



| | |
|---|---|
| Project Number: | **CELTIC / CP7-011** |
| Project Title: | Mobile Networks Evolution for Individual Communications Experience – MEVICO |
| Document Type: | PU (Public) |

| | |
|---|---|
| Document Identifier: | D2.2 |
| Document Title: | **Architectural EPC extensions for supporting heterogeneous mobility schemes** |
| Source Activity: | WP2 |
| Main Editor: | Suneth Namal (CWC) |
| Authors: | Jörgen ANDERSSON (Ericsson AB), Erick BIZOUARN (ALBLF), Michael BOC (CEA), Alexandru PETRESCU (CEA), Çağatay EDEMEN (AVEA), Salih ERGÜT (Turk Telekom), Zoltán FAIGL (BME-MIK), Jean-Luc LAFRAGETTE (ALBLF), Conny LARSSON (Ericsson AB), Rashmi PURUSHOTHAMA (Ericsson AB), Ahmet Serdar TAN (Turk Telekom), Engin ZEYDAN (AVEA), László BOKOR (BME-MIK), Khadija Daoud (Orange), Wolfgang HAHN (NSN) |
| Status / Version: | 0.1 |
| Date Last changes: | 31.01.2013 |
| File Name: | D2.2 Architectural EPC extensions for supporting heterogeneous mobility schemes.doc |


| | |
|---|---|
| Abstract: | This document describes mobility management schemes in heterogeneous networks in the scope of MEVICO, WP2. The document presents partner specific technologies, their impacts on MEVICO architecture options and Key Performance Indicators (KPIs) related to different technologies. Finally, the document discusses integration issues of proposed WP2 technologies and their future research directions. |



Keywords:
WP2 technologies, scenarios, architecture options, integration issues, KPIs, future directions


| Document History: | |
|---|---|
| 01.12.2011 | Draft document with TOC created… |
| 23.04.2012 | AALTO revised TRILL |
| 18.07.2012 | NSN Germany updated "Dynamic mobility anchoring" |
| 26.07.2012 | France Telecom updated section 2.6 |
| 02.08.2012 | Turk Tele updated user cooperation |
| 05.10.2012 | Ericsson updated Terminal based mobility management |
| 19.10.2012 | NSN-FIN updated section 3.3 |
| 25.10.2012 | BME-MIK updated section 4.1 |
| 29.10.2012 | ALU updated section 2.1 |
| 31.10.2012 | CEA added text on PMIP-RO |

# Table of contents

## Authors


| Partner | Name | Phone / Fax / e-mail |
|---|---|---|
| BME-MIK | Zoltán FAIGL | |
| | | Phone: +36 70 943 9862 |
| | | e-mail: zfaigl@mik.bme.hu |
| CEA | Michael BOC | |
| | | Phone: +33 16 908 1984 |
| | | e-mail: michael.boc@cea.fr |
| CEA | Alexandru PETRESCU | |
| | | Phone: +33 16 908 9223 |
| | | e-mail: alexandru.petrescu@cea.fr |
| ALBLF | Jean-Luc LAFRAGETTE | |
| | | Phone: +33 13 077 2738 |
| | | e-mail: jean-luc.lafragette@alcatel-lucent.com |
| ALBLF | Erick BIZOUARN | |
| | | Phone: +33 13 077 2724 |
| | | e-mail: erick.bizouarn@alcatel-lucent.com |
| AVEA | Engin ZEYDAN | |
| | | Phone: +90 216 987 6386 |
| | | e-mail: engin.zeydan@avea.com.tr |
| AVEA | Çağatay EDEMEN | |
| | | Phone: +90 216 987 6386 |
| | | e-mail: cagatay.edemen@avea.com.tr |
| TURK TELEKOM | Ahmet Serdar TAN | |
| | | Phone: +90 212 309 9975 |
| | | e-mail: ahmetserdar.tan@turktelekom.com.tr |
| Ericsson AB | Rashmi PURUSHOTHAMA | |
| | | Phone: +46 10 715 5964 |
| | | e-mail: rashmi.purushothama@ericsson.com |
| Ericsson AB | Jörgen ANDERSSON | |
| | | Phone:´ +46 10 719 7013 |
| | | e-mail: jorgen.andersson@ericsson.com |

| | | |
|---|---|---|
| Ericsson AB | Conny LARSSON | |
| | | Phone: +46 10 714 8458 |
| | | e-mail: conny.larsson@ericsson.com |

| | | |
|---|---|---|
| BME-MIK | László BOKOR | |
| | | Phone: +36 14 633 420 |
| | | e-mail: bokorl@hit.bme.hu |

| | | |
|---|---|---|
| Nokia Siemens Networks | Wolfgang Hahn | |
| | | Phone: +49 89 515 924122 |
| | | e-mail: wolfgang.hahn@nsn.com |

| | | |
|---|---|---|
| Nokia Siemens Networks | Johanna Heinonen | |
| | | Phone: +35 84 075 86791 |
| | | e-mail: johanna.heinonen@nsn.com |

| | | |
|---|---|---|
| Nokia Siemens Networks | Pekka Korja | |
| | | Phone: +35 84 076 65979 |
| | | e-mail: pekka.korja@nsn.com |

| | | |
|---|---|---|
| CWC | Suneth Namal | |
| | | Phone: +358417282646 |
| | | e-mail: namal@ee.oulu.fi |

## Executive Summary

The deliverable D2.2 from MEVICO proposes to address challenges of smart traffic steering and mobility management functionalities. The technology proposals included in the document may impact current mobility management and traffic steering procedures and also new problems of integration may occur. The attempt to utilize the different interfaces simultaneously may also lead to specific mobility management issues. In this document multiple access mobile technologies and impact of traffic steering on different MEVICO architecture options are presented. Then, there is a description of the chosen topics on which each partner will focus on, and how they will evaluate their proposals.
Document also describes the co-existence of different technologies in defined architecture options. Integration of technologies introduces new challenges when trying to use different interfaces which typically lead to IP configuration issues due to terminal mobility. Load balancing, flow mapping and offloading are traffic steering techniques which guarantee the optimal use of network resources. Document also addresses different mobility management techniques that are based on SIP, HIP and PMIPv6. Also the impacts on different architecture options are proposed too. Access authorization is important in mobility management point of view and attempt to exclude unauthorized users from network.

The MEVICO deliverable D2.1 [1] indicates the problems related to traffic steering, IP mobility management, identifier and locators management and support of moving networks. And D2.3 [2] presents the validation results in WP2.

## List of acronyms and abbreviations

| | |
|---|---|
| AAA | Authentication, Authorization and Accounting |
| ADSL | Asynchronous Digital Subscriber Line |
| A-GW | Access GW |
| AKA | Authentication and Key Agreement |
| ANDSF | Automatic Network Decision Selection Function |
| BEX | Base Exchange |
| BNG | Broadband Network Gateway |
| BS | Base Station |
| CAPEX | Capital Expenditure |
| CERT | Certificate |
| CMAC | Cipher-based Message Authentication Code |
| CQI | Channel Quality Indicator |
| CTS | Clear to Send |
| DEX | Diet Exchange |
| DHCP | Dynamic Host Control Protocol |
| DoS | Denial of Service |
| EC | Elliptic Curve |
| E-E | End-to-end |
| eNB | Evolved NodeB |
| eNodeB | Evolved NodeB |
| EPC | Evolved Packet Core |
| ePDG | Evolved Packet Data Gateway |
| ePGW | Evolved Packet Gateway |
| GGSN | Gateway GPRS Support Node |
| GTP | GPRS Tunneling Protocol |
| GW | Gateway |
| HA | Home Agent |
| HIP | Host Identity Protocol |
| UFA-HIP | HIP-based UFA |
| HIT | Host Identity Tag |
| HO | Handover |
| HSDPA | High-Speed Downlink Packet Access |
| HSS | Home Subscriber Server |
| IA | Intermediate Anchor |
| IKEv2 | Internet Key Exchange Protocol version 2 |
| IMS | IP Multimedia Service |
| KPI | Key Performance Indicator |
| L2 | Layer-2 |
| L3 | Layer-3 |
| LFN | Local Fixed Node |
| LMA | Local Mobility Anchor |
| LTE | Long Term Evolution |
| MAG | Mobility Anchor Gateway |
| MIIS | Media Independent Information Service |

| | |
|---|---|
| MIMO | Multiple-Input and Multiple-Output |
| MIPv6 | Mobile IPv6 |
| MME | Mobility Management Entity |
| MPTCP | MultiPath Transport Control Protocol |
| MR | Mobile Router |
| NAT | Network Address Translation |
| NEMO | Network Mobility Protocol |
| NEMO BS | NEMO Basic Support |
| NMIP | Non Mobile IP |
| OFDMA | Orthogonal Frequency Division Multiplexing |
| OPEX | Operational Expenditure |
| P-CSCF | Proxy-Call Service Control Function |
| PGW | Packet Data Network Gateway |
| PMIPv6 | Proxy Mobile IPv6 |
| PoA | Point of Access |
| POP | Point of Presence |
| PSK | Pre-shared Key |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial In User Service |
| RAN | Radio Access Network |
| RN | Relay Node |
| RTS | Request to Send |
| RTT | Round-trip time |
| SA | Security Association |
| SCTP | Stream Control Transmission Protocol |
| SEG | Security Gateway |
| SGW | Serving Gateway |
| SINR | Signal to Interference and Noise Ratio |
| TLS | Transport Layer Security |
| UE | User Equipment |
| UFA | Ultra Flat Architecture |
| UMTS | Universal Mobile Telecommunications System |
| UPnP | Universal Plug and Play |
| USIM | Universal Subscriber Identity Module |

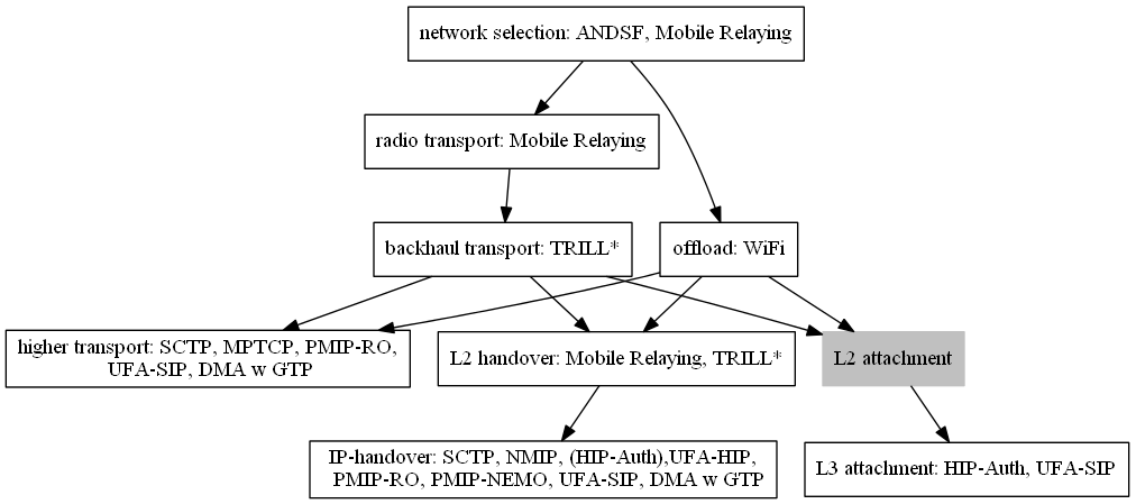
# 1. Introduction

From the facts that are shown in the MEVICO D2.1 [1], the demanding mobile and data traffic must be satisfied by the future networks. It was understood the future core networks must be capable of supporting a huge bandwidth. However, expansion of the core networks are always limited by the cost the operators would have to bear. Thus, traffic offloading is a demanding requirement in any mobile network (i.e. small cells, Wi-Fi). In this approach, roaming between different technologies must be preserved in order to ensure the efficiency. In other words, it should not affect the end user experience. Seamless handover in both application and hardware level must be preserved to support certain delay sensitive applications, such as gaming, real-time video and teleconferences. Also, it is important that the networks support smooth handover between inter system and intra system.

A decade back, majority of the mobile subscribers were using only the voice traffic except the video, online streaming or data. Later on, the newly introduced applications and services started to consume a huge bandwidth. And also preserving the service quality was a problem with the increasing number of subscribers. As a result the demand on the required network resources was increasing in terms of radio link capacity and subscriber handling capacity of the network elements. The challenge for the future networks is how to anticipate the inevitable growth of demand on the required network resources and how different technologies co-exist. The introduction of smart handsets that support multiple access technologies such as cellular, Wi-Fi and CDMA helps to anticipate the challenges.

Meantime, the different technologies that are applied in different level of the network architecture must have a good correlation among them to improve the ultimate end-user experience. The Figure 1 presents different technologies that are proposed within the scope of mobility management topics of MEVICO. The technologies have been assigned to different network layers and functionalities where they have influence on certain key performance indicators such as E-E throughput, load distribution, E-E, handover or attachment delay, etc.

This document is an attempt to summarize the technologies and to understand how they jointly can face the future challenges. Further, it presents the both horizontal and vertical co-relations of the technologies.




* TRILL (Transparent Interconnect of Lots of Links) provides Ethernet-layer mobility solution described in D2.3 [26]

**Figure 1: WP2 research technologies.**

## 1.1 Mobility in Evolved Packet Core.

The rapid growth of internet and packet data services in last few years called for a need for evolution of core network (CN). The CN of 3GPPs Universal Mobile Telecommunications System (UMTS) has been under development for last few years. The progression of the core network is called System Architecture

Evolution (SAE) and resulted in Evolved Packet Core (EPC). There are numerous benefits of SAE including flat architecture with less network nodes, smaller delays and bigger data rate support.

The radio access part has also been under development. This process is called Long Term Evolution (LTE) and the outcome is called Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). As E-UTRAN is solely packet-data based, EPC also provides the IP connectivity to non-3GPP radio access network (RAN) domains such as WLAN or WiMAX. The data flow in EPS, between EPC and different radio access technologies (RATs), is provided by two primary gateways. User data is transmitted from E-UTRANs base stations (eNodeBs) to EPC through Serving Gateway (S-GW). It is also an anchor point for intra-LTE mobility, as well as between GSM/GPRS, WCDMA/HSPA and LTE.

Packet Data Network Gateway (PDN GW) is a user plane node connecting EPC to the external IP networks and non-3GPP services. Another important node is Mobility Management Entity (MME). It is responsible for managing all control plane functions related to subscriber and session management, assigning the network resources and handling, among others, handovers (HOs). Figure 2 presents EPS architecture together with other supported RANs. Note that only key nodes for this paper are shown.

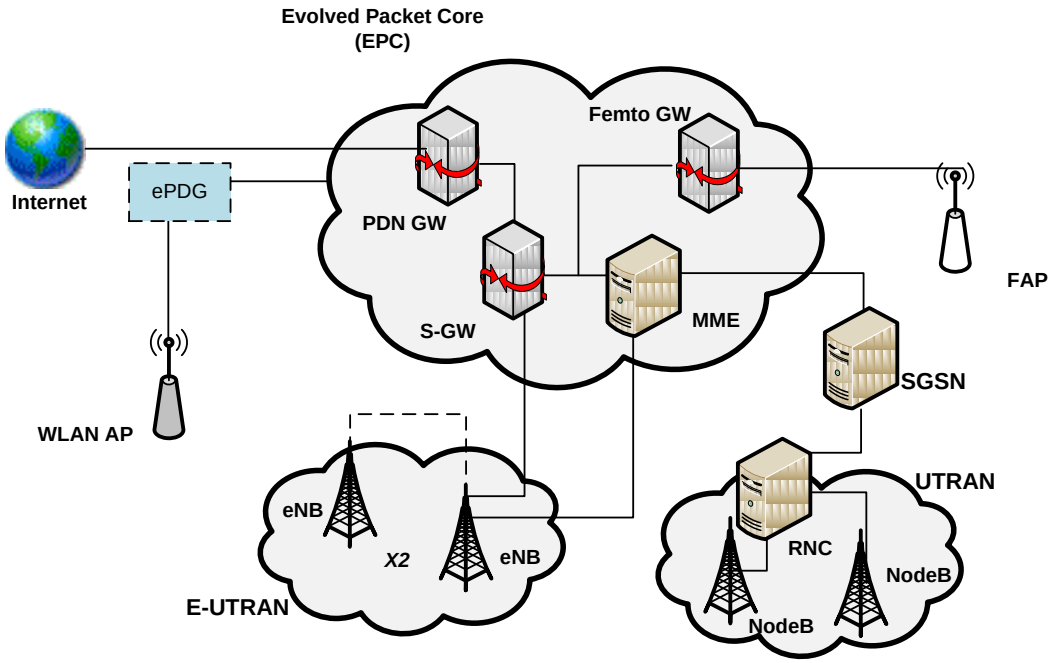



**Figure 2: Evolved packet core architecture.**

The main idea behind a handover (or handoff) is to maintain a continuous data session while being transferred to different cell. In every handover procedure there's a source cell, which UE moves from, and the target cell which UE moves to. The nodes in cells are also called accordingly. In general, all handovers are divided into preparation and execution phase. During preparation phase target cell is informed about the handover and appropriate resources (if available) are allocated in both target RAN and core network. Execution phase can be further divided into execution and completion phases. During those phases, downlink (DL) packets are buffered or forwarded to target cell. UE performs the handover and establishes connection with target RAN and core network. Source CN is informed of HO completion, forwards buffered packets to target CN and resources are released in source RAN.

# 2. Technology proposals for smart traffic steering and mobility management functionalities

## 2.1 Decision and handover preparation methods for efficient load balancing and flow mapping

### 2.1.1 Multi-path decision making

#### 2.1.1.1 Description of the Technology

Nowadays most of the smart phones have several radio interfaces that may be used. Thus the selection issue of which interface should be used preferentially arises, which one is the most suitable for the current use. Several criteria may be selected to do the choice such as cost, interface characteristics; traffic condition … The knowledge of the localization of the UE may be also taken into account if it is know that there are new available radio accesses in the neighborhood. But the choice of the path is not limited to radio access part; it may also be extended to the complete path between the UE and its Correspondent Node. For the first part we will use the IEEE 802.21 standard and for the second one the IETF ALTO service.

#### 2.1.1.2 Relevance of the Technology

The first optimization on the preferred radio access will allow to both speed up the HO process that is at the heart of the mobility process. This may be used for offloading techniques. The last one let the application be aware of the network conditions and be able to make a choice about the best path that should be taken.

#### 2.1.1.3 Expected Gains and identified issues

As the best path should be used, the quality of the traffic should improve as well as the user perception (QoE). It may also have impact on global traffic. The main foreseen issues are the need to have some additional software part on the UE for both 802.21 and ALTO and even some changes at application level.

## 2.2 Offloading

### 2.2.1 Operator managed Wi-Fi access point

#### 2.2.1.1 Description of the Technology

All existing smart phones on the market today are equipped with cellular and Wireless LAN network interfaces. These smart phones are said to be dual-mode. In the near future it's foreseen that also cheaper smart phones will have smart phone like features, including support for dual-mode. Additionally, laptops and note pads are also equipped with dual-mode network interfaces.

By using an upgraded Wireless LAN Access Point (AP) for Wi-Fi indoor coverage, primarily at home, but also in public hot-spots and small offices, the operator may offer personalized service also over Wi-Fi. Operator managed Wi-Fi is a technology where an operator can provide personal connectivity services for devices in residential network, hot spots etc. e.g. firewall, secure authentication. Before the user gets access to the Wi-Fi network, the user's credentials are sent to HSS, via BNG, for authentication. When the user has been authenticated, traffic may be sent both externally and locally.

External traffic is sent via the fixed broadband access network to the BNG. From the BNG, user traffic is routed either directly to the Internet (EPC offload) or tunneled via GTP back to the operator's P-GW. By bringing the traffic to the P-GW the user gets access to the operator's services. The preferred route is defined in the user profile and configured during the authentication process. In both cases cellular offload is achieved. However, when traffic is sent from the BNG via GTP to the P-GW only the cellular radio access network is offloaded.

The WLAN AP has a built in support for DLNA (Digital Living Network Alliance) which facilitates access to local (residential) services. Traffic destined to local services is routed locally in the residential network. The operator managed Wi-Fi setup is illustrated below in Figure 3.

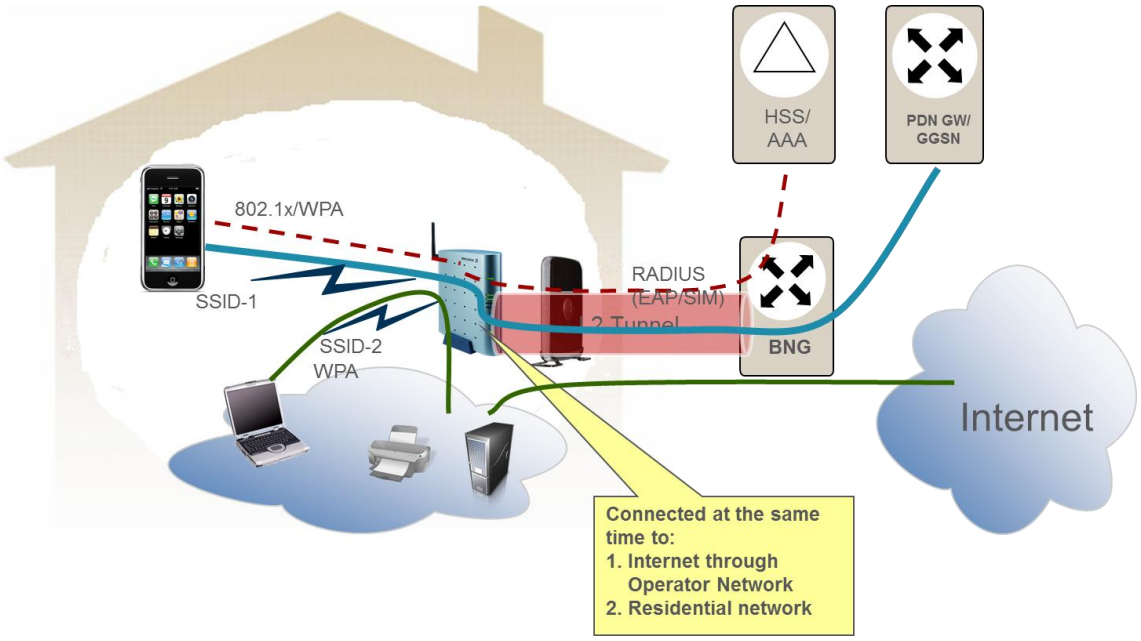



**Figure 3: Operator Managed Wi-Fi**

#### 2.2.1.2 Relevance of the Technology

By using a modified AP, we can access the operator services over WLAN behind RGW. It also helps to offload broadband traffic from wide area radio network to Wi-Fi. Moreover, it also provides some additional advantages like increased bandwidth by using the unlicensed spectrum, increased network capacity and higher performance.

#### 2.2.1.3 Expected Gains and identified issues

Following are some of the gains with operator managed Wi-Fi:

- Operator can provide personal connectivity services for devices in residential network, e.g. firewall, content filtering, secure authentication
- Operator partner services tied to mobile subscription also over WLAN behind RGW, e.g. Spotify
- Operator (Fixed, Mobile or ISP) manages the Wi-Fi AP
- Increased bandwidth by using the unlicensed spectrum
- Mobile Operator can provide better indoor coverage for Wi-Fi enabled devices
- Off-load of broadband traffic from wide area radio network to Wi-Fi
- This technology helps to reduce the complexity with cell planning

There are no technical issues with this technology. It works equally well with all types of architectures (centralized, distributed or flat). But, there might be some legal and business issues when it comes to real world deployment.

### 2.3 Dynamic Mobility Anchoring

### 2.3.1 OpenFlow Controlled EPC

#### 2.3.1.1 Introduction

Mobile broadband networks are expected to experience significant data traffic growth in the future. It is claimed that the current centralized network architecture will face excessive traffic concentration on a single gateway element and possibly un-optimized routing. Mevico is studying whether distributed gateway architecture could be an alternative that offers scalability, optimized routing and failure tolerance in cost efficient way.

Distributed gateway architecture is not without challenges either: current mobility management procedures are not always optimal and frequent handovers might require the relocation of the distributed gateway elements in order to maintain the optimized routing. This might lead to increased signaling load. As a conclusion it can be said that optimized routing in the user plane can be achieved with the distributed architecture but in case of control plane functionalities the situation is more complicated. Therefore placing all the 3GPP specified functionalities in an optimal way is a key to the success of distributed architecture.

One attempt to achieve the benefits of both distributed and centralized architecture at the same time is to separate all control plane functionalities from the distributed forwarding elements and use a control protocol (e.g. OpenFlow) between these elements. The optimal solution should offer

- Centralized view and visibility to the whole network
- Optimized routing and offloading as soon as possible
- Scalability.

## OpenFlow

Openflow or more broadly software defined networking is an approach that enables a centralized control plane and a view of the whole network and gives a possibility to do the actual packet forwarding in the distributed switches. OpenFlow is a protocol that can be used to program the flow table in different switches and routers [10]. OpenFlow is based on an Ethernet switch, with an internal flow-table, and a standardized interface to add and remove flow entries. OpenFlow controller is the entity that pushes the flow entries to the flow table. Thus the OpenFlow switch (Figure 4) consists of three parts:

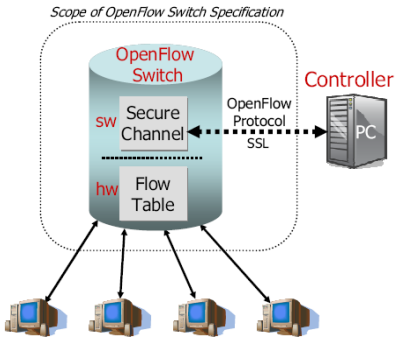



**Figure 4: OpenFlow Switch [10]**

- A Flow Table (Figure 5), with an action associated with each flow entry, to tell the switch how to process the flow

| In Port | VLAN ID | Ethernet | | | IP | | | TCP | |
|---|---|---|---|---|---|---|---|---|---|
| | | SA | DA | Type | SA | DA | Proto | Src | Dst |

**Figure 5: Flow table entry.**

- A Secure Channel that connects the switch to a remote controller allowing commands and packets to be sent between a controller and the switch using
- The OpenFlow Protocol, which provides an open and standard way for a controller to communicate with a switch.

The default behavior of the OpenFlow switch is that the incoming packet is routed according to the action of the matching flow. In case there is no matching entry in the flow table the unknown packet is routed to the Openflow controller which makes the routing decision and installs a new flow to the switches. Subsequent packets belonging to the same flow are routed based on this newly installed flow.

Openflow widens the scope of traditional routing. It is possible to define flow entries to cover fields from L2, L3 or L4 headers and make forwarding decisions based on the mixture of those. It enables different

levels of granularity (e.g. TCP connection, IP address, VLAN) for routing and gives also a possibility to forward packets requiring special processing to the elements that have relevant capabilities. If it is possible to treat the whole network as one logical but still distributed entity, it is worth investigating the impacts of this concept to the distributed EPC architecture.

### 2.3.1.2 Overall Description

OpenFLow controlled EPC introduces a new type of combined S/P-GW element. According to the 3GPP specifications S-GW and P-GW elements are responsible for user plane handling. Both of these elements have though functionalities other than pure user data processing/forwarding such as signaling termination, IP address allocation, maintaining UE contexts, charging etc. In OpenFlow controlled EPC the introduced new type of combined S/P-GW entity splits the functionalities of these elements in a new way as presented in Figure 6. The centralized GW element has a wide view about the network: via OpenFLow protocol it learns the properties of all the existing switches and their ports. Port and/or flow based statistics provide means for collecting information about the traffic.

In addition to this the centralized GW element has knowledge about all active PDN connections. It can utilize this information when it makes the routing decisions and inserts relevant flows to the distributed GW elements that do the actual packet forwarding together with GTP termination. OpenFlow controller is thus located in the centralized GW element. The centralized GW element combined with a group of distributed GW elements can be seen as one combined S/P-GW entity, the intelligence and decision making is in the centralized part, only the packet forwarding capability and GTP termination is distributed.

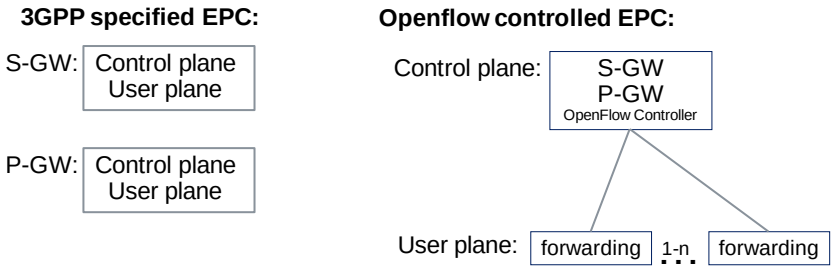



**Figure 6: Functional Split in OpenFlow controlled Distributed EPC.**

Despite of the new way to split the S- and P-GW functionalities the OpenFlow controlled EPC is expected to be 3GPP compliant. Standard MME, eNB and all other network elements communicate with the OpenFlow controlled GW element by using standard interfaces and protocols (Figure 7). The OpenFlow interface is considered to be a GW internal interface.

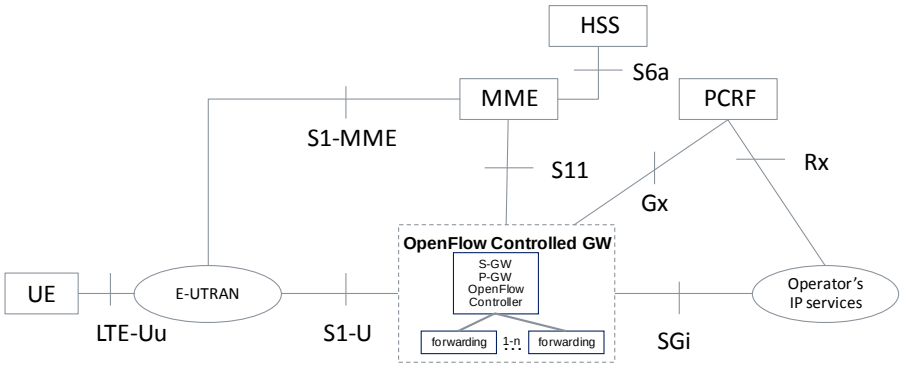



**Figure 7: 3GPP compliant OpenFlow Controlled EPC Architecture.**

The centralized GW element has full view to the whole network: it is the termination point of the 3GPP specified signaling; it allocates the UE IP addresses, keeps the UE contexts, and runs routing protocols. Centralized control minimizes the need for signaling between elements e.g. the GW relocation

procedures could be simplified to only update the routing in the distributed elements. OpenFlow gives a possibility to forward packets requiring special processing to the elements that have relevant capabilities. In distributed EPC this feature can be beneficial, packets of the subscribers requiring e.g. DPI or lawful interception can be routed towards relevant nodes. The OpenFlow controlled distributed EPC architecture is presented in Figure 8.

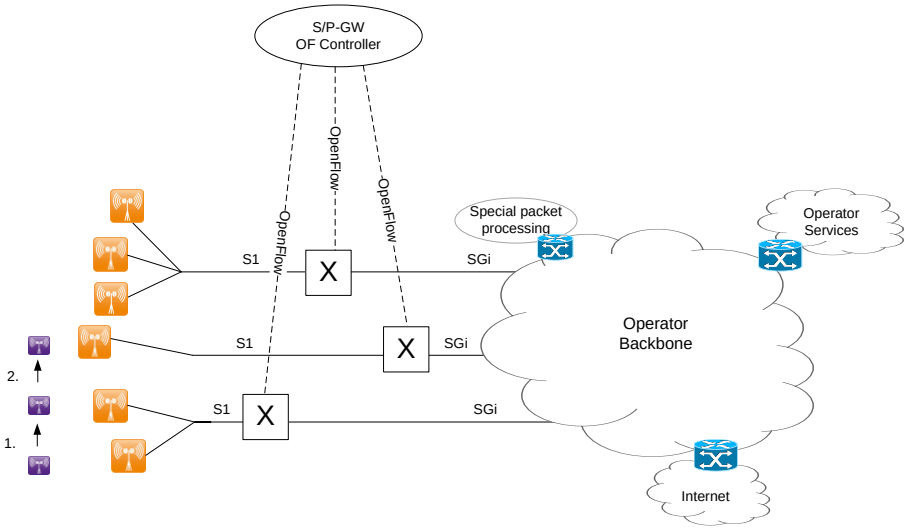



**Figure 8: OpenFlow Controlled EPS.**

The distributed GW elements can be located in the access network, co-located with eNBs or both. Also the capacity of each distributed element can be adjusted in an optimal way.

### 2.3.1.3 Gateway Internal Functionality

As mentioned in the previous subsection the GW element in the OpenFlow controlled EPC is supposed to be 3GPP compliant. However, because of the new internal OpenFlow based interface and the distributed forwarding plane, some new internal functionalities and concepts need to be defined. According to the 3GPP specification the MME selects the GW element which in the case of OpenFlow controlled EPC is always the centralized part of the GW. Centralized GW element is in turn responsible for selecting the distributed forwarding element for each UE.

This functionality is tied to the UE IP address allocation procedure. In order to keep routing consistent there is a pool of UE IP addresses assigned to each distributed GW element. Therefore selecting an IP address means selecting the distributed forwarding element as well. If there is a need to achieve optimized routing and offloading as soon as possible, the distributed element closest to the eNB under which the attaching UE is located should be selected. Any of the identity types available in User Location Information (ULI) included in the attach request/create session request message can be used to select the optimal distributed GW element.

There might be cases where optimal routing is not the primary selection criteria for the forwarding element selection. For example UEs requiring special processing or connectivity such as lawful interception or corporate access can use forwarding elements located deeper in the operator network. Because the centralized GW element has full view to the whole network, it can take into consideration also load in the distributed GWs when allocating IP address to attaching UE.

### 2.3.1.4 GTP Termination

In OpenFlow controlled EPC the standard 3GPP signaling messages are terminated to the centralized part of the GW but GTP tunnel termination, downlink packet buffering and optionally other user plane related functions are implemented in the distributed element. In general the centralized GW element utilizes standard OpenFlow protocol to send information to the distributed elements.

Related to GTP termination the information required to encapsulate and de-capsulate GTP packets need to be transferred from the centralized controller to the GTP termination point. The problem here is that standard OpenFlow protocol is capable of transferring information only related to protocol layers L2, L3

and L4 and not on application layer where the GTP header information is carried. As a consequence standard OpenFlow switches are not capable of creating GTP tunnels either.

There are two possibilities to solve this problem. One option is to define extensions to the standard OpenFlow protocol that enable the GTP tunnel termination by means of OpenFlow protocol and flow entries. Another option is to keep OpenFlow protocol untouched and define a separate entity e.g. a line card that is responsible for GTP tunneling termination. In this document the latter option is covered.

The GTP tunneling termination point in the distributed element is implemented with a separate device e.g. a line card called here as a tunneling device. GTP header information together with transport IP addresses is sent to the tunneling device in a specific IP packet. This packet can be sent straightly from the centralized part to the tunneling device or it can be embedded in an OpenFlow packet-out message.

Downlink user data packets arrive to the distributed element as native IP packets destined to a UE IP address. These will be encapsulated into a GTP packet and therefore all the packets destined to a UE IP addresses must be forwarded to the tunneling device (Figure 9). All GTP encapsulated packets are then routed to the relevant eNB. Uplink user data is embedded in the GTP packets having tunneling device as a transport layer destination IP address. After GTP de-capsulation they will be routed further based on a matching flow if available. Otherwise the unknown packet is sent to the controller to get the routing information.

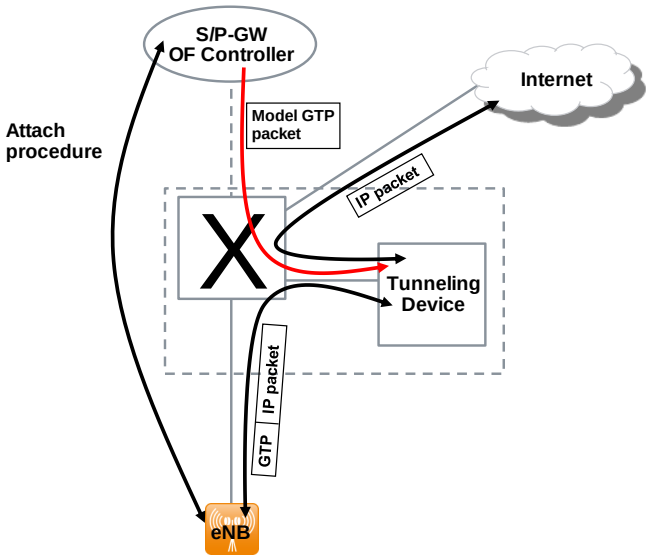



**Figure 9: Distributed GW element with GTP tunneling termination.**

#### 2.3.1.5 Discussion

The OpenFlow controlled EPC introduced in this chapter is an attempt to have a new point of view to the distributed mobility management. It is a concept that tries to combine the benefits of both the centralized and distributed GW architectures by providing optimal routing and full view to the whole network at the same time. The solution described here is 3GPP compliant. The GW element that consists of a centralized control part and a group of distributed forwarding elements can be seen as one combined S/P-GW element. MME, eNBs and all other network elements communicate with it by using standard 3GPP specified interfaces and protocols. The OpenFlow interface between the centralized and distributed parts is considered as GW internal interface which is assumed to be according to standard OpenFlow protocol. Possible optimizations and alternative solutions that require extensions to either 3GPP specification or OpenFlow protocol are for further study.

### 2.3.2 Improvements for distributed GW deployment

Distribution of mobility anchors and gateway functions (GWs) bring certain benefits:

- More direct/optimal routing is decreasing traffic latency and saving transport cost, in particular for local traffic (cache, CDN, mobile to mobile traffic).
- DMA (Distributed Mobility Anchoring) has been initially discussed in IETF to improve MIP/PMIP by distributing mobility anchors and use as much as possible local, not tunnelled

addresses. The technology proposed here instead intends to optimize the EPC based on the ideas of the DMA, but utilizing existing 3GPP protocols like GTP with as less as possible changes, to enabling SW upgrades to optimize the usage of existing resources.

- But the distribution of GWs brings also some challenges. To cope with these some optimizations are proposed what are not needed in a centralized architecture.

### 2.3.2.1 Optimization for PGW reselection

A proposal is to relocate the used PGWs using intelligence introduced in the PGW for routing optimization, another to change SGWs for routing optimization and reducing the number of hops in the data path. The first solution applies after a UE has moved into a new "gateway area". The PGW selects IP (PDN) connections for what a new IP address and service interruption may be acceptable from application point of view and forces a reconnection that allocates a new more optimal PGW and new IP address. This leads to more optimal routing and savings in transport networks.

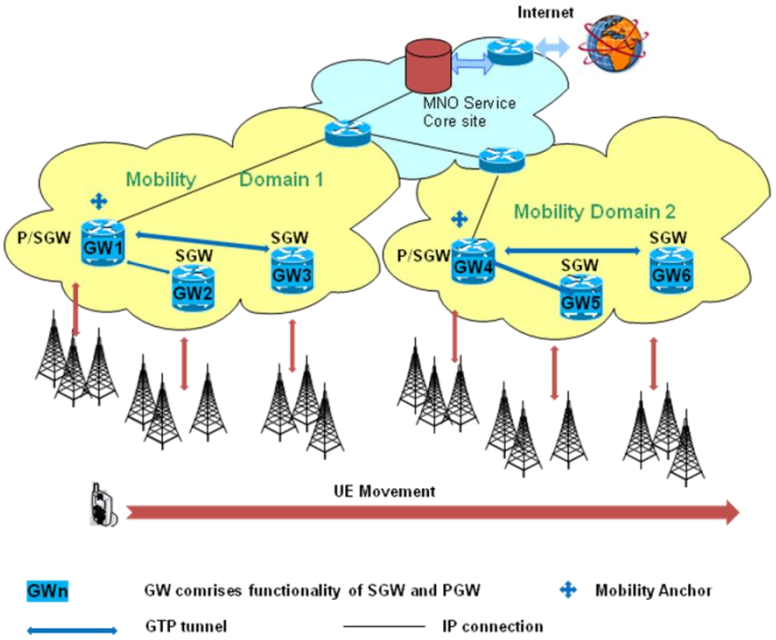



**Figure 10: Distributed GW deployment**

The following process is considered like illustrated in Figure 10. After attachment the UE is served by a local combined S/P-GW (GW1). After changing tracking areas a SGW relocation may take place e.g. due to connectivity restrictions (GW2, GW3), When the UE arrives at GW4 this is considered as trigger for a local GW (anchor) relocation to enforce more optimal routing. In the following different solutions and optimizations are proposed for the GW relocation.

**Facilitation of anchor changes in active mode**

The MME is not aware of UE inactivity if the UE is in active mode. The MME can only be sure not to interrupt ongoing data connections if it releases PDN connection during IDLE mode of the user devices, e.g. enforcement of PGW relocation during TAU in IDLE mode. But the behavior of new smart-phones may prevent that the UE will enter the IDLE mode: Different applications may make use of the "always on connectivity" e.g. for sending periodically reports for presence information keep the UE active. This can be solved if the decision to relocate the PGW is shifted from the MME to the S/PGW. To decide for a release and reconnection procedure the PGW determines an optimal point in time by monitoring user inactivity phases.

**Check for non optimal routing**

Different solution to detect (and release) non-optimal routed connections (GW based) are possible. During UE roaming a new SGW may be selected. This triggers the process to check for PGW relocation:

1) The PGW may be configured with SGW addresses for which routing is assumed to be optimal or

2) The "optimal mobility domain" decision can be coupled with the IP routing topology of the NW (what simplifies the management of the feature in a "self-configuration" way). The local PGW may assume all SGWs in the same IP sub-network as optimal GWs (avoid additional delay an additional router-hop would introduce). Alternatively the IP router functionality of the GWs can be used to determine how the SGW can be reached (e.g. the routing cost to the destination).

**Relocation decision with application awareness**

Taking into account what applications are running in the UEs can be achieved by use of the packet inspection (DPI/TDF) capability of the GWs:

- Exclude PDN connections with special content from being mobility/routing optimized (like secured VPN connections). For a small number of traffic non optimal routing may be acceptable for an operator compared with the poor user experience when loosing IP connectivity
- Avoid interruption of ongoing sessions with dedicated QoS and policy control. This may be the case for special applications like voice over LTE. In this case the PDN GW may be not changed to avoid the need for a relocation or reestablishment of the context e.g. in the SIP servers
- Set special (longer) inactivity timers depending on the applications running in the PDN connection. The timers are used to check the activity level of the user before releasing. This way an acceptable user experience can be achieved

In summary, advantages of the proposed solutions are:

1) Also always active UEs can be forced to use optimal GWs
2) The UE gets an explicit trigger when to request a new PDN connection/IP address
3) The network is in full control over the usage of local PDN connection and doesn't depend on UE behavior or UE policies when to use a new/local IP address
4) All traffic can be forced through one S/P GW regardless if the UE moves over a long time or not. (This is an advantage over the dynamic mobility anchoring concept what may generate NW overhead due to the need to maintain many parallel tunnel connections to many anchors)
5) Compared to the standardized MME based solution there is no need have core NW topology information managed in the MME
6) A PGW based implementation can take into account the user data content and cope better with issues that can result from changing the IP addresses for some applications

#### 2.3.2.2 Optimization for SPGW selection for multiple PDN connections

A second solution proposes to relocate the SGW to achieve maximal SGW-PGW collocation in a distributed architecture when UEs use different PDN connections. This saves at the end GW capacity. Different gateway locations may result from the fact that a UE may connect to local and/or central networks or Internet providers. The number of data/user plane nodes might be not minimal in certain situations when multiple connections to different networks are established. Improvements are proposed to achieve optimal flat network architecture.

In the EPC a UE may have different PDN connections in parallel that are terminated in different PGWs. But only one SGW connects with the eNodeBs and serves as a mobility anchor for the eNodeBs and for all PDN connections of an UE. A feature that makes use of the different PDN connections is the Selective IP Traffic Offload (SIPTO) what was introduced in 3GPP Rel.10. The solution is based on an enhanced GW selection that has the capability to select a mobile core network GW near to a RAN node (RNC, eNB). This is then also termed a local or distributed GW. The SIPTO function enables an operator to offload traffic that is destined to the Internet close to the UE's point of attachment to another network bypassing the operator service core network.

Depending on the used services and applications the UE may keep a local or a central connection as "always on" connection and establish a second central or local PDN connection if needed. E.g. the UE may select the always on PDN connection with the central PGW and for certain Internet applications it could establish a local/SIPTO PDN connection on demand.

During the UE attachment a PDN connection is established and the GW can be assigned in an optimal flat way, what means a co-located S/P-GW. This could be freely located at a central or local site. If another PDN connection is established only a new PGW can be allocated e.g. according to SIPTO requirements for a new SIPTO APN. As mentioned before no other second SGW can be selected as the first one serves all UE connections and provides the "first" mobility anchor. And what is of special interest: there is no "mobility" trigger for a SGW relocation procedure. This leads to the fact that the first chosen SGW will

be kept for the second PDN connection. And this may lead to not optimal routing situations as depicted on the left side of Figure 11.

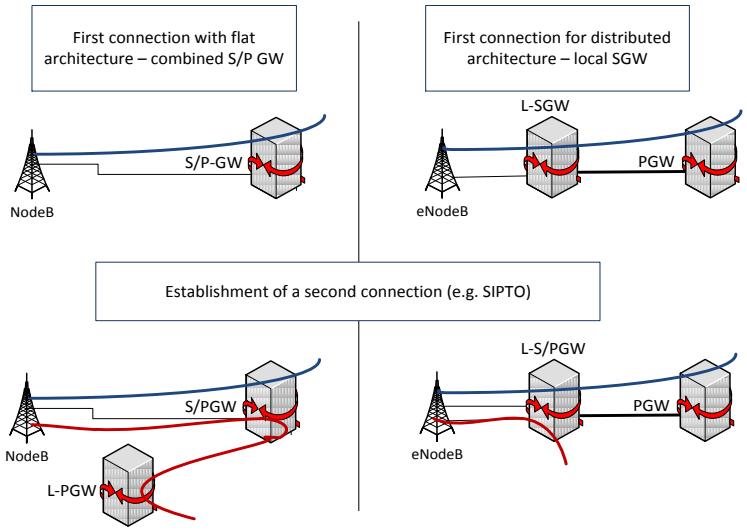



**Figure 11: Combined and separated S/P GWoptions**

To avoid this non optimal routing and to have the option to allocate a local/distributed PGW for any PDN connection it is needed to always select a local SGW - even in case a central PGW is chosen. This solution is depicted on the right side of figure. Although now non optimal routing for local traffic can be avoided a drawback of this solution is the forced separation into SGW and PGW. It introduces a limitation for the target to limit the number of involved mobile specific nodes in the data path to achieve a flat network architecture. It can be summarized that a) the existing procedure lead to either non optimal routing or b) a maximally flat architecture can't be achieved although it would be possible by the deployment of combined S/PGW nodes.

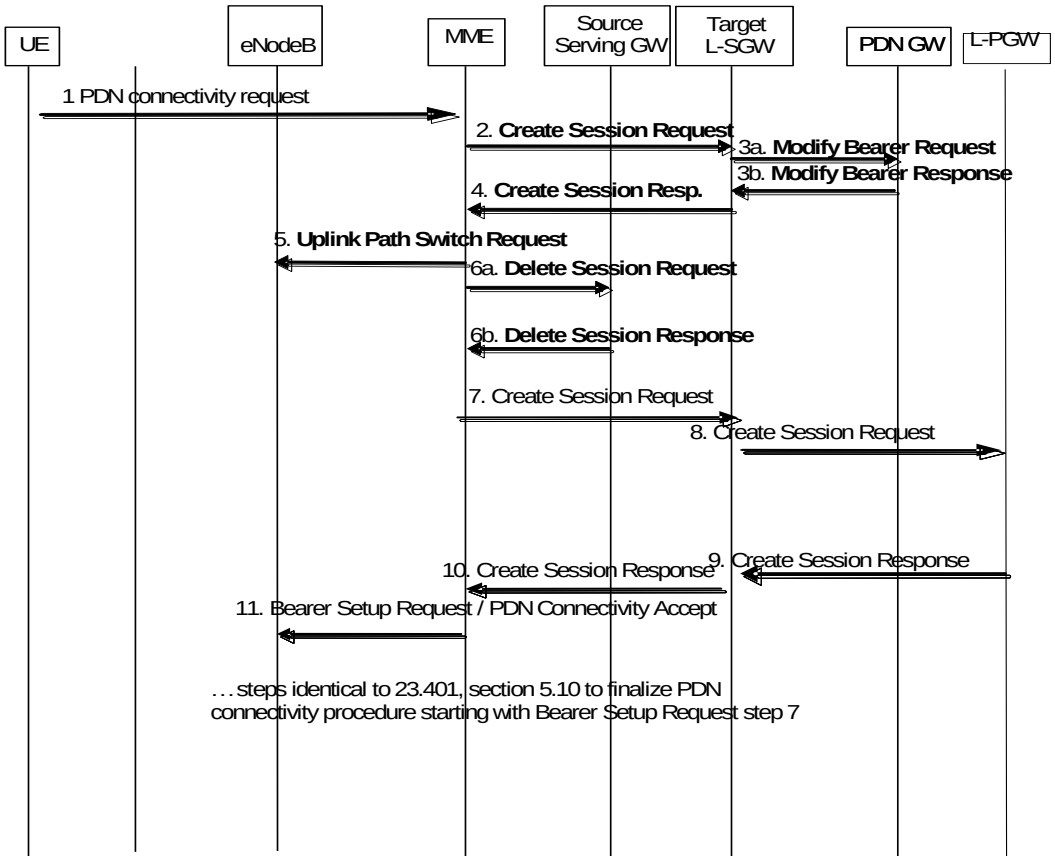



**Figure 12: Modified PDN connectivity procedure**

To overcome the non optimal split into SGW and PGW in two different locations for many cases it is proposed to add the SGW reselection/relocation procedure to the PDN connectivity related procedures (establishment and release of a PDN connection). Here an example is given of a modified PDN connection establishment procedure that adds a new IP connection for the UE. As this connection is suited for local offload a new local PGW is selected and the SGW is relocated to be combined/collocated with the new L-PGW. The UE requested PDN connectivity procedure in [8] can be modified as illustrated in Figure 12: The example introduces a new S1-C message on the MME–eNB interface; the new information for uplink tunnel endpoint can be contained in existing messages as well.

This flow shows that the problem can be solved if the procedures that are creating and releasing data connections are enhanced with a SGW change capability. For local data connections a local SGW can be selected. If the local connection is released and still another central PGW /PDN connection is in use the local SGW can be released and a SGW collocated with the PGW can be allocated. This way a maximally flat architecture with co-located S/PGW can be achieved.

#### 2.3.2.3 Expected Gains and identified issues

Distributed GWs provide some benefits for user experiences (close link to content sources) and transport cost saving (more optimal routing) as well as reliability and scalability advantages but introduce some challenges as well. The enhancements proposed here mitigate the challenges like

- Non optimal routing in case the user is moving over large distances
- User impact in case of new PGW and IP Address allocation
- Need to separate the GW into SGW and PGW what results in increased resource and energy consumption

The introduction of OpenFlow controlled EPC can on the other hand hide the higher number of distributed GWs from the EPC control/MME and from the user and allows a more flexible management of the network. In this case a new technology can be implemented fully transparent to existing EPS network components. For the other optimizations small adaptations to existing standards are needed.

## 2.4 Terminal-based mobility management

### 2.4.1 SCTP

#### 2.4.1.1 Description of the Technology

SCTP is a transport protocol operating on top of a connectionless packet network such as IP. The protocol is defined in RFC 4960 [9]. SCTP offers a connection oriented reliable service and congestion control services, like TCP. Additionally, multi-streaming and multi-homing is supported by SCTP that provides resiliency in case of path failure. SCTP could be useful in case of data losses due to a mobility handled by EPC. Prior to data transmission, a connection or, as it is called in SCTP parlance, association, is setup between the two communicating endpoints, and is maintained during their entire communication.

One of SCTP's novel features, multi-homing, enables the endpoints of a single association to support multiple IP addresses and support session continuity while shifting between different access networks. Each IP address is equivalent to a different non overlapping network path towards the communicating peer, for sending and receiving data through the network. Currently, SCTP uses multi-homing as a means for path-level redundancy to provide uninterrupted service during resource failures, and not for load balancing.

A new layer called the 'Session layer' (not specific to SCTP) is introduced between the application and the transport layer in the Internet protocol suite as shown in Figure 13.

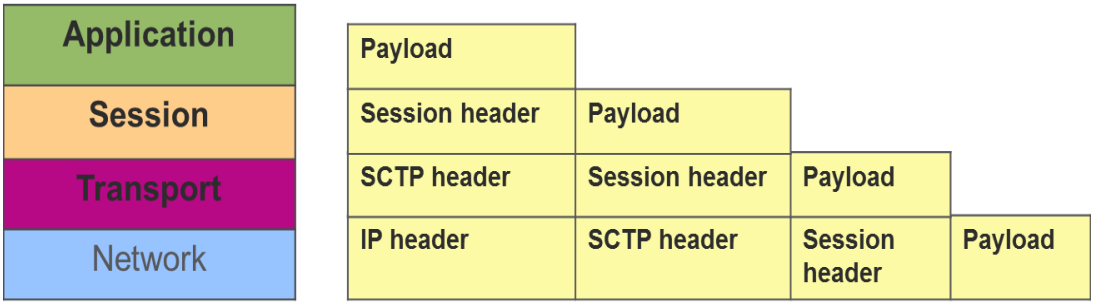



**Figure 13: A new session layer in the OSI stack**

The session layer Abstraction provides:

- a well-defined API to the application
- session creation and session setup
- data transfer
- session suspend and session resume
- session close

It also addresses the challenges with mobility events such as network disconnections, IP address change etc. It suspends the application if the network is lost and resumes it later when the connection is back.

#### 2.4.1.2 Relevance of the Technology

The inherent support of SCTP for multi-homed endpoints (at either or both ends of an association), as well as its dynamic address reconfiguration extension, makes SCTP quite attractive as an Internet mobility solution at the transport layer. The SCTP includes a path management function that chooses the destination transport address for each outgoing SCTP packet based on the SCTP user's instructions and the currently perceived reachability status of the eligible destination set. The path management function monitors reachability through heartbeats when other packet traffic is inadequate to provide this information and advises the SCTP user when reachability of any far-end transport address changes.

This work has investigated how SCTP's features can be used to support mobility. A mobility framework has been designed based on SCTP which is explained in chapter 4 of this document. The basic component of this mobility framework, namely the "SCTP Mobility Manager" reacts to local network interface events (including interface failure, addition or removal of an interface, change of IP address, etc.), and interacts with the SCTP stack for achieving quick switchover to the most preferred interface. Additionally, a well-defined API for mobility-aware, SCTP-enabled applications is provided in our implementation. By utilizing the API, application developers can easily take advantage of the advanced features offered by the proposed SCTP mobility framework.

#### 2.4.1.3 Expected Gains and identified issues

Following are some of the gains by using SCTP for session continuity

- preserves communication upon changes in host's location
- suspends communication upon long network disconnections
- resumes communication upon network connectivity
- mobility on demand
- IP-mobility signaling load is moved from the network to the UEs

SCTP requires support on the UE or the application, and do not need modifications on the network side. It can provide end-to-end anchorless mobility. SCTP performance is independent of the architecture selected. It works equally well with all the architectures (centralized, distributed or flat). SCTP protocol can co-exist with other technologies as well. Charging policies, gateway selection etc. is not considered in Ericsson's implementation. There is one issue with SCTP which is that, not all firewalls allow SCTP packets through. The firewalls have to be modified and new rules have to be added in order to use SCTP protocol.

### 2.4.2 NMIP MPTCP SCTP

The aim of this technology solution is to analyze three end to end protocols and look how they behave in LTE context. A Wi-Fi access and internet connection are added to test offloading techniques.

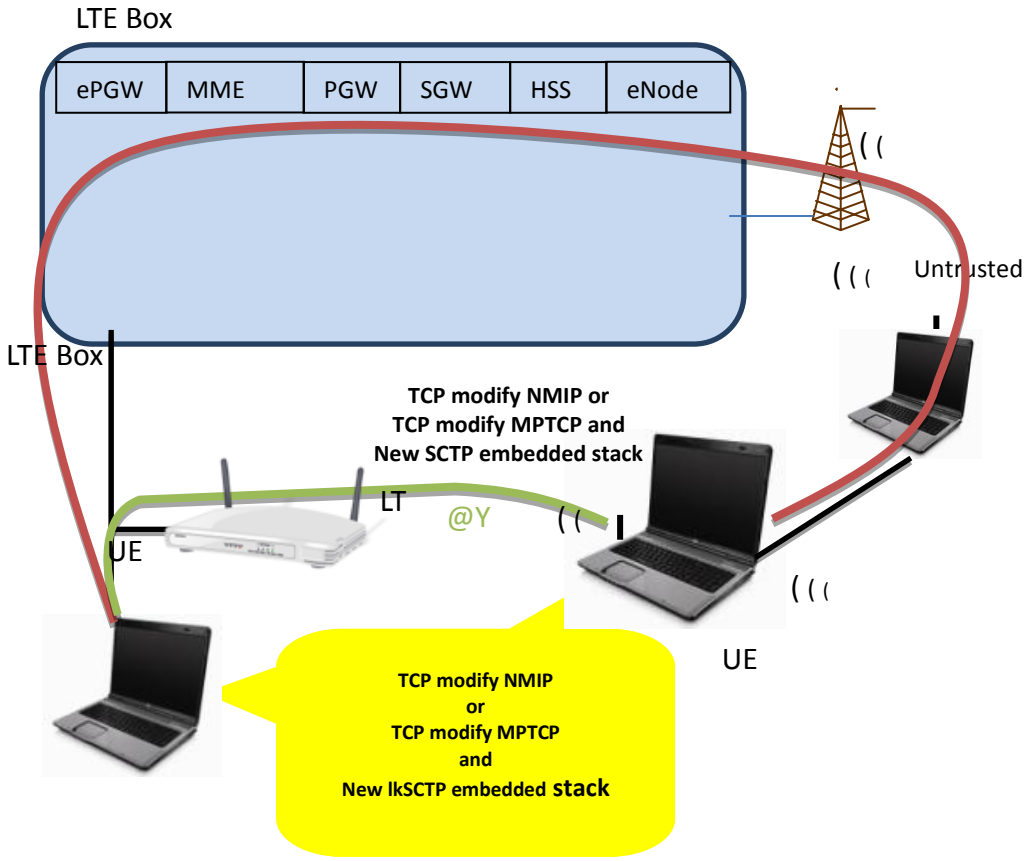



**Figure 14: Test-bed description**

#### 2.4.2.1 Description of the Technology

The protocol analysis will be done on three end to end protocols : NMIP [25], MPTCP and SCTP.

- **NMIP:**

  Not MIP may be viewed as an extension of the TCP protocol and it is a host to host approach to manage IP address change. Both end hosts have to implement the solution and there is no other impact on other network elements. If only one node implements the solution it behaves exactly like TCP.

  One of the advantages of this protocol is that it does not need any additional message, information is transmitted via the TCP option, and the overhead is very light (only on retransmission and the first messages after an IP address change). One consequence is that the duration to take into account an IP address change corresponds to a RTT which is one of the fastest and does not depend on other network element; impact on the HO process is minimal.

- **MPTCP:**

  MPTCP (Multipath TCP) is a protocol that adds the capacity to TCP to manage multiple paths. The mostly probable use should be with multi interfaces devices and especially mobile terminals with several radio interfaces. It is an end to end protocol; it only needs that the two end points implement MPTCP. Otherwise the MPTCP session will behave as a TCP session. The compatibility with TCP was one of the requirements to avoid the lack of applications that implement it like SCTP.

  The use of several paths may be used to realize multi-homing and link aggregation to improve the total throughput. But the implementation of MPTCP puts some limits on it by considering fairness on each link to avoid starvation effect on these links.

- **SCTP:**
  This protocol has already been described in the previous section.

The KPIs are based on throughput and HO measurements.

#### 2.4.2.2 Relevance of the Technology

Mobility induces new issues that may be solved at transport layer. Each analyzed protocol has its own solution to tackle this problem. Either the IP address change resilience (NMIP) or the multipath / multi streaming management (SCTP / MPTCP) are a way to solve the mobility issue.

#### 2.4.2.3 Expected Gains and identified issues

A better knowledge of these protocols with their own advantages and drawbacks will allow a more pertinent choice. Performance analysis will show the behavior of each protocol. One identified issue is the incompatibility between NMIP and MPTCP as their implementations modify the TCP stack.

## 2.5 Routing optimization

### 2.5.1 Routing optimization support in Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6), specified at the IETF [RFC 5213], is a network-based mobility management protocol supported by 3GPP in [21]. Available on the S5 and S8 interfaces within the 3GPP EPC, it also supports mobility management with trusted and un-trusted non-3GPP networks through S2a and S2b interfaces. The PMIPv6 architecture is composed by two main elements:

1) the Local Mobility Anchor, or LMA, located on the P-GW ensures user registration management, IPv6 prefix assignment and anchoring, data flow tunneling and routing.
2) The Mobile Access Gateway, or (MAG, located on the S-GWs, A-GWs, and ePDGs, ensures attachment and detachment detection of mobile users, users identification and registration at the LMA, and data flow tunneling towards LMA(s). Recall that the P-GW is the gateway between the core network and the operator's IP network or Internet; the S-GW (or A-GW, ePDG, HSGW) on the other hand is the gateway between the core network and radio access network(s).

The protocol does not require the user equipment to be involved in the mobility management protocol operation. It is a network-based protocol which can manage almost all types of devices (sensors, smart phones, tablets, etc.) without having specific requirements on the user equipment capabilities. Furthermore, as it operates at the IP layer, it can be easily integrated in interworking scenarios such as between E-UTRAN, cdma2000, and WiFi networks for instance. All those features make PMIPv6 a very promising protocol for future LTE deployments.

However, the deployment of PMIPv6 will be operated in a very challenging context where communication patterns are evolving. In the near future, vehicles' on-board units (OBUs) will constantly use the mobile broadband network to communicate with sensors along the highways, video-conferences would take place between vehicles and/or walking users, machine-to-machine communication scenarios will be more prominent. It is expected that phone calls and SMS would be considered as data exchange in future data-only plans sold by the operators [22].

There will be a shift from the client to server main data communication paradigm to a more extended client-to-client scheme. Hence, the hierarchical and centralized management of data flows may highlight some shortcomings in such scenario. Taking into account this evolution a new extension to PMIPv6, PMIP-RO [23], is introduced to handle routing optimization within a PMIPv6 domain. The main idea is that Client to Client communications can gain in performance by using more optimized data paths than by remaining anchored at a central LMA.

In the current hierarchical architecture, Clients connected to MAGs have their communications tunneled towards a central LMA and then redistributed to MAGs for final delivery. According to the network architecture, this indirection may lead to a crucial problem of scalability that mobile broadband operator are already facing with bandwidth-demanding video streams and the explosion of the number of users. PMIP-RO does bring a form of distribution of data anchoring servers throughout the network.

When possible, data flows bypass the central LMA although the latter is still required to manage the control plane. PMIP-RO, also called PMIP-IA (IA for Intermediate anchor), relies on intermediate

anchors distributed in the network to anchor data traffics closer to the communicating user equipments. Therefore, the operation of PMIP-RO could also be related to the concept of "localized routing".

#### 2.5.1.1 Overall description

In PMIPv6, the LMA concentrates two important features. The first feature is the user registration management, i.e., the control plane. Between MAGs and LMA(s), two main signaling messages are exchanged: 1) the Proxy Binding Update (PBU) and 2) the Proxy Binding Acknowledgment (PBA). The PBU is sent by a MAG to the LMA and indicates, for instance, the attachment of an UE. The LMA, at the reception of this PBU, performs a lookup in its database to check if a record already exists for this UE.

Note that a record may exist and point to a different registered MAG in a handover scenario. The record information is sent to the MAG, in the PBA, so that proper routing and addressing information are provided to the UE. This procedure, hence, do show that the UE's LMA centralizes all information about the UE and most of all its current point of attachment (MAG). In the EPC, the UE's LMA address is provided by the UE's profile in the HSS according to the requested APN. Such profile information is retrieved by the MAG at the UE attachment.

The second important feature is data anchoring. An IPv6 address is assigned to the UE by the LMA and communicated to the MAG. This assigned address is anchored at the LMA meaning that incoming communications from the Internet arrive at the LMA which further tunnel the data packets to the right MAG (where the UE is currently attached to). Data streams coming from the UEs are tunneled from MAG(s) to LMA(s) for further routing decision. Data anchoring helps any router inside or outside the EPC to take routing decision even if the current UE's point of attachment is not globally known (only one MAG and the APN's related LMA know at each instant).

In this context, PMIP-RO is an extension to current PMIPv6 procedure. It is build on top of the localized routing extension [24] to control communications data paths within the EPC, i.e., between UEs registered at the same LMA. This extension relies on the concept of intermediate data anchors (IAs) located throughout the EPC. In a network setup where MAGs are located in local PoPs and the LMA in a national PoP, the IA function could be located between (or inside) local or regional PoPs. The role of IA could be played by MAGs or intermediate LMAs or other specific hardware having routing capability.

Knowing that the P-GW (where the LMA is generally located) has specific treatments to perform on flows (such as charging, lawful interception, or content filtering), it is expected that IAs are able to perform a subset, all, or additional services of what the P-GW is normally expected to be capable of. The LMA through new signaling messages and for a given traffic characteristic is now able to change, update, or generate a specific data path after selection of one or several IAs.

Because data flows are tunneled in the PMIPv6 domain, the resulting data path will be a succession of tunnels between MAGs and IAs (see Figure 15 ). The IA selection could be based on the set of services to perform on a data flow or according to the load at some point(s) of the network. For example, the operator may want to redirect data traffic coming from sensors connected to specific MAG(s) to a specific IA for data aggregation reducing the treatment load at the LMA. In a vehicular scenario, two communicating vehicles along a highway could have their communications redirected to closer IA(s) to gain jitter performance. One IA could be used temporarily for a UE as data buffering close to the attached MAG in case of radio link disruptions.

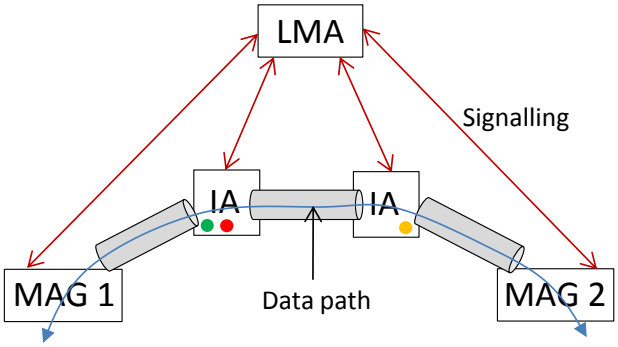



**Figure 15: Principle of routing optimization in PMIPv6.**

In all cases, the decision could be triggered by external events (e.g., operator rules) or after receipt of EPC performance measurements. The time scale and the form of the trigger are out of the scope of this

extension. Furthermore the EnableMAGLocalRouting flag, defined in PMIPv6, must be deactivated on all MAGs.

As a summary, the Intermediate Anchor (IA):

- Is a new PMIPv6 related functionality
- Requires the capability to route data packets and to establish communication tunnels
- Should operate on existing MAGs, LMAs, or independent hardware
- Could be located in the EPC or outside to achieve offloading
- Could run services such as lawful interception, content filtering, buffering, traffic shaping, etc.

PMIP-RO relies and extends two new signaling messages, by providing additional flags and new options, defined in PMIP-LR [24] to support all kind of scenarios (presented in the next section):

- The localized routing initiation message (LRI)
- The Localized routing acknowledgment message (LRA)

### 2.5.1.2 Routing optimization procedure

This section presents the generic procedure to handle routing optimization in PMIPv6. It describes how and when the signaling messages are used during the procedures. For the sake of clarity, a detailed specification of the two signaling messages is proposed in the next section. The routing optimization procedure is composed by three steps: initiation, update, and termination. For faster operations, the content of the new signaling messages could be included in PBU and PBA messages making the optimization working at UE attachment. For clarity, however, we expose the procedure when only one IA is selected by the LMA. The procedure can be easily extended for more than one IA.

Figure 16 presents the initiation procedure. One assumes that UE1 is attached to MAG1 and UE2 is attached to MAG2. UE1 and UE2 are exchanging data and are already registered at the LMA. Then, the step 1 does show that data coming from UE1 is tunneled by MAG1 and transmitted to the LMA. Step 2 does show that Data are tunneled from LMA to MAG2 for delivery to UE2. The communication is bidirectional.

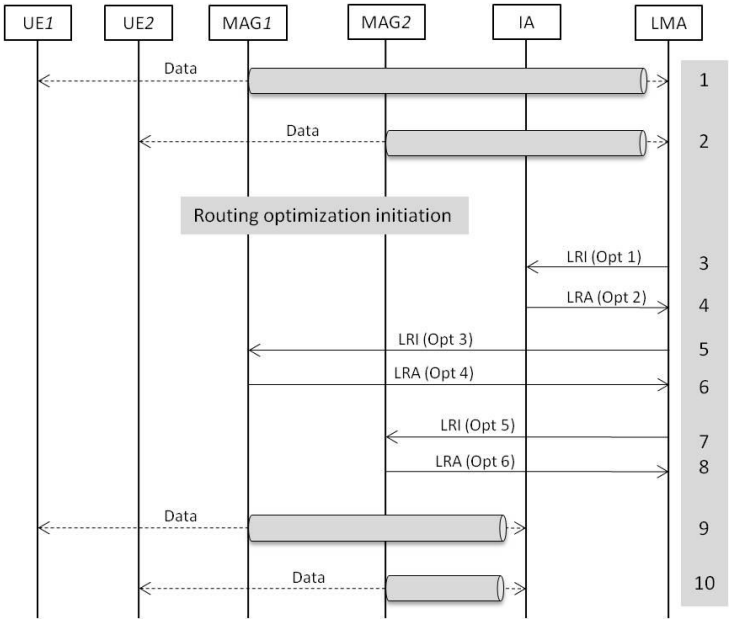



**Figure 16: PMIPv6 routing optimization initiation diagram of sequence.**

The routing optimization initiation procedure is then operated as follow:

- Step 3. The LMA after selection of the IA, sends a Localized routing initiation message to this IA to provide:
    - The IPv6 address of MAG1 and MAG2 to establish IPv6-in-IPv6 tunnels.

  - The IPv6 prefix of UE1 and UE2 to establish routing rules, i.e., which IPv6 prefix has to be routed in which tunnel.
  - The routing optimization record lifetime.
  - The type of service to apply to the flow.
- Step 4. The IA acknowledges the LRI message by returning a Localized Routing Acknowledgment (LRA) message with a success or error code.
- Step 5. If the IA returns a success code in the LRA, the LMA then sends a LRI message to MAG1 by providing:
  - The IPv6 address of the IA to establish an IPv6-in-IPv6 tunnel towards the IA.
  - The IPv6 prefix of the destination UE2 and the source UE1 to establish the routing rule. The rule says that traffic from UE1 to UE2 will be routed in the tunnel towards IA.
  - A routing optimization record lifetime.
- Step 6. MAG1 acknowledges the LRI message by a LRA message returning a success or error code. If the returned code is a success, the stream from UE1 to UE2 is routed in the tunnel towards the IA, then tunneled from the IA to MAG2 and then delivered to UE2. So far the data stream from UE2 to UE1 is still anchored at LMA preventing traffic disruption in case of failure.
- Step 7. In case of success from step 6, the LMA sends a LRI message to MAG2 providing:
  - The IPv6 address of IA to establish the tunnel from MAG2 to IA.
  - The IPv6 prefix of UE1 and UE2 to establish the new routing rules. The rule says that traffic from UE2 to UE1 will be routed in the tunnel towards IA.
  - A routing optimization record lifetime.
- Step 8. MAG2 acknowledges the LRI message by a LRA message returning a success or error code. If the returned code is a success the bidirectional traffic between UE1 and UE2 is now anchored at the IA.

Step 9 and 10 presents the resulting data path with the traffic anchored at the IA. For memory optimization, steps 3 and 5 could be done at the same time using the information back from the LRA message of step 4. Figure 17 presents a generic sequence diagram to update a routing optimization record. Here, one considers that the IA remains the same and that UE1 is moving from MAG1 to MAG3. Step 1 and 2 are the copy of step 9 and 10 from Figure 17.

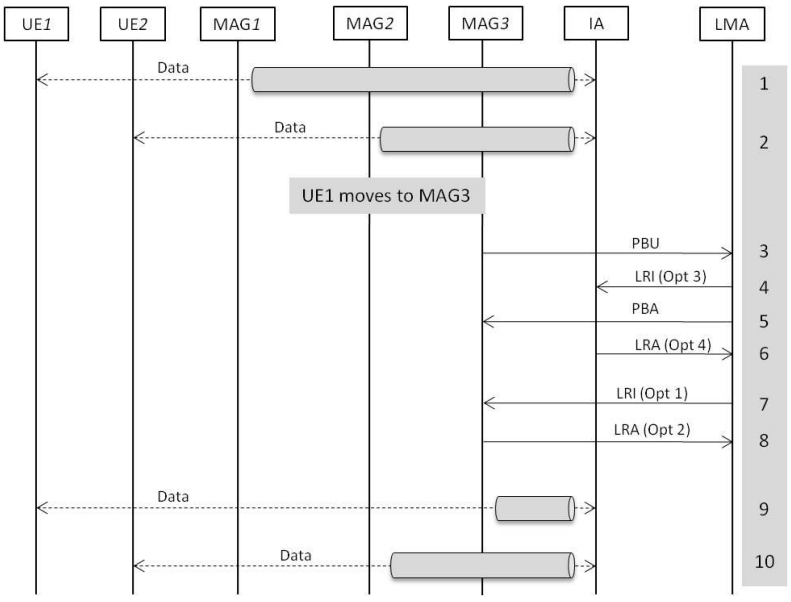



**Figure 17: Routing optimization update diagram of sequence.**

The routing optimization update procedure is then operated as follow:

- Step 3. After reception of the PBU, the LMA knows that UE1 has moved from MAG1 to MAG3. The routing optimization record has then to be updated.

- Step 4. The LMA sends a LRI message to IA providing updated information about the new point of attachment of UE1. The LRI then provides:
    - The IPv6 address of MAG3 to recreate a tunnel now between IA and MAG3.
    - The IPv6 prefixes of UE1 and UE2 to establish the routing rules as in step 3 of initiation procedure.
- Step 5. With the routing optimization updated information sent to IA, the LMA can then send a PBA message to acknowledge the PMIPv6 registration of UE1 at MAG3. At this point, traffic coming from UE2 can be delivered to UE1 while being anchored at IA.
- Step 6. IA acknowledges the routing optimization update with a LRA message.
- Step 7. With the confirmation from the IA, the LMA sends a LRI message to MAG3 as in step 5 of the routing optimization initiation procedure.
- Step 8. Step 8 is the same as step 6 of the routing initiation procedure.

Step 9 and 10 presents the resulting data path with the traffic anchored at the IA. The routing optimization termination procedure is the same than the initiation procedure but with the lifetime set to 0 (zero). It is then not presented in detail here.

**Signaling messages format**

In the following is described the format of the two signaling messages (LRI and LRA) and the proposed mobility options. They are included in a mobility header (as defined in [RFC 5213]) with the type value of 17 (LRI) and 18 (LRA). The LRI and LRA formats have been specified in [24]. In this section, additional flags and new mobility options to handle the specificities of PMIP-RO are proposed.

**Localized Routing Initiation (LRI)**

Tunnels establishments and routing modifications information to achieve routing optimization are provided in LRI. LRI messages are sent by the LMA. The format of the header is presented below in Figure 18:

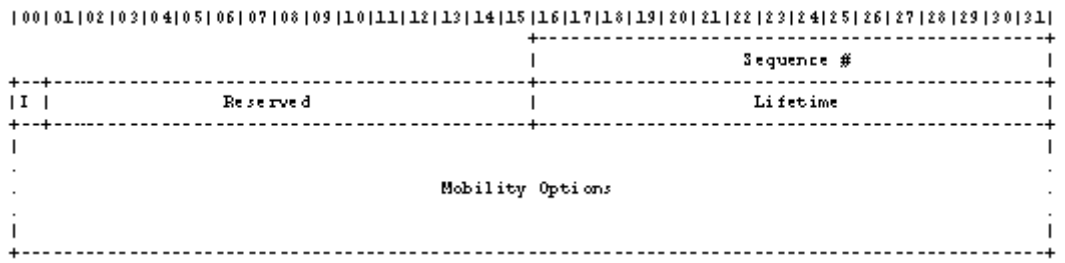



**Figure 18: LRI message format.**

**Sequence number:**

The sequence number is an incrementally increasing unsigned integer provided by the LMA. This 16-bit value is intended to sort arrival of LRI messages and to not apply older actions.

**'I' flag:** When set to 1, it indicates the receiver is an IA.

**Reserved:**

This field is unused for now. The value must be initialized to 0 by the sender and must be ignored by the receiver.

**Lifetime:**

The lifetime indicates how long the procedure has to be maintained by the receiving entity. When this 16-bit field is set to 0, it indicates that the set of actions within the packet has to be stopped. A value of 0xffff (all ones) indicates that the action(s) has to be performed for an infinite duration.

**Mobility Options:**

The LRI message is composed by one or several mobility options. These options will indicate the IPv6 prefixes to optimize towards which destination(s) and using which next hop. We propose in the following the Traffic Anchoring Option (TAO) as a candidate. The mobility options field is of a variable length.

**Localized Routing Acknowledgment (LRA)**

The LRA message is used to acknowledge the reception of the LRI and to indicate the status of the provided actions, i.e., if an error occurs or if the actions have been performed correctly. LRA messages are sent by MAGs and IAs. The header format is presented below in Figure 19:

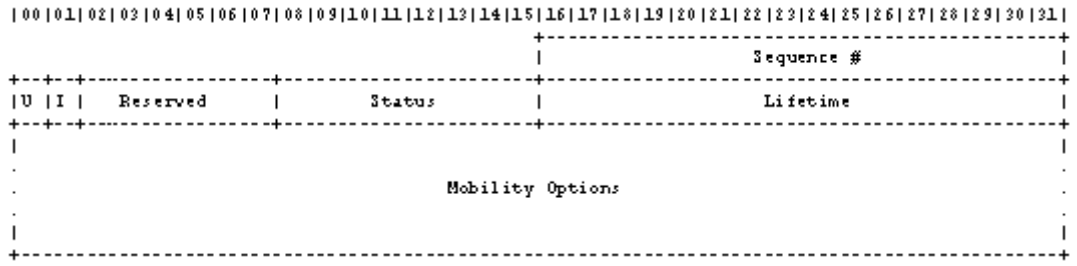



**Figure 19: LRA message format.**

**Sequence number:**

The sequence number is directly copied from the sequence number field of the received LRI.

**'U' flag:** when set to 1, it indicates an unsolicited LRA. It may be used to extend the procedure lifetime (requested by the MAG/IA). The LMA should send an LRI message to confirm the request.

**'I' flag:** When set to 1, it indicates this is sent by an IA.

**Reserved:**

This field is unused for now. The value must be initialized to 0 by the sender and must be ignored by the receiver.

**Status:**

0: success.

128: Localized routing not allowed.

129: The UE is not attached to the MAG.

132: PMIP-IA routing optimization is not allowed.

**Lifetime:**

The lifetime is copied from the lifetime field of the received LRI.

**Mobility Options:**

The mobility options field is a copy of the mobility options field from the received LRI.

**Traffic Anchoring Option**

As Mobility Option, PMIP-RO proposes to rely on a new option called "Traffic Anchoring Option" (TAO). TAO is composed by a fixes-sized part providing the Destination prefix and the next hop. The second part is of variable lengths and indicates the source UE(s) concerned by the optimization, i.e., this optimization may concern one or several source IPv6 prefixes. The MAG/IA, according to the received TAO, must be able to perform per-flow routing optimization. The flows may belong to the same APN or not. An LRI message may be composed by one or several TAOs. TAO has an 8n alignment requirement. The option format is presented below in Figure 20:

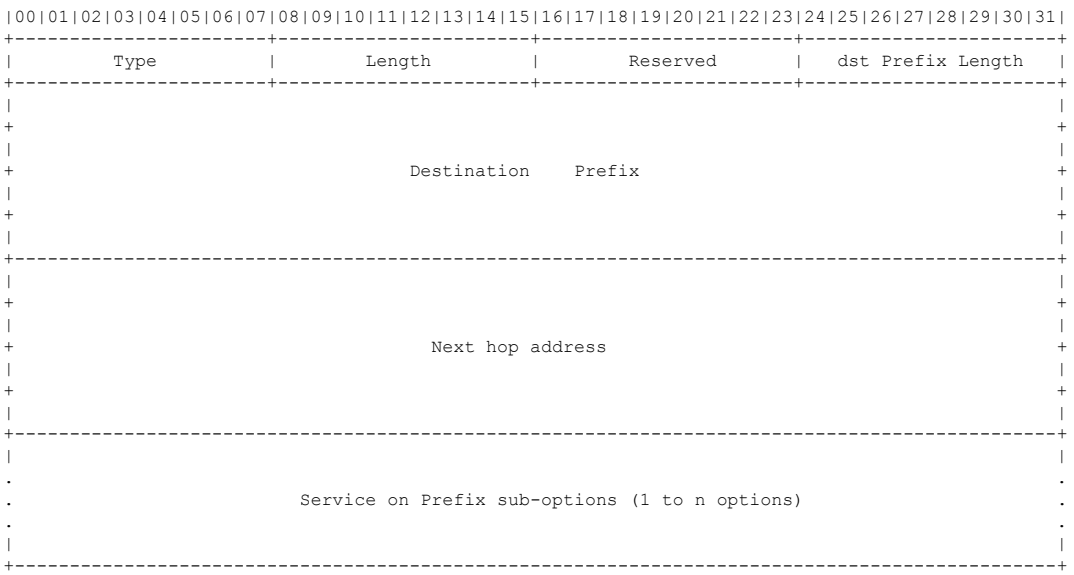



**Figure 20: Traffic Anchoring Option format.**

**Type:**

This 8-bit field indicates the option type. The value remains to be decided. We suggest 28.

**Length:**

8-bit unsigned integer indicating the length of the whole TAO in octets, excluding the type and length fields.

**Reserved:**

This 8-bit field is unused for now. The value must be initialized to 0 by the sender and must be ignored by the receiver.

**Destination Prefix Length:**

This 8-bit field indicates the length of the destination prefix. The value is correct between 0 and 128.

**Destination Prefix:**

The IPv6 destination prefix on 128 bits (16 bytes).

**Next Hop Address:**

The IPv6 address of the next hop. From the IA, the next hop may be another IA or a MAG. From a MAG it may be an IA or another MAG.

**Service on Prefix Sub-Options:**

The TAO may include one or several SOP options all concerned by the 2-tuple <destination, next hop>. The SOP format is presented in the following.

**Service on Prefix sub-option**

The Service on Prefix sub-option (SOP) indicates the set of services to be applied on an IPv6 prefix allocated to a UE Mobile node identifier (MNID). The SOP sub-option is related to the destination prefix and next hop IPv6 address announced in the associated TAO. Figure 21 presents prefix sub option format.

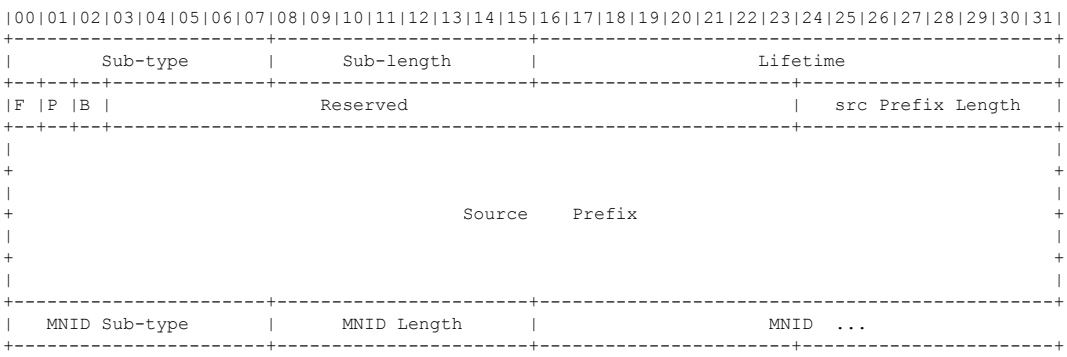



**Figure 21: Service on Prefix sub-option**

**Sub-type:**

This 8-bit field indicates the type of the option. The value remains to be decided. We suggest 29.

**Sub-length:**

This 8-bit unsigned integer field indicates the length of the SOP in octets, excluding the sub-type and sub-length fields. This field takes into account potential padding after the MNID field. Padding helps to maintain the whole TAO alignment requirement.

**Lifetime:**

The lifetime indicates how long the services on the prefix have to be maintained by the receiving entity. When this 16-bit field is set to 0, it indicates that the set of services has to be stopped. A value of 0xffff (all ones) indicates that the service(s) has to be performed for an infinite duration.

**'F' flag:**

When set to 1, indicates that a specific service has to be performed such as content filtering. How this service is practically performed is out of the scope of this document.

**'P' flag:**

When set to 1, indicates that a specific service has to be performed such as pricing. How this service is practically performed is out of the scope of this document.

**'B' flag:**

When set to 1, indicates that a specific service has to be performed such as billing. How this service is practically performed is out of the scope of this document.

**Reserved:**

This field is unused for now. The value must be initialized to 0 by the sender and must be ignored by the receiver.

**Source Prefix Length:**

This 8-bit field indicates the length of the source prefix. The value is correct between 0 and 128.

**Source Prefix address:**

The IPv6 source prefix on 128 bits (16 bytes).

**MNID Sub-type:**

The Mobile node identifier specific type as used within the PMIPv6 domain..

**MNID length:**

This 8-bit field indicates the Mobile Node IDentifier specific type length, excluding the MNID sub-type and MNID length fields.

**MNID:**

The MNID value associated to the provided UE prefix.

### 2.5.1.3 Relevance of the Technology

Current bandwidth-consuming applications such as Video-On-Demand, video streaming or Peer-to-Peer, as well as machine-to-machine and vehicular communications are great challenges for mobile network operators. Concepts such as WiFi offloading, IP anchoring relocation or local IP breakout are under investigation as they are considered as a mean to address those challenges. However, in some cases, the operator has the responsibility on the flows and has to perform content filtering or lawful interception. Hence, it is not always possible to offload traffics without keeping control over them.

PMIP-RO extends PMIPv6 to support the relocation of the data anchoring function on on-going data flows. High throughput accesses, such as WiFi or LTE as well as standard 3GPP accesses such as UTRAN are supported. This service could be used, eventually, to ensure P-GW and even mobile network offloading, e.g., the IA could be located outside of the EPC. By keeping signalization at the LMA and by using IAs under the control of the operators, data flows can still be managed and lawful interception performed.

#### 2.5.1.4 Expected Gains and identified issues

The gain one could expect from PMIP-RO is an increase of the network capacity as long as UE to UE communications in the same PMIPv6 domain increase. There would be a reduction of charge on the main P-GW (in a centralized architecture with P-GWs in national PoP(s)) and the possibility to create new services on flows according to increased knowledge about moving and non-moving UEs.

So far, however, QoS, policy, and charging enforcement in PMIPv6 are out-of-band, i.e., the BBERF entity on the S-GW exchanges information with the PCRF on the P-GW in parallel. Such an approach may be considered as not complete or sub-optimal in the context of routing optimization. More work has to be done to clarify the problematic, to take advantage of this procedure or to resolve this possible issue.

## 2.6 Flat and distributed mobility management

### 2.6.1 Common Section about UFA

The Ultra Flat Architecture (UFA) represents the ultimate step towards flattening IP-based core networks, e.g., the Evolved Packet Core (EPC) in 3GPP. The objective of the UFA design is to distribute core functions into single nodes at the edge of the network. HIP-based UFA (UFA-HIP) addresses mobility, service establishment, security questions for all application types. QoS enforcement in UFA-HIP is controlled by the PCRF and enforced by transport network level bearers. SIP-based UFA (UFA-SIP) can exist alone in a network to manage for all applications (SIP native and non-SIP native): QoS, security, mobility, service establishment.

### 2.6.2 HIP-based Ultra Flat Architecture

#### 2.6.2.1 Relevance of the Technology

Covered challenges:

- In the near future the realization of Internet-of-Things will also bring applications requiring high security. E.g. M2M communication related usage scenarios will contain a subset of monitoring and controlling applications that will communicate over 3GPP architecture and will require high security.
- Regarding the concept of distributed/flat 3GPP architecture, which have been introduced due to increasing traffic demands, one important challenge is the provision of service continuity during inter-GW handovers. The GW means the first IP-hop in case of 3GPP, non-3GPP accesses to the EPC.
- Seamless inter-GW handover should be provided for real-time applications
- Currently, attachment to new GWs, e.g. in case of changing ePDG, the complete attachment procedure is performed. Due to the distribution of GWs inter-GW handovers will happen more and more frequently. Reduction of security overhead due inter-GW handovers an important challenge within the focus of this technology.
- 3GPP and non-3GPP accesses provide different set of security services. An important objective is to provide unified security services, independent of the access. UFA-HIP e.g., provides confidentiality, integrity, message origin authentication and anti-replay services on L3 within the user security and network security domains.
- Besides securing user plane, the 3GPP architecture shall continue QoS enforcement, Accounting, Legal interception of secure communication. Hence end-to-end security associations are not considered as the best overlay option. The IPsec connections are segmented between the communicating end-points and the GWs.

### 2.6.2.2 Description of the Technology

#### 2.6.2.2.1 Service data flow mapping to HIP transport

UFA-HIP changes the end-to-end nature of original HIP protocol by introducing a HIP signaling delegate for the HIP-enabled UEs. Typically the first IP GW of the UE shall be the UFA-HIP GW, which runs HIP signaling delegation service. This change causes that on the path between the endpoints of the service data flows the IPsec SA pair is segmented to multiple IPsec BEET mode tunnels by the GWs. User data packets must be mapped at each UFA-HIP GW from one IPsec security association to another IPsec security association. Flow mapping in UFA-HIP GWs is illustrated in Figure 22. Control plane header is required for unique mapping of service data flows. SPI and IP address based mapping can cause SPI collisions because SPI is locally selected for each IPsec SA.

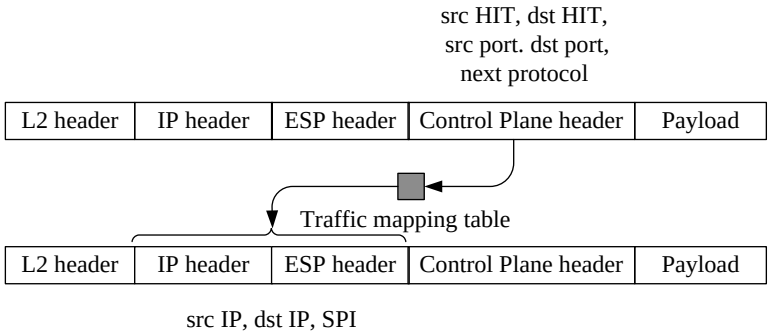



**Figure 22: Basic service data flow mapping in HIP UFA GWs.**

#### 2.6.2.2.2 QoS enforcement by the transport network layer

QoS in UFA-HIP solution is enforced by lower layer tunneling protocols. In the short-term, the tunneling option can be any option specified in the 3GPP standard that provides IP connectivity and separate bearers for QoS enforcement for the UE. In the long-term, tunneling is HIP/IPsec based on the top of transport network layer. The transport network layer implements separate bearers, e.g., MPLS PWs, VPLS. VPNs, 802.1p VLANs, and provide IP connectivity to the GWs and eNodeBs. Figure 23 depicts service data flow mapping to IPsec SAs and transport network level bearers in HIP UFA GWs and UEs. The mapping is based on the [source HIT, destination HIT, source port, destination port, transport protocol] quintuplet describing the service data flow. Note: applications that require different QoS may use similar ports. All parameters that are needed for the derivation of the application class should be considered here, hence it is possible to add to the control plane header a field for application class ID.

The service data flow is mapped to the appropriate IPsec SA that goes to the next UFA-HIP GW on the path, or the recipient UE or end-node on the top of the appropriate transport network bearer (e.g., using the appropriate virtual network interface). This assumes that transport network layer has pre-configured or dynamically established bearer levels that implement all QoS options required by the service network layer. Note: mapping of 3GPP QoS classes to TNL bearer levels requires further research. Direct mapping is impossible. PCRF or other standardized alternatives, such as the HSS through MME or AAA provide QoS rules to the UFA-HIP GWs. QoS rules are either based on service data flows, i.e., the traffic filters contain source port, destination port, transport protocol, or based on subscriber-profile and service type, i.e., the traffic filters also contain the HIT of the user.

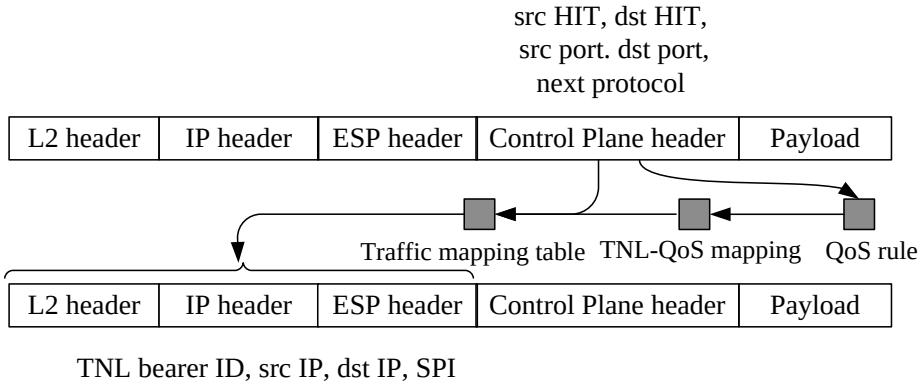



**Figure 23: Service data flow mapping to IPsec and transport network layer bearers in HIP UFA GWs**

#### 2.6.2.2.3 HIP delegation services

The delegation of signaling rights is motivated by the optimization of resource utilization between the delegator and the delegate. Delegates are temporarily authorized by the delegator to proceed in certain tasks, such as periodic location updates, rekeying. The delegator may issue a public-key authorization certificate [15] to the delegate to proceed in his name at the peers.

HMAC key could also be issued to a delegate in order to generate HMACs admitted by the peer, as described in [14]. Before right delegation it is important that the delegator establishes trust relationship with the delegate, i.e., the identity of the delegate must be authenticated. Delegation chains require implicit trust chains. In our signaling scheme, we apply public key authorization certificates containing the following information:

- public key, HIT of delegator
- public key, HIT of delegate
- roles of the delegate, such as provision of Type 1 or Type 2 services to a UE or GW.
- restrictions, such as expiration date, number of uses
- the digital signature of the delegator

Two new HIP delegation service types, i.e., Type 1 and Type 2 HIP Delegation Services, are introduced for the following reasons:

- make possible fast inter-GW handovers
- reduce performance overhead between the UE and the GW (i.e., computation and messaging demands of L3 network access service)
- reduce the number of intial L3 access authorization flows in all the network
    - by the usage of delegation service, only the first attachment to a new authority's domain triggers full L3 access authorization.
    - inte-GW handovers do not trigger full L3 access authorization procedure within the domain of the authority

**Type 1 HIP Delegation Service and CXTP**

- Type 1 Delegation Service requires
    - pre-existing IPsec SA between the Delegator and the Delegate, and
    - HIP host association between the Delegate and the UE's peer (CN).

- Delegate
    - establishes new HIP and IPsec SA with the CN, in the name of the Delegator, i.e. replaces HIP BEX between the delegator and the CN. New cryptographically separate master keys must be derived from existing keying material between the delegate and CN.
    - sends to the Delegator the new HIP and IPsec SA contexts using CXTP protocol, protected with IPsec

  Note: Type-1 Delegation service is used in the following ways
    - During HIP-based L3 handover preparation, the target GW must establish HIP and IPsec SAs with the UE and its peers (CNs or the UFA GW's of CNs, RVS)
    - The Type 1 Delegate of the target GW is the source GW.

Figure 24 depicts the signaling in case of Type-1 HIP Delegation service.

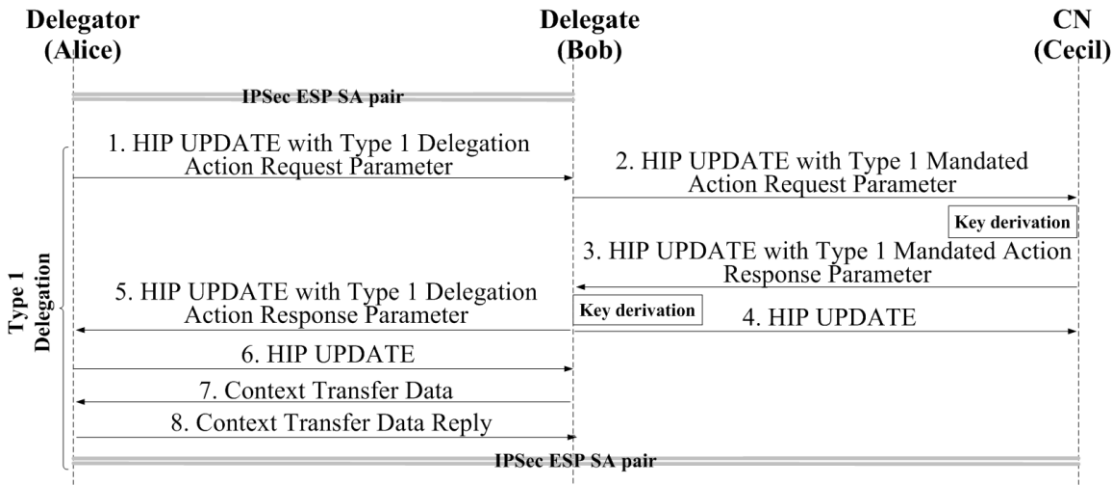



**Figure 24: Type-1 HIP delegation service**

**Type 2 HIP Delegation Service**

- The Delegate
  - executes HIP Base Exchanges (BEX), HIP Updates, IPsec SA establishment in the Delegator's name, with the Delegator's authorization, towards the peers of the Delegator.
  - maintains the established HIP and IPsec associations for Delegator (periodic re-keying) with the peers
  - ~ and the Delegator notify each other in order to create the HIP host association also in the Delegator, as soon as a new HIP host association is created with a peer of the Delegator. These HIP host associations use the existing IPsec SA between the Delegator and the Delegate as transport protocol.

  Note: The GW performs Type 2 mandated actions in UE's name, during
  - session establishment (HIP, IPsec SA establishment and periodic rekeying)
  - Location and traffic forwarding policy update at the peers (CNs, RVS) of the UE during HIP-based L3 handover preparations

Figure 25 presents the message chart of Type-2 HIP delegation service.

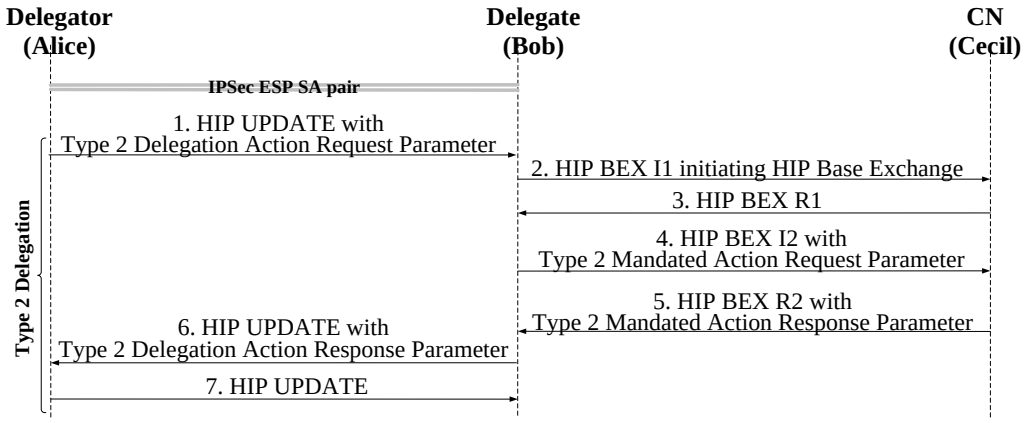



**Figure 25: Type-2 HIP delegation service.**

**Registration to Type 1/2 Delegation Service**

Figure 26 illustrates the registration procedure to HIP delegation service. The Delegate gets an Authorization Certificate (or Token) from the Delegator that will prove for the CN that the Delegate is authorized to proceed in Delegator's name

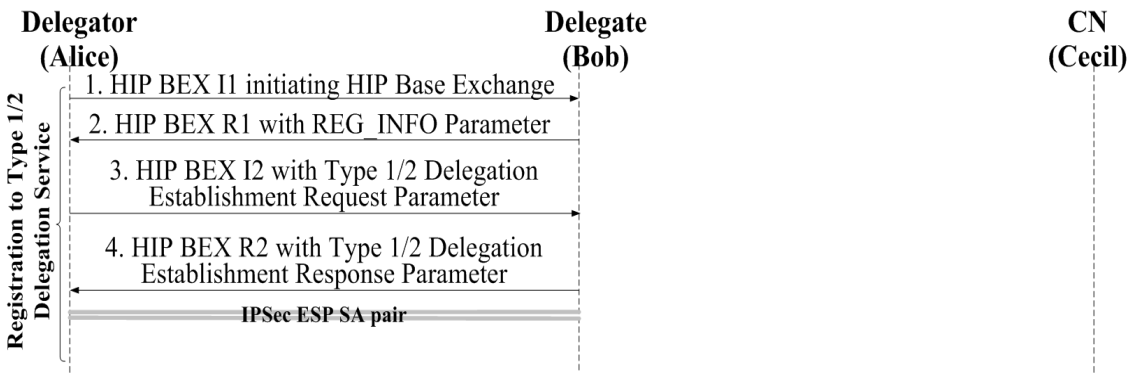



**Figure 26: Registration to HIP delegation service**

**Meaning of HIP delegation messages:**

Table 1: Meaning of HIP delegation messages,Figure 26 summarizes the HIP delegation messages.

**Table 1: Meaning of HIP delegation messages**

| HIP Parameter | Explanation |
|---|---|
| Delegation Establishment Request | The Delegator sends to the Delegate in order to request Type 1/2 delegation service using HIP REG_REQ parameter. Authorization Certificate chain of the entity requiring delegation service must be included in HIP NOTIFICATION parameter(s). |
| Delegation Establishment Response | The Delegate sends to the Delegator in order to acknowledge or reject Type 1/2 delegation service establishment using HIP REG_RESP or REG_FAILED parameter. |
| Delegation Action Request | The Delegator sends to the Delegate in order to request HIP and/or IPsec association creation or update. In case of Type 1 Delegation Service the state information will be transfered to the Delegator. For Type 2 Delegation Service, the states resulted by the action will be created and further maintained by the Delegate. |
| Delegation Action Response | The Delegate sends to the Delegator in order to report the Type 1/2 delegation action results in HIP NOTIFICATION parameter(s). |
| Mandated Action Request | The Delegate sends to third party node(s), e.g., the CNs, RVS of the UE . For Type 1 Delegation Service HIP and/or IPsec associations will be created by the Delegate and transfered to the Delegator. In case of Type 2 Delegation Service, new HIP and/or IPsec states are created on behalf of the Delegator by the Delegate and/or traffic mapping rules will be updated. HIP NOTIFICATION parameters are used to transfer the required information such as supported IPsec SPI values of the Delegator, global locator(s) of the Delegator, list of supported HIP and IPsec transforms, traffic mapping rules, Delegator peer list, configuration and service registration parameters, etc. |
| Mandated Action Response | Third party node(s) send to the Delegate in order to report Type 1/2 mandated action results in HIP NOTIFICATION parameter(s). |
| Context Transfer Data (CTD) | Sent by the Delegate to Delegator, and includes feature data (i.e., HIP and IPsec context data). |
| Context Transfer Data Reply (CTDR) | Sent by Delegator to Delegate, indicating success or failure of context transfer. |

#### 2.6.2.2.4 Main communication procedures of UFA-HIP

**L3 Attachment:**

Figure 27 presents the L3 attachment procedure in UFA-HIP.

The described attachment procedure starts after L2 attachment. It contains the following phases:

- UE acquires IP address, and discovers the GW. The usage of DHCPv6 is illustrated in the figure, but other alternatives are also possible, such as stateless auto-configuration, usage of link local address, DHCP, configuration during L2 network access service.
- L3 network access service (NAS) using HIP Diet Exchange with EPS-AKA (HIP DEX-AKA), as described in section 2.7.1.2 for resource constrained UEs. After successful authentication an IPsec BEET mode SA pair is created between the UE and the GW.

  Note: Alternative options for L3 NAS exist as well, such as HIP Base Exchange extended with the EPS AKA procedure; HIP Base Excange using certificate-based authentication [13], HIP BEX/DEX extended with EAP and using the EAP Re-authentication Protocol (ERP) [12].

  Note: in case of QoS enforced by separate transport network layer bearers, multiple IPsec SA pairs shall be created for separate bearers.
- The IPsec connections enables secure bootstrapping including e.g., the configuration of the address of MIH PoS (i.e., the GW), DNS. The GW may act as a DHCP server or relay when bootstrapping the UE.

- After bootstrapping and service discovery, registration to various services is performed. The GW (PoS) discovers the MIH capabilities of the UE, and registers to its MIH event services to monitor the UE's link-state. The UE registers to the GW's HIP Type 2 signaling delegation service. As a result, the GW gets a temporary authorization to delegate the UE towards the UE's peers, i.e., it can perform signaling such as location update at RVS, IPsec and HIP association maintenance, and L3 handover preparation and execution in the UE's name. To provide initial reachability from new CNs, the GW registers the UE's current location within the addressing service, i.e., updates the RVS. For SIP-based applications, the UE also performs a SIP registration procedure.

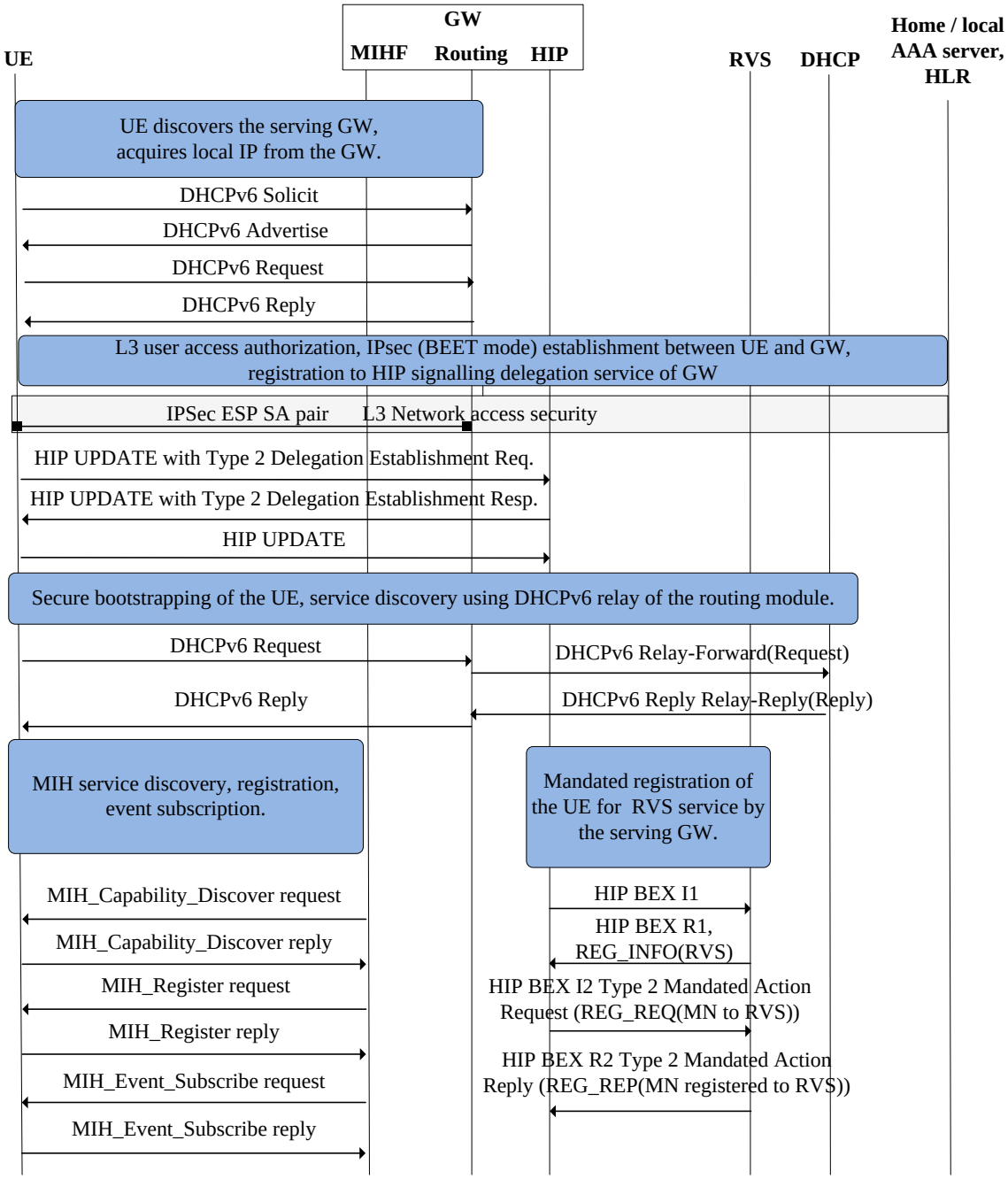



**Figure 27: L3 attachment procedure of UFA-HIP.**

**Session establishment :**

The HIP session establishment between UE and its peers is illustrated in Figure 28. Before applications can establish sessions, the HIP/IPsec connections must be established towards the UE's peer. The peer may be another HIP-enabled UE or a HIP-enabled server that can be reached though a remote delegate UFA-HIP GW or directly from the serving GW of the UE.

The UE already has HIP/IPsec connection to its serving GW. Using Type 2 HIP delegation service, the GW is notified by the UE to establish the HIP host association and IPsec transport towards the peer. If the HIP host association did not exist between the GW and the peer then a HIP BEX is performed extended with mandated action request parameters, as illustrated in Figure 28.

If the HIP/IPsec association has already been established between the serving GW of the UE and the peer, then a HIP update procedure extended with the mandated action request parameters must be called between the serving GW and the peer. In both cases, traffic mapping tables must be updated; the new HIP host associations must be created in the UE, serving GW, peer (and possibly the serving GW of the peer) and mapped to the appropriate IPsec SAs.

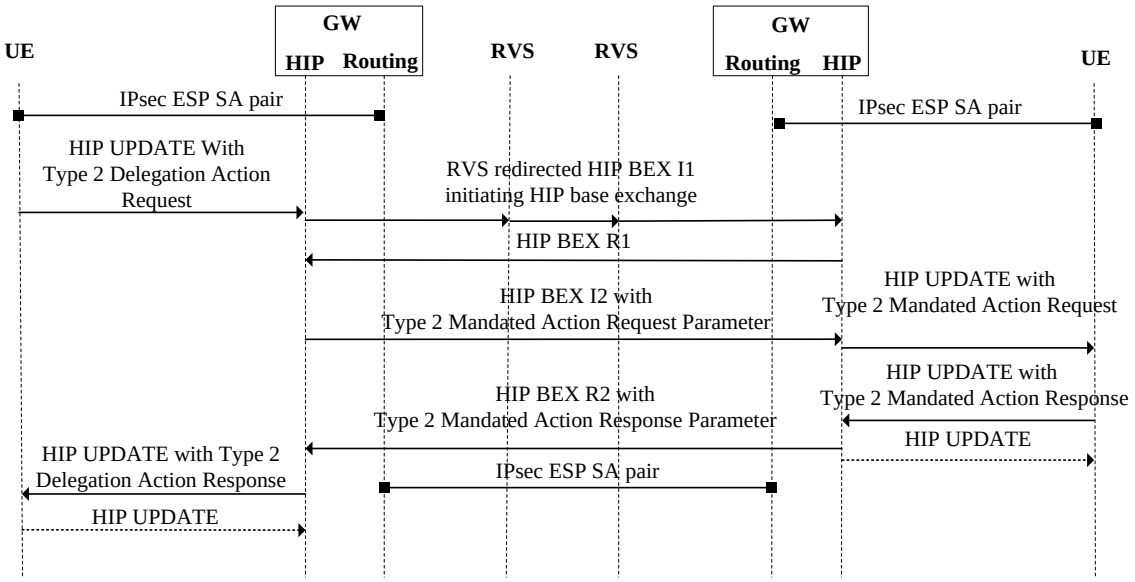



**Figure 28: Session establishment procedure in UFA-HIP**

**Handover procedure:**

- UFA-HIP integrates IEEE 802.21 MIH and HIP delegation services in order to perform handovers
- Both for inter- and intra-GW handover procedures network-controlled MIH is applied as described in [11], Appendix C.2. The Point-of-Service (PoS) collecting the information for handover decision is the serving GW of the UE.
- In case of intra-GW handover procedure, if the IP address of the UE is changed in the new access network, HIP mobility update procedure must be called as described in [16]. This will update the address of the UE in the IPsec SAs towards the serving GW.
- In case of inter-GW handover procedure HIP delegation services provide the necessary context transfer to the new GW, and the update of HIP and IPsec contexts in the UE, peers of the UE.
- In the followings we describe the inter-GW handover procedure phases.

**MIH Handover initiation:**

The serving GW configures the UE with the set of QoS thresholds using the MIH Command service flow, as described in Section 6.4.2 of [11]. As a result, the serving access interface periodically notifies the registered MIH user (i.e., the handover decision manager in the serving GW) about its QoS parameters. Based on this information, the GW can trigger the handover preparation phase before connectivity is lost.

**MIH Handover preparation (on L2):**

Figure C.2 in [11, pp193-194] illustrates a full network initiated handover procedure. In the handover preparation phase it is possible to perform information query from MIH Information service and resource

availability check in candidate radio access networks (i.e., MIH Point of Accesses). Static information on neighboring PoAs shall be cached in the serving GW.

**Handover decision procedure:**

The serving GW decides on the target MIH PoA and target GW for a set of service data flows of the UE.

**HIP-based Handover Preparation:**

Figure 29 and Figure 30 illustrate the HIP-based handover preparation procedure. The serving GW of the UE triggers the procedure.

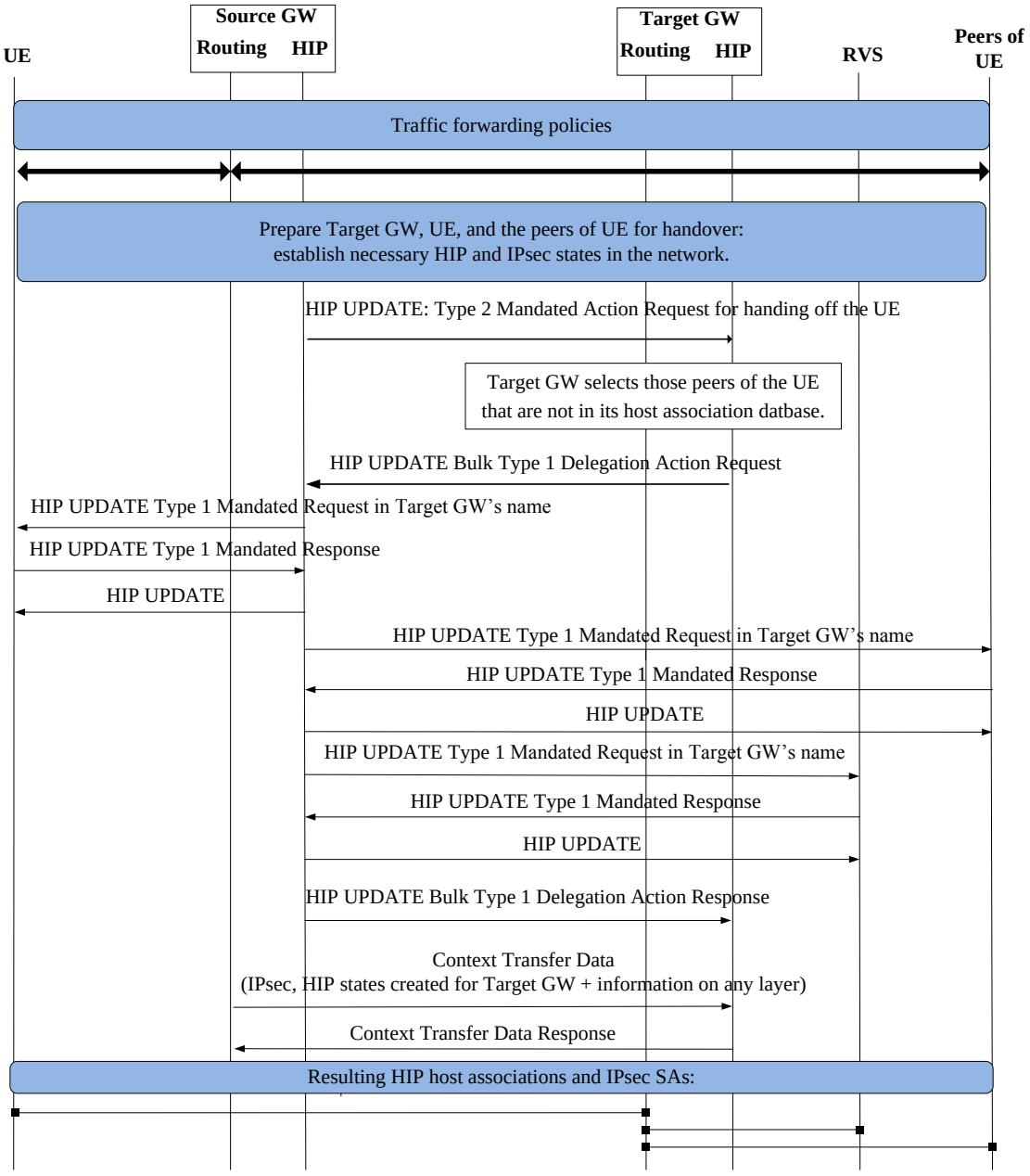



**Figure 29: HIP-based handover preparation procedure (part 1)**

First, it asks the target GW to establish HIP and IPsec associations with the UE and the peers of the UE

- In Type 2 Mandated Action Request, the source GW sends to the target GW the list of the HITs of the peers of the UE and the HIT of the UE. The target GW shall establish HIP and IPsec associations only with the nodes that it had not previously established HIP and IPsec associations.

- The target GW asks the source GW to establish HIP and IPsec associations in his name with the UE and the peers of the UE using Bulk Type 1 Delegation Action Request. The source GW already has security contexts with the intended nodes, so the security contexts between the nodes and target GW can be derived using symmetric cryptography primitives in the source GW and the nodes. Then context transfer protocol over IPsec conveys the security contexts from the source GW to the target GW.
- Next, in Figure 30, the traffic forwarding policies are updated by the target GW in the peers of the UE. After that Type 2 Mandated Action Response to hand-off the UE is sent back from the target to the source GW.

Next, the source GW sets up a delayed traffic forwarding update in the UE with Mandated request (in the name of the target GW). Delaying means that the traffic forwarding policies for the selected traffic flows from the UE to the GW will be updated after physical handover to the new L2 PoA.

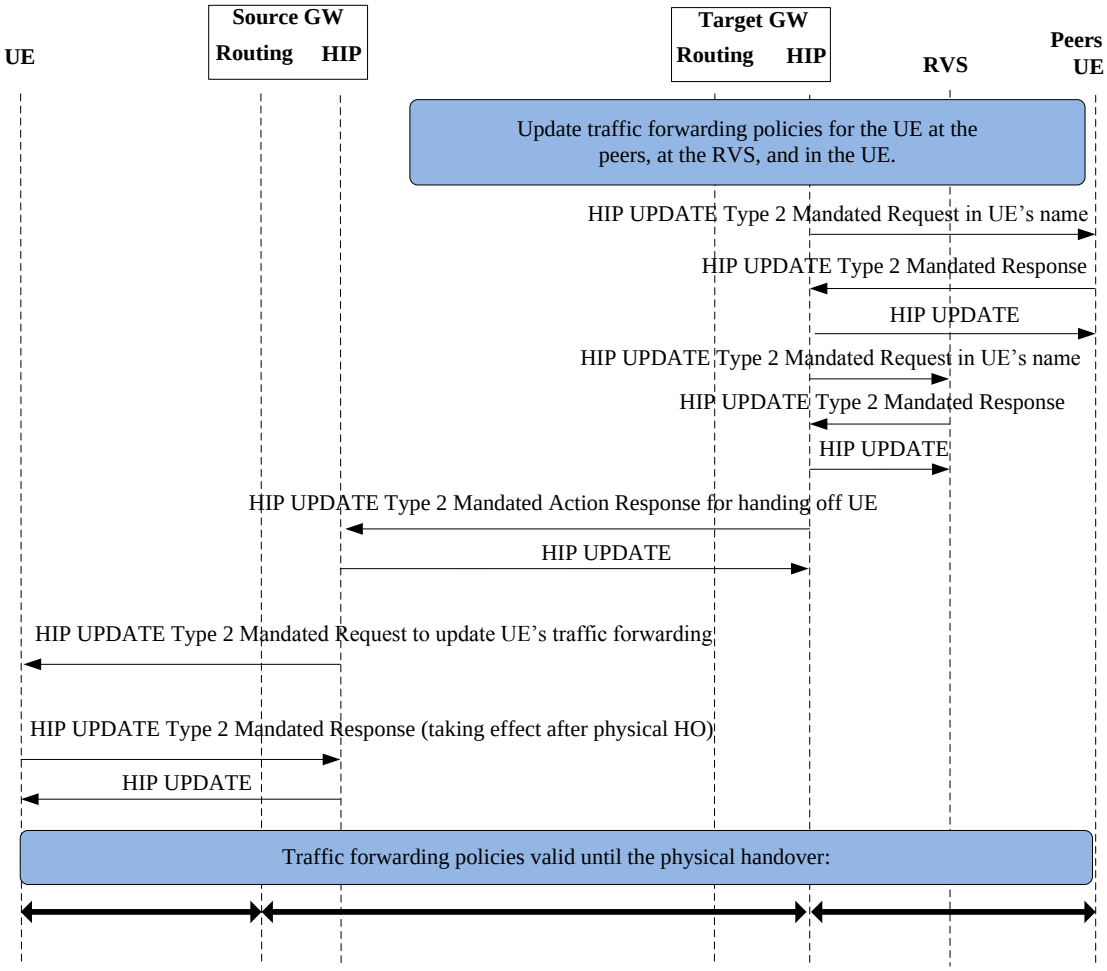



**Figure 30: HIP-based handover preparation procedure (part 2).**

**MIH Resource preparation, establishment of new L2 connection, link up indication**

These MIH phases follow the HIP-level handover preparation, as depicted in Figure C.2 in [11, p195-196]

**MIH Resource release**

The L3 mobility management have been proactively done in the HIP-based handover preparation procedure. So After L2 connection establishment and link up indication MIH resource release phase shall come, as depicted in Figure C.2 in [11, p196]. Under this phase the source and target GWs update the UE's traffic forwarding policy. UE's data traffic is forwarded via the target GW to the peers of the UE.

### 2.6.2.3 Expected Gains and identified issues

Current 3GPP architecture provides user access authorization and data protection on different layers depending on the access type. Due to the features of different technologies these provide different security services to transport and application layer.

In the followings we summarize the security features of different access types in 3GPP Rel-11:

**3GPP-access** (TS 33.401, TS 33.102):

- user and network authentication with EPS-AKA procedure
- user identity (IMSI) and device identity (IMEI) confidentiality shall be provided
- confidentiality protection of S1, X2, RRC messages and NAS messages shall be provided
- integrity protection, and replay protection, shall be provided to NAS and RRC-signalling. *User plane packets between the eNB and the UE shall not be integrity protected on the Uu interface*. User plane packets between the RN and the UE shall not be integrity protected.

**Trusted non-3GPP access** (TS 33.402):

- L2 mutual authentication of the UE and the AAA server, access authentication using EAP-AKA' (RFC5448) or EAP-AKA (RFC4187). The non-3GPP access network relays the EAP messaging.
- Confidentiality of user identity in the non-3GPP access part is out of the scope of 3GPP standards. If EAP-messages are encrypted within the L2 access authorization protocol then user identity confidentiality is provided.
- device identity confidentiality is out of the scope of 3GPP standards
- user and signalling data confidentiality and integrity between the UE and the non-3GPP access network is provided using the access specific security services on L2.
- between the access and the security GW, IPsec ESP SAs may provide network-security services (see later)

**Untrusted non-3GPP access** (TS 33.402):

- IKEv2 based mutual authentication of UE and ePDG, using EAP-AKA to authenticate the user and the network, and certificate to authenticate the ePDG.
- IKEv2 protects the confidentiality of user identity (IMSI) and device identity (IMEI)
- IPsec ESP tunnel protects the user plane packets between the UE and the ePDG on L3. Protection services include confidentiality, integrity, message origin-authentication, anti-replay protection.
- If the UE moves to a new untrusted non-3GPP access network and its IP address changes, MOBIKE can be used to update the IKEv2 and IPsec security associations. This only holds if the ePDG is not changed. Whenever the ePDG changes the whole IKEv2 procedure must be repeated.

**Network-security** (TS 33.401): It shall be possible to protect user, control and management plane data between network elements, on the X2 and S1 interfaces with transport or tunnel mode IPsec using ESP. Network security service is also relevant in case of non-3GPP access between the radio access network and the Security GW of the provider:

- confidentiality protection
- integrity protection
- anti-replay protection
- message origin authentication
- mutual authentication of network elements (eNBs, S-GWs / SEGs) with certificate-based IKEv2.
- in case of DiffServ QoS for each DSCP value (QoS class) separate IPsec child security association pair shall be created.

Expected security gains from UFA-HIP architecture are described in the followings.

HIP based user access establishes IPsec SA with ESP in BEET (or tunnel) mode between the first IP gateway and the UE. It provides the following security services.

**Untrusted non-3GPP access**

- confidentiality protection of user plane on L3 at the SWu interface
- integrity protection of user plane on L3 at the SWu interface
- anti-replay protection on L3 at the SWu interface
- message origin authentication of user plane on L3 at the SWu interface
- mutual authentication between the UE and the network. Certificate-based authentication of ePDG is optional, because the HIP host identity of the ePDG is self-certifying, furthermore the assumption is that if the network authentication with EAP-AKA is successful then the ePDG is also trusted (only a correct AAA (in ePDG) can get the correct authentication vectors from the HSS).

**Trusted non-3GPP access**:

- Depending on the tunnelling solution, the first GW may be the P-GW (in case of GTP option on the S2a interface (TS 23.402) or a router in the trusted non-3GPP access network (e.g. in case of PMIP tunnelling option on the S2a interface (TS 23.402).
- Security services on L2 between the UE and the trusted non-3GPP access network are as described before, i.e. depends on L2 access type.
- The IPsec ESP tunnel between the UE and the first GW (P-GW / router in the trusted non-3GPP access domain ) established by HIP DEX provides in this case the following additional features:
    - integrity protection,
    - message origin authentication,
    - confidentiality,
    - anti-replay protection on L3, independent of whether these are implemented in L2.

**3GPP access**:

- Depending on the tunnelling solution in S1, S5/S8 interfaces, the first GW might be the P-GW (e.g., GTP option), or the S-GW (GTP tunnel on S1 and PMIP-based IP GRE tunnel on S5/S8).
- Similar security services are provided as in case of standardized 3GPP-access described before
- Additionally, IPsec ESP tunnel between the UE and the first GW shall provide:
    - Integrity protection, message origin authentication, confidentiality, anti-replay protection on L3.

      Note: integrity protection, message-origin authentication and anti-replay protection is not currently provided in 3GPP-access for user plane traffic. HIP-DEX AKA hence adds this security service in 3GPP-access.

Note that security solutions on L3 may not always prevent or detect attacks on L2. Hence L2 threats of access networks must be considered, and appropriate security control must be enforced. Hence current security features in 3GPP-access should remain as described in the 3GPP standards, and appropriate measures out of the scope of 3GPP standard must be realized in non-3GPP access networks.

Other expected gains of UFA-HIP are:

- service continuity during inter-GW handover for any application using the HIP sockets
- seamless inter-GW handover for real-time applications
- reduction of security overhead due to frequent GW change
- support of resource constrained devices by light-weight network access protocol, i.e., HIP DEX-AKA (see Section 2.7.1)

Identified issues:

- Introduction of control plane header adds overhead for each user data packet. Further research for enabling compression of the control plane header is required.
- QoS enforcement shall require separate IPsec SA pairs for each QoS priority level enforced by transport network bearers. Currently HIP protocol enables one IPsec transport between two HIP peers. The network interface is selected by the routing table. Further development of the protocol

is needed to negotiate multiple IPsec pairs at once for different traffic priorities enforced by the transport network layer (e.g., 802.1q/p, MPLS).

- Signaling delegation currently is based on certificate issuance of the UE to the delegate GW, and further delegation of the UE's rights between GWs. The length of delegation chain must be lower than a maximum value. Other lightweight solutions should be searched for in order to achieve signaling right delegation.
- Communication of HIP-enabled UEs with non-HIP enabled end-nodes with the use of HIP-proxy solutions is not recommended due to security reasons. Allowing a HIP-enabled UE to communicate through a proxy with non-HIP enabled peer, or allowing a HIP-enabled node to open ports through non-IPsec transport might help an attacker to exploit back doors and to by-pass the IPsec firewall in HIP-enabled nodes.

### 2.6.3 SIP-based Ultra Flat Architecture

Scalability issues anticipated for the EPC and IMS architectures has lead to define a new mobile network architecture called UFA (Ultra Flat Architecture) [3][4]. UFA in not a unique technology but a set of technologies comprising architectural and procedural aspects. It applies to the centralized, distributed and flat architecture scenarios, but better fits to distributed and flat scenarios. In UFA, the EPC and some IMS functions are not only co-localized, but are combined in a single node in an optimized way, called the UFA-GW. In UFA-SIP most of procedures (authentication, establishment, and mobility) are managed using SIP protocol.

#### 2.6.3.1 Description of the Technology

UFA-SIP is based on SIP to provide service control for all services during service access and mobility procedures. Thus, non-SIP native services are extended to be controlled by SIP protocol. Controlling non-SIP native services by SIP has required an interaction between SIP protocol, these services and SCTP in the Mobile Node (MN) and the Correspondent Node (CN).

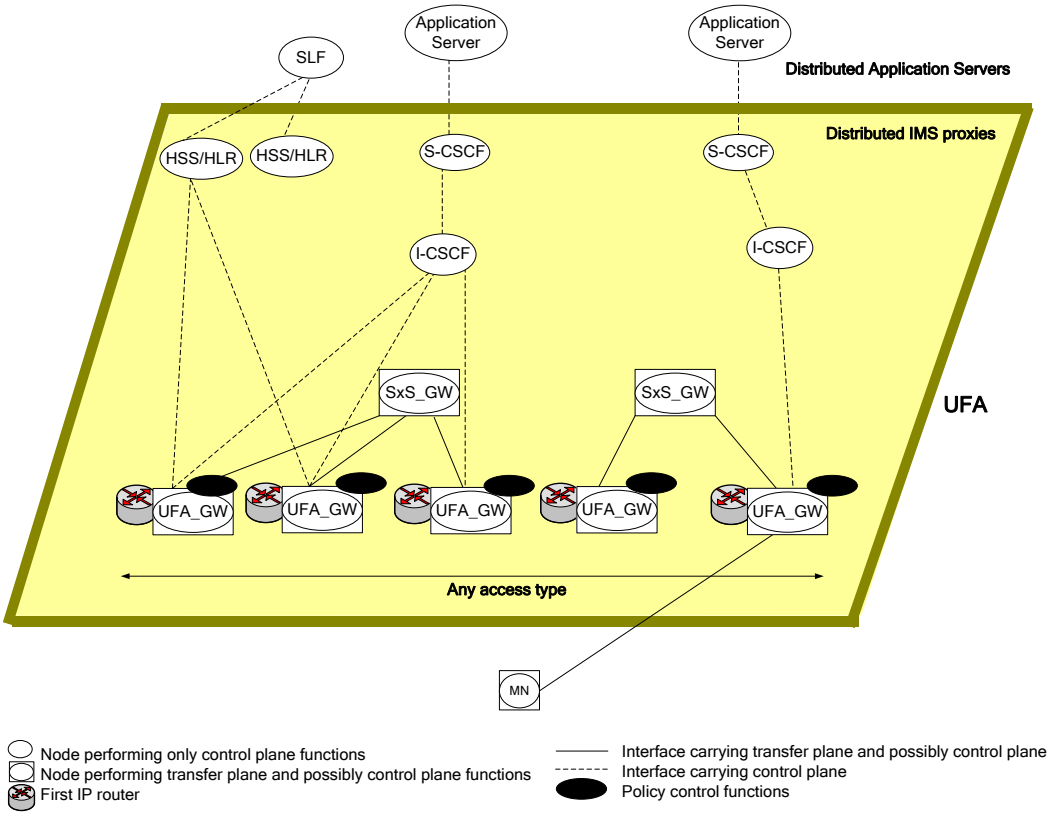



**Figure 31: UFA architecture**

UFA is constituted of 6 network nodes: the e-NB, the I-CSCF (IMS proxy node), the S-CSCF (IMS proxy node), the HSS and two new nodes, that are:

- UFA Gateway (UFA_GW): the UFA_GW is the main node in UFA. It gathers the classical LTE/EPC node functions (MME, S-GW, P-GW), policy control (PCC) functions [22], P-CSCF functions, SCC AS functions [23] and new introduced functions that control the service access and mobility procedures. This means that the UFA_GW controls the session and offers IP connectivity (UFA_GW is the first IP router) to users. It has to be noted that the UFA_GW is not just a co-location of functions and equipments, but an optimal combination of functions in unique equipment.

- SIPcrossSCTP Gateway (SxS_GW): this node handles, for non-SIP native services, the cases where the interaction between SIP protocol and non-SIP native services is not supported in the CN. The Figure 31 presents the UFA so far discussed in this section.

#### 2.6.3.1.1 UFA nodes and control functions

Most of the UFA control functions are within the network, specifically in the UFA_GW. The MN and the CN act as slaves to the network intelligence. We describe hereafter the UFA_GW, emphasizing on its control functions. We also detail the other UFA nodes on the control and transfer planes (Figure 31).

**UFA Gateway**

The UFA Gateway (UFA_GW) control functions are within a controller module. This module generates decisions regarding the service access and mobility procedures. Decisions are enforced by acting on SIP messages, thanks to the SIP Back-to-Back User Agent (B2BUA).

The Controller contains the SCC AS function, the IMS functions, the policy control functions, and other control functions adding more intelligence to the UFA_GW. These control functions enable to:

– Decide on mobility from the current UFA_GW to a target UFA_GW in case of coverage loss, current overload or better conditions detected on the target UFA_GW. The interaction with the SCC AS functions enable to decide whether the handover decision is compliant with the the home operator policies.

– During service establishment phase or mobility procedure, determine:

* The service configuration for SIP native services, or the SCTP layer configuration for non-SIP native services transported over SCTP, the CN should have:
  - The service configuration for SIP native services contains the new MN IP address and the service adaptation (i.e. downgrade or upgrade), based on the (target) UFA_GW available resources.
  - The SCTP layer configuration for non-SIP native services contains the new MN IP address and the SCTP congestion control parameters. It is assumed that non-SIP native services, transported over SCTP on the transfer plane, do not need service adaptation. They adapt their bitrate to the available bandwidth. However, to use efficiently the available bandwidth, SCTP layer needs to be configured with optimal values for its congestion control parameters.
* The all-OSI layer configuration the MN should have. It includes, among other things, the MN IP address and the service configuration for SIP native services or the SCTP layer configuration for non-SIP native services.

The Controller then communicates these configurations to the B2BUA, which sends them within SIP messages to the MN and CN.

To trigger the previous actions, the Controller receives and treats inputs coming from other internal sub-modules (Figure 32). The Radio sub-module collects the radio measurements, sent by the MNs about their current UFA_GW and neighboring ones. These measurements enable to trigger a handover based on coverage criterion. The Resource information sub-module calculates the UFA_GW available resources in order to trigger a handover based on load criterion or to adapt the service. The controller also stores the contexts generated following the service access procedure.

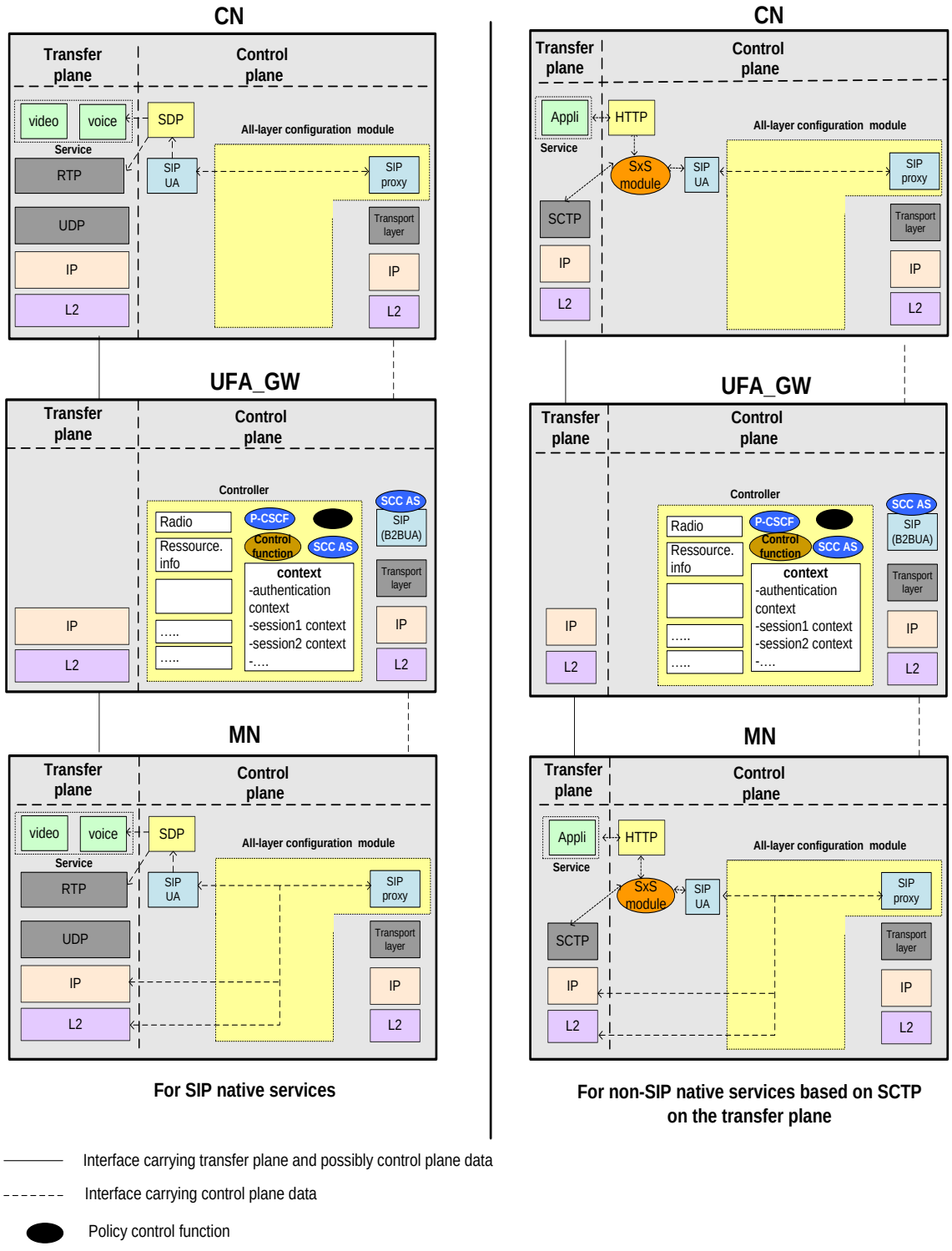



**Figure 32: UFA user and control planes**

**The Back-to-Back User Agent (B2BUA):** is quite similar to the SCC AS B2BUA with added/modified features. Like the SCC AS B2BUA, it terminates the SIP dialog (dialog1) initiated by the MN and establishes a second SIP dialog (dialog2) with the CN. Unlike the SCC AS B2BUA, it modifies the content of SIP messages exchanged between the MN and the CN or builds SIP messages that are sent to the MN and CN based on decisions and configuration information received from the Controller.

**Terminal (MN/CN)**

In addition to the classical SIP UA responsible for controlling applications, the MN/CN implements UFA specific modules on the control plane. As shown in Figure 32, these modules are:

- SIP proxy: As described in the previous section, SIP messages received from the UFA_GW may contain configuration information. The SIP proxy in the MN/CN is responsible for filtering and extracting the different layer-related configuration information and relaying them to the all-layer configuration module.
- All-layer configuration module: It receives the different layer-related configuration information from the SIP proxy and relays each part to its concerned layer (layer 2, IP, SIP UA). For non-SIP native services, the SIP UA relays the received information to the SIPcrossSCTP module.
- SIPcrossSCTP module (SxS module): This module within the UFA_GW is specific to non-SIP native services. It is responsible for the interaction between the service, SIP and SCTP. It has a central role in making non-SIP native services controlled by SIP. It locally detects the service related events (establishment, release) and triggers the equivalent events on the SIP level. For example, when a service is going to be launched, it establishes a SIP session and fills equivalent SDP fields (service name, flow descriptors).

It receives from the SIP UA, the SCTP-related configuration information sent by the UFA_GW, and relayed to it by the all-layer configuration module. Then, it enforces this configuration by interacting with SCTP.

**SIPcrossSCTP Gateway (SxS_GW)**

The support of non-SIP native services in UFA requires that the MN and the CN implement both SIP and SxS module. However, if the CN lacks these functions, to handle non-SIP services over UFA, a proxy network node, called SIPcrossSCTP Gateway (SxS_GW), is needed. When the MN initiates a non-SIP native service, SIP signaling is sent to the CN. The SxS_GW, intercepts this signaling and translates it to service specific signaling (e.g. RTSP or HTTP), that it sends to the CN. Thus, the SxS_GW anchors the control plane traffic. It also anchors the data plane traffic.

### 2.6.3.1.2 Attachment procedures

For UFA (Figure 33), the same registration/authentication steps, as those for the LTE/EPC+IMS model, have to be executed. Some choices regarding the means to execute some steps are made (for ATH_1) in order for example to provide more network convergence. Some other steps (ATH_4 and ATH_5) are naturally optimized thanks to the flat UFA model.

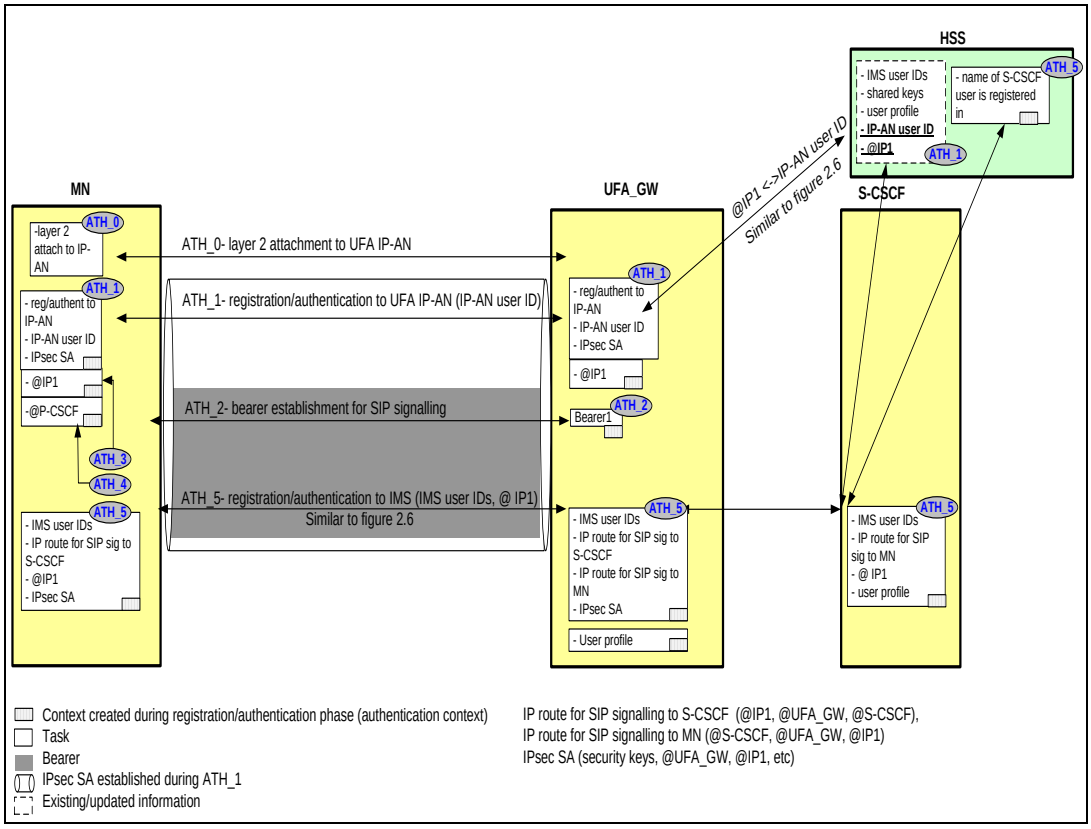



**Figure 33: UFA attachment procedure**

The detailed description of the registration/authentication steps in UFA is given hereafter:

- ATH_0: layer 2 attachment to UFA

The MN attaches to the UFA_GW at layer 2 level in order to have a physical connectivity.

- ATH_1: registration/authentication to UFA

First, the MN needs to discover the UFA_GW IP address. It uses DHCP or the stateless IPv6 configuration (the content of Router Advertisement).

Then, the MN uses EAP and the AKA authentication method, to authenticate itself. During this step, an IP address is allocated to the MN and an IPsec SA is built between the MN and the UFA_GW.

- ATH_2: bearer establishment for SIP signaling

A bearer (bearer1) is established between the MN and the UFA_GW to transport SIP signaling that will be sent/received by the MN beginning from ATH_5.

- ATH_3: IP address acquisition

The MN has already acquired its IP address in ATH_1. Therefore, this step has been already performed implicitly.

- ATH_4: P-CSCF discovery

The MN knows the P-CSCF IP address through ATH_1 step. Indeed, in ATH_1, it has discovered the UFA_GW which implements P-CSCF functions. Therefore, this step has been already performed implicitly.

- ATH_5: registration/authentication to IMS

The delay of this step is reduced compared to the classical model (LTE/EPC+IMS) in which ATH_5 requires two rounds of SIP REGISTER/SIP OK messages [3]. Moreover, during this step, an IPsec SA is built between the MN and P-CSCF to secure SIP messages.

In UFA, ATH_5 is performed with only one round of SIP REGISTER/SIP OK messages based on the following principles [8] (NASS-IMS bundled authentication):

(1) an initial binding between the network IDs (e.g. IMSI in UMTS) and the IMS user IDs, is set in the HSS network database and in the MN, (2) during ATH_5, the S-CSCF checks directly or indirectly that the user trying to register/authenticate using IMS user IDs has a network user ID compliant with the binding in the HSS. It is proposed, in UFA, that the S-CSCF performs this checking similarly to [8].

Indeed, as shown in Figure 33, during ATH_1 when the MN acquires its IP address (@IP1), the UFA_GW informs the HSS that the user having the network user ID has @IP1. The HSS deduces a mapping between the IMS user ID and @IP1, based on the already existing IMS user ID – network user ID mapping. Then, in ATH_5, when the S-CSCF receives the SIP REGISTER message natively containing the IMS user ID and @IP1, it asks the HSS to check this mapping. If the result is positive, registration/authentication to IMS is accomplished. Thus, there is no need to perform a second round of SIP REGISTER/SIP OK exchange.

The drawback of the solutions presented in [8] for the classical model, is that they don't enable the establishment of the IPsec SA between the MN and the P-CSCF. In UFA, as the P-CSCF functions are within the UFA_GW, the same IPsec SA built during ATH_1 between the MN and UFA_GW can be used to secure SIP signaling.

We propose that, during the step authentication/registration to the IMS (ATH_5), the user profile is sent from the S-CSCF to the UFA_GW to ease local decisions. At the end of the registration/authentication phase, an authentication context is built in the MN, UFA_GW, S-CSCF and HSS, as shown in Figure 33.

#### 2.6.3.1.3 Session establishment

In UFA, the service establishment procedure is applicable for SIP native and non-SIP services. Each non-SIP native service is controlled through a SIP session launched when the service is launched. It is described in SIP messages using a content type "text-plain", called SDPN (Session Description Protocol for Non-SIP native services). The SDPN is the equivalent of the SDP for SIP native services. It provides the service name and the data flows descriptors and may contain the SCTP congestion control parameters, whose use is detailed in the following.

In UFA, the service establishment procedure is guided and controlled by the network, more specifically the UFA_GW. The reduction of the number of nodes to a single node (UFA_GW), and the collocation of different layers (SIP, IP, layer 2) and different control functions in the UFA_GW has led to two advantages. Firstly, the service establishment is performed in only one step (Estb_UFA) which saves the

access delay. Secondly, the service or SCTP congestion control parameters can be adapted according to the available resources.

Step Estb_UFA: a single step for service establishment in UFA during Estb_UFA, the Source UFA_GW (UFA_GW_S) performs different tasks, as indicated in Figure 34 for SIP natives services. It is worth to mention that these tasks are almost the same for the two kinds of services and differ only regarding the use of SDP or SDPN, that contain respectively information about the service adaptation or the SCTP congestion control parameters tuning.

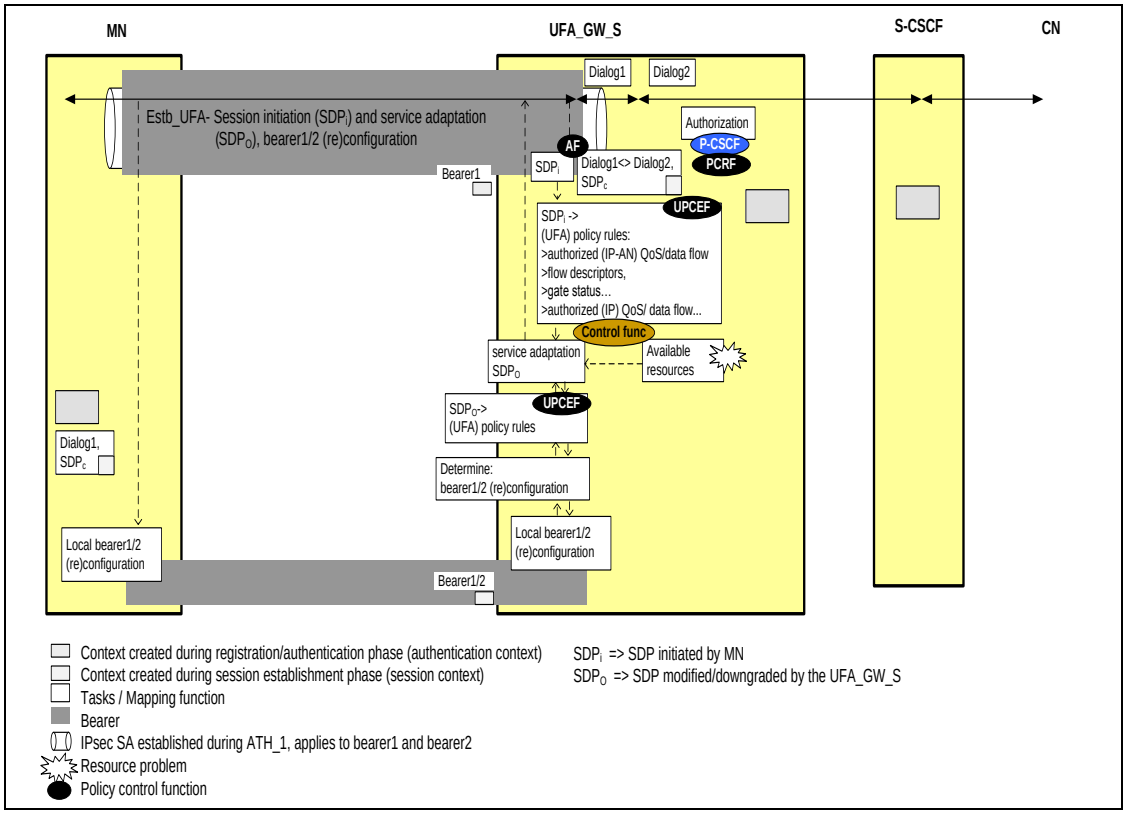



**Figure 34: UFA session establishment procedure**

**UFA_GW_S tasks are:**

- The UFA_GW_S authorizes the service based on: the initiated SDP/SDPN (SDPi/SDPNi), UFA_GW_S abilities, user profile and advanced information.
- The UFA_GW_S involves policy control functions to calculate the (UFA) policy rules, mainly the authorized QoS, corresponding to SDPi or SDPNi and:
- For SIP native services, it compares the authorized QoS to its available resources. When the latter is inferior to the former, it proposes a service adaptation by eliminating some of the applications proposed to be part of the service, or tuning their codecs. Finally, the (UFA) policy rules are updated to take into account SDPO.
- For non-SIP native services, it allocates a bandwidth considering the authorized QoS and the available resources. Then, it determines/tunes SCTP congestion control parameters values. These values enable a rapid and efficient use of the allocated bandwidth. Tuned SCTP congestion control parameters are inserted in SDPN (SDPNO, which is sent to the data sender CN. Finally, the (UFA) policy rules are updated according to SDPNO. Note that if tuning is not applied, SCTP considers initial default values (cwnd=2MTU , ssthresh=65536bytes, RTO=3s) for data transmission.
- The UFA_GW_S determines for SDPO/SDPNO the reconfiguration of bearer1 established during ATH_2, or the configuration of the new bearer (bearer2) to be established.
- The UFA_GW_S sends SDPO/SDPNO and bearer (re)configuration to the MN, which enforces them.

For SIP native services, the UFA_GW_S deduces during service establishment the SDP common to MN and CN (SDPc) independently of its resources. This SDPc is used by the UFA_GW_S during the call to upgrade the service, if resources become available. It can be also used by a target the UFA_GW to upgrade the service during mobility. For non-SIP native services, there is no common SDPN, however SDPNi is noted SDPNc is the following.

#### 2.6.3.1.4 Mobility procedures

Mobility procedure in UFA has the following characteristics:

- Mobility is controlled, decided and executed by the UFA_GWs. It takes into account different kinds of inputs.
- Mobility is based on a proactive context transfer. It is efficient as all of the contexts to be transferred are co-located in the UFA_GW. Mobility procedure includes two phases as shown in Figure 35:
    - A preparation phase initiated by the UFA_GW_S to the UFA_GW_T, aiming at predetermining:
        - The service configuration for SIP native services, or the SCTP layer configuration for non-SIP native services, the CN should have after the MN handover.
        - The all-OSI layer configuration the MN should have after its handover.
    - An execution phase aiming at providing the MN and the CN with the predetermined configurations.

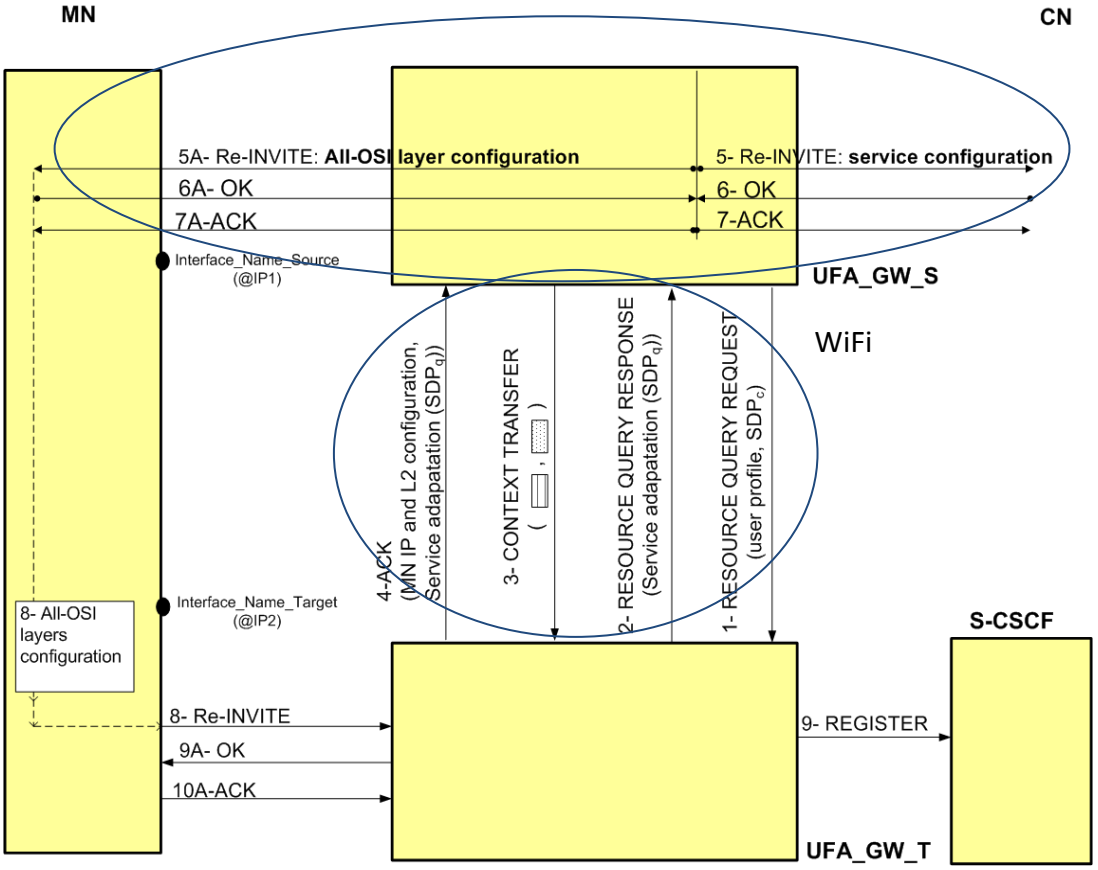



**Figure 35: UFA mobility procedure.**

Hence mobility procedure enables service adaptation for SIP native services or SCTP congestion control parameters tuning for non-SIP native services, according to the UFA_GW_T available resources.

• Mobility procedure is the same for SIP and non-SIP native applications and uses SIP protocol. For applications transported over SCTP, SIP replaces m-SCTP use and enables in addition to tune SCTP congestion control parameters.

• Mobility procedure is independent of the radio technology. It can be intra-technology or inter-technology depending on whether the UFA_GW_S and the UFA_GW_T implement the same radio access technology or not.

• Mobility is performed on a per-service basis meaning that: (1) if a given MN has many ongoing services, for each service the MN will receive a dedicated service configuration or SCTP layer configuration, (2) when handover is inter-technology, the UFA_GW_S may decide to only transfer a set of services to a UFA_GW_T.

#### 2.6.3.2 Relevance of the Technology

Thanks to the reduction of network node types in UFA, redundant context information and task necessary to handle an ongoing call are deleted. Thus, the network processing delay is reduced.

UFA flat model enables to optimize network procedures:

- In the attachment procedure, the step ATH_5 can be performed thanks to a single round of SIP REGISTER/SIP OK messages (unlike in classical model where it is done in two rounds). Moreover, during this step, the IPsec SA built for SIP signaling can be used to protect user data.
- The service establishment is performed in only one step (Estb_UFA) which saves the access delay. Secondly, the service or SCTP congestion control parameters can be adapted according to the available resources.
- Mobility is optimized and adapts to hard and soft handover cases. It is efficient as all of the contexts to be transferred are co-located in the UFA_GW. It is also radio agnostic.

#### 2.6.3.3 Expected Gains and identified issues

Gains:

-better scalability

-more optimized network procedures with lower delay

Issues:

-complexity for non-SIP based solutions

Perspectives:

-the same concepts can be used with other protocols

## 2.7 User Access Authentication and Authorization

### 2.7.1 Lightweight HIP-based Access Authorization

#### 2.7.1.1 Background and Motivation

In the future mobile networks, operators are faced with mainly three challenges in security: (1) how to enforce a consistent security policy to every element in the network given the security measures are specific and limited to RAN technologies, as are their capabilities and achieved level of security different from each other, (2) how to ensure adequate strength of confidentiality and integrity protection over every RAN access to the mobile network, and (3) how to identify users and hosts in a consistent manner given that each RAN access uses different credentials and identities specific to the respective technology.

The future mobile networks simultaneously using disparate and heterogeneous RAN accesses clearly require homogenization in regards to security mechanisms. One approach to tackle the above mentioned problem is to implement the security mechanisms independently from access technology by using a set of overlaid technologies. This approach pushes the security logic to the higher network layers from the link layer. As a consequence, the security mechanisms are implemented by software as part of operating system kernels and/or as separate applications.

This kind of approach would allow designing consistent security policies for mobile networks over disparate underlying RAN technologies. Naturally, this implies using the IP protocol as the integrating technology to carry all security related signaling over with.

#### 2.7.1.2 Host Identity Protocol (HIP)-based Authentication and Key Agreement

In this section, we describe a lightweight Host Identity Protocol (HIP)-based Authentication and Key Agreement (HIP-AKA), a novel approach to address the above mentioned ailments with the security in mobile networks. The HIP-AKA scheme serves the same role as the IKEv2 EAP-AKA method in the non-3GPP non-trusted access. It is responsible for network layer user access authentication between the UE (Initiator) and the ePDG (Responder). As the end-result of the HIP-AKA-based authentication, a tunnel mode IPSec SA pair is also established between the Initiator and the Responder. Detailed description of the HIP-DEX scheme is described in [5].

In HIP-AKA, UE is represented by Host Identity (HI). The user of the UE, in turn, is represented by International Mobile Subscriber Identity (IMSI) allocated to the user and stored on her USIM card by the operator. While HI is a self-certifying identity due to its cryptographic properties, IMSI, a 15-digit ASCII string, must be verified by proofing the possession of a secret key shared between the user and operator and the operator. In HIP-AKA, the standard 3GPP AKA scheme [6] embedded inside the HIP protocol is used to achieve this. The signaling process of HIP-DEX is illustrated in Figure 36.

HIP-AKA begins with the UE initiating an I1 packet towards the gateway. The IP address and the target Host Identity Tag (HIT) of the gateway are assumed to be dynamically learned from the bootstrapping information received during the attachment to the access network through, e.g. a query to a HIP-capable DHCP server. Alternatively, the I1 packet can be sent as an opportunistic broadcast packet without knowing the target HIT or IP address in advance. Upon receipt of the I1 packet, the gateway selects a pre-computed R1 packet and attaches it with a random nonce for the puzzle challenge.

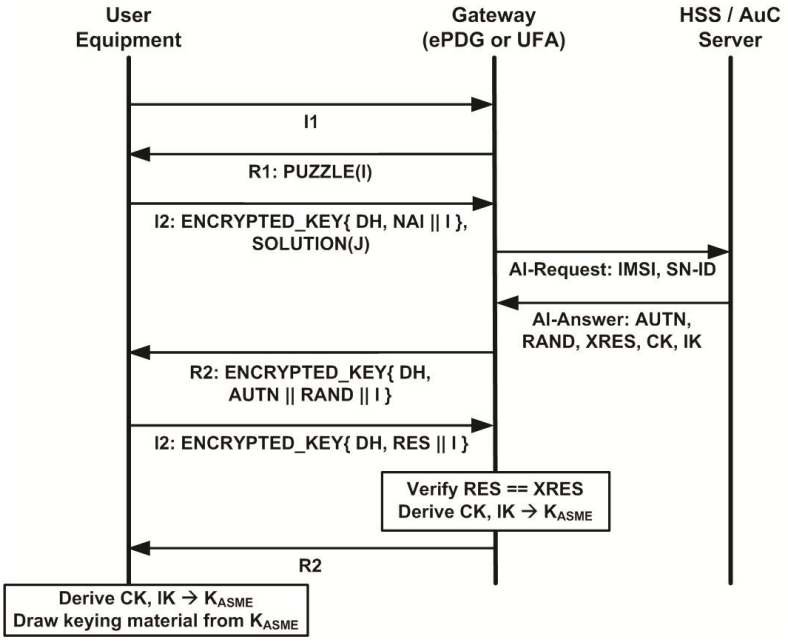



**Figure 36: Authentication process of HIP-AKA.**

Upon receiving the R1 packet, the UE solves the puzzle and adds corresponding solution to an I2 packet along with the subscriber identity. The identity is represented by a Network Access Identifier (NAI), an ASCII string of form *(IMSI)@realm*, where the realm part is the name of the serving network the UE has received locally during the bootstrapping process in the access network or statically set in the device.

During the HIP-AKA authentication process, the gateway communicates directly with an HSS server located in the user's home network. When the gateway receives correct puzzle solution and the IMSI string from the UE in I2 packet, it verifies that the received IMSI (and possible realm part in NAI) is correct and requests an AV for the user from the HSS. HSS constructs a fresh AV including ciphering and integrity keys for the respective user. The gateway forwards the RAND and AUTN parameters from the AV to the UE inside R2 packet.

UE calculates its own version of the AUTN parameter and compares it with the one received from the gateway. If they are consistent, the UE has successfully authenticated the network and can proceed with the HIP-AKA. The UE generates a response RES using the shared secret and RAND, and transmits it encrypted to the gateway inside a second I2 packet. Upon receipt of the second I2, the gateway verifies the response by comparing it to the XRES parameter received earlier from the HSS. If they match, the gateway has authenticated the user, as well as the host, and finalizes the authentication process with a R2 packet to the UE.

#### 2.7.1.3 Deployment of HIP-base Access Authorization

The HIP-AKA authentication method is intended to be used by low-end devices that perform e.g. M2M communication via mobile network. Hence, it is designed to induce less signaling and computational overhead than the IKEv2 EAP-AKA. It also has slightly different security features from that of IKEv2 EAP-AKA. From the deployment point of view, both methods require support on the UE/MR and the ePDG.

In long-term, in flat topology several functional entities, such as the eNodeB, MME, ePDG, P-CSCF will probably be collocated. Hence, all above mentioned authentication procedures could be realized using one unique IP layer access authorization. In that case, the gateway could be the authenticator and it might provide AAA server or proxy functionality as well. HIP-AKA could serve as a solution for low-end devices for unique user access authorization.

However, we must note that when link layer access authorization is missing, then attackers are able to exploit L2 control messages for attacks and might be able to attach to the access point. This is valid for the current non-3GPP non-trusted access as well, if the operator of the non-3GPP access does not protect its access points. In case of the 3GPP-access and trusted non-3GPP access L2 protection is obligatory in current standards.

It depends on the operator's trust model whether a uniform L3 access authorization suits its needs or is better to defend against L2 attacks and deploy EAP-AKA authentication separately for each RAN technology.

## 2.8 Support for user cooperation

### 2.8.1 Mobile Relaying in Heterogeneous Networks

#### 2.8.1.1 Description of the Technology

In recent years, the use of heterogeneous network (HetNet) deployments is investigated as an efficient way to improve system performance by increasing network efficiency in the 4G research community. The fourth generation technologies call for very high data rates (such as 100 Mbps for mobile and 1 Gbps for fixed environments) with a robust relay and backhaul architecture.

In HetNet deployments, the traditional deployment of base stations is overlaid with devices having heterogeneous characteristics deployed on coverage holes or capacity-demanding hotspots. This gives important advantages such as ease of deployment and reduced deployment cost compared to deploying regular Base Stations (BS). Relaying, femtocells, pico-cells and WiFi hotspots are some of the examples of HetNet deployments.

Using mobile relaying in combination with one of other heterogeneous devices such as Wi-Fi networks can further increase efficiency due to additional infrastructures and can extend coverage in specific locations and hotspots regions when the signal power of edge users are low.

For the cell edge users, where the signal-to interference and noise ratio (SINR) are typically low, joint mobile relay with Wi-Fi selection capability increases the opportunities for higher data rates for the end users. The main objective is to provide Quality-of-Service (QoS) support for the edge users with low SINR using mobile relays or Wi-Fi hotspots and to build a strong interface for smooth communication between radio access network, components, Wi-Fi controllers and core network components. We mainly look for schemes for some of the important issues in relay and Wi-Fi assisted heterogeneous networks for LTE-Advanced technologies like relay and WiFi deployment planning, relay and Wi-Fi node selection criteria based on channel conditions and other network parameters, resource allocation techniques between theses 3GPP (LTE-Advanced) and non-3GPP (Wi-Fi hotspot) access technologies.

The proposed algorithm will consist of two phases. In the first phase, the resource allocation to all UEs will be done by eNodeBs, based on frequency and time planning. This way the users will be able communicate on assigned channels with eNodeB, relay node or Wi-Fi hotspots. In the second phase, the

eNodeB will try to pair the relay nodes (RNs) or Wi-Fi hotspots with their corresponding UEs. The detailed analysis of the each phase is explained below.

**Phase 1: Resource Allocation (RA) to UEs.**

In LTE, each sub-band has 12 subcarriers and the representative value of the sub-band is chosen by averaging these subcarriers Signal-to-Noise Ratio (SNR).

RA includes only sub-band allocation to the users and is based on maximization on sum data rate with giving more opportunity to the users far from base station (The classical sum data rate algorithm starts to schedule the user which has the maximum sub-band SNR or CQI). The algorithm sorts the users according to their distance from base station and then starts with the farthest user to schedule. The criterion is that the best sub-band that has the highest CQI is scheduled to that user. The algorithm ends after scheduling all users based on the same criterion. If there are more users than the number of the sub-bands, the classical sum data rate algorithm is performed and the relay selection does not work since there are no remaining resources for relays.

**Phase 2: Pairing Scheme for the Selection of Relay.**

Relay selection is performed for the outer region users for empty sub-bands. These users can choose relays from the middle or inner zone in an area with radius (3*R/2). The relay is selected based on the maximum CQI value of the total link BS-RS-UE (Also, different relay selection algorithms such as path loss (PL) based, distance based etc. can be used). For each relay candidates, best empty sub-bands are selected according to their CQI between BS-RS and RS-UE and then the sub-band which has the best CQI value is chosen.

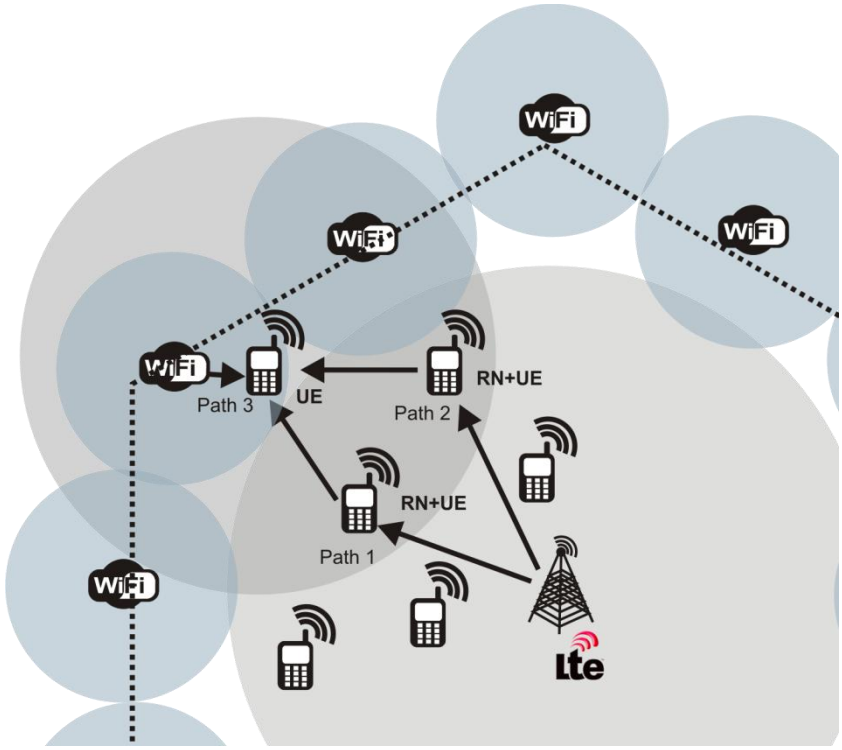



**Figure 37: MoRe-Het architecture and seamless handover between macro network and Wi-Fi infrastructure**

**MoRe-Het in LTE-Advanced E-UTRAN Architecture:**

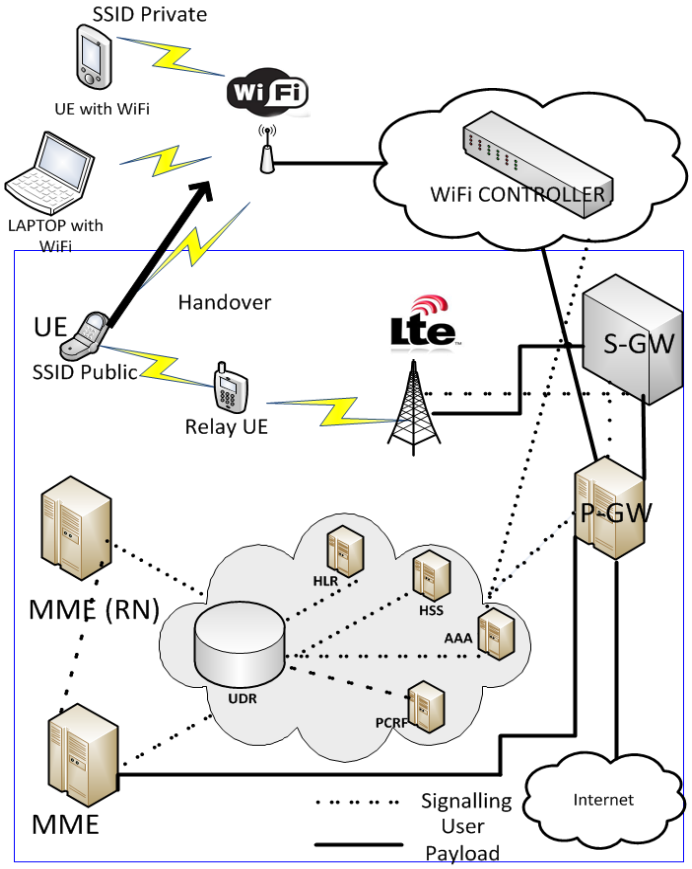



**Figure 38: MoRe-Het architecture and seamless handover between macro network and Wi-Fi infrastructure**

In the above figure, Wi-Fi controller is inserted into the core network for the proposed MoRe-Het architecture. The Wi-Fi controller is sending control signals to AAA (Authentication, Authorization, and Accounting) server and is direct communication with P-GW. The MME (RN) is responsible for controlling mobile relaying strategy. The UDRs (Usage Detail Records) consist of HLR, PCRG, HSS and AAA servers.

### 2.8.1.2 Relevance of the Technology

Mobile Relaying is a major step in user cooperation proposed to be used in next generation networks. The technology supports basic user cooperation by enabling the forwarding of other users data to increase throughput. With the traditional cellular architecture, increasing the capacity along with the coverage would require the deployment of a large number of Base Stations (BS), which turns out to be a cost-wise inefficient solution to service providers. However, introducing Relay Stations (RS) in each cell can alleviate this problem since the RS can forward high data rates in remote areas of the cell while keeping a low cost of infrastructure.

### 2.8.1.3 Expected Gains and identified issues

Our algorithm will primarily investigate edge-user throughput improvements over possible deployment of relay nodes and its impact on the core network performance. The other KPI parameters like delay, signaling overhead, overall UE power consumption etc. will be investigated.

The edge user throughput is expected to increase and initial simulation results prove a throughput increase by a factor of 2 at the cell edge. The signaling overhead of relay deployment is not considered as significant compared to data traffic in the backhaul or core network. It is estimated that core data traffic requirements will increase to 130 Gbps (Current core bandwidth requirements are less than 40 Gbps) in Europe. Overall UE power consumption is expected to decrease due to cooperation and lower power used by the cell edge users.

## 2.9 Support of moving networks

### 2.9.1 Support of moving networks in Proxy Mobile IPv6

Proxy Mobile IPv6 is a protocol that was designed initially with the goal of supporting Mobile Hosts (MH) like end-user terminals, handsets, smart phones. The goal was to allow such an MH to dynamically change its point of attachment by performing a *hand-over* between different access points. Upon attachment to a new access point, a new IPv6 address would be attributed to the MH; changing the address of the terminal would pose a significant threat to the good behavior of ongoing applications – hence a mechanism was needed that would allow MH handovers without a change in the IP address. The protocol Proxy Mobile IPv6 offers this feature, by dynamically changing the network routing (with tunnels) corresponding to one particular address, which moves itself together with MH movement.

On another hand, the protocol PMIPv6 was not designed to support groups of hosts moving together as a whole. This is referred as *moving networks*. Although PMIPv6 assigns an entire prefix to the MH (i.e. the leftmost common 64bits of an address – the HNP "Home Network Prefix") this prefix cannot be used by nodes in the moving network to attribute an address for themselves. This HNP can only be used by MH to self-configure one single address.

This has negative implications in the case of moving networks. If we consider the typical topology of a moving network (several LFNs and a MR moving together), IP applications between LFN and an arbitrary CN in the Internet are not possible; first, the LFNs do not have globally routable addresses, because only one address is delivered by PMIPv6 to MR's egress interface; second, even if a LFN had a statically configured globally routable IP address, this is not reachable: a CN sending a packet to that address would be dropped at LMA, because the routing path is not set up between CN, LMA, MAG, MR and LFN. There may exist trivial solutions to address this problem but which have several inconvenient; for example, if we consider IPv4, a NAT and DHCP may be implemented in the MR; this would offer unidirectional access from LFNs to arbitrary CNs; however, this would not offer reverse reachability from CN to LFN; it is also worth noting that the NAT concept is proper to IPv4 and does not have counterpart in the IPv6 addressing architecture.

In the following, we present methods to affect a Mobile Network Prefix "MNP" to a Mobile Router, which could thus perform handovers within networking domain where the PMIPv6 protocol is used. This would allow the support of moving networks – each moving network is under the responsibility of a Mobile Router, which moves together with all other computers within.

The goal is to allow bidirectional communication between a Local Fixed Node (in the moving network) and a Correspondent Node (situated arbitrarily somewhere in the Internet). First, a mechanism of "prefix division" is presented, whereby the Home Network Prefix typically assigned by PMIPv6 to a MH is used by MR to form Mobile Network sub-Prefix(es); they are used by LFNs within the moving network to form addresses; this avoids changes in the PMIPv6 protocol specification. A second mechanism proposes enhancements to the use of the DHCPv6 Prefix Delegation protocol entities informing the PMIPv6 entities about the allocated MNP; this is achieved by equaling MNID and DUID.

#### 2.9.1.1 Description of the Technology

The term Mobile Router has several meanings. One of the agreed meanings at IETF, documented in terminology RFCs, is that of an entity implementing the Mobile IPv6 protocol with NEMOv6 extensions, and accommodating changes in its Care-of Address, maintaining a stable Home Address with the help of a Home Agent, and in charge of LFNs in a moving network whose addresses do not change. Another meaning is that of a router which moves around and does not necessarily change its IP address. In the context of this document we consider this latter meaning. We ignore whether or not the MR runs Mobile IPv6.

The work presented in this document is developed in the context of Proxy Mobile IPv6 [20]. With respect to prefix division, similar methods have been alluded to in the context of DHCPv6 Prefix Delegation by [5] (with a slide presentation in the DHC WG at IETF77) and of OSPFv3 by draft-arkko-homenet-prefix-assignment-01. Mechanisms for supporting Mobile Routers with PMIPv6 and DHCPv6 are presented in [21] and preceding individual drafts.

The methods presented in this document are different than most if not all existing documented methods to accommodate moving networks with PMIPv6. In particular, the HNP Division offers several MNPs for use by LFNs, does not modify PMIPv6 (contrary to all other methods PMIP-NEMO, which do), does not require the use of DHCPv6-PD but has an inconvenient in that it may not accommodate Ethernet LFNs with SLAAC (State-Less Address Auto-Configuration). Alternatively, the DHCPv6-PD and PMIPv6 enhancements offer MNPs (which are potentially completely different than HNP, not derived from it), may use Ethernet LFNs with SLAAC, and modify MAG, LMA, DHCP Relay and potentially DHCP Server.

Moreover, the PMIPv6 and DHCPv6 enhancements presented in this document rely on the use of MNID being equal to the DUID, a feature absent from existing proposals. Also, with this mechanism the entity performing the allocation of an MNP is the DHCPv6 Server (and not the LMA).

**HNP Division**

The mechanism "HNP Division" divides the Home Network Prefix into two or more Mobile Network Prefixes (MNPs). It is assumed that in a domain running PMIPv6 the LMA assigns a Home Network Prefix (HNP) to the Mobile Host. If we consider this Mobile Host to be a Mobile Router, in charge of a set of Local Fixed Nodes (LFNs) in a moving network, it is necessary to use a Mobile Network Prefix (MNP) within the moving network. Simply using HNP to form addresses for LFNs, without modifying MR behaviour with respect to its routing table, is not sufficient.

The topology illustrated in the next figure depicts a domain where PMIPv6 is run, and a Mobile Router in charge of a set of LFNs forming a moving network.

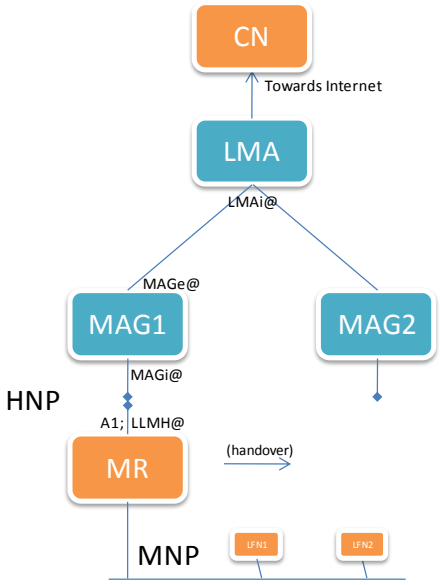



**Figure 38: Moving Network and handover within a PMIPv6 domain**

For a HNP with prefix length 64, two or more MNPs are generated, each having a prefix length longer than 64. For brevity of graphs, and without forgetting that IPv6 addresses are actually 128bit long, we present a detailed division example for a fictitious addressing system whose "IP" addresses are of a maximum length of 5 bits (instead of 128 bits of IPv6).

In this example, the HNP/2 11000 is assigned by LMA to MR. The MR divides this into MNP1 1101/4 and MNP2 111/3, and an address A1 11001/5. The MNP1 and MNP2 are used to help LFNs within the moving network to configure full /5 addresses. This may be achieved either with DHCPv6 (MR or a DHCPv6 Server send these addresses) or with stateless address auto-configuration (MR or a Router send Router Advertisements containing MNP1 and/or MNP2).

In many PMIPv6 implementations supporting MHs, the MAG contains a routing table entry with respect to the allocated HNP. Depending on the nature of the link between MAG and MR, this entry has two different forms: [HNP, vif, *] in case of point-to-point links (typically used in some cellular systems) and [HNP, eth, *] (typically used in WiFi hotspot shared links). The vif is a virtual interface, e.g. "ppp0", whereas eth is a real interface, e.g. "eth0".

In the case of point-to-point links, it is not necessary to add any additional behaviour for MR to work (LFN to be reachable from CN). It is sufficient for MR to perform HNP division as described above.

On the contrary, in the case of shared links, it is necessary to perform an operation of Neighbor Discovery proxying on the Mobile Router. The *shared* links are named, for example, WiFi or Ethernet; future cellular networks (LTE) may use some forms of links between terminal and base station that have features of shared links (e.g. CDECM driver type in Linux for USB LTE). When MAG receives a packet from CN addressed to LFN, it would solicit the MAC address of LFN on the MAG-MR link (even though LFN is not present on that link). For this reason, the MR must pretend it owns the IP address of LFN and respond to that solicitation with its own MAC address.

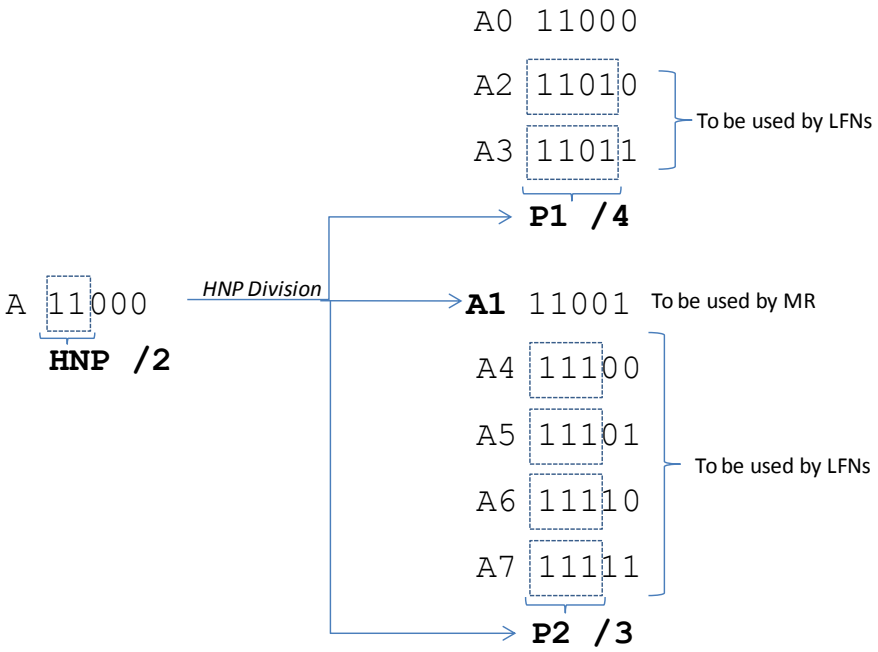



**Figure 40: Example of HNP Division for a fictitious 5-bit address**

The HNP division mechanism requires that the MNP be part of the HNP (e.g. MNP must have the leftmost n bits the same as the prefix length of HNP), and its length be longer. In case of an HNP/64 and the use of Ethernet for LFNs, only the DHCPv6 protocol can be used by LFNs, and not SLAAC, because stateless address auto-configuration is not possible for MNPs whose prefix length is longer than 64, the Interface ID being of length precisely 64 for Ethernet.

**Enhancements to DHCPv6-PD and PMIPv6**

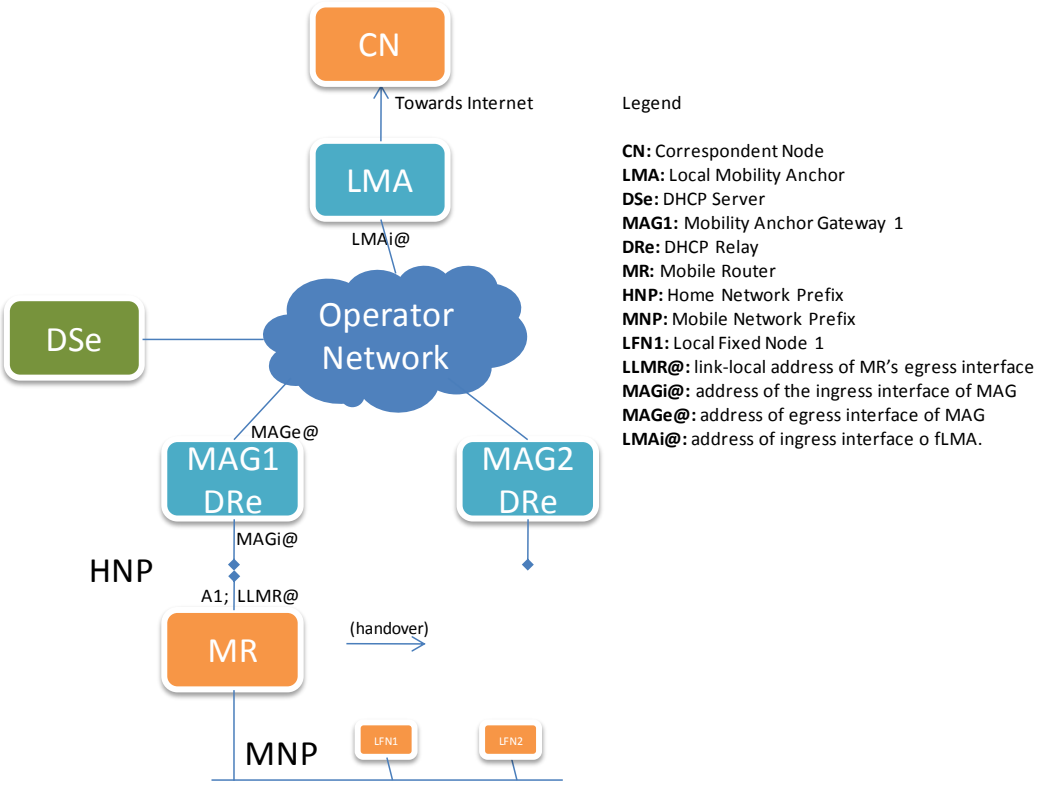



**Figure 39: Topology of Network Mobility with DHCPv6-PD and PMIPv6 Enhancements**

A second mechanism, alternative to HNP Division, considers the use of MNP completely different than HNP. With HNP Division, the HNP and MNP necessarily have a common set of leftmost leading bits (2 in the previous example). But with this method, HNP and MNP may differ at the leftmost bit. This has an immediate advantageous consequence: it allows the use of SLAAC with Ethernet LFNs even when the HNP is of length 64. The inconvenient is that the PMIPv6 protocol implementation must be modified; this mechanism involves also the use of the DHCPv6 Prefix Delegation protocol, which may be considered as an additional burden (DHCP software must be installed and configured on a new entity which is the DHCP Server, etc. For this mechanism, we consider the following PMIP topology augmented with DHCP entities:

The DSe entity is a DHCPv6 Server. Each MAG also runs a DRe which is a DHCPv6 Relay. It is necessary to modify the DRe, LMA and MAG behaviour. Depending on deployment, it may be preferable to modify or to otherwise avoid all modifications the DHCPv6 Server. In case it is not acceptable to modify the DSe we propose the protocol depicted in the following figure:

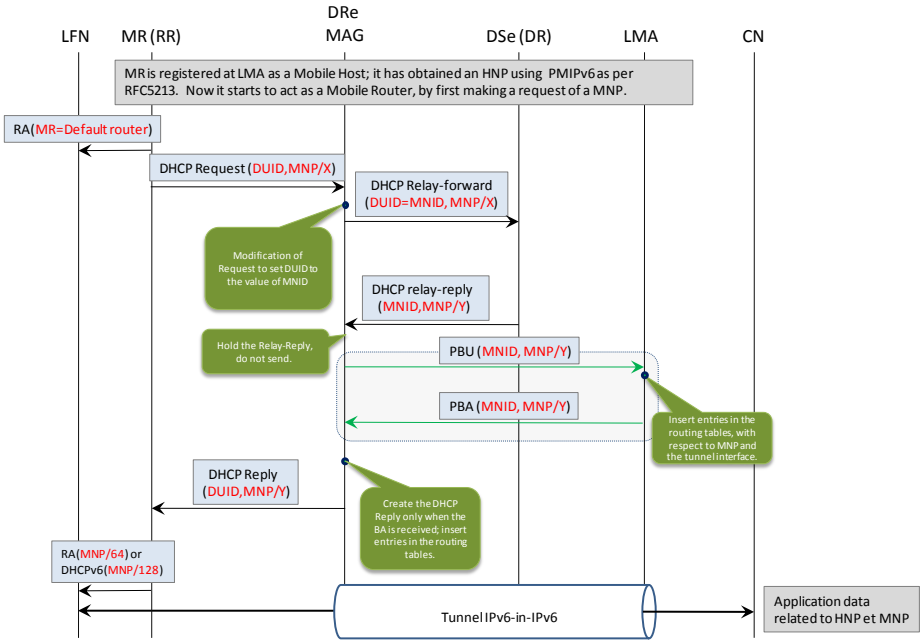



**Figure 40: Message Exchange Diagram for PMIPv6 NEMO support with DHCPv6-PD (avoid modifications on DHCPv6 Server)**

Initially, the Mobile Router had acted as a simple Mobile Host. It has registered at LMA and obtained an HNP as per [20], with a simple exchange PBU/PBAck.

Following this initial operation, the MR needs a prefix to advertise towards its Local Fixed Nodes. It requests this prefix (MNP) by using DHCP Request message – the arrow from MR to MAG. DHCPv6 Request is a standard message which is part of the existing DHCPv6 Prefix Delegation procedure. This message contains a field named "DUID" (DHCP Unique Identifier) which uniquely identifies this Mobile Router. In order to ensure interoperability with PMIPv6, it is necessary to equal the value of DUID with the a specific PMIPv6 identifier which has the same role – identify the mobile node.

This PMIPv6 identifier is named "MNID" (Mobile Node Identifier) and is already present in the PMIPv6 implementations. Thus, the DUID field of the relayed message (DHCP Relay-forward) is set to the value of MNID. At the reception of a Relay-forward, the DHCP Server allocates a new prefix MNP for the respective MNID (==DUID). It subsequently sends the MNP in a message Relay-reply addressed to the DRe (MAG). The modified DHCP Relay implementation on MAG (DRe) will receive this message and *hold* it, instead of transmitting it to the Mobile Router. This is enhanced behavior of DHCP.

Before transmitting this message to the MR, the MAG needs to inform the LMA about the reachability of this prefix MNP. It sends a message PBU (Proxy Binding Update) containing the respective MNP as well as the MNID – the identifier of the mobile router. When LMA receives this PBU, it extracts the MNID and identifies the existing tunnel interface corresponding to this MNID; this tunnel interface also corresponds to the HNP allocated initially for the MR's egress interface. The LMA subsequently inserts an entry in its routing table which holds the MNP and the tunnel interface.

In this way, routing is set up at LMA about this MNP. Then, LMA sends the PBAck (Proxy Binding Acknowledgement) to the MAG. Only when the PBAck has been received at the MAG, this latter will *release* the DHCP Relay-reply. This message is then transformed by MAG into a DHCP Reply (this transformation is standard DHCP behavior). The DHCP Reply is sent to the Mobile Router. Upon reception of this message the Mobile Router extracts the MNP and the respective prefix length from the DHCP Reply message. This prefix is then advertised to the LFNs in the moving network, preferably by using Stateless Address Auto-Configuration.

At the end of this entire message exchange, packets may be exchanged bi-directionally between a Local Fixed Node and an arbitrary Correspondent Node in the Internet. It is possible that LFN initiates the communication, as well as that the CN initiates the communication. All applications using IP addresses may execute normally between those entities.

# 3. Evaluation of the Proposed Technologies for Mobility Management

A key aspect of the 3GPP system architecture evolution is the specification of an evolved packet core that supports multiple access networks. The EPC enables operators to deploy and operate one common packet core network for 3GPP radio accesses (E-UTRAN, UTRAN, and GERAN), as well as other wireless and wire line access networks (e.g., eHRPD, WLAN, WIMAX, and DSL/Cable), providing the operator with a common set of services and capabilities across the networks. This section contained the WP2 Proposed Architectural Extensions for the technologies belong to each category.

## 3.1 Decision and handover preparation methods for efficient load balancing

In the following subsections, IEEE 802.21, ANDSF and different decision methods are validated. Validations should point out their efficiency in improved support for load balancing and inter-PGW handovers in the EPC network.

### 3.1.1 Performance evaluation of IEEE 802.21 and ANDSF based handover preparation for improving network assistance for multiple network access capability

#### 3.1.1.1 Covered challenges

Network introspection: information about the radio accesses is made publicly available, allowing improvements on the handover management by reducing the number of radio accesses to be successfully scanned, and receive an approval from the AAA process.

#### 3.1.1.2 Key Performance Indicators

- KPI 1.1 Throughput gain in 3GPP access and backhaul
- KPI 1.4 Efficient load distribution in the backhaul and in the core
- KPI 2.1 Offload gain due to the usage of multi-access capabilities
- KPI 2.3 Service interruption delay due to handover
- KPI 3.1 E-E delay between UE and content

#### 3.1.1.3 Applicability and Dependencies to Other Technologies

Impacts are related to the handover process in both UE and radio accesses, and additional host is needed to manage the information database that may be duplicated in more local locations, but this will not really improved the process as query to the information database is not time critical. On UE the main change is done on the connection manager part that will take into account the information gather by the IEEE 802.21 processes.

#### 3.1.1.4 Main Validation Results

There are five steps in this technology solution.

- The first step is the initialization of the communication between the client and the servers (the POA for the radio accesses and POS for the information server).

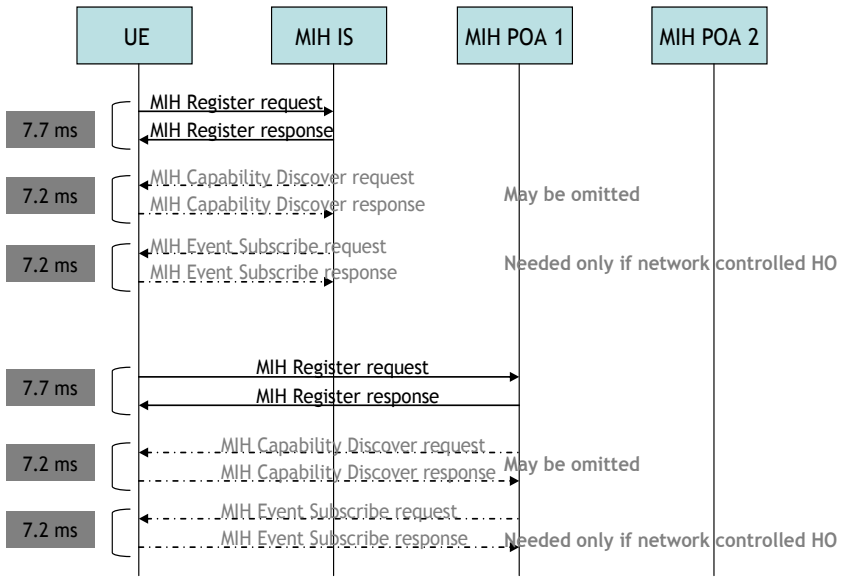



**Figure 41: Initial set-up**

Initialization step is less than 30ms per network element.

- The second one is to gather the information and should be done before the HO preparation process.

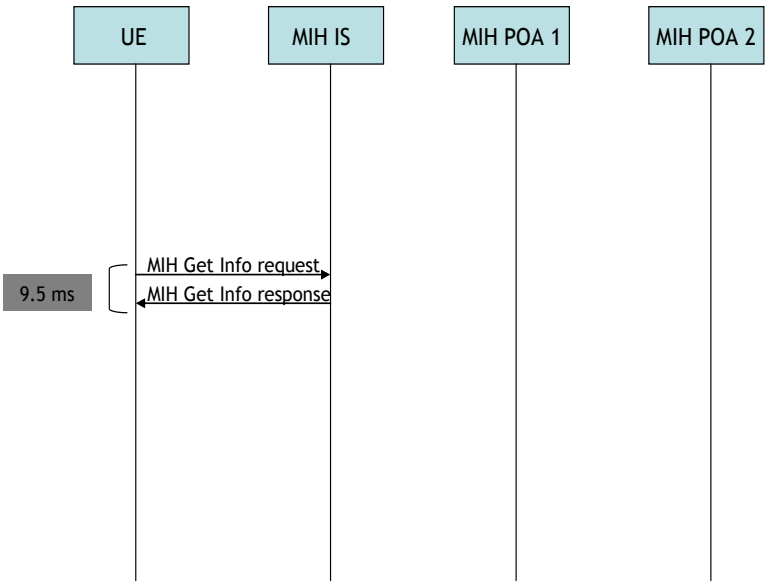



**Figure 42: HO preparation**

The duration of this step is dependent of the length of the messages. In our case, the query is about the information on the radio accesses in a defined area. If it is a large area, there will be a lot of data that will be put in the response but this step will have to be done less frequently. It is a balance between the size of the data (in the message and stored on the mobile) and the number of requests to be done when the mobile may exit the area defined in the previous request.'

Minimal duration is about 10ms.

- The third part is used to check if the resources on the potential target are really available (like in the Call Admission Control in the horizontal handover.)

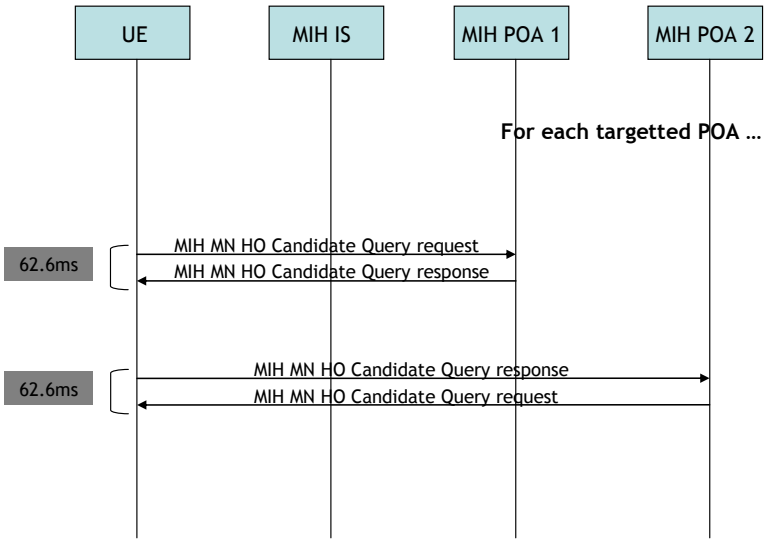



**Figure 43 : Potential target availability**

This step's duration depends of the number of available radio accesses:
Duration = Nb access x 70ms.

- Then the target radio access is chosen and the HO process is confirmed.

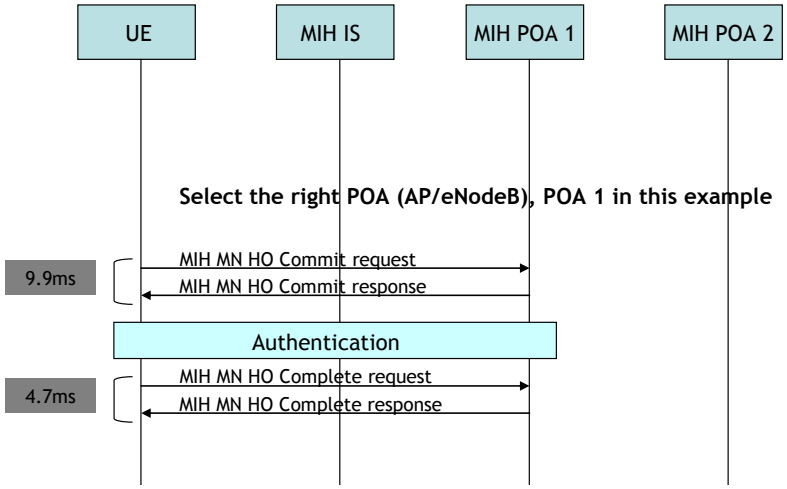



**Figure 44: Target radio access**

The duration is around 15ms which is negligible compared to the duration of the authentication process.
So the added delay in the HO process is around: 15ms + 70ms x nb targeted POA which can be easily taken into account by changing the threshold values (SINR, PER …) used to trigger the HO.

- The last one is the closing of the connection with the servers when the service is no longer needed.

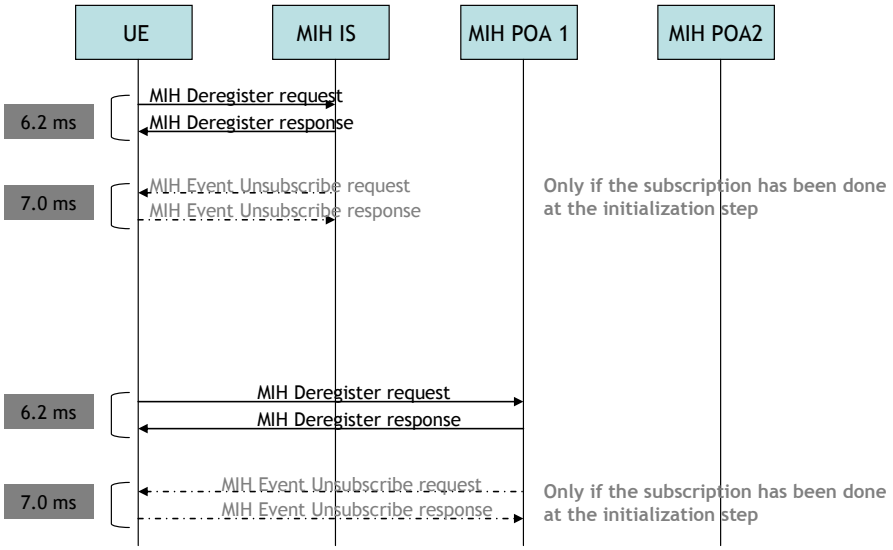



**Figure 45: Closing connection**

The duration for each network element MIH service ending is around 14ms. This step has no impact on HO process.

## 3.2 Offloading

This validation topic demonstrates the offloading capabilities of Wi-Fi technology.

### 3.2.1 Improving UE's multiple network access capability and load balancing through Wi-Fi offloading

#### 3.2.1.1 Covered challenges

Operator managed Wi-Fi is a technology where an operator can provide personal connectivity services for devices in residential networks, hot spots etc. e.g. firewall, secure authentication and content filtering. A number of challenges are covered like relative capacity increase, offload gain, network throughput offloaded, and operator service continuity, better indoor coverage for Wi-Fi enabled devices provided by mobile operators, and reduced complexity with cell planning.

#### 3.2.1.2 Key Performance Indicators

- KPI 1.4: Efficient load distribution (in backhaul and in the core)
- KPI 2.1: Offload gain due to the usage of multi-access capabilities
- KPI 2.4: Service interruption delay due to handover
- KPI 2.3: Service Interruption and Handover delay
- KPI 3.3: Offload gains for core network elements

#### 3.2.1.3 Applicability and Dependencies to Other Technologies

In order to implement this technology, modifications have to be done to the Wi-Fi access point including DHCP proxy, local services proxy, tunnel set up and maintenance and multiple SSID capability and add to the BNG RADIUS proxy, S2a functionality and router configuration.

#### 3.2.1.4 Main Validation Results

It was demonstrated that the traffic flow is redirected via the access point to either the mobile network or directly to the Internet as a local breakout depending on which SSID is selected.

## 3.3 Dynamic Mobility Anchoring

The following technologies try to achieve optimal mobility management related signaling and path allocation. This section covers path and gateway selection questions.

### 3.3.1 DMA principles applied to GTP based mobility

#### 3.3.1.1 Covered challenges

Distributed GWs contribute to the challenge of providing sufficient user experience in highly loaded networks by reducing traffic path length and number of hops in the path. An optimized selection of the gateways also provides more efficient network resource utilization like less transport resources or more equally loaded gateways. For OpenFlow based EPC the impact to KPIs have not yet been investigated.

#### 3.3.1.2 Key Performance Indicators

- KPI 1.1: throughput gain in 3GPP access and backhaul
- KPI 3.2 E-E delay between UE and content or path lengths in terms of transport hops / IP hops
- KPI 3.3 analyze offload gains for core network equipments: e.g., number of active user contexts per network equipment
- New KPI: E2E QoS provisioning, load distribution in core, no impact to UE implementation

#### 3.3.1.3 Applicability and Dependencies to Other Technologies

The proposed improvements are fully compatible with the 3GPP architecture. So they can coexist with all technologies that are compatible and applicable for the 3GPP EPS/EPC.

#### 3.3.1.4 Main Validation Results

To evaluate the need for routing optimization in a distributed GW network topology calculations have been carried out based on a traffic and network model. This way, mobility related performance estimation on the effects of distribution of GWs was carried out.

The model shows that for the 3GPP GW architecture a fast moving UE would pass 3 to 8 GWs (depending on the number of cells per GW). This leads to the following conclusions:

- Only for fast moving terminals the problem of GW changes/routing optimization need to be considered (e.g. for transport systems). For these highly mobile scenarios it is worth investigating how dynamic mobility anchoring principles can be applied to the EPC.

## 3.4 Terminal-based mobility management

This section validates terminal-based mobility protocols which do not need infrastructure in the network and are anchorless. For the initial reachability of UEs, some support from the infrastructure is required. Optimized routing and flow mobility is provided by them for the supported protocols.

### 3.4.1 Functional and performance validation of NMIP, SCTP and MPTCP

#### 3.4.1.1 Covered challenges

Mobility, radio interface change and handover generate problems in packet delivery. Source or destination addresses may change, and break the data connection. Several proposals have been presented to solve this issue; here we focus on finding a solution at the transport layer. The comparison of end to end transport protocols will be helpful to give indications about the respective performance of each protocol that have their own way to solve this issue. A special care has been taken on how the seamless HO can be obtained and how the multihoming functionalities may be used.

- NMIP is a TCP extension that allows IP address change of one of its end point without breaking the connection.
- SCTP was intended to be used as a solution for fail over link, but it may also be used to solve the mobility issue by providing several available paths even if only one is used at a time. Maintaining session continuity and being able to survive long network disconnections is one of the main challenges covered in this project.

- MPTCP is also a TCP extension but it manages multipath between the two end-points and thus allowing load balancing among all the available paths.

#### 3.4.1.2 Key Performance Indicators

- KPI 1.3: reliability (response time to link failures, bootstrap time)
- KPI 1.4: fair load distribution
- KPI 2.1 Offload gain due to the usage of multi-access capabilities
- KPI 2.2 capacity aggregation
- KPI 2.3 Handover delay
- KPI 2.4 Service interruption delay due to handover
- KPI 2.5 handover related signaling load on the network
- KPI 3.2 E-E delay between UE and content or path lengths in terms of transport hops / IP hops

#### 3.4.1.3 Applicability and Dependencies to Other Technologies

Each of these three protocols is end to end protocol, meaning that only the two end-points need to implement the protocol. Otherwise no other network elements are impacted. No additional services are needed. For NMIP an additional service can be provided (by the operator) in order to optimize the interface selection at the attachment time.

#### 3.4.1.4 Main Validation Results

**SCTP:**

With the session layer extension to SCTP protocol, we plan to demonstrate session 'suspend' and 'resume' functionality. It enables applications to request suspension and resumption of communication at any given time, for surviving long disconnection periods, and for re-establishing the previous communication upon reconnection. The evaluation is performed based on the interaction of the session layer and a file transfer application under various mobility scenarios. The evaluation environment to test the session layer is as shown below:

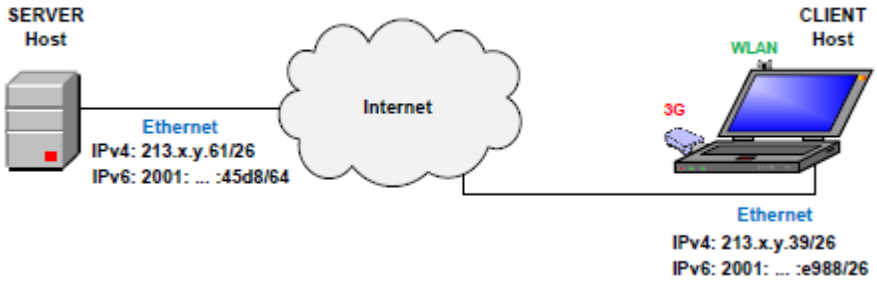



**Figure 46: Evaluation environment for testing session layer**

The server host has a single network interface with both IPv4 and IPv6 addresses configured. The client host has multiple network interfaces configured, such as Ethernet interface (with both IPv4 and IPv6 addresses configured), a wireless LAN interface, and a 3G interface (using a 3G USB modem). The client host is connected only through one network interface since the purpose of the test scenarios is to show that the session layer survives from long disconnection periods and re-establishes communication upon reconnection to the same or different IP address.

The file transfer application implemented to test the session layer is a graphical client-server application where the client requests the download of a specific file from the server. Initially, both the server and the client establish network communication and initiate a session through their Ethernet interface. After the session establishment, the client starts downloading the particular file. At this stage, either the client or the server application may request suspension and resumption of communication at any given time. Session layer messages are sent to the server if the client application requests for a suspension and vice versa. This demonstrates mobility on demand from the applications. The other mobility scenarios that can

be tested are suspend and resume from short and long network disconnections. In this case, network disconnection (mobility event) is generated by unplugging the Ethernet cable.

**NMIP MPTCP and SCTP comparison:**

The main validation results have been obtained by doing measurement of throughput on different packet size for each interface (Ethernet, LTE, Wi-Fi). Other measurements on HO performance have been realized.

- NMIP is the most efficient protocol for the throughput and has good performance on handover.
- MPTCP has some performance issues but it's multipath functionality allows it to perform well for handover management.
- SCTP has also some performance issues, but its failover functionality may be the key point to select this protocol.

## 3.5 Flat and distributed mobility management

This section describes the validation of flat or distributed mobility management protocols. These protocols need network infrastructure. Several candidate technologies are investigated. Solutions providing network mobility are also discussed within this section.

### 3.5.1 Functional and performance validation of UFA-SIP

#### 3.5.1.1 Key Performance Indicators

- KPI 1.1: throughput gain in mobile access and backhaul
- KPI 1.4: Efficient load distribution (in backhaul and in the core)
- KPI 2.3 Service Interruption and Handover delay
- KPI 2.5 handover related signaling load on the network
- KPI 3.2 E-E delay between UE and content

Applicability and Dependencies to Other Technologies:

UFA-SIP can be used alone. Other technologies may bring more optimization such as SON or MIH.

#### 3.5.1.2 Main Validation Results

Validation results are related to each of the procedures defined for UFA-SIP (see section 2.6.3.1). They concern the service establishment delay, Implementation and performance of UFA mobility procedure for SIP native services and the performance of UFA mobility procedure for non-SIP native services.

### 3.5.2 Functional and performance validation of HIP-based Ultra Flat Architecture with 802.21 and NEMO support

#### 3.5.2.1 Covered challenges

UFA-HIP is a special architecture supported with an advanced proactive distributed mobility management protocol designed to address the scalability problems of centralized mobility systems by flattening the architecture and shifting network intelligence closer to the end user terminals.

#### 3.5.2.2 Key Performance Indicators

As collected in MEVICO, UFA-HIP addresses those following main KPIs:

- KPI 1.4 Efficient load distribution in the backhaul and in the core
- KPI 2.1 Offload gain due to the usage of multi-access capabilities
- KPI 2.3 Service interruption delay due to handover
- KPI 2.4 Handover related signaling load on the network
- KPI 3.1 E-E delay between UE and content

#### 3.5.2.3 Applicability and Dependencies to Other Technologies

In the previous sections the inter-GW handover properties of the HIP-based Ultra Flat Architecture has been in focus. Service continuity during inter-GW handovers and seamless inter-GW handover for real-time applications was a criterion during the design of this technology. The validation has shown that the technology is able to provide these services within the constraints that are discussed in the followings.

Note that besides the inter-GW handover procedure, the initial attachment procedure of the UE with HIP DEX-AKA has also been considered. In Section 3.7.1 we discuss the performance features of the protocol, while in Section 3.7.2 we evaluate the suitability of HIP DEX-AKA-based L3 initial attachment procedure to predefined set of criteria by comparing it with other L3 initial attachment technologies from the 3GPP standard or state-of-the-art.

Here are the main points that must be considered when evaluating the applicability of the technology

- UFA-HIP technology provides a secure, HIP controlled IPsec overlay both for HIP-aware and non HIP-aware applications as described in [17], [18].

- Transition between HIP- and non HIP-enabled nodes is not recommended to be used. There exist an IETF draft for HIP-proxy technology [19], but it does not specify any NAT-like service that would be needed for traffic flow mapping. E.g the current HIP-proxy specification cannot solve the situation where the same non-HIP node (e.g. UE, Application server, Web server) must be reached by more than one HIP-enabled UEs. Besides the lack of NAT service in HIP-proxy specification, there is another issue with HIP proxy service.

  Allowing the attachment of non-HIP nodes into the secure HIP/IPsec overlay network causes access of weakly protected nodes through the IPsec firewall of HIP-enabled nodes. For security reasons, it is not recommended to use HIP/IPsec based and other weakly protected tunneling for different service flows on the same device. Applications, services that require ports not protected by IPsec security policies should be minimized.

- UFA-HIP technology influences both user access security and network security features of the 3GPP architecture.
  - 3GPP network security basically employs IPsec on untrusted links/paths between network elements. IPsec security association establishment is controlled by certificate-based IKEv2 protocol.
  - UFA-HIP technology requires IPsec SAs (as the default transport protocol for HIP based applications) between the GWs. IPsec SAs are automatically created by UFA-HIP for user service data flows between the GWs of the communicating UEs, or between the GW of the UE and a HIP-enabled correspondent node.

- The technology creates new tunneling option for the 3GPP architecture. As discussed in Section 4.2.1, the HIP/IPsec based tunneling can be deployed in two phases.
  - In the first phase, existing tunneling options, such as GTP, PMIP/IP GRE, are used to provide IP connectivity to the UE. All functionalities related to these tunneling options remain untouched. The HIP/IPsec overlay network links are established between the UE and P-GW and between the P-GWs (P-GWs are the UFA-HIP GWs)
  - In the second phase the tunneling protocols stack is changed, leading to simplified protocol architecture. The tunneling of traffic between the UE and distributed UFA GWs (i.e., ePDGs, P-GWs, S-GWs, GWs in trusted non-3GPP access), and between the GWs is realized by IPsec in BEET mode (or tunnel mode). GTP tunnel only remains in case of 3GPP-access on the S1 interface.

Possible ways to integrate the technology to the 3GPP architecture are presented in Appendix A – Deployment of UFA-HIP and Sections 4.2.1, 4.2.2 and 4.2.3. Appendix X contains the protocol architecture figures for different access types and deployment phases. Sections 4.2.1, 4.2.2 and 4.2.3 present high-level reference models for UFA-HIP integrated to the 3GPP EPC using centralized, distributed, and flat topologies.

#### 3.5.2.4 Main validation results

The validation of UFA-HIP was focusing on the service interruption delay (or handover delay). Performance of the technology was compared to the standard MIPv6 (RFC 6275) and standard HIP (RFC

4423) procedures. Measurements show that the service interruption delay of UFA-HIP is decreased by 72% with respect to the MIPv6 case and by 71% compared to the HIP case in average, thanks to the advanced proactive operation which basically reduces the handover disruption to the Layer 2 (re-) attachment delay.

## 3.6 Routing Optimization

### 3.6.1 Functional and performance validation of PMIPv6 Route Optimization

#### 3.6.1.1 Covered challenges

PMIP-RO is designed to address the issue of centralized mobility anchoring in distributed to flat architectures. In such a context, centralization of both data and signaling may potentially cause un-optimized routing, P-GW overload, and contention.

#### 3.6.1.2 Key Performance Indicators

As collected in MEVICO, PMIP-RO addresses those following KPIs:

- KPI 1.1: throughput gain in 3GPP access and backhaul
- KPI 1.4: fair load distribution in backhaul
- KPI 2.2 capacity aggregation
- KPI 3.2 E-E delay between UE and content or path lengths in terms of transport hops / IP hops
- KPI 3.3 analyze offload gains for core network equipments: e.g., number of active user contexts per network equipment
- new KPI: load distribution in core

#### 3.6.1.3 Applicability and Dependencies to Other Technologies

This technology is an extension of PMIPv6 and must be used when the UE mobility is handled by PMIPv6. Because, the LMA remains the signaling anchor of optimized data traffics, PMIP-RO will suffer of any gateway reselection mechanism applied on on-going sessions.

#### 3.6.1.4 Main Validation Results

PMIP-RO performance validations have been performed and are presented in D2.3. The main result is that the implementation that has been done following the provided specification validates the expected results of the technology.

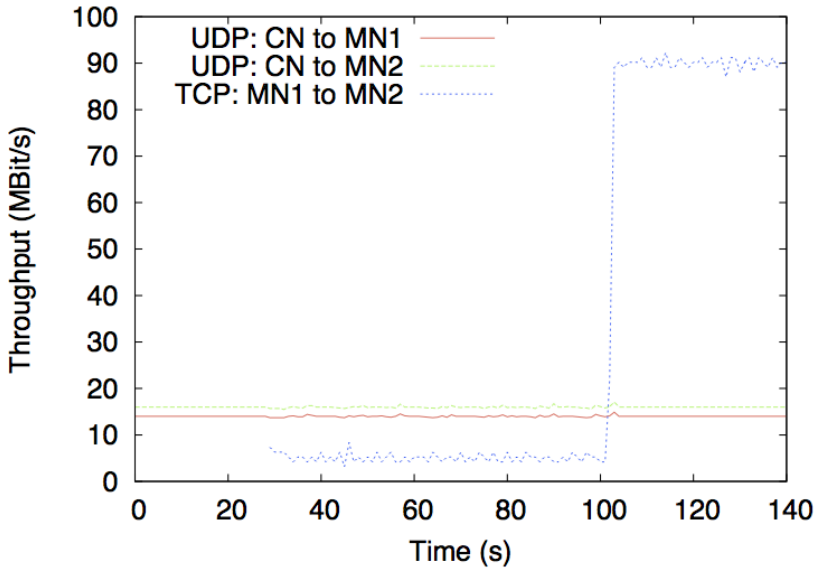



**Figure 47: Throughput improvement before and after activation of PMIP-RO.**

As presented in Figure 47, one observes that the throughput of a TCP stream that suffers from concurrent UDP flows is highly increased after activation of PMIP-RO at time 102 second. The throughput limited to 4-7 Mbit//s increases to 90 Mbit/s.

### 3.6.2 Functional and performance validation of PMIPv6 with NEMO support

#### 3.6.2.1 Covered challenges

PMIP-NEMO is an extension of PMIPv6 to support mobility of moving networks. A moving network is a network composed by one or more gateways connected to the mobile network and that provide connectivity of several UEs, internally. This functionality is important as it will reduce the number of stored contexts in the network while ensuring the handling of the increasing number of UEs.

#### 3.6.2.2 Key Performance Indicators

As collected in MEVICO, PMIP-RO addresses those following KPIs:

- KPI 2.5 handover related signaling load on the network
- KPI 3.3 analyze offload gains for core network equipments: e.g., number of active user contexts per network equipment
- new KPI: load distribution in core

#### 3.6.2.3 Applicability and Dependencies to Other Technologies

This technology is an extension of PMIPv6 and must be used as long as PMIPv6 handles mobility of the concerned UEs. Specific architectural requirements are addressed in Section 2.9.1.

#### 3.6.2.4 Main Validation Results

The validation results are presented in D2.3. The main conclusion of these results is that the implementation that has been done following the provided specification validates the proposed functionality.

## 3.7 User access authorization

This topic validation covers terminal attachment related functional and performance validations. Within that, new L3 access authorization schemes are investigated. The main challenges to be covered here are reduction of security setup overhead and seamless interworking with different access technologies.

### 3.7.1 Performance evaluation of new HIP access authorization methods compared with IKEv2-based methods

#### 3.7.1.1 Covered challenges

This work evaluates the performance benefits of Host Identity Protocol Diet Exchange (HIP DEX), and HIP DEX with Authentication and Key Agreement (AKA) protocols. HIP DEX AKA provides similar functionality to the Internet Key Exchange protocol v2 (IKEv2) with EAP-AKA that controls user access authentication and authorization of USIM based UEs in non-managed non-3GPP access networks. With HIP mobility extension, it provides the same functionality as MOBIKE, i.e., supports IP mobility while the UE remains attached to the same ePDG. Both services provide mutual authentication and establish an IPsec security association pair to protect the path between the UE and the ePDG in the network layer.

Several challenges of the EPC have been identified in the mobility work package. This technology may tackle the following challenge:

- Reduce security setup overhead. This challenge becomes more important if GWs are distributed and pushed down to regional and local POPs, because at each inter-GW handover user access authorization must be controlled.
- We plan also to examine whether seamless handover is achievable for real-time services during re-attachment procedures without making further optimizations of the technologies.

#### 3.7.1.2 Key Performance Indicators

The following performance indicators have been used:

- Computational cost: the main performance metric is the CPU clock intervals occupied by one authentication flow in the UE, GW and AAA server. However, we also measure the computational times on these network elements, and the proportion of computational time in the

overall authentication delay. The relative gain of the methods compared to IKEv2 EAP-AKA is relevant.

- Memory consumption: the performance metric is the occupied heap and stack memory size in kBytes, by one authentication flow and the initialization of the methods, on the UE, GW and AAA server. The relative gain compared to IKEv2 EAP-AKA method is relevant.
- Real-time service interruption delay: the applied metric is the authentication delay of the L3 authentication, security association and key establishment procedure. Objective constraints for the re-attachment delay to a new access network for real-time applications are defined by the packet delay budgets for different application types in TS 23.203 [6]. The authentication delay is compared to these values in different reference scenarios; hence we can see whether a given method could be used if seamless handover for real-time applications have been defined as a MUST requirement.

  Note: in MEVICO this has not been defined as a MUST requirement, but it is a significant feature of an authentication method, if it enables the fulfillment of packet delay budgets for real-time applications.

  Note: L3 authentication delay is only part of the budget, because L1/L2 attachment and optionally the IP mobility procedure is also part of that. The authentication methods under evaluation support non--simultaneous IP address update of the entities. Typically the UE will change its IP address.

  Note: GW change is not supported by any of these methods, i.e., complete re-association is required, which interrupts ongoing sessions if not handled by an IP mobility management protocol. That would require security context transfer between the GWs. A possible solution for HIP-based methods is the UFA-HIP technology.
- Message complexity of signaling: this is measured by counting the average number of signaling messages for one L3 authentication on the RAN and backhaul (i.e., between the UE and GW) and on the aggregation and core network, i.e., between the GW and AAA/HSS). The average total size of the control messages have been also measured for one authentication flow on the two network parts.

#### 3.7.1.3 Main Validation Results

The reduction in the amount of non idle CPU intervals occupied by the HIP DEX-AKA authentication process is significant compared to IKEv2 EAP-AKA in relative terms. On the UE 12%, on the GW 2% is the proportion of the computational cost of HIP DEX-AKA versus IKEv2 EAP-AKA. DEX proves to be the less demanding method, however it is less appealing for mobile operator based environment where the USIM based subscriber authentication is already in place.

Note: In absolute terms, the frequency and cost of re-authentications is so low, that no significant influence is on the battery consumption of the UE. CPU typically consumes less than 10% of the total energy consumption. The frequency of re-authentications can be estimated as the sum of the intensity of GW change due to mobility and the frequency of lifetime expiration. In order to reduce the frequency of complete re-authentications, support of GW change should be added to these authentication methods.

The proportion of computational time in the overall authentication delay is 7-10% for HIP DEX-AKA, while 40-50% for Ikev2 EAP-AKA in case of Wi-Fi access. The exact values depend on the validation scenario. HIP DEX-AKA and HIP DEX reduce the computational time part significantly compared to the other methods

The results show, that reduction of memory utilization of HIP DEX-AKA, and HIP DEX is significant compared to the other authentication methods. Comparing HIP DEX-AKA with IKEv2 EAP-AKA, HIP DEX-AKA provides 80% gain on the UE and the GW. The AAA server is not utilized by HIP DEX-AKA.

The authentication delay results show that HIP DEX-AKA highly improves the authentication delay compared to IKEv2 EAP-AKA. Regarding the packet delay budget, only in case of the Wi-Fi access it results authentication delays between 150 and 300 ms. I.e. HIP DEX-AKA could be used in case of buffered video streaming and could enable seamless handover for these applications, if the overall delay is less than 300 ms together with other delay factors.

Note that no one of the evaluated authentication methods were designed with fast re-authentication in focus in case of break-before-make handovers. It also can be stated for the authentication methods applicable in large environment, i.e., for IKEv2 EAP-AKA, IKEv2 EAP-TLS and HIP-DEX AKA, the scenario causing the lowest delay was the distributed scenario. However, in case of IKEv2 EAP-AKA and HIP DEX-AKA, the flat scenario also results very close results.

Regarding message complexity, both in terms of number of messages and in terms of the total size of the messages at different parts of the network, HIP DEX-AKA significantly outperforms EAP-AKA. The ratio of the number and total size of messages is 56% and 37%, respectively, between HIP DEX-AKA and IKEv2 EAP-AKA. Another important aspect is the number of control messages charging the aggregation and core network. HIP DEX-AKA requires on average two messages less per re-authentication than IKEv2 EAP-AKA.

#### 3.7.1.4 Future Work for Improvements

Due to the high service time overhead with the AKA process and authentication vector retrieval, HIP-DEX requires optimizations if it is to be used in environments where re-authentications take place constantly (e.g. inter-GW handovers). To improve the protocol for such environments, the gateway could retrieve several AVs at once or/and UE could be granted with an authenticating ticket or certificate so that time consuming AKA would be run only upon the first attachment.

This kind of optimization for re-authentications would improve the performance of subsequent HIP-AKA runs and decrease the signaling overhead further in the core network. Other future research directions include deploying HIP-AKA closer to the user in the Wi-Fi and (E)-UTRAN access points and using the scheme to carry bootstrapping information as well.

### 3.7.2 Suitability analysis of different L3 authentication methods for the MEVICO architecture and requirements

#### 3.7.2.1 Covered challenges

The suitability of a new technology to an existing architecture depends on many criteria and requirements. The appropriate decision for the applicability of a new technology should consider all important requirements and features of the technology.

The main objective of this validation is to compare the HIP DEX and HIP DEX-AKA authentication methods with IKEv2 EAP-AKA and other L3 authentication methods form a broader aspect, using a multi-criteria decision technique.

The compared alternatives are the following technologies:

- Host Identity Protocol Diet Exchange with EPS-AKA authentication (HIP DEX-AKA)
- Internet Key Exchange version 2 with EAP-AKA authentication (IKEv2 EAP-AKA): reference alternative currently applied in untrusted non-managed access
- Host Identity Protocol Diet Exchange (HIP DEX)
- Host Identity Protocol Base Exchange without certificates (HIP BEX)
- Internet Key Exchange version 2 with pre-shared key based authentication (IKEv2 PSK)
- Internet Key Exchange version 2 with EAP-TLS authentication (IKEv2 EAP-TLS)

#### 3.7.2.2 Key Performance Indicators

Figure 48 summarizes the criteria applied for the comparison of the L3 authentication methods. It also describes the performance metrics for each criterion at the leaves of the criteria tree. Some of the metrics are qualitative, some of them are quantitative. Under each leaf of the criteria tree a performance grade assignment is needed, which normalizes the metrics and renders them to a higher-the-better scale of integer values. The detailed description of the authentication methods under these metrics can be found in D2.3 Final Evaluation Report, Section 2.6.2.5


**Figure 48: Criteria for the suitability analysis of authentication methods**

### 3.7.2.3 Main Validation Results

The terminal scores obtained by the methods are similar in flat, distributed and centralized scenarios, because they differ only in the "Authentication delay", i.e., the metric applied for the real-time service interruption delay. IKEv2 EAP-AKA is the most preferred method in case of HSDPA/UMTS access, while HIP DEX-AKA method is the most preferred in case of Wi-Fi access. The difference seems very small between the two methods in both access types. The aggregated scores are the result of the actual trade-off between different criteria specific to each authentication method under the criteria weights defined by multiple decision makers.

IKEv2 PSK, HIP DEX and HIP BEX have been rejected, i.e. got zero terminal score, because of their rejection under the configuration criteria in the UE and GW. This is due to the bad scalability of the management/configuration of these authentication methods in large-scale network, the key management cost of pre-shared keys in case of IKEv2 PSK, or management of access control lists based on HITs in case of HIP DEX and BEX. Under performance criteria, the computational and memory cost of HIP DEX and DEX-AKA are the best among the methods. Regarding signaling cost, i.e., the number of control messages, HIP DEX-AKA performs the same as IKEv2 EAP-AKA, HIP DEX performs the same as HIP BEX and IKEv2 PSK.

Under authentication time criterion, in case of HSDPA/UMTS access, all the authentication methods got the same terminal score, because all of them obtained zero grades due to non fulfillment of the 300 ms packet delay budget of real-time applications. On the other hand, in case of Wi-Fi access, HIP-based methods obtained positive grades, between 1 and 4, while IKEv2 EAP-TLS and EAP-AKA methods got 0 grades. This is reflected by the terminal scores under authentication time in case of Wi-Fi access. Note

that if the support of real-time packet delay budgets during handover was a "MUST" requirement, then only HIP DEX-AKA could be acceptable among the authentication methods working in large-scale environment, but it can work only for video streaming applications.

Among the deployment criteria, IKEv2-based methods naturally get higher terminal scores, since IKEv2 EAP-AKA is assumed to be supported already by the network. Under the extra functionalities criterion, HIP-based methods perform somewhat better due to their better multipath capability feature, then in case of IKEv2-based methods.

The robustness of the final scores of the authentication methods has been evaluated as well, under perturbed weights of the four main criteria. The results show that HIP DEX-AKA should be the preferred method in case of high performance and extra functionality requirements. Otherwise, increasing security requirements bring IKEv2 EAP-AKA method the preferable alternative. If only security requirements count, IKEv2 EAP-TLS is the most preferable method, because it supports digital signature of the TLS-client and TLS-server, additionally to EAP-AKA method where no digital signatures are incorporated in the protocol. Increasing deployment cost requirements favour the selection of IKEv2 EAP-AKA method.

#### 3.7.2.4 Future work for improvements

HIP BEX based authentication extended with EPS-AKA or EAP-AKA support could enable the selection of HIP-based technologies in a much wider range of usage scenarios. HIP BEX-AKA could have stronger security features than IKEv2 EAP-AKA due to the application of digital signature, optional host identity protection with BLIND, and still brings the better features in extra functionalities. However, the performance cost of HIP BEX-AKA should be validated before bringing final conclusions. Currently HIP-BEX requires half of the computational and memory cost of IKEv2 EAP-AKA, but the influence of the addition of EPS-AKA or EAP-AKA to the method should be analyzed.

Seamless inter-GWs handover for real-time services proved to not to be supported by any of the non rejected technologies, i.e., IKEv2 EAP-AKA, EAP-TLS, and HIP-DEX-AKA. A small exception is that HIP DEX-AKA causes an authentication delay between 150 and 300 ms in the reference scenarios using Wi-Fi access. If the sum of the authentication delay and additional delay factors for L1/L2 handover and IP mobility management were below 300 ms, the technology could be used for real-time video streaming applications. The main conclusion is that other approaches should be used in order to enable seamless inter-GW handovers. The UFA-HIP technology aims to provide solution for this problem for HIP-based architectures, by proactive L2, HIP and IPsec state establishment before physical hand-off of the UE.

#### 3.7.2.5 Applicability of the results

The results show that HIP-DEX-AKA method should only be used for UEs with very low computational and memory resources, and requiring the most important security features. The security of the original IKEv2 EAP-AKA method is stronger. IKEv2 EAP-AKA should be the applied method in use cases where there are no extra requirements regarding performance and multipath capabilities. Possible usage cases of HIP DEX-AKA technology are remote industrial control and monitoring applications.

## 3.8 Support for user cooperation

Relaying techniques are considered as an alternative solution to enhance capacity for the cell network, to extend coverage in specific locations, to increase throughput in hotspots or to overcome excessive shadowing. It gives important advantages such as ease of deployment and reduced deployment cost compared to deploying regular Base Station (BS).

### 3.8.1 Performance evaluation of mobile relaying and its management

#### 3.8.1.1 Covered challenges

Covered challenges are:

C.Mo.10: Support for user cooperation

C.Tr.1: Increase data throughput in mobile transport network

#### 3.8.1.2 Key Performance Indicators

- Edge user throughput
- Power consumption

### 3.8.1.3 Applicability and Dependencies to Other Technologies

We envision two cases of deployment for the mobile relay assisted communication for EPC architecture. First, MME (RN) (or MME directly) and DeNB cooperation will be required. In this case, MME will store the location information of the UE and it will choose the appropriate relay for UE. In the second case, DeNB will initiate relay signaling with target UE and the relay UE. In this case, DeNB will handle all coordination. This will simplify the load on EPC and will also increase the complexity of DeNB.

### 3.8.1.4 Main Validation Results

Matlab platform is used to simulate our proposed mobile relaying system model. The following table consists of the real LTE network parameters which are used in our simulation platform

**Table 2: Simulation parameters**

| Simulation Parameters | Value |
|---|---|
| Frequency | 2.14GHz |
| Bandwidth | 20MHz |
| Thermal Noise Density | -134.89dBm per Hz |
| nTX & nRX antennas | 1 x 1 |
| eNodeB transmission power | 43dBm |
| UE transmission power in relay mode | 23dBm |
| Cell radius | 500m |
| Pathloss Model | 128.1+37.6*log10(d) |
| Shadowing Model | Log normal distribution, μ=0 and σ=10dB |
| Multipath Model | Extended Pedestrian A (EPA) |
| UEs position | Uniformly distributed for each zone |
| Number of Simulations | 10e3 per each scenario |

The cell structure consists of three zones, namely inner, middle and outer, respectively. In the proposed model, the users are uniformly distributed based on the real network topology with the following percentages: 20% at inner zone, 70% at middle zone and %10 at outer zone. These values are flexible and can be changed. The proposed mobile relaying system is depicted in the following figure.

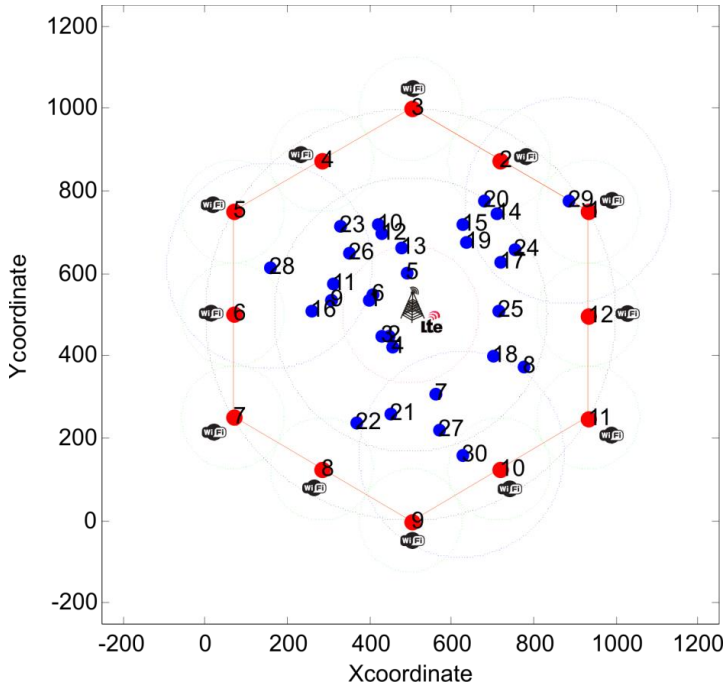



**Figure 49: subscriber distribution**

Channel is modeled according to path loss, shadowing and multipath. In order to model PL, PL = 128.1 +37.6* log10 (R) where R is the base station-UE separation in km is used. For shadowing, zero-mean Gaussian distribution and for multipath, three different channel models such as Extended Pedestrian A (EPA), Extended Vehicular A (EVA) and Extended Typical Urban (ETU) are used. During the allocation (1ms), the channel is not changing.

In the next term, we will specially focus on NS3 platform to determine the effect of the proposed mobile relaying to capacity improvement of backhaul network in LTE.

‘

# 4. Integration of technologies

For the derivation of the network architecture the coexistence of the currently deployed and the newly proposed technologies must be analyzed and integration issues must be dealt with. Besides this the proposed architecture must meet system validation criteria regarding performance, deployment and technology maturity questions.

This chapter describes the integration questions and results for the technologies proposed to handle mobility management related challenges. The analysis considers the coexistence of mobility management technologies and other technologies that influence the successful operation of traffic management without degrading any function in the system.

## 4.1 System validation KPIs

This section describes the system validation criteria, i.e., specifies the criteria and the related performance metrics (i.e., system validation KPI). Furthermore this section provides a view on how to assess/measure each system validation KPI and what are the expectations related to them, i.e., proposes recommendations for ranking assignment method.

### 4.1.1 Throughput gain in 3GPP access and backhaul

The proposed technology will increase the network throughput and will be measured in terms of increase of number of packets and packets size in the access and backhaul. The requirements in 3GPP defined for different classes of traffic should be considered when measuring this KPI.

Related technologies and reasoning:

- **UFA-HIP**: UFA-HIP uses IPsec between the UEs and GWs and between GWs. Hence it adds overhead per each packet (64 bit ESP header and 96 bit ESP trailer, i.e. 20 bytes per packet).
- **UFA-SIP**: UFA-SIP is described in Section 2.6.3. As UFA reduces the number of network elements and proposes to localize the UFA_GW lower in the network, the backhaul needed to connected UFA-SIP allows a gain in the Access and backhaul compared to a centralized architecture.
- **PMIP-RO**: PMIP-RO (described in Section 2.5.1) addresses this KPI when is considered the LIPA scenario. PMIP-RO assumes as optimized data path two MAGs (for the source and destination UEs) and a certain number of intermediate IAs. In the LIPA scenario, the function of MAG could be co-located with a HeNB or other network element(s) belonging to the operator but out of the EPC. Furthermore IA could be located outside of the EPC and even located on L-GWs [3GPP TS 23.829].
- ANDSF: Knowledge of the other available radio accesses will help to improve the throughput, either by choosing a better radio access or by using simultaneous access over the available radio links.
- **DMA with GTP** contributes to optimal GW and offload point selection what increases the network throughput.
- **More-Het**: More-Het increases the edge-user throughput by utilizing users as mobile relays. Thus the number packets and packet sizes per edge user increases.
- **TRILL**: TRILL handles mobility in the access networks at Ethernet level without the need to propagate to core network and enables faster mobility without buffering packets during handover which results in higher throughput in the access and backhaul network.

### 4.1.2 Reliability, recovery time from link failures, congestions and OPEX reduction

This KPI should consider the 3GPP requirements defined for link failure recovery. The KPI could measure the route establishment in switches when link break happens. The 50ms delay for link failure recovery is the starting point and it should be reduced. This KPI should calculate mean time between failures and recovery.

Other technologies such as SON can provide rough figures in terms of OPEX to compare the labor effort to be done against not having such technology in place.

Related technologies and reasoning:

- **SCTP**: Prior to data transmission, an association is setup between the two communicating endpoints, and it is maintained during their entire communication. SCTP is a protocol that supports multi-homing. Multi-homing enables the end points of a single association to support

multiple IP addresses. Each IP address is equivalent to a different network path towards the communicating peer, for sending and receiving data through the network. Since an association is aware of all the available IP addresses, it is quick to shift to a different interface during link failures. So, the actual delay is in the link failure detection and end node software implementation.

- **MPTCP**: The multipath use is a way to solve link failure and may help to reduce congestion. MPTCP is not efficient enough when managing several interfaces that have very different throughput.
- **TRILL**: TRILL reduces congestion in access network by handling the mobility process in layer 2 without need to trigger upper layer handover process.

### 4.1.3 Efficient load distribution in backhaul and core networks

This KPI should show that the application of load balancing mechanism contributes to the non-congested states of the network in case of high traffic demands. The traffic load, the inter-arrival time and transmission delay should be measured either on end points or in the routers/switches if possible. The KPI could also use global packet loss ratio to measure the congestion of the end to end network

Related technologies and reasoning:

- **Wi-Fi**: Operator managed Wi-Fi technology is described in section 2.2. As per our prototype, Wi-Fi technology is not mainly used to offload traffic from the backhaul and/or the core network but, it is implemented in a way that makes it possible for an operator to use it efficiently for load distribution. The operator can provide service continuity; better indoor coverage for Wi-Fi enabled devices and this technology can also be used to offload broadband traffic from wide area radio network to Wi-Fi.
- **UFA-HIP**: UFA-HIP technology may enable load balancing by appropriate decision mechanisms implemented in the serving GWs of the UEs. The decision algorithm might trigger the hand-off of flows from a loaded access and backhaul network segment to less congested access network. However finding the appropriate decision making algorithm is part of future work.
- **UFA-SIP**: UFA-SIP is described in section 2.6.3. UFA is flat and introduces distributed signaling and data anchors that are the UFA_GWs and the SxS_GWs. This enables to better distribute the traffic load, unlike the centralized anchors. UFA_GWs distribution enables to distribute the S-CSCF and the Application Servers (e.g. TV servers), which enhances their scalability and reduces the delay for accessing the Application Servers content.

  The UFA_GWs are "natural" anchors as they offer physical connectivity to users. They are also temporary anchors as they do not stay on the path towards the MN, when this latter moves. Indeed, after MN mobility, the traffic passes through a new UFA_GW, the MN is physically attached to, and the old one is no more on the control or transfer plane path. The temporary anchors have been made possible in UFA, thanks to the use of SIP protocol for mobility management, instead of tunneling-based protocols, like GTP or MIP.

  Thanks to the reduction of network node types in UFA, redundant context information and tasks necessary to handle an ongoing call are deleted. Thus, the network processing delay is reduced.
- **NMIP** allows realizing fast and seamless handover and thus permits to use alternate path such as done with Wi-Fi offload. Hence backhaul use may be reduced.
- **ANDSF** information given to the UE helps to optimize the HO process and then allows efficient mobility. This can be used for offloading techniques that make contribute to decrease the backhaul traffic.
- **MPTCP** multipath capability is an obvious solution to realize load balancing over the different path then optimizing the backhaul capacity.
- **DMA with GTP** introduces more flexibility in selecting available GWs. This could contribute to load distribution for both the link load and the GW load
- **More-Het**: More-Het uses offloading to Wi-Fi if eNB is congested or the expected throughput is low.

### 4.1.4 Offload gain due to the usage of multi-access capabilities

The KPI can measure the user and operator point of view.

- User point of view. The KPI should measure the traffic that goes on each interface of the UE in case of simultaneous use of radio interfaces or it should measure the end to end delay of transmission.
- Operator point of view. The KPI should measure the load on different elements of the network. It could measure the proportion of load in different access i.e. Wi-Fi access versus LTE access.

Related technologies and reasoning:

- **Wi-Fi:** By using operator managed Wi-Fi, users can get operator partner services tied to mobile subscription also over WLAN behind RGW. E.g. Spotify. From the operators' point of view, they manage the Wi-Fi access point and they can provide personal connectivity services for devices in residential network. They can provide better indoor coverage and also offload broadband traffic from wide area radio network to Wi-Fi.
- **UFA-SIP**: As the UFA_Gws are distributed and located near the users, UFA allows an offload whatever the situation.
- **UFA-HIP**: same applies as for UFA-SIP.
- **NMIP** fast handover processing allows when by using the Wi-Fi as the first chosen access to realize the offloading of the traffic in an efficient way.
- **ANDSF** information permits to retrieve the load of POA (eNodeB, Wi-Fi access point) and choose the best traffic distribution
- **MPTCP** like any other solutions that use multipath solves partially the offloading solution by doing load balancing among the available paths.
- **More-Het**: More-Het uses offloading to Wi-Fi if eNB is congested or the expected throughput is low. Thus, offload gain is achieved using multi-access capabilities.

### 4.1.5 Capacity aggregation and E2E QoE provision

This KPI should measure the throughput gain including goodput. The KPI will also measure QoS packet delay jitter packet loss plus any additional QoE measurements.

Related technologies and reasoning:

- **SCTP**: Although SCTP supports multi-homing, currently it uses multi-homing as a means for path-level redundancy to provide uninterrupted service during resource failures, and not for load balancing. Each of the endpoints chooses a single primary destination address and as long as this primary path is reachable, all data is transmitted on this path. So, there is no capacity aggregation with SCTP.

  But, since an SCTP association is aware of all the available IP addresses, it is quick to change to another interface when the primary interface fails. This leads to less delay during a failover and in turn contributes to better QoS. Also, the session continuity feature with SCTP protocol provides users with some additional functionality during network interruptions.
- **MPTCP** multipath ability helps to realize capacity aggregation. Nevertheless the QoE will be managed independently on each path, so coherent E2E may not be achievable.
- **DMA with GTP** allow to select GWs close to content sources and optimal internet exchange points what reduces packet delay and jitter. Intelligent IP address changes contribute to QoE by limiting the impact on applications.

### 4.1.6 Service interruption delay due to handover

This KPI will measure the packet transmission additional delay due to flow mobility/handover. The KPI can measure the service interruption delay and it can measure jitter due to HO. Packet delay budgets for guaranteed bitrates real-time services can be considered as hard constraints for induced E-E service interruption delay.

Related technologies and reasoning:

- **Wi-Fi:** Operator managed Wi-Fi technology does not mainly intend to reduce the handover delay during a service interruption. The Wi-Fi AP broadcasts two SSIDs; one is the operator managed SSID and the other is the private SSID. The UE can select any of these. If the private SSID is selected, the traffic is sent directly to the Internet through the BNG. But, if the operator managed SSID is selected, at power on, a managed Wi-Fi tunnel is set up between the Wi-Fi AP and the BNG. Packets are forwarded in/out of the managed Wi-Fi tunnel through BNG either to the mobile core network or to the Internet.

- **UFA-SIP**: UFA-SIP mobility procedure is described in section mobility is ,In UFA .2.6.3 .optimised and adapts to hard and soft handover cases

  The handover delay is reduced as it is based on a preparation procedure and context transfer procedure. Moreover, all the contexts to be transferred are co-located in the UFA_GW.

- **UFA-HIP**: UFA-HIP can provide seamless inter-GW handover due to proactive operations for all applications.

- **SCTP:** One of SCTP's novel features is multi-homing. Multi-homing enables the endpoints of a single association to support multiple IP addresses. An SCTP association is aware of all the available IP addresses. Hence, there is less delay associated with the handover during service interruption. In our implementation, we have a module called the mobility manager which receives notifications about the local interface changes (additions/deletions) and reacts with the SCTP stack in order to achieve quick handover to the most preferred interface. It contains all the intelligence for ensuring proper behavior of a SCTP application in a dynamic mobile environment.

- **NMIP** helps to reduce the HO process duration and then decreases the interruption delay.

- **ANDSF** by knowing the current available radio access permits to optimize the selection decision by avoiding wrong radio access due to radio condition or congestion status.

- **TRILL** : Micro-mobility support in L2-TRILL **TRILL** together with an additional extension using Distributed Hash Tables (DHT), and based on Carrier Ethernet can be deployed in the mobile backhaul. Ethernet mobility utilizes VLANs to separate different traffic types and define the QoS treatment. In order to make the solution scalable VLAN stacking with 802.1ad frames. Outer VLAN (S-VLAN) is used to separate traffic destined to different eNB groups. If several operators share the network they can have S-VLANs of their own. The target is that handovers are rare between the groups. Inner VLANs (C-VLANs) are used to separate different traffic types and QoS classes. 3GPP signaling towards the MME element has a C-VLAN of its own. A further benefit of using Ethernet VLAN tags is that the carrier network can switch packets based on VLAN tags. This is very beneficial in terms of scaling the network segments and minimizing any state stored on the switches.

  TRILL allows performing localized handover process in the access network in the Ethernet layer. This will reduce S1 signaling since the addressing updates are performed faster which reduces latency (and implicitly reduces packet loss) when transferring the session within the access network. The L2 mobility supports higher number of handovers in small cells scenarios where handover process increases. Thus, reducing the overall handover delay since the handover is handled locally in the Ethernet switches.

  The deployment in EPC network requires either upgrading the Ethernet switch in the eNODEB or including TRILL based Ethernet switch in the egress connection to the eNODEB to inform Customer Edge Switch about the changes in the binding between UE IP an eNODEB MAC address.

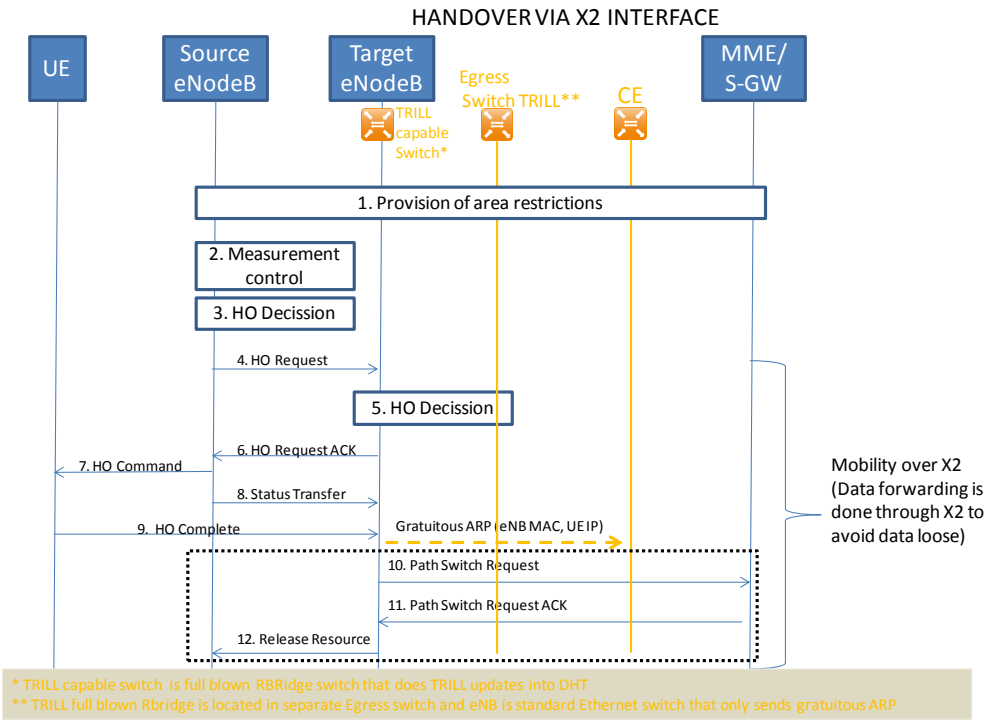



**Figure 50: Handover via X2 interface**

### 4.1.7 Handover related signaling load on networks

Analyze the handover procedures together with handover initialization, preparation, completion phases. Show that compared to state-of-the-art handover the new technologies provide reduced signaling load on different parts of the network.

This KPI can measure transmitted data overhead for HO process. This KPI can measure the number of HO messages and their size.

Related technologies and reasoning:

- **UFA-SIP:** As the number of network nodes is reduced within UFA (compared to centralized architecture), the number of messages exchanged to handle mobility is also reduced.
- **UFA-HIP**: the number of signaling messages is quite high for UFA-HIP architecture. It includes MIH handover preparation, HIP handover preparation, MIH Resource preparation, and MIH resource release procedures. This means approximately 40 signaling messages in different parts of the network. This number increases approximately by 6 messages per active sessions.
- **PMIP-NEMO**: PMIP-NEMO (described in Section 2.9.1) considers the scenario of moving networks. In such networks, a mobile router typically aggregates mobility (and by extension, handovers) of its LFNs (standard UEs). In this solution, a mobile router offers connectivity to LFNs with, for instance, Wi-Fi while it is attached to the core network with, for instance, 3G. Therefore, the mobile network operator is able to provide connectivity to a group of UEs without having to handle all of their contexts and profiles reducing the handover signaling load.
- **SCTP**: In our implementation of session continuity, we have a new layer called the session layer in the IP stack. When an application requests for a session suspend or when there is network interruption, a suspend message is sent to the communicating peer. Similarly, when the application wishes to resume the session or when the network connectivity is regained, a resume message is sent to the peer with the previous session ID in order to be identified by the peer.
- **HIP-Auth**: compared to IKEv2 EAP-AKA applied in untrusted non-3GPP access, HIP DEX-AKA reduces the number of signaling messages for initial authentication and IPsec SA establishment. The ratio of the number and total size of messages is 56% and 37%, respectively, between HIP DEX-AKA and IKEv2 EAP-AKA
- **TRILL**: Access network limited mobility –TRILL

  The handover performed via the X2 interface where the binding between the UE IP and the new eNODEB MAC address where the UE is attached will be handled locally by the Ethernet switches. This will reduce the S1 signaling required in the later stage when MME needs to be informed about the MAC address where the UE can be reached.

### 4.1.8 E2E delay between UE and content

This KPI can measure RTT (on UE or server). The 3GPP Requirements by application type in terms of E2E delay budget should be considered. This KPI could also measure the path lengths in terms of number of L2/L3 hops.

Related technologies and rationales:

- **UFA-SIP:** As UFA is flat, contents could be placed low in the network. This makes the E-E delay reduced. Moreover, as the number of nodes in UFA is reduced, the delay is more reduced.
- **UFA-HIP:** Due to the distribution of GWs UFA-HIP reduces path lengths, hence the E-E delay.
- **PMIP-RO:** PMIP-RO (described in Section 2.5.1) addresses this KPI by proposing a mean to redirect traffic to specific data paths. By doing so, we are able to reduce in most cases the end-to-end delay for data exchange. However, by exploiting alternate paths than the generic one, it is also possible to balance data traffics and to improve the overall QoE for users.
- **DMA with GTP** can provide a shorter path to content sources as described above
- **TRILL:** Reducing mobility process by performing the required updates in the switches avoids having to buffer packets in old eNodeB during the handover process, thus reducing overall E2E delay between UE and content when moving.

### 4.1.9 Offload gains for core network equipments

This KPI can measure the throughput (i.e. number of data flows) on network elements such as S/P-GW, furthermore, user signaling reduction (i.e. number of signaling messages, the number of active user contexts per network equipment) on network elements such MME or S/P-GW. It can also measure goodput values on the specific network element.

Related technologies and rationales:

- **UFA-HIP**: UFA-HIP optimizes data paths hence distribute load between several GWs.
- **PMIP-RO**: PMIP-RO (described in Section 2.5.1) addresses this KPI by proposing optimized data paths that avoid passing through the LMA (P-GW). Even if signaling is still anchored at the LMA, the main purpose of this solution is also to take advantage of the distributed architecture to anchor data traffics to intermediate nodes (IAs).
- **HIP-Auth**: In case of deploying HIP DEX-AKA authentication method e.g. instead of IKEv2 EAP-AKA, it could provide computational and memory utilization gains on the GWs (i.e., ePDG, S/P-GW) and the AAA server. The AAA server is not utilized by the current HIP DEX-AKA prototype (i.e., the GW directly accesses the HSS), hence it provides 100% gain in terms of memory and computational requirements. Comparing HIP DEX-AKA with IKEv2 EAP-AKA, HIP DEX-AKA provides 80% gain on the GW in terms of memory utilization and 98% gain in terms of CPU utilization.
- **DMA with GTP** can free resources by allocating combined SGW and PGW. OpenFlow based EPC provides signaling offload to the MME/EPC by handling mobility and GW changes transparently.

## 4.2 MEVICO Architecture Options

It was noted that certain architectures in WP2 can be exploit in any architecture option; centralized, distributed or flat. Such technologies do not demand any modification in the core network elements since they are not sensitive on the topology.

| Architecture independent WP2 technologies | Description |
|---|---|
| 1. Improving UE's multiple network access capability and load balancing through Wi-fi offloading | Wi-Fi AP traffic is routed to P-GW via a fixed network instead of a mobile network and no additional functionality in the core network elements is needed. The technology is not topology sensitive in the sense that as long as there is a defined anchor point it will work. |
| 2. Decision and handover preparation methods for efficient load balancing and | SCTP requires support on the UE or the application, and does not need modifications on |

| | |
|---|---|
| flow mapping and Terminal-based mobility management | the network side. It can provide end to end anchorless mobility. Its performance is independent of the architecture. |

In the following subsections, we illustrate possible deployment options for UFA-HIP and UFA-SIP technologies. Both technologies were originally designed and validated using the flat or distributed architecture option. Inter-GW handover procedures however can be provided by these technologies as long as there are multiple distributed GWs, regardless of their location. The techno-economical validations proved that either the centralized or the distributed architecture option is the most preferred, depending on the proportion of the evolution of the costs of transport network and the cost of LTE platforms per offered capacity unit [27].

### 4.2.1 Centralized Architecture Option

The following figures show the centralized architecture option for HIP-enabled UEs and applications using HIP sockets.

HIP deployment could be done in the following two phases.

Phase 1 (see Figure 51)

- Current tunneling options are used on S2a, S2b, S5, S8 (i.e., PMIP and GTP based options)
- HIP/IPsec overlay over existing tunneling options

Phase 2 (see Figure 52)

- Protocol architecture is simplified, standardized tunneling options are replaced by HIP/IPsec tunneling between GWs and between UE and GW
- For 3GPP-Access, still GTP tunneling is required between the first GW and the eNodeB.
- GTP is not required in case of eUTRAN-access, only in case of a completely flat architecture where the eNodeB is part of the gateway.

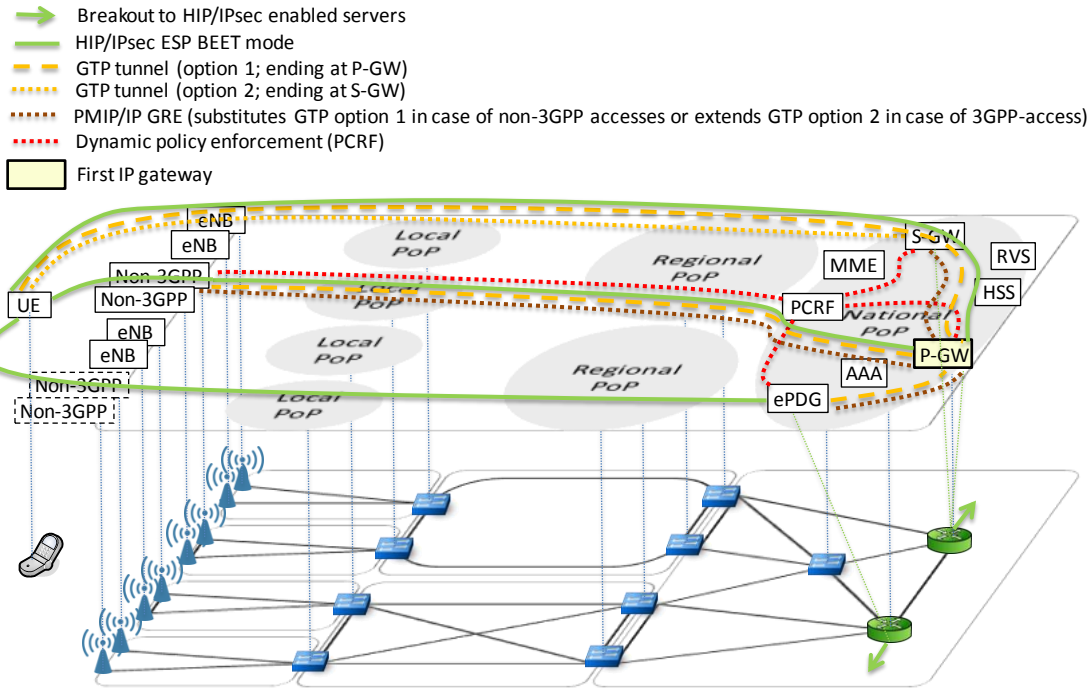



**Figure 51: HIP/IPsec overlay for applications using HIP sockets (Phase 1, centralized case)**

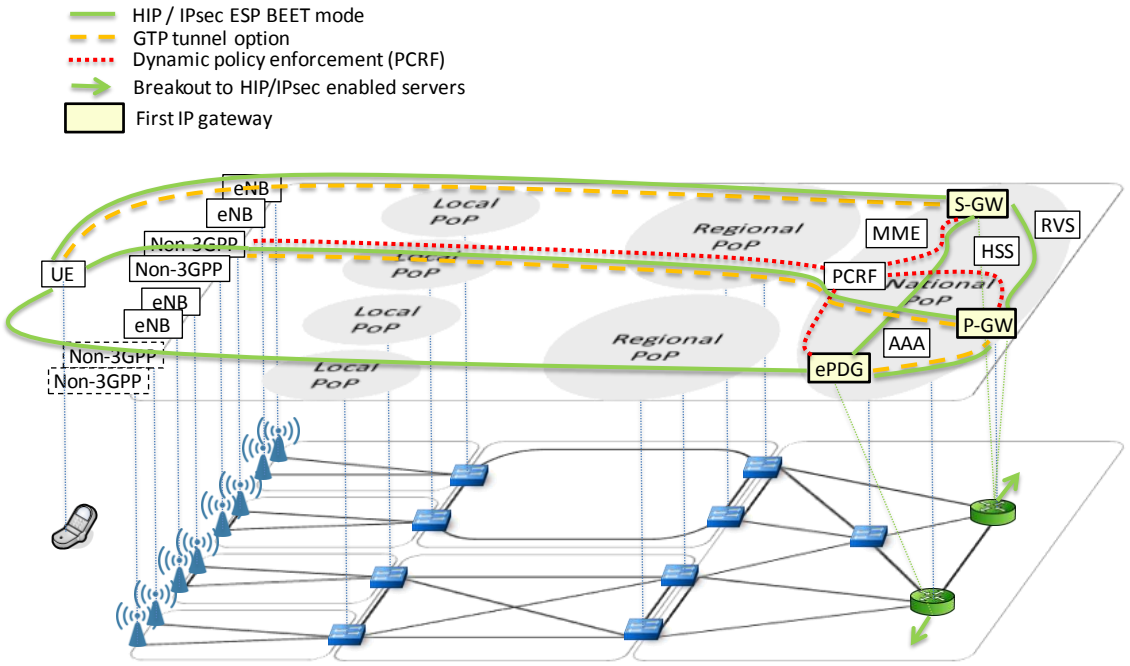



**Figure 52: HIP/IPsec overlay for applications using HIP sockets (Phase 2, centralized case)**

### 4.2.2 Distributed Architecture Option

The following figures show the distributed architecture option for HIP-enabled UEs and applications using HIP sockets. In phase 1 existing tunneling options could be used to provide IP connectivity for the UE (see Figure 53). In Phase 2 current tunneling options are replayed by HIP/IPsec tunneling (see Figure 54).

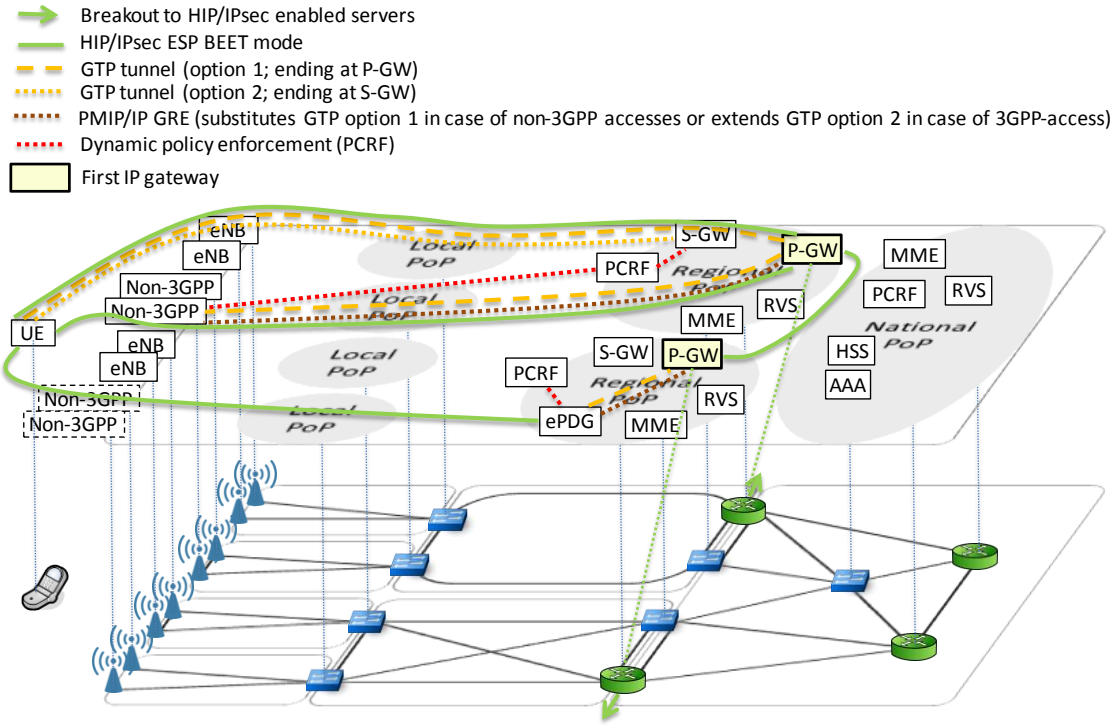



**Figure 53: HIP/IPsec overlay for applications using HIP sockets (Phase 1, distributed case)**

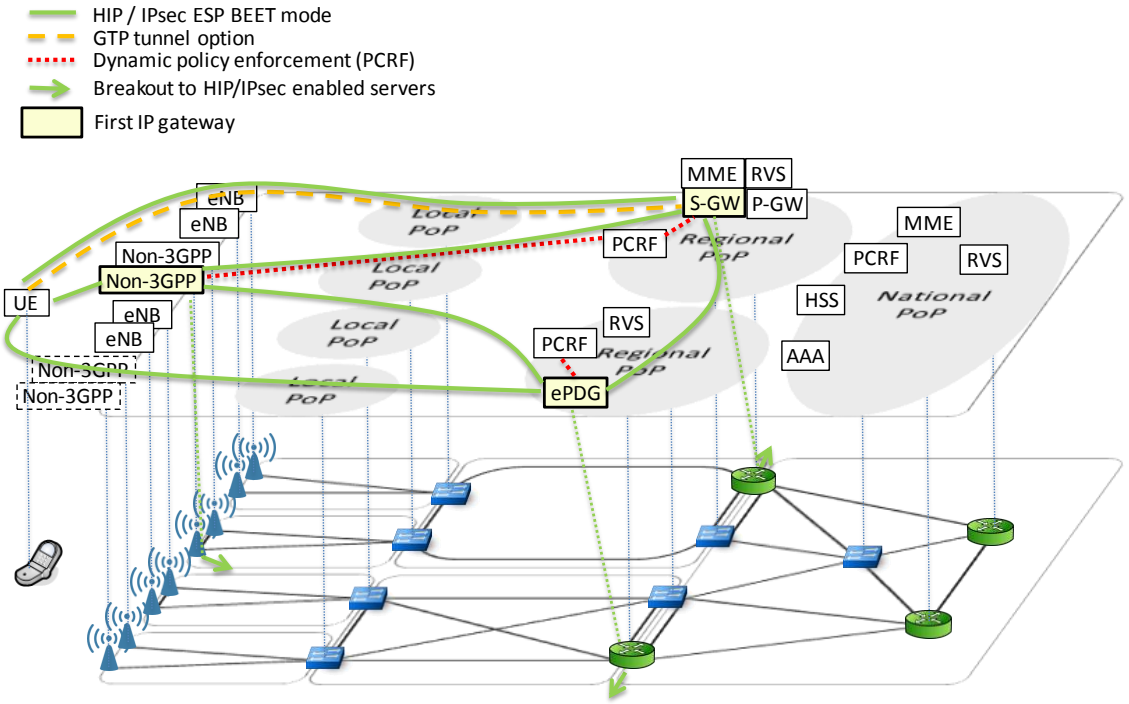



**Figure 54: HIP/IPsec overlay for applications using HIP sockets (Phase 2, distributed case)**

In a centralized only architecture DMA principles applied as GTP optimizations are not needed. If applying GW functions in the flat architecture in the eNodeB the proposed solutions may result in un-proportionally high signaling overhead. Hence GTP optimizations work best in a distributed architecture with distributed GWs, see Figure 54: Distributed GW deployment.

### 4.2.3 Flat Architecture Option

The following figures show the flat architecture option for HIP-enabled UEs and applications using HIP sockets. . In phase 1 existing tunneling options could be used to provide IP connectivity for the UE (see Figure 55). In Phase 2 current tunneling options are replayed by HIP/IPsec tunneling (see Figure 56).

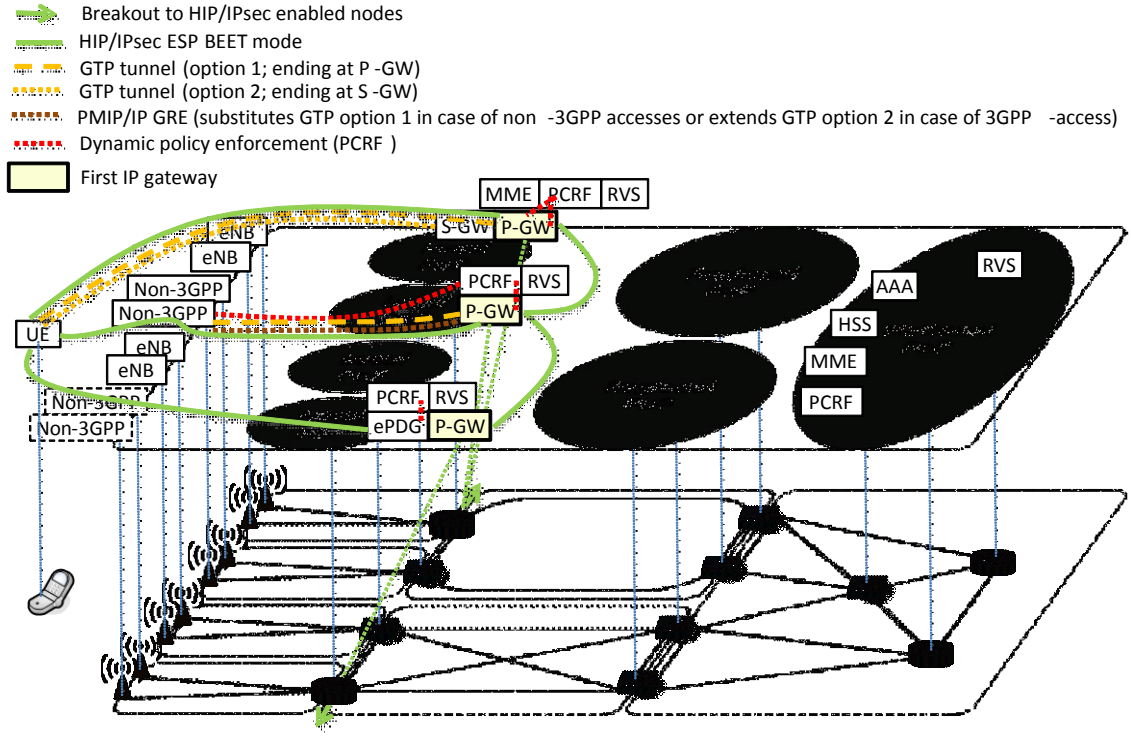



**Figure 55:HIP/IPsec overlay for applications using HIP sockets (Phase 1, flat case)**

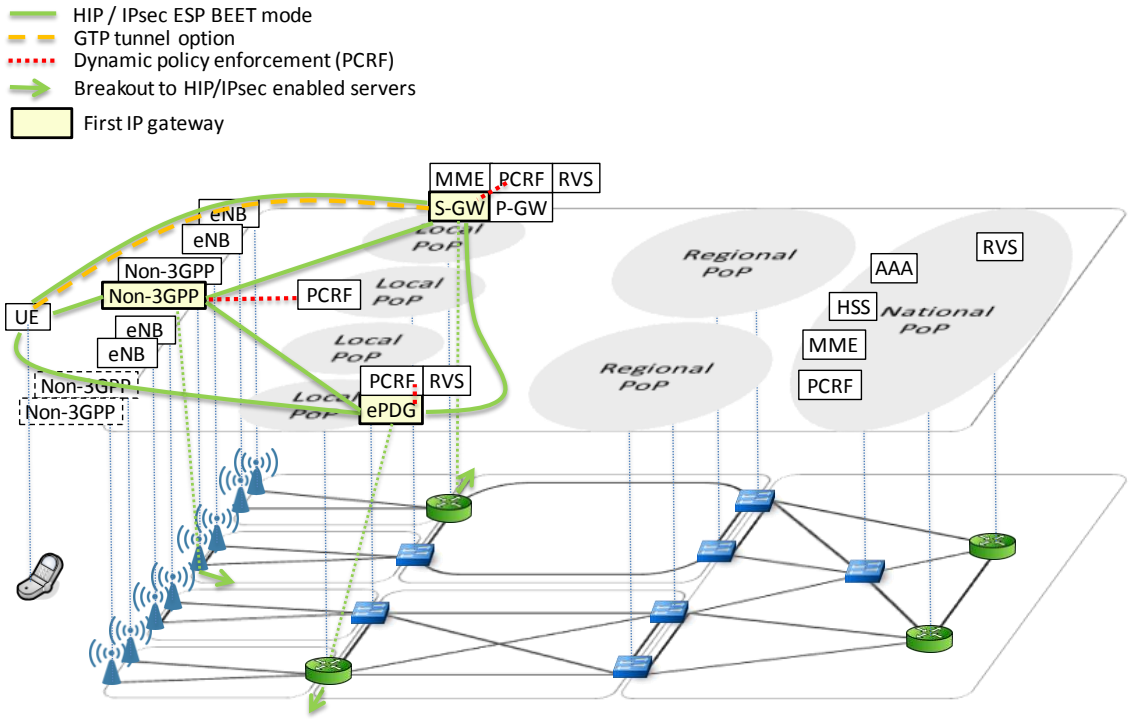



**Figure 56: HIP/IPsec overlay for applications using HIP sockets (Phase 2, flat case)**

The UFA flat architecture encompasses within the UFA_GW the EPC, the PCRF and the P-CSCF functions; in optimized manner.

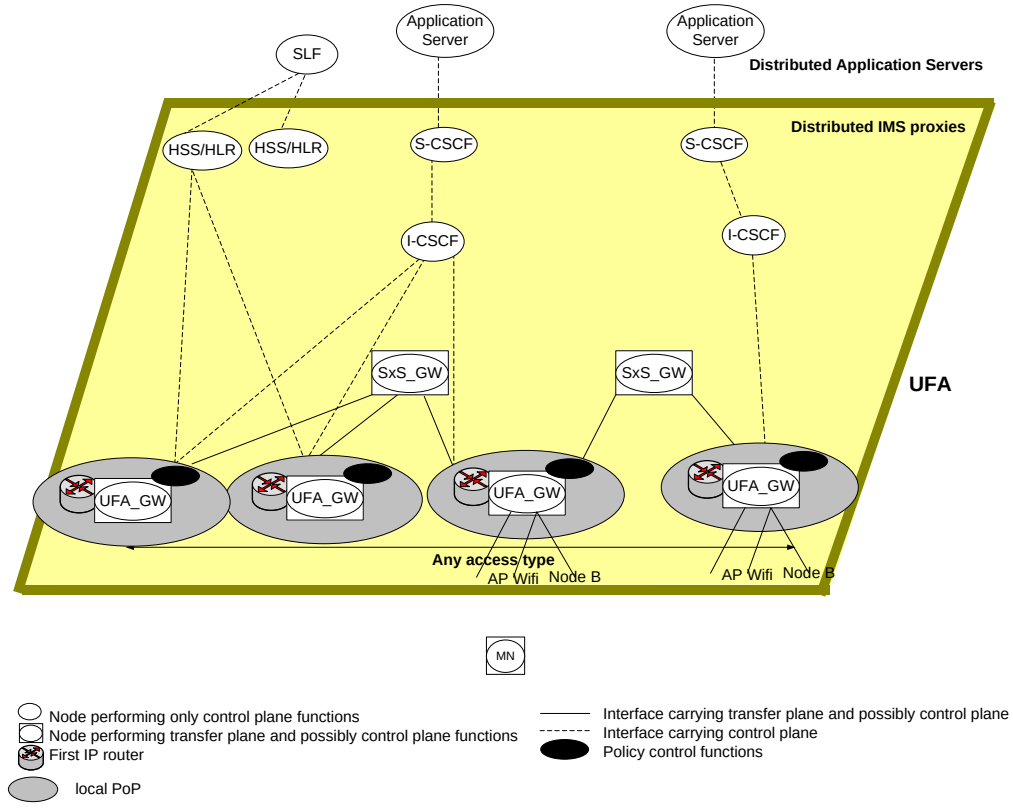



**Figure 57: UFA-SIP flat architecture**

## 4.3 Integration Issues of technologies in mobility management

This section presents the integration issues of WP2 mobility management technologies on top of the EPC transport architecture. In a nutshell, EPC is a part of the System Architecture Evolution (SAE) which is an evolutionary flat and all-IP architecture different from old GPRS Core networks. That support mobility between multiple heterogeneous access networks, including LTE, LTE Advance, 3GPP legacy systems and also non 3GPP systems too. Being all-IP compatible; EPC enables flexibility to integrate or extend the current technologies. In here, the challenges of integrating WP2 technologies for mobility management and the impact on current transport architecture are discussed. Below, the issues related to technologies are addresses in detail.

### 4.3.1 Terminal based mobility management

SCTP is a transport protocol that inherits most of its features from the most predominant reliable transport protocol on the Internet: the Transmission Control Protocol (TCP). The rationale for choosing SCTP as the transport protocol was its main features like multi-streaming and multi-homing. SCTP is to our knowledge the only transport layer protocol that actually supports a layer other than the application on top of it, and has a special field in its header that indicates the next protocol to receive the data. Other transport protocols like TCP and UDP do not provide this option and always assume that the next layer is the application layer.

Our implementation includes a new layer called the session layer above the transport layer. The main modules of this new session layer are as follows:

- The session layer abstraction module - provides a novel interface to the application layer that enables the two layers to interact and communicate with each other.
- The session layer protocol module - introduces the packet format of session messages and the protocol to be followed by the session layer when control messages need to be exchanged between the communicating peers.
- The state machine module - is the "brain" of the session layer as it interacts with all the other components, and keeps information about the session and its state at any given time.
- The mobility manager - is mainly responsible for receiving notifications about changes in the network interfaces, and contains all the intelligence to properly respond to these notifications, especially in dynamic mobile environments.

We plan to demonstrate session continuity whenever a mobility event occurs. For e.g. while changing between the different available access networks, network disconnections etc.

Our implementation does not have major integration issues with other technologies. It works equally well when combined with other technologies. Its performance is independent of the architecture selected as well. SCTP requires support on the UE or the application, and do not require modifications on the network side. Both the server and the client have to be modified to include the code for session layer and its modules. It can provide end-to-end anchorless mobility.

The only disadvantage of using SCTP is that it does not have universal support from the middle boxes and firewalls. A firewall can block or discard SCTP packets if the rules for SCTP on the firewall are not properly set.

### 4.3.2 Dynamic mobility anchoring

For the introduction of optimizations for more distributed and dynamic mobility anchoring emphasis was put on smooth integration into existing networks. This was the reason to base the technology on GTP what is widely used in today’s cellular networks.

Avoiding significant changes and implementation effort to existing 3GPP procedures to ensure backwards compatibility towards network deployments already in the field for selection of optimal P-GW location (preferably collocated with the S-GW) in order to have more optimal routing as the tunnels are terminated more close to the base station can be introduced by GTP enhancements with addition of new cause values (S11).

In general 3GPP has assured the coexistence of PMIP and GTP. The question of co-existence has to be looked more for the suggested technologies and concepts rather than looking for PMIP-GTP co-existence only.

PMIP-RO proposes tunnelling the traffic between MAGs (SGWs), bypassing the LMAs (PGWs) and traversing over an intermediate anchor (IA) developed for the PMIP protocol. DMA with GTP proposes to change PGWs using intelligence in the PGW or changing SGW for routing optimization.

The DMA proposals with PGW relocation may not coexist with PMIP-RO as they provide different solutions for the routing problem: The PMIP-RO solution provides tunnel modification while keeping the UE IP address, the other solution is to select IP (PDN) connections in the PGW for what a new IP address and service interruption may be acceptable from application point of view and force a reconnection that allocates a new more optimal PGW and new IP Address. It is clear that these are alternative solutions for optimal GW locations but can't be applied simultaneously.

The proposal to relocate the SGW to achieve maximal SGW-PGW collocation and optimal routing (DMA) could also coexist with PMIP-RO, if MAG changes are possible and may also result in MAG-LMA collocations.

In principle the NB-IFOM would not directly conflict the functionality of DMA with GTP, because NB-IFOM operates on the finer granularity (IP flow level) inside the single Packet Data Network (PDN) connection. It should be ensured that the potential anchoring point change (with DMA) is conformant with the all potentially related IFOM connections.

For the OpenFlow based EPC the approach even allows to introduce a new technology in part of the network without impacting the existing deployment i.e. the proposed approach is considered as gateway internal interface.

### 4.3.3 Routing optimization and support of moving networks in Proxy Mobile IPv6

PMIP-RO is an extension to current PMIPv6 procedure to control communications data paths within and/or outside the EPC, i.e., between MAGs and within the LMA's realm. This extension relies on the concept of intermediate data anchors (IAs) located throughout the EPC. In a network setup where MAGs are located in local PoPs and the LMA in a national PoP, the IA function could be located between (or inside) local or regional PoPs. The role of IA could be played by MAGs or intermediate LMAs or other specific hardware having routing capability. Knowing that the P-GW (where the LMA is generally located) has specific treatments to perform on flows (such as charging, lawful interception, or content filtering), it is expected that IAs are able to perform a subset, all, or additional services of what the P-GW is normally expected to be capable of.

The LMA through new signaling messages and for a given traffic characteristic is now able to change, update, or generate a specific data path after selection of one or several IAs. Because traffics are tunneled in the PMIPv6 domain, the resulting data path will be a succession of tunnels between MAGs and IAs. For example, the operator may want to redirect data traffic coming from sensors connected to specific MAG(s) to a specific IA for data aggregation reducing the treatment load at the LMA. In a vehicular scenario, two communicating vehicles along a highway could have their communications redirected to closer IA(s) to improve jitter . One IA could be used temporarily for a UE as data buffering close to the attached MAG in case of radio link disruptions.

The deployment of the technology requires modification of existing network elements and protocols. The PMIP's LMA daemon must be updated on P-GW(s) as well as PMIP's MAGs on RAN GWs (S-GW, ePDG, etc.). New network elements may need to be deployed as Intermediate Anchors. Furthermore, current operation of BBERF and PCRF may be extended to handle localized and optimized routing.

PMIP-RO relies on the distribution of data anchors throughout the network to localize and optimize data traffics. Hence, it is not best fitted for centralized deployments. PMIP-RO will benefit from distributed topologies, though there is a tradeoff to consider with the amount of signaling messages to maintain optimized routing paths during mobility.

PMIP-RO enables localized routing and traffic optimization within and/or outside of the EPC while keeping the LMA (located on the P-GW) as signaling anchor. This means that any protocols that may change or relocate the P-GW would affect negatively the performance of PMIP-RO. Hence, DMA with GTP should not be applied simultaneously to the same traffics. On the other hand, NB-IFOM is compliant with DSMIPv6, which is not compatible with PMIPv6. Therefore, PMIPv6 and DSMIPv6 (and by extension PMIP-RO and NB-IFOM) may co-exist if the network selects which of the two mobility management protocols would handle the PDN connection or the UE.

### 4.3.4 Flat and distributed mobility management

UFA-HIP technology introduces a new tunneling option between the UE and the first GW and between the GWs, using IPsec for user plane data transmission and HIP extended with signaling delegation services for access authorization and security association negotiation. Hence it is an alternative for other

tunneling options in 3GPP EPC, such as the GTP or PMIP-based tunnels on different interfaces, like S2b, S2c, S1 and S5. Annex 7 introduced several deployment options for UFA-HIP. In the first phase it could be implemented over any tunneling option providing IP connectivity to the UE, in the second phase the protocol architecture could be simplified.

Currently, 3GPP specifies two tunneling alternatives for UEs attaching via the E-UTRAN: GTP or GTP combined with PMIP/GRE on the S5 interface. In trusted non-3GPP access, GTP or PMIP/GRE tunnel are the standardized options between the Border Network Gateway (BNG) and the P-GW. In untrusted non-3GPP access, IKEv2/IPSec tunneling is used between UE and ePDG, and GTP or PMIP/GRE tunneling shall be used between the ePDG and the P-GW. In untrusted and trusted non-3GPP accesses, DSMIPv6 can be also used between UE and P-GW with IKEv2-based authentication and IP-in-IP tunnel establishment.

In the future EPC, HIP-based authentication and mobility combined with IPSec security tunneling could provide an additional tunneling option both for 3GPP and non-3GPP accesses. We envision that the change towards a HIP-based EPC architecture could take place in two phases. The first phase would include a parallel use of DSMIP/PMIP/GTP-based tunneling and the HIP-based UFA (UFA-HIP). The intra-GW handover and tunnel management would be handled by the existing IP tunneling services. However inter-GW handovers between P-GW, S-GW, ePDG, BNGs would be managed by the UFA-HIP solution by deploying the UFA-HIP technology in the P-GWs. This would cause an additional tunneling overhead but still several benefits from HIP/IPSec tunneling could be the followings: (1) uniform security over any access network, (2) service continuity (note: not seamless continuity) in case of inter-GW handovers, (3) support for legacy application that do not implement mobility nor security, and finally (4) support of coexistence of IPv4 and IPv6 network segments, transparent for UEs and applications becomes possible due to HIP.

In the second phase, the protocol architecture could be further simplified, and standardized tunneling options would be replaced HIP/IPsec tunneling both between GWs and between UEs and GWs. For 3GPP-Access GTP tunneling would be still required between the first GW and the eNodeB, but not required in case of non-3GPP accesses. The added value of this phase is the support of seamless inter- and intra-GW handovers due to HIP mobility, multihoming and UFA-HIP based inter-GW mobility service .

### 4.3.5 User Access Authentication and Authorization

HIP DEX-AKA user authentication could be deployed as an alternate option to IKEv2 EAP-AKA used over SWu in Untrusted Non-3GPP IP Access. HIP DEX-AKA could provide an option for the Network Access Service in use cases where the UEs are highly resource-constrained devices. Other HIP-based alternatives should be considered for normal UEs, smart phones, e.g., HIP BEX extended with EPS-AKA authentication.

### 4.3.6 Mobile Relaying in Heterogeneous Networks

The mobile relaying in heterogeneous networks considers the throughput enhancements of mobile edge users experiencing low signal quality levels. In this architecture, by increasing the number of possible interfaces to connect to, the UEs may connect to most advantageous interface such as relay-users, Wi-Fi Access Points (APs) or to base stations (BSs). This connection decision based on the access network quality and availability is done by the network operator itself. The core network elements such as Wi-Fi controller and S-GW collects the interface qualities of Wi-Fi APs and relay-user access links and the decision is based on the MME's feedback into the radio access network (RAN).

Regarding the integration issues with other technologies, the mobile relaying in heterogeneous network architecture does not require significant enhancements to the existing 3GPP-IP access technology. Considering compatibility issue for hardware level, the only one new element deployed in the core network is Wi-Fi controller which collects quality indicator between users and access points and sends them to MME. Considering compatibility issue for protocol level, Since the proposed cooperative user-relay assisted communication technology considers on the co-existence and mobility management with heterogeneous access technologies, the signaling increases. Firstly, the cooperative behaviors are required in the 3GPP handsets in such a way that the channel quality indicator between the cooperative users is required to fed back to BS. In order to reduce this signaling, the users in a certain distance cooperate each other. Moreover, there is one more signaling issue regarding to declaration of the decision to the users. At the end of the proposed procedure, based on the network operators' decision, the interface selection will be enforced by the core network (by gateways such as MME (Mobility Management Entity)) through the users experiencing lower capacity.

# 5. Future research directions of Mobility Management in heterogeneous networks

There is a growing expectation among the subscribers that they should be able to access the internet and the services wherever they move. In a nutshell it implies the requirements for advanced mobility management. However, during the past decade there was a tendency towards the flat and distributed architecture in general. Distributed and flat architectures became popular due to transparency, openness, reliability, performance and scalability. In the other hand, centralized architectures seem to be a single point of failure even though it is still used by many operators all over the world. A major reason to this is the network restructuring cost. Distribution of network functions need relocation of the network close to the provider edges. That, in turn, improves the quality of service by guaranteeing the minimum handover delay, packet loss, jitter, and etc. In terms of mobility management flat or distributed architecture make sure the mobility related network functions and elements are relocated close to the subscribers. Therefore, the events do not have to be processed in a centralized system which is several hops away from the subscriber.

In the scope of MEVICO we have studied new directions of mobility management that are the enablers of virtualization and cloudification in modern networks. The concept of small cells which in turn the best clue to growing number of subscribers was a major focus in WP2. For example, a base station can handle only a limited number of handsets at a time. Thus, deployment of small cells found beneficial in many aspects, such as reduced maintenance and deployment cost, better coverage, scalability, and reliability. Smaller the cell size the networks must be capable of efficient handling of transition between the cells, such as session continuity, resource allocation, policy management, and location management. Later on, concept of network virtualization became popular among the operators due to the combination of network resources with the networks functionalities into a single software based administrative domain. This concept brought mobility management into a new virtual layer. However, managing mobility services in a virtual domain is best suited in cloud-based deployments. Today, after the removal of mainframes, client/server and internet computing, virtualized applications are placed in clouds by enabling the accessibility for mobile subscribers.

In order to address the simultaneous needs for mobility, security, and virtualization the concept of Software Defined Networks (SDN) was introduced. In MEVICO context we have investigated the impact of SDN with OpenFlow concepts. The fundamental concept of SDN is to separate the control and data planes of the network by providing interfaces and thousands of APIs to provision the services in the network using the external systems. In other words it disaggregates the traditional vertically integrated networking stacks to improve performances in specialized environments. However, SDN does not currently include the mobility management. Thus, the network controller must be improved to handle the mobility related functions.

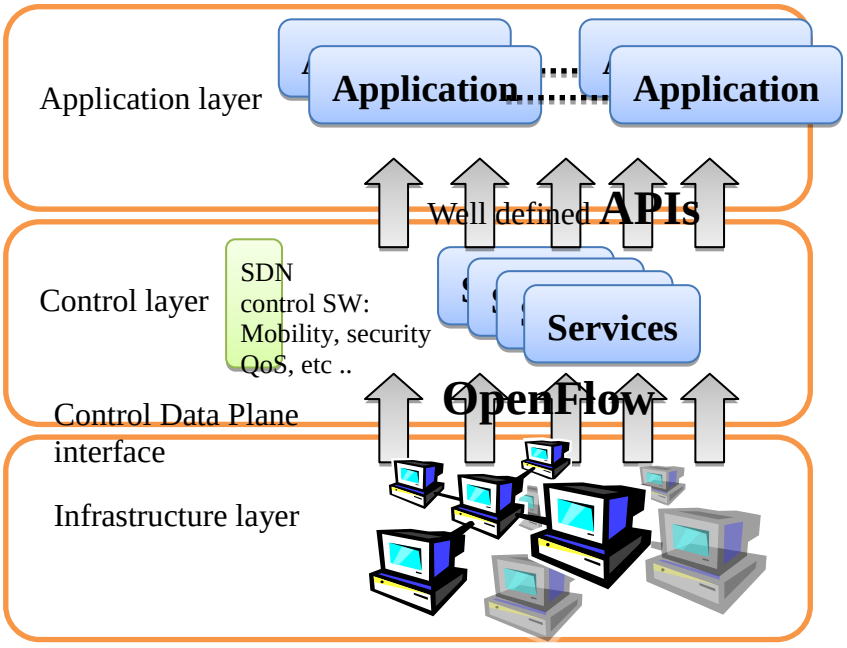



**Figure 60: SDN architecture.**

Therefore one of the demanding researches would be to study the mobility management in virtual networks in general. Specifically, the design concept of SDN controller must be reinvestigated to make sure that it provides the demanding requirements in mobility management (for example: investigating the ability to relocate and co-locate the 3GPP functional elements and their functions.

| **Partner specific technology** | **Future research directions** |
|---|---|
| 1. Terminal-based mobility management | As future work, session layer mobility extension for SCTP can be integrated into mobile devices. As a first step, performance tests on mobile phones need to be conducted since smart phones and mobile devices have limited performance and efficiency in comparison to laptops. The mobility extensions are now implemented in the user space. In future, these changes can be integrated into the kernel so that there will not be need for extra buffers and hence no extra delays. |
| 2. Improving UE's multiple network access capability and load balancing through Wi-fi offloading | Operator managed Wi-Fi technique is now available as a product offering from several vendors. Future work will be to further develop functionalities so it will be a full-fledged Access Point in a HetNet solution. Areas for future work could be e.g. Seamless handover, Wi-Fi <-> Wi-Fi handover, Forced handover, voice call. |
| 3. Functional and performance validation of PMIPv6 with NEMO support and PMIPv6 Route optimization | Current standardized mobility management protocols assume that the managing entity (HA or LMA for instance) is the IP anchor of attributed IP addresses. In a cloud environment where the managing entity is decoupled from the forwarding entities, this assumption may be challenged. Proposing alternative solutions without this assumption may lead to more optimized routing paths and performance. |
| 4. Flat or distributed mobility management using HIP-based Ultra Flat Architecture (UFA-HIP technology) | Possible future work is to implement HIP delegation services in a real prototype, e.g., extension of the infraHIP implementation. An interesting task would be to investigate the performance and integration issues of UFA-HIP in case of deploying it on the top of Openflow-based transport network. |
| 5. Lightweight user authentication using HIP DEX-AKA | Possible future work for HIP DEX-AKA method is 1) to involve the AAA proxies and server in the process of getting the authentication vectors from the HSS to decrease the load on the HSS, 2) extend the prototype with security policy database and security association management. |

# 6. References


[1] CELTIC/MEVICO D2.1; "Advanced EPC architecture for smart traffic steering"; November 2011.

[2] CELTIC/MEVICO D2.1; "Final Evaluation Report", October 2012.

[3] K.Daoud, P.Herbelin, K.Guillouard, N.Crespi, "Performance and implementation of UFA: A SIP-based Ultra Flat Architecture Mobile Network Architecture", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2009.

[4] K.Daoud, K.Guillouard, P.Herbelin, N.Crespi, "A Network-Controlled Architecture for SCTP Hard Handover", in proceedings of Vehicular Technology Conference (VTC-fall), 2010.

[5] 3GPP, "IP Multimedia Subsystem (IMS)", TS 23.228, Release 9.

[6] 3GPP, "Policy Control and charging architecture", TS 23.203, Release 9.

[7] 3GPP, "IP Multimedia Subsystem (IMS) Service Continuity", TS 23.237, Release 9.

[8] 3GPP, "Access security for IP-based services", TS 33.203, Release 9.

[9] IETF, "Stream Control Transmission Protocol", RFC 4960.

[10] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner: ―OpenFlow: Enabling Innovation in Campus Networks ACM SIGCOMM Computer Communication Review 69 Volume 38, Number 2, April 2008

[11] IEEE, IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover, IEEE Std 802.21-2008 (Jan. 2009).

[12] László Bokor, Zoltán Faigl, Sándor Imre, A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture., in Proceedings of the 2nd International Workshop on Security and Communication Networks. Karlstad, Sweden, May 26-28, 2010.

[13] T. Heer, S. Varjonen, "Host Identity Protocol Certificates", RFC 6253, May 2011.

[14] J. Melen et al., "Host Identity Protocol-based Mobile Router (HIPMR)," IETF Draft, May 2009

[15] P. Nikander and J. Arkko, "Delegation of Signalling Rights," in Security Protools, ser. Lecture Notes in Computer Science, B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, Eds. Springer, 2004, vol. 2845, pp. 575–586.

[16] P. Nikander et al., "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206. April 2008.

[17] T. Henderson, P. Nikander, M. Komu, "Using the Host Identity Protocol with Legacy Applications", RFC 5338, September 2008.

[18] T. Henderson, A. Gurtov, "The Host Identity Protocol (HIP) Experiment Report", RFC 6538, March 2012

[19] J. Melen, J. Ylitalo, P. Salmela, "Host Identity Protocol-based Mobile Proxy", August 2009.

[20] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", RFC5213, August 2008.

[21] 3GPP, "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3", TS 29.275, Release 10.

[22] InvestorPlace, "AT&T: Data-Only Plans Are 'Invevitable'", Article Web: http://www.investorplace.com/2012/06/att-data-only-plans-are-invevitable/

[23] M. Boc, C. Janneteau, A. Petrescu, "RO Extensions for PMIPv6-LR (ROEXT)", Internet draft, July 2011.

[24] S. Krishnan, R. Koodli, P. Loureiro, Q. Wu, A. Dutta, "Localized Routing for Proxy Mobile IPv6", IETF RFC6705,.

[25] Mongazon-Cazavet, "TCP Rehash draft-mongazon-tcpm-tcp-rehash-00"

[26] CELTIC/MEVICO D3.2; "Innovative Solutions for Mobile Backhaul"; December 2012.

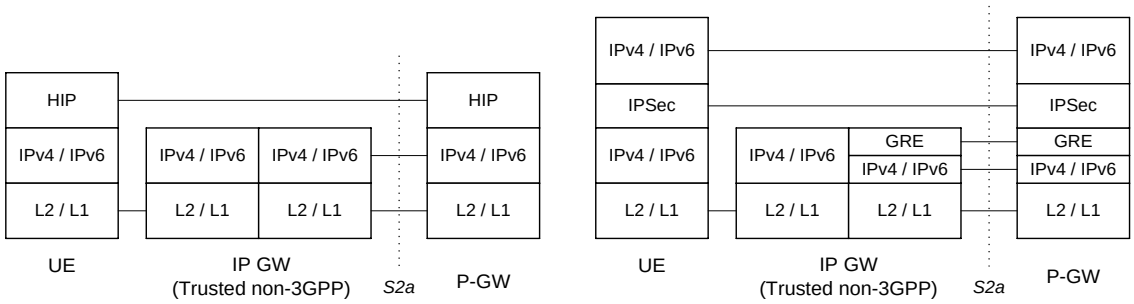
[27] CELTIC/MEVICO D1.4; "Architecture Design Release 3 Documentation"; December 2012.

# 7. Appendix A – Deployment of UFA-HIP

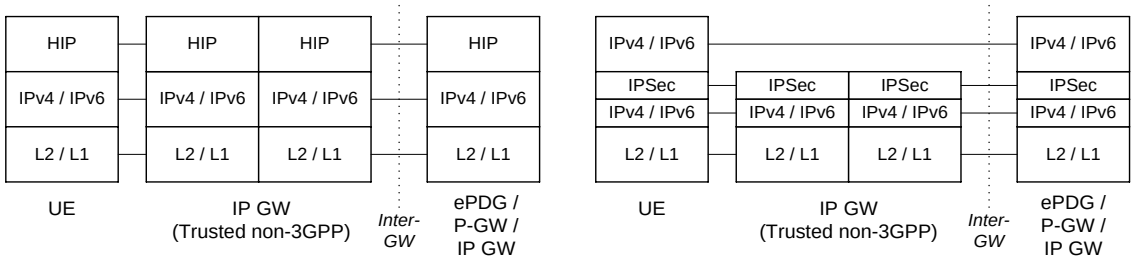
This section describes the effects on the protocol stack by the deployment of UFA-HIP in the future mobile networks. The deployment is anticipated to take place in two phases: Phase 1, short-term deployment, and Phase 2, long-term deployment. In the figures below, control plane is depicted on the left hand side and user plane on the right hand side. The interface denoted as "Inter-GW" refers to the interface between elements P-GW, S-GW, ePDG, and an IP gateway in a trusted non-3GPP access network or outside the core network. Inter-GW covers the interfaces S2a, S2b, S5, S8, and Gx.

## 7.1 Trusted Non-3GPP Access

**Phase 1**

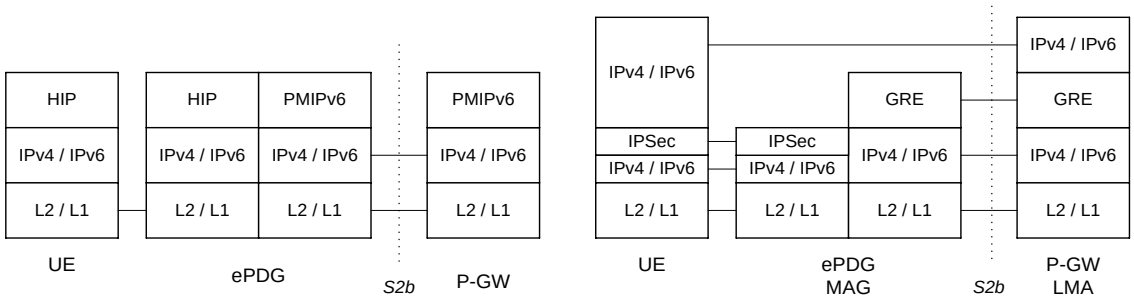



**Phase 2**

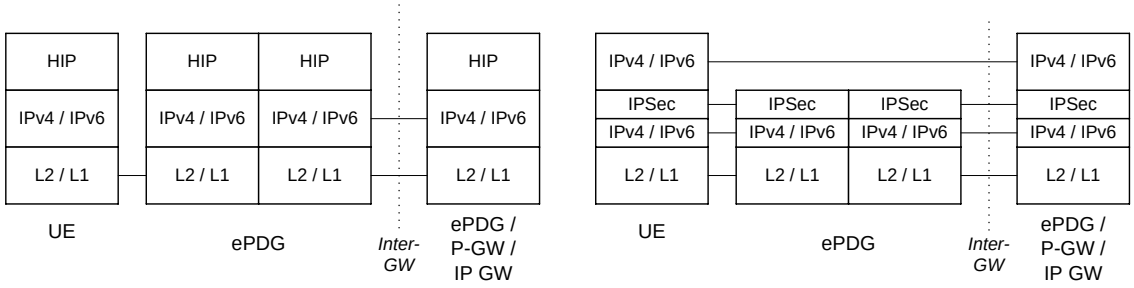



## 7.2 Untrusted Non-3GPP Access

**Phase 1**

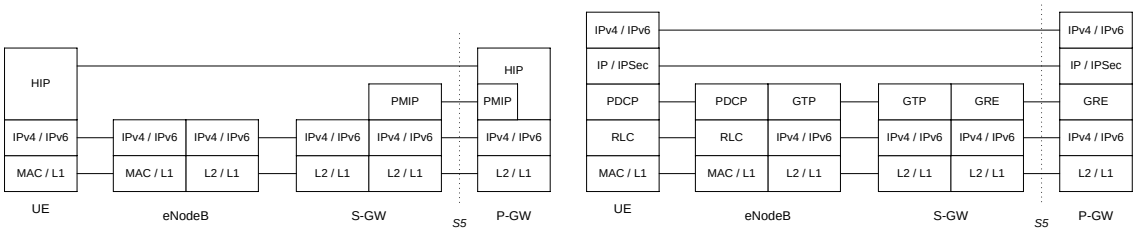


**Phase 2**

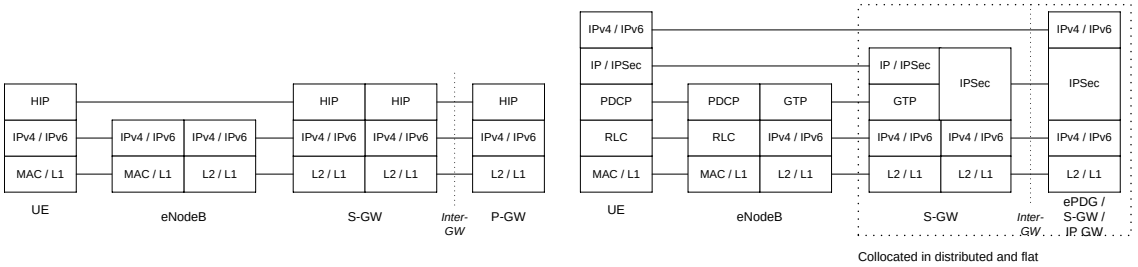



## 7.3 3GPP E-UTRAN Access

**Phase 1**




**Phase 2**




**Ultra Flat Option**