. An instance of the CM runs in the mMAR too, in order to manage the mobility of the external interface in a harmonized way with respect to the MN mobility procedure, but for the host-based scheme only.
- **Unicast Mobility Engine (UME).** It is the module in charge of performing the unicast IP mobility operations and signalling following the DMM paradigm. It is implemented in the MAR for the network-based part of mobility management and in the terminal for the host-based part.
- **Multicast Mobility Engine (MUME).** It resides in the MAR and it manages the IP mobility support for the multicast flows. Multicast is treated in detail in Deliverable D4.2.
- **NEMO Mobility Engine (NME).** It resides in the mMAR only, of which it manages the IP mobility according to a host-based DMM solution. When MNs are moving with the NEMO the NME is responsible of informing the current MAR about the MNs’ presence, so that a new prefix can be delivered to them by the MAR through the mMAR. This allows MNs to start flows with a new address, topologically correct at the current serving MAR.

Besides designing a dedicated module to carry out the mobility operations, the Mobility architecture also comprises interactions with the other MEDIEVAL subsystems to harmonize the handover process according to the video transport enhancements defined as MEDIEVAL’s objectives. For this purpose the mobility subsystem provides the following interfaces for the external communications:

- Interface with the Transport Optimization subsystem. It is needed to receive triggers whenever a terminal should move video flows to another PoA, that eventually the MN might be already attached to through the other interface, so that traffic can be moved to a less congested part of the network (Network Initiated HandOver – NIHO). In addition, when a handover initiated by the mobile node occurs, the Transport Optimization subsystem is requested to weight the candidate target networks, according to the availability of content caches located nearby.

- Interface with the Wireless Access subsystem. It is used to exchange information with lower layers regarding the radio connectivity and availability of points of access. The communication is established through IEEE 802.21, and it also allows sending commands to the interfaces. In addition, through the CM and FM modules, the mobility subsystem enables cross-layer interaction with the video applications for true link aware network operations.
- Interface with the Video Service Control subsystem. It is used to exchange information related to the fact that a handover is going to happen (or has ended) so the video quality parameters can be loosened or otherwise adapted before and/or during the process and then recovered after the procedure. It is also used to gather knowledge about the different IP flows a service/application is composed of and whether IP address continuity is required for those.

The pictures below depict the subsystem's modules, mapping functionalities into devices and including interfaces with external modules.

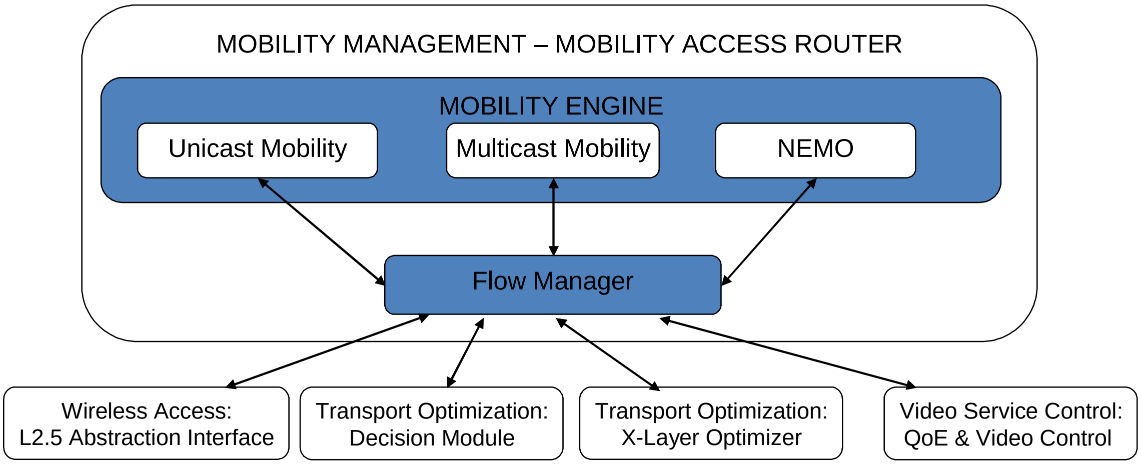
MOBILITY MANAGEMENT – MOBILITY ACCESS ROUTER
MOBILITY ENGINE
Unicast Mobility
Multicast Mobility
NEMO
Flow Manager
Wireless Access: L2.5 Abstraction Interface
Transport Optimization: Decision Module
Transport Optimization: X-Layer Optimizer
Video Service Control: QoE & Video Control

Figure 7: MAR modules and external interfaces

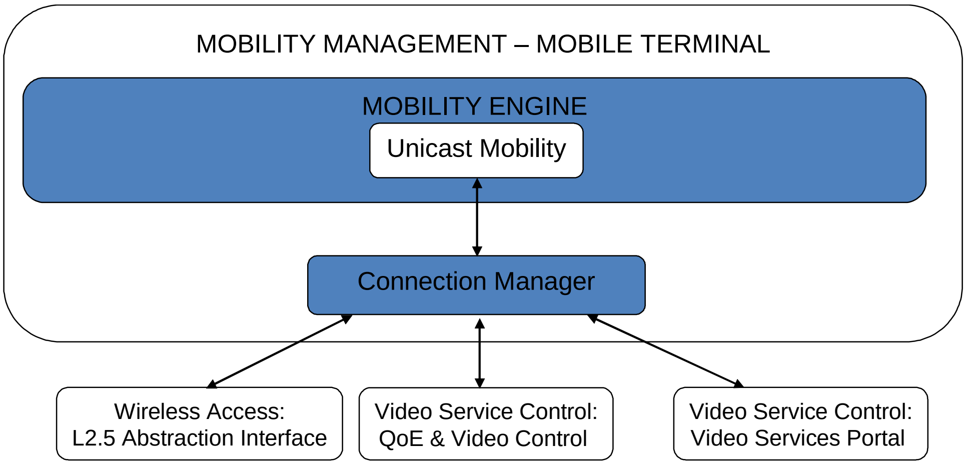
MOBILITY MANAGEMENT – MOBILE TERMINAL
MOBILITY ENGINE
Unicast Mobility
Connection Manager
Wireless Access: L2.5 Abstraction Interface
Video Service Control: QoE & Video Control
Video Service Control: Video Services Portal

Figure 8: MN modules and interfaces

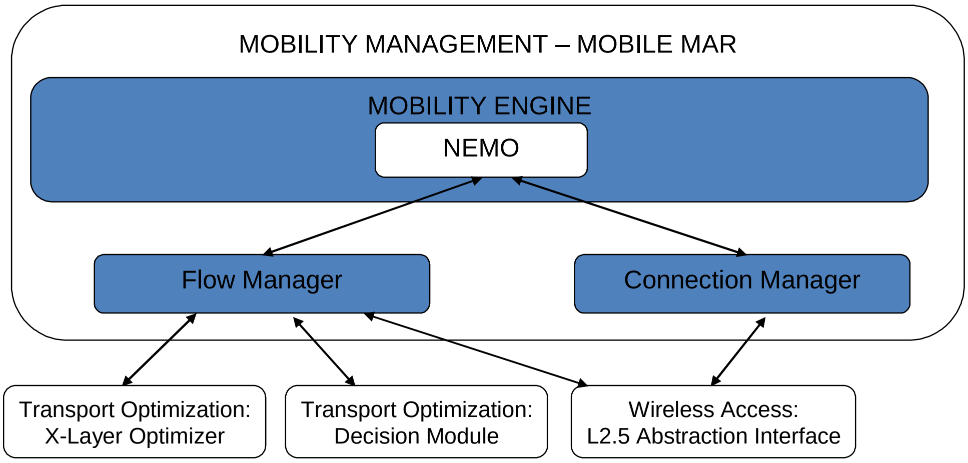
MOBILITY MANAGEMENT – MOBILE MAR
MOBILITY ENGINE
NEMO
Flow Manager
Connection Manager
Transport Optimization: X-Layer Optimizer
Transport Optimization: Decision Module
Wireless Access: L2.5 Abstraction Interface

Figure 9: mMAR modules and interfaces

5.2 Distributed and Dynamic Mobility Management concept

As stated in the previous section the MEDIEVAL mobility architecture leverages the split between local and global mobility management. Local mobility management is achieved by means of network-based mobility protocols while the global mobility management solution is achieved by means of client-based mobility solution (used for both inter LMD intra domain handover and inter-domain handover). Also, Section 3.2 illustrates four different levels of mobility anchors distribution and Section 4.1 suggests the AR level model as the most suitable scenario.

Based on these assumptions we now proceed in defining the key building blocks of the DMM approach.

Control/Data Plane Split. Traditionally, IETF mobility protocols combine the data plane and the control plane. In other words, the same communication channel is used to send binding updates as well as data traffic. In a distributed approach we could envision the split of the data plane (routing) and the control plane. A central function could maintain the control of connected nodes in the access network and could manage the routing setup of mobile devices roaming across the access network. As an example, if we consider PMIP, it would mean that the MAGs contact the LMA for sending binding updates and that IP address allocation is done directly at the MAG level. The LMA keeps track of the location of the terminal and of the associated MAGs. Conversely the central function can be distributed on each mobility anchor keeping the association control/data plane. In this case a protocol for coordination of the different mobility anchors is required. The MEDIEVAL project selected the fully distributed approach.

Dynamic Mobility Management. Traditionally, IP mobility support is enabled by default even for applications that do not require a seamless mobility service. This functionality, taking into account the applications requirements, aims at enabling the seamless service only for applications that need to survive an IP address change. In case the application (e.g., progressive download) can survive an IP address change when the MN is connected to the new mobility anchor, standard IPv6 address configuration takes place. In case the application has strict seamless service requirements, the DMM protocol will help in establishing the tunnelling overlay for packet forwarding between the A-MAR and the S-MAR. The cross-layer interaction of the CM with the application layer helps in seamlessly managing IP flows.

Flow Mobility Support. The concept of flow mobility has been well investigated for the core level anchoring model. In case of AR level anchoring model, flow mobility mechanisms are implemented according to the Dynamic Mobility Management requirement. The typical example is a MN simultaneously connected to the same mobility anchor offering both LTE and WiFi wireless access and, for a radio coverage issue, the MN has to connect to a different WiFi mobility anchor. In this case, the A-MAR can split ongoing connections over the LTE access and the new WiFi mobility anchor (provided that a tunnelling overlay is proactively established between the two anchors). It should be noted that under normal operations the MN configures a local IPv6 address and that new applications will be selecting the freshly configured IP address to start new communications.

IP Source Address Selection. The MN potentially has several IPv6 addresses configured at the same time. The MN should be able to use enhanced source address selection to pick up the most convenient IPv6 address. In addition, the network should be able to colour prefixes aiming at deprecation of the obsolete prefixes. Such mechanisms can be implemented as part of the neighbour discovery protocol upon network attachment. Unicast Router Advertisements could contain information on what prefixes have to be deprecated over the specified link.

MN to MAR Interface. The MN needs to communicate to the network its current IPv6 addresses to let the new mobility anchor to contact the old mobility anchor for seamless service. This can be achieved through extensions to the neighbour discovery protocol or via external protocol such as the IEEE 802.21. In the context of MEDIEVAL the IEEE 802.21 solution has been selected; however from an IETF standpoint we will provide additional solutions.

5.3 Bootstrapping

In Mobile IPv6 terminology the bootstrapping phase is the phase during which the MN authenticates itself towards the anchor and acquires all the parameters necessary to the mobility operations.

MEDIEVAL mobility solution relies on network-based mobility management in the local domain and on client-based mobility solution in the global domain (i.e. for handover between different administrative domains or different LMDs).

As stated in RFC5213 [11], when the MN attaches to a link connected to the MAG the deployed access security protocols on that link should ensure that the network-based mobility management service is offered only after authenticating and authorizing the mobile node for that service.

The security architecture used for network access authentication is out of scope of the MEDIEVAL project.

In case of a traditional client-based mobility solution the MN needs to know the Home Agent Address, the Home Address and he must share a security association with the configured Home Agent. DSMIPv6 provides methods to dynamically discover Home Agent Address (e.g., DHCP or DNS), to dynamically receive an Home Address (e.g., via Binding Update message) and to dynamically set up a security association with the Home Agent (e.g., IKEv2 with EAP-based authentication).

In case of DMM and MEDIEVAL architecture the client-based mobility solution is only used for inter-LMD handovers and for inter-domain handovers.

In case of inter-LMD handovers the MN moves to a LMD belonging to his Home provider but that, for some reasons, cannot be integrated with the previous domain. The Home provider is in this case both mobility provider and access provider.

In the case the MN has an already active session with a MAR (A-MAR) when crossing LMDs, he must dynamically activate the mobility service with the A-MAR using the client-based mobility solution. Once in the new LMD old communications that need mobility continue to be anchored to the A-MAR while new communications start using the address received in the new LMD and its mobility service. No bootstrapping functions are required for this scenario.

In case of inter-domain handovers the MN moves to a different administrative domain where he cannot use any mobility service: the new domain is used as an access service provider but not as a mobility provider. We can distinguish two cases:

- The mobile node attaches in the foreign domain.
- The mobile node has an already active session in its home domain and handovers to the foreign domain.

In case of attachment in the foreign domain, the MN needs to discover a suitable Home Agent. In this case, solutions as the ones described for standard DSMIPv6 (e.g., discovery based on DNS and security association negotiated via IKEv2) can be used. The mobile node behaves like a standard DSMIPv6 client and discovers a Home Agent in its home domain (it could be a centralized Home Agent deployed for this use). No DMM solution can be applied to this scenario because if the MN attaches in the foreign domain the MN must use the mobility service provided by its home provider and so it must anchor to its domain Home Agent (HA).

In case of an MN that handovers to a foreign domain, the MN has an already active session with a MAR (A-MAR) in its home domain and, consequently, it has an already active Home Address. In this case, it must dynamically activate the mobility service with the A-MAR and, after the handover, communicate the new Care-of-Address to the A-MAR itself.

5.4 Connection Manager operations

The MEDIEVAL Connection Manager, depicted in Figure 10, is located in the MN and it acts as an MIH client.

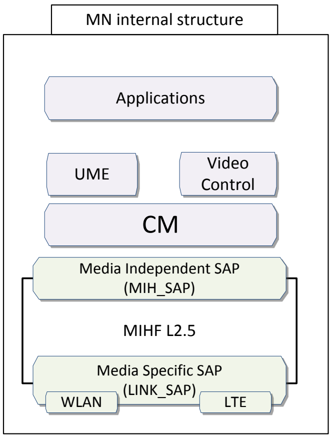

Figure 10: CM and MN internal interaction

The CM is capable of handling the access technologies in the terminal such as powering on and off of network devices, performing scans and monitoring link layer conditions. The CM detects radio coverage issues and can send mobility triggers to the appropriate module. In addition, it can perform access network discovery to select handover candidates. Given the nature of the heterogeneous wireless access the CM leverages the IEEE 802.21 protocol to achieve the above functions.

The CM is capable to retain user profile and preferences for interface management (e.g., by combining location with previously visited networks). This information can be combined with information received by the network or can be overwritten by the network itself.

The CM receives network decisions and associated policies and acts upon. This principle is valid for session establishment and for session mobility. The corresponding peer is the FM and the communication exchange is based on the IEEE 802.21 protocol.

The CM has an interface with the local OS and is capable to drive host behaviour (e.g., network configuration, battery consumption, CPU load). Although not specified in the formal interfaces specifications the CM leverages the Netlink-Socket[1] Linux implementation to achieve the above functionalities.

The CM allows to exchange application triggers (e.g., application start/stop, notification for requirements) and to provide notification of selection decision from the CM towards applications (i.e., to let the applications change their behaviour if it is appropriate). The CM allows the applications to register with itself to receive general purpose notifications. In addition, the CM behaves as a message routing entity in the MN allowing cross-layer interaction between the different layers of the ISO OSI stack. The CM should be regarded as the referee for the all the connection related procedures.

Although security is not in scope of the MEDIEVAL project, from a conceptual point of view the CM manages the authentication procedures preceding any IP configuration method. For instance, the mentioned EAP SIM mechanism for WiFi trusted access would be part of any security module implemented by the CM.

The CM, as MIH client, implements at least the following functions:

- **Getting network access**: the CM is responsible to perform network attachment and configure an IP address (or multiple IP addresses) over a given network device.

[1] Netlink socket manual page, http://www.kernel.org/doc/man-pages/online/pages/man7/netlink.7.html

- **Starting an application**: the CM exchanges with the relevant modules to provide the necessary information to video-enabled MEDIEVAL applications. In case of legacy applications, extensions to current socket APIs have to be implemented. The CM leverages the specificity of a given wireless access to bootstrap video applications.
- **Trigger a MIHO**: the CM is responsible to trigger a video aware mobile initiated handover when the required conditions are verified.
- **Support a NIHO**: the CM should support a video aware network controlled handover initiated by the network.
- **Disconnect from the network**: the CM should support network detachment of a network device and subsequent IP address release.

An example of a functional architecture of a Connection Manager is given in Figure 10. The Connection Manager supports the functions described above and it implements interfaces with all the involved actors (e.g., user, application, operator) and with other functional modules on the terminal (i.e., access monitoring, mobility management protocol, etc.). The CM is the enabler for cross-layer interaction between the different layers of the protocol stack and the MEDIEVAL video applications.

5.5 Flow Manager operations

The Flow Manager (FM), depicted in Figure 11, acts as an MIH client and is located at the MAR. The FM is involved in all mobility procedures and has interfaces with internal Mobility subsystem modules as well as with external modules defined in Wireless Access and Transport Optimization subsystems. The FM implements functions for both data plane and control plane management.

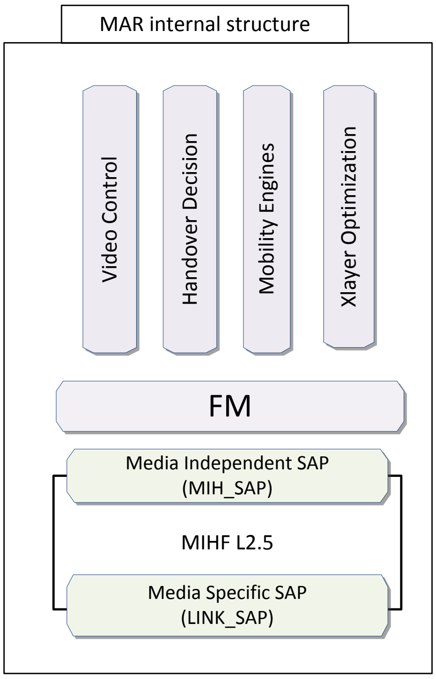

Figure 11: FM and MAR internal structure interaction

To comply with the functional behavior of the MME entity in the context of the Evolved Packet Core, the FM implements part of the session management and bearer setup upon network attachment and handover procedures. People skilled in the art will certainly find in the current MEDIEVAL specifications the main principles defined by the 3GPP standardization body.

Being defined as an MIH client (and part of the control plane mobility management), the FM implements the IEEE 802.21 protocol and is the control logic of all Mobility subsystem operations. For internal Mobility interactions, the FM exchanges signalling messages with the CM located in the MN and keeps handover status for each connected mobile device. The handover procedure can be initiated by the mobile device, denoted as *mobile initiated and network supported handover*, or it can be initiated by the network (FM), denoted as *network initiated and mobile assisted handover*. The procedures defined in the standard IEEE 802.21 protocol are enhanced with MEDIEVAL specific extensions in particular for the interaction with the Unicast Mobility Engine (DMM support).

During the handover procedures, the FM interacts with the Decision Module (DM) in the Transport Optimization subsystem. The key innovation is to validate the handover candidates considering the video content currently being consumed by a given mobile device. In fact, in addition to the check about available resources on the target PoA (through IEEE 802.21 signalling), the FM also validates the PoA from a content perspective. This is a key feature when deploying CDN in the cellular core and access network. We argue that this allows an efficient management of the cached content triggering reactive procedures upon user mobility.

The FM also controls the radio bearer establishment during the handover phase. To this end the FM exchanges messages with the Wireless Access Abstract Interface modules collocated at the MAR and instructs the low layers to open the radio bearer when requested. Considering that the MAR can support heterogeneous wireless technologies the same methods apply to the WiFi configuration, although the 802.21 messages are differently mapped to the device drivers.

The FM can receive triggers from Transport Optimization subsystem (X-layer Optimization module) to leverage mobility procedures as a mean of network optimization.

As part of the handover execution, the FM is in charge of triggering the mobility engine modules for seamless session support. It should be noted that another key innovation is to enable mobility in a dynamic way and only upon request (as part of the session description). That is, PMIP engine is triggered only when conditions are met and if not the handover procedures are completed with no seamless service support.

As mentioned earlier, the FM also participates in the session establishment of each video service and, upon exchange with Transport Optimization subsystem, it keeps track of the session setup specific parameters. Considering that the Transport Optimization subsystem has an application level view, the FM needs the specific information about the session to map all the IP flows related to a given application. For instance, if an application has two IP flows, one for the control plane and one for the data exchange, the FM must be capable of grouping both flows to the same session. To this end, during the session setup of a MEDIEVAL service, the FM is contacted by the Transport Optimization subsystem modules on the new session freshly started. Based on this information the FM is capable to route the IP flows and to keep track of the required information. It should be noted that the FM is able to classify each flow and implements the following functionalities:

- Flow add function: if the 6-tuple (5-tuple plus the transport type) parameters extracted from data packets refer to a new flow, an ”add flow” request is sent to the mobility engine, which first checks if the destination prefix is consistent with those stored in the MAR. If succeeded, it then replies to the FM indicating the flow-ID generated and the interface-ID used for that flow, otherwise no indication is provided, meaning that the flow cannot be processed/routed. Upon receiving the reply, FM stores in the flow table this new stream with the related parameters, i.e. the 6-tuple, the flow ID and the interface used. In the meantime the packet is waiting in the queue for a signal by the FM.
- Mark verdict function: the signal can be a mark verdict if a suitable flow-ID is provided (in this case the mark will be exactly the flow-ID), or a void verdict in case of empty response by the mobility engine. If the 6-tuple corresponds to an existing flow, then communication with the mobility engine is not necessary and the packet is marked with the related flow-ID.
- Flow handover function: a flow table stores the interface-ID through which the flow is currently forwarded. When the flow has to be seamlessly moved (the FM can receive external triggers), the request dispatcher on the FM side sends a ”move” request indicating the flow-ID and the interface in use. The request dispatcher on the mobility engine side checks for the availability of alternative interfaces for that MN in its internal data structure. If the lookup succeeds, the rule manager function adds a ”fwmark-rule” pointing to a route that specifies as default device the interface retrieved before. After this rule is set, the packets are forwarded through the new interface, bypassing the default route based on longest prefix matching method.
- Flow delete function: both the FM and the mobility engine can delete a flow by issuing a “del message”. The command will delete the forwarding rule in the special purpose routing table. The FM can delete a

flow based on timer expiration for an existing entry in the FM table, while the mobility engine can delete a flow based on the network detachment of a mobile device (and subsequent binding table update).

5.6 Unicast Mobility Engine

The mobility operations for unicast flows comprise a large number of messages and actions that can be divided into two main categories:

- Handover control. These operations are related to the procedure required for a Make-Before-Break handover: signal power sensing, best PoA selection, resource preparation, detachment/attachment detection, link establishment, IP configuration and resource release. This phase is assisted and controlled by means of IEEE 802.21 infrastructure and Neighbour Discovery signalling. This is performed each time the mobile terminal is forced to change its PoA regardless the reason.
- IP address continuity. This is related to maintaining reachable the IP address acquired by an MN upon changing the access router. Previous serving MARs are informed by means of a Proxy Binding Update (PBU) and Proxy Binding Acknowledgment (PBA) handshake when the MN is roaming inside an LMD, or Binding Update and Binding Acknowledgment exchange when the MN does not have direct access to the LMD. This phase is not always necessary and can be skipped according to applications' requirements. However, the deliverable covers the case in which IP continuity service is always provided, so that even those applications which can survive an address change will not suffer a sudden disruption of the communication before refreshing the session with the new IP address. This feature is not mandatory but it is considered here for the sake of homogeneity in the description.

The proposed flat architecture requires a network node playing both roles of access router and mobility anchor, here called Mobility Access Router (MAR). It is the router in the access network seen by the terminal as the first IP hop and default gateway; it is also the mobility anchor for the flows started in its network, as it inherits features of its centralized counterparts as the Home Agent (HA) and the Local Mobility Anchor (LMA) to provide the mobility support. In addition, for the proposed scheme, a MAR is also equipped with the functions of a Mobile Access Gateway (MAG) for its capability of using mobility messages as PBU/PBA.

The picture below, Figure 12, depicts the reference high level architecture components as described in Section 5.1, but focusing on the unicast mobility case only. Following subsections are devoted to the detailed description of the operations.

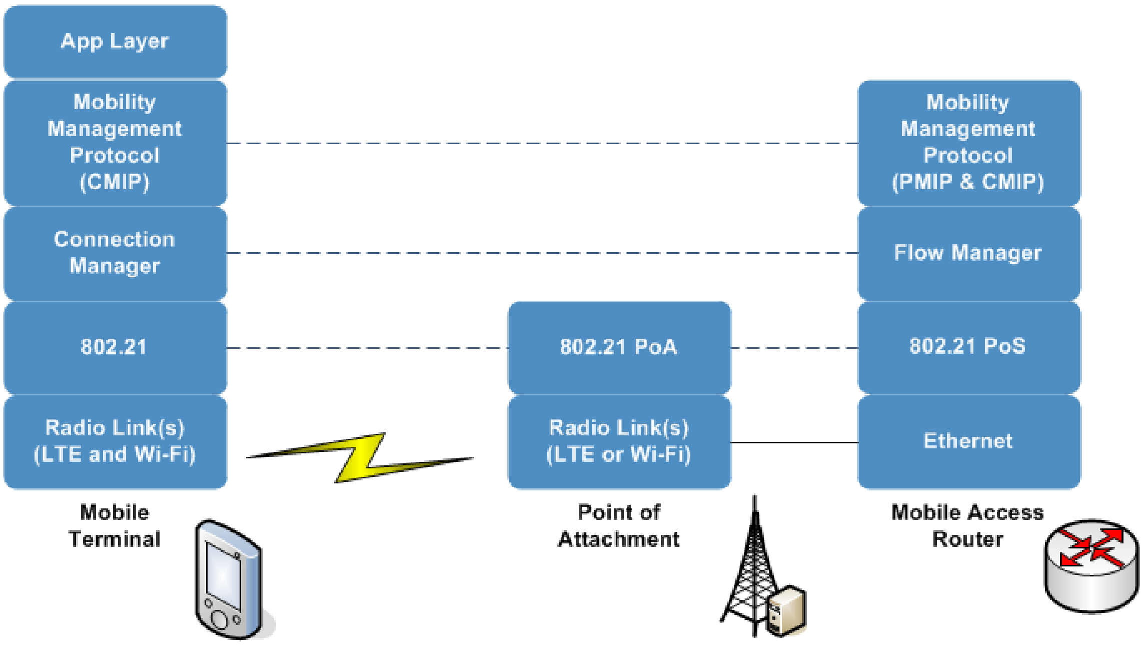
App Layer
Mobility Management Protocol (CMIP)
Connection Manager
802.21
Radio Link(s) (LTE and Wi-Fi)
Mobile Terminal
802.21 PoA
Radio Link(s) (LTE or Wi-Fi)
Point of Attachment
Mobility Management Protocol (PMIP & CMIP)
Flow Manager
802.21 PoS
Ethernet
Mobile Access Router

Figure 12: Reference Architecture

5.6.1 Mobility Access Router operations

The Mobility Access Router handles terminals' mobility whether they are roaming inside the LMD or not. In the former situation, besides the handover control functions, it runs services intrinsic of an access router, an LMA and a MAG, provided according to the flows' needs. In the latter case it runs the functionalities of a HA. Here is the list of operations performed by MARs (for related MSCs refer to Figure 13, Figure 14 and Figure 15):

1. Upon MN's attachment to a link connected to the MAR, the implemented access security protocols on that link should ensure that the network-based mobility management service is offered only after the mobile node is authenticated and authorized for the service, similarly to what happens when attaching to a MAG. After the AAA procedures, the MAR registers the MN in a database called Binding Cache and assigns a unique IPv6 prefix to the mobile node issuing a Router Advertisement. The prefix is used by the MN to configure an address and is kept routable by the MAR, which forwards packets to/from the MN without encapsulation or special packet handling.

2. The Flow Manager accepts notifications by the Transport Optimisation subsystem (X-Layer Optimisation)(XLO) through an API-based protocol and also registers to remote MIHF Event Service (see [4]) in the terminal, to detect when the MN is moving. These are the procedures to accept triggers respectively for Network-Initiated (NIHO) and Mobile-Initiated (MIHO) handovers. In the following steps, whenever NIHO and MIHO operations differ, the NIHO case is considered first. A dedicated step is hence added for MIHO as alternative operation.

3. A NIHO is waved upon a `FM_XLO_CongestedNetwork.request` message is received from the XLO module in the MAR. The next action is the target selection. The FM gets the information about MN's surrounding candidate PoAs from the MIIS, through the `MIH_Get_Information` primitives exchange. The FM solicits a scan report of those PoAs to the MN via the `MIH_Net_HO_Candidate_Query` messages.

    a. A MIHO is triggered by a `MIH_MN_HO_Candidate_Query.request` message issued by the MN, after it has performed the aforementioned operations

4. Upon receiving the scan result, the FM queries the resource availability for the sensed PoAs contacting the corresponding PoSs in the C-MARs with the `MIH_N2N_HO_Query_Resources` messages. This message contains the IP address of the current S-MAR. The message should be extended to include the list of A-MARs' IP addresses too. The addresses are used later by the T-MAR for the IP mobility signalling. The FMs in the C-MARs send back the response to the resource query.

    a. In the MIHO case a `MIH_MN_HO_Candidate_Query.response` is sent back to the MN to conclude the exchange.

5. The list with the subset of available PoAs is forwarded by the FM to the X-Layer Optimisation using the `DM_FM_HO_Decision` messages, including the set of flows involved in the handover. The FM gets back the same list with the PoAs re-ordered according to the DM decision algorithm.

6. The FM selects the target PoA for the handover according to all the data gathered. After the decision, it negotiates with the `MIH_N2N_HO_Commit` messages the resource allocation with the FM in the T-MAR. After the task is accomplished by the remote FM, the local FM forces the MN to switch PoA issuing a `MIH_NET_HO_Commit` command to the CM. Also, the FM informs the QoE engine of the Video Services Control subsystem that a handover imminent for some flows in downlink using the messages `FM_QoEVC_HOCommit`. According to the information received by the terminal in the preparation phase, the MN knows whether the PoA belongs to the LMD or not. In the former case see next step, otherwise skip to step 8.

7. Upon detecting the attachment by means of `MIH_Link_UP` events, the FM in the T-MAR (now the S-MAR) triggers the mobility operations using the `FM_UME_ActivateMobility` messages. The current S-MAR signals with a `Proxy Binding Update` (PBU) message to the P-MARs the MN's Care-of Address, i.e. the S-MAR's IP address. P-MARs reply with a `Proxy Binding Acknowledgment` (PBA) message and they update their entry in the BC for the MN with the binding between the prefix they advertised to the MN and its current location. Tunnels are

established between the MARs and the flows are redirected through the tunnels, without changing the IP addresses pair in the communication. The success of the task is indicated to the FM that now is ready to receive a MIH_MN_HO_Complete message from the MN that is translated into a MIH_NET_HO_Complete primitive and sent to the FM in the previous MAR. This triggers the old S-MAR to free the resources allocated to the MN that now is no more attached to it, When a response to such message is received the procedure is over, and the Video Control Services subsystem is notified through FM_QoEVC_HOComplete messages.

8. When the MAR is handling mobility for terminals outside the LMD, it acts as a Home Agent. Since MIHF and/or network-based DMM are assumed to be not fully supported in the foreign domain (e.g. the MN might enter a totally different architecture, or an LMD disjoint with the previous one), a host-based mobility management is adopted, and MARs anchoring flows negotiate mobility support directly with the MNs by means of a Binding Update (BU) message sent by the MN and a Binding Acknowledgment (BA) message sent as response. A MAR turns into an HA when it receives a BU, and it releases the resource formerly allocated upon receiving a MIH_MN_HO_Complete message. Although a DSMIPv6-like approach is used, mobility management remains distributed and dynamic in nature because an MN might have more than a single HA, and might start new communication without traversing the original domain (e.g., when the non-LMD belongs to the same authoritative entity as the LMD). However, if such communications require IP mobility the MN should use the host-based mobility scheme and not rely on the foreign mobility architecture.

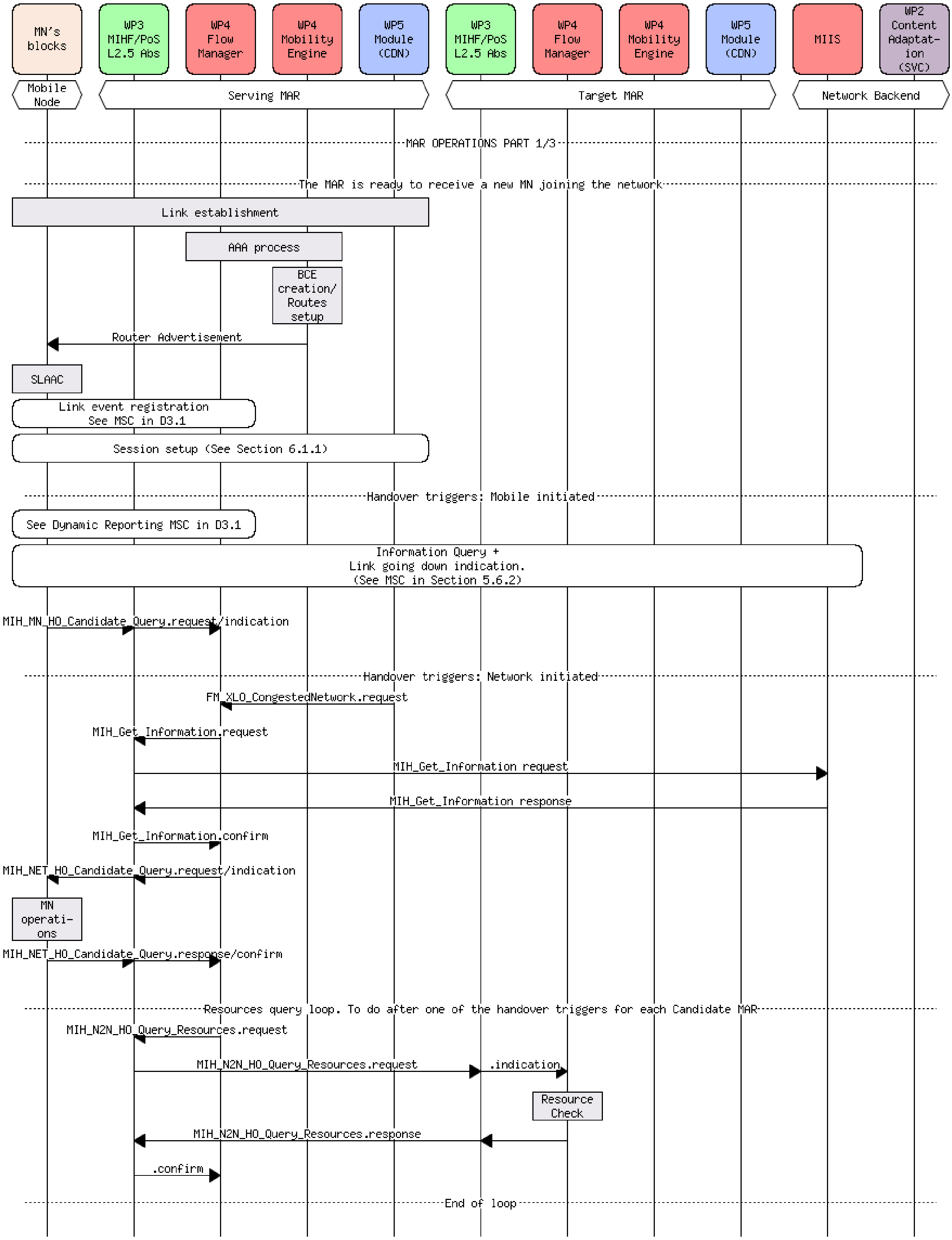
MN's blocks
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 Module (CDN)
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 Module (CDN)
MIIS
WP2 Content Adaptat-ion (SVC)
Mobile Node
Serving MAR
Target MAR
Network Backend
MAR OPERATIONS PART 1/3
The MAR is ready to receive a new MN joining the network
Link establishment
AAA process
BCE creation/ Routes setup
Router Advertisement
SLAAC
Link event registration See MSC in D3.1
Session setup (See Section 6.1.1)
Handover triggers: Mobile initiated
See Dynamic Reporting MSC in D3.1
Information Query + Link going down indication. (See MSC in Section 5.6.2)
MIH_MN_HO_Candidate_Query.request/indication
Handover triggers: Network initiated
FM_XLO_CongestedNetwork.request
MIH_Get_Information.request
MIH_Get_Information request
MIH_Get_Information response
MIH_Get_Information.confirm
MIH_NET_HO_Candidate_Query.request/indication
MN operati-ons
MIH_NET_HO_Candidate_Query.response/confirm
Resources query loop. To do after one of the handover triggers for each Candidate MAR
MIH_N2N_HO_Query_Resources.request
MIH_N2N_HO_Query_Resources.request
.indication
Resource Check
MIH_N2N_HO_Query_Resources.response
.confirm
End of loop

Figure 13: MAR operations message sequence chart (part 1/3)

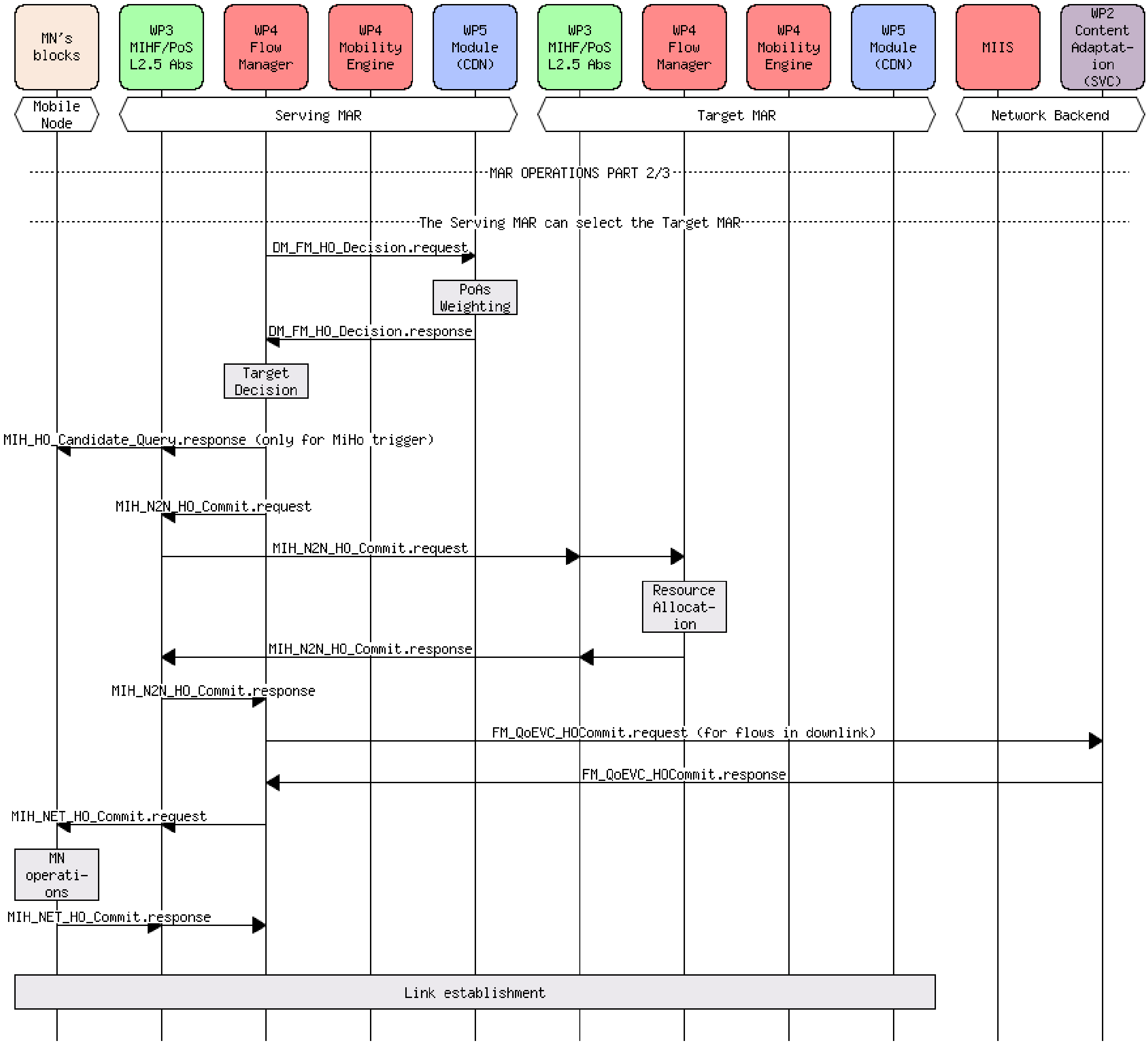
MN's blocks
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 Module (CDN)
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 Module (CDN)
MIIS
WP2 Content Adaptat-ion (SVC)
Mobile Node
Serving MAR
Target MAR
Network Backend
MAR OPERATIONS PART 2/3
The Serving MAR can select the Target MAR
DM_FM_HO_Decision.request
PoAs Weighting
DM_FM_HO_Decision.response
Target Decision
MIH_HO_Candidate_Query.response (only for MiHo trigger)
MIH_N2N_HO_Commit.request
MIH_N2N_HO_Commit.request
Resource Allocat-ion
MIH_N2N_HO_Commit.response
MIH_N2N_HO_Commit.response
FM_QoEVC_HOCommit.request (for flows in downlink)
FM_QoEVC_HOCommit.response
MIH_NET_HO_Commit.request
MN operati-ons
MIH_NET_HO_Commit.response
Link establishment

Figure 14: MAR operations message sequence chart (part 2/3)

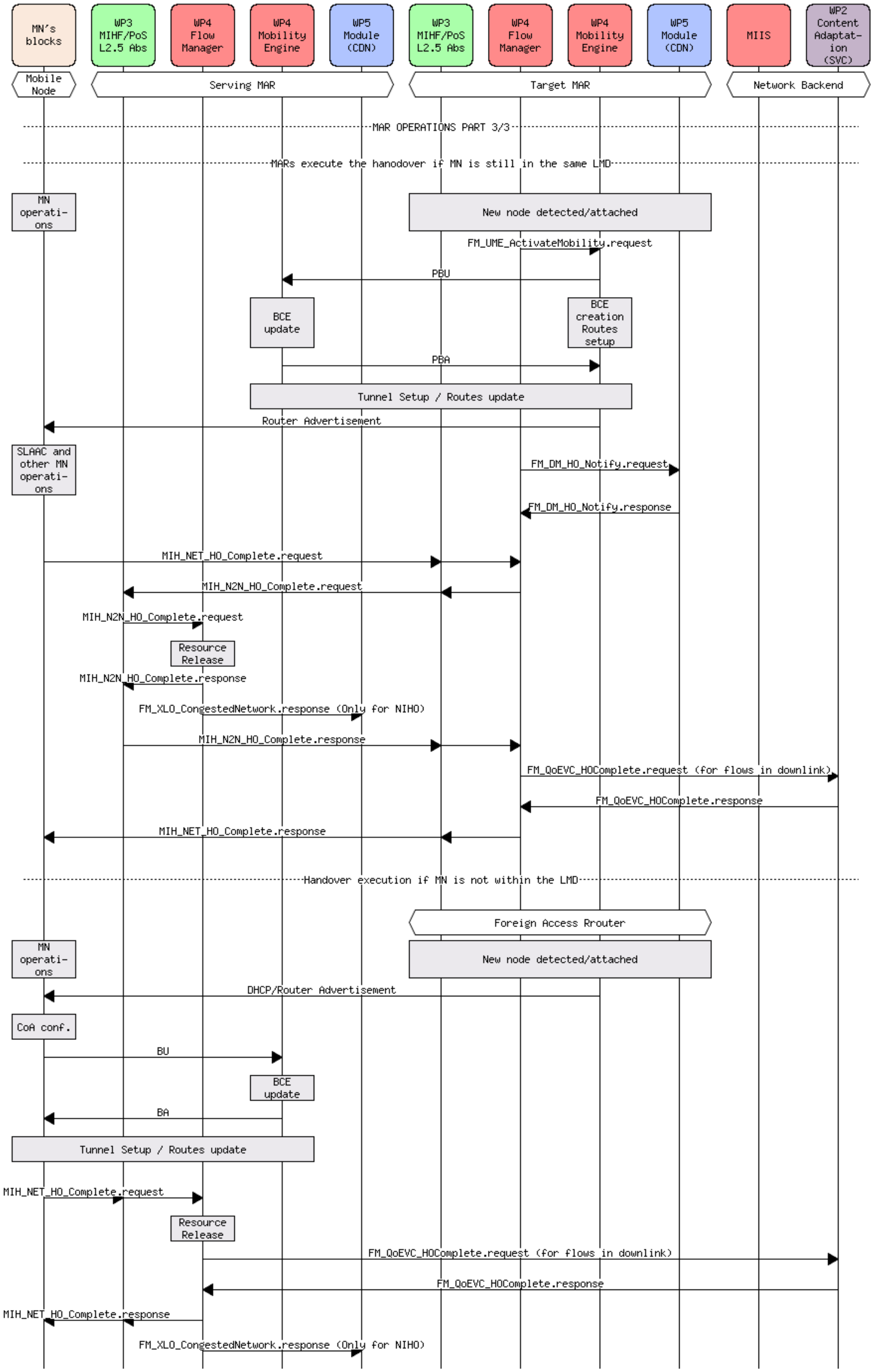
MN's blocks
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 Module (CDN)
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 Module (CDN)
MIIS
WP2 Content Adaptat-ion (SVC)
Mobile Node
Serving MAR
Target MAR
Network Backend
MAR OPERATIONS PART 3/3
MARs execute the hanodover if MN is still in the same LMD
MN operati-ons
New node detected/attached
FM_UME_ActivateMobility.request
PBU
BCE update
BCE creation Routes setup
PBA
Tunnel Setup / Routes update
Router Advertisement
SLAAC and other MN operati-ons
FM_DM_HO_Notify.request
FM_DM_HO_Notify.response
MIH_NET_HO_Complete.request
MIH_N2N_HO_Complete.request
MIH_N2N_HO_Complete.request
Resource Release
MIH_N2N_HO_Complete.response
FM_XLO_CongestedNetwork.response (Only for NIHO)
MIH_N2N_HO_Complete.response
FM_QoEVC_HOComplete.request (for flows in downlink)
FM_QoEVC_HOComplete.response
MIH_NET_HO_Complete.response
Handover execution if MN is not within the LMD
Foreign Access Rrouter
MN operati-ons
New node detected/attached
DHCP/Router Advertisement
CoA conf.
BU
BCE update
BA
Tunnel Setup / Routes update
MIH_NET_HO_Complete.request
Resource Release
FM_QoEVC_HOComplete.request (for flows in downlink)
FM_QoEVC_HOComplete.response
MIH_NET_HO_Complete.response
FM_XLO_CongestedNetwork.response (Only for NIHO)

Figure 15: MAR operations message sequence chart (part 3/3)

5.6.2 Mobile Node operations

When moving within the same LMD, the mobile node configures an IPv6 address per each IPv6 prefix advertised by the MARs. Since the MAR routes directly (i.e., no tunnels) packets carrying the address configured using the prefix advertised, an MN should always start new communications with that address. For this reason, after several handovers, an MN might keep flows anchored at different MARs. The Connection Manager is the entity in charge of enforcing mobility support for those flows which require it, as address continuity might not always be requested. Applications which can survive IP address change (i.e., which do not necessitate IP continuity) usually work opening and closing consecutive IP sessions (e.g., web browsing), so sooner or later they will start connections with a fresh IP address. Still, IP continuity gives some benefits to such applications because the ongoing flow is not suddenly cut off, but it is driven to its normal end instead. For applications that can survive an address change but use a single stream for the communication (i.e., they will try to use the old address as long as possible, even if the new one leads to shorter path/delay), there should be an intelligence in the CM informing the application that the new address is preferred over the old one.

Upon crossing the LMD boundaries, the MN activates the mobility client and signals its location change directly to all the MARs that are anchoring the flows it wishes to keep alive. Therefore, a tunnel is established with those MARs, and, according to the foreign domain policy, either packets belonging to new communications must be encapsulated and forwarded though the tunnels or they might be routed directly by the foreign serving gateway using the new address. However, for flows requiring mobility, the host-based scheme should be preferred over the mobility support offered by the foreign architecture.

The list of MN operations is presented below (for details on related MSCs refer to Figure 16, Figure 17 and Figure 18). Please note that the MIHO case is presented here as the default working scheme, while a separated alternative step is included when the NIHO procedure differs.

1. After bootstrapping and AAA, the MN configures its IP address (with SLAAC or DHCPv6) from the prefix advertised by the MAR. The Connection Manager is the MIH user in the terminal in communication with the MIH user in the MAR (the FM). If the MN is multihomed to different MARs through both its interfaces, it has interactions with two PoSs residing in different MARs. MARs handles LTE and Wifi PoAs and the MN might be connected to the same MAR through both radio links. In this case the MN configures the same IP address on both IFs (the Logical Interface copes with the management of addresses and IFs) and in principle sees only one PoS (for the actual details refer to the IEEE 802.21 standard).
2. The CM monitors the status of the links by means of the MIH services offered by lower layers (see [4]). Upon crossing a pre-configured power level threshold, the CM is informed by the L2.5 abstraction module with a `MIH_Link_Parameters_Report.indication` message. The CM queries the MIIS about the surrounding PoAs using the `MIH_Get_Information` messages, and performs a scan looking for those PoAs. The information collected is transmitted to the FM issuing a `MIH_NET_HO_Candidate_Query.request` message. This is the event that triggers a MIHO resource preparation.
    a. In the NIHO case, the MIIS is queried by the FM in the MAR. The MN is informed of the need to perform a handover when the CM receives a `MIH_NET_HO_Candidate_Query` request. The CM sends a command to lower layers to scan the PoAs obtained in the message and replies to the FM including the scan report.
3. The resource preparation is a task mainly performed by network components, thus the MN is idle until it gets a `MIH_NET_HO_Commit.request` message from the FM indicating the target PoA. Before actually switching to the new PoA, the MN negotiates with the Video Control Services subsystem the parameters of uplink videos during the handoff through `CM_QoEVC_ContentAdaptionCommit` messages exchange and finally sends `MIH_NET_HO_Commit.response` back to the FM.
4. A link is established with the new PoA and the CM is informed with a `MIH_Link_Up` event. The MN can configure an address topologically correct at the new access network.

   a. The MN knows whether the PoA belongs to the LMD or not. In the former case skip to the next step. Otherwise, the CM triggers the host-based mobility issuing a `CM_UME_ActivateMobility` to the Unicast Mobility Engine which will send a BU message to the A-MARs it wishes to maintain. When the BA message is received a tunnel can be established with MARs so that ongoing flows can be recovered through it.

5. When the IP connectivity is restored, the CM negotiates the new QoS parameters with the Video Service Control subsystem having another `CM_QoEVC_ContentAdaptionComplete` message exchange. The CM also sends a `MIH_MN_HO_Complete.request` message to the new FM so that the unnecessary resources can be freed in the network.

6. In the host-based case, this message is sent to the FM in the last visited MAR, as it is the latest access router having reserved resources for the MN and the CM cannot rely on the presence of a PoS in the foreign network.

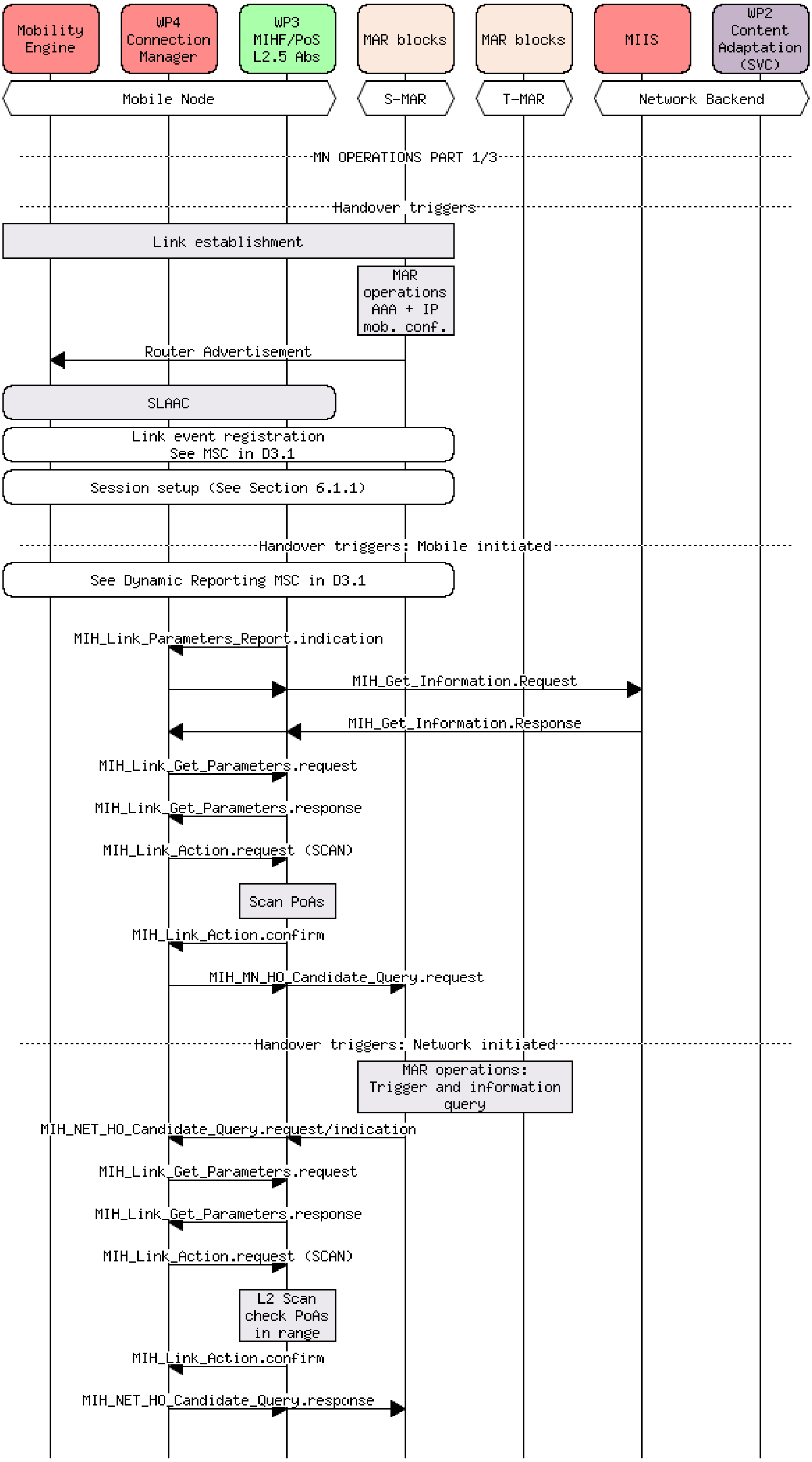
Mobility Engine
WP4 Connection Manager
WP3 MIHF/PoS L2.5 Abs
MAR blocks
MAR blocks
MIIS
WP2 Content Adaptation (SVC)
Mobile Node
S-MAR
T-MAR
Network Backend
MN OPERATIONS PART 1/3
Handover triggers
Link establishment
MAR operations AAA + IP mob. conf.
Router Advertisement
SLAAC
Link event registration See MSC in D3.1
Session setup (See Section 6.1.1)
Handover triggers: Mobile initiated
See Dynamic Reporting MSC in D3.1
MIH_Link_Parameters_Report.indication
MIH_Get_Information.Request
MIH_Get_Information.Response
MIH_Link_Get_Parameters.request
MIH_Link_Get_Parameters.response
MIH_Link_Action.request (SCAN)
Scan PoAs
MIH_Link_Action.confirm
MIH_MN_HO_Candidate_Query.request
Handover triggers: Network initiated
MAR operations: Trigger and information query
MIH_NET_HO_Candidate_Query.request/indication
MIH_Link_Get_Parameters.request
MIH_Link_Get_Parameters.response
MIH_Link_Action.request (SCAN)
L2 Scan check PoAs in range
MIH_Link_Action.confirm
MIH_NET_HO_Candidate_Query.response

Figure 16: MN operations message sequence chart (part 1/3)

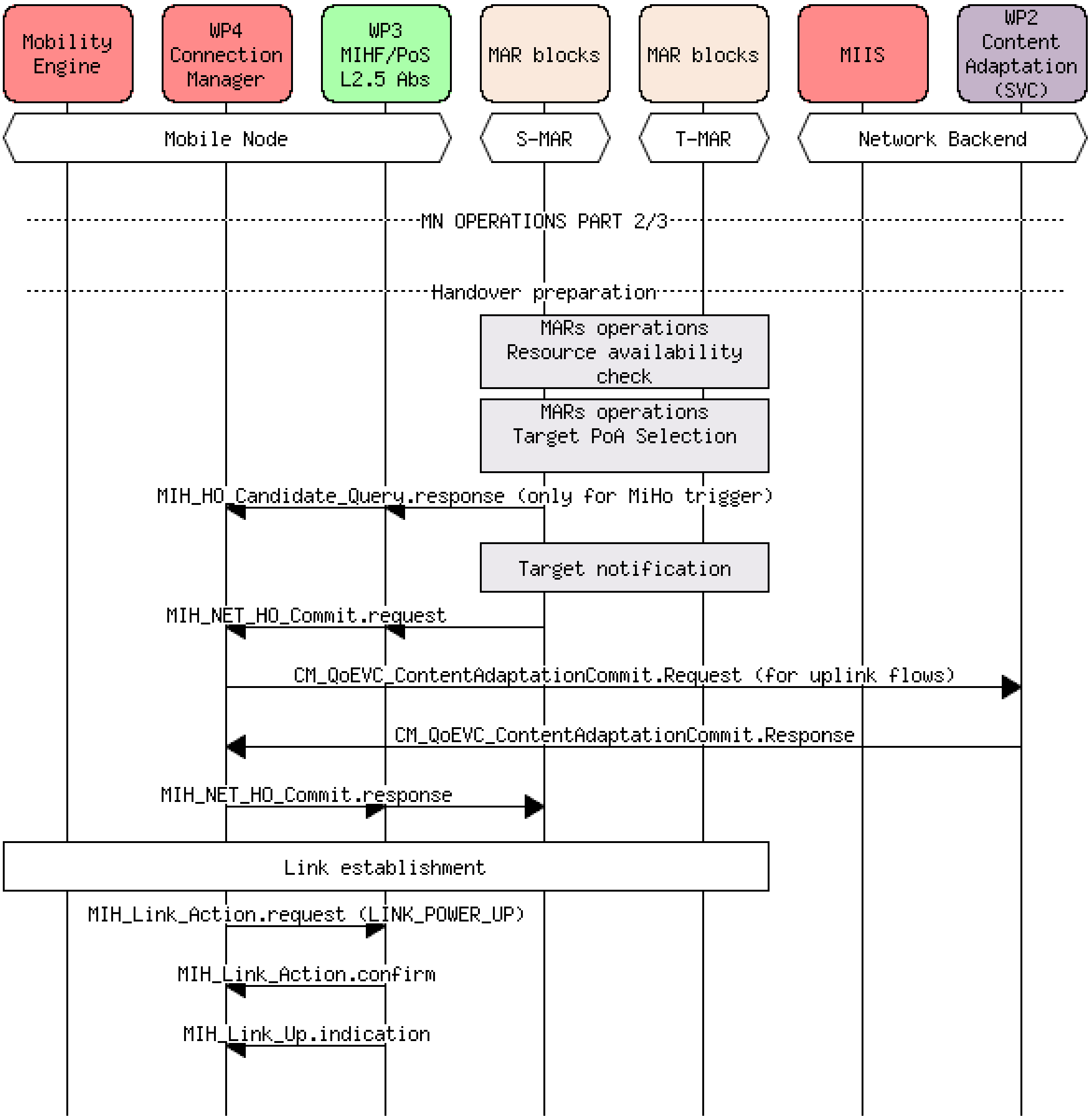
Mobility Engine
WP4 Connection Manager
WP3 MIHF/PoS L2.5 Abs
MAR blocks
MAR blocks
MIIS
WP2 Content Adaptation (SVC)
Mobile Node
S-MAR
T-MAR
Network Backend
MN OPERATIONS PART 2/3
Handover preparation
MARs operations Resource availability check
MARs operations Target PoA Selection
MIH_HO_Candidate_Query.response (only for MiHo trigger)
Target notification
MIH_NET_HO_Commit.request
CM_QoEVC_ContentAdaptationCommit.Request (for uplink flows)
CM_QoEVC_ContentAdaptationCommit.Response
MIH_NET_HO_Commit.response
Link establishment
MIH_Link_Action.request (LINK_POWER_UP)
MIH_Link_Action.confirm
MIH_Link_Up.indication

Figure 17: MN operations message sequence chart (part 2/3)

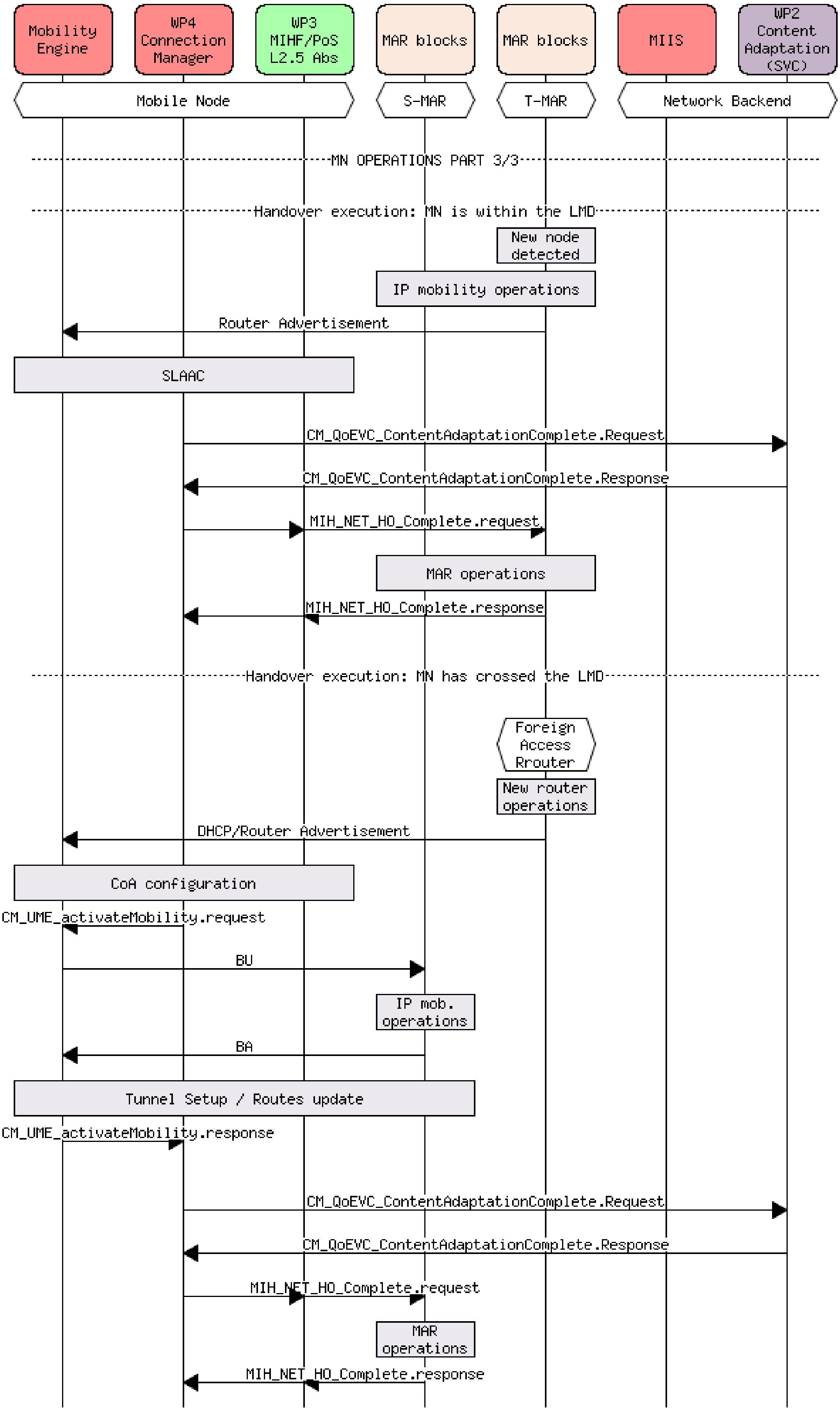
Mobility Engine
WP4 Connection Manager
WP3 MIHF/PoS L2.5 Abs
MAR blocks
MAR blocks
MIIS
WP2 Content Adaptation (SVC)
Mobile Node
S-MAR
T-MAR
Network Backend
MN OPERATIONS PART 3/3
Handover execution: MN is within the LMD
New node detected
IP mobility operations
Router Advertisement
SLAAC
CM_QoEVC_ContentAdaptationComplete.Request
CM_QoEVC_ContentAdaptationComplete.Response
MIH_NET_HO_Complete.request
MAR operations
MIH_NET_HO_Complete.response
Handover execution: MN has crossed the LMD
Foreign Access Rrouter
New router operations
DHCP/Router Advertisement
CoA configuration
CM_UME_activateMobility.request
BU
IP mob. operations
BA
Tunnel Setup / Routes update
CM_UME_activateMobility.response
CM_QoEVC_ContentAdaptationComplete.Request
CM_QoEVC_ContentAdaptationComplete.Response
MIH_NET_HO_Complete.request
MAR operations
MIH_NET_HO_Complete.response

Figure 18: MN operations message sequence chart (part 3/3)

5.7 Media Independent Information Service

The Media Independent Information Service (MIIS) provides a framework by which an MIHF, residing in the MN or in the network, discovers and obtains 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. MIIS in the network is generally a PoS-non-PoA.

The MAR, the MT or the PoAs can access the MIIS server via standard IEEE 802.21 interface to retrieve the required information.

5.8 Multicast Mobility Engine

This section shortly summarizes basic building blocks of the Multicast Mobility Engine (MUME) component. Details of IP multicast operations are part of Deliverable D4.2 [5].

In MEDIEVAL, users are expected to be most of the time roaming within a single LMD (see Section 5.1), but, in cases where this is not possible (e.g., roaming to a network owned by a different operator or running a different mobility support scheme), a host-based approach (like DSMIPv6) is followed.

When a multicast source/listener moves outside the current LMD, if a host-based scheme is applied, a point-to-point tunnel is established for multicast traffic from the A-MAR to the MN like for the unicast traffic. If many MNs attaching to the same A-MAR move outside the same LMD, many tunnels would be established to the A-MAR. The result of using point-to-point tunnels raises some multicast-related issues such as routing optimization, packet replication, etc. and in general does not bring any advantage in using multicast for video services.

For the above reasons, within the MEDIEVAL context, IP multicast mobility will be only considered in the intra-LMD case. If the mobile node changes LMD, multicast traffic will be disrupted and the mobile would need to subscribe again to the content (for the case of listener mobility) or use a different source address (for source mobility).

The Multicast Mobility Engine (MUME) is the logical module responsible for multicast operations. It is located at the MAR to make sure that the mobility process is transparent to the mobile terminal. This mobility architecture supports both multicast source and multicast listener mobility. Therefore, the MUME executes different operations for multicast source and listener.

5.8.1 Mobility Access Router operations

The Multicast Mobility Engine in MAR can be split into 4 main logical functions: multicast group management function, multicast routing function, mobility management function and multicast context transfer function.

The MAR executes the operations corresponding with these functions. The multicast group manager function refers to the multicast group management operations related to MLDv2 , such as multicast listener query/report processing to/from the attached MNs, multicast membership database management and forwarding packets. The considered multicast routing protocols are PIM-SM and PIM-SSM. The multicast routing function then corresponds to PIM-SM operations such as join/prune message processing, multicast states management, forward multicast traffic operations. For the mobility management function, the MUME executes the operations based on the operations of the LMA and MAG in PMIPv6. Finally, the multicast context transfer function allows the exchange of multicast group information between the routers, and may be allied to the mobility function resulting specifically in the integration of multicast information in the Proxy Binding Acknowledge message.

The aforementioned, MAR operations are different for multicast source and multicast listener. For multicast source, the Anchoring MAR plays the role of LMA while the current Serving MAR acts as the MAG. From a multicast scope and considering the multicast source, the A-MAR acts as a multicast router and the S-MAR as a MLD proxy, receiving the multicast traffic through one of its downstream interfaces for multicast listeners; the S-MAR acts as a MLD-proxy, performing multicast membership management and acting as a multicast Querier for its subnet and as a host for an upstream proxy or multicast router. As for the A-MAR, it will typically act as a regular multicast router.

5.8.2 Mobile Node operations

To support multicast listener, the MN performs the host part of multicast group membership protocols (IGMP for IPv4, MLD for IPv6): processes MLD reports/queries (and IGMP for IPv4). The MN also provides to the MAR parameters relevant to multicast group management of the terminal, such as group identifier (IP multicast), source address, etc. To support multicast source functionality, a modified signalling is used to inform MAR that the MN is the multicast source.

5.9 NEMO Mobility Engine

At IP level, an mMAR attaches to MARs and changes point of attachment without affecting the communications of the mobile nodes that are connected to its network. The handover phase is transparent for mobile nodes as they are not involved in updating their location. However, when an mMAR moves and joins another access network, it informs the new S-MAR about the MNs carried in its on-board network, so an individual prefix can be allocated by the MAR and relayed to them by the mMAR. This allows the MNs to start a communication traversing the closest MAR. For the specific NEMO's mMAR mobility pattern, the MIHO case is considered only. This is due to the fact that forcing a mMAR to switch PoA might result in a ping-pong effect, as the mMAR is always "on the move" and might need to handover immediately after.

5.9.1 Mobile MAR operations

The mMAR is equipped with the NEMO mobility engine that operates according to a host-based DMM solution similar to [18]. For the sake of simplicity, the 802.21 operations are omitted, as the CM's working scheme reproduce the one for the CM in the MN, and similarly, the FM works as the one residing in the MAR. Please refer to Sections 5.6.1 and 5.6.2 for the details. Hence, the operations listed below refer to the IP-NEMO mobility only.

1. The mMAR powers up and obtains a topologically correct prefix in the current access network. The MNs that joins its on-board network are registered at the S-MAR by means of a special PBU sent by the mMAR with a NEMO flag. The MAR assigns a prefix to the MN and acknowledges the operation with a PBA. The prefix is finally advertised by the mMAR to the MN. In this phase the mMAR acts as MAG registering the MN at the LMA and subsequently advertising the assigned prefix to the MN.
2. The mMAR changes PoA with the support provided by the 802.21 infrastructure as an MN does. However, the procedure differs in the IP mobility part as the mMAR is responsible for updating its location. When the mMAR establishes a link with a new S-MAR it configures a new IP address using the prefix advertised to it. This new address is communicated as CoA to its A-MARs by means of a BU message. The A-MARs reply with a BA and a bidirectional tunnel is set up. In this way, the mMAR maintains active and routable the addresses configured in the visited access network.
3. Nevertheless, when a new MAR's network is joined, the mMAR is in charge of informing the MAR about the MNs connected to the NEMO. This is required to allow the MNs to send/receive traffic with a prefix topologically correct at the new MAR, hence to benefit from traversing the closest MAR. This is obtained by the transmission of a NEMO PBU from the mMAR to the MAR per each MN attached as mentioned in step 1.
4. In general, the PoS residing in the mMAR can be contacted only by the PoS in the S-MAR, thus IP continuity can be offered only if the MN is coming from the same access network the mMAR is attached to.
5. When the MN leaves the NEMO, it either joins the same mMAR's access network, or another MAR. In the latter case the FM in the T-MAR should be provided with the current S-MAR's address and not the mMAR's.

5.9.2 Mobility Access Router operations

The MAR’s NEMO Mobility Engine is responsible for updating the mMAR’s location and MNs’ session when they are attached to the NEMO (i.e., to a mMAR connected to the MAR). This mainly involves creating proper routing entries for the mMAR and MNs in order to maintain their reachability. The list of operations is the following.

1. An mMAR that connects to one of the MAR’s links is assigned an IPv6 prefix topologically anchored at the MAR. The S-MAR should update the MIIS indicating that a mMAR is attached to it so that MNs are informed of a NEMO availability when they scan the surrounding PoAs.
2. When an MN joins the NEMO, the mMAR sends a NEMO PBU to the MAR. Upon receiving such message, the MAR creates a BCE for the MN with a special flag that allows recursive lookup. This is required to inspect the binding cache twice: one to look for MN’s location and then the mMAR’s location. In such way the routing table is created accordingly, that is, the entry for the mMAR indicates the “on-link” presence of the mMAR, and the MN’s entry indicates its reachability via the mMAR.
    a. A PoS in a MAR is in general not aware of an mMAR attached to another MAR. Hence the handover from a MAR to an mMAR not attached to the same MAR cannot benefit from IP continuity.
3. If the MN leaves the NEMO and joins directly the MAR, the entry is updated by replacing the next hop to the MN with “on-link”. In order to allow the MN to join another MAR the T-MAR should be provided with an S-MAR’s IP address. In this way the T-MAR sends a plain PBU to the previous S-MAR which can establish the tunnel and update the routing table accordingly.

5.9.3 Mobile Node operations

The MN operations are divided into three categories and are described below.

- The MN travels with the mMAR. In this case the MN is not involved in any particular operation, except the IP address configuration with the prefix advertised in the new MAR’s network.
- The MN joins the NEMO. As the in-vehicle radio technology is assumed to be WiFi, this case can be described as a plain WiFi-to-WiFi handover, or a WiFi offload. In both cases the operation is driven by 802.21 and is similar to a normal handover, with the FM in the mMAR being the target PoS. However, IP continuity can be ensured only when the MN joins an mMAR that is connected to the same MAR, as it is aware of the presence of a PoS in a mobile MAR, while other MARs in general are not.
- The MN leaves the NEMO. Again this is regarded as a standard handover and is coordinated by the network. It should be noted that an MN leaves the NEMO when the user gets off the vehicle, thus the handover needs to be performed fast enough as the vehicle can suddenly disappear. Thus it is suggested to handoff to a long range radio PoA attached to the same MAR to quickly recover the connectivity. The case in which an MN leaves an mMAR to join another one is not covered.

5.10 Multilink aggregation concept

The multilink aggregation concept leverages the multi-homing capability of the terminal and the aggregation functionality implemented at the Flow Manager side. We consider the multilink aggregation function in both the core level anchoring model and in AR level anchoring model.

The main goals for supporting mobility for multilink aggregation are to:

- Maintain high bandwidth and/or resiliency for applications that require that, when possible, thus enable higher QoS and monetization options (it should be noted as explained later that the MEDIEVAL PBS can leverage the link diversity especially for the uplink to increase the available data rate).
- Provide “make before break”, “smart” off-loading from LTE networks to WiFi while still providing high SLA service continuity.

In case of the Core Level anchoring model the LMA handles the multi access connectivity of a given terminal. According to operator policies, application requirements and device capabilities, it should be possible to configure the Flow Manager (located in the LMA) operations to aggregate flows instead of selectively move flows across wireless access networks. In this context the Flow Manager can aggregate available bandwidth on both the LTE access and the WiFi access resulting in a bigger fat pipe. The Flow Manager collocated with the LMA functionality can therefore combine LTE & WiFi uplinks and/or LTE & WiFi downlinks independently, capacity for any given video service. We argue that this service can be particularly useful for downlink bandwidth consuming applications or for uplink demanding applications such as PBS.

In case of AR Level anchoring model the multilink aggregation function needs careful configuration. Given the nature of the DMM model the MN is multi-homed thus having two different IP addresses on each access link. To ensure the selected video service exploits the bandwidth aggregation scheme all flows have to be sent to the same mobility anchor and have to be managed by the same Flow Manager. In this case, when the CM located at the MN decides to boost its uplink/downlink channel, it has to exchange signalling with the network to: i) select the Flow Manager/mobility anchor that will be used as aggregator (say Aggregator Flow Manager [AFM]), ii) instruct the other Flow Manager (assuming the terminal has only wireless interfaces and two active connections) to establish a tunnel towards the AFM and to route the specific flows to the AFM. The trigger to start this procedure should be initiated at the MN side (CM) and 802.21 signalling should be used to configure the network side accordingly.

The Flow Manager shall support being instructed to achieve certain performance targets rather than “blindly” combining the two uplinks. Such goals are in term of QoS. For example, the Flow Manager may be instructed to try and achieve between 1.5mbps to 1.8 mbps UL of received information. Such a scheme shall provide the “right” level of support to each service, as requested by the application, if conditions allow. The applications/services can also give priority, e.g. “telepresence” at high priority and PBS at lower priority. The Flow Manager shall try to maintain the total service levels during mobility. It should be further noted that it is up to the application level to adapt to the heterogeneous wireless environment (e.g. different round trip delays, jitter, etc…) while preserving the desired Quality of Experience.

6 Usage scenario

The purpose of this section is to describe main operations of MEDIEVAL Mobility subsystem through MSCs that are related to the “mobility events” occurring in the following “Arriving at the city” use case.

6.1 Arriving at the city

The scenario has been split into different steps, each one corresponding to a specific operation on the network. For most of them a detailed MSC is provided including textual description. The purpose is to show how the Mobility subsystem works, detailing the interaction between the modules. When necessary, also some interactions with other MEDIEVAL subsystems are provided.

- Step 1:

John is going to Cannes to view the Cannes Film Festival. He lives in Italy and the best way to go there is by train. So right now he is taking the bus to the train station.

His smart phone is on and attached (registered) to the LTE network of the operator he is subscribed to (Home Operator). He is waiting for a bus (his company strongly suggests to use public transportation rather than taxis when at home). While he is waiting he starts to watch a video on his screen to distract himself (VoD service).

In Section 6.1.1 the MSC related to session set-up and flow activation is provided.

- Step 2:

The bus arrives, John moves inside, where he sits and continues watching the video.

During the whole trip John continues watching the video without loosing his connection or his video breaking.

In Section 6.1.2 the MSC related to an intra LMD (only intra-LTE) handover is provided.

- Step 3:

John starts a new application (e-mail) (on LTE) while the video flow runs in the background.

The related MSC, describing the starting of the new application, is reported in Section 6.1.3.

- Step 4:

John arrives at the train station (he is still watching the video and handling e-mail (two active flows). His mobile terminal detects the presence of a WiFi network from his Mobile Operator. The video flow is moved to WiFi (WiFi offload). E-mail remains on LTE.

This flow HO is inter-technology / intra-domain: the Hotspot Wifi is managed by the same operator. The related MSC is in Section 6.1.4.

- Step 5:

The train arrives and John moves inside, where he sits and continues. The train at the station connects through LTE to the MAR that handles the network in the station.

The train is equipped with a WiFi-based NEMO network. Due to a status of network congestion in the WiFi hotspot of the Station, John’s smart phone switches the video-streaming to the WiFi network offered by the train while maintaining the e-mail flow anchored to LTE. The HO intra-technology is intra-domain (we assume that the WiFi over the train is operated by the same operator as the WiFi hotspot).

The two MSCs describing how the NEMO joins the LTE network when arriving at the station and how John's terminal joins the NEMO at the station are described in Section 6.1.5

Step 6:

John arrives at Cannes, in France. Even if WiFi is available at the train station his mobile (based on interactions with the network) connects to the LTE network since the video requirements are better met by the available provider. This way he connects to the local French provider (inter-domain/inter-technology HO) and enters a taxi. Refer to Section 6.1.6 for the related MSC.

Step 7:

After arriving at the Cannes film festival, John is waiting in the queue. He starts watching a live feed on his mobile (through Mobile TV video service) as most of the people who are also queuing. Everybody is trying to watch what is happening inside and on the red carpet interviews. The video is accessible through multicast (this step of the scenario mainly refers to multicast; detailed MSCs for multicast operation can be found in D4.2).

6.1.1 Session set-up and flow activation MSC (step 1)

This new flow preparation (Figure 19) is triggered when the MEDIEVAL compliant application sends an *APP_CM_GetServiceList.request/CM_VSP_GetServiceList.request* message to the Video Service Portal (VSP) through the local Connection Manager (CM). Upon reception the VSP queries it's local database for services available for the current Mobile Node (MN). Available services are sent to the application in a *CM_VSP_GetServiceList.response/APP_CM_GetServiceList.response* message (via CM).

Once the application receives this message, it shows the service list to the user so that he can now choose. Once the service is selected an *APP_CM_SelectService.request/CM_VSP_SelectService.request* is issued from the application to the VSP (via CM). The VSP will then gather a list of available content for this service and send it back to the application (via CM) for the user to choose. After the user chooses the content the application asks the CM to gather connection information from the terminal by sending it an *APP_CM_GetTerminalInfo.request* message.

The CM will first ask the Media Independent Information Server (MIIS) service for PoA information, by means of an exchange of *MIH_Get_Information.request/response* messages. Then the CM will check the local interfaces for local interface information, by exchanging a *MIH_Link_Get_Parameters.request/confirm* message sequence with the MIHF/L2.5 Abstraction Module. Once the information is filtered by the CM it will be reported to the application through an *APP_CM_GetTerminalInfo.response* message.

The application now has enough information to request the VSP for the service to be prepared (*APP_CM_PrepareService.request/CM_VSP_PrepareService.request* message, via CM). The VSP will then start procedures on the network side to setup the service requirements.

It starts by asking the Decision Module (DM) which is the best service source (local cache) to handle the service (*DM_VSP_PrepareService.request*). The DM in turn will gather information, from the network side, on which is the best PoA to provide the service by asking the Flow Manager (FM) for link resource information from the PoAs (*DM_FM_GetNetworkInfo.request/response* message exchange).

Once the DM has decided on the best local cache for the selected service, it will reply this decision to the VSP (*DM_VSP_PrepareService.response*). The VSP will then trigger the QoEVC (*QoEVC_VSP_PrepareService.request* message).

In the meanwhile the Cross-Layer Optimization (XLO) must be informed of a new service requirement in the network for purposes of traffic optimization (*QoEVC_XLO_QoESensitivity.update/ack* message exchange). Then the QoEVC asks the DM to setup the streaming conditions on the network side (*QoEVC_DM_SetStream.request* message).

Afterwards the FM sets up the network to prepare for this new service *(DM_FM_SetStream.request message*). The FM tries to allocate resources on the decided PoA (*MIH_Link_Action.request/confirm* message exchange) and on success it registers the flows on it's local Database and communicates this new information to the DM (*DM_FM_SetStream.response*), which will send it to the QoEVC (*QoEVC_DM_SetStream.response* message).

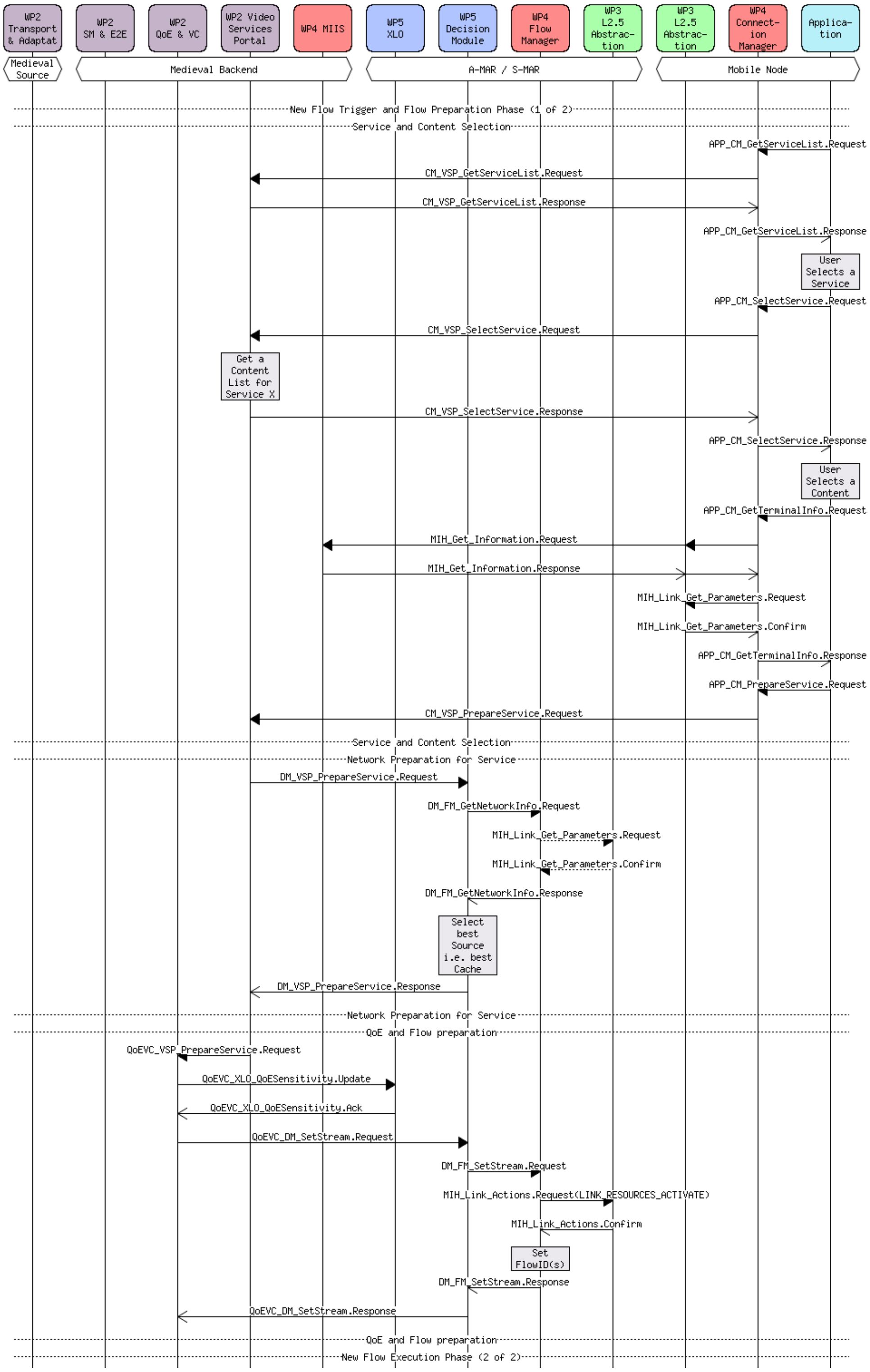
WP2 Transport & Adaptat
WP2 SM & E2E
WP2 QoE & VC
WP2 Video Services Portal
WP4 MIIS
WP5 XLO
WP5 Decision Module
WP4 Flow Manager
WP3 L2.5 Abstrac-tion
WP3 L2.5 Abstrac-tion
WP4 Connect-ion Manager
Applica-tion
Medieval Source
Medieval Backend
A-MAR / S-MAR
Mobile Node
New Flow Trigger and Flow Preparation Phase (1 of 2)
Service and Content Selection
APP_CM_GetServiceList.Request
CM_VSP_GetServiceList.Request
CM_VSP_GetServiceList.Response
APP_CM_GetServiceList.Response
User Selects a Service
APP_CM_SelectService.Request
CM_VSP_SelectService.Request
Get a Content List for Service X
CM_VSP_SelectService.Response
APP_CM_SelectService.Response
User Selects a Content
APP_CM_GetTerminalInfo.Request
MIH_Get_Information.Request
MIH_Get_Information.Response
MIH_Link_Get_Parameters.Request
MIH_Link_Get_Parameters.Confirm
APP_CM_GetTerminalInfo.Response
APP_CM_PrepareService.Request
CM_VSP_PrepareService.Request
Service and Content Selection
Network Preparation for Service
DM_VSP_PrepareService.Request
DM_FM_GetNetworkInfo.Request
MIH_Link_Get_Parameters.Request
MIH_Link_Get_Parameters.Confirm
DM_FM_GetNetworkInfo.Response
Select best Source i.e. best Cache
DM_VSP_PrepareService.Response
Network Preparation for Service
QoE and Flow preparation
QoEVC_VSP_PrepareService.Request
QoEVC_XLO_QoESensitivity.Update
QoEVC_XLO_QoESensitivity.Ack
QoEVC_DM_SetStream.Request
DM_FM_SetStream.Request
MIH_Link_Actions.Request(LINK_RESOURCES_ACTIVATE)
MIH_Link_Actions.Confirm
Set FlowID(s)
DM_FM_SetStream.Response
QoEVC_DM_SetStream.Response
QoE and Flow preparation
New Flow Execution Phase (2 of 2)

Figure 19: Session Setup (Preparation phase)

As depicted in Figure 20, the QoEVC works with the Session Manager (SME2E) to start the session (*QoEVC_SME2E_SetSession.request/response*). The Transport and Adaptation module (A&T) is contacted afterwards (*QoEVC_A&T_StartService.request/response*) to provide the Video Stream to the user (*Video Stream*).

On the final phase some information on the video stream is propagated to the application so that it is aware that the streaming has started and the user can finally watch it (*CM_VSP_PrepareService.response* and *APP_CM_PrepareService.response* messages).

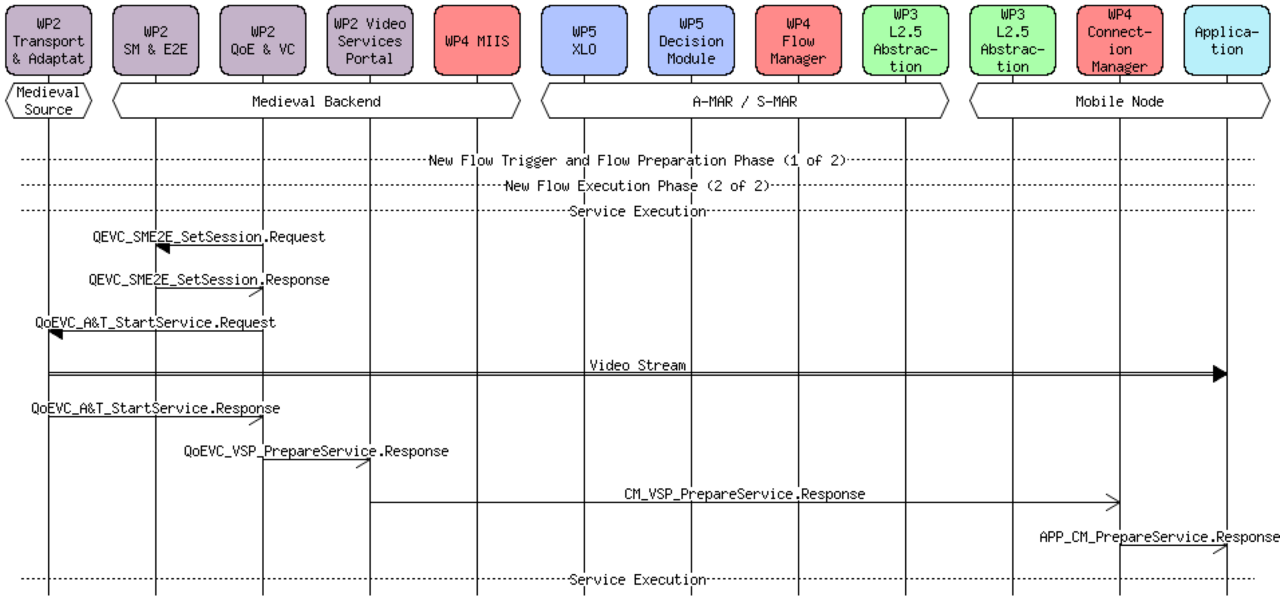
WP2 Transport & Adaptat
WP2 SM & E2E
WP2 QoE & VC
WP2 Video Services Portal
WP4 MIIS
WP5 XLO
WP5 Decision Module
WP4 Flow Manager
WP3 L2.5 Abstrac-tion
WP3 L2.5 Abstrac-tion
WP4 Connect-ion Manager
Applica-tion
Medieval Source
Medieval Backend
A-MAR / S-MAR
Mobile Node
New Flow Trigger and Flow Preparation Phase (1 of 2)
New Flow Execution Phase (2 of 2)
Service Execution
QEVC_SME2E_SetSession.Request
QEVC_SME2E_SetSession.Response
QoEVC_A&T_StartService.Request
Video Stream
QoEVC_A&T_StartService.Response
QoEVC_VSP_PrepareService.Response
CM_VSP_PrepareService.Response
APP_CM_PrepareService.Response
Service Execution

Figure 20: Session Setup (Execution phase)

6.1.2 Intra-technology (LTE) intra LMD handover MSC (step 2)

The actions of John will trigger an Intra-technology (LTE) intra-domain handover, whose message sequence is described in Figure 21, Figure 22 and Figure 23.

In the preparation phase (Figure 21), the first message is the handover trigger. The *MIH_Link_Parameters_Report.indication* message is issued when the LTE interface signal strength gets below the threshold. The CM will firstly ask the MIIS for any available PoAs in the area (*MIH_Get_Information.request/response* exchange), followed by a local request of parameters (*MIH_Link_Get_Parameters.request/confirm*), and a Layer 2 Scan (*MIH_Link_Action.request/confirm*) in order to check which of those PoAs are reachable by the Mobile Node.

Then the CM will ask the FM for candidates from the network, based on available resources (*MIH_MN_HO_Candidate_Query.request*).The FM will check every T-MAR individually, for available resources (*MIH_N2N_HO_Query_Resources.request/response* exchange). After all T-MARs have been consulted, the FM requests the DM to give him advice by means of a list of PoAs by order of preference (*FM_DM_HODecision.request/response* message exchange). Once the FM takes the final decision on the destination of the handover, it replies to the CM with a *MIH_MN_HO_Candidate_Query.response* message.

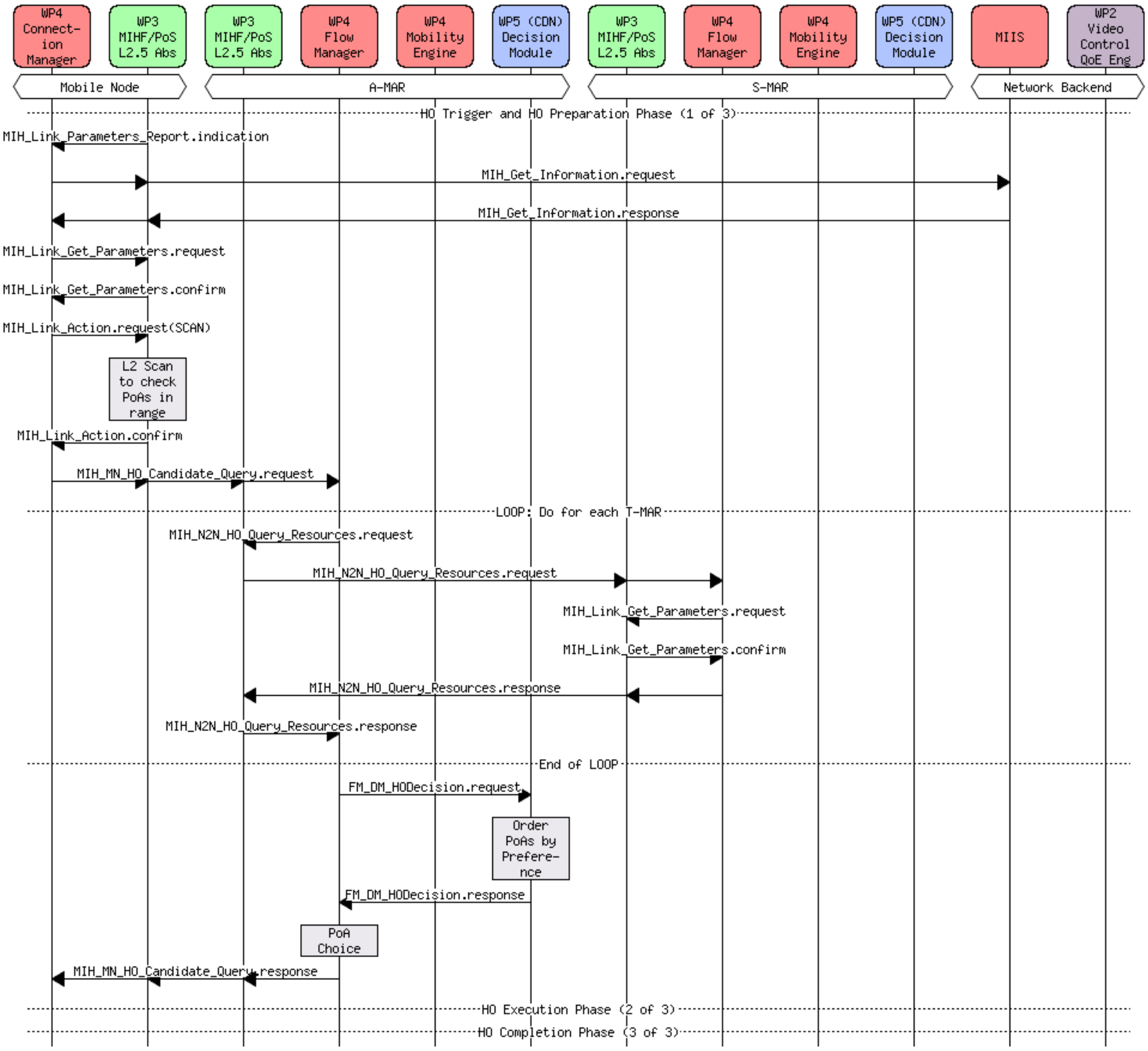
WP4 Connect-ion Manager
WP3 MIHF/PoS L2.5 Abs
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
MIIS
WP2 Video Control QoE Eng
Mobile Node
A-MAR
S-MAR
Network Backend
HO Trigger and HO Preparation Phase (1 of 3)
MIH_Link_Parameters_Report.indication
MIH_Get_Information.request
MIH_Get_Information.response
MIH_Link_Get_Parameters.request
MIH_Link_Get_Parameters.confirm
MIH_Link_Action.request(SCAN)
L2 Scan to check PoAs in range
MIH_Link_Action.confirm
MIH_MN_HO_Candidate_Query.request
LOOP: Do for each T-MAR
MIH_N2N_HO_Query_Resources.request
MIH_N2N_HO_Query_Resources.request
MIH_Link_Get_Parameters.request
MIH_Link_Get_Parameters.confirm
MIH_N2N_HO_Query_Resources.response
MIH_N2N_HO_Query_Resources.response
End of LOOP
FM_DM_HODecision.request
Order PoAs by Prefere-nce
FM_DM_HODecision.response
PoA Choice
MIH_MN_HO_Candidate_Query.response
HO Execution Phase (2 of 3)
HO Completion Phase (3 of 3)

Figure 21: Intra-Technology Intra-LMD Handover (Preparation phase)

Starting the Execution phase (Figure 22), the FM will firstly ask the chosen T-MAR to allocate resources to host properly the MN (*MIH_N2N_HO_Commit.request/response*). Secondly, the FM will contact the Video Control (VC), to announce its movement (*FM_QoEVC_HOCommit.request/response*), so that if any content adaptation action is required it can be done in advance. Thirdly, the FM informs the CM to commit the handover (*MIH_MN_HO_Commit.request/response*).

After the L2 handover, there will be a link up event (MIH*_Link_Up.indication*), indicating attachment to the new PoA; this event will be received by the CM (in the MN). At the same time the S-MAR detects the L2 attachment of the MN and the FM will trigger the activation of the mobility protocol (*FM_UME_ActivateMobility.request/response)*. The mobility protocol will not only exchange PBU/PBA messages with the A-MAR but also setup a tunnel between them. The FM will then notify the DM by means of a *FM_DM_HOCommit.request/response m*essage exchange.

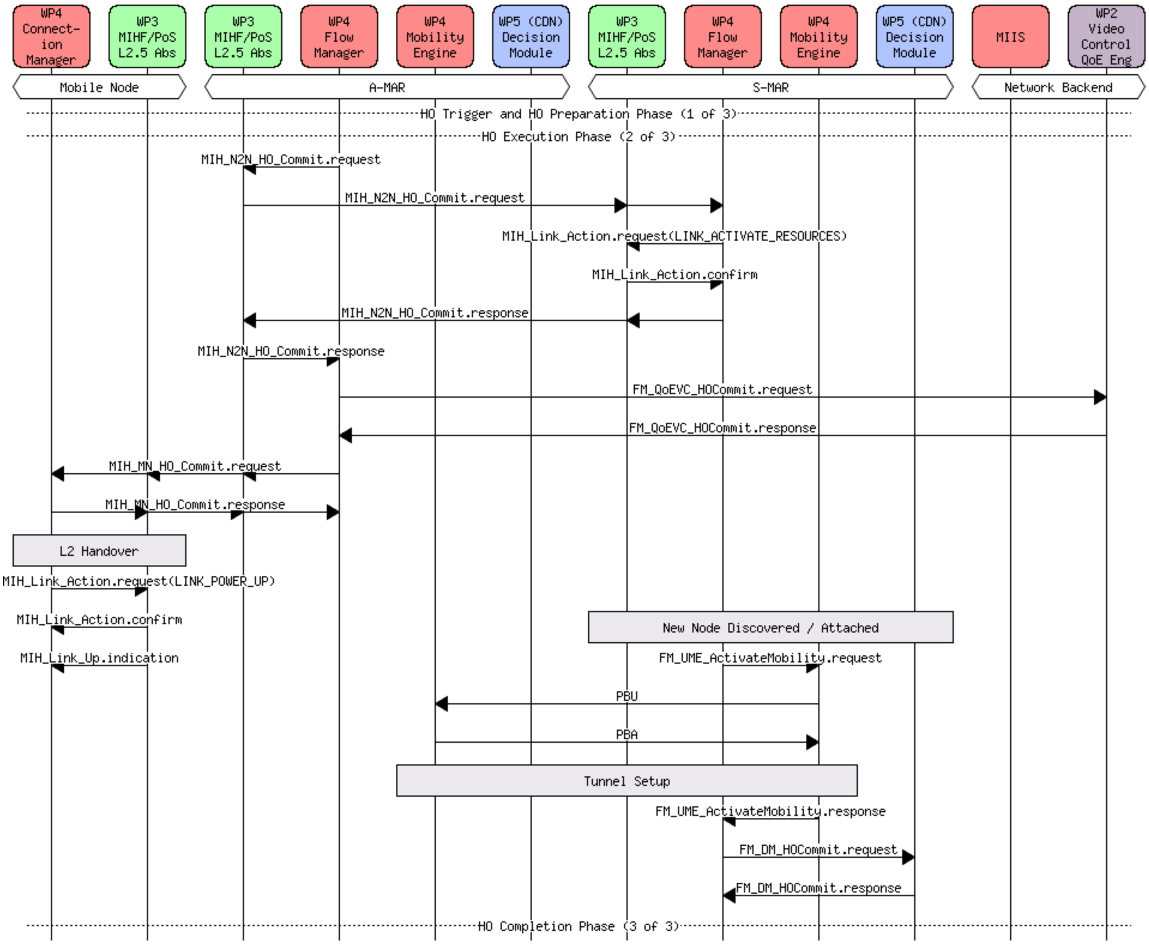
WP4 Connect-ion Manager
WP3 MIHF/PoS L2.5 Abs
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
MIIS
WP2 Video Control QoE Eng
Mobile Node
A-MAR
S-MAR
Network Backend
HO Trigger and HO Preparation Phase (1 of 3)
HO Execution Phase (2 of 3)
MIH_N2N_HO_Commit.request
MIH_N2N_HO_Commit.request
MIH_Link_Action.request(LINK_ACTIVATE_RESOURCES)
MIH_Link_Action.confirm
MIH_N2N_HO_Commit.response
MIH_N2N_HO_Commit.response
FM_QoEVC_HOCommit.request
FM_QoEVC_HOCommit.response
MIH_MN_HO_Commit.request
MIH_MN_HO_Commit.response
L2 Handover
MIH_Link_Action.request(LINK_POWER_UP)
MIH_Link_Action.confirm
MIH_Link_Up.indication
New Node Discovered / Attached
FM_UME_ActivateMobility.request
PBU
PBA
Tunnel Setup
FM_UME_ActivateMobility.response
FM_DM_HOCommit.request
FM_DM_HOCommit.response
HO Completion Phase (3 of 3)

Figure 22: Intra-Technology Intra-LMD Handover (Execution phase)

On the completion phase (Figure 23) a simple mechanism of releasing allocated resources in the A-MAR is put in place. The CM asks the S-MAR to do so on its behalf (*MIH_MN_HO_Complete.request/response*). Then the S-MAR will contact the A-MAR (*MIH_N2N_HO_Complete.request/response*), which in turn releases the no longer required resources by the MN. The CM in the meantime notifies the VC that the handover is completed through the new attached network (*FM_QoEVC_HOComplete.request/response* messages).

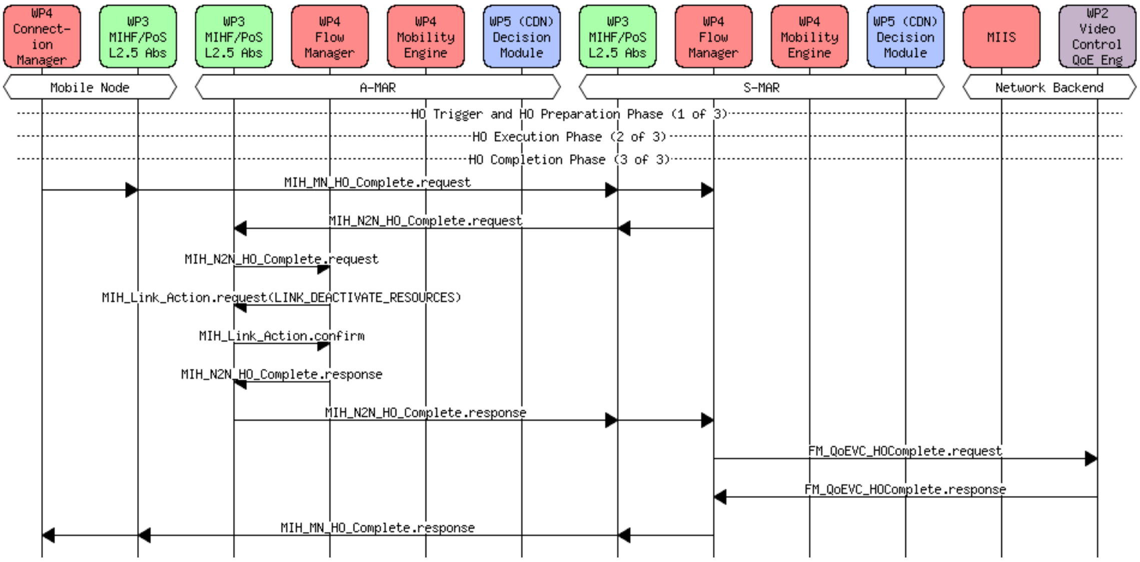
WP4 Connect-ion Manager
WP3 MIHF/PoS L2.5 Abs
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
MIIS
WP2 Video Control QoE Eng
Mobile Node
A-MAR
S-MAR
Network Backend
HO Trigger and HO Preparation Phase (1 of 3)
HO Execution Phase (2 of 3)
HO Completion Phase (3 of 3)
MIH_MN_HO_Complete.request
MIH_N2N_HO_Complete.request
MIH_N2N_HO_Complete.request
MIH_Link_Action.request(LINK_DEACTIVATE_RESOURCES)
MIH_Link_Action.confirm
MIH_N2N_HO_Complete.response
MIH_N2N_HO_Complete.response
FM_QoEVC_HOComplete.request
FM_QoEVC_HOComplete.response
MIH_MN_HO_Complete.response

Figure 23: Intra-Technology Intra-LMD Handover (Completion phase)

6.1.3 Set-up of a new flow (step 3)

The setting up of a new e-mail flow (Figure 24) is triggered when the user already selected the e-mail service by launching a MEDIEVAL compliant e-mail client. The E-mail client then issues an *APP_CM_SelectService.request/CM_VSP_SelectService.request* to the VSP (via CM). The VSP will then gather a list of available content for this service and send it back to the E-mail client (via CM). The E-mail client then asks the CM to gather connection information from the terminal by sending it a *APP_CM_GetTerminalInfo.request* message.

The CM will first ask the MIIS service for PoA Information, by means of an exchange of *MIH_Get_Information.request/response* messages. Then the CM will check the local interfaces for local interface information, by exchanging a *MIH_Link_Get_Parameters.request/confirm* message sequence with the MIHF/L2.5 Abstraction Module. Once the information is filtered by the CM it will be reported to the application through an *APP_CM_GetTerminalInfo.response* message.

The application now has enough information to request the VSP for the service to be prepared (*APP_CM_PrepareService.request/CM_VSP_PrepareService.request* message, via CM). The VSP will then start procedures on the network side to setup the service requirements.

It starts by asking the DM which is the best service source (local cache) to handle the service (*PrepareService.request*). The DM in turn will gather information, from the network side, on which is the best PoA to provide the service by asking the FM for link resource information from the PoAs (*DM_FM_GetNetworkInfo.request/response* message exchange).

Once the DM has decided on the best local cache for the selected service, based on the service requested (e-mail) it will skip sensitivity checks and select the appropriate delivery method (best effort).

Afterwards the FM sets up the network to prepare for this new service *(DM_FM_SetStream.request message*). The FM tries to allocate resources on the decided PoA (*MIH_Link_Actions.request/confirm* message exchange) and on success it registers the flows on it's local Database and communicates this new information to the DM (*DM_FM_SetStream.response*), which will send it to the VSP.

The VSP then replies to the application (via CM) the status on the service preparation on the network (*CM_VSP_PrepareService.response/APP_CM_PrepareService.response* message). Once this last message is received, the Application can directly communicate with the E-mail server and start its session.

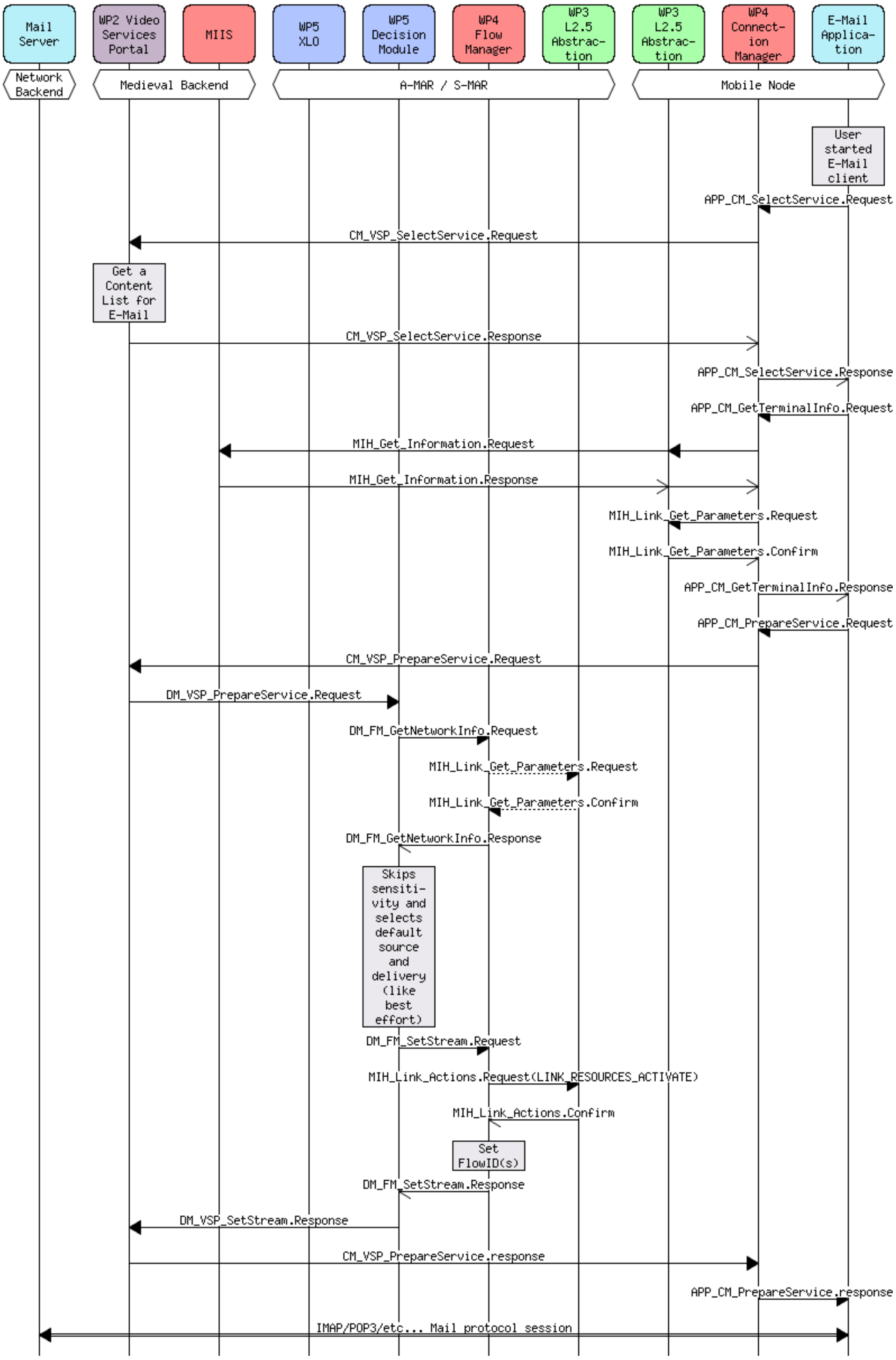
Mail Server
WP2 Video Services Portal
MIIS
WP5 XLO
WP5 Decision Module
WP4 Flow Manager
WP3 L2.5 Abstrac-tion
WP3 L2.5 Abstrac-tion
WP4 Connect-ion Manager
E-Mail Applica-tion
Network Backend
Medieval Backend
A-MAR / S-MAR
Mobile Node
User started E-Mail client
APP_CM_SelectService.Request
CM_VSP_SelectService.Request
Get a Content List for E-Mail
CM_VSP_SelectService.Response
APP_CM_SelectService.Response
APP_CM_GetTerminalInfo.Request
MIH_Get_Information.Request
MIH_Get_Information.Response
MIH_Link_Get_Parameters.Request
MIH_Link_Get_Parameters.Confirm
APP_CM_GetTerminalInfo.Response
APP_CM_PrepareService.Request
CM_VSP_PrepareService.Request
DM_VSP_PrepareService.Request
DM_FM_GetNetworkInfo.Request
MIH_Link_Get_Parameters.Request
MIH_Link_Get_Parameters.Confirm
DM_FM_GetNetworkInfo.Response
Skips sensiti-vity and selects default source and delivery (like best effort)
DM_FM_SetStream.Request
MIH_Link_Actions.Request(LINK_RESOURCES_ACTIVATE)
MIH_Link_Actions.Confirm
Set FlowID(s)
DM_FM_SetStream.Response
DM_VSP_SetStream.Response
CM_VSP_PrepareService.response
APP_CM_PrepareService.response
IMAP/POP3/etc... Mail protocol session

Figure 24: Setup of a New Flow (e-Mail)

6.1.4 Flow handover MSC (step 4)

The handover process (Figure 25) starts with the event *MIH_Link_Detected.indication* issued by the MN's MIH component towards the Connection Manager (CM) reporting that a new WiFi PoA is available. Thereafter the FM checks the running flows and decides to handover the video streaming flow. The FM queries the candidate access network to check if resources are available to receive this flow without degrading its quality (*MIH_N2N_HO_Query_Resources.request/response*). If resources are available, the FM queries the Decision Module to check whether the WiFi PoA can actually receive such flow from the CDNs perspective by using *FM_DM_HODecision. request/response* primitives. With this information the handover decision is made and the serving FM notifies the target FM that the terminal will hand off to the WiFi network (Figure 26) (*MIH_N2N_HO_Commit. request/response*). Upon receiving this message the target FM executes the reservation of the required resources for the video flow. The serving FM then reports to the CM on the MN that the resources were reserved, the CM starts the handover procedure by requesting a content adaptation for the flow to be moved (*CM_QoEVC_HOCommit.request/response* messages). Finally, the L2/L3 handover is performed and an MIH event (*MIH_Link_Up.indication*) is triggered reporting the target FM that MN is connected to the PoA. The target FM then triggers PMIP on the Mobility Engine which will send a Proxy-BindingUpdate to the serving MAR in order to re-establish the network tunnel. Once the PMIP tunnel is established the Decision Module is informed (*FM_DM_HOCommit. request/response*) and the flow is moved to the new PoA. When this step is concluded the CM requests for another content adaptation (*CM_QoEVC_HOComplete. request/response*) for current flow. Finally, the CM triggers the handover completion phase (*MIH_MN_HO_Complete. request/response*) and the target FM initiates the procedure (*MIH_N2n_HO_Complete. request/response*) to release the network resources on the previous access link (Figure 26).

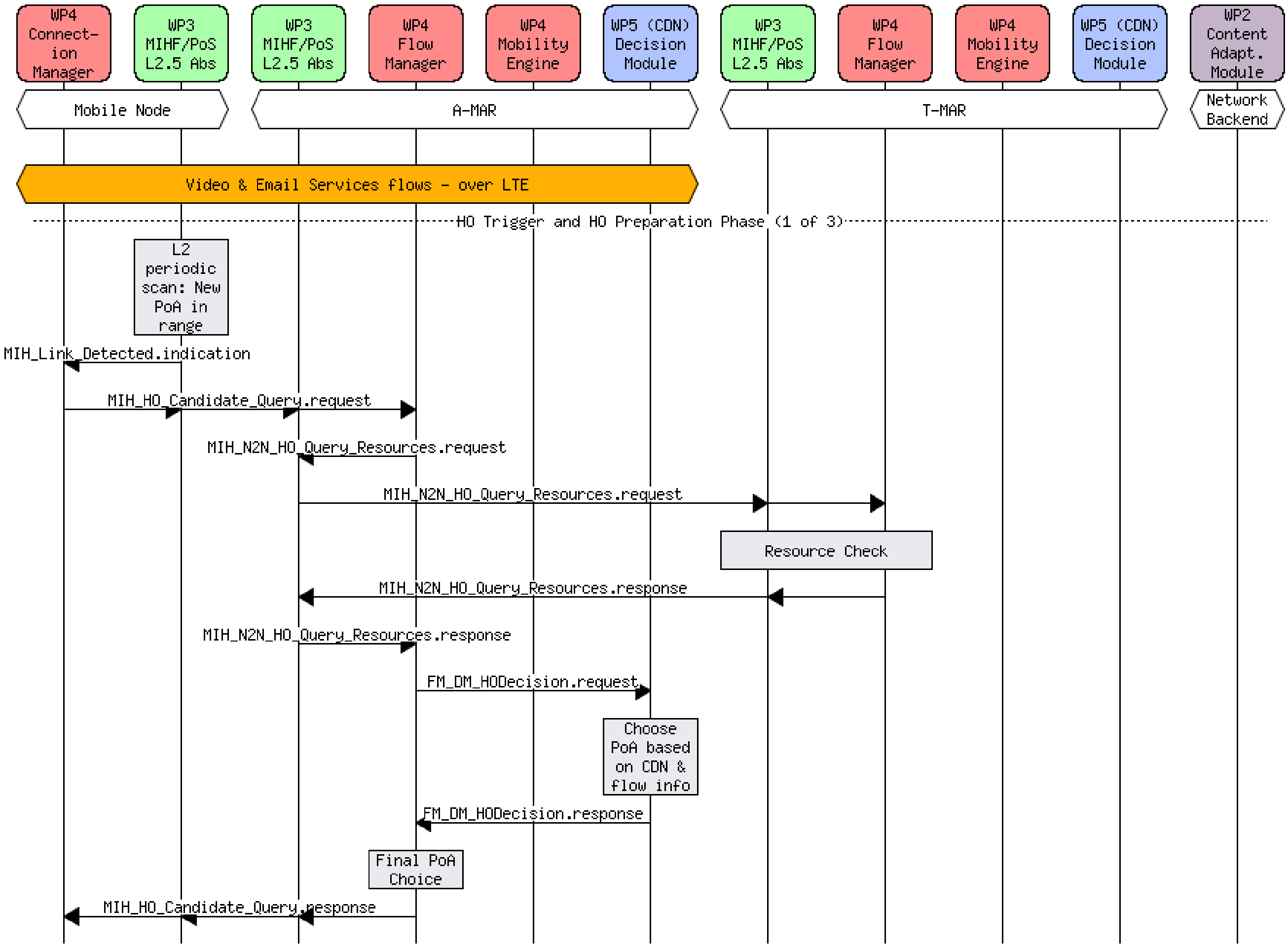
WP4 Connect-ion Manager
WP3 MIHF/PoS L2.5 Abs
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP2 Content Adapt. Module
Mobile Node
A-MAR
T-MAR
Network Backend
Video & Email Services flows - over LTE
HO Trigger and HO Preparation Phase (1 of 3)
L2 periodic scan: New PoA in range
MIH_Link_Detected.indication
MIH_HO_Candidate_Query.request
MIH_N2N_HO_Query_Resources.request
MIH_N2N_HO_Query_Resources.request
Resource Check
MIH_N2N_HO_Query_Resources.response
MIH_N2N_HO_Query_Resources.response
FM_DM_HODecision.request
Choose PoA based on CDN & flow info
FM_DM_HODecision.response
Final PoA Choice
MIH_HO_Candidate_Query.response

Figure 25: Step 4 – HO Trigger and Preparation Phases

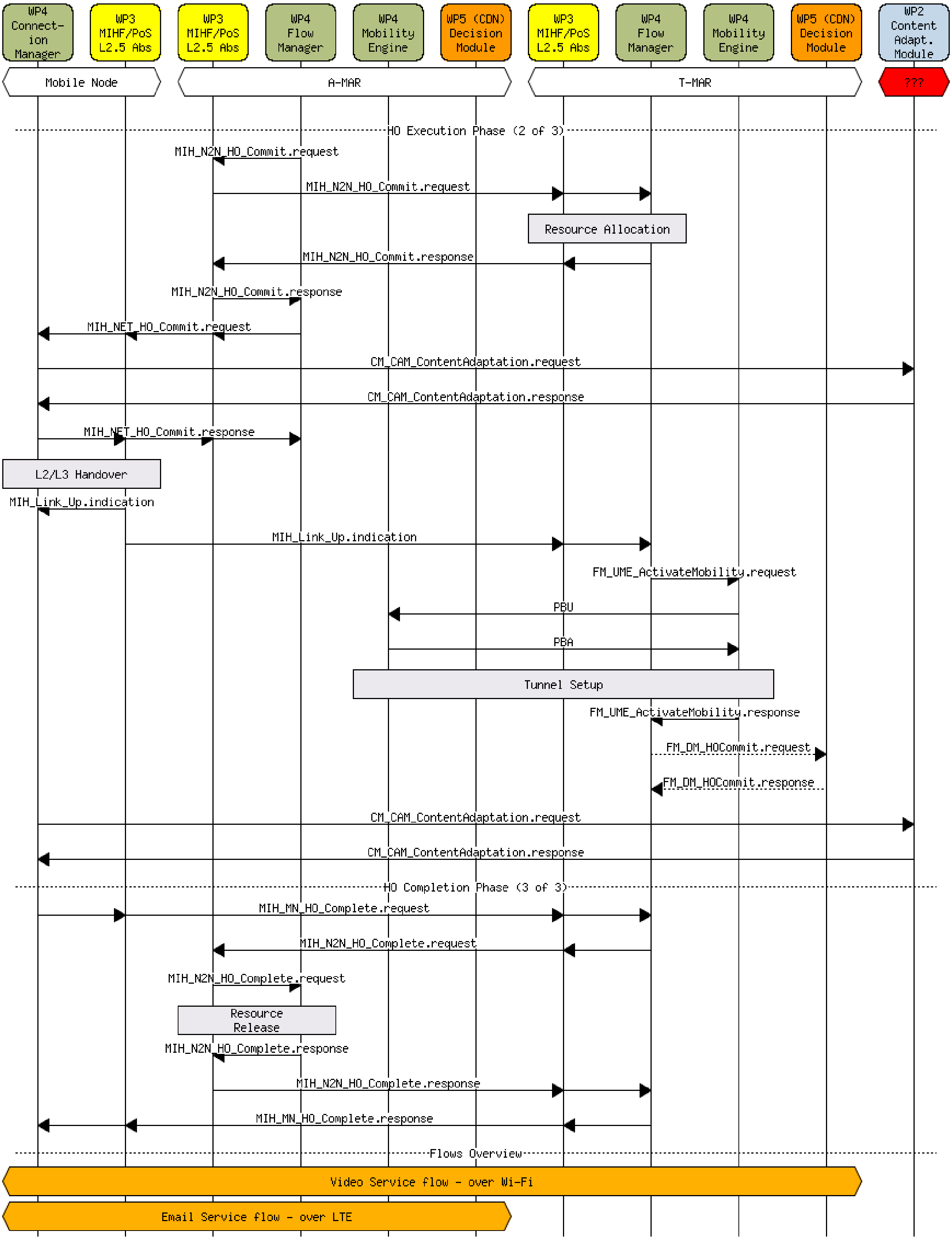
WP4 Connect-ion Manager
WP3 MIHF/PoS L2.5 Abs
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP3 MIHF/PoS L2.5 Abs
WP4 Flow Manager
WP4 Mobility Engine
WP5 (CDN) Decision Module
WP2 Content Adapt. Module
Mobile Node
A-MAR
T-MAR
???
HO Execution Phase (2 of 3)
MIH_N2N_HO_Commit.request
MIH_N2N_HO_Commit.request
Resource Allocation
MIH_N2N_HO_Commit.response
MIH_N2N_HO_Commit.response
MIH_NET_HO_Commit.request
CM_CAM_ContentAdaptation.request
CM_CAM_ContentAdaptation.response
MIH_NET_HO_Commit.response
L2/L3 Handover
MIH_Link_Up.indication
MIH_Link_Up.indication
FM_UME_ActivateMobility.request
PBU
PBA
Tunnel Setup
FM_UME_ActivateMobility.response
FM_DM_HOCommit.request
FM_DM_HOCommit.response
CM_CAM_ContentAdaptation.request
CM_CAM_ContentAdaptation.response
HO Completion Phase (3 of 3)
MIH_MN_HO_Complete.request
MIH_N2N_HO_Complete.request
MIH_N2N_HO_Complete.request
Resource Release
MIH_N2N_HO_Complete.response
MIH_N2N_HO_Complete.response
MIH_MN_HO_Complete.response
Flows Overview
Video Service flow - over Wi-Fi
Email Service flow - over LTE

Figure 26: Step 4 – HO Execution and Completion Phases

6.1.5 NEMO related MSCs (step 5)

Figure 27 shows how the mMAR joins a new access network (LTE based) when arriving at the station. The procedure is similar to the intra-LTE intra-domain scenario described in Section 6.1.2 up to the link establishment stage. Afterwards the procedure deviates and observes the following steps.

The FM in the fixed MAR detects a link establishment by a node that is not a MN, and hence triggers the IP configuration procedure on the NEMO Mobility Engine (NME). After this phase the mMAR has an IPv6 address routable at the MAR, and can start the mobility procedure: the CM in the mMAR requests the NME to activate the host-based mobility protocol (*CM_NME_ActivateMobility.request*). When the mobility procedure is successfully concluded the mMAR requests the resource release on the Serving-MAR (S-MAR) by sending a *MIH_MN_HO_Complete.request* message. Then the CM notifies the FM in the mMAR with a *CM_FM_NEMOCompleteHO.request* message to trigger the registration of the MNs carried in the NEMO domain. The registration is accomplished through a Proxy Binding Update containing a NEMO option, that indicates to the S-MAR that the MNs are requesting a valid IPv6 prefix in that access network but they are not directly connected to the MAR. This mechanism offers MNs a way to always exploit an optimal path towards the destination.

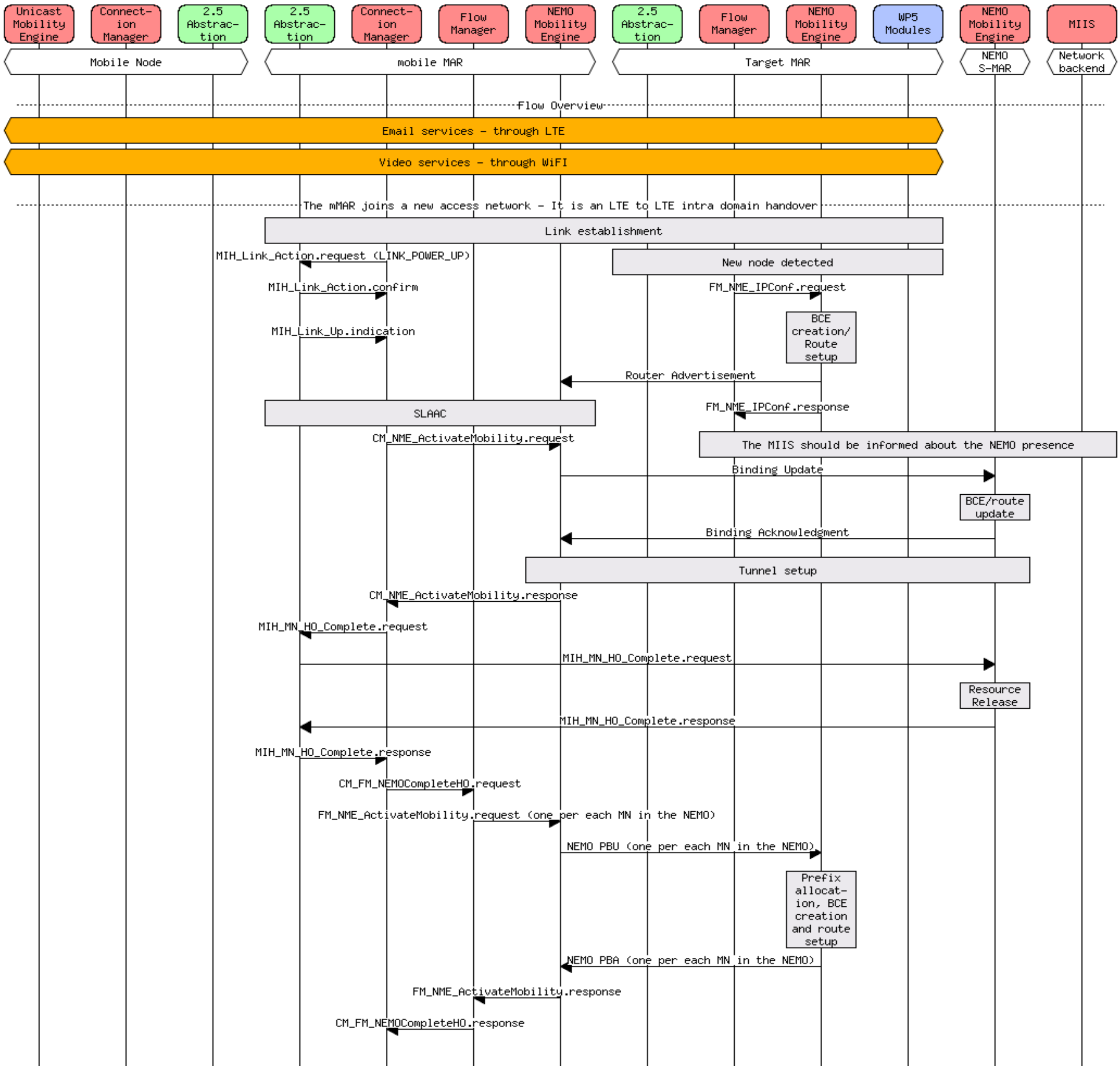
Unicast Mobility Engine
Connect-ion Manager
2.5 Abstrac-tion
2.5 Abstrac-tion
Connect-ion Manager
Flow Manager
NEMO Mobility Engine
2.5 Abstrac-tion
Flow Manager
NEMO Mobility Engine
WP5 Modules
NEMO Mobility Engine
MIIS
Mobile Node
mobile MAR
Target MAR
NEMO S-MAR
Network backend
Flow Overview
Email services - through LTE
Video services - through WiFI
The mMAR joins a new access network - It is an LTE to LTE intra domain handover
Link establishment
MIH_Link_Action.request (LINK_POWER_UP)
New node detected
MIH_Link_Action.confirm
FM_NME_IPConf.request
BCE creation/ Route setup
MIH_Link_Up.indication
Router Advertisement
SLAAC
FM_NME_IPConf.response
CM_NME_ActivateMobility.request
The MIIS should be informed about the NEMO presence
Binding Update
BCE/route update
Binding Acknowledgment
Tunnel setup
CM_NME_ActivateMobility.response
MIH_MN_HO_Complete.request
MIH_MN_HO_Complete.request
Resource Release
MIH_MN_HO_Complete.response
MIH_MN_HO_Complete.response
CM_FM_NEMOCompleteHO.request
FM_NME_ActivateMobility.request (one per each MN in the NEMO)
NEMO PBU (one per each MN in the NEMO)
Prefix allocat-ion, BCE creation and route setup
NEMO PBA (one per each MN in the NEMO)
FM_NME_ActivateMobility.response
CM_FM_NEMOCompleteHO.response

Figure 27: The NEMO joins the network at the station

Now that the train is at the station, John can step in, and its video flow is moved to the Wireless LAN on-board. Figure 28 depicts this procedure.

This is an intra-WiFi intra-domain network-initiated handover. The procedure starts after the *FM_XLO_CongestedNetwork.request* message is issued by the X-Layer Optimization component residing in the MAR. The handover takes place according to the operation defined in Sections 5.6.1 and 5.6.2 up to the link establishment stage. The FM in the mMAR triggers the NEMO mobility engine which task is to register the MN at the MAR. The scope of the NEMO engine specification is limited to the case in which the MN joins a NEMO that is connected to its same MAR. In this way, upon receiving the NEMO PBU, the MAR updates the mobility entry and the route to the MN by changing it from “on-link” to “via mMAR”.

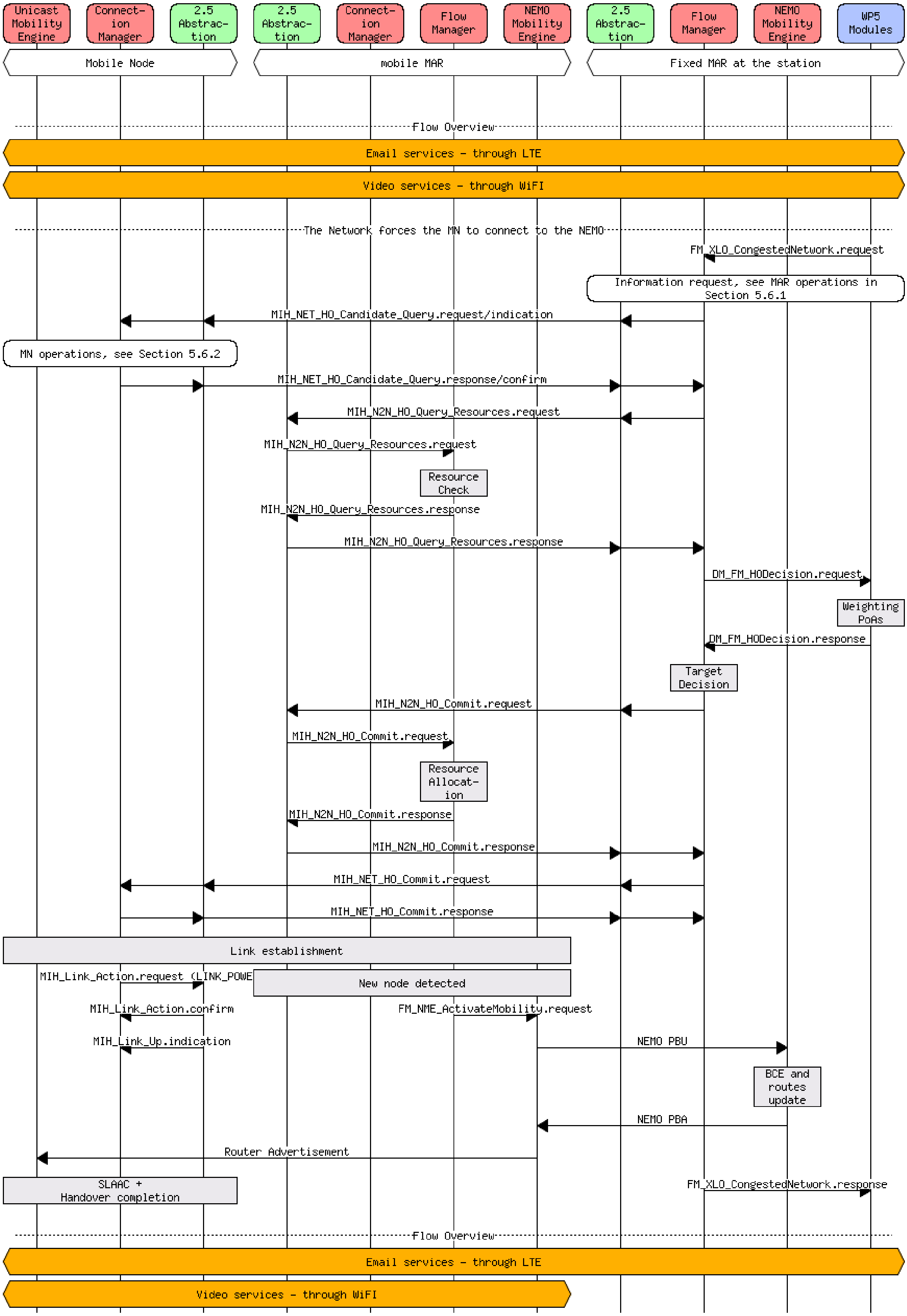
Unicast Mobility Engine
Connect-ion Manager
2.5 Abstrac-tion
2.5 Abstrac-tion
Connect-ion Manager
Flow Manager
NEMO Mobility Engine
2.5 Abstrac-tion
Flow Manager
NEMO Mobility Engine
WP5 Modules
Mobile Node
mobile MAR
Fixed MAR at the station
Flow Overview
Email services - through LTE
Video services - through WiFI
The Network forces the MN to connect to the NEMO
FM_XLO_CongestedNetwork.request
Information request, see MAR operations in Section 5.6.1
MIH_NET_HO_Candidate_Query.request/indication
MN operations, see Section 5.6.2
MIH_NET_HO_Candidate_Query.response/confirm
MIH_N2N_HO_Query_Resources.request
MIH_N2N_HO_Query_Resources.request
Resource Check
MIH_N2N_HO_Query_Resources.response
MIH_N2N_HO_Query_Resources.response
DM_FM_HODecision.request
Weighting PoAs
DM_FM_HODecision.response
Target Decision
MIH_N2N_HO_Commit.request
MIH_N2N_HO_Commit.request
Resource Allocat-ion
MIH_N2N_HO_Commit.response
MIH_N2N_HO_Commit.response
MIH_NET_HO_Commit.request
MIH_NET_HO_Commit.response
Link establishment
MIH_Link_Action.request (LINK_POWE
New node detected
MIH_Link_Action.confirm
FM_NME_ActivateMobility.request
MIH_Link_Up.indication
NEMO PBU
BCE and routes update
NEMO PBA
Router Advertisement
SLAAC + Handover completion
FM_XLO_CongestedNetwork.response
Flow Overview
Email services - through LTE
Video services - through WiFI

Figure 28: John's terminal joins the NEMO at the station

6.1.6 NEMO related MSCs (step 6)

Figure 29 depicts how the traffic is moved from the NEMO to an available LTE PoA belonging to another operator.

For the flow received to the WiFi interface, this is an inter-technology inter-domain handover initiated by the mobile node. Again the procedure is analogous to all the handover described in previous sections. However, when the MN receives the *MIH_NET_HO_Commit.request* message, it is aware that the PoA does not belong to the LMD, so when the MN configures a valid IPv6 address in the new network, the CM wakes up the host-based mobility engine issuing a *CM_UME_ActivateMobility.request* message to the Unicast Mobility Engine. At this stage a *Binding Update* message is sent by the UME in the MN to the UME of the A-MARs that are anchoring the flows that require to be kept active. Upon receiving the *Binding Acknowledgment* a tunnel is set up with the MN and the A-MARs and the communications are recovered.

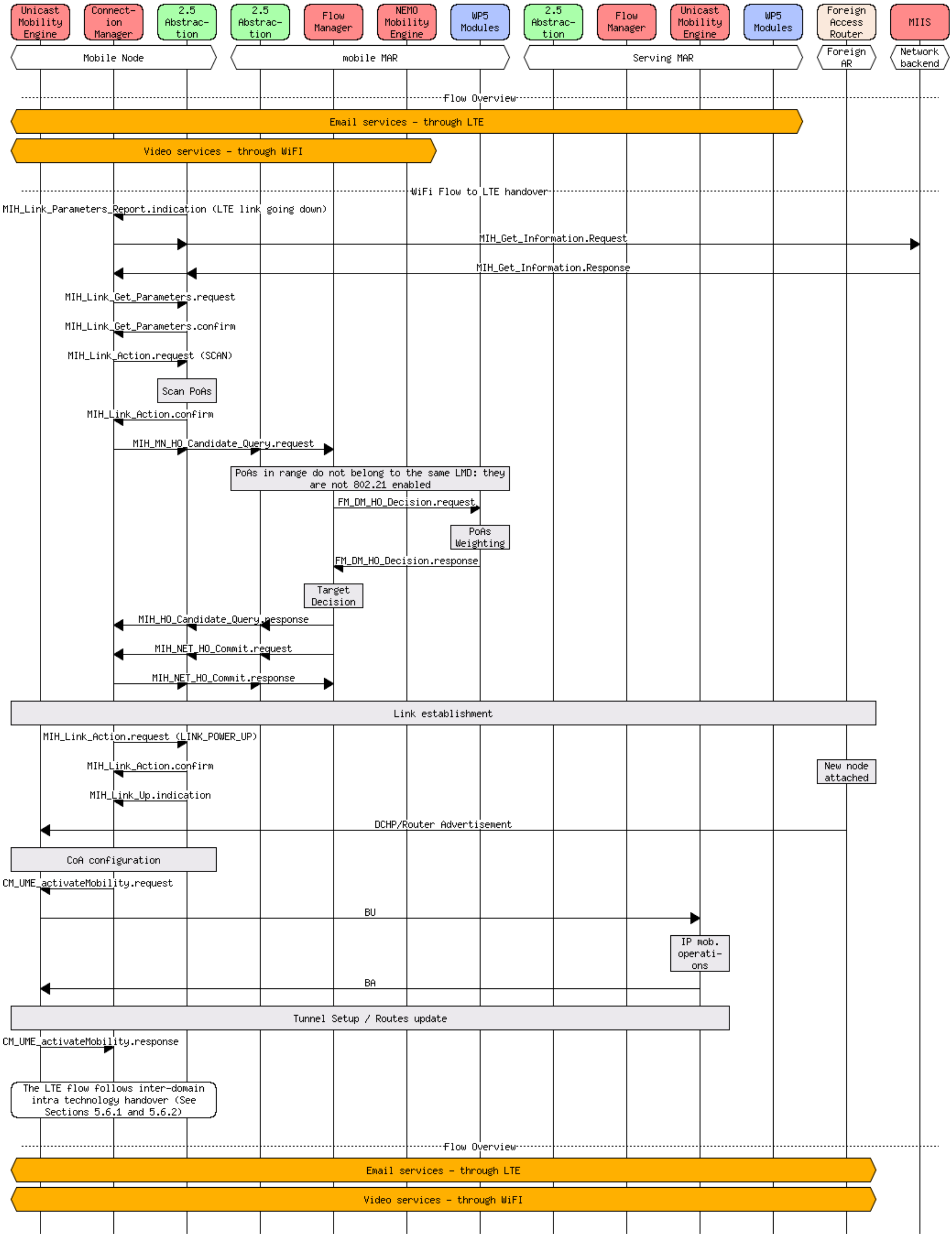
Unicast Mobility Engine
Connect-ion Manager
2.5 Abstrac-tion
2.5 Abstrac-tion
Flow Manager
NEMO Mobility Engine
WP5 Modules
2.5 Abstrac-tion
Flow Manager
Unicast Mobility Engine
WP5 Modules
Foreign Access Router
MIIS
Mobile Node
mobile MAR
Serving MAR
Foreign AR
Network backend
Flow Overview
Email services - through LTE
Video services - through WiFI
WiFi Flow to LTE handover
MIH_Link_Parameters_Report.indication (LTE link going down)
MIH_Get_Information.Request
MIH_Get_Information.Response
MIH_Link_Get_Parameters.request
MIH_Link_Get_Parameters.confirm
MIH_Link_Action.request (SCAN)
Scan PoAs
MIH_Link_Action.confirm
MIH_MN_HO_Candidate_Query.request
PoAs in range do not belong to the same LMD: they are not 802.21 enabled
FM_DM_HO_Decision.request
PoAs Weighting
FM_DM_HO_Decision.response
Target Decision
MIH_HO_Candidate_Query.response
MIH_NET_HO_Commit.request
MIH_NET_HO_Commit.response
Link establishment
MIH_Link_Action.request (LINK_POWER_UP)
MIH_Link_Action.confirm
New node attached
MIH_Link_Up.indication
DCHP/Router Advertisement
CoA configuration
CM_UME_activateMobility.request
BU
IP mob. operati-ons
BA
Tunnel Setup / Routes update
CM_UME_activateMobility.response
The LTE flow follows inter-domain intra technology handover (See Sections 5.6.1 and 5.6.2)
Flow Overview
Email services - through LTE
Video services - through WiFI

Figure 29: The terminal moves all the flows to another operator's LTE PoA

7 Interfaces

In the following sub-sections both internal and external interfaces description will be provided. Regarding external interfaces just an high level description is provided (further details are in D1.1[2]), whilst for internal interfaces both high-level and detailed description (i.e., protocols/primitives and parameters) are provided.

Concerning interface naming the following format is used:

<module_acronym_A>_<module_acronym_B>_If,

where modules A and B are ordered alphabetically.

7.1 External interfaces

By external interfaces we mean the interfaces between components of the Mobility subsystem (WP4) and components of the other subsystems building up the MEDIEVAL general architecture as defined in D1.1[2]: Video Services Control (WP2)[3], Wireless Access (WP3)[4], Transport Optimization (WP5) [6].

7.1.1 Application_CM_If

This interface is between the “MEDIEVAL compliant applications” and the Connection Manager. The specification of this interface is still under study and will include results from current on-going work in IETF MIF working group [45] and WP6 (Integration and Experimentation) feedback.

7.1.2 CM_VSP_If (WP4 -> WP2)

This is the interface between the “WP4 Connection Manager” and the “WP2 Video Services Portal”. It is used by the local application at the mobile terminal to request the list of services available on the network.

This interface is also used to take video application requirements as important criteria for choosing the best mobility scheme and the best connection. So, when a MEDIEVAL video application flow is selected, the “WP2 Video Services Portal” provides the “WP4 Connection Manager” with information related to:

- QoS/QoE requirements in terms of bandwidth, delay, jitter and loss
- Mobility requirements, in order to know if this flow needs to be anchored or not
- Any possible other critical constraints related to this flow

Another approach (still under investigation), which could be alternative to this, could be based on packet marking. This would imply that at session setup the information on a specific flow is directly encoded into the Flow Label and the Traffic Class fields of IPv6 packet headers. The Traffic Class field will be used to signal QoS classes only, while the Flow Label is used to mark the packet to encode information about “IP address continuity required”, “Flow Division”, etc.

7.1.3 CM_QoEVC_If (WP4->WP2)

This is the interface between the “Connection Manager (WP4)” and the “QoE & Video Control (QoEVC) (WP2)”. It is located in the terminal and is based on an API. It is used to allow the mobility management function to trigger content adaptation for the uplink traffic (the scenario refers to a Mobile Terminal generating streaming content – e.g.: PBS use case) before and after the HO process. Main scopes are:

- To adapt the video-content distributor in the MT to prepare handover
- To adapt the video-content distributor in the MT to prepare video to be streamed according to the new (target) network conditions
- To adapt the video-content distributor in the MT after the HO to the effective traffic load

7.1.4 FM_QoEVC_If (WP4->WP2)

This is the interface between the "Flow Manager (WP4)" and the "QoE & Video Control (QoEVC) (WP2)". The FM is located in the MAR and the QoEVC is located into a cache/video server). It applies to VoD or mobile TV scenarios and it is used to allow the mobility management function to trigger content adaptation for the downlink traffic before and after the HO process. Main scopes are:

- To adapt the video-content distributor to prepare handover
- To adapt the video-content distributor to prepare the video to be streamed according to the new (target) network conditions
- To adapt the video-content distributor after the HO to the effective traffic load

7.1.5 CM_L2.5_If and FM_L2.5_If (WP3-WP4)

The objective of this cross-layer interface is to extend the media-independent signalling functionalities provided by IEEE 802.21 to support specific mobility functionalities (e.g.: related to DMM) and video aware services. The extensions will/may concern all the three services of IEEE 802.21, namely the Media Independent Events, Commands and Information Services.

As described in Sections 5.4 and 5.5, both CM (in the MT) and FM (in the MAR) are MIH users. They interact, through the MIH-SAP, with the co-located MIHFs (also referred as L2.5 Abstraction component).

7.1.6 DM_FM_If (WP4->WP5)

This interface is needed in the HO process due to UE movement. Through this interface the "WP4 Flow Manager" provides "WP5 Decision Module" with the list of IP addresses of base stations (PoAs) the UE may see (candidate PoAs).

The provided list of PoAs is ordered by the handover decision algorithm taking into account the resources availability and IP flow requirements. The Transport Optimization subsystem weights each one of the candidate PoAs (e.g.: based on CDNs availability) and sends the updated list back to the FM (ordered list of PoAs). Based on the WP5 response, the FM decision algorithm selects the handover target network.

This same interface is also used in the following case we refer to as WiFi offload: e.g. let's assume that "WP4 Connection Manager" detects a new WiFi link; the CM forwards the "event" to the serving "WP4 Flow Manager" which triggers the "WP5 Decision Module" in order to evaluate the chance to optimally distribute the currently active flows.

A further use of this interface concerns the exchange of primitives in the session establishment of each video service. The exchange with Transport Optimization subsystem allows the FM to keep track of the session setup specific parameters. Considering that the Transport Optimization subsystem has an application level view, the FM needs the specific information about the session to map all the IP flows related to a given application. For instance if an application has two IP flows, one for the control plane and one for the data exchange, the FM must be capable of grouping both flows to the same session. To this end during the session setup of a MEDIEVAL service the FM is contacted by the Transport Optimization subsystem modules on the new session freshly started. Based on this information the FM is capable of routing the IP flows and to keep track of the required information.

7.1.7 FM_XLO_If (WP5 -> WP4)

This interface is needed in the interaction due to network congestion. Through this interface the "WP5 X-layer Optimisation" notifies (through an API based protocol) the "WP4 Flow Manager" that the network is congested (providing a list of IP flows whose distribution should be improved).

7.2 Internal interfaces

The following sections highlight internal interfaces between components defined within WP4.

7.2.1 Connection Manager

7.2.1.1 CM_UME_If

This is the interface between the Connection Manager (CM) and the Unicast Mobility Engine (UME). This interface is an internal WP4 interface.

7.2.1.1.1 CM_UME_ActivateMobility

CM_UME_ActivateMobility.request

Function

This message is used to notify the Unicast Mobility Engine in the terminal, to trigger the mobility protocol.

Semantics of the service primitive

```
CM_UME_ActivateMobility.request (
    Mobile_Terminal_ID,
    Interface_ID
)
```

Parameter	Type	Description
Mobile_Terminal_ID	STRING	The identifier of the Mobile Terminal (usually a NAI)
Interface_ID	STRING	The identifier of the interface where to activate mobility

Table 1: CM_UME_ActivateMobility.request parameter list

When generated

The message is generated when the CM is notified that it has attached to the new MAR. It forwards this notification to the UME through this message.

Effect on receipt

After receiving this message the UME should start the Mobility Protocol for the mentioned node.

CM_UME_ActivateMobility.response

Function

This message is used to notify the CM that the mobility protocol has finished the setup for the mobile terminal.

Semantics of the service primitive

```
CM_UME_ActivateMobility.response (
    Mobile_Terminal_ID,
    Interface_ID,
    ResultCode
)
```

Parameter	Type	Description
Mobile_Terminal_ID	STRING	The identifier of the Mobile Terminal (usually an NAI)
Interface_ID	STRING	The identifier of the interface where to activate mobility
ResultCode	UINT_8	The result of the protocol setup. (0 on OK, otherwise return an error code)

Table 2: CM_UME_ActivateMobility.response parameter list

When generated

The message is generated by the UME when the mobility procedure of the protocol is over. It contains the result of this process.

Effect on receipt

After receiving this message, the CM should either complete the handover, if it receives an affirmative result, or take appropriate actions otherwise.

7.2.1.2 CM_NME_If

This is the interface between the CM and the NEMO Mobility Engine. This interface is an internal WP4 interface.

7.2.1.2.1 CM_NME_ActivateMobility

CM_NME_ActivateMobility.request

Function

This message is used to notify the NEMO Mobility Engine in the mMAR, to trigger the mobility protocol.

Semantics of the service primitive

```
CM_NME_ActivateMobility.request (
    Mobile_Terminal_ID,
    Interface_ID
)
```

Parameter	Type	Description
Mobile_MAR_ID	STRING	The identifier of the Mobile MAR
Interface_ID	STRING	The identifier of the interface where to activate mobility

Table 3: CM_NME_ActivateMobility.request parameter list

When generated

The message is generated when the CM is notified that the mMAR has attached to a new MAR. It forwards this notification to the NME through this message.

Effect on receipt

After receiving this message the NME should start the Mobility Protocol for the mentioned node.

CM_NME_ActivateMobility.response

Function

This message is used to notify the CM that the mobility protocol has finished the setup for the mobile MAR.

Semantics of the service primitive

```
CM_NME_ActivateMobility.response (
    Mobile_MAR_ID,
    Interface_ID,
    ResultCode
)
```

Parameter	Type	Description
Mobile_MAR_ID	STRING	The identifier of the Mobile MAR
Interface_ID	STRING	The identifier of the interface where to activate mobility
ResultCode	UINT_8	The result of the protocol setup. (0 on OK, otherwise return an error code)

Table 4: CM_NME_ActivateMobility.response parameter list

When generated

The message is generated by the NME when the mobility procedure of the protocol is over. It contains the result of this process.

Effect on receipt

After receiving this message, the CM should either complete the handover, if it receives an affirmative result, or take appropriate actions otherwise.

7.2.1.3 CM_FM_If

The interface between the Connection Manager (CM) and the Flow Manager (FM) is common to the same MIH_SAP provided by MIHF since this interface's primitives are part of the IEEE 802.21 MIH protocol. The interface will reuse the existing primitives and parameters defined in the IEEE 802.21 standard [7], which should be consulted for further details. Concretely, the CM and FM will exchange the following handover-related 802.21 primitives:

- **MIH_MN_HO_Candidate_Query.request and MIH_MN_HO_Candidate_Query.response**

- **MIH_MN_HO_Commit.request and MIH_MN_HO_Commit.response**

- **MIH_MN_HO_Complete.request and MIH_MN_HO_Complete.response**

Nevertheless, the CM and FM running in the mMAR are able to communicate with each other through the following primitive.

7.2.1.3.1 CM_FM_NEMOCompleteHO

CM_FM_NEMOCompleteHO.request

Function

This message is used to notify the Flow Manager in the mMAR to trigger the registration at the S-MAR of the MNs carried in the NEMO.

Semantics of the service primitive

```
CM_FM_NEMOCompleteHO.request (
    S_MAR_IPaddress,
    Interface_ID
)
```

Parameter	Type	Description
S_MAR_IPaddress	IPv6 ADDRESS	The S-MAR's address seen by the mMAR
Interface_ID	STRING	The identifier of the interface connected to the S-MAR

Table 5: CM_FM_NEMOCompleteHO.request parameter list

When generated

The message is generated when the CM is notified that the mMAR has successfully attached to a new MAR and the mobility procedure for the mMAR is over.

Effect on receipt

After receiving this message the NME should start the Mobility Protocol for the mobile nodes attached to the mMAR.

CM_FM_NEMOCompleteHO.response

Function

This message is used to notify the CM that the mobility protocol has finished the setup for the mobile terminals in the NEMO.

Semantics of the service primitive

```
CM_FM_NEMOCompleteHO.response (
    S_MAR_IPaddress,
    Interface_ID,
    ResultCode
)
```

Parameter	Type	Description
S_MAR_IPaddress	IPv6 ADDRESS	The S-MAR's address seen by the mMAR
Interface_ID	STRING	The identifier of the interface connected to the S-MAR
ResultCode	UINT_8	The result of the protocol setup. (0 on OK, otherwise return an error code)

Table 6: CM_FM_NEMOCompleteHO.response parameter list

When generated

The message is generated by the FM in the mMAR when the registration of the MNs at the S-MAR is over. It contains the result of this process.

Effect on receipt

After receiving this message, the CM should either complete the handover, if it receives an affirmative result, or take appropriate actions otherwise.

7.2.1.4 CM_MIIS_If

The interface between CM and MIIS is common to the same MIH_SAP provided by MIHF since these interface's primitives are part of the IEEE 802.21 MIH protocol. As such we will not detail on this, limiting to just list the 802.21 primitives exchanged.

- **MIH_Get_Information.request and MIH_Get_Information.response**

7.2.2 Flow Manager

7.2.2.1 FM_UME_If

This is the interface between the Flow Manager (FM) and the Unicast Mobility Engine (UME). This interface is an internal WP4 interface.

7.2.2.1.1 FM_UME_ActivateMobility

FM_UME_ActivateMobility.request

Function

This message is used to notify the Unicast Mobility Engine to trigger the mobility protocol.

Semantics of the service primitive

```
FM_UME_ActivateMobility.request (
    Mobile_Terminal_ID,
    Interface_ID
)
```

Parameter	Type	Description
Mobile_Terminal_ID	STRING	The identifier of the Mobile Terminal (usually a NAI)
Interface_ID	STRING	The identifier of the interface where to activate mobility

Table 7: FM_UME_ActivateMobility.request parameter list

When generated

The message is generated when the FM is notified that a new node has attached to the MAR. It forwards this notification to the UME through this message.

Effect on receipt

After receiving this message the UME should start the Mobility Protocol for the mentioned node.

FM_UME_ActivateMobility.response

Function

This message is used to notify the FM that the mobility protocol has finished the setup for the mobile terminal.

Semantics of the service primitive

```
FM_UME_ActivateMobility.response (
    Mobile_Terminal_ID,
    Interface_ID,
    ResultCode
)
```

Parameter	Type	Description
Mobile_Terminal_ID	STRING	The identifier of the Mobile Terminal (usually a NAI)
Interface_ID	STRING	The identifier of the interface where to activate mobility
ResultCode	UINT_8	The result of the protocol setup. (0 on OK, otherwise return an error code)

Table 8: FM_UME_ActivateMobility.response parameter list

When generated

The message is generated by the UME when the mobility procedure of the protocol is over. It contains the result of this process.

Effect on receipt

After receiving this message, the FM should either complete the handover, if it receives an affirmative result, or take appropriate actions otherwise.

7.2.2.2 FM_NME_If

This is the interface between the Flow Manager (FM) and the Nemo Mobility Engine (NME). This interface is an internal WP4 interface, and is described in more detail in Section 7.2.5.

7.2.2.2.1 FM_NME_IPConf

FM_NME_IPConf.request

Function

This message is used to notify the NEMO Mobility Engine that a mMAR has joined and needs to configure an IP address.

Semantics of the service primitive

```
FM_NME_IPConf.request (
    Mobile_MAR_ID,
    Interface_ID
)
```

Parameter	Type	Description
Mobile_MAR_ID	STRING	The identifier of the Mobile MAR
Interface_ID	STRING	The identifier of the interface where to configure the address

Table 9: FM_NME_IPConf.request parameter list

When generated

The message is generated when the FM is notified that an mMAR has attached to the MAR and forwards this notification to the NME through this message.

Effect on receipt

After receiving this message the NME should advertise an IPv6 prefix to the mMAR.

FM_NME_IPConf.response

Function

This message is used to notify the FM that the mobility protocol has finished the setup for the mobile MAR.

Semantics of the service primitive

```
FM_NME_IPConf.response (
    Mobile_MAR_ID,
    Interface_ID,
    ResultCode
)
```

Parameter	Type	Description
Mobile_MAR_ID	STRING	The identifier of the Mobile MAR
Interface_ID	STRING	The identifier of the interface where to configure the address
ResultCode	UINT_8	The result of the address setup. (0 on OK, otherwise return an error code)

Table 10: FM_NME_IPConf.response parameter list

When generated

The message is generated by the NME when the configuration procedure is over. It contains the result of this process.

Effect on receipt

After receiving this message, the FM should either consider the registration successful, if it receives an affirmative result, or take appropriate actions otherwise.

7.2.2.2.2 FM_NME_ActivateMobility

FM_NME_ActivateMobility.request

Function

This message is used to notify the NEMO Mobility Engine to trigger the registration at the S-MAR of a MN in the NEMO.

Semantics of the service primitive

```
FM_NME_ActivateMobility.request (
    Mobile_Terminal_ID,
    Interface_ID
)
```

Parameter	Type	Description
Mobile_Terminal_ID	STRING	The identifier of the Mobile Terminal (usually a NAI)
Interface_ID	STRING	The identifier of the interface where to activate mobility

Table 11: FM_UME_ActivateMobility.request parameter list

When generated

The message is generated when the FM is notified that a new node has attached to the mMAR or by the CM when the mMAR has successfully joined a new MAR and the mMAR's mobility procedure is over.

Effect on receipt

After receiving this message, the NME should start the Mobility Protocol for the mentioned node issuing a NEMO PBU to the S-MAR.

FM_NME_ActivateMobility.response

Function

This message is used to notify the FM that the mobility protocol has finished the setup for the mobile terminal.

Semantics of the service primitive

```
FM_NME_ActivateMobility.response (
    Mobile_Terminal_ID,
    Interface_ID,
    ResultCode
)
```

Parameter	Type	Description
Mobile_Terminal_ID	STRING	The identifier of the Mobile Terminal (usually a NAI)
Interface_ID	STRING	The identifier of the interface where to activate mobility
ResultCode	UINT_8	The result of the protocol setup. (0 on OK otherwise return an error code)

Table 12: FM_UME_ActivateMobility.response parameter list

When generated

The message is generated by the NME when the mobility procedure of the protocol is over. It contains the result of this process.

Effect on receipt

After receiving this message, the FM, should either conclude the operation, if it receives an affirmative result or notify the CM if the message was generated upon an mMAR handover. Appropriate actions are taken otherwise.

7.2.2.3 FM_MUME_If

This is the interface between the Flow Manager (FM) and the Multicast Mobility Engine (MUME). This interface is an internal WP4 interface, and is described in more detail in [5].

7.2.2.4 FM_FM_If and CM_FM_If

The interfaces between CM and FM and between FMs are common to the same MIH_SAP provided by MIHF since these interfaces' primitives are part of the IEEE 802.21 MIH protocol. The interface will reuse the existing primitives and parameters defined in the IEEE 802.21 standard [7], which should be consulted for further details. Concretely, the CM and FM (as well as between FMs) will exchange the following handover-related 802.21 primitives:

- **MIH_N2N_HO_Query_Resources.request and MIH_N2N_HO_Query_Resources.response**
- **MIH_N2N_HO_Commit.request and MIH_N2N_HO_Commit.response**
- **MIH_N2N_HO_Complete.request and MIH_N2N_HO_Complete.response**
- **MIH_MN_HO_Candidate_Query.request and MIH_MN_HO_Candidate_Query.response**
- **MIH_MN_HO_Commit.request and MIH_MN_HO_Commit.response**
- **MIH_MN_HO_Complete.request and MIH_MN_HO_Complete.response**

7.2.3 Unicast Mobility Engine

7.2.3.1 CM_UME_If

See Section 7.2.1.1.

7.2.3.2 FM_UME_If

See Section 7.2.2.1.

7.2.4 Multicast Mobility Engine

The interfaces and primitives relevant to this block are described in detail in [5]. As such, please refer to this document for having a better notion of how multicast-related operations are executed in MEDIEVAL.

7.2.5 NEMO Mobility Engine

7.2.5.1 CM_NME_If

See Section 7.2.1.2.

7.2.5.2 FM_NME_If

See Section 7.2.2.2.

8 Summary and conclusion

This deliverable describes a mobility architecture based on the “Distributed Mobility Management” (DMM) model currently under study in IETF within MEXT Working Group[46]. Main idea is to distribute mobility anchors at the edge of mobile networks and to activate mobility resources only for applications/flows which need them. The objective is to verify the benefits of this model when applied to video services. In our view a flatter mobility plus an optimised and possibly dynamic CDN distribution could represent a good alternative to traditional core anchoring models to cope with the increasing demand for high bandwidth consuming video services.

The proposed distributed mobility management architecture considers both global (inter-domain) and local (intra-domain) mobility domains/scenarios and is based on the already existing IP mobility protocols: MIPv6 (inter-domain) and PMIPv6 (intra-domain).

Along with architectural choices description, some detailed MSCs for different mobility scenarios have been depicted with the aim to provide the description of how the mobility subsystem should work. This is a basic step for the upcoming specification and implementation phases. Always in this direction a detailed specification of interfaces has also been provided.

Next specification and implementation work will allow to validate the architecture and to perform some experimental evaluation of effective advantages (e.g., in terms of better scalability and reliability, lower signalling overhead and shorter handover latencies, better control on the mobility granularity offered by the network) of a DMM based approach when compared to traditional core based anchoring models.

With the feedback and experience gained from initial implementation experience, as well as other validation/evaluation means (e.g., simulation), the specification defined in this deliverable will be subject to revision, and the final architecture will be part of D4.3 [41].

Acknowledgements and disclaimer

This work was partially funded by the European Commission within the 7th Framework Program in the context of the ICT project MEDIEVAL (Grant Agreement No. 258053). The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the MEDIEVAL project or the European Commission.

References

[1] MEDIEVAL: MultiMEDia transport for mobIlE Video AppLications http://www.ict-MEDIEVAL.eu/, retrieved June 2011

[2] MEDIEVAL Project, Deliverable D1.1 – "Preliminary architecture design", July 2011

[3] MEDIEVAL Project, Deliverable D2.1 – "Requirements for video service control", July 2011

[4] MEDIEVAL Project, Deliverable D3.1 – "Concepts for Wireless Acess in relation to cross-layer optimisation", July 2011

[5] MEDIEVAL Project, Deliverable D4.2 – "IP Multicast Mobility Solutions for Video Services" July 2011

[6] MEDIEVAL Project, Deliverable D5.1 – "Transport Optimisation: initial architecture"

[7] LAN/MAN Committee of the IEEE Computer Society, "IEEE Std 802.21-2008, Standards for Local and Metropolitan Area - Part 21: Media Independent Handover Services", 2009

[8] 3GPP Specifications TS23.402, http://www.3gpp.org/ftp/Specs/html-info/23402.htm, retrieved June 2011

[9] T. Melia, A. de la Oliva, N. Amram, M. Wetterwald, L. Marchetti, G. Kunzmann, D. Munaretto, D. Chiarotto, "Efficient Video Delivery in Mobile Wireless Networks: the MEDIEVAL project",. Submitted to Bell Labs Technical Journal (BLTJ)

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

[11] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008

[12] H. Chan (Ed.), "Problem statement for distributed and dynamic mobility management", IETF Draft, March 2011, draft-chan-distributed-mobility-ps-01.txt, presented in the 80th IETF (Prague, March 2011)

[13] H. Yokota, P. Seite, E. Demaria, Z.Cao, "Use case scenarios for Distributed Mobility Management", IETF Draft, October 2010, draft-yokota-dmm-scenario-00.txt, presented in the 79th IETF (Beijing, November 2010)

[14] P. Seite, "Dynamic Mobility anchoring", IETF Draft, May 2010 draft-seite-netext-dma-00.txt

[15] P. Bertin, "A Distributed Dynamic Mobility Management Scheme designed for Flat IP Architectures", New Technologies, Mobility and Security, 2008

[16] C. J. Bernardos, A. de la Oliva, F. Giust, "A IPv6 Distributed Client Mobility Management approach using existing mechanisms", IETF Draft, March 2011, draft-bernardos-mext-dmm-cmip-00.txt, presented in the 80th IETF (Prague, March 2011)

[17] A. de la Oliva, F. Giust, C. J. Bernardos, "Distributed Mobility Management using IEEE 802.21", https://mentor.ieee.org/802.21/dcn/11/21-11-0045-00-0000-dmm-approach-using-21.pptx, presented in the 43th IEEE 802.21 meeting, March 2011.

[18] F. Giust, A. de la Oliva, C. J. Bernardos, "Flat Access and Mobility Architecture: an IPv6 Distributed Client Mobility Management solution", best paper award at Mobiworld 2011, workshop collocated with INFOCOM 2011

[19] F. Giust, C. J. Bernardos, S. Figueiredo, P. Neves, T. Melia, "A Hybrid MIPv6 and PMIPv6 Distributed Mobility Management: the MEDIEVAL approach", accepted in Mediawin 2011, workshop collocated with ISCC 2011

[20] P. Seite, T. Melia, "Connection Manager requirements", IETF Draft, October 2010, draft-seite-mif-connection-manager-02.txt, presented in the 79th IETF (Beijing, November 2010)

[21] T. Melia (Ed.), S. Gundavelli (Ed.), "Logical Interface Support for multi-mode IP Hosts", IETF Draft, March 2011, draft-ietf-netext-logical-interface-support-02, presented in the 80th IETF (Prague, March 2011)

[22] A. de la Oliva, I. Soto, M. Calderon, C. J. Bernardos, "Analysis of the combinations of different IP mobility schemes", submitted to Wireless and Personal Communication Journal

[23] A. de la Oliva, M. Calderon, C. J. Bernardos, R. Wakikawa, "Client and Network-based Dual Stack Mobility Management", submitted to IEEE Wireless Communications Magazine

[24] I. Soto, C. J. Bernardos, M. Calderon, T. Melia, "PMIPv6: A Network-Based Localized Mobility Management Solution", The Cisco Internet Protocol Journal (IPJ), Volume 13, Number 3 (September 2010)

[25] C. J. Bernardos, M. Gramaglia, L. M. Contreras, M. Calderon, I. Soto, "Network-based Localized IP mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, September 2010

[26] A. de la Oliva, M. Calderon, T. Melia, J. C. Zuniga, "IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks", Submitted to IEEE Communications Magazine, Feature Topic on Traffic Management for Mobile Broadband Networks

[27] Carlos J. Bernardos (Ed.), "Proxy Mobile IPv6 Extensions to Support Flow Mobility", IETF Draft, March 2011, draft-bernardos-netext-pmipv6-flowmob-03, presented in the 80th IETF (Prague, March 2011)

[28] I. Soto, C. J. Bernardos, M. Calderon, A. Banchs, A. Azcorra, "NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios", IEEE Communications Magazine, Automotive Networking - Technology, Design, and Applications series, Vol.47, No.5, May 2009.

[29] T. Schmidt, M. Waehlisch, S. Krishnan, "Base Deployment for Multicast Listener Support in PMIPv6 Domains", IETF Draft, October 2010, draft-ietf-multimob-pmipv6-base-solution-06.txt,

[30] J. C. Zúñiga, A. Rahman, L. M. Contreras, C. J. Bernardos, I. Soto, "Support Multicast Services Using Proxy Mobile IPv6", IETF Draft, March 2011, draft-zuniga-multimob-smspmip-05.txt, presented in the 80th IETF (Prague, March 2011)

[31] L.M. Contreras, C.J. Bernardos, I. Soto, "Rapid acquisition of the MN multicast subscription after handover", IETF Draft, June 2010, draft-contreras-multimob-rams-00.txt, presented in the 79th IETF (Beijing, November 2010)

[32] D. Corujo, S. Figueiredo, R. L. Aguiar, "Media-Independent Multicast Signaling for Enhanced Video Performance in the MEDIEVAL Project", Accepted in Future Network and Mobile Summit 2011

[33] L. M. Contreras, C. J. Bernardos, I. Soto, "RAMS: Improved Handover Performance for Multicast Traffic in PMIPv6", Accepted for publication in Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications

[34] S. Randriamasy (Ed.), "ALTO in Mobile Core", IETF Draft, March 2011, draft-randriamasy-alto-mobile-core-01.txt, presented in the 80th IETF (Prague, March 2011)

[35] S. Randriamasy, (Ed.), "Multi-Cost ALTO", IETF Draft, March 2011, draft-randriamasy-alto-multi-cost-02, presented in the 80th IETF (Prague, March 2011)

[36] S. Randriamasy, (Ed.), "Provider Confidential ALTO with Relays", IETF Draft, March 2011, draft-randriamasy-alto-relay-00, Offline discussion in the 80th IETF (Prague, March 2011)

[37] T. Melia, F. Giust, A. de la Oliva, C. J. Bernardos, R. Manfrin, M. Wetterwald, "IEEE 802.21 and Proxy Mobile IPv6: A Network Controlled Mobility Solution", accepted in Future Network and Mobile Summit 2011

[38] H. A. Chan, A. de la Oliva, J. Jee, "Revision to IEEE 802.21c Single Radio Handover Proposal", https://mentor.ieee.org/802.21/dcn/11/21-11-0036-01-srho-comments-to-21c-proposal.doc, presented in the 43th IEEE 802.21 meeting, March 2011

[39] H. A. Chan, J. Jee, A. de la Oliva, G. Babut, “Candidate Media Independent Services Discussion”, https://mentor.ieee.org/802.21/dcn/11/21-11-0046-01-0000-media-independent-service.ppt, presented in the 43th IEEE 802.21 meeting, March 2011

[40] M. Gramaglia, P. Serrano, J. A. Hernández, M. Calderon, C. J. Bernardos, “New Insights from the Analysis of Free Flow Vehicular Traffic in Highways”, accepted in IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WOWMOM 2011)

[41] MEDIEVAL Project, Deliverable D4.3 – “Final Specification for mobility components & interfaces”, June 2012

[42] R. Moskowitz (Ed.) ,”Host Identity Protocol Version 2”, RFC 5201, April 2008

[43] H. Haverinen, Ed. ,” Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”, RFC 4186, January 2006

[44] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005

[45] IETF Multiple Interfaces (MIF) Working Group; current charter at http://datatracker.ietf.org/wg/mif/charter/

[46] IETF Mobility Extensions (MEXT) Working Group; current charter at http://datatracker.ietf.org/wg/mext/charter/

Annex I: Relevant contributions to dissemination

This annex provides a selected list of the dissemination work on technological topics considered within WP4 in the first year of the MEDIEVAL project. Both published papers for conferences, journals, magazines and contributions to standardization are presented.

I.1 Papers for Conferences

Title: **Flat Access and Mobility Architecture: an IPv6 Distributed Client Mobility Management Solution**

Authors: Fabio Giust, Antonio de la Oliva, Carlos J. Bernardos

Conference: MobiWorld 2011 workshop in conjunction with INFOCOM 2011, Shanghai, China, April 2011 (Best paper award)

MEDIEVAL project aims to deploy a distributed mobility management (DMM) architecture. This paper proposes the host based solution based on Mobile IPv6 and the use of Cryptographic Generated Addresses.

Abstract

The use of centralized mobility management approaches - such as Mobile IPv6 – poses some difficulties to operators of current and future networks, due to the expected large number of mobile users and their exigent demands. All this has triggered the need for distributed mobility management alternatives, that alleviate operators' concerns allowing for cheaper and more efficient network deployments. This paper proposes a distributed mobility solution, based on Mobile IPv6 and the use of Cryptographic Generated Addresses. We analytically compare the solution to Mobile IPv6, and derive in which scenarios it performs best.

Title: **A Hybrid MIPv6 and PMIPv6 Distributed Mobility Management: the MEDIEVAL approach**

Authors: Fabio Giust, Carlos J. Bernardos, Sergio Figueiredo, Pedro Neves

Conference: MediaWiN 2011 workshop in conjunction with ISCC 2011, Corfu, Greece, June 2011

In MEDIEVAL both network and host based mobility solutions are considered as possible deployment solutions of DMM architecture. This paper presents the MEDIEVAL proposed hybrid solution where the two schemes are extended and merged into a hybrid network.

Abstract

Video is a major challenge for the future mobile Internet as it is foreseen to account for close to 64% percent of consumer mobile traffic by 2013. However, the current Internet, and in particular the mobile Internet, was not designed with video requirements in mind and, as a consequence, its architecture is very inefficient when handling this type of traffic. This paper presents a novel mobility architecture inspired by the Distributed Mobility Management paradigm, capable of coping with the future video traffic demands, in a distributed and more scalable way. In the proposed solution, mobility support services are spread among several nodes at the edge of the network, thus realizing a flatter architecture and pushing services closer to the terminals. Our approach overcomes some of the major limitations of centralized IP mobility management solutions, by extending existing standard protocols.

Title: **IEEE 802.21 and Proxy Mobile IPv6: A Network Controlled Mobility Solution**

Authors: T. Melia et al.

Conference: Future Network and MobileSummit 2011, Warsaw, Poland, June 2011

This paper presents the integration of Media Independent Handover Services with PMIPv6 for an optimized Make-Before-Break approach for network based handovers. The MEDIEVAL effective implementation of such approach will start from here.

Abstract

IP Mobility has been a deeply investigated topic in the past years and standardization bodies have specified a wide suite of protocols enabling seamless mobility across heterogeneous wireless access technologies. However, despite the constant and expensive effort, mobility helping technologies are not yet widely spread as compared to other emerging technologies such as Wireless LAN hotspots. This paper aims at filling the gap between research and real case deployments by specifying and implementing a novel solution for mobility support in wireless heterogeneous environments taking into consideration the trends in standardization bodies (IETF, 3GPP and IEEE 802.21). Our solution includes protocol operations and associated functions installed in both mobile devices and network nodes. Mobility management is achieved via the Proxy Mobile IPv6 (PMIPv6) protocol while optimized handover control is provided by the integration of the IEEE 802.21 framework with PMIPv6. The paper evaluates the performance of the proposed platform, which shows results obtained through live experiments on the field, thus making concrete step toward real deployment.

Title: **A Network-based Localized Mobility Solution for Distributed Mobility Management**

Authors: Fabio Giust, Antonio de la Oliva, Carlos J. Bernardos, Rui Pedro Ferreira Da Costa

Conference: Mobility Management for Flat Networks – MMNF 2011 workshop in conjunction with WPMC 2011, Brest, France, October 2011

MEDIEVAL project aims to deploy distributed mobility management (DMM) architecture. This paper addresses the network based solution based on extensions to PMIPv6.

<u>Abstract</u>

Internet traffic has increased steeply in recent years, due in great part to social platforms and peer-to-peer networks. In addition, users' wireless access represents an ever-growing portion of such demand, thus posing a paradigm shift in the flow of Internet information, for which most deployed architectures are not prepared for. This evolution in user traffic demand is tackled by a different approach for IP mobility, called Distributed Mobility Management, that is focusing on moving the mobility anchors from the core network and pushing them closer to the users, at the edge of the network. The work presented here copes with the distributed approach, describing a novel solution for network-based localized mobility support in a flat architecture without central mobility anchors. It leverages PMIPv6 standard, but it is intended to overcome most of the issues in current centralized architectures, by splitting the control plane from the data plane and distributing them throughout the access networks.

I.2 Paper for Journals and Magazines

Title: **Network-based Localized IP mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization**

Authors: Carlos J. Bernardos, Marco Gramaglia, Luis M. Contreras, Maria Calderon, Ignacio Soto

Journal: Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications

Since MEDIEVAL aims at offering the best mobility management scheme according to users' mobility patterns, a further distinction between local and global mobility is done. This paper deals with local mobility where a network-based localized mobility management scheme is adopted.

<u>Abstract</u>

IP mobility support has been a hot topic over the last years, recently fostered by the role of IP in the evolution of the 3G mobile communication networks. Standardization bodies, namely IETF, IEEE and 3GPP are working on different aspects of the mobility aiming at improving the mobility experience perceived by users. Traditional IP mobility support mechanisms, Mobile IPv4 or Mobile IPv6, are based on the operation of the terminal to keep ongoing sessions despite the movement. The current trend is towards network-based solutions where mobility support is based on network operation. Proxy Mobile IPv6 is a promising specification that allows network operators to provide localized mobility support without relying on mobility functionality or configuration present in the mobile nodes, which greatly eases the deployment of the solution. This paper presents Proxy Mobile IPv6 and the different extensions that are been considered by the

standardization bodies to enhance the basic protocol with interesting features needed to offer a richer mobility experience, namely, flow mobility, multicast and network mobility support.

Title: **IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks**

Authors: Antonio de la Oliva, Carlos J. Bernardos, Maria Calderon, Telemaco Melia and Juan Carlos Zuniga

Magazine: IEEE Communications

Another key-feature in the MEDIEVAL architecture is the support of IP flow mobility since mobility support is envisioned to be provided at IP-flow granularity, differently from the classical mobility approaches. This paper presents and compares two possible approaches to IP flow mobility offloading that are currently being considered by the IETF: the first one is based on extending client-based IP mobility solutions and the second one is based on extending network-based IP mobility solutions.

Abstract

The recent proliferation of smartphone-based mobile Internet services has created an extraordinary growth in data traffic over cellular networks. This growth has fostered interest in exploring alternatives to alleviate data congestion while delivering a positive user experience. It is known that a very small number of users and applications cause a big percentage of the traffic load. Hence, adopting smarter traffic management mechanisms is one of the considered alternatives. These mechanisms allow Telecom operators to move selected IP data traffic, for instance between the cellular infrastructure and the WLAN infrastructure, which is considered a key feature in the latest 3GPP and IETF specifications. This paper presents and compares two possible approaches to IP flow mobility offloading that are currently being considered by the IETF. The first one is based on extending existing client-based IP mobility solutions to allow flow mobility where the user terminal is fully involved in the mobility process, and the second one is based on extending current network-based IP mobility solutions where the user terminal is not aware of the mobility.

Title: **IP flow mobility in PMIv6 based networks: solution design and experimental evaluation**

Authors: Telemaco Melia, Carlos J. Bernardos, Antonio de la Oliva, Fabio Giust, Maria Calderon

Journal: Springer Wireless Personal Communications

MEDIEVAL implementation of IP flow mobility will mainly deal with PMIPv6 extensions. This paper is in line with this scope.

Abstract

The capacity of offloading selected IP data traffic from 3G to WLAN access networks is considered a key feature in the upcoming 3GPP networks, the main goal being to alleviate data congestion in cellular networks while delivering a positive user experience. Lately, the 3GPP adopted solutions that enable mobility of IP-based wireless devices relocating mobility functions from the terminal to the network. To this end, the IETF has standardized ProxyMobile IPv6 (PMIPv6), a protocol capable to hide often complex mobility procedures from the mobile devices. This paper, in line with the mentioned offload requirement, further extends Proxy Mobile IPv6 to enable dynamic IP flow mobility management across access wireless networks according to operator policies. Considering energy consumption as a critical aspect for hand-held devices and smart-phones, we assess the feasibility of the proposed solution and provide an experimental analysis showing the cost (in terms of energy consumption) of simultaneous packet transmission/reception using multiple network interfaces. The end-to-end system design has been implemented and validated by means of an experimental network setup showing the achieved Quality of Experience improvement compared to state of the art solutions.

Title: **IEEE 802.21: Media independence beyond handover**

Authors: Antonio de la Oliva, Ignacio Soto, Albert Banchs, Johannes Lessmann, Christian Niephaus, Telemaco Melia

Journal: Elsevier, Computer Standards & Interfaces

IEEE 802.21 is a basic part of MEDIEVAL cross-layer architecture. This paper aims at updating the reader with the main challenges and functionalities required to create a Media Independence Service Layer

Abstract

The IEEE 802.21 standard facilitates media independent handovers by providing higher layer mobility management functions with common service primitives for all technologies. Right after the base specification was published, several voices rose up in the working group advocating to broaden the scope of IEEE 802.21 beyond handovers. This paper aims at updating the reader with the main challenges and functionalities required to create a Media Independence Service Layer, through the analysis of scenarios which are being discussed within the working group: 1) Wireless Coexistence, and 2) Heterogeneous Wireless Multihop Backhaul Networks.

Title: **PMIPv6: A Network-Based Localized Mobility Management Solution**

Authors: Carlos J. Bernardos, Maria Calderon, Ignacio Soto, Telemaco Melia

Journal: The Cisco Internet Protocol Journal

Since MEDIEVAL aims at offering the best mobility management scheme according to users' mobility patterns, a further distinction between local and global mobility is done. This paper deals with local mobility where a network-based localized mobility management scheme is adopted.

Abstract

Traditional IP mobility procedures are based on functions residing in both the mobile terminal and the network. Recently, we have been assisting in a shift in IP mobility protocol design, mostly focusing on solutions that relocate mobility procedures from the mobile device to network components. This new approach, known as Network-Based Localized Mobility Management (NetLMM), allows conventional IP devices (for example, devices running standard protocol stacks) to roam freely across wireless stations belonging to the same local domain. This property is appealing from the operator's viewpoint because it allows service providers to enable mobility support without imposing requirements on the terminal side (for example, software and related configuration). For this purpose the Internet Engineering Task Force (IETF) has standardized Proxy Mobile IPv6 (PMIPv6). This article details the Proxy Mobile IPv6 protocol, providing a general overview and an exhaustive description of a few selected functions.

I.3 Contributions to Standardization

Title: **Use case scenarios for Distributed Mobility Management**

Authors: H. Yokota, P. Seite, E. Demaria, Z.Cao

IETF Network WG

MEDIEVAL's research team is very active in IETF in pushing and contributing to the Distributed Mobility Management (DMM) concept. A significant example is this standardization submission, which explores the applicability of Distributed Mobility Management (DMM) and use case scenarios for different parts of the mobile network.

Abstract

This document explores applicability of Distributed Mobility Management (DMM) and use case scenarios for different parts of the mobile network. DMM approaches and scenarios are divided into two cases: partially and fully distributed. For each case, benefits and issues are provided. It also refers to applicability of existing protocols and necessity of development of new protocols in order to provide a guideline for best suited solutions for the target architecture.

Title: **A IPv6 Distributed Client Mobility Management approach using existing mechanisms**

Authors: Carlos J. Bernardos, Antonio de la Oliva, Fabio Giust

IETF MEXT WG

This standardization submission, in line with the DMM approach proposed in MEDIEVAL, focuses on host based solution and Mobile IPv6 extensions.

Abstract

The use of centralized mobility management approaches -- such as Mobile IPv6 -- poses some difficulties to operators of current and future networks, due to the expected large number of mobile users and their exigent demands. All this has triggered the need for distributed mobility management alternatives, that alleviate operators' concerns allowing for cheaper and more efficient network deployments. This draft describes a possible way of achieving a distributed mobility behavior with Client Mobile IP, based on Mobile IPv6 and the use of Cryptographic Generated Addresses.

Title: **A PMIPv6-based solution for Distributed Mobility Management**

Authors: Carlos J. Bernardos, Antonio de la Oliva, Fabio Giust, T. Melia

IETF MEXT WG

This standardization submission, in line with the DMM approach proposed in MEDIEVAL, focuses on network based solution and PMIPv6 extensions.

Abstract

The number of mobile users and their traffic demand is expected to be ever-increasing in future years, and this growth can represent a limitation for deploying current mobility management schemes that are intrinsically centralized, e.g., Mobile IPv6 and Proxy MIPv6. For this reason it has been waved a need for distributed and dynamic mobility management approaches, with the objective of reducing operators' burdens, evolving to a cheaper and more efficient architecture. This draft describes a solution to distribute the data forwarding plane on Proxy Mobile IPv6 domains, thus trying to overcome the suboptimal data path introduced when the LMA is traversed.

Title: **Proxy Mobile IPv6 Extensions to Support Flow Mobility**

Authors: Carlos J. Bernardos Ed.

IETF NETEXT WG

This standardization submission, in line with the IP flow mobility solutions proposed in MEDIEVAL, focuses on PMIPv6 extensions to support flow mobility.

Abstract

Proxy Mobile IPv6 (PMIPv6) is a network-based localized mobility management protocol that enables mobile devices to connect to a PMIPv6 domain and roam across gateways without changing their IP addresses. PMIPv6 basic specification also provides limited multihoming support to multi-mode mobile devices. The ability of movement of selected flows from one access technology to another is missing in basic PMIPv6. This document describes enhancements to the Proxy Mobile IPv6 protocol that are required to support flow mobility over multiple physical interfaces.

Title: **Rapid acquisition of the MN multicast subscription after handover**

Authors: Carlos J. Bernardos, Luis M. Contreras, Ignacio Soto

IETF MULTIMOB WG

The MEDIEVAL mobile architecture aims at providing support not only to unicast flows, but also to multicast transmissions, for which a dedicated effort was put in the investigation in order to integrate the two functionalities into the same framework. The following paper is part of the solution for PMIPv6.

Abstract

A new proposal is presented for speeding up the acquisition by the MAG of the MN's active multicast subscription information, in order to accelerate the multicast delivery to the MN during handover. To do that, an extension of the current PMIPv6 protocol is required. The solution described in this memo is not only applicable to the base multicast solution, but also it can be applied to other solutions envisioned as possible architectural evolutions of it. Furthermore, it is also independent of the role played by the MAG within the multicast metwork (either acting as MLD proxy or multicast router).

Title: **Logical Interface Support for multi-mode IP Hosts**

Authors: T. Melia, Ed., S. Gundavelli, Ed.

IETF NETEXT WG

This paper focuses on the logical interface concept. The logical interface support is a key point of MEDIEVAL mobile node architecture to support different mobility features of multi-mode hosts. A specific component, the Connection Manager, has been defined to cope with this.

Abstract

A Logical Interface is a software semantic internal to the host operating system. This semantic is available in all popular operating systems and is used in various protocol implementations. The Logical Interface support is required on the mobile node operating in a Proxy Mobile IPv6 domain, for leveraging various network-based mobility management features such as inter-technology handoffs, multihoming and flow mobility support. This document explains the operational details of Logical Interface construct and the specifics on how the link-layer implementations hide the physical interfaces from the IP stack and from the network nodes on the attached access networks. Furthermore, this document identifies the applicability of this approach to various link-layer technologies and analyzes the issues around it when used in context with various mobility management features.

Title: **Support Multicast Services Using Proxy Mobile IPv6**

Authors: J.C. Zuniga, A. Rahman, L.M. Contreras, C.J. Bernardos, I. Soto

IETF MULTIMOB WG

The MEDIEVAL mobile architecture aims at providing support not only to unicast flows, but also to multicast transmissions, for which a dedicated effort was put in the investigation in order to integrate the two functionalities into the same framework. The following paper is part of the solution for PMIPv6.

Abstract

The MULTIMOB group has specified a base solution to support IP multicasting in a PMIPv6 domain [RFC6224]. In this document, an enhancement is proposed to the base solution to use a multicast tree mobility anchor as the topological anchor point for multicast traffic, while the MAG remains as an IGMP/MLD proxy. This enhancement provides benefits such as reducing multicast traffic replication and supporting different PMIPv6 deployments scenarios.

Title: **Distributed Mobility Management using IEEE 802.21**

Authors: Antonio de la Oliva, Fabio Giust, Carlos J. Bernardos

Presentation at IEEE 802.21 session #43 in Singapore

The focus of this presentation concerns the application and the extensions of IEEE 802.21 framework to support optimized handovers and cross-layer interaction in mobility architecture based on the distributed mobility management approach.

Abstract

Mechanism to support DMM through IEEE 802.21.

Title: **Network-based Distributed Mobility Approach**

Authors: Antonio de la Oliva, Fabio Giust, Carlos J. Bernardos

Presentation at IEEE 802.21 session #46 in Bangkok

The work presents different approaches (partially and fully distributed) for network-based distributed mobility management with the integration of IEEE 802.21 framework for network-controlled handovers.

Abstract

This document presents an IEEE 802.21 based mechanism to enabled network based distributed mobility management.