Network-Based Mobility Management in the Evolved 3GPP Core Network

Irfan Ali, Motorola Inc.
Alessio Casati, Alcatel-Lucent
Kuntal Chowdhury, Starent Networks
Katsutoshi Nishida, NTT DoCoMo Inc.
Eric Parsons, Nortel Networks
Stefan Schmid, NEC Europe Ltd.
Rahul Vaidya, Samsung India Software Operations

ABSTRACT

A key aspect of the 3GPP system architecture evolution is the specification of an evolved packet core that supports multiple access networks. The EPC enables operators to deploy and operate one common packet core network for 3GPP radio accesses (E-UTRAN, UTRAN, and GERAN), as well as other wireless and wireline access networks (e.g., eHRPD, WLAN, WIMAX, and DSL/Cable), providing the operator with a common set of services and capabilities across the networks. A key requirement of the EPC is to provide seamless mobility at the IP layer as the user moves within and between accesses. This article provides an overview of the EPC specifications that use a network-based mobility mechanism based on Proxy Mobile IPv6 to enable mobility between access networks. An important facet of providing seamless mobility for a user's sessions across technologies is to ensure that quality of service is maintained as the user moves between accesses. An overview of the "off-path" QoS model to supplement PMIPv6 is also provided.

INTRODUCTION

The desire of Third Generation Partnership Project (3GPP) operators to maintain a competitive wireless network for the years 2010 to 2020 has been the key driver in the standardization effort known as system architecture evolution (SAE). The standardization effort has two primary objectives. One objective is to create a new radio access network, called evolved-universal mobile telecommunications system (UMTS) terrestrial radio access network (E-UTRAN), based on orthogonal frequency division multiplexing (OFDM) radio technology that significantly increases data rates for mobile terminals, lowers end-to-end latency for real-time communications, and reduces set-up times for new connections. The other objective is to create a common packet core network, the evolved packet core (EPC), to support mobile services, not only over the 3GPP defined-radio access technologies, but also over other non-3GPP defined-radio access technologies, such as wireless local area network (WLAN), worldwide interoperability for microwave access (WiMAX), and code division multiple access (CDMA)2000.

An important aim of the EPC is to provide seamless service continuity for multi-mode terminals as these terminals move from one radio access technology to another. These requirements are specified in 3GPP TS 22.278 [1]. Two different mobility approaches were specified for the EPC to achieve mobility between 3GPP and non-3GPP access systems, namely the network-based mobility protocol Proxy Mobile IPv6 (PMIPv6) [2] and client-based mobility protocols Dual-Stack Mobile IPv6 (DSMIPv6) [3] and Mobile IPv4 [4]. This article provides an overview of how PMIPv6 is used to achieve seamless handovers across different access systems connected to the EPC. Apart from providing session continuity, the EPC also is required to provide quality of service (QoS) support as user equipment (UE)[1] moves between the different access technologies. The interaction of PMIPv6 with QoS support also is covered in this article.

The remainder of this document is organized as follows. The next section describes the basic idea of network-based mobility management. We then discuss how the EPC uses network-based mobility management and the architectural aspects, interfaces, and challenges (e.g., QoS management). The following section provides the handover flows for both optimized and non-optimized inter-access system handovers. The final section concludes the article and identifies future work.

[1] *In the context of 3GPP, the user equipment (UE) describes the device that is used to communicate with the network (e.g., a mobile terminal or a data card in a laptop computer).*

[2] *No interface from the PCRF to ePDG in untrusted non-3GPP IP access has been defined in the Release 8 version of the EPC.*

0163-6804/09/$25.00 © 2009 IEEE

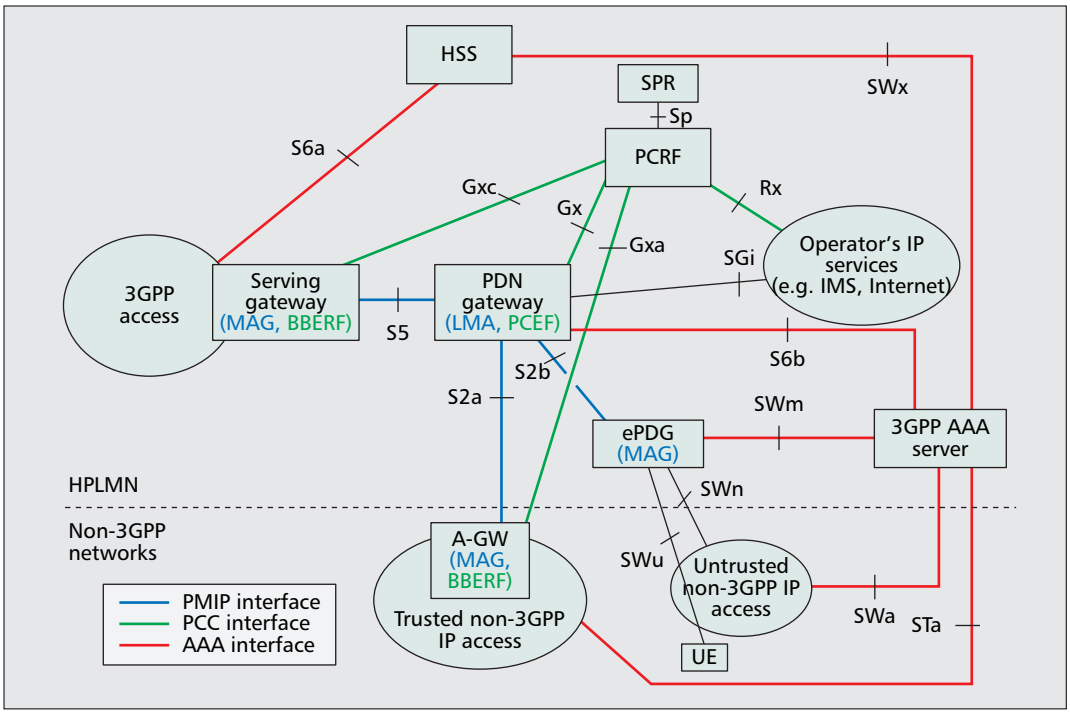

Figure 1. *The PMIPv6-based mobility architecture of the evolved packet system.*

IP-based mobility management enables the UE to preserve IP address(es), even when the UE changes its point of attachment to the network. There are two basic approaches to providing IP-based mobility management: network-based mobility management and client-based mobility management.

Network-Based IP Mobility Management

IP-based mobility management enables the UE to preserve IP address(es), referred to as home address(es) in the rest of the article, even when the UE changes its point of attachment to the network. There are two basic approaches to providing IP-based mobility management: network-based mobility management and client-based mobility management.

In the case of network-based mobility management, the network (e.g., access gateway), on detecting that the UE has changed its point of attachment, provides the UE with the same IP address that it had at its previous point of attachment. The network entity providing the IP address to the UE also handles updating the mobility anchor in the network so that the packets arrive at the new point of attachment of the UE. The UE is not aware of the mobility management signaling within the network. In contrast, for client-based mobility management, the UE obtains a new local-IP address (also referred to as care-of-address) when it moves to a new point of attachment. It is then the responsibility of the UE to update its home agent, which maintains a binding between the care-of-address and the home address of the UE.

3GPP has closely investigated the mobile operator requirements from a service aspect point of view [1]. The requirement to provide handover capability within and between access systems with no perceivable service interruption has been identified. This means that the delay introduced by the mobility management procedure must be minimized. Efficient use of wireless resources is another requirement for mobility management because wireless resources could be a bottleneck. Finally, it is generally desirable to minimize UE involvement in mobility management to improve the battery life of the terminal. Because network-based mobility management fulfills these requirements well, PMIPv6 was adopted as the IP mobility protocol for mobility between 3GPP and non-3GPP accesses and as an option for intra-3GPP access mobility.

PMIPv6 [2] introduces two new functional entities:

- The local mobility anchor (LMA), the equivalent of a home agent, which is the topological anchor point for the home network prefix(es) and manages the binding state of the mobile node.
- The mobile access gateway (MAG), which acts as the proxy (foreign) agent for the terminal and handles the mobility signaling (e.g., a proxy binding update) toward the LMA upon terminal movement.

Network-Based Mobility Architecture of the EPC

The focus of this article is on the analysis of network-based mobility management and in particular on the option based on PMIPv6 [2]. The relevant aspects of the EPC architecture are shown in Fig. 1. The functional entities related to PMIP-based mobility management are indicated in blue, whereas the functional entities related to policy and charging control (PCC) are shown in green. Note that although GPRS Tunneling Protocol (GTP)v2 (an evolution of the existing 3GPP GTP protocol) can be used alternatively for mobility management within 3GPP accesses only, PMIPv6 is used for network-based IP mobility management between 3GPP and non-3GPP accesses.

A UE can access the EPC from both 3GPP accesses and non-3GPP accesses. Non-3GPP accesses are classified into trusted and untrusted accesses. An untrusted access is one that requires the operator to deploy an evolved packet data gateway to provide the appropriate security to enable the UE to securely access the EPC.

Figure 1 shows that a UE can access the EPC from both 3GPP accesses and non-3GPP accesses. Non-3GPP accesses are classified into trusted and untrusted accesses. An untrusted access is one that requires the operator to deploy an evolved packet data gateway (ePDG) to provide the appropriate security, that is, authentication of the UE and data encryption (based on IPsec/IKEv2), to enable the UE to securely access the EPC. For trusted non-3GPP accesses, an ePDG is not required.

The PMIPv6 mobility architecture of the evolved packet system (EPS) includes the following entities:

PDN Gateway (PDN GW): The PDN GW provides access to different packet data networks (PDNs) by assigning an IP address to the UE from the address space of the PDN. This address can be an IPv4 address, an IPv6 prefix, or both. The PDN GW is also the mobility anchor point for the address/prefix of the UE and acts as a PMIPv6 LMA.

Serving Gateway (S-GW): The S-GW includes the PMIPv6 MAG functionality for IP mobility management. The S-GW acts also as a layer-2 mobility anchor, as the UE moves within 3GPP accesses (i.e., E-UTRAN, UTRAN, and GERAN).

Access Gateway (A-GW): The A-GW belongs to trusted non-3GPP accesses and includes the PMIPv6 MAG functionality for IP mobility management. It also can manage layer-2 mobility as the UE moves within the trusted non-3GPP access.

Evolved Packet Data Gateway (ePDG): For untrusted non-3GPP accesses, the ePDG secures the access of the UE to the EPC by means of an IP Security (IPSec) tunnel between itself and the UE. In case local mobility occurs within the untrusted non-3GPP access, MOBIKE [5] is used to update the IPSec security association.

In addition to the functionality provided by the PMIPv6 specification, there are several additional requirements that the EPC must fulfill that have impact on PMIPv6. Some of the key requirements and impacts are as follows:

Support of IPv4 UE: The EPC requires support for IPv4 only, IPv6 only, and dual stack IPv4 and IPv6 hosts. IPv4 support in PMIPv6 is defined in the IPv4 extension draft [6] to PMIPv6.

Simultaneous access to multiple PDNs: A PDN is an IP domain that the UE wants to communicate with. Examples of PDNs are the Internet, a corporate network, and an operator's private network. An access point name (APN), is used to identify a PDN. The EPC assigns to the UE an IP address that belongs to the PDN to which it is connected and allows the UE to simultaneously access multiple PDNs. Extensions defined in RFC 5149 [7] to PMIPv6 enable the MAG to include the APN in the proxy binding update (PBU) request, such that the PDN GW can assign an IP address to the UE from the appropriate PDN. Furthermore, multiple bindings for a particular UE, one for each PDN, must be supported by the LMA.

Support for overlapping address spaces of different PDNs: In addition to the UE being able to simultaneously access multiple PDNs, the IPv4 addresses assigned to the UE in different PDNs can potentially overlap, for example, the use of private address spaces. To allow for overlapping IPv4 address spaces, the generic routing encapsulation (GRE) key extensions for tunneling packets between the LMA and MAG PMIPv6 [8] are employed. This PMIPv6 extension enables the network to disambiguate traffic related to different PDNs based on the GRE key — even when the IP addresses allocated to the UE by the PDNs are identical.

Unique UE identification across accesses on EPC PMIPv6 interfaces: Because the UE can access the EPC from different accesses, and each access can use its own UE identity scheme, the problem of uniquely identifying a UE on the different PMIPv6 interfaces S5, S2a, and S2b arises. To resolve this issue, 3GPP has specified that an international mobile subscriber identity (IMSI)-based network-access identifier (NAI), where the IMSI is the identity that currently is used to identify the UE in GSM/UMTS networks, is used on all PMIPv6 interfaces. Hence, non-3GPP accesses must obtain the IMSI of the UE during access authentication (either from the UE or from the home subscriber server/authentication, authorization, and accounting (HSS/AAA) and use the IMSI-based NAI on the PMIPv6 interfaces. This does not require any extensions to PMIPv6 because the specification in conjunction with RFC 4283 [9] allows for an IMSI-based NAI to be used as the UE identity in the PBU/proxy binding acknowledgment (PBA).

Providing a PDN GW address to the target access: The EPC can support multiple PDN GWs serving the same PDN. As a consequence, the MAG function in the target access network must identify to which PDN GW to send the PBU upon handover. TS 23.402 [10] specifies that the PDN GW identity along with the corresponding APN is stored in the HSS/AAA and provided to the MAG in the target access during authentication at handover attach. An extension to the Diameter protocol addresses this issue [11].

In addition to the above requirements, signaling of QoS and charging information must occur in the EPC as the UE moves across different access networks. An overview of the architectural aspects related to PCC and QoS provisioning is provided in the next subsection.

PCC and QoS Provisioning

The objective of the PCC architecture is to enable operators to provide QoS to subscribers for IP-based service data flows and charge for the resources provided based on the user's subscription information and other policy information related to the access, network, and service. To not overload PMIPv6 signaling with QoS and PCC aspects, an "off-path" PCC model was developed and documented in TS 23.203 [12].

The key network entities and interfaces of the PCC architecture are illustrated in Fig. 1 and are as follows:

- Subscription profile repository (SPR): The SPR contains the QoS and charging subscription policies for the users.

- Policy and charging rules function (PCRF): The PCRF makes policy decisions for a UE upon request and provides charging and QoS rules to the policy and charging enforcement function (PCEF) and QoS rules to the bearer binding and event reporting function (BBERF) for enforcement. The charging rules contain information to identify flows (e.g., five tuple) along with charging rates. The QoS rules contain information to identify flows along with the QoS behavior to be enforced, such as the QoS class indicator, maximum bit rate, and so on.
- Policy and charging enforcement function: The PCEF performs the function of IP flow detection and charging based on the PCC rules provided by the PCRF.
- Bearer binding and event reporting function (BBERF): The BBERF performs the function of applying the QoS rules to service data flows in the access network, binding of the IP flows to access bearers, and reporting of QoS-related events (e.g., change-of-access technology) to the PCRF.

The following example scenario helps explain the PCC architecture in more detail. Assume a user is placing a voice over IP (VoIP) call through the IP multimedia subsystem (IMS) situated in the operator's IP services domain. During the call set up, a SIP server in IMS provides QoS-related information (e.g., application type, required bandwidth) and the required information for identification of the service data flows (e.g., the set of five tuples to identify the RTP packets of a VoIP flow) to the PCRF, over the Rx interface. Rx is a Diameter-based interface used by the IMS to request QoS resources for a given set of IP flows and also to be informed by the PCRF about the status of the resource allocation. Based on the operator's policies stored in the PCRF, the user's subscription information obtained from the SPR through the Sp interface, and the application-related information dynamically signaled across the Rx, the PCRF determines both the charging rate to be applied and the QoS behavior (e.g., guaranteed bit rate or not, delay and drop targets, maximum bit rates) to be provided to the set of IP flows requested by the application function. The PCRF encapsulates this request in a so-called PCC rule and forwards it to the PCEF located in the PDN GW node for charging enforcement.

The QoS information with the associated IP-flow description also must be provided to the access network through the S-GW or A-GW node (for 3GPP and trusted non-3GPP access, respectively). Because the PMIPv6 protocol is used only for mobility management and has no notion of QoS tunnels, the off-path paradigm relies on the signaling of QoS information off-the-bearer-path and from the PCRF directly to the access network. The PCRF has a separate interface, namely Gxc for 3GPP accesses and Gxa for trusted non-3GPP accesses,[2] toward the functional entity responsible for QoS enforcement in the access network, referred to as the BBERF.

Inter-Access System Mobility Flows

This section provides the handover flows to illustrate how the architecture principles are applied. Inter-access system handover flows according to TS 23.402 [10] are classified into two categories: non-optimized handover flows and optimized handover flows. Non-optimized handover flows cover a situation where the source network is not involved in preparing resources in the target network. In the case of optimized handovers, the source network is involved in preparing resources in the target network. Optimized handovers are typically used when the UE is unable to transmit and receive in both the source and target networks simultaneously. This section first covers the high-level flows for PMIPv6-based, non-optimized handovers between access networks, and then we present the corresponding flows for optimized handovers.

For the flows in the following subsections, it is assumed that the network initiates the set up of QoS resources on behalf of the UE. Details of a UE-initiated QoS set up are provided in TS 23.402 [10] and TS 23.203 [12].

Non-Optimized Handovers

Figure 2 provides the high-level flow when a UE attaches to a trusted non-3GPP access that is connected to the PDN GW using PMIPv6 on the S2a interface, initiates a VoIP call through IMS resulting in the set up of QoS for the VoIP media flows, and then hands over to a 3GPP access with PMIPv6 used on the S5 interface. Steps 1 through 9 are related to the UE attaching to the trusted non-3GPP access network. Steps 10 through 15 are related to setting up the VoIP call and the QoS establishment for the media flow. Steps 16 through 24 are related to the UE discovering and handing over to the 3GPP access. Steps 25 through 28 are related to the cleanup of resources in the trusted non-3GPP access.

The attachment of the UE to the EPC through a trusted non-3GPP access is triggered by the UE sending a layer 2 or layer 3 attach trigger (Step 2), for example, an *attach request* message. The UE authenticates with the trusted non-3GPP access network. In case the non-3GPP access supports multiple PDNs, the PDN to which the UE must be connected is either provided by the UE in the attach request message or is obtained from the HSS/AAA. For the set up of default QoS resources, the BBERF in the non-3GPP access registers itself with the PCRF, providing the UE identity and the APN to the PCRF. The MAG function in Step 5 sends a PBU to the LMA to obtain the IP address of the UE. The PBU contains the IMSI-based NAI of the UE, the APN to which the UE must be connected and a GRE key, which the PDN GW should use to tunnel downlink packets for the UE. Based on the APN in the PBU, the PDN GW provides an IP address to the UE in the PBA that is further relayed to the UE (Steps 8 and 9), completing the attachment of the UE to the non-3GPP access. In the PBA, the PDN GW also provides the GRE key that the MAG should

Because the PMIPv6 protocol is used only for mobility management and has no notion of QoS tunnels, the off-path paradigm relies on the signaling of QoS information off-the-bearer-path and from the PCRF directly to the access network.

For dual-radio-capable UEs, non-optimized handovers can provide a seamless handover experience to the end user. A "make-before-break" can be achieved as the UE can still maintain connectivity through the source access while it establishes connectivity over the target access.

use for tunneling the uplink traffic of the UE. In parallel, the PDN-GW registers itself with the PCRF and obtains charging rules for the default connectivity of the UE. The PDN GW also registers its address and the APN to which the UE is connected with the HSS through the AAA server. The HSS stores this information to be provided to the 3GPP access at a later stage when the UE hands over to the 3GPP access.

When the UE wants to set up a VoIP call, SIP signaling occurs between the UE and the SIP server (Step 10). In turn, the SIP server requests the PCRF to set up QoS resources for the UE in the access network by providing the identity of the UE and the relevant information to enable identification of the IP flow and the QoS to be applied to the flow. The PCRF determines the charging rules and the QoS rules to be applied based on the subscription information. The PCC charging rules are provided to the PDN GW (Step 13), and the QoS rules are provided to the BBERF in the trusted non-3GPP access network (Step 14). The BBERF then sets up a bearer with the appropriate QoS for the VoIP media (Step 15). After these steps, the VoIP data traffic is carried over the dedicated VoIP bearer; the other traffic remains on the default bearer.

When the UE decides to hand over to the 3GPP access, the UE initiates the attach procedure to the 3GPP access (Step 17). In the attach request, the UE indicates that the attach type is *handover attach* and is hence requesting to be attached to the same PDN GW and also to be provided with the same IP address that it had when attached through the trusted non-3GPP access. During the authentication procedure (Step 18), the HSS provides the 3GPP access with the IP address of the PDN GW of the UE. The BBERF function in the 3GPP access registers itself with the PCRF and obtains the QoS rules for the default traffic but also for the VoIP traffic (Step 19). It sets up the required bearer resources during the attach procedure itself to avoid disruptions due to lack of resources in the target access.

The MAG function in the serving GW then sends a PBU to the LMA in the PDN GW in which the hand-off indicator value is set to *handoff* between two interfaces of the UE (Step 21). The LMA updates the PMIPv6 tunnel to point to the 3GPP access and provides the IPv6 home network prefix and/or the IPv4 home address of the UE to the MAG function in the 3GPP access as part of the PBA (Step 23). In parallel, the PDN GW also updates the PCRF that the UE is connected to the EPC through the 3GPP access and obtains the corresponding charging rules.

In the EPC, the PDN GW initiates the resource release procedure in the source access system after the user-plane tunnel has been switched. The PDN GW initiates proxy binding revocation indication (BRI) as defined in [13], which triggers the resource release procedure in the source access (Steps 25–27). The BBERF in the non-3GPP access also deregisters itself with the PCRF (Step 28).

For dual-radio-capable UEs, where the radios of both access technologies can transmit and receive packets simultaneously, non-optimized handovers can provide a seamless handover experience to the end user. A "make-before-break" can be achieved as the UE can still maintain connectivity through the source access while it establishes connectivity over the target access.

Optimized Handovers

Whereas the non-optimized handover is well suited for dual-radio-capable terminals, for single-radio terminals it would lead to substantial interruption time during inter-technology handovers. As a result, optimized handovers were defined for specific instances of inter-technology mobility, allowing for seamless handovers even for single-radio terminals.

The architecture used for optimized handover between CDMA2000 eHRPD and an E-UTRAN is shown in Fig. 3.

The additional network entities in this architecture that were not discussed yet are:

- Mobility Management Entity (MME): The MME is a control-plane entity in an E-UTRAN access network responsible for managing the mobility of the UE. It also authenticates the UE with the HSS. Details of the MME functions are described in TS 23.401 [14].
- HRPD Access Network (HRPD AN): The HRPD AN is the network entity in the evolved eHRPD access network that is responsible for managing the mobility of the UE.
- HRPD Serving Gateway (HSGW): The HSGW is an entity in the eHRPD access network that performs functions similar to that of the serving GW and MME in 3GPP accesses. The HSGW contains the MAG and the BBERF functions.

Optimized handovers between E-UTRAN and eHRPD rely on the UE managing the context establishment within the target access network while still operating on the source system. This is achieved through a tunnel with the target system allowing the UE to interact with the target system with minimal support from the source system. The S101 interface is used for tunneling the UE traffic to the target access system. The source system still provides network control to trigger interactions between the UE and the target system but otherwise is not involved in the establishment of context in the target system. The S103 interface is used for temporarily forwarding the downlink traffic of a UE from the source to the target system during the handover execution.

To describe the different phases of an optimized handover, the following terms are introduced:

- **Pre-Registration**: In the pre-registration phase, the UE communicates with the target system by tunneling registration signaling through the source system to prepare session context (e.g., authentication, session parameters).
- **Preparation**: The assumption is that the UE has performed pre-registration and now has been instructed by the source system to initiate a handover. In this phase, the target system prepares for the UE to handover and provides the UE with the required

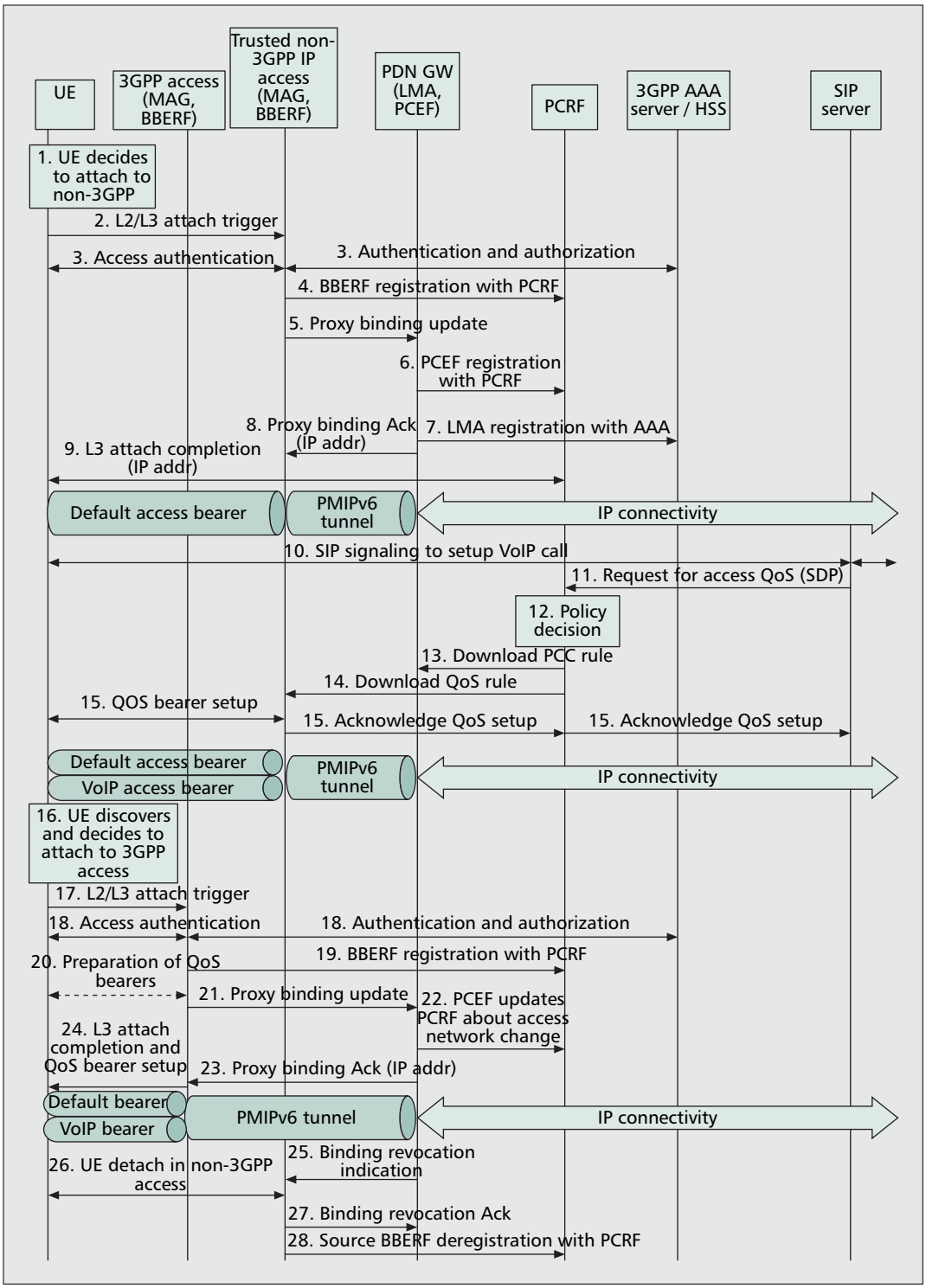

Figure 2. *Illustration of the scenario when a UE attaches to non-3GPP access, initiates a service, and then hands over to 3GPP access.*

Optimized handovers between E-UTRAN and eHRPD rely on the UE managing the context establishment within the target access network while still operating on the source system. This is achieved through a tunnel with the target system where the UE can interact with the target system with minimal support from the source system.

information to establish radio connectivity over the target access network.

- **Execution**: In the execution phase, the UE uses the information provided by the target system in the preparation phase (delivered through the source system) to switch radio technologies.

Release 8 of the EPC standard only defines optimized handover between eHRPD and E-UTRAN. Future releases may also define optimized handover with other non-3GPP access networks.

Figure 4 provides the flow for optimized handover of the UE from E-UTRAN to eHRPD. It is assumed that the UE already is attached to the E-UTRAN access and has an active VoIP call whose media traffic flows through the VoIP bearer with appropriate QoS in the E-UTRAN access.

In anticipation of possible handover as the UE

At the end of pre-registration, the UE has established its credentials in the target eHRPD access. Also, the BBERF in the target eHRPD access has obtained QoS rules for all active sessions and can prepare resources in anticipation of a handover.

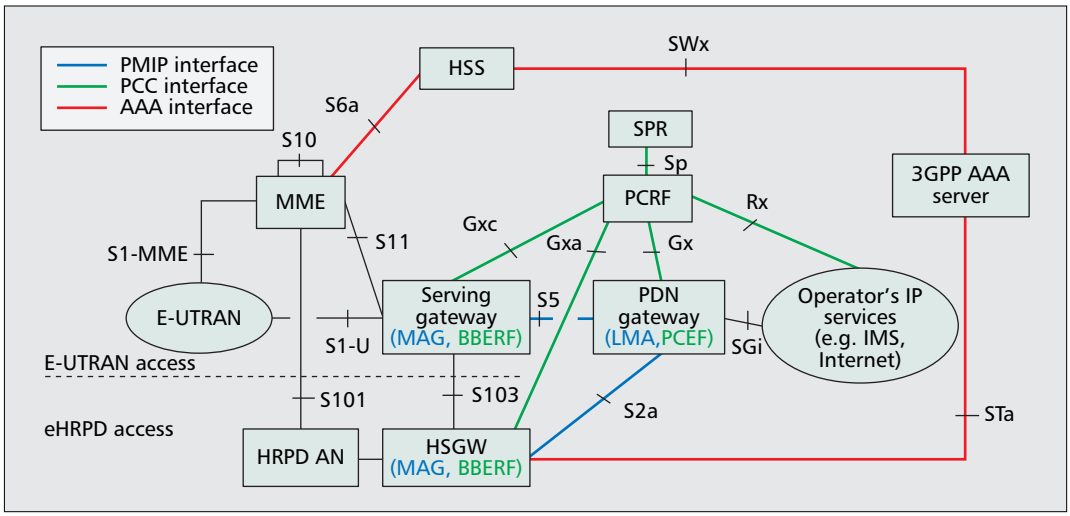

Figure 3. *Architecture for optimized handovers between E-UTRAN and eHRPD access.*

approaches the source technology coverage boundary, the source network provides system information (broadcast or unicast) indicating that the UE should pre-register with the target system. The purpose of pre-registration is to avoid lengthy delays in the handover procedures because pre-registration can take several seconds. The steps for pre-registration are shown in the steps A1 through A7. The pre-registration messages are sent by the UE as direct transfer messages to the MME through the eNodeB. The eNodeB adds the identification of the closest target eHRPD cell to enable the MME to determine the HRPD AN to tunnel the UE messages. At the end of pre-registration, the UE has established its credentials in the target eHRPD access. Also, the BBERF in the target eHRPD access has obtained QoS rules for all active sessions and can prepare resources in anticipation of a handover.

Steps B1 through B4 correspond to the preparation phase of the optimized handover. When the UE approaches the technology coverage area boundary, radio conditions dictate that an inter-technology handover is required. For this, the network configures the UE to report when the source system signal quality drops below a specific threshold, and the target technology is above a specific threshold. After the source system receives this indication, it triggers the UE to initiate handover preparation and execution procedures (Step B2). As part of the preparation phase, the UE requests from the target system (through the source system) to allocate the required radio resources and the establishment of the S103 tunnel for forwarding the UE traffic from E-UTRAN to eHRPD (Step B3–B4).

Steps C1 through C9 correspond to the execution phase of the optimized handover. In this phase, the UE uses the traffic channel allocation information provided during the preparation phase to perform the handover procedures. Although there is no explicit context transfer from the source system to the target system, the entire procedure is controlled by the source system so as to provide the operator greater control. The MAG in the HSGW updates the bearer tunnel by exchanging a PBU/PBA with the LMA in the PDN GW. The PDN GW interacts with the PCRF to obtain charging rules corresponding to eHRPD access for the user traffic. Steps C6 through C9 are for the cleanup of resources in the source network.

The optimized handover procedures in the opposite direction, that is, from eHRPD to E-UTRAN, follow the same basic principles. The main difference is that the handover execution phase takes place immediately after the completion of the pre-registration phase, and no data forwarding is performed through the S103 tunnel.

Summary and Future Work

This article presented the motivation, design, and realization of inter-access system mobility support based on Proxy Mobile IPv6 for the 3GPP EPC, enabling a common packet core architecture to be used for a wide range of access technologies. The document also addresses the issues of QoS provisioning and seamless handover support. Detailed flows illustrating the use of PMIPv6 to achieve non-optimized handovers between 3GPP accesses and other non-3GPP accesses, as well as optimized handovers between E-UTRAN and eHRPD were provided.

Release 8 is the first release of the EPC specification, and additional work is required to enhance and adapt the new system to the ever changing industry requirements. For instance, further study is required to determine how to support the UE to access the EPC through multiple-access networks simultaneously while providing mobility management and controlling the routing of individual IP flows between the different radio interfaces.

Finally, as operational experience for "always best-connected terminals" increases, optimizations, and lessons learned from the field will drive additional enhancements of the EPC.

References

[1] 3GPP TS 22.278 Tech. Spec., "Service Requirements for Evolution of the 3GPP System, Stage 1, Release 8," June 2008.
[2] IETF RFC 5213, "Proxy Mobile IPv6," Aug. 2008.

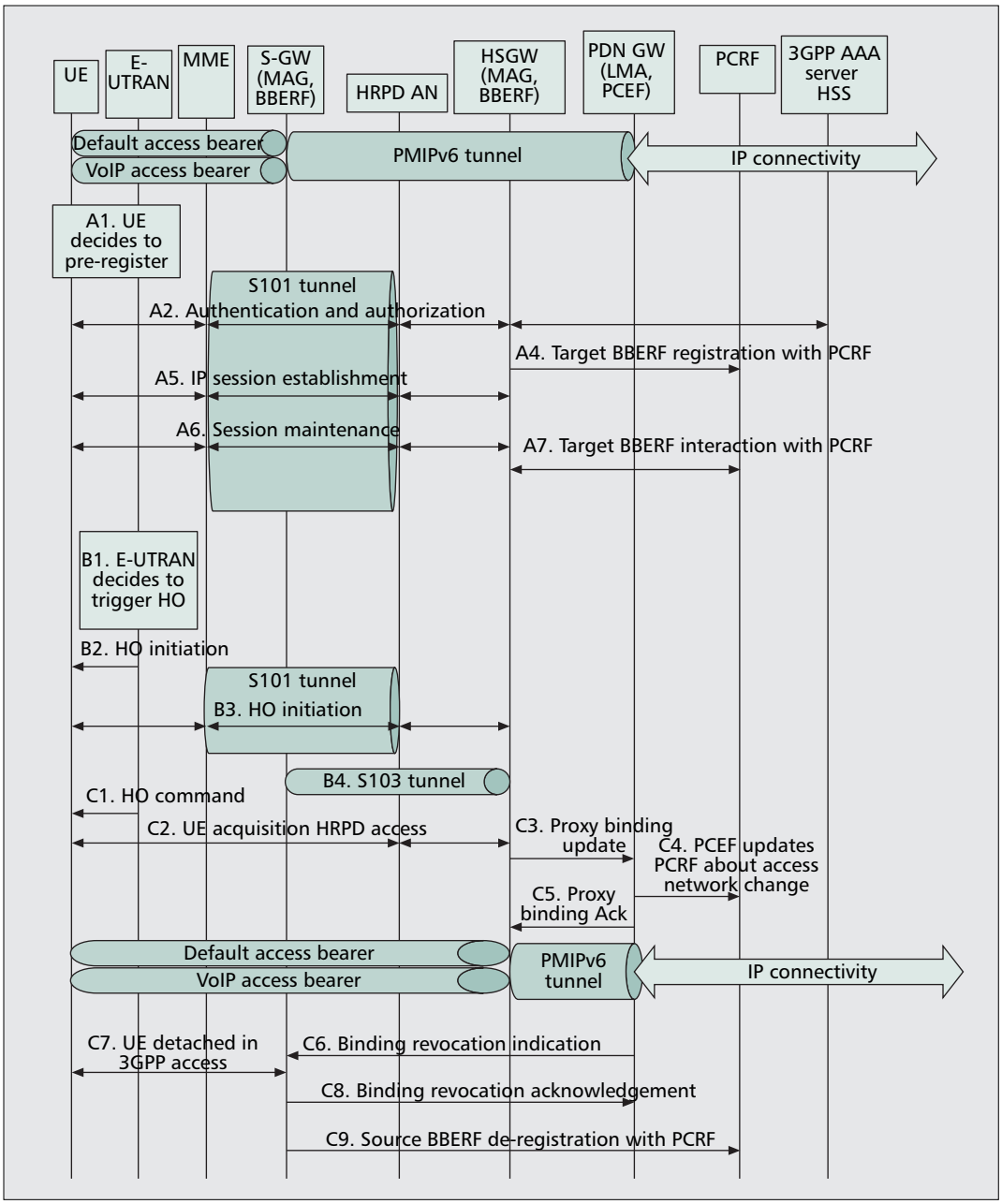

Figure 4. *Flow for optimized handover from E-UTRAN access to eHRPD access.*

Further study is required to determine how to support the UE to access the EPC through multiple-access networks simultaneously while providing mobility management and controlling the routing of individual IP flows between the different radio interfaces.

[3] "Mobile IPv6 Support for Dual Stack Hosts and Routers," work in progress; IETF Internet draft, draft-ietf-mext-nemo-v4traversal-05.txt
[4] IETF RFC 3344, "Mobility Support for IPv4," Aug. 2002.
[5] IETF RFC 4555, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)."
[6] IETF Internet-draft, draft-ietf-netlmm-pmip6-ipv4-support-04.txt, "IPv4 Support for Proxy Mobile IPv6," work in progress.
[7] IETF RFC 5149, "Service Selection for Mobile IPv6," Feb. 2008.
[8] "GRE Key Option for Proxy Mobile IPv6," work in progress; IETF Internet draft, draft-muhanna-netlmm-grekey-option-04.txt
[9] IETF RFC 4283, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)," Nov. 2005.
[10] 3GPP TS 23.402 Tech. Spec., "Architecture Enhancements for Non-3GPP Accesses, Release 8," work in progress, Aug. 2008.
[11] "Diameter Proxy Mobile IPv6: Support for Mobility Access Gateway and Local Mobility Anchor to Diameter Server Interaction," work in progress; IETF Internet draft, draft-korhonen-dime-pmip6-02
[12] 3GPP TS 23.203 Tech. Spec., "Policy and Charging Control Architecture," work in progress, June 2008.
[13] "Binding Revocation for IPv6 Mobility," work in progress, IETF Internet draft, draft-ietf-mext-binding-revocation-01.txt
[14] 3GPP TS 23.401 Tech. Spec., "GPRS Enhancements for E-UTRAN Access, Release 8," work in progress, Aug. 2008.

Additional Reading

[1] IETF RFC 4831, "Goals for Network-Based Localized Mobility Management," Apr. 2007.
[2] IETF RFC 3775, "Mobility Support in IPv6," June 2004.

Biographies

Stefan Schmid (stefan.schmid@neclab.eu) received his M.Sc. in computer science (Dipl.-Inf.) from the University of Ulm, Germany, in 1999. In 2002 he received his Ph.D. in computer science from Lancaster University. After his post-doctoral research, he joined NEC Laboratories Europe in

Heidelberg where he now leads the Next-Generation Networking research group. In addition, he actively contributes to the standardization of core network and systems aspects in 3GPP. He has published many scientific papers in international workshops, conferences, and journals.

IRFAN ALI received his Ph.D. in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, New York, in 1993. Since 1998, he has been with Motorola, where he works on design and standardization of cellular network infrastructure. His research interests are in system architecture design, mobility management, quality of service, and LEO systems. From 1993 to 1998, he was with the GE Corporate Research & Development Center. He holds 13 patents and has published several papers and a book.

KATSUTOSHI NISHIDA obtained a Master's degree in electronics, information, and communications engineering from Waseda University in 2002. Since 2002 he has been with NTT DoCoMo Inc., where he worked on IP-based mobility management for the All IP Network. In 2004 he started the standardization activity for the network-based mobility management protocol in IETF, led the establishment of the new WG (NETLMM WG), and took part in the standardization of the network-based mobility protocol. At the same time, he participated in 3GPP standardization to realize the IP-based all IP core network.

ALESSIO CASATI obtained a Master's degree in computer and automation systems engineering from the Polytechnic of Milan in 1995. He is with Alcatel Lucent, responsible for standardization of core network and systems aspects of 3GPP systems. He was previously involved in R&D of the UMTS packet core and with Alcatel Central R&D for video on demand systems and IP and ATM networking projects. He has published two books in the area of convergence and mobile data networks.

KUNTAL CHOWDHURY received a B.E. degree from NIT, Surat, India, and an M.Sc. in telecommunications from Southern Methodist University, Dallas, Texas, in 2002. He is responsible for standards participation and technology evolution at Starent Networks. Prior to joining Starent, he held various technical positions at Nortel, Motorola, and Glenayre. He started his career as a systems engineer in 1993. He authored/co-authored numerous RFCs, drafts, and papers in the areas of mobility management and AAA.

ERIC PARSONS received his Ph.D. in computer science from the University of Toronto in 1997. He is currently with Nortel, where he works on architecture and standards for wireless systems. He is also an adjunct professor with Carleton University. He has published numerous papers in the area of system performance and multiprocessor operator systems, and holds several patents.

RAHUL VAIDYA completed a Master's degree in computer science and engineering from the Indian Institute of Science, Bangalore, India, in 2004. Since 2004, he has worked for Samsung India Software Operations, where he works on standardization of mobile networks. His research interests include system architecture and design, mobility management, interworking of networks, vertical handovers, and quality of service.