IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks

Antonio de la Oliva*, Carlos J. Bernardos*, Maria Calderon*, Telemaco Melia† and Juan Carlos Zuniga‡
*Universidad Carlos III de Madrid, E-mail: {aoliva,cjbc,maria}@it.uc3m.es
†Alcatel-Lucent Bell Labs, E-mail: telemaco.melia@alcatel-lucent.com
‡InterDigital LLC., E-mail: JuanCarlos.Zuniga@InterDigital.com

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

I. Introduction and Motivation

In the past few years we have been witnessing an extraordinary data explosion over cellular networks. Telecom operators have been carefully monitoring the disconnection between the Average Revenue Per User (ARPU) and the associated Cash Costs Per User (CCPU) and, despite the remarkable volume increase of broadband data over mobile networks, the mobile data revenue is falling fast.

There are a number of reasons for such disconnection between data explosion and revenue growth, including among others, terminal subsidies, marketing and sales costs, new services and new content creation, staled data plans and tariffs, network capacity or network coverage, and management. In the context of network operational expenditure cost, efficient technology solutions seem to be the most promising approaches. Smaller installation footprints, reduced power consumption and transmission costs, efficient use of multi-radio bandwidth, simplified network management, reliable and cost effective coverage are just examples of the plethora of existing solutions.

Presently, the typical scenario is a user equipped with a dual mode mobile phone (e.g., integrating 3G/4G and WiFi radio devices) attaching to the available networks either sequentially or simultaneously. The latter case is commonly referred as multi-homing case, that is, the user can receive data over different networks (WiFi or 3G/4G) simultaneously.

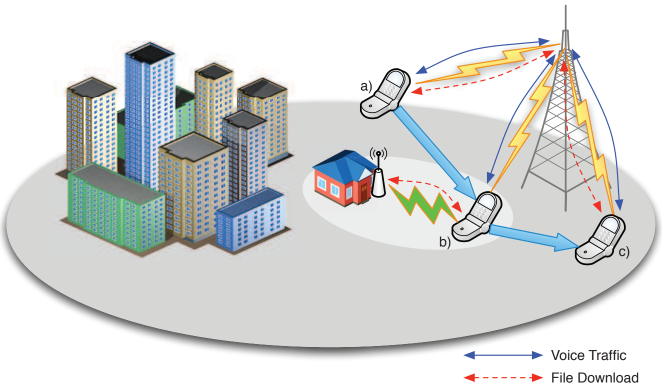


Fig. 1. 3G offload example scenario

In this work, starting from the above considerations, we focus on an emerging technology, referred hereafter as IP flow mobility. This technology allows a Telecom operator to seamlessly and selectively switch over a single IP flow (e.g., user application) to a different radio access, while keeping all other ongoing connections for this and the rest of the users on both radio accesses untouched. The technology is currently being standardized in the IETF and it has been adopted by 3GPP as technique for seamless 3G offload. Fig. 1 shows an example of this kind of scenario. Suppose a user is attached to a 3GPP base station (NodeB) and he is having several simultaneous flows, e.g., a voice call and a file download, as shown in the case *a)* of Fig. 1. At some point of time, the user gets home. The terminal or the network, upon detection of the availability of the WLAN access, decides to offload the file download traffic (i.e., best-effort traffic) to the WLAN access, to alleviate congestion in the 3GPP access and/or in order to provide the user with a faster download experience – as shown in case *b)* of Fig. 1. Once the user leaves home (therefore going out of the WLAN access coverage), the file download flow is seamlessly moved back to the 3GPP network, as depicted in the case *c)* of Fig. 1, to keep the ongoing communications.

IP flow mobility technology has the following key advantages: *i)* it allows the user to enjoy high bandwidth connections in the proximity of WLAN hotspots while being always

The research of Antonio de la Oliva, Carlos J. Bernardos and Telemaco Melia has been partially funded by the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project). Carlos J. Bernardos and Maria Calderon have been also partially funded by the Ministry of Science and Innovation of Spain under the QUARTET project (TIN2009-13992-C02-01)

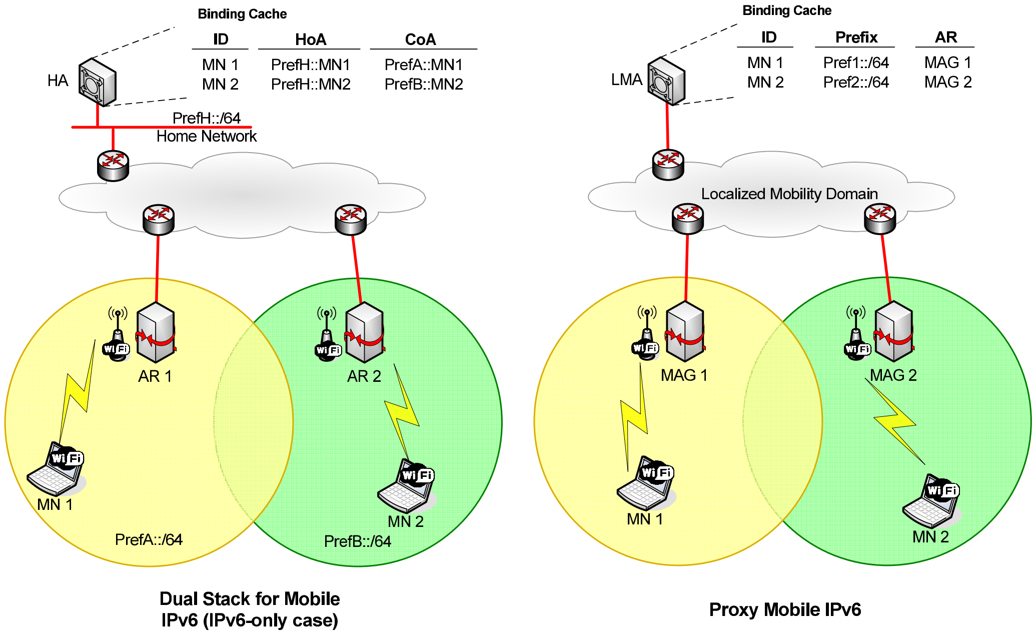


Fig. 2. Dual Stack for MIPv6 and PMIPv6 overview

reachable from the Internet, *ii)* it allows the operator to manage the bandwidth in the presence of greedy user connections, and *iii)* it allows the operator to provide different levels of service by applying different policies for different users, tariffs and specific traffic types evolving from a simple pipe provider to a high leverage network provider. The access and core networks are therefore capable of classifying data traffic traversing their nodes and, in agreement with the mobile devices, can apply policies to deliver the best Quality of Experience (QoE) possible. Note that traffic redirection always introduces some kind of delay, due to processing, forwarding and the difference in Round Trip Time (RTT) between the different accesses. Nevertheless, the solutions being investigated at the 3GPP do not consider the redirection of real-time or delay sensitive traffic, such as real-time video or voice. Offloading traffic to the non-3GPP access is currently considered only for non-critical traffic such as bulk downloads, non real-time video or P2P traffic.

This article analyzes and compares two possible approaches to IP flow mobility, namely client-based and network-based IP flow mobility. The former relies on an IP host centric solution introducing a mobility client in the host and a mobility agent in the core network (Section II). The latter relocates the IP mobility client functionality from the host to the network thus making the mobile device agnostic to any IP mobility signaling (Section III). The article summarizes the key functional boxes and associated protocol operations and discusses the pros and cons of each solution. The paper also generalizes the adoption of network-based solutions in the context of 3GPP and the use of alternative network-based mobility protocols like the GPRS Tunneling Protocol (GTP).

II. Flow Mobility in Client Based IP Mobility

Client-based IP mobility solutions require the user terminal to be involved in the management of the mobility, by running a specialized stack that is able to detect, signal and react upon changes of point of attachment. Dual Stack for Mobile IPv6 [1] is standardized by the IETF to provide client-based IP mobility support.

A. Dual Stack for Mobile IPv6

The Mobile IPv6 Support for Dual Stack Hosts and Routers specification [1] – also known as DSMIPv6 – is based on Mobile IPv6 (MIPv6) [2], extending its basic functionality to also support dual stack IPv4/IPv6 scenarios. Mobile IPv6 (MIPv6) [2] enables global reachability and session continuity by introducing the Home Agent (HA), an entity located at the Home Network of the Mobile Node (MN) which anchors the permanent IP address used by the MN, called Home Address (HoA). The HA (see Fig. 2) is in charge of defending the MN's HoA when the MN is not at home, and redirecting received traffic to the MN's current location. When away from its home network, the MN acquires a temporal IP address from the visited network – called Care-of Address (CoA) – and informs the HA about its current location. An IP bi-directional tunnel between the MN and the HA is then used to redirect traffic from and to the MN. There is also optional support to avoid this suboptimal routing and enable the MN to directly exchange traffic with its communication peers – called Correspondent Nodes (CNs) – without traversing the HA. This additional support is called Route Optimization (RO), and allows the MN to also inform a CN about its current location.

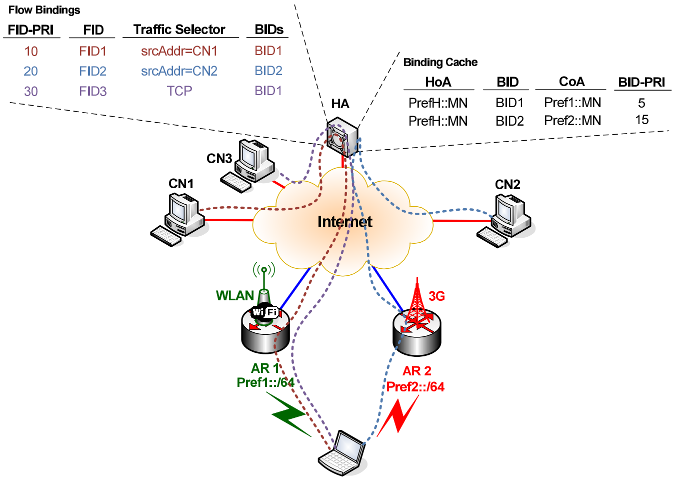
DSMIPv6 extensions add to basic Mobile IPv6 the capabilities required to support the registration of IPv4 addresses and the transport of both IPv4 and IPv6 packets over the tunnel with the HA. These extensions also enable the mobile node to roam between IPv4 and IPv6 access networks.

B. Flow mobility extensions for Mobile IPv6

The basic Mobile IPv6 specification and the extensions defined to enable IPv4 operation provide a very limited multi-homing support, as each permanent address (home address) can only be associated to a single temporal address (care-of address). Therefore, the only possible scenario in which a mobile node can use more than one care-of address simultaneously is that in which the node is using different home addresses (one per care-of address). This limits the scope and usability of this basic solution as it prevents different flows to be routed to different care-of addresses, and consequently, does not support a scenario in which a mobile node is reachable – via a single home address – through different physical interfaces.

In order to enable flow mobility in a client-based mobile IP context, the IETF has standardized the basic components that are required. These components are: *i)* multiple care-of address registration support, *ii)* flow bindings support, and *iii)* traffic selectors definition. We next explain in further detail how each one of these pieces works, pointing out the basic functionality they provide and how each component fits in the overall flow mobility solution.

Basic Mobile IPv6 protocols provide the tools to bind a home address to a single care-of address. Since flow mobility requires the ability of receiving traffic destined to the same home address via different care-of addresses, Mobile IPv6 needed to be extended to support the registration of several care-of addresses with the same home address. This is the purpose of the Multiple Care-of Addresses Registration extensions, standardized in the RFC 5648 [3]. These extensions allow a mobile node to register multiple care-of addresses for a home address and create multiple binding cache entries. In order to do so, the Binding Update (BU) message defined by Mobile IPv6 is extended with a new mobility option used to carry a care-of address and a number to uniquely identify the binding entry, called Binding Identification (BID) number. A mobile node can include a number of these new mobility options in the BU message, triggering the creation of multiple binding cache entries in the home agent, each of them identified by the respective BID. Note that the binding cache and binding update list structures are also extended to support the multiple care-of address registration. Fig. 3 shows with an example how the flow mobility extensions for mobile IPv6 work. A mobile node (MN) – identified by its home address `PrefH::MN` – is simultaneously attached to two different heterogeneous access networks (WLAN and 3G), therefore configuring two care-of addresses (`Pref1::MN` and `Pref2::MN`). Thanks to the use of the multiple care-of addresses registration extension, the MN is able to register its two care-of addresses at the home agent. Note that although we are always referring to the registration at the home agent in this example (and in the explanation of the different extensions), the protocols are also defined for its use in the registration with correspondent nodes.



Flow Bindings

FID-PRI	FID	Traffic Selector	BIDs
10	FID1	srcAddr=CN1	BID1
20	FID2	srcAddr=CN2	BID2
30	FID3	TCP	BID1

Binding Cache

HoA	BID	CoA	BID-PRI
PrefH::MN	BID1	Pref1::MN	5
PrefH::MN	BID2	Pref2::MN	15

Fig. 3. Overview of the flow mobility extensions for Mobile IPv6

In addition to the capability of associating a single home address with multiple care-of addresses, the ability to use and control them simultaneously is required. This is the goal of the second set of extensions, the Flow Bindings in Mobile IPv6 and NEMO Basic Support – standardized in RFC 6088 [4] – which allows mobile nodes to bind one or more IP flows to a specific care-of address. With this extension, a mobile node can instruct the home agent (or the correspondent node) how to route inbound packets (i.e., to which care-of address packets of a specific flow should be sent). Note that the mobile node also needs to have support to be able to route outbound packets via different care-of addresses, being that packet forwarding coherent with the inbound policy signaled by the mobile node. The flow bindings specification basically defines a set of Mobile IPv6 options and sub-options allowing the mobile node to associate a particular IP flow (which is also assigned a Flow Identifier, called FID) with a particular care-of address (identified by its BID). These bindings between IP flows and entries in the binding cache are stored in a different conceptual list, that is looked up in order to determine which entry of the binding cache has to be used to forward a data packet (see Fig. 3). This list basically includes the FID, a traffic selector that is used to assign packets to flows (i.e., a flow is defined as a group of packets matching a traffic selector), and a FID priority (FID-PRI) – used to break the tie between overlapping flow bindings. Note that a lower FID-PRI number indicates a higher priority.

The last above-mentioned extension required to enable IP flow mobility is the definition of traffic selectors for flow bindings, standardized in RFC 6089 [5]. This extension basically defines binary formats for IP traffic selectors to be used in conjunction with the flow binding extensions, so IP flows can be identified according to different criteria, such as: Source Address, Destination Address, IPsec SPI (Security Parameter Index) value [6], Flow Label, Source Port, Destination Port, Traffic Class or type of Next Header. A flow can be identified by any subset of these parameters or by specifying a range of values for each one, hence identifying several flows at the same time.

If we refer back to the example shown in Fig. 3, the use of the IP flow mobility extensions allows for example to influence which data path is followed by the different traffic that the mobile node is sending/receiving. In this example, any traffic sent by CN1 is forwarded by the home agent to the care-of address that the mobile node has configured from the WLAN access. Traffic sent by CN2 is similarly received by the mobile node via its 3G interface. Any TCP traffic not sent by CN1 or CN2 is received via WLAN (note here the use of the FID-PRI). Finally, any traffic not matching any of these rules is forwarded by the home agent to the WLAN interface of the mobile node, as indicated by the binding cache entry with the highest order BID priority (BID-PRI). Note that a lower BID-PRI number indicates a higher priority.

In addition to these basic protocol components, complementary support might be needed to deploy a complete IP flow mobility solution in an operator's network, such as a framework to transport policies from the operator to the mobile node. The Access Network Discovery and Selection Function (ANDSF) framework defined by the 3GPP, or the Policy and Charging Control (PCC) support can be used/extended for that purpose, as briefly discussed in Section IV.

III. Flow mobility in Network Based IP mobility

Network-based IP mobility solutions locate the mobility management control of the terminal in the network. In this way, the terminal is not required to perform any kind of signaling (e.g., binding updates) to react upon changes of its point of attachment to the network, being these changes transparent for the mobile terminal IP protocol stack. Proxy Mobile IPv6 (PMIPv6) is the protocol standardized by the IETF to provide network-based IP mobility support. Although this protocol provides basic multi-interface functionality, in its current state it is not able to provide full flow mobility granularity, hence extensions to support it are required and are being standardized at the IETF NETEXT WG [7].

A. Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) [8] is a network-based mobility management protocol. This means that the MNs are provided with mobility support without their involvement in the mobility management and IP signaling, as the required functionality is relocated from the MN to the network. In particular, movement detection and signaling operations are performed by a new functional entity – called Mobile Access Gateway (MAG) – which usually resides on the Access Router for the MN (see Fig. 2). In a Localized Mobility Domain (LMD), which is the area where the network provides mobility support, there are multiple MAGs. The MAG learns through standard terminal operation, such as router and neighbor discovery or by means of link-layer support, about an MN's movement and coordinates routing state updates without any mobility specific support from the terminal. The IP prefixes (Home Network Prefixes) used by MNs within an LMD are anchored at an entity called Local Mobility Anchor (LMA), which plays the role of local HA of the LMD. Bi-directional tunnels between the LMA and the MAGs are set up, so the MN is enabled to keep the originally assigned IP address despite its location changes within the LMD. Through the intervention of the LMA, packets addressed to the MN are tunneled to the appropriate MAG within the LMD, making hence the MN oblivious of its own mobility.

As previously explained, the standard PMIPv6 protocol allows basic multi-homing capabilities, that is, the MN is able to attach to the network using multiple interfaces. In the current specification, for each of the attachments the LMA creates a different mobility session and can provide one or several home network prefixes (HNP) to each interface. The basic functionality provided by PMIPv6 enables the LMA to move the complete set of prefixes associated to one interface to another, but it does not support the movement of an arbitrary number of prefixes from one interface to other (i.e., not the complete set) or just a single IP flow identified by any other mechanism different from the prefix used at the MN to route the flow. In order to support full flow mobility granularity, the PMIPv6 protocol must be extended to: *i)* span one mobility session across multiple MN interfaces, *ii)* allow the MN to configure the same home network prefixes on multiple interfaces and *iii)* transfer the policies between the MN and the network to install the required filters in the LMA/MAG for flow routing.

In the following section we analyze how each of these issues is being addressed in the current standardization efforts.

B. Flow mobility extensions for Proxy Mobile IPv6

Although the basic specification of PMIPv6 provides limited multihoming support to multimode devices, it does not include the ability to move selected flows from one access technology to another. This functionality is currently being developed by the IETF NETEXT WG[1] as described in [7]. The rest of this section focuses on the description of the key concepts behind the flow mobility support for PMIPv6.

Flow mobility assumes simultaneous connection to the same PMIPv6 domain through different interfaces. The simultaneous use of different attachments to the network increases the complexity of the solution due to two main reasons:

- In order to support flow mobility, the MN must be able to send and receive traffic to/from any prefix associated to it through any of its interfaces. This functionality can be provided by different mechanisms. Two of the mechanisms that have been studied at the IETF are the Weak Host Model and the Logical Interface (LIF). On one hand, the Weak Host Model [9] corresponds to the implementation decision taken while designing the IP stack. In a mobile node implementing the Weak Host Model, the IP stack accepts any locally destined packet regardless of the network interface on which the packet was received. On the other hand, the Logical Interface is a software entity which presents one single interface to the IP stack, and hides the real physical interface implementations (e.g., modems). Hence, the IP stack binds its sessions to this Logical Interface and it is oblivious of the actual physical interfaces receiving or sending packets. One of the principles of PMIPv6 is to achieve a mobility solution in which the IP stack of the mobile node is completely unaware of the mobility. In order to maintain the MN's IP stack unaware of mobility

[1] `http://datatracker.ietf.org/wg/netext/`

while providing flow mobility support, the IETF has chosen to rely on the concept of Logical Interface [10].

- In the general case, through the use of flow mobility, the MN will be able to receive any traffic destined to any of its IPv6 addresses through any of its interfaces. This represents a problem at the MAG level, since in order to support flow mobility, the MAGs must be able to forward any prefix associated to the MN even if this prefix was delegated by a different MAG. This situation is being solved by the IETF through the addition of extra signaling to the standard PMIPv6 so that the MAGs can be configured appropriately.

In the following we explain in detail the solution to both issues presented above.

1) Logical Interface: The Logical Interface is a software entity that hides the real physical interface implementation to the host IP layer. Its use allows the MN to provide a single and permanent interface view to IP and the layers above, that can bind to this interface in order to establish any remote communication. Internally the logical interface is able to leverage several functionalities such as inter-technology handover, multihoming or flow mobility, while presenting always the same IP address (or set of IP addresses) to higher layers. The logical interface is commonly implemented as part of the connection manager software of the mobile terminal, which is in charge of handling and automatically configuring the different network interfaces. Therefore, although the implementation of the logical interface concept require some changes on the client side, those are part of an already required terminal component (the connection manager), and do not have any impact on the IP stack, which remains standard.

This interface is implemented as a logical entity that bonds several physical interfaces (e.g., WiFi and 3G) into a unique interface, which is used by IP and higher layers. The LIF hides to the IP layer the physical interface used to actually send each data, hence a movement of a flow from one interface to another is transparent to the IP and higher layers. Even more, it supports sequential attachment of interfaces as they come up, so the flow mobility features can be started in order to offload some interface or network (e.g., 3G offload) as soon as a new interface becomes active (e.g., a WiFi interface associates with an Access Point), without the higher layers being aware of it. The LIF is sometimes referred to as Virtual Interface.

2) Signalling extensions to PMIPv6: As explained above, signaling extensions to PMIPv6 are required in order to provide the MAGs with the information regarding the different prefixes used by the MN. This information exchange is needed since, in general, a MAG will not forward traffic from/to a prefix that has not been delegated by it to the MN.

In [7] several cases showing the possible configurations for the combinations of prefixes and interfaces are detailed. The IETF currently focuses on two scenarios: *i)* the so-called "handover with full flow granularity", which consists in the movement of a specific flow from one interface to another (e.g., a video-conference where the voice is going through a reliable interface such as 3G and the video through a high bandwidth link such as WiFi, but both flows are addressed to the same prefix), and *ii)* the movement of a complete prefix and all the communications using it, to another interface, scenario often referred to as "partial handover".

Both cases face the problem of requiring the target MAG to get knowledge regarding the prefixes through which the MN is receiving traffic. Flow mobility signaling takes place whenever the LMA decides to move a flow from one access to another. At the time of movement, either the prefix is already known at the target MAG or the LMA must advertise it to the MAG which is going to receive traffic addressed to this prefix. In the case the MAG already knows the target prefix, the LMA simply switches the flow to the target MAG, and no extra signaling is required. In the case signaling is required, the IETF is defining new messages to manage the notification to the MAG of the new flow/prefix to be forwarded.

Fig. 4 shows an example of the initial and resulting routing state of the network upon a flow mobility procedure is completed. Let us suppose the following scenario; An MN (MN 1) is attached to the network through two interfaces `if1`, connected to MAG1, and `if2`, connected to MAG2 and each one receives a prefix, `pref1::/64` for `if1` and `pref2::/64` for `if2` respectively. The MN is receiving two flows, Flow X and Y. Flow X is addressed towards `pref1:lif` (being `lif` the resulting EUI64 identifier of the Logical Interface) and is forwarded through MAG1, while Flow Y is addressed to `pref2:lif` and is forwarded though MAG2. Following this configuration, the LMA has a conceptual data structure called the Flow Mobility Cache containing the mapping of flows and corresponding MAGs. This mapping can be based on any of the flow identifiers defined in [4].

At some point of time the LMA decides to move Flow Y from MAG2 to MAG1. The decision can be based on application profiles, or traffic type oriented policies triggered due to network congestion, for instance. In order to do so, the LMA needs to signal MAG1 that Flow Y is going to be forwarded through it. Through some signaling message, the LMA is able to install state in MAG1 regarding the identification of the flow and the identity of MN 1. Once this state is installed on MAG1, the LMA modifies the mapping stored in its Flow Mobility Cache, indicating that Flow Y is routed through MAG1 and starts forwarding the packets towards MAG1. The final state after flow mobility completion of the routing configuration on the network is also presented on Fig. 4.

It should be further noted that one of the most common technologies to perform traffic classification is Deep Packet Inspection (DPI). It can be performed offline – for instance for billing and charging purposes, or for security checks – or online. In the context of IP flow mobility we envision the use of online DPI to classify traffic according to operator policies. By means of DPI the network becomes intelligent and enables innovative use cases on traffic handling (e.g., multi link diversity utilization, bandwidth aggregation, etc.).

IV. IP Flow Mobility adoption in 3G/4G architectures

The 3GPP SA2 Working Group has specified in [11] the evolved architecture to support simultaneous Packet Data

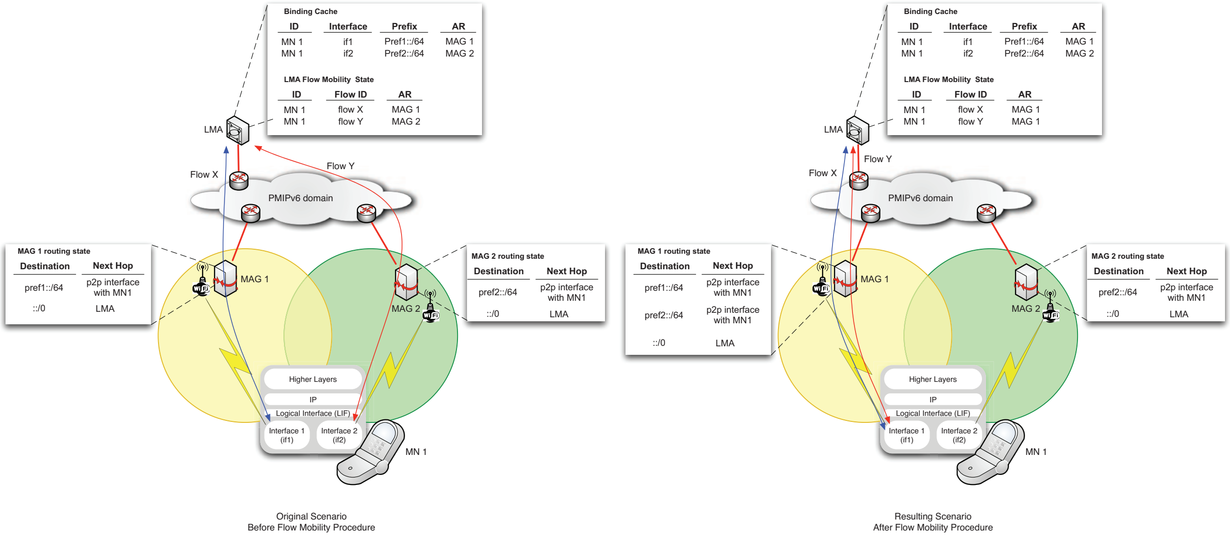


Fig. 4. PMIPv6 flow mobility operation

Network (PDN) connections across different radio accesses for mobile devices equipped with multiple interfaces. This specification defines the system architecture to provide simultaneous usage of 3GPP and non-3GPP radio accesses. The support for multiple accesses allows a mobile user receiving and sending data over a 3GPP cellular bearer while taking advantage of a non-3GPP radio access such as WiFi or WiMAX.

The following examples provide a general overview of the considered scenarios:

1) A premium customer is connected to a 3GPP cellular access as well as a domestic WiFi. He is having several simultaneous IP flows including a voice call, a media file synchronization, a video streaming, and a peer-to-peer download. Based on either the operator's policies or the user's profile, the voice call and the video streaming are routed via the 3GPP access, while the other two flows are declared as best effort and therefore are routed via the non-3GPP radio technology.
2) When the user moves out of reach of the domestic WiFi, the IP flows on this radio access are moved to the 3GPP access to ensure seamless service continuity. By means of multiple PDN support, the network will then be able to handover these flows while providing uninterrupted services. If later on the user returns into the domestic WiFi coverage, the best effort flows can seamlessly be moved back again to the WiFi access.
3) In addition to the traditional radio coverage problem, the Core network can implement methods to perform load balancing or traffic optimization by redirecting selected IP flows to the least loaded or most suitable access network. In this case the network can for instance steer an IP flow to redirect a video download from the 3GPP to the WiFi access in case the end-to-end QoE measure over the 3GPP access does not meet expectations.

Considering the aforementioned scenarios, several system requirements can be derived, such as:

- Service continuity should be provided when the MN roams across different accesses.
- Flows should be redistributed across different accesses while connected.
- The MN should be able to exploit multiple radio accesses to enhance its performance when possible.
- Different types of services should be provided to customers, i.e., operator-based and non-operator-based.
- Flows should be moved from one access to another in case of radio connectivity loss.
- The Telecom operator should be able to control the simultaneous usage of accesses.
- Changes in the capabilities of the difference accesses (e.g., network congestion) should trigger flow mobility.
- The operator should be able to control flow mobility.

In order to address these requirements, 3GPP considers two possible alternatives:

1) DSMIPv6 client-based solution. This approach is being adopted in 3GPP release 10 and uses the DSMIPv6 protocol stack described in Section II with the extensions for flow mobility specified by the IETF.
2) PMIPv6/GTP network-based solution. These solutions exploit the network-based mobility management paradigm and propose supporting multi-homing according to the logic specified in [7]. PMIPv6 extensions are currently being discussed in IETF as described in Section III. Also, the GPRS Tunneling Protocol (GTP) provides a pre-existing network mobility management alternative to PMIPv6. The extensions required to accommodate network-based IP flow mobility (NB-IFOM) are being discussed in 3GPP for release 11 and beyond. Both PMIPv6 and GTP solutions would rely on the above-mentioned logical interface concept implemented at the terminal, as described in [10]. It is worth noticing that the latest developments for network based mobility on non-3GPP access networks (e.g., WLAN) focus on the full adoption of the GTP protocol. While the GTP protocol by itself is a well known state of the

art protocol, it is interesting to note its adoption for all mobility related issues in the Evolved Packet Core (EPC). In fact the only IETF protocol adopted so far is the DSMIP protocol stack for IP flow mobility support. There is general consensus among service providers that cost wise it is probably not appealing to deploy a new set of specifications for a single feature and most likely they will fall back to the network based solution based on the GTP protocol.

In addition one method for the service provider to optimally steer traffic is the Access Network Service Discovery Function. The ANDSF function provides inter-system routing policies for any given APN (Access Point Name) to be used on the terminal. ANDSF steers traffic in the case of non seamless 3G offload, multiple access PDN connections (e.g., the use of two different APNs on the terminal) and IP flow mobility. Current 3GPP Release 10 defines the use of ANDSF policies for the DSMIP solution by matching a given traffic selector on a given access network. It should be noted that in the case of IP flow mobility the same APN is configured simultaneously over LTE and WiFi access. We argue that in the case of network-based IP flow mobility the same mechanisms apply, being the MN the recipient of the ANDSF rules for uplink (UL) and downlink (DL). The LMA will simply map the DL packets to the UL packets.

V. Conclusion

In this article, we have presented and discussed the advantages and drawbacks of the two approaches to enable IP flow mobility that are being standardized in the IETF and 3GPP standards development organizations (SDOs), namely client-based and network-based IP flow mobility. At this stage it is still hard to forecast the evolution of the technology market, however it is clear that Telecom operators are seeking for low cost solutions addressing the smart traffic steering problem beyond classical IP routing functionalities. From the two approaches, network-based flow mobility seems to be a more promising technology that can help Telecom operators that have heterogeneous access networks to extend their network capacity and tier services offerings at low cost, relying on simple software constructs and without modifying the core protocol stack at the terminal.

Current 3GPP discussions head to the definition of a full network-based mobility solution (most likely GTP based) and the use of WiFi network as trusted non-3GPP network. According to mobile operators' requirements the EAP-SIM authentication mechanism is used to provide seamless authentication service to the mobile users and to enable a full fledged fixed-mobile convergence. In this view the IP flow mobility support for network-based mobility management becomes even more interesting for handset manufacturers, greatly simplified by the use of lighter authentication procedures.

Finally, we want to highlight two important future research directions on the user mobility and smart IP flow management areas. On the one hand, additional modifications on the client side may be required to fully exploit the mobility and traffic management enhancements performed on the network counterpart, and to benefit from simultaneous connectivity from heterogeneous accesses. In that area, standardization efforts are crucial, as existing terminal support is mostly based on proprietary connection manager solutions, jeopardizing interworking and interoperability. On the other side, there is a trend towards denser wireless networks deployments, as a way of solving the problem of bandwidth scarcity. The use of these kinds of network architectures would require to carefully revisit existing mobility management solutions, to adapt to a more challenging environment, in which interference management and dynamic reconfiguration will also become critical.

References

[1] H. Soliman, "Mobile IPv6 Support for Dual Stack Hosts and Routers," RFC 5555 (Proposed Standard), Internet Engineering Task Force, June 2009.

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775 (Proposed Standard), Internet Engineering Task Force, June 2004.

[3] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of Addresses Registration," RFC 5648 (Proposed Standard), Internet Engineering Task Force, Oct. 2009.

[4] G. Tsirtsis, G. Giarreta, H. Soliman, and N. Montavont, "Traffic Selectors for Flow Bindings," RFC 6088 (Proposed Standard), Internet Engineering Task Force, Jan. 2011.

[5] G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support," RFC 6089 (Proposed Standard), Internet Engineering Task Force, Jan. 2011.

[6] S. Kent, "IP Encapsulating Security Payload (ESP)," RFC 4303 (Proposed Standard), Internet Engineering Task Force, Dec. 2005.

[7] C. J. Bernardos, "Proxy Mobile IPv6 Extensions to Support Flow Mobility," Work in Progress, draft-bernardos-netext-pmipv6-flowmob-02, Internet Engineering Task Force, Feb. 2011.

[8] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213 (Proposed Standard), Internet Engineering Task Force, Aug. 2008.

[9] R. Braden, "Requirements for Internet Hosts - Communication Layers," Internet Engineering Task Force, RFC 1122 (Standard), October 1989.

[10] T. Melia and S. Gundavelli, "Logical Interface Support for multi-mode IP Hosts," Work in Progress, draft-ietf-netext-logical-interface-support-01, Internet Engineering Task Force, Oct. 2010.

[11] 3GPP, "3GPP TS 23.402; Architecture enhancements for non-3GPP accesses," 3GPP, 2011.

PLACE
PHOTO
HERE

Antonio de la Oliva received a Telecommunication Engineering degree in 2004, and a PhD in Telematics in 2008, both from the University Carlos III of Madrid (UC3M), where he worked as a research and teaching assistant from 2005 to 2008 and, since then, has worked as an Visiting Professor. His research is focused to mobility and specifically to Media Independent Handovers. He has published over 20 scientific papers in prestigious international journals and conferences.

PLACE
PHOTO
HERE

Carlos J. Bernardos received a telecommunication engineering degree in 2003 and a Ph.D. in telematics in 2006, both from UC3M, where currently he works as an associate professor. From 2003 to 2008 he worked at UC3M as a research and teaching assistant. His current work focuses on vehicular networks and IP-based mobile communication protocols. His Ph.D. thesis focused on route optimization for mobile networks in IPv6 heterogeneous environments. He has served as guest editor of IEEE Network.

PLACE
PHOTO
HERE

Maria Calderon is an Associate Professor in the Telematics Engineering Department of the University Carlos III of Madrid, Spain. She received the computer science engineering degree in 1991, and the PhD degree in computer science in 1996, both from the Technical University of Madrid (UPM), Spain. She has published over 25 papers in the fields of advanced communications, reliable multicast protocols, programmable networks, network mobility and IPv6 mobility, in outstanding magazines and conferences. Some of the recent European research projects in which she has participated are E-NEXT, LONG, GCAP, DAIDALOS and GEONET.

PLACE
PHOTO
HERE

Telemaco Melia received his Informatics Engineering degree in 2002 from the Polytechnic of Turin, Italy, and his Ph.D. in Mobile Communications from the University of Goettingen in April 2007. He worked on IPv6-based Mobile Communication focusing on IP mobility support across heterogeneous networks and resource optimization control. In September 2008 he joined Alcatel Lucent Bell Labs. His main research interests include wireless networking and next-generation networks. He his author of more than 20 publications and he actively contributes to the IETF.

PLACE
PHOTO
HERE

Juan Carlos Zuniga has participated in several standardisation bodies including IETF, IEEE 802.11, 802.16, and he is currently vice-chair of the 802.21 WG. He has been with InterDigital since 2001. Previously he worked with Harris Canada, Nortel Networks in the UK and Kb/Tel in Mexico. He received his engineering degree from the UNAM, Mexico, and his M.Sc. and DIC from the Imperial College, London. His research interests are on heterogeneous wireless networks, IP mobility, and distributed content management.