

# A 3GPP System Architecture Evolution Virtualized Experimentation Infrastructure for Mobility Prototyping (Invited Paper)

Miguel Gómez Rodríguez  
Telefónica I+D  
Emilio Vargas, 6  
28043 Madrid (Spain)  
+34 91 337 41 40  
miguelg@tid.es

Fermín Galán Márquez  
Telefónica I+D  
Emilio Vargas, 6  
28043 Madrid (Spain)  
+34 91 337 45 59  
fermin@tid.es

Emilio J. Torres Mateos  
Telefónica I+D  
Emilio Vargas, 6  
28043 Madrid (Spain)  
+34 91 337 40 85  
ejtm@tid.es

## ABSTRACT

The 3GPP System Architecture Evolution (SAE) is a very attractive environment from the service provisioning perspective, thanks to the variety of access technologies and mobility features introduced. In such a diverse environment, experimentation infrastructures (i.e., testbeds) become a key instrument for telecom operators, since mobility solutions and service behavior in their presence need to be validated under the different possible configurations from early development stages. However, the complexity of 3GPP SAE scenarios hinders conventional testbeds from adhering to cost-effectiveness and business-oriented criteria, due to the high infrastructure and operational costs involved. In order to overcome these limitations, this paper proposes an experimentation infrastructure that, based on combining virtualization techniques with several of the available open source IMS and mobility toolkits, allows the easy creation and deployment of complex 3GPP SAE network emulation scenarios while minimizing the associated expenditures.

## Categories and Subject Descriptors

C.4 [Performance of Systems]: Modeling techniques.

## General Terms

Measurement, Performance, Experimentation.

## Keywords

Testbeds, Virtualization, 3GPP System Architecture Evolution, IMS.

## 1. INTRODUCTION

As part of its work towards the enhancement of the 3G Mobile System, the 3<sup>rd</sup> Generation Partnership Project (3GPP) is currently undertaking a System Architecture Evolution (SAE) study whose objective is twofold. First, it aims at improving the packet-

switched domain in order to achieve higher data rates and lower latency, thus obtaining an Evolved Packet Core (EPC) optimized for the provision of advanced IP-based real-time multimedia services. Secondly, it focuses on complementing the currently available 3GPP access networks (i.e., the GSM/EDGE Radio Access Network and the UMTS Terrestrial Radio Access Network) with a comprehensive set of access technologies, ranging from radio access networks like Worldwide Interoperability for Microwave Access (WiMAX) or Wireless Local Area Network (WLAN) to wireline technologies such as Digital Subscriber Line (DSL).

As a consequence of these goals, mobility enhancements are a key element of the 3G System Architecture Evolution since, due to the potential availability of a heterogeneous set of access networks per domain, mobility can no longer be exclusively handled at access level. Therefore, as we will discuss in detail in Section 2, a new series of mobility-specific functions have been included in the Evolved Packet Core in order to allow users to switch their access network with no noticeable impact on their active service sessions.

Although this environment is very appealing from the service provisioning point of view, it also presents a series of challenges from the validation and evaluation perspective that might slow down both the adoption of such mobility solutions and service development for such systems. In first place, the number of possible mobility configurations increases considerably when compared to previous releases, due to the combinations resulting from the different access options, the availability and location of the mobility functions, and the mobility solution in place. Additionally, the complexity of each mobility scenario is also larger since, in order to enable potential inter-technology handovers, even intra-technology configurations are more complex in terms of involved interfaces and network elements.

Accordingly, setting up a SAE testbed that enables to validate such mobility solutions themselves or service behavior in their presence constitutes a very resource-consuming and effort-intensive task. Each configuration comprises many network elements, most of the times based on expensive specific hardware and involving complex configuration processes. Moreover, testing every possible network scenario requires either an extensive testbed including all possible options or modifying the network configuration in order to recreate each scenario sequentially. None of these options is particularly convenient, since the former

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*Tridentcom 2008*, March 18 - 20, 2008, Innsbruck, Austria.

Copyright 2008 ACM 978-1-60558-009-8.

maximizes hardware expenditure while the latter reduces testbed availability and involves higher operation costs.

In order to overcome these limitations, in this paper we propose a testing platform that, by combining virtualization techniques with several of the available open source IMS and mobility toolkits, allows the easy creation and deployment of complex multi-domain 3GPP SAE emulation scenarios, customized to the requirements of the mobility configuration or configurations under study while keeping minimal infrastructure and operation costs.

The remainder of this paper is structured as follows. First, Section 2 provides an overview of mobility in 3GPP SAE networks. Next, Section 3 outlines the requirements for SAE testbeds stemming from the environment description provided in the previous section. Section 4 introduces the SAE emulation framework proposal, highlighting how virtualization techniques are an optimal solution for fulfilling the requirements drafted in Section 3. Section 5 describes how the generic framework introduced in Section 4 may be used for mobility evaluation and testing, providing some practical testbed configurations and presenting how operators might benefit from this kind of framework and export the obtained results to real services and/or network configurations. Section 6 summarizes the conclusions that the undertaken experiences have allowed us to extract, and presents the ongoing work based on the obtained results. Finally, the acknowledgement and reference sections complete the structure of the paper.

## 2. MOBILITY IN 3GPP SAE NETWORKS

As described in the previous section, one of the main goals of the System Architecture Evolution is providing users with a new series of access options to the Evolved Packet Core, thus broadening 3G access beyond the scope of the currently available 3GPP radio technologies [1][2].

In order to integrate this heterogeneous set of access networks into a consistent mesh, mobility can no longer be considered an intra-technology issue manageable at link level. Accordingly, new network-layer mobility functions need to be introduced in the Evolved Packet Core in order to extend its mobility capabilities beyond the link-based procedures available at each access technology. As summarized in Figure 1, such mobility solutions may be adopted at two different levels, depending on the terminal's degree of involvement in the mobility process:

- Global or host-based mobility is based on the ability of the terminal to maintain a persistent globally-accessible address independently of its current point of attachment to the network. As its name indicates, it requires the terminal's awareness and involvement in the mobility process, usually by applying a mobility management protocol to map the persistent address with the temporary local address(es) available at each moment and modify accordingly the end-to-end routing of packets in order to maintain connectivity. Apart from host involvement, it also requires the presence of a Global Mobility Anchor (GMA) entity in the home network, where the permanent address of the terminal is attached and the mapping with the temporary address(es) kept.
- Local or network-based mobility [3] is intended to allow terminals to maintain connectivity when moving across a

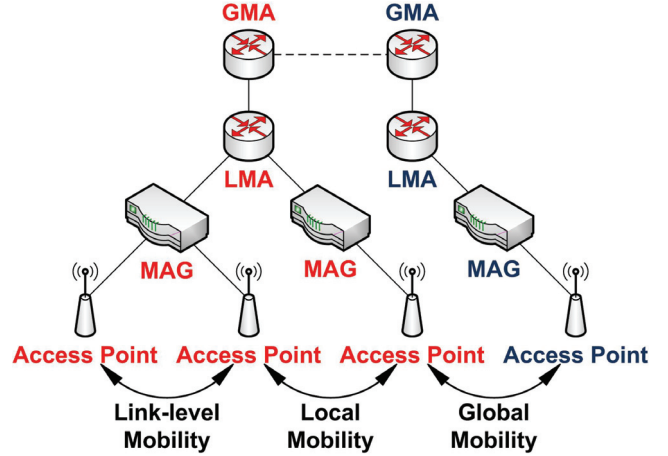


Figure 1. Mobility scopes.

certain network area, known as Local Mobility Domain. As its name indicates, this type of mobility is provided by the network with no need of terminal intervention or awareness. Local mobility is based on the presence of two network entities: the Mobility Access Gateway (MAG) and the Local Mobility Anchor (LMA). The MAG is in charge of tracking terminal location and updating it on the LMA on behalf of the terminal by means of a mobility management protocol, whereas the LMA is devoted to keeping the terminal's persistent address and routing inbound and outbound traffic.

Both mobility levels have been implemented in the Evolved Packet Core, thus covering the full mobility range depicted in Figure 1. The following sections detail the 3GPP SAE architecture, describing the network elements implementing these mobility functions and the different configurations resulting from the location of these elements and the mobility solution in place.

### 2.1 Intra-domain Mobility

As shown in Figure 2, network-layer mobility functions are implemented by three separate logical entities in the Evolved Packet Core: the Serving Gateway (S-GW), the Packet Data Network Gateway (PDN-GW or P-GW), and the Evolved Packet Data Gateway (ePDG).

In case of 3GPP access, the Serving Gateway terminates the GPRS Tunneling Protocol (GTP) interface towards the 3GPP radio access networks, and therefore is the extended equivalent of the Gateway GPRS Support Node (GGSN) of previous 3GPP

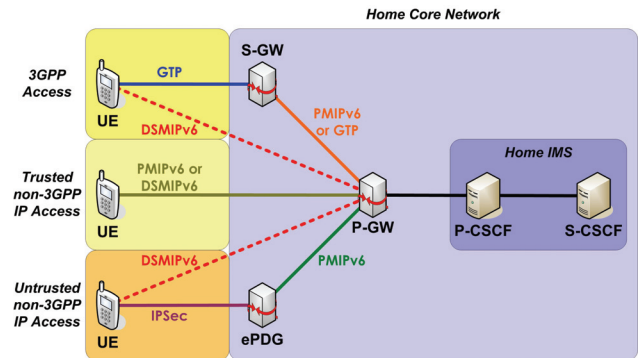


Figure 2. Non-roaming 3GPP SAE architecture.

releases. In addition, it provides IP routing features and takes the MAG role for the provision of network-based mobility. Conversely, the P-GW provides the interfacing towards packet-data networks, and takes the LMA role. As shown in the figure, local mobility management between the S-GW and the P-GW may be based on the GPRS Tunneling Protocol or on Proxy Mobile IPv6 (PMIPv6) [4], a local mobility implementation based on the Mobile IPv6 (MIPv6) [5] protocol. There are also plans for global mobility support under 3GPP access, thus making the P-GW take also the GMA role and basing global mobility management between the User Equipment (UE) and the P-GW on Dual Stack MIPv6 (DSMIPv6) [6], a MIPv6 variant for dual stack (IPv4 + IPv6) hosts. However, the implications of such mobility solution have been postponed for further study.

Thanks to the GMA and LMA functions provided by the P-GW, both local and global mobility are supported for trusted non-3GPP access networks. In case of local mobility, the MAG role is delegated to an access network router, and therefore is not provided by the Evolved Packet Core. Local mobility management between such router and the P-GW is based on PMIPv6, whereas global mobility management between UE and P-GW takes place through DSMIPv6.

Finally, in case of untrusted non-3GPP access, the adopted structure resembles that of 3GPP access networks. In this case, the ePDG provides packet tunneling features based on IPsec [7], thus securing communications in the untrusted network section and creating a traffic hub that enables the enforcement of the home network's QoS policy. In this scenario, both local and global mobility are supported as well by the GMA and LMA functions provided by the P-GW. It is worth noting that, for untrusted non-3GPP access, the MAG role cannot be delegated to the access network, and therefore is provided in the Evolved Packet Core by the ePDG. Local mobility management between the ePDG and the P-GW is based on PMIPv6, whereas global mobility management between UE and P-GW takes place through DSMIPv6.

As already described, the P-GW is the Evolved Packet Core entryway to IP networks, including 3G operator networks, corporate Intranets or the Internet via the 3GPP system. One of the most important of such networks is the IP Multimedia Subsystem (IMS) [8], since it constitutes the core platform for 3G IP-based real-time multimedia services. Figure 2 depicts the two most relevant IMS session control nodes for this mobility discussion:

- The Proxy Call Session Control Function (P-CSCF) is the IMS entry point for subscribers. It behaves as a signaling proxy in charge of handling all requests to/from users and routing them as required. It also performs resource authorization and QoS management in the access network.
- The Serving Call Session Control Function (S-CSCF) is the central node of the IMS session control framework, and therefore is always located in the home network. It takes care of user registration and constitutes the access point to the operator's IMS services.

## 2.2 Roaming

In case of roaming, two different groups of configurations are possible in function of the P-GW location: home routing and local traffic breakout.

Figure 3 depicts the 3GPP SAE architecture for home-routed roaming. As its name indicates, the P-GW remains located in the home core network, and thus all IP traffic is backhauled there prior to its delivery to the appropriate IP network. Accordingly, IMS access takes also place in the home network, not taking advantage of the visited network's IMS capabilities (if any).

As shown in the figure, the 3GPP access scenario is similar to the non-roaming configuration, being the only exception that the S-GW is located in the visited core network in this case.

In case of trusted non-3GPP access, the two options discussed for the non-roaming scenario remain available: DSMIPv6-based global mobility between UE and P-GW and PMIPv6-based local mobility between an access router taking the MAG role and the P-GW. However, a third option becomes available on this roaming configuration: the S-GW located in the visited core network may take both the PMIPv6 LMA role towards the access network router and the GTP or PMIPv6 MAG role towards the P-GW, thus allowing to chain two local mobility stages: PMIPv6 between the access network router and the S-GW plus PMIPv6 or GTP between the S-GW and the P-GW.

Untrusted non-3GPP accesses present a similar situation. In this case, the ePDG is always located in the visited core network, and the two mobility configurations already presented for the non-roaming case remain available: DSMIPv6-based global mobility between UE and P-GW and PMIPv6-based local mobility between ePDG and P-GW (both of them undergoing IPsec tunneling between UE and ePDG). Nevertheless, a new mobility configuration is also available in this scenario. Taking advantage of the LMA + MAG features provided in the visited core network by the S-GW, it becomes possible to chain two local mobility stages: PMIPv6 between ePDG and S-GW plus PMIPv6 or GTP between S-GW and P-GW.

Figure 4 depicts the 3GPP SAE architecture for roaming with local breakout. In this scenario, the P-GW is located in the visited core network, allowing traffic to be routed directly towards its destination. Consequently, IMS access takes place in the visited network, thus enabling to profit from the local operator's IMS capabilities.

As shown in the figure, mobility configurations in this case are similar to those presented for the non-roaming scenario, being the only difference the location of all mobility-related functions (i.e., P-GW, S-GW and ePDG) in the visited core network, and the local access to all IP networks, including the IMS, from the

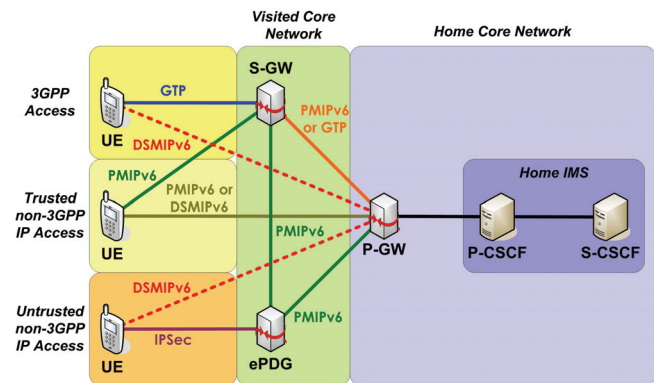
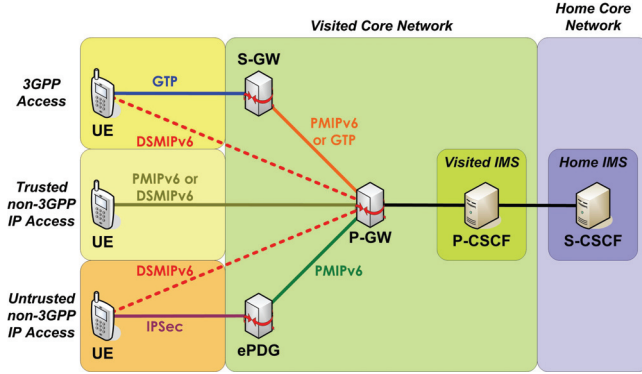


Figure 3. Home-routed roaming SAE architecture.



**Figure 4. SAE architecture for roaming with local breakout.**

visited core network as well.

## 2.3 Inter-domain Mobility

In Sections 2.1 and 2.2 we have discussed the mobility functions that enable intra-domain mobility across the different access networks available in a 3G realm, no matter whether the user is connected to his native network or to a foreign operator holding a roaming agreement with his home provider. Inter-domain mobility goes one step further, and refers to the ability to switch to an access network belonging to a separate 3G domain. Such process may involve re-connecting at the new location and recovering both network access and the service environment (i.e., nomadism), or may be achieved through a handover mechanism that enables to maintain connectivity and, eventually, preserve the ongoing multimedia sessions (i.e., seamless mobility).

Therefore, inter-domain mobility comprises the transition from a non-roaming or roaming scenario to a new roaming configuration. When migrating to a home-routed roaming configuration, no new P-GW is assigned, and therefore mobility may be achieved through the available local or global mobility solutions. When migrating to a roaming configuration with local breakout, a new P-GW is assigned, and thus no network-layer mobility is possible. In this case, mobility must be attained through application-layer procedures, like those available through IMS session control [9]. Consequently, seamless mobility is more easily accomplished when migrating to home-routed scenarios, whereas local-breakout configurations are prone to nomadism but for a limited set of soft handover configurations based on temporary dual-homing.

## 3. TESTBED REQUIREMENTS

As can be deduced from the overview provided in the previous section, a testing platform that enables the validation of 3GPP SAE mobility configurations or service behavior in such context requires a very complex network environment. Considering that, as we will describe in detail in Section 5.1.2, an inter-domain mobility scenario may comprise up to eight different networks, the difficulties for implementing this kind of testing infrastructure are easily appreciated.

In order to allow reliable service validation and/or mobility infrastructure evaluation while remaining feasible to deploy and operate, a 3GPP SAE mobility testing infrastructure should comply with the following requirements:

**Cost-effectiveness.** To enable affordable and competitive testing, the testbed infrastructure should be created at a fraction cost of the equivalent production environment. Cost reduction is usually

achieved by targeting the two main testbed expenditure sources: infrastructure and operational costs. Infrastructure costs are reduced by cutting down the required number of hardware and software elements and by reducing the price of these items. The former is usually achieved by concentrating on the same system as many logical functions as possible, and the latter by supplying such systems with general-purpose hardware and open-source software when feasible, thus avoiding the high expenditures associated with specific software or hardware solutions. Operational costs are reduced by keeping the testbed reconfiguration and management requirements to a minimum, thus limiting the necessary interventions and the effort associated to each of them. This last condition is very tightly related to the next requirement category.

**Flexibility.** As outlined in Section 2, the number of 3GPP SAE mobility scenarios resulting from the initial and final access technologies, the location of the Evolved Packet Core mobility functions and the mobility solution and management protocol in place are extremely numerous. Therefore, a valid testing infrastructure must allow the evaluation of any possible resulting combination without requiring substantial changes (ideally, none) in the underlying physical infrastructure. Additionally, in order to facilitate the testing process itself, it should enable to easily modify each particular scenario. For instance, migrating from home-routed roaming to a local breakout configuration to evaluate service behavior in both conditions, or changing the terminal's point of attachment to the network for handover simulation, will be common practices during the tests.

**Connectivity, interworking and federation.** One of the main purposes of this kind of experimentation infrastructure is the validation or evaluation of external solutions, as well as interoperability and compatibility testing. In order to cover these goals, the testing infrastructure must allow connecting external elements on any network location and at any architectural level. In addition, interworking with counterpart testing or production infrastructures should be straightforward, therefore allowing the evaluation of actual multi-site inter-domain scenarios. Finally, interworking should be allowed to progress further, enabling the segregation of the testbed infrastructure into a set of separate but federated sites. This requirement stems from two different necessities. First, the potential capacity-sharing requirements derived from the complexity of the network scenarios to be tested, thus compelling to the usage of several integrated test sites for capacity aggregation. Secondly, to allow creating combined multi-site testing infrastructures based on the integration of solutions provided by different parties, thus enabling the accomplishment of interoperability and integration tests.

## 4. 3GPP SAE EMULATION FRAMEWORK

The combined analysis of the network scenarios outlined in Section 2 and the testbed requirements drafted in Section 3 confirm the difficulty of implementing an affordable and versatile 3GPP SAE testing environment sustained on real network infrastructure. In order to overcome these limitations, in this section we propose a testbed that, based on combining virtualization techniques with several of the available open source IMS and mobility toolkits, allows the creation and deployment of complex multi-domain 3GPP SAE network emulation scenarios, easily customizable to the requirements of the mobility



configuration under study while keeping minimal infrastructure requirements.

Each of the following sub-sections deals with one of the layers composing the proposed framework: Section 4.1 describes the physical infrastructure supporting the testbed. Next, Section 4.2 presents the virtualization framework that constitutes the core of the proposed solution. Finally, Section 4.3 details the open source IMS and mobility toolkits that, deployed on top of the virtualized network infrastructure, provide the required 3GPP SAE functions.

## 4.1 Physical Infrastructure

Thanks to the adoption of virtualization techniques, the 3GPP SAE emulation framework can be entirely hosted in a single system. In our tests, we have employed a high-end PC-based machine whose hardware profile consists of 4 dual core Intel Xeon 2.8GHz processors, 8GB of RAM and a 146.7 GB hard disk. Although any Linux-based system would be adequate, in our test environment we have adopted Red Hat Enterprise Linux ES release 4 running a 2.6.9 kernel with 802.1q VLAN (*Virtual Local Area Network*) support as host operating system. No special software package is required, apart from the virtualization tool and its associated components, which will be described in Section 4.2.

User terminals usually require direct interaction through GUIs and media capture and presentation capabilities, which can be difficult to achieve if they are emulated as virtual machines in the physical host. Thus, UEs can be implemented as external machines (typically, commodity PCs) connected to the host through its physical network interface. Nevertheless, if no interactivity is required (e.g. when using automated traffic generation tools), nothing prevents from integrating the UEs as virtualized hosts within the emulated network infrastructure.

Apart from UEs, additional external devices can be connected to the emulator. This opens the possibility for seamlessly integrating third-party vendor-specific entities (e.g., SIP Application Servers) into the emulated core networks, thus enhancing the capabilities of the emulation platform in a very modular and flexible way.

The physical host has a single physical network interface, configured in *trunk* mode. An arbitrary number of subinterfaces can be created on this interface, each assigned to a specific VLAN within the *trunk*. Note that a VLAN-capable network switch is required in order to multiplex two or more physical devices connected to the host (which is a very common case, e.g., when using two external PCs as UEs).

## 4.2 Virtualized Network Environment

As described in previous sections, proposed testbed solution relies on virtualization techniques for the emulation of complex 3GPP SAE network environments in a single physical host. In this section we provide an overview at the virtualization tool supporting the framework, detailing next its particular usage for the setup of the 3GPP SAE emulation platform under study.

### 4.2.1 Virtual Network User Mode Linux

VNUML (*Virtual Network User Mode Linux* [10]) is a general purpose open source tool designed to help building virtual network scenarios automatically. Basically, VNUML is a front-end to UML (*User Mode Linux* [11]) which is a virtualization technique to run virtual Linux machines over a Linux host as user space processes. Using UML as back-end, VNUML allows the

user to define, start and interact with virtual scenarios made of Linux virtual machines interconnected through virtual networks.

VNUML relieves users from all the complex UML details required by virtual network scenario creation, allowing them to focus on the purpose of the scenario rather than on its creation and management. The tool is made of two main components: the XML (*eXtended Markup Language*) based VNUML language that allows describing the virtual network scenario; and the language interpreter that parses the description and builds and manages the scenario.

Figure 5 shows the general VNUML use case. First, the user writes the scenario specification using the VNUML language by means of a standard XML editor. Later, it invokes the VNUML parser to process the specification and start the virtual network scenario (building mode). Finally, the user interacts with the scenario to achieve his goals. Interaction with virtual machines can be achieved by accessing them through their consoles or by executing programmed command sequences on them with the aid of the VNUML tool (execution mode), e.g., to start and stop services in the scenario. Eventually, the user can dismantle the scenario, releasing the host resources, running VNUML in release mode.

A VNUML specification is made of two main sections (see example in Section 5.1.1): virtual networks and virtual machines. Two other sections exist (global and host) but they are not described here for the sake of brevity. A complete reference of the VNUML language can be found in [10].

The virtual networks interconnecting virtual machines among themselves or with the host network interfaces are defined using the `<net>` tag. Virtual networks are implemented by means of virtual software bridges running on the host machine.

Later, the `<vm>` tag is used to describe each virtual machine. The language allows describing their main characteristics in terms of: the kernel and filesystem to be run (`<kernel>` and `<filesystem>` tags), the network interfaces they have (`<if>` tag) and the addresses associated with them, either IPv4 or IPv6 (`<ipv4>` and `<ipv6>` tags), as well as the associated IP routes (`<route>` tag). Besides, virtual machine specifications can include `<filetree>` and `<exec>` tags to define files to be copied from the host to the virtual machines and commands to be executed on them.

Virtual scenarios created with VNUML can be interconnected with external equipment and networks, opening the possibility to create heterogeneous virtual/real testbeds. This is a key feature in order to allow UE and vendor-specific equipment connections (as described in Section 4.1), along with testbed federation (Section 5.2).

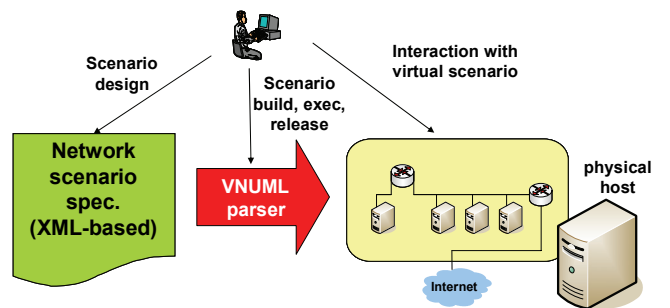


Figure 5. VNUML use case.

#### 4.2.2 Emulator Reference Architecture

In order to recreate the network scenarios described in Section 2 with the virtualization techniques described in the previous section, we propose to run in the physical host the reference architecture shown in Figure 6. It includes three domains, although an arbitrary number could be added inexpensively, as far as the physical host can cope with the computational load of all the virtual machines involved.

Each domain consists of an IMS core and an arbitrary number of access networks (ANs). In Figure 6, domains 1 and 2 have only an access network, whereas domain 3 has two. The IMS core is accessed through the P-GW, acting as edge router also, and it is composed of P-CSCF, S-CSCF and I-CSCF<sup>1</sup>. The different domains are connected through an interconnection point (IX), also known as inter-PLMN (*Public Land Mobile Network*) backbone. The IX also interconnects a segment of auxiliary network elements (such as a DNS server).

Due to the limitations in mobility middleware availability (see Section 4.3.1), the architecture focuses on the trusted non-3GPP IP access case (shown in Figures 2, 3 and 4). Thus, the access network (to which the UEs will be connected using external interfaces) consist on just a DHCPv6 server, which is in charge of IPv6 address provisioning and local P-CSCF allocation [12] when the terminal is attached to the network.

Each AN is connected to its corresponding IMS core through an Access Router (AR). Note that in case of several ANs per domain, a common AR is used for all of them (although an AR per AN could be introduced, this only adds more complexity to the architecture with no functional advantages). It is also worth noting that, although several P-GWs are present on inter-domain mobility scenarios, only one acts as LMA/GMA for each given UE while the others behave as conventional routers (see Section 2).

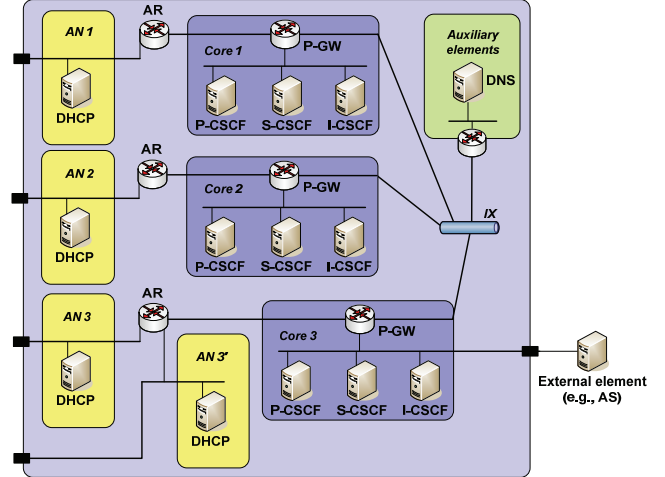
There are two kinds of attachment points for external equipment: access networks (for UEs) and IMS cores (for core entities, such as the SIP Application Server shown as example in Figure 6 connected to domain 3). Each attachment point corresponds to an external VLAN-based interface, multiplexed in the *trunk* of the host's physical network interface (as detailed in Section 4.1).

Regarding addressing, apart from the UEs (which are configured using the DHCPv6 server, as mentioned before), there are several options for network nodes: static address allocation, placing DHCPv6 servers on each IMS core (like the ones in the access networks) or stateless configuration. The current emulator version uses static addressing, since it is the most straightforward solution, but adopting a more flexible approach (i.e., stateless configuration) is planned for future releases.

### 4.3 Application Layer Components

Sections 4.1 and 4.2 have described how to sustain the complex network infrastructures required by 3GPP SAE on single system thanks to the virtualization of Linux-based hosts and routing equipment. However, these virtualization techniques do not suffice to generate the 3GPP SAE environments presented in Section 2. Therefore, the virtual hosts and routers need to be

<sup>1</sup> P-CSCF and S-CSCF have already been described in Section 2.1. The I-CSCF (Interrogating Call Session Control Function) constitutes the entry point to the IMS domain for foreign IMS networks.



**Figure 6. Multi-domain 3GPP SAE emulation platform.**

enhanced with application-layer elements that enable to provide the required 3GPP SAE functions, namely, mobility functions (i.e., S-GW, P-GW and ePDG), IMS session control functions (i.e., IMS UEs and CSCFs), and a series of auxiliary functions not explicitly described in Section 2 but required for the scenarios to work. Each of the following sub-sections presents one of these functional groups in further detail.

#### 4.3.1 Mobility Middleware

As described in Section 2, the 3GPP System Architecture Evolution supports both local and global mobility. Global mobility is based on DSMIPv6, whereas local mobility support is based on PMIPv6 or GTP. In order to incorporate these mobility solutions into the 3GPP SAE emulation framework and implement the associated mobility management protocols, the appropriate mobility middleware needs to be installed in the virtualized Linux hosts taking the routing equipment role.

Although some open-source GTP implementations exist, introducing GTP support in the Evolved Packet Core emulated in this framework has no practical advantages unless the testbed is interconnected to an external radio access network implementing GPRS features. Therefore, the inclusion of this kind of middleware has been postponed for further study, and the S-GW function omitted in this version of the emulation environment.

Regarding PMIPv6, the protocol specification is still in draft status and therefore, although some early prototypes exist, a stable and comprehensive implementation is not available. For this reason, we have decided to postpone also the inclusion of this kind of middleware in the framework, and focus initially on global mobility support only. Nevertheless, it should be noted that the flexibility provided by the framework will allow introducing these features as soon as a reference implementation becomes available.

Regarding global mobility support, DSMIPv6 is also in an early development phase yet, and no stable protocol implementations exist. However, it is possible to emulate 3GPP SAE host-based mobility assuming all-IPv6 core and access networks, and basing global mobility support on plain MIPv6 middleware, such as MIPL [13]. In order to incorporate this mobility solution in the emulated Evolved Packet Core, both UEs and core routers taking the P-GW role should include this middleware.

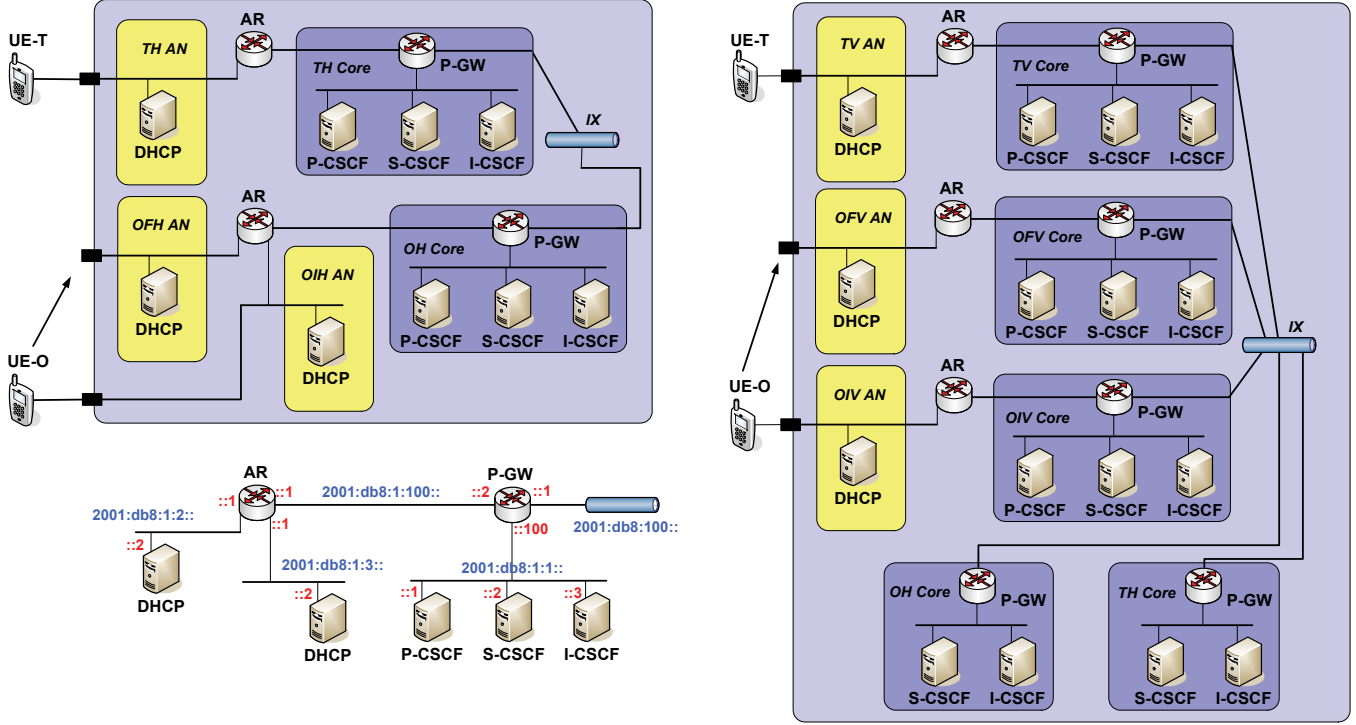


Figure 7. Intra-domain (left), including addressing details, and inter-domain (right) mobility scenarios.

Although global mobility support is available in both trusted and untrusted 3GPP access, in this emulator release we have focused on the trusted scenario, since adding an ePDG element and an IPSec tunnel would involve additional scenario complexity without significant enhancements from the functional point of view.

#### 4.3.2 IMS Signaling Plane Elements

In order to implement the required IMS session control functions, the virtualized Linux hosts created for this purpose must be equipped with the appropriate applications. With this aim, we have installed the Open IMS Core implementation [14] in the IMS core network hosts, configuring the settings file associated to the relevant IMS session control role (i.e., P-CSCF, S-CSCF or I-CSCF) on each of them. In order to emulate IMS User Equipment behavior, two options are possible depending on whether a load generator or a full interactive terminal with multimedia capabilities is required. For automated traffic generation purposes, the SIPp [15] traffic generator may be installed in the virtual or external hosts taking the UE role, configuring the appropriate IMS headers in the test scenario definition files. For interactive terminal emulation, we recommend the usage of IMS Communicator [16] as *IMS softphone* in the UE hosts.

#### 4.3.3 Auxiliary Elements

Last but not least, some auxiliary functions are required for proper scenario operation, like the DHCPv6 server included on each

access network or the DNS server provided in a separate network segment. For DHCPv6 support we have selected the Dibbler [17] open source implementation, whereas DNS capabilities have been provided by adopting the Berkeley Internet Name Domain (BIND) [18] implementation.

## 5. SCENARIO DEPLOYMENT AND EXPLOITATION RECOMMENDATIONS

Based on the generic framework presented in the previous section, this section provides some network emulation scenario examples that replicate the most relevant configurations described in Section 2, along with some recommendations for multi-site testbed deployment and practical exploitation.

### 5.1 Sample Network Emulation Scenarios

#### 5.1.1 Intra-domain Mobility

Figure 7 (left) shows the intra-domain mobility scenario, consisting of a particularization of the general architecture described in Section 4.2.2. It is composed of two home domains, each one corresponding to a different UE, involving 13 virtual machines (the auxiliary elements segment is not shown for the sake of simplicity). The handover procedure is assumed to be initiated by the originating UE during an established multimedia session, moving from an initial access network (OIH AN) to a final access network (OFH AN).

```

<vnuml>

<net name="acc1_1" external="eth0.101"/>
<net name="acc1_2" external="eth0.102"/>
<net name="ppp1"/>
<net name="core1"/>
<net name="ix"/>

<vm name="dhcp1_1">
  <filesystem>/emul-sae/dhcpv6_fs</filesystem>
  <if id="1" net="acc1_1"><ipv6>2001:db8:1:2::2/64</ipv6></if>
  <route gw="2001:db8:1:2::1">2000::3</route>
</vm>
<vm name="dhcp1_2">
  <filesystem>/emul-sae/dhcpv6_fs</filesystem>
  <if id="1" net="acc1_1"><ipv6>2001:db8:1:3::2/64</ipv6></if>
  <route gw="2001:db8:1:2::1">2000::3</route>
</vm>
<vm name="ar1">
  <filesystem>/emul-sae/n3vlr_fs</filesystem>
  <if id="1" net="acc1_1"><ipv6>2001:db8:1:2::1/64</ipv6></if>
  <if id="2" net="acc1_2"><ipv6>2001:db8:1:3::1/64</ipv6></if>
  <if id="3" net="ppp1"><ipv6>2001:db8:1:100::1/64</ipv6></if>
  <route gw="2001:db8:1:100::2">2000::3</route>
  <forwarding />
</vm>
<vm name="p_cscf1">
  <filesystem>/emul-sae/ims-node_fs</filesystem>
  <if id="1" net="core1"><ipv6>2001:db8:1:1::1/64</ipv6></if>
  <route gw="2001:db8:1:1::1">2001:db8:1:2::/64</route>
  <route gw="2001:db8:1:1::100">2000::3</route>
</vm>

<vm name="s_cscf1">
  <filesystem>/emul-sae/ims-node_fs</filesystem>
  <if id="1" net="core1"><ipv6>2001:db8:1:1::2/64</ipv6></if>
  <route gw="2001:db8:1:1::1">2001:db8:1:2::/64</route>
  <route gw="2001:db8:1:1::100">2000::3</route>
</vm>
<vm name="i_cscf1">
  <filesystem>/emul-sae/ims-node_fs</filesystem>
  <if id="1" net="core1"><ipv6>2001:db8:1:1::3/64</ipv6></if>
  <route gw="2001:db8:1:1::1">2001:db8:1:2::/64</route>
  <route gw="2001:db8:1:1::100">2000::3</route>
</vm>
<vm name="p_gw1">
  <filesystem>/emul-sae/n3vlr_fs</filesystem>
  <if id="1" net="core1"><ipv6>2001:db8:1:1::100/64</ipv6></if>
  <if id="2" net="ix"><ipv6>2001:db8:100::1/64</ipv6></if>
  <if id="3" net="ppp1"><ipv6>2001:db8:1:100::2/64</ipv6></if>
  <route gw="2001:db8:1:100::1">2001:db8:1:2::/64</route>
  <route gw="2001:db8:1:100::1">2001:db8:1:3::/64</route>
  <route gw="2001:db8:100::2">2001:db8:2::/48</route>
  <route gw="2001:db8:100::3">2001:db8:3::/48</route>
  <route gw="2001:db8:100::4">2001:db8:4::/48</route>
  <route gw="2001:db8:100::5">2001:db8:5::/48</route>
  <route gw="2001:db8:100::200">2001:db8:200::/48</route>
  <forwarding />
</vm>

[...]
```

**Figure 8. VNUML specification (simplified fragment for one domain).**

An excerpt from the VNUML XML specification<sup>2</sup> used to build this scenario is shown in Figure 8, presenting the description of the UE-O domain (i.e., OH domain). Five different networks (<net>) are defined: two access networks (*acc1\_1* and *acc1\_2*, externally connected to VLAN ID 101 and 102 respectively), a core network (*core1*), a network for the AR to P-GW link (*ppp1*) and a network to connect the IX with the counterpart domain (*ix*).

Regarding virtual machines (<vm>), each one uses the master filesystem (<filesystem>) corresponding to its role, containing the required middleware described in Section 4.3.3. There are three different master filesystems available: one for DHCPv6 servers (*dhcp\_v6*), other for IMS nodes (*ims-node\_fs*) and a very lightweight one for routers (*n3vlr\_fs*). As shown by the 'net' attributes (that reference the aforementioned networks) included in the <if> elements, the topology described in the specification file matches the one depicted in Figure 7 (left) for the OH domain. Note the static configuration of IPv6 addresses<sup>3</sup> on interfaces (<ipv6>) and routes (<route>), which would not be necessary if stateless IPv6 configuration and dynamic routing were used (this improvement is currently in progress).

Regarding UE-O's handover, it can be easily emulated changing the VLAN configuration in the UE's physical network interface. Assuming UE-O starts with an interface to OIH AN (i.e., VLAN ID 101) the handover to OFH AN can be emulated by creating a

new interface in the UE with VLAN ID 102 and tearing down the VLAN ID 101 interface. The creation and teardown order and the interface coexistence interval (if any) can be tuned to emulate different handover procedures.

### 5.1.2 Inter-domain Mobility and Roaming

In the most complex scenario possible, where two roaming users belonging to different operators are maintaining an active multimedia session when one of them migrates to a new visited network, eight different networks are involved in the mobility process. Assuming a handover procedure initiated by the originating user, the resulting network list would read as follows:

- Originating Initial Visited Access Network (OIV AN)
- Originating Initial Visited Core Network, including IMS (OIV IMS)
- Originating Final Visited Access Network (OFV AN)
- Originating Final Visited Core Network, including IMS (OFV IMS)
- Originating Home Core Network, including IMS (OH IMS)
- Terminating Home Core Network, including IMS (TH IMS)
- Terminating Visited Core Network, including IMS (TV IMS)
- Terminating Visited Access Network (TV AN)

The scenario layout is shown in Figure 7 (right), being a five-domain particularization of the general architecture described in Section 4.2.2 (two domains do not require an access network).

The VNUML specification of this scenario is similar to the one described in Section 5.1.1 for the intra-domain mobility case, although involving almost twice as many nodes (24 virtual machines). The handover procedure is emulated in the same way,

<sup>2</sup> The complete specification (along with its supporting material) for the present scenario and the one described in Section 5.1.2 can be freely accessed at <http://www.dit.upm.es/vnuml/wiki/index.php/3gpp-emulator>

<sup>3</sup> According to RFC 3489, the 2001:db8::/32 prefix is used for documentation purposes.



although in this case the final access network belongs to a different domain.

## 5.2 Testbed Federation

As argued in Section 3, testbed federation is a highly desirable feature on this kind of testing environments. It basically consists on splitting the experimentation scenario (which runs in a single physical host in the conventional case) in several network segments, each of them to be deployed in a different site. Thus, the deployment environment is distributed and the interconnection of its different parts through external networks has to be addressed. This section describes how the flexibility and modularity of the VNUML-based environment described in Section 4.2 allow the design of federated architectures in an easy and convenient way.

Figure 9 shows a setup example of the eight-network inter-domain mobility scenario described in Section 5.1.2, considering its deployment on four federated network sites (potentially belonging to different organizations). The OIV and OFV networks (both ANs and Cores) are implemented by the emulator running on site 1. TH and TV Core networks run on site 2, while TV AN is deployed on site 3. This proves that the architecture is flexible enough to allow even deploying parts of the same domain (i.e., access network and core) on different sites. Finally, the OH Core is implemented by a real platform on a fourth site, showing how vendor-specific implementations can be integrated in a seamless way. It is worth noting that the various federated environments could present different functionalities and capabilities, but VNUML-based management allows a homogeneous integration.

The VNUML specifications used to build the different segments on sites 1, 2 and 3 are derived from the mono-host non-federated specification, just splitting the corresponding *<vm>* and *<net>* elements into three different XML files (currently, this procedure has to be carried out manually). Note that some networks which are not defined as external in Figure 8 (i.e., *ppp* and *ix*) need to be

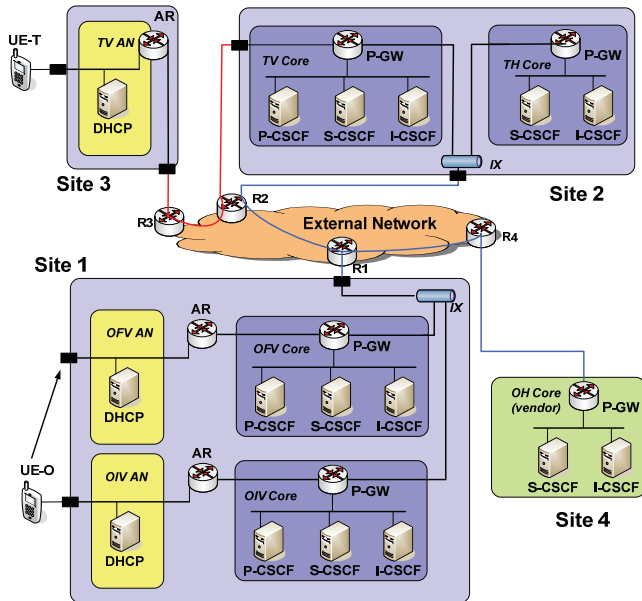


Figure 9. Inter-domain mobility in roaming scenario (federated).

assigned to a VLAN-based external network interface in the federated case.

Regarding interconnection, it is assumed that all sites connect to a common external IP network through edge routers (R1, R2, R3 and R4 in Figure 9). This external network can be private (i.e., corporate) or public (such as the Internet). Tunnels are the most convenient interconnection mechanism, so (for the example included herein) a point-to-point tunnel is connecting TV domain's P-GW and AR (sites 2 and 3) and a separate multi-point tunnel connects site 2's and 3's IX, along with the core in site 4. The tunnel implementation details are out of the scope of this paper, because they entirely depend on the external network's nature (e.g., IPSec, (G)MPLS, etc.).

Although manual procedures are the straightforward mechanism for site interconnection, they involve a lot of configuration effort on site edge routers. Thus, a more convenient solution would be to specify each site's connection attributes and create all the required connections through an automated entity (i.e., a *federation broker*). In particular, each site should specify the public address of its edge router in the interconnecting network; the emulator exported connections (e.g., site 1 exports the IX, while site 2 exports the IX and the P-GW); and cryptographic credentials (e.g., SSL certificate), specially if public networks are being used and tunneled traffic needs to be encrypted. These parameters could even be embedded in XML-based VNUML specification corresponding to each site's emulator. Currently, the design and implementation of such federation broker is being worked out.

## 5.3 Testbed Exploitation Opportunities

There are several ways in which a telecom operator may benefit from a 3GPP SAE testbed like the one described in this paper by including it on its pre-production infrastructure.

First, it will allow testing SAE-related components reproducing the conditions of the target production environment, but only at a fraction cost of the equivalent real infrastructure. Such components include application servers (i.e., SIP Application Servers) from third-party providers willing to integrate their services into the operator's network, vendor IMS entities or middleware (including complete IMS solutions, as shown in Figure 9) or even UEs and mobility stacks. Our testbed architecture is flexible enough to allow the integration of all these elements in a seamless and inexpensive way, therefore decreasing the testing and certification costs and reducing time-to-market for new services. It is worth noting that these are two key advantages from a business perspective, since the former reduces the investment risks, and therefore enables operators to try and deploy a higher number of services, and the latter allows to provide such services earlier than competitors.

Another interesting possibility is related to infrastructure federation, which is currently a challenging topic for large worldwide operators (especially the ones using "follow the sun" business models), willing to improve resource utilization (e.g., an architecture where the IMS is located in Spain, but shared with core networks in U.K., Argentina, etc.). The federation approach described in Section 5.2 considers such a distributed environment, and a distributed testbed itself could be employed as field-trial to develop and test the solutions to be used in the federated production infrastructure.

## 6. CONCLUSION AND FUTURE WORK

The 3GPP System Architecture Evolution defines a series of access and mobility enhancements that will introduce major breakthroughs from the service provisioning perspective. However, no progress comes at zero cost, and such improvements entail an increase in network complexity and possible configuration options. This complexity and diversity makes conventional testing infrastructures very inconvenient for SAE experimentation, since their rigidity and high infrastructure and operational costs are incompatible with validation and testing under business-oriented criteria.

In order to overcome these limitations, we consider that combining virtualization techniques with some of the available open-source mobility and IMS toolkits constitutes an optimal solution. Thanks to virtualization, complex 3GPP SAE network emulation scenarios can be easily created and deployed on minimal physical infrastructure, providing also flexible reconfiguration capabilities and comprehensive connectivity, interworking and federation features. Reciprocally, the available pool of open source 3GPP-related implementations complements the virtualized network environment with the required 3GPP SAE functions in an inexpensive manner.

As a proof-of-concept for the proposed solution, we have implemented a 3GPP SAE experimentation infrastructure based on the virtualization features provided by the VNUML tool in combination with the application-layer functions provided by the software components listed in Section 4.3. Using such infrastructure, we have been able to deploy and test in a single host some of the most relevant 3GPP SAE mobility scenarios. As outlined in section 5.3, telecom operators may benefit intensively from this kind of infrastructure, since the flexible and customizable testing features provided reduce the product and service validation cycle, and allow to easily export the obtained results to the corresponding production environments.

In order to continue this research line and expand the obtained results, we are presently targeting two main issues: federation and virtual host packaging.

Currently, our testbed deployments have focused on the mono-host case, where all emulated elements are located on the same system. However, we are currently working towards the federation environment described in Section 5.2. In fact, a segmentation process to split virtual network scenarios into distributed sites from a central controller (a preliminary version of the federation broker) has already been defined [19] and is currently being developed.

Similarly, virtual hosts in our current testbed implementation are generated manually and reused by means of kernel and filesystem replication. Although virtual machine packaging is still in an early standardization stage (Open Virtual Machine Format, OVF [20]), current production infrastructures tend to base service management flexibility (quick provisioning, high availability, etc.) on virtualization techniques. Therefore, in order to benefit on the testbed itself from the reutilization features provided by packaging, and reduce time-to-market for the tested services, OVF packaging could be used to replicate testbed elements (i.e., CSCF implementations) or ease their migration to the production environment (assuming a common packaging format –e.g., OVF– is used). The introduction of OVF (or any other packaging

standard that could arise in the future) into VNUML is being currently considered.

## 7. ACKNOWLEDGMENTS

The work described in this paper has been supported by the Business Oriented Infrastructure (BOI) research initiative within the Business Support Systems (BSS) unit at Telefónica I+D.

The authors would like to thank Emilio Javier García Escobar and David Fernández Cambronero (DIT UPM); and David Perales Ferrara, Verónica Rubiato Bermejo and Fernando de la Iglesia Medina (TID) for their valuable support during the implementation of the emulator described in this paper.

## 8. REFERENCES

- [1] 3GPP, Technical Specification Group Services and System Aspects, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 8),” TS 23.401 v8.0.0, Dec. 2007.
- [2] 3GPP, Technical Specification Group Services and System Aspects, “Architecture Enhancements for non-3GPP accesses (Release 8),” TS 23.402 v8.0.0, Dec. 2007.
- [3] J. Kempf et al., “Problem Statement for Network-Based Localized Mobility Management (NETLMM),” IETF RFC 4830, Apr. 2007.
- [4] S. Gundavelli et al., “Proxy Mobile IPv6,” IETF Internet-Draft draft-ietf-netlmm-proxymip6-07 (work in progress), Nov. 2007.
- [5] D. Johnson, C. Perkins and J. Arkko, “Mobility Support in IPv6,” IETF RFC 3775, Jun. 2004.
- [6] H. Soliman et al., “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6),” IETF Internet-Draft draft-ietf-mip6-nemo-v4traversal-06 (work in progress), Nov. 2007.
- [7] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” IETF RFC 4301, Dec. 2005.
- [8] A. Cuevas, J. I. Moreno, P. Vidales and H. Einsiedler, “The IMS service platform: a solution for next-generation network operators to be more than bit pipes,” IEEE Communications Magazine, vol. 44, no. 8, pp. 75-81, Aug. 2006.
- [9] H. Schulzrinne and E. Wedlund, “Application-layer mobility using SIP,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 4, no. 3, pp. 47-57, Jul. 2000.
- [10] Virtual Network User Mode Linux (VNUML), <http://www.dit.upm.es/vnuml>.
- [11] J. Dike, “User Mode Linux (UML),” Prentice Hall, 2006.
- [12] H. Schulzrinne and B. Volz, “Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers,” IETF RFC 3319, Jul. 2003.
- [13] MIPL Mobile IPv6 for Linux, <http://www.mobile-ipv6.org>.
- [14] The Open IMS Core Project, <http://www.openimscore.org>.
- [15] SIPp, <http://sipp.sourceforge.net>.
- [16] IMS Communicator, <http://imscommunicator.berlios.de>.
- [17] Digger - a portable DHCPv6, <http://klub.com.pl/dhcpv6/>.
- [18] Berkeley Internet Name Domain (BIND), <http://www.isc.org/products/BIND/>.
- [19] F. Galán and D. Fernández, “Distributed Virtualization Scenarios Using VNUML,” DMTF Systems and Virtualization Management Workshop (SVM’07), Toulouse (France), Oct. 2007.
- [20] Distributed Management Task Force, “Open Virtual Machine Format Specification (OVF) v0.9,” Sept. 2007.