Client and Network-based Dual Stack Mobility Management

Antonio de la Oliva*, Maria Calderon*, Carlos J. Bernardos*, Ryuji Wakikawa†
*Universidad Carlos III de Madrid, Spain
Email: {aoliva, maria, cjbc}@it.uc3m.es
†Toyota ITC, USA
Email: ryuji@us.toyota-itc.com

***Abstract*— We are witnessing how the Internet is evolving to tackle users' demands: mobility (users are mobile) and ubiquitous connectivity (billions of devices are demanding IP connectivity). The former caused the design of IP mobility protocols aimed at enabling terminals to be able to seamlessly roam among heterogeneous access networks, while the latter has sped up the depletion of the IPv4 addressing space, triggering the design of a new version of the IP protocol (IPv6) and the development of transition mechanisms to enable the co-existence of IPv4 and IPv6-based networks. During the transition period, which is expected to last many years, there will be dual stack IPv4 and IPv6 mobile nodes roaming across IPv4-and-IPv6, IPv6-only and IPv4-only networks. This article presents a comprehensive tutorial of the mechanisms that have been standardized recently to support dual stack IP mobility management.**

I. Introduction

The Internet is becoming increasingly mobile. The current trend shows that billions of mobile devices, such as smart phones, hand-held gadgets, or even cars will become online in the near future. Driven by the requirements posed by the different scenarios where connectivity is demanded, the Internet Engineering Task Force[1] (IETF) has standardized several IP mobility solutions. On the other hand, the rapid growth of the Internet has led to the anticipated depletion of addresses in the current version of the Internet Protocol (IP), i.e., IPv4, triggering the design of a new IP version: IPv6. IPv6 provides sufficient address space and a number of new features to meet the predicted increase of the size of the Internet. The transition from IPv4 to IPv6 is a long process (that might never end), and during this period of transition, the newly deployed IPv6-based networks will be operated in parallel with IPv4-based networks. This ultimately means that during this transition period there will be dual stack mobile nodes (and routers) roaming among IPv4-and-IPv6, IPv6-only and IPv4-only networks, and communicating to IPv4 and IPv6 nodes.

Initially, the IETF defined different mobility solutions for IPv4 and IPv6. An IPv4 node can use Mobile IPv4 (MIPv4) [1] to maintain connectivity while moving between IPv4 networks. Similarly, an IPv6 node can use Mobile IPv6 (MIPv6) [2] to maintain connectivity while moving between IPv6 networks. Although a mobility protocol is mostly a tunnel management solution, current mobility protocols are tightly coupled with the IP version due to particularities of IPv4 and IPv6 (e.g., movement detection, address management, etc.).

Both MIPv4 and MIPv6 are client-based approaches, meaning that nodes are aware of their mobility and are in charge of performing the operations required to keep their ongoing sessions despite the movement. Lately, there is a new trend towards solutions that enable mobility of IP devices within a local domain only with support from the network: the so-called network-based localized mobility approaches. This is very interesting from the point of view of operators, because it allows them to provide mobility support without depending on software and complex mobility related configuration in the user devices. The protocol specified by the IETF to offer network-based localized mobility support is Proxy Mobile IPv6 (PMIPv6) [3].

The trend of increasing users' mobility and the incipient perspectives of IPv6 transition triggered the need for developing IP mobility solutions suited for mixed IPv4/IPv6 mobile environments. This is a challenging task, mainly due to the tight coupling of the existing mobility solutions to the IP version, and also because of the long-tail expectation of IPv4 networks. The latter introduces the requirement of providing service continuity for applications using IPv4 addresses, while the former brings the need to avoid any dependency on the IP version of the access network, so a mobile is able to seamlessly roam between disparate visited networks. The main goal of this article is to describe this problem and go through the different challenges and solutions that the standardization fora have faced in order to provide a mobility framework suitable for the upcoming roaming scenarios.

A first approach to support the scenario described above consists in deploying both the mobility management protocols defined for IPv4 and IPv6 in a dual stack node. Running IPv4 and IPv6 mobility protocols in parallel introduces a number of issues: *i)* it requires to send two sets of signaling messages whenever the terminal hands off to a new location, *ii)* network administrators have to run and maintain two sets of mobility management systems, one for IPv4 and another for IPv6, and *iii)* the connectivity across different networks would not be guaranteed since that also depends on the IPv4/IPv6

The research of the Antonio de la Oliva and Carlos J. Bernardos leading to these results has received funding from the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project). The research of Maria Calderon has received funding from the Spanish MICINN through the I-MOVING project (TEC2010-18907).

[1] `http://www.ietf.org/`

capabilities of the networks the mobile node is visiting; i.e., a node attempting to connect via an IPv4-only network would not be able to maintain the connectivity of its IPv6 applications and vice versa. Therefore, the approach recommended by the IETF is to have only one mobility management protocol (i.e., extending one of the existing mechanisms) that can support the mobility for a dual stack node and, consequently, is able to: *i)* manage IPv4 and IPv6 tunnels, *ii)* signal the mobility of IPv4 and IPv6 home addresses and *iii)* allow to connecting to IPv4 and IPv6 access networks.

Considering that it is foreseen that IPv6 will be the only version at the end (i.e., we will finally reach a situation where there is only IPv6, or at least it will be the dominant one) it seems more reasonable from a deployment viewpoint to extend IPv6 mobility protocols to handle dual stack nodes. This approach allows for a long lasting mobility solution, avoiding the need for changing the mobility solution in the future IPv6 Internet. This solution is the one adopted by the 3rd Generation Partnership Project[2] (3GPP), which is probably the main consumer of IP mobility protocols. Since seamless connectivity between cellular and WiFi is considered as a key feature from mobile operators, which need from WiFi accesses to offload traffic from their congested networks (without decreasing the Quality of Experience of their users), mobile operators are starting to provide IPv6 connectivity, together with IPv4, considering the use of IPv6-based dual stack mobility protocols as a valid transition mechanism.

This article presents the recently defined standards to extend the IPv6 mobility management mechanisms so they support dual stack nodes roaming among IPv4-and-IPv6, IPv6-only and IPv4-only networks (Section III. Both client-based (Section IV) and network-based solutions (Section V) are considered. We first summarize the operation of the main IPv6 mobility solutions in Section II.

II. IPv6 Mobility Management

This section is devoted to presenting the two main paradigms of IP mobility support: *i)* client-based mobility management, where the terminal is aware of its own mobility and takes active part on its management, and *ii)* network-based mobility management, where mobility is transparent for the terminal and is performed by the network on its behalf.

As motivated in the introduction, in this article we focus only on IPv6 mobility management protocols. The main protocol designed for client-based mobility management is Mobile IPv6. Extensions to Mobile IPv6 have also been defined in order to support the roaming of complete networks (Network Mobility).

In the case of network-based mobility, the IETF has defined the Proxy Mobile IPv6 protocol to enable terminals in a localized domain to be able to roam transparently (i.e., without any kind of additional support).

A. Mobile IPv6 and NEMO Basic Support protocol

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 home agent (see Fig. 1) is in charge of defending the mobile's home address when it is not at home, and redirecting received traffic to the mobile's current location. When away from its home network, the mobile node acquires a temporal IP address from the visited network – called Care-of Address (CoA) – and informs the home agent about its current location, by sending a Binding Update message. An IP bi-directional tunnel between the mobile node and the home agent is then used to redirect traffic from and to the mobile. In this way the packets generated by the mobile node's communication peer – called Correspondent Node (CN) – sent to the permanent address of the mobile (i.e., its home address) are tunneled to the current location of the MN, and hence arrive at the care-of address. There is also optional support to avoid this suboptimal routing and enable the mobile node to directly exchange traffic with a correspondent node without traversing the home network. This additional support is called Route Optimization, and allows the mobile to also inform correspondent nodes about its current location.

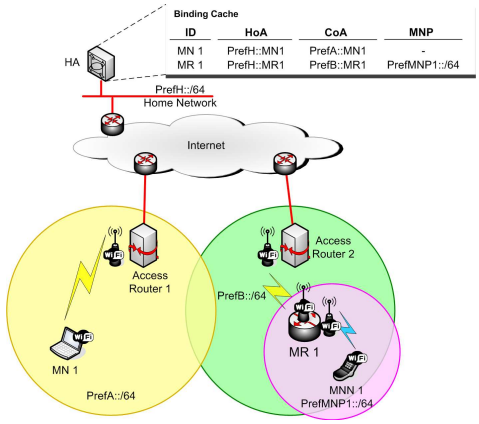

Fig. 1. Mobile IPv6 and Network Mobility Basic Support protocol.

The Network Mobility Basic Support (NEMO B.S.) protocol [4] extends MIPv6 to also support the movement of a whole network, by the router of the network – called Mobile Router (MR) – taking care of the mobility management (i.e., mobility signaling and tunnel setup) of the entire network on behalf of its nodes – called Mobile Network Nodes (MNNs). The IP addresses of the MNNs belong to the Mobile Network Prefix of the mobile network, which is anchored at the mobile router's home agent. There is no route optimization support standardized for NEMO.

B. Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) [3] is a network-based localized mobility management protocol. This means that user terminals are provided with mobility support without their involvement in the mobility management and signaling, as the required functionality is relocated from the terminal 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

[2] http://www.3gpp.org/

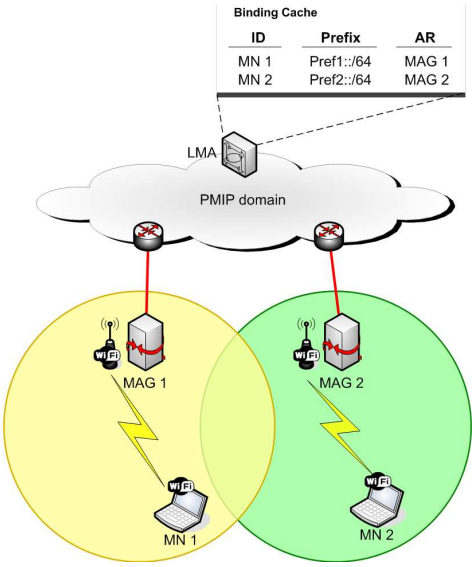

Fig. 2. Proxy Mobile IPv6.

the access router (see Fig. 2). In a Localized Mobility Domain (LMD), which is the area where the network provides mobility support, there are multiple mobile access gateways. The MAG learns through standard terminal operation, such as router and neighbor discovery or by means of link-layer support, about a terminal movement and coordinates routing state updates without any mobility specific support from the terminal. The IP addresses used by nodes within an LMD are anchored at an entity called Local Mobility Anchor (LMA), which plays the role of local home agent of the domain. Bi-directional tunnels between the local mobility anchor and the mobile access gateways are set up, so the mobile node is enabled to keep the originally assigned IP address despite of its location within the localized mobility domain. Through the intervention of the local mobility anchor, packets addressed to the mobile are tunneled to the appropriate gateway within the domain. Upon arrival, packets are locally forwarded to the mobile node, which is therefore oblivious to its own mobility. PMIPv6 is based on MIPv6, extending its signaling.

III. Dual Stack Mobility Management Scenarios

This section identifies and describes the issues that a dual stack mobility management should address. As pointed out in the introduction, mobile operators are currently very interested in enabling their customers to be able to roam not only within their cellular networks, but also to WiFi accesses, either supporting simultaneous connectivity via cellular and WiFi, or handing off from one to the other. This is basically one of the main triggers of the need of efficient IP-based mobility solutions nowadays. Additionally, as opposed to when Mobile IPv4 and Mobile IPv6 solutions were initially designed, the mechanisms to be adopted and deployed need to be capable of operating during the IPv4/IPv6 transition phase (which might perfectly never end). This basically translates into the following two general requirements:

i) The mobile has to be able to enjoy seamless service continuity while using IPv4 and IPv6 applications (i.e., seamless address continuity for both IPv4 and IPv6 type of addresses).

ii) The type of network visited by the mobile node – in terms of IP connectivity capabilities (i.e., IPv4 or IPv6) – should be transparent, so the user is able to roam between IPv4 and IPv6 networks (and of course, also to both IPv4 and IPv6 capable domains), even if the user is behind a Network Address Translator (NAT).

In order to better understand what are the specific technical challenges behind these two general requirements, we present next the main scenarios for dual stack mobility management [5]. While describing these scenarios, we identify the main challenges to be tackled by the extensions to the base-line specifications MIPv6/PMIPv6 [6] [7], in relation to the general requirements previously highlighted. Note that the scenarios are not mutually exclusive, and therefore several scenarios can coexist simultaneously in a given situation.

The different scenarios are shown in Fig. 3. Note that hereinafter the term mobile node (MN) refers to both a mobile host or a mobile router. In the next scenarios we assume that the MN as well as all the mobility related entities (HA, LMA, MAG) are IPv4 and IPv6 enabled (i.e., dual stack).

A. Public IPv4-only visited network

This scenario encompasses a mobile node which hands off or attaches to an IPv4-only network. For instance, this is the case of a mobile node performing a handover to a typical WiFi enabled domestic network (see *Network A* in Fig. 3), as currently very few Internet Service Providers (ISPs) provide IPv6 connectivity at home. This scenario is even more relevant in the short term as most of the public/private hotspots provide IPv4-only connectivity.

Considering that an IPv4-only network does not support the use of IPv6 transport, nor provides a mobile node with an IPv6 Care-of Address (CoA), the major issues that a mobile node must face when handing off to an IPv4-only network are the following ones:

- The mobility management protocol must be able to use an IPv4 address as current locator (i.e., CoA) of the mobile node. As previously noted, the network does not provide the mobile with an IPv6 address, thus the mobility management protocol must be capable of using IPv4 addresses as locators.
- The mobility management signaling must be able to handle IPv4 addresses. Currently mobility protocols are very tight to the IP address family. To support roaming to IPv4-only networks, the mobility management protocol must be able to signal IPv4 addresses as locators (i.e., CoAs).
- Support of data transport over IPv4. Currently both MIPv6 and PMIPv6 use IPv6-in-IPv6 tunnels to deliver data packets to the mobile node. If IPv4-only networks are also to be supported, mobility tunnels must be decoupled from the actual IP family, that is, both IPv6 and IPv4 tunneling must be allowed.

These three issues are related to the second general requirement identified at the beginning of this section, as applications

Scenario	Support for IPv6 user traffic	Support for IPv4 user traffic	Support for IPv6 locator and transport	Support for IPv4 locator and transport	NAT traversal support
A. Public IPv4-only visited network	DEPENDS	DEPENDS	NO	YES	NO
B. IPv4-only correspondent node or application	NO	YES	DEPENDS	DEPENDS	DEPENDS
C. IPv6 and IPv4 network	DEPENDS	DEPENDS	YES	NO	NO
D. IPv4 NATed network	DEPENDS	DEPENDS	NO	YES	YES

TABLE I

SUMMARY OF IPV4-IPV6 TRANSITION SCENARIOS AND REQUIREMENTS ON THE IP MOBILITY SUPPORT

running on a mobile node should be able to benefit from seamless continuity despite the mobile node roaming between visited networks providing different IP version connectivity types. Note that this requirement should be met independently of whether the application is an IPv4 or an IPv6 one.

B. IPv4-only Correspondent Node or Application

This scenario encompasses two different cases. The first case corresponds to a mobile node attached to an IPv6 network (see *Networks B or C* in Fig. 3) that wants to communicate with a correspondent node located in an IPv4-only network (see *Correspondent Network* in Fig. 3). For instance, this may be the case of a mobile connected to an IPv6 enabled network that wants to reach a Home Media Server located at its IPv4-only network at home.

The second one would be the case of a mobile node that wants to use an IPv4-only legacy application, e.g., a worker accessing a business related application which only supports IPv4. Note that in this case it does not matter if the underlying network is IPv6 enabled, since the application is only able to handle IPv4 addresses.

We argue that both cases are highly relevant for mobility management protocols during the IPv6 transition phase. The first scenario will appear as often as the one depicted in the previous section, due to the time required to widely deploy IPv6. The second case will be progressively solved with the upgrade of the IPv4-only applications. However we cannot underestimate the reluctance of companies to modify their critical legacy business applications.

In order to address these scenarios, mobility management protocols have to be extended to provide connectivity and reachability for IPv4 prefixes and addresses at every moment, so a mobile node is able to communicate with IPv4-only correspondent nodes and using IPv4-only applications.

The issues brought up by these two scenarios clearly falls into the first general requirement identified at the beginning of the section. The mobility solution should be able to provide seamless address continuity for both IPv4 and IPv6 type of addresses.

C. IPv6 and IPv4 capable networks

A mobile node may be attached to a visited access network that is both IPv4 and IPv6 capable (see *Network C* in Fig. 3). In this case the mobile will likely prefer to use IPv6 as transport of its data packets for both IPv4 and IPv6. An obvious reason to prefer IPv6 over IPv4 transport, is to avoid traversing NATs. We argue that this scenario will become the most common one until the whole Internet is IPv6 enabled. As IPv6 is deployed in a network, IPv4 support will not be discontinued in order to support IPv4-only peers.

This scenario brings the need for the mobility protocol to be able to transport both IPv4 and IPv6 traffic indistinctly inside an IPv6 tunnel. This issue is related to the second general requirement identified at the beginning of the section, since mobility support should be provided independently of the type of visited access network.

D. Network Address Translation considerations

Current Internet massively uses NATs as a simple way of connecting to the Internet using private addressing in small and home office environments. Mostly all IPv4 networks found in such environments use a NAT incorporated in the gateway, that allows the management of a private address block while maintaining connectivity with the Internet. In spite of their proliferation, NATs are a well known problem for all mobility protocols as they prevent direct communication between the mobile node and the anchor point without previous proper configuration. In the general case, each of the previous scenarios where IPv4 connectivity is present is subject to be behind a NAT.

Therefore, it is required that the dual stack mobile nodes implement mechanisms for NAT-traversal to grant the communication between the mobile and its anchor point. This also falls into the second general requirement of provision of service continuity independently of the IP characteristics (in terms of family version and NAT presence) of the visited access network.

E. Summary of scenario requirements

In this section, some dual stack mobility management scenarios have been described, with the goal of highlighting the main issues posed by them, and deriving the technical requirements that the IP mobility solutions should meet. A summary of this analysis is shown in Table I. Note that the scenarios are chosen to highlight specific issues/technical requirements, without fully describing the whole scenario (e.g., when explaining the IPv4-only visited network, it is not specified whether the mobile node is running an IPv6 or IPv4 application), and that is the reason why in Table I some requirements are marked as “DEPENDS”.

Sections IV and V are devoted to present – with the support of the scenario and requirements analysis performed in this section – the different extensions designed for Mobile IPv6 and Proxy Mobile IPv6 to enable their operation in dual stack scenarios.

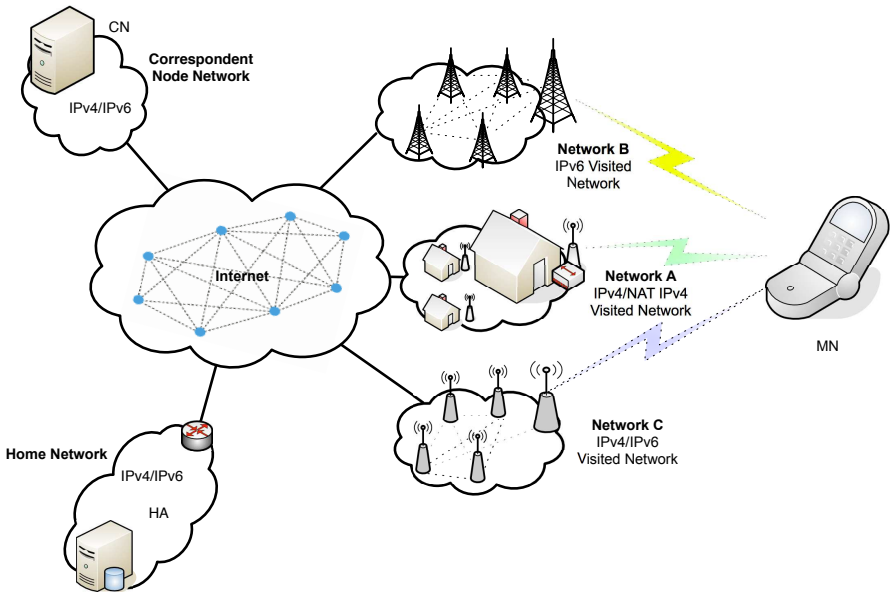

Fig. 3. IP mobility transition scenarios.

IV. Mobile IPv6 Support for Dual Stack Hosts and Routers

Mobile IPv6 standards (i.e., MIPv6 and NEMO B.S.) have been extended in RFC 5555 (Dual Stack Mobile IPv6, DSMIPv6) [6] to support the operation of dual stack mobile hosts and routers, by enabling them *i)* to roam over both IPv4 and IPv6 visited networks, *ii)* to register IPv4 home addresses and mobile network prefixes, and *iii)* to transport IPv4 and IPv6 traffic over the tunnel between the mobile node/router and its home agent.

As hinted in the introduction, the use of an IPv6 mobility protocol to handle dual stack nodes brings an important advantage: it allows for a long lasting mobility solution. While IPv6 presence in current deployed networks and in the Internet is very little compared to the one of IPv4, it is expected that this will change in the short future. By extending Mobile IPv6 to support dual stack nodes – instead of the alternative approach of doing so with Mobile IPv4 – the need for changing the mobility solution when IPv6 is introduced within a deployed network is eliminated.

Basically, there are three different extensions to MIPv6 that are required in order to support dual stack nodes: *i)* signaling extensions to allow carrying IPv4 addresses (and prefixes) and detecting NATs, *ii)* new types of tunnels, allowing for the transport of IPv4 and IPv6 data packets, even traversing NATs, and *iii)* support for attachment to IPv4-only networks (this involves IPv4 care-of address support and NAT detection). It is assumed that a home agent serving a dual stack mobile host/router has also an IPv4/IPv6 dual stack.

Regarding the first requirement, modifications to MIPv6 signaling, there are just a couple of significant changes. On the one hand, a new option (called IPv4 Home Address option) is defined, which allows a mobile node not only to use an IPv6 Home Address, but also an IPv4 one (see Sec. III-B). The option of carrying an IPv4 care-of address is also defined in RFC 5555, as there are scenarios in which the mobile node will not be able to configure a global IPv6 address as care-of address (see Sec.III-A). A new option is also defined to allow the home agent notify the mobile node that there is a NAT in the path, including a flag that indicates to the mobile node if UDP tunneling should be used, and optionally including a suggested NAT binding refresh time (in case the home agent knows the NAT timeout value, e.g., when the NAT belongs to the same administrative domain that the home agent). If we refer to the requirements summarized in Table I, this signaling changes are part of the extensions needed to allow supporting both IPv4/IPv6 user traffic and locators, as well as to detect and traverse NATs.

Regarding the last two requirements, both of them are addressed on RFC 5555 allowing the configuration of several tunneling mechanisms for different scenarios. A dual stack mobile node can get attached to an IPv6/IPv4 dual stack, an IPv6-only or an IPv4-only access network. In case the mobile node is able to configure an IPv6 care-of address, this should be used as source address for the MIPv6 signaling (and also as the local end of the bi-directional tunnel with the home agent). In case the access network only provides IPv4 connectivity, the mobile node needs to detect if it is behind a NAT or not. In order to do so, the initial IPv6 Binding Update (source address set to the mobile's home address, destination address set to the home agent's IPv6 address) is encapsulated in UDP, which is transported using IPv4 (with source address the mobile node's IPv4 care-of address, and destination address the home agent's IPv4 address). The home agent compares the IPv4 address of the source address field in the IPv4 header with the address included in the IPv4 care-of address option. In case the two addresses do not match, that means that there is a NAT in the path, and the home agent includes a NAT detection option in

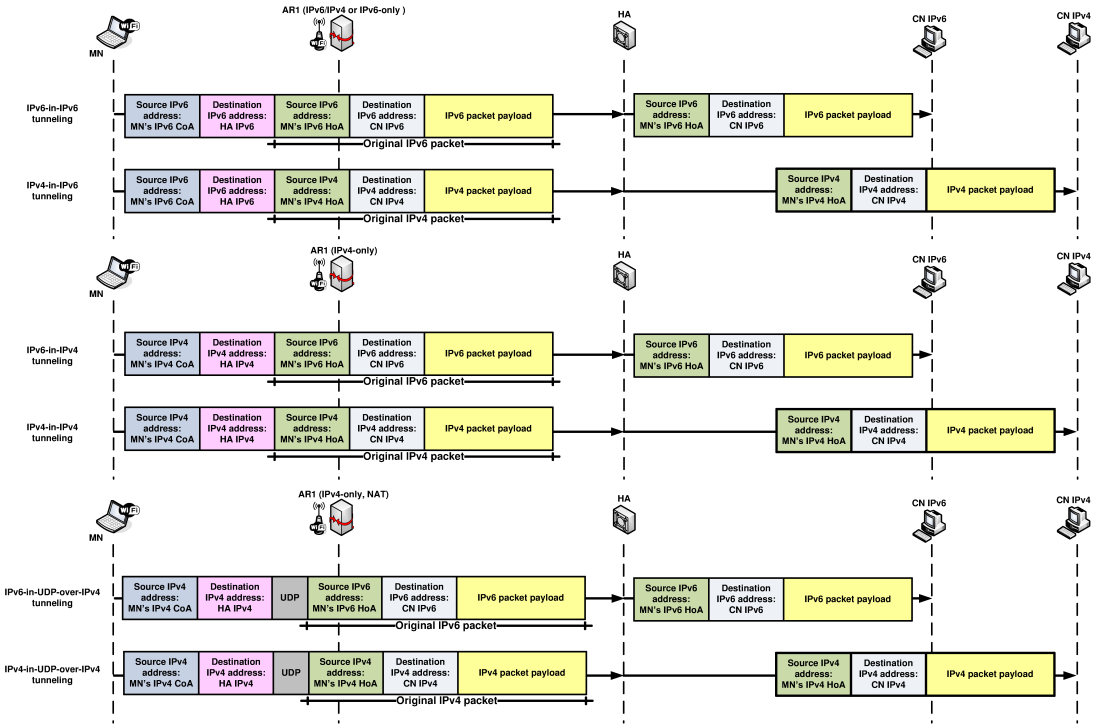

Fig. 4. DSMIPv6 tunneling approaches.

the Binding Acknowledgment.

Fig. 4 shows the different tunneling approaches defined by RFC 5555 for communications between a dual stack mobile node and IPv6 or IPv4 correspondent nodes. Due to space constraints, only packets sent by the MN are shown in Fig. 4, the other direction will follow the symmetric path, as the tunnels are bi-directional). Both IPv4 and IPv6 data forwarding between the mobile node and its home agent are supported. IPv6 tunneling is generally preferred in case the mobile node has a valid IPv6 care-of address. If the mobile is behind a NAT device, UDP tunneling is used. If a public IPv4 care-of address is available (i.e., no NAT detected), then UDP tunneling is generally not required, although there are a few exceptions, such as when the local domain does not allow IP-in-IP traffic, where UDP might be used even when the mobile node is not behind a NAT.

The support of different tunneling options is required in order to meet the requirements of support of IPv4/IPv6 locators and transport of Table I and also to be able to traverse NATs. In order to meet this last requirement, the mechanisms and signaling options defined to detect NATs are used.

The variety of tunneling formats defined by the RFC 5555 deserves additional attention. First, a mobile node might need to change the tunneling format as a result of a movement, which can impact on the link and path MTU visible to the applications hosted on the mobile hosts (or on the nodes attached to the mobile network, in case of a mobile router). Because of this, it is not recommended that the mobile node changes the selected tunneling approach unless it is aware that it can do it beforehand (note that probing the different tunneling options takes time and therefore the mobile should avoid doing it every time it moves). Second, the overhead introduced by the tunneling can account for a large portion of the bandwidth consumed by the mobile node, especially for applications such as Voice over IP, which exhibit small payloads. For example, if we take the iLBC (internet Low Bitrate Codec) [8] codec (it is one of the codecs used by the well-known Skype application) with an encoding length of 20 ms, that results in a payload rate of 15.20 kbps. For a VoIP application using this codec and RTP/UDP over IPv4, the additional packet overhead introduced by Dual Stack Mobile IPv6 is of 33.9% for IPv4-in-IPv6, 20.4% for IPv4-in-IPv4 and 26.4% for IPv4-in-UDP-over-IPv4 encapsulation. Finally, it is worth highlighting, from a performance viewpoint, the impact of roaming between networks with different IP versions deployed. Moving from an IPv6 to an IPv4 visited network takes generally more time, due to the fact that the mobile node usually detects that it is attached to an IPv4-only network only after the IPv6 movement-detection algorithm fails to configure an IPv6 address.

In this section we have identified and described the technical protocol extensions to Mobile IPv6 required to meet the requirements listed in Section III, resulting in the DSMIPv6 specification. This protocol has been adopted by the 3GPP as one of the mechanisms to support mobility between heterogeneous accesses (i.e., 3GPP and non-3GPP networks) and it is part of the specifications since Release 8. Next section is devoted to conduct the same exercise for the case of Proxy Mobile IPv6, identifying and explaining the different extensions required to meet the requirements posed by a dual stack scenario.

V. IPv4 Support for Proxy Mobile IPv6

In order to operate over IPv4, extensions to the basic Proxy Mobile IPv6 protocol have been defined in RFC5844 [7]. These extensions provide two main functionalities: *i)* IPv4 transport network support, and *ii)* IPv4 mobility support. A network provider managing a PMIPv6 domain can choose to deploy either one or both of these functions depending on their operational requirements. Fig. 5 presents a possible scenario for the deployment of these extensions. In Fig. 5, MAG2 and MAG3 are located in IPv4 networks and establish bi-directional tunnels to the local mobility anchor by using IPv4 transport network support. Additionally, IPv4 mobility support enables mobile nodes to obtain IPv4-only, IPv6-only or both IPv4 and IPv6 addresses. In the following subsections each of these functionalities is explained in detail.

A. IPv4 Transport Network support

Although Proxy Mobile IPv6 requires an IPv6 transport network and an IPv6 home network for its operation, network operators cannot migrate their entire PMIPv6 domain to IPv6 at once due to network backward compatibility, financial risk, service disruption avoidance, etc. Therefore, it is important for network providers that the LMA and the MAGs are placed at both IPv6 and IPv4 networks during the IPv6 transition phase. Thus, local mobility anchors and mobile access gateways must be able to forward any packets meant to/from mobile nodes over IPv4 transport networks.

In order to support IPv4 transport networks, both LMAs and MAGs must support dual stack and obtain an IPv4 address that can be of private or global scope.

When LMA and MAG exchange the standard PMIPv6 signaling messages as defined in RFC5213 [3], the IPv6 signaling packets must be encapsulated in IPv4 packets. The use of IPv4 packets to encapsulate the signaling messages imposes that they are securely exchanged with IPsec. As opposed to DSMIPv6 [6], the LMA and MAG must establish an IPsec security association (IPv4 IPsec ESP) between their IPv4 addresses for securing signaling packets. As LMA and MAGs are stable routers and a part of operators' infrastructure, having additional security association for IPv4 support is easily archived. In addition, Proxy Binding Update and Acknowledgement messages are no longer carried in a mobility header but in the UDP payload, due to the limitations of IPv4 options.

User's traffic can be encapsulated between LMA and MAG with the following tunnel mechanisms:

- IPv4: IPv4 or IPv6 payload packet carried in an IPv4 packet.
- IPv4-UDP: payload packet carried in an IPv4 packet with UDP header.
- IPv4-UDP-TLV: payload packet carried in an IPv4 packet with UDP and TLV (Type, Length, Value) header.
- IPv4-GRE: payload packet carried in an IPv4 packet with a Generic Routing Encapsulation header.

If we perform the same overhead analysis than in Section IV (i.e., a VoIP application using the iLBC codec with an encoding length of 20ms and RTP/UDP over IPv4), the additional packet overhead introduced by the Proxy Mobile IPv6 solution is of 33.9% for IPv4-in-IPv6 (native IPv6 transport between LMA and MAG), 20.4% for IPv4-in-IPv4, 26.4% for IPv4-in-UDP-over-IPv4, 29.1% for IPv4-UDP-TLV and 26.4% for IPv4-GRE encapsulation. These values are similar to the ones obtained for DSMIPv6, with the important difference that in this case the added overhead is not carried over-the-air in the wireless hop between the mobile node and the MAG.

All the extensions described in this section can be categorized under the second general requirement that was described in Section III, namely the transparent support for different types of IP visited networks. It is worth mentioning, that due to the shift of mobility operations from the mobile terminal to the MAG, it is not the mobile node itself who needs to support roaming between IPv4 and IPv6 networks, but the MAG to be able to exchange traffic with the LMA via IPv4 or IPv6 networks. The link between the MAG and the mobile node can be considered to be IPv4/IPv6, if the mobile is running both IPv4 and IPv6 applications, as described next.

B. IPv4 mobility support

As long as operators continue supporting IPv4 based applications running on mobile nodes, an IPv4 home address must be assigned to mobile nodes (see MN1 in Fig. 5). Since PMIPv6 cannot modify mobile nodes at all, it only supports existing address assignment mechanisms such as Dynamic Host Configuration Protocol (DHCP) [9], PPP Internet Protocol Control Protocol (IPCP) [10] or Internet Key Exchange (IKEv2) protocol [11]. One of the challenges is how to keep the consistency of the address assignment status between PMIPv6 and those address assignment mechanisms, specially when a mobile node attaches to a different MAG. In RFC5844, the LMA manages an IPv4 home addresses pool and any address assignment mechanisms used to deliver the IPv4 home address assigned by PMIPv6 to the mobile nodes. This guarantees assigning the same IPv4 home address whenever a mobile node switches MAG. The IPv4 mobility support functionality provided by RFC5844 [7] supports flexible DHCP settings in a PMIPv6 domain such as:

- DHCP server co-located with every MAG.
- DHCP relay co-located with every MAG and DHCP server located anywhere in PMIPv6 domain (most likely DHCP server co-located with LMA).

When a mobile node detects a link change (i.e., handover), the mobile node may run DNAv4 (Detecting Network Attachment version 4) [12]. In this case, it may not identify the link change because Proxy Mobile IPv6 is responsible for providing the same default router at any visiting links. Therefore, the mobile node will not perform any DHCP operation after the link change. If the mobile node does not support DNAv4, it may start DHCP rebooting procedure after the link change event. However, the mobile node will obtain the same home address anyway and continue its sessions.

These protocol extensions meet the first general requirement described in Section III, allowing the mobile node to enjoy seamless IP connectivity, regardless of it is IPv4 or IPv6.

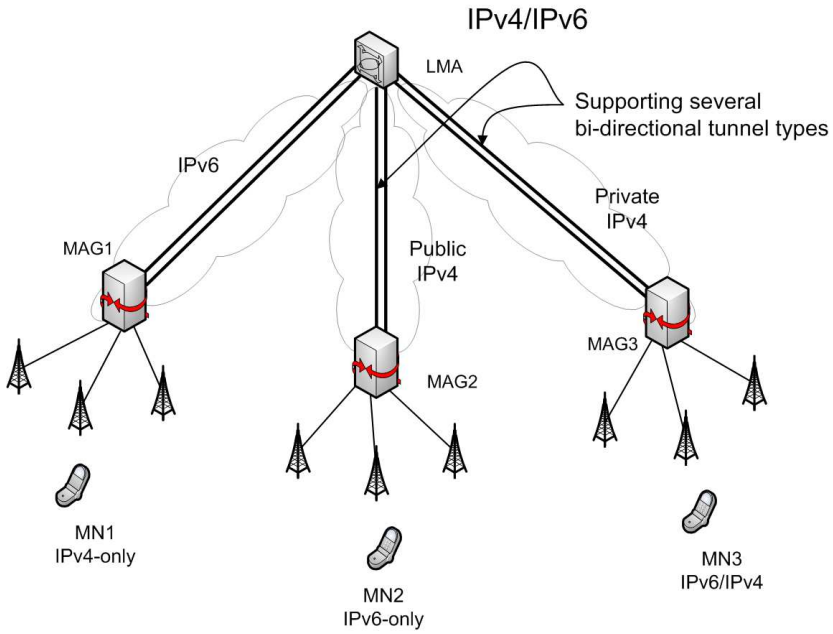

Fig. 5. IPv4 support for Proxy Mobile IPv6.

VI. Conclusion

In this article, we have discussed the recent standards defined to extend the IPv6 mobility management mechanisms to support the mobility of dual stack nodes roaming across IPv4/IPv6, IPv6-only and IPv4-only visited networks. We have considered the two main paradigms followed by the IETF and the 3GPP to manage mobility, namely, client-based and network-based. Thus, we have analyzed both the extensions to Mobile IPv6 and Proxy Mobile IPv6.

These previously mentioned extensions assume that both the mobile node and the mobility entities (i.e., LMA, MAG, HA) are dual stack (IPv4/IPv6) enabled. However it is presumed that applications and visited networks may be IPv4-only, or the mobility management entities may be located at IPv4 networks. So, the proposed extensions cover the challenges posed by several mobility scenarios that are foreseen to be frequent and relevant in the IPv6 transition period (that might never end) where newly deployed IPv6-based networks will be operated in parallel with IPv4-based networks.

From a deployment point of view, client and network-based solutions present different issues. On the one hand, client-based solutions pose the disadvantage of requiring client stack modifications, which can be seen as a burden on the deployability of the solution. On the other hand, a client-based solution relies less on support locally available at the visited network, as compared with a network-based solution which requires the visited network to implement (at least some of) the extensions described in this article in order to provide seamless service to a dual stack mobile node. If we take the 3GPP as a reference, both client and network-based solutions are included in the specifications, being also enhanced to not only support dual stack mobile devices, but also some other advanced features such as IP flow mobility and seamless WiFi offload.

To our understanding, these standards will play a crucial role in the future Internet with billions of mobile devices moving in mixed IPv4/IPv6 environments. As more and more IPv6 networks will be deployed, the coexistence and inter-working between current IPv4-based networks and the newly added IPv6-based networks become imperative.

References

[1] C. Perkins, “IP Mobility Support for IPv4,” RFC 3344 (Proposed Standard), Internet Engineering Task Force, Aug. 2002.
[2] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” RFC 3775 (Proposed Standard), Internet Engineering Task Force, June 2004.
[3] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6,” RFC 5213 (Proposed Standard), Internet Engineering Task Force, Aug. 2008.
[4] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, “Network Mobility (NEMO) Basic Support Protocol,” RFC 3963 (Proposed Standard), Internet Engineering Task Force, Jan. 2005.
[5] G. Tsirtsis and H. Soliman, “Problem Statement: Dual Stack Mobility,” RFC 4977 (Informational), Internet Engineering Task Force, Aug. 2007.
[6] H. Soliman, “Mobile IPv6 Support for Dual Stack Hosts and Routers,” RFC 5555 (Proposed Standard), Internet Engineering Task Force, June 2009.
[7] R. Wakikawa and S. Gundavelli, “IPv4 Support for Proxy Mobile IPv6,” RFC 5844 (Proposed Standard), Internet Engineering Task Force, May 2010.
[8] S. Andersen, A. Duric, H. Astrom, R. Hagen, W. Kleijn, and J. Linden, “Internet Low Bit Rate Codec (iLBC),” RFC 3951 (Experimental), Internet Engineering Task Force, Dec. 2004.
[9] R. Droms, “Dynamic Host Configuration Protocol,” RFC 2131 (Draft Standard), Internet Engineering Task Force, Mar. 1997.
[10] G. McGregor, “The PPP Internet Protocol Control Protocol (IPCP),” RFC 1332 (Proposed Standard), Internet Engineering Task Force, May 1992.
[11] C. Kaufman, “Internet Key Exchange (IKEv2) Protocol,” RFC 4306 (Proposed Standard), Internet Engineering Task Force, Dec. 2005, obsoleted by RFC 5996, updated by RFC 5282.
[12] B. Aboba, J. Carlson, and S. Cheshire, “Detecting Network Attachment in IPv4 (DNAv4),” RFC 4436 (Proposed Standard), Internet Engineering Task Force, Mar. 2006.