PMIPv6: A Network-Based Localized Mobility Management Solution

by Ignacio Soto, Universidad Politécnica de Madrid; Carlos J. Bernardos, and María Calderón, Universidad Carlos III de Madrid; and Telemaco Melia, Alcatel Lucent Bell Labs

Traditional IP mobility procedures[4] are based on functions residing in both the mobile terminal and the network. Recently, we have been assisting in a shift in IP mobility protocol design, mostly focusing on solutions that relocate mobility procedures from the mobile device to network components. This new approach, known as *Network-Based Localized Mobility Management* (NetLMM), allows conventional IP devices (for example, devices running standard protocol stacks) to roam freely across wireless stations belonging to the same local domain. This property is appealing from the operator's viewpoint because it allows service providers to enable mobility support without imposing requirements on the terminal side (for example, software and related configuration). For this purpose the *Internet Engineering Task Force* (IETF) has standardized *Proxy Mobile IPv6* (PMIPv6)[1].

This article details the Proxy Mobile IPv6 protocol, providing a general overview and an exhaustive description of a few selected functions.

Why Network-Based Localized Mobility?

The ability to move while being connected to a communication network is very attractive for users, as demonstrated by the success of cellular networks. However, while designing the IP stack, mobility was not retained as a requirement and, as a consequence, IP does not natively support mobility. The reason is a very basic design choice adopted in IP, both in IPv4[2] and in IPv6[3], namely that addresses have two roles: they are used as locators and identifiers at the same time.[16]

IP addresses are *locators* that specify, by means of the routing system, how to reach the node (more properly, the *network interface*) that is using a specific destination address. The routing system keeps information about how to reach different sets of addresses that have a common network prefix, thus improving scalability of the system itself. However, IP addresses are also *identifiers* used by upper-layer protocols (for example, the *Transmission Control Protocol* [TCP]) to identify the endpoints of a communication channel. Additionally, names of nodes are translated by the *Domain Name System* (DNS) to IP addresses (which, in that way, play the role of node identifiers).

The linking of these two roles (*locators* and *identifiers*) is appealing because name resolution of the peer with whom we want to communicate and location finding translate to the same problem (that is, no translation mechanism is needed). However, the negative side effect is that supporting mobility becomes difficult.

Mobility implies separating the identifier role from the location one. From the identification standpoint, the IP address of a node should never change, but from the location point of view the IP address should change each time the node moves, showing its current location within the routing hierarchy (that is, the IP subnet to which the node is currently attached).

The IETF has studied the problem of terminal mobility in IP networks for a long time. It has developed IP-layer solutions for both IPv4 (Mobile IPv4[4, 5]) and IPv6 (Mobile IPv6[6]), enabling the movement of terminals and providing transparent service continuity. These solutions, being IP-based, are independent of the Layer 2 technologies. They provide Mobile Nodes with a permanent address (the *Home Address* [HoA]) to be used as identifier, and a temporal address (the *Care-of Address* [CoA]) to be used as locator. The CoA changes in each IP subnet visited by the Mobile Node. An entity in the network, the *Home Agent,* binds both addresses with the help of signaling generated by the Mobile Node. The Home Agent serving a Mobile Node must be placed in the subnet where the Home Address of that Mobile Node is topologically correct (the home network).

Although Mobile IP enables a host to move (that is, change the point of attachment in an IP network) while keeping session continuity, this ability is not sufficient for true mobility. Enabling efficient handoffs is an additional and critical requirement. Because the IP handoff latency is affected by the time required to exchange signaling between the Mobile Node and the Home Agent, a new family of solutions proposes to use a local Home Agent (that is, a Home Agent closer to the Mobile Node) to provide mobility in a local domain; that is, to provide localized mobility support. Changing the point of attachment within the local domain requires only signaling to the local Home Agent, allowing faster signaling messages exchange because it is limited within the local domain. This approach is attractive because users typically move in localized environments (for example, they commute between their living homes and their work places) that can be covered with localized domains. Examples of these types of solutions are "Regional Registrations for IPv4"[7] or "Hierarchical Mobile IPv6 for IPv6"[8]. Note that the term "localized" refers to a particular area from the point of view of the IP network topology, but depending on the access technology, geographically the area can be large, as happens when applying a localized mobility approach to cellular networks.

A common feature of Mobile IP and the localized mobility proposals mentioned previously is that all of them are *host-based*. Mobile Nodes must signal themselves to the network when their location changes and must update routing states in the Home Agent, in the local Home Agent, or in both. This situation also raises the problem of complex security configurations to authenticate those signaling exchanges and modifications of routing states.

Therefore, the IETF decided to work on a solution for NetLMM[10, 11], compounding the advantages of a network-based approach with the benefits of localized mobility management strategies. In NetLMM the network provides mobility support, although the Mobile Node does not participate in IP mobility procedures. That is, network operators can provide mobility support without requiring additional software and complex security configuration in the Mobile Nodes. Thus the deployment of network-based mobility solutions is greatly facilitated. Moreover, the Mobile Node can implement any global mobility solution, because the localized one is transparent and independent from it.

There are several target scenarios for Network-Based Localized Mobility Management[9]:

- Large campus networks with *Wireless Local-Area Network* (WLAN) access: Users move with IP standard devices (that is, no additional hardware or software is required) within a campus that provides WLAN access and mobility support.
- Advanced beyond-third-generation (3G) networks: Cellular operators have been important promoters in the development of the NetLMM solution in the IETF. *Universal Mobile Telecommunications System* (UMTS) and *General Packet Radio Service* (GPRS) networks use a proprietary network-based localized mobility mechanism to provide mobility support for user data traffic (typically IP). This mechanism is based on the GPRS Tunneling Protocol[11], a special-purpose solution developed for *Third-Generation Partnership Project* (3GPP) networks that uses TCP/IP application layer tunnels. A standardized NetLMM protocol for the Internet has important advantages:
  - Reduced costs in network management and in equipment supporting the technology (because of economy of scale)
  - Easier extension of mobility support to other technologies
  - Easier integration with other networks
- Other more-complex scenarios involving network mobility, as in automotive scenarios[12], could benefit from a NetLMM approach to support mobility.

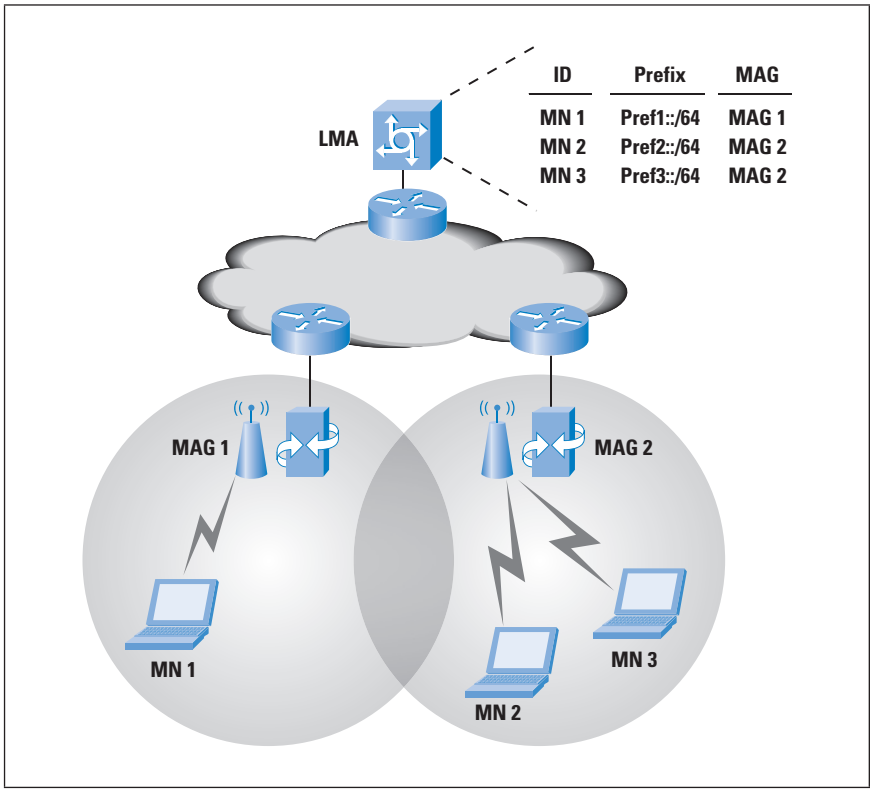
With these advantages in mind, the IETF has standardized a protocol to provide Network-Based Localized Mobility support in IP networks, the *Proxy Mobile IPv6* (PMIPv6) protocol.

Operation of Proxy Mobile IPv6

The main idea of PMIPv6 is that the mobile node is not involved in any IP layer mobility-related signaling. The Mobile Node is a conventional IP device (that is, it runs the standard protocol stack). The purpose of PMIPv6 is to provide mobility to IP devices without their involvement. This provision is achieved by relocating relevant functions for mobility management from the Mobile Node to the network.

PMIPv6 provides mobility support within a localized area, the *Localized Mobility Domain* (LMD) or PMIPv6 domain. While moving within the LMD, the Mobile Node keeps its IP address, and the network is in charge of tracking its location. PMIPv6 is based on *Mobile IPv6* (MIPv6), reusing the Home Agent concept but defining nodes in the network that must signal the changes in the location of a Mobile Node on its behalf.

Figure 1: Network Entities in Proxy Mobile IPv6

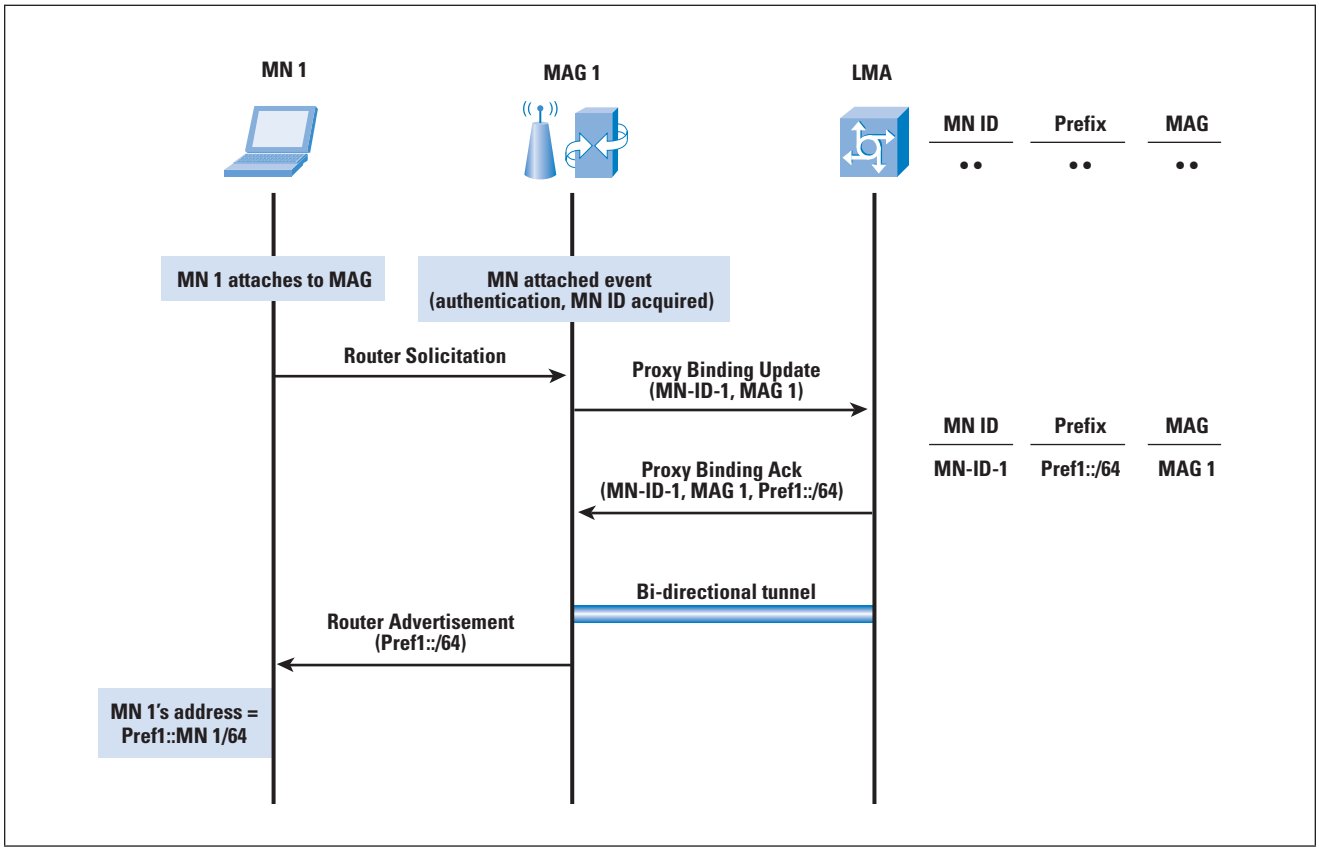


The functional entities in the PMIPv6 network architecture (refer to Figure 1) include the following:

- *Mobile Access Gateway* (MAG): This entity performs the mobility-related signaling on behalf of the Mobile Nodes attached to its access links. The MAG is usually the access router for the Mobile Node, that is, the first-hop router in the Localized Mobility Management infrastructure. It is responsible for tracking the movements of the Mobile Node in the LMD. An LMD has multiple MAGs.
- *Local Mobility Anchor* (LMA): This entity within the core network maintains a collection of routes for each Mobile Node connected to the LMD. The routes point to MAGs managing the links where the Mobile Nodes are currently located. Packets sent or received to or from the Mobile Node are routed through tunnels between the LMA and the corresponding MAG. The LMA is a topological anchor point for the addresses assigned to Mobile Nodes in the LMD, meaning that packets with those addresses as destination are routed to the LMA.

The basic operation of PMIPv6 follows. When a Mobile Node enters a PMIPv6 domain, it attaches to an access link provided by a MAG. The MAG proceeds to identify the Mobile Node, and checks if it is authorized to use the network-based mobility management service. If it is, the MAG performs mobility signaling on behalf of the Mobile Node (see in Figure 2 the signaling when the Mobile Node enters the PMIPv6 domain). The MAG sends to the LMA a *Proxy Binding Update* (PBU) associating its own address with the identity of the Mobile Node (for example, its *Media Access Control* [MAC] address or an identifier related to its authentication in the network). Upon receiving this request, the LMA allocates a prefix to the Mobile Node. Then the LMA sends to the MAG a *Proxy Binding Acknowledgment* (PBA) including the prefix allocated to the Mobile Node. It also creates a *Binding Cache* entry and establishes a bidirectional tunnel to the MAG. The MAG sends *Router Advertisement* messages to the Mobile Node, including the prefix allocated to the Mobile Node, so the Mobile Node can configure an address (stateless autoconfiguration). The Mobile Node can alternatively use stateful address autoconfiguration mechanisms. For simplicity, we assume in the rest of the article that the stateless address autoconfiguration mechanism is used, except when indicated otherwise.

Figure 2: Signaling When a Mobile Node Connects to the PMIPv6 Domain



Whenever the Mobile Node moves, the new MAG updates the location of the Mobile Node in the LMA and advertises the same prefix to the Mobile Node (through Router Advertisement messages), thereby making the IP mobility transparent to the Mobile Node. In this way the Mobile Node keeps the address configured when it first enters the LMD, even after changing its point of attachment within the network, and the LMD appears as a single link from the perspective of the Mobile Node. It should be noted that all the MAGs configure the same link local address for a specific Mobile Node. That is, the Mobile Node will never see a change in its default route configuration.

The bidirectional tunnel between the LMA and the MAG and associated routing states in both LMA and MAG manage the Mobile Node data plane. Downlink packets sent to the Mobile Node from outside of the LMD arrive to the LMA, which forwards them through the tunnel to the serving MAG. The MAG, after decapsulation, sends the packets to the Mobile Node directly through the access link. Uplink packets that originated in the Mobile Node are sent to the LMA from the MAG through the tunnel, and then are forwarded to the destination by the LMA. Traffic originated inside the LMD and directed to a Mobile Node also inside the LMD follows a similar procedure, going through two tunnels from the originating MAG, to the LMA, and then to the destination MAG. It should be noted that PMIPv6 allows a MAG to short-circuit the tunneling in case two mobile nodes directly communicate through any of its interfaces.

Protocol Details

We next describe the PMIPv6 primary functions. Because PMIPv6 is based on the Mobile IPv6 protocol format, we will highlight the differences and extensions to MIPv6. Readers interested in knowing all protocol details should refer to the RFC[1].

Entering a PMIPv6 Domain

The Mobile Node enters the PMIPv6 domain by attaching to an access link. PMIPv6 defines a new functional entity, the MAG, typically residing in the access router. The MAG detects the attachment of the Mobile Node to the access link. The only access link types supported in PMIPv6 are point-to-point links; other types of links can be used as long as they are configured to emulate point-to-point links.

The MAG, upon detecting a Mobile Node attachment, verifies if the Mobile Node is eligible to the network-based mobility management service. Specific procedures to achieve this verification are out of the scope of the PMIPv6 standard. A Mobile Node that uses the mobility support service is identified by the network entities using a *Mobile Node Identifier* (MN-ID). The MN-ID must be stable and unique for the Mobile Node throughout the PMIPv6 domain, but the exact nature of this identifier is not specified. Possible examples are the Mobile Node MAC address or an identifier obtained as part of the Mobile Node authentication procedure.

After the MAG identifies the Mobile Node, authorizes its use of the NetLMM service, and acquires its Mobile Node Identifier, the MAG sends a PBU to the LMA; that is, it sends a registration request on behalf of the Mobile Node to the LMA. The PBU message is based on the MIPv6 *Binding Update* (BU) message with some extensions, but whereas the BU is sent by the Mobile Node, the PBU is sent by the MAG on behalf of the Mobile Node. A flag in the message is used to indicate that it is a PBU and not a BU. The PBU has as source address (and also in the alternate CoA option, if present) the global address configured in the egress interface of the MAG. This address is called *Proxy-CoA* in PMIPv6 terminology and is used by the LMA as locator of the Mobile Node. In the PBU, unlike in the BU, a Home Address destination option is not present; instead a *Mobile Node Identifier Option*[13] has to be included with the Mobile Node Identifier, which is used to identify the Mobile Node throughout the PMIPv6 domain.

The PBU also contains additional information, such as the access link technology, a handoff indicator, the requested lifetime for the registration, and other optional data. The *handoff indicator* is a new mobility option defined in PMIPv6 that allows the MAG to signal the LMA whether the PBU originated upon network attachment or upon handover of a Mobile Node (if known by some unspecified mechanisms), and that information could be useful to support advanced functions such as multihoming. Examples of values of the handoff indicator include: a Mobile Node entering the PMIPv6 domain, a reregistration to update the registration lifetime, a handoff between MAGs, or a handoff between interfaces of the Mobile Node.

Upon sending the PBU, the MAG creates a Binding Update List entry[6] for the Mobile Node. Note that this data structure in Mobile IPv6 is maintained by the Mobile Node to keep track of its bindings, but consequently to the PMIPv6 philosophy, the MAG maintains a *Binding Update List* (BUL) storing the bindings of the Mobile Nodes attached to it. The information in the Binding Update List allows the MAG to link the information about the Mobile Node, the interface in the MAG to which the Mobile Node is connected, and the LMA serving it, among others.

When the LMA receives the PBU sent by the MAG, it first checks that the message is correct according to the PMIPv6 specification, rejecting the registration otherwise. If the LMA accepts the PBU, it has to verify if its *Binding Cache* contains an entry for the Mobile Node identified in the PBU. When a Mobile Node first enters the PMIPv6 domain, the LMA cannot find an entry in its Binding Cache and has to create a new one. The Binding Cache entry is an extended version of the data structure defined for the Binding Cache entries in Mobile IPv6[6].

The entry in the Binding Cache has a flag to indicate that it is a proxy registration, and it links all the information related to the Mobile Node, including its identification and the MAG serving it; that is, the location of the Mobile Node. If there is no entry for the Mobile Node in the Binding Cache (that is, the Mobile Node is entering the PMIPv6 domain), the LMA allocates one or more network prefixes to the Mobile Node. These prefixes are called *Home Network Prefixes,* and it must be noted that at least one network prefix is assigned per Mobile Node.

If the LMA cannot allocate a network prefix to a Mobile Node, it has to reject the registration. The address(es) that the Mobile Node uses while inside the PMIPv6 domain are configured from those Home Network prefixes. The decision of allocating one or more network prefixes depends on a global policy in the PMIPv6 domain or a per-Mobile Node policy. When the registration request is accepted, the LMA creates a *Binding Cache Entry* (BCE) with the accepted values for the registration, including the Mobile Node Identifier, the Proxy CoA (the address of the MAG serving the Mobile Node), and the Home Network prefix(es) allocated to the Mobile Node.

Upon BCE creation, the LMA creates an IPv6-in-IPv6 bidirectional tunnel, if one does not already exist, to the MAG sending the PBU. The LMA sets up forwarding routes through the tunnel for any traffic received that is addressed to the Home Network prefixes of the Mobile Node. Finally, the LMA creates a *Proxy Binding Acknowledgment* (PBA) and sends it to the corresponding MAG. The PBA message is based on the MIPv6 *Binding Acknowledgment* (BA) message with a few more extensions, including a flag that indicates that the message is a Proxy Binding Acknowledgement. The PBA informs the MAG about the registration request result, if it has been rejected (and why, using a status code) or accepted. The PBA contains the Mobile Node Identifier and the Home Network prefixes allocated to the Mobile Node. Unlike the Binding Acknowledgment, the PBA does not include a type 2 routing header (that in the Binding Acknowledgment includes the Home Address of the Mobile Node). Also the PBA is received and processed by the MAG, and not by the Mobile Node.

If the PBA confirms that the registration request has been accepted for the Mobile Node, the MAG creates an IPv6-in-IPv6 bidirectional tunnel, if one does not already exist, to the LMA. The MAG sets up forwarding routes, through the tunnel, for uplink or downlink packets received or sent from or to the Mobile Node. The MAG also updates the Binding Update List entry to reflect the accepted binding registration values.

Upon network attachment and during the PBU or PBA procedure, the Mobile Node can send a *Router Solicitation* in the access link as part of the standard neighbor discovery procedures. The MAG should not reply to this Router Solicitation until the registration in the LMA has been successfully completed. When the MAG receives the PBA indicating a successful registration, the MAG sends a Router Advertisement to the Mobile Node announcing the Home Network prefix(es). The Mobile Node can then apply the stateless address autoconfiguration mechanism or the stateful one (using the *Dynamic Host Configuration Protocol* [DHCP]) according to the indication in the Router Advertisement. For supporting DHCP, a DHCP relay agent has to be present in every MAG in the domain, and the relay agent must include in the link-address field of the *Relay Forward* message an IPv6 address from the Home Network prefix, to indicate to the DHCP server the range of addresses it can assign.

The PMIPv6 specification, as mentioned previously, supports only point-to-point access links with the Mobile Nodes. An interesting use case is to have a broadcast access link and to emulate point-to-point links with the Mobile Nodes to be able to apply the PMIPv6 specification. This case raises the problem of sending Router Advertisements that should be received only by the corresponding Mobile Node, and not by other Mobile Nodes present in the broadcast link. There are several ways to send these advertisements. The Router Advertisements could be sent to the IPv6 link-local address of the Mobile Node that the MAG can learn from the source address of router solicitations sent by the Mobile Node, or by some other unspecified means. Another possibility is to send Router Advertisements to the all-nodes multicast address at the IP layer but to the Link Layer 2 address of the Mobile Node.

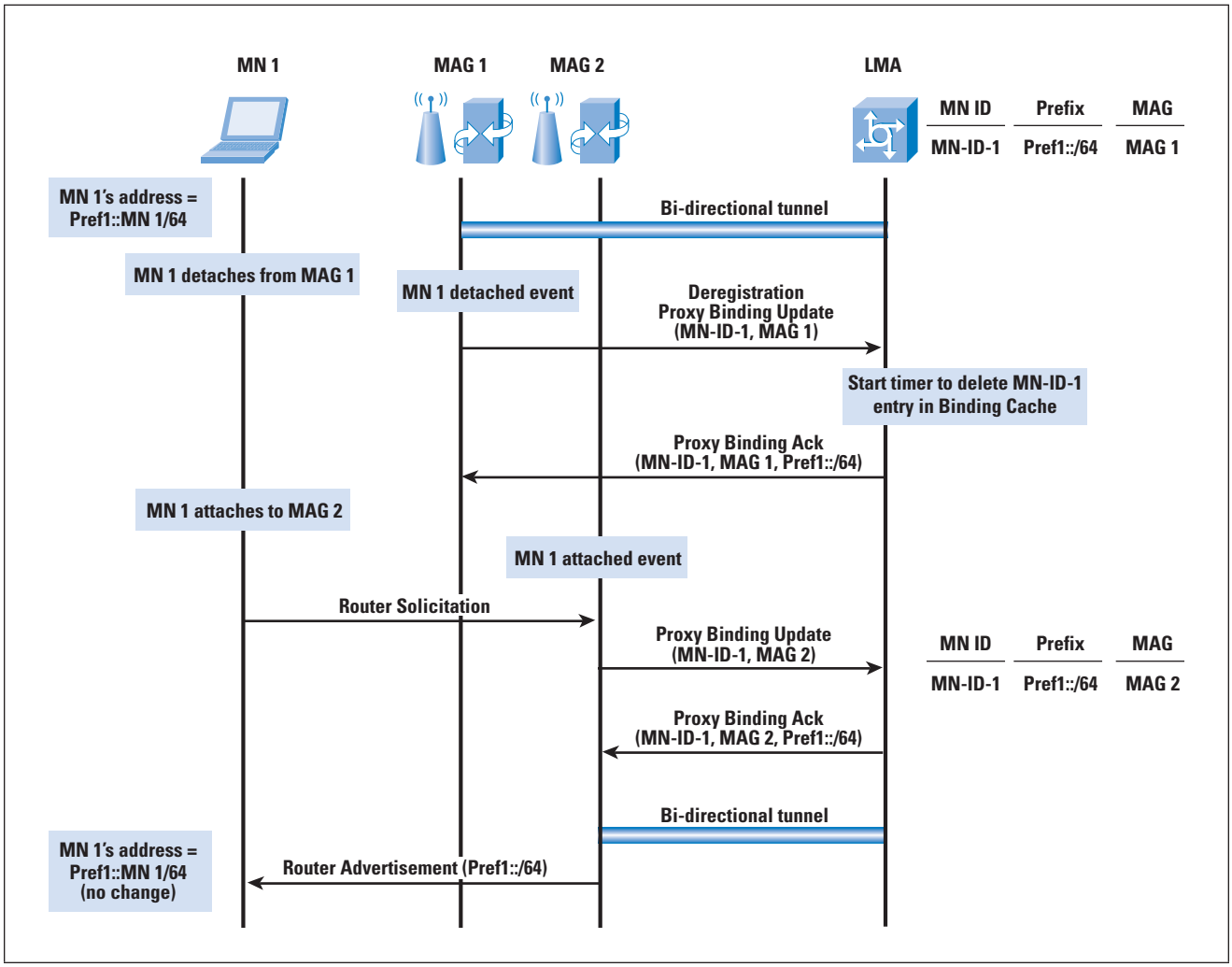
Changing MAG in a PMIPv6 Domain

The complete signaling for supporting the change of attachment by a Mobile Node in a PMIPv6 domain is described in Figure 3.

When a Mobile Node leaves a link, the event is detected by the corresponding MAG. The mechanism for Mobile Node movement detection is not specified in PMIPv6, but some possible options are link-layer events or an *IPv6 Neighbor Unreachability Detection* event. The MAG that detects that the Mobile Node has left the link must send a PBU with a Mobile Node de-registration request to the LMA. Upon receiving a PBA replying to the PBU or after a timer, the MAG deletes all the states associated with a specific Mobile Node.

When the LMA receives a PBU with a de-registration request for a Mobile Node with a valid entry in the Binding Cache, it sends the corresponding PBA and starts a timer. During the period defined by the timer the LMA drops any packets received for the Mobile Node. The use of this timer allows the LMA to receive a PBU from a new MAG updating the location of the Mobile Node. If the PBU is not received during that time, the LMA deletes the state associated with the Mobile Node.

Figure 3: Signaling When a Mobile Node Changes Point of Attachment



In a handoff situation the Mobile Node, after leaving a link, attaches to a new access link associated with a new MAG. The new MAG detects the Mobile Node and sends a PBU to the LMA on behalf of the Mobile Node. The LMA receives and processes the PBU, and detects that there is already a Binding Cache entry for that Mobile Node (the same Mobile Node Identifier). The LMA updates the Binding Cache entry with the new information, in particular with the Proxy CoA (egress IPv6 address) of the new MAG, updating also the tunnel and routing information for handling the traffic from or to the Mobile Node. The LMA sends a PBA to the new MAG in which it includes the Home Network prefix(es) already assigned to the Mobile Node. This scenario allows the new MAG to send a Router Advertisement with the same network prefix information as the Mobile Node received from the previous MAG. As stated before, the Mobile Node does not detect a link change and it keeps the same address(es). To make the change of link completely transparent to the Mobile Node, it must also continue receiving the Router Advertisements from the same link-local and link layer address; otherwise the Mobile Node would detect a change of default router. We describe how this problem is addressed in the next section.

Home Network Emulation and Address Uniqueness

MAGs must ensure that Mobile Nodes do not detect link changes when moving in a PMIPv6 domain; that is, MAGs must provide a home network emulation to the Mobile Nodes. To achieve this emulation, all the MAGs in the PMIPv6 domain must send, to a particular Mobile Node, Router Advertisements with the same network prefix information, as described previously. Additionally, the source IPv6 link-local address and the source link layer address in Router Advertisements sent to a Mobile Node must never change, independently of the MAG sending them. Therefore, the PMIPv6 specification requires all the MAGs to use, in any access link to which a particular Mobile Node attaches, the same link-local and link layer address.

PMIPv6 proposes two ways to meet this requirement:

- Configure a fixed link-local and link layer address to be used in all the access links in a PMIPv6 domain.
- Generate at the LMA the link-local address to be used by MAGs with a particular Mobile Node, and send it to the serving MAG through PMIPv6 signaling messages.

Both of these configuration methods are also helpful to guarantee address uniqueness in the access links of the PMIPv6 domain. The global addresses are always unique because all links are point-to-point and only one Mobile Node uses unicast global addresses over that link. Link-local addresses are used by the MAG and the Mobile Node on the link and a collision is possible. However, because the PMIPv6 specification requires that the link-local address used by the different MAGs with a particular Mobile Node is always the same while the Mobile Node moves across the PMIPv6 domain, the collision problem can happen only when the Mobile Node enters the PMIPv6 domain.

When a Mobile Node enters the domain, we must rely on *Duplicate Address Detection* (DAD) to detect a collision. If we use a globally unique link-local address for all the MAGs in the PMIPv6, then it is easy for the MAGs to respond to DAD requests from Mobile Nodes, because MAGs always know the address they must defend. If the link-local address to be used by the MAG with a Mobile Node is generated in the LMA, then it is desirable that the MAG learns that link-local address (that is, completes the PMIPv6 registration procedure) to defend it before the Mobile Node carries out the DAD procedure. You can ensure the MAG can learn this address by ensuring that the Layer 2 attachment is not completed until finishing the PMIPv6 signaling registration, or by configuring the PMIPv6 registration procedure in such a way that it is likely to be completed before the default waiting time of a DAD procedure.

Security Considerations

As with Mobile IPv6 signaling, PMIPv6 signaling is very sensitive to security threats, because it changes routing states of nodes in the network on behalf of the Mobile Nodes. PMIPv6 specification recommends using *IP Security* (IPsec) to protect the signaling exchanges between the MAGs and the LMA. A security association is needed between MAGs and the LMA, but how it is created is not defined. Two cases are possible:

- The network elements (LMA and MAGs) belong to the same operator.
- The elements belong to different operators with an agreement for roaming support.

In both scenarios, creating the security association is an affordable problem.

Traffic Handling in a PMIPv6 Domain

Traffic sent to any address belonging to a Home Network prefix is received by the LMA, the anchor point for those addresses. The LMA forwards the traffic through the tunnel to the MAG serving the Mobile Node, and the MAG decapsulates the packets and forwards them to the Mobile Node through the access link. Packets sent by the Mobile Node are forwarded by the MAG through the tunnel to the LMA. The LMA decapsulates the packets and forwards them to the destination. If a MAG has data traffic that originated in one of its access links and is destined to another of its access links, it can forward the traffic locally to avoid the forwarding through the LMA. This forwarding is done according to a policy configured in the MAG.

Performance Considerations

PMIPv6 presents two performance advantages compared with MIPv6. First, the LMA is a local network entity, so in principle the delay of sending signaling to the LMA will be lower than sending signaling to a remote Home Agent. And second, because the tunnel required to handle the traffic is terminated in the MAG instead of in the Mobile Node (as happens in MIPv6), we avoid the overhead of having a tunnel (two IP headers) over the radio interface. This overhead avoidance is relevant because bandwidth resources are scarcer over the air interface than in the backhaul network.

IPv4 Support Considerations

PMIPv6 acknowledges the existence of a dual-stack mobile host. To this end there are ongoing efforts to standardize IPv4 support for PMIPv6 operations. The extensions defined in [14] specify how to assign an IPv4 Home Address to a mobile host accessing the PMIPv6 domain. That is, the MAG—upon Mobile Node detection attachment and verification that the Mobile Node is eligible for PMIPv6 service—inserts in the PBU an "IPv4 Home Address Request Option."

The LMA, upon reception of the PBU message, assigns an IPv6 *Home Network Prefix* (HNP) or an IPv4 Home Address by attaching an "IPv4 Home Address Reply Option" to the PBA. How the information is delivered to the Mobile Node depends on the interface between the Mobile Node and the MAG, possible examples being DHCP or *Internet Key Exchange Version 2* (IKEv2). The Mobile Node—independent of the method deployed—configures the HNP and the IPv4 Home address assigned by the LMA, thus supporting both IPv4- and IPv6-based applications.

Conclusions

PMIPv6 is a promising specification that allows network operators to provide localized mobility support without relying on mobility functions or configuration present in the mobile nodes. This reality greatly eases the deployment of the solution.

The IETF is currently working in the *Network-Based Mobility Extensions* (netext) Working Group on extending the PMIPv6 specification to add functions such as enhanced multihoming and intertechnology handoff support, and localized routing for traffic between MAGs to avoid going through the LMA. Additionally, the *Multicast Mobility* (multimob) Working Group is working on the support of multicast in PMIPv6.

References

[1] S. Gundavelli (Ed.), K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213, August 2008.

[2] Jon Postel, "Internet Protocol," RFC 791, September 1981.

[3] Stephen E. Deering and Robert M. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December 1998.

[4] William Stallings, "Mobile IP," *The Internet Protocol Journal,* Volume 4, Number 2, June 2001.

[5] Charles E. Perkins, "IP Mobility Support for IPv4," RFC 3344, August 2002.

[6] David B. Johnson, Charles E. Perkins, and Jari Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[7] E. Fogelstroem, A. Jonsson, and C. Perkins, "Mobile IPv4 Regional Registration," RFC 4857, June 2007.

[8] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management," RFC 5380, October 2008.

[9] J. Kempf (Ed.), "Problem Statement for Network-Based Localized Mobility Management (NETLMM)," RFC 4830, April 2007.

[10] J. Kempf (Ed.), "Goals for Network-Based Localized Mobility Management (NETLMM)," RFC 4831, April 2007.

[11] 3GPP TS 29.060, "GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface," 2009. Available at: **http://www.3gpp.org/ftp/Specs/html-info/29060.htm**

[12] Ignacio Soto, Carlos J. Bernardos, Maria Calderon, Albert Banchs, and Arturo Azcorra, "NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios," *IEEE Communications Magazine,* Vol. 47, No. 5, May 2009.

[13] A. Patel, K. Leung, M. Khalil, H. Akhtar, and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)," RFC 4283, November 2005.

[14] R. Wakikawa and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6," RFC 5844, May 2010.

[15] Carlos J. Bernardos, Ignacio Soto, and María Calderón, "IPv6 Network Mobility," *The Internet Protocol Journal,* Volume 10, Number 2, June 2007.

[16] Dave Meyer, "The Locator Identifier Separation Protocol (LISP)," *The Internet Protocol Journal,* Volume 11, Number 1, March 2008.

IGNACIO SOTO received a telecommunication engineering degree in 1993, and a Ph.D. in telecommunications in 2000, both from the University of Vigo, Spain. He was a research and teaching assistant in telematics engineering at the University of Valladolid from 1993 to 1999. In 1999 he joined University Carlos III of Madrid, where he was an associate professor from 2001 until 2010. In 2010, he joined Universidad Politécnica de Madrid as associate professor. His research activities focus on mobility support in packet networks and heterogeneous wireless access networks. E-mail: **isoto@dit.upm.es**

CARLOS J. BERNARDOS received a telecommunication engineering degree in 2003, and a Ph.D. in telematics in 2006, both from the University Carlos III of Madrid, where he worked as a research and teaching assistant from 2003 to 2008, and since then as an associate professor. His Ph.D. thesis focused on route optimization for mobile networks in IPv6 heterogeneous environments. He has published more than 30 scientific papers in prestigious international journals and conferences, and he also contributes to the IETF. He served as TPC chair of WEEDEV 2009 and as guest editor of *IEEE Network*. E-mail: **cjbc@it.uc3m.es**

MARÍA CALDERÓN is an associate professor at the Telematics Engineering Department of University Carlos III of Madrid. She received a computer science engineering degree in 1991 and a Ph.D. degree in computer science in 1996, both from the Technical University of Madrid. She has published more than 40 papers in the fields of advanced communications, reliable multicast protocols, programmable networks, and IPv6 mobility. E-mail: **maria@it.uc3m.es**

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. From June 2002 to December 2007 he worked at NEC Europe Ltd. in Heidelberg, Germany, in the Mobile Internet Group. 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. He is currently working on interworking architectures spanning 3GPP, WiMAX forum, and IETF standardization bodies. 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. E-mail: **telemaco.melia@alcatel-lucent.com**