Scenarios Designed for the Verification of Mobile IPv6 Enabling Technologies

Miguel Ponce de Leon, Waterford Institute of Technology, Wenbing Yao, Brunel University, Miguel A. Diaz, Consulintel.

Conveying the innovations of an infrastructural based technology such as Mobile IPv6 is not easy. The identification of an application scenario can be a beneficial way to guide the development of Mobile IPv6 enabling technologies and to assist the real life deployment of Mobile IPv6. Well defined scenarios can also become an important part of the final system integration and test bed deployment.

This paper will first describe additional functional components for Mobile IPv6, particularly the ones that have been successfully integrated, i.e. MIPv6 bootstrapping based on EAP (with and without MIPv6 DHCPv6 extensions and DNS/IKEv2), AAA for MIPv6 bootstrapping, and HA load sharing.

We will then highlight a methodology used in identifying an application scenario chosen to demonstrate the operational mobility service. We will briefly review the state of the art in the domain and seventeen scenarios in the "Mobile and Wireless Systems and Platforms beyond 3G" area. We will then show the process of defining one specific demonstrable scenario, which adequately verifies the technical and business requirements for the deployment of a Mobile IPv6 service.

Keywords: Mobile IPv6, application scenario, operational mobility service, EAP bootstrapping, AAA, DHCPv6, IKEv2, HA load sharing.

Introduction

It is clear over the past few years, that mobile operators have been offering significant data services through their cellular infrastructure, but mobile-phone-based technologies is only one of the technological options. Other options include: satellite links, wireless metropolitan area networks (mainly IEEE 802.16), Wireless LAN (mainly IEEE 802.11) and Wireless Personal Area Networks (e.g. Bluetooth, UWB), all of them available to fulfil the mobility demand of business and consumer users. Thanks to this set of technologies and the rapid falling equipment prices, the resulting overall communication access picture is inherently multi-access and multi-provider (Figure 1) in a market where ISPs (fixed and mobile), in some cases joined in consortiums, co-exist with much smaller and often unmanaged entities (e.g. private or home WLANs).

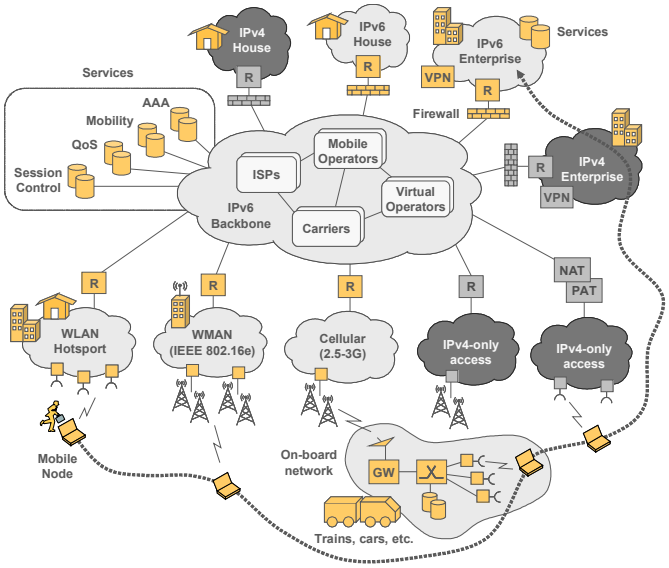

Figure 1 ENABLE "Universe"

The paper will show a solution to improve the reliability of Mobile IPv6 for large scale deployments within a provider, and will go some way towards showing how to validate the results of the developed mechanisms and technologies through prototyping and laboratory testing on a specific application scenario. It is a difficult and risky excise to predict customers' needs in the foreseeing scenario depicted in the Figure 1 as ENABLE "Universe". However, it is clear that more and more users will expect to be "always-connected" and be provided a variety of voice, data and multimedia services disregard their geographical locations. In order to satisfy such needs from the users, a "global" mobility service as well as the next generation of Internet Protocol (IPv6) [1] will have to be deployed for supporting the foreseen growth in the number of mobile users without comprising the end-to-end transparency of the Internet. Solutions based on Mobile IPv6 [2], standardized by the IETF) will be one of the enabling technologies for the provisioning of the "global" mobility service. This paper will present a solution for improving the reliability of Mobile IPv6 in large scale deployment in the domain of one network provider, and a method of validating results through proto-typing and testing in a designed application scenario in laboratory environments.

Enabling Technologies of MIPv6

Amongst many candidate technologies, a Mobile IPv6 (MIPv6, [2,3]) based solution is seemly the only viable option for delivering ubiquitous mobility services in an integrated heterogeneous access networks while serving the both needs of network operators and network users. However, there are many issues not being specified in the current MIPv6 standard but crucial for its large scale real deployment. For example, MIPv6 itself does not provide security protection for MIPv6 signalling messages (unlike MIPv4) between the mobile node and the home agent (HA) but relies on IPSec for this purpose.

In order to aid the deployment of an efficient and operational mobility service in large scale IPv6 network environments, the IST ENABLE project [4] has identified six functional components to develop further into working prototypes, with four of the components integrated seamlessly, namely, EAP-based MIPv6 bootstrapping (with and without MIPv6 DHCPv6 extensions and DNS/IKEv2), AAA for MIPv6 bootstrapping, interworking with IPv4 networks, and HA load sharing. These components will be explained further below. MIPv6 firewall traversal and Fast Mobile IPv6 (FMIPv6) were the other two components being developed. However as they are separate mobility solutions they will not be discussed further in this paper.

EAP-based MIPv6 bootstrapping

Mobile IPv6 assumes that MNs are configured with a set of parameters, namely Home Address, Home Agent Address, and credentials to establish a security association between the MN and the HA. One of the main issues is that, the current MIPv6 specification assumes that the MN has to be provisioned with those parameters beforehand (e.g., static configuration). This leads to a deployment problem. Additionally, in some dynamic environments these parameters might change, for example, due to service provider policies, home agent overload, etc. To address these issues, there is an on-going activity within the IST ENABLE project to define methods to allow a MN to dynamically configure a set of parameters that would allow delivering MIPv6 service to customers. The process is known as MIPv6 bootstrapping [5] and is executed when a MN has not obtained all the information it needs to register with a HA.

This issue has been considered as an important issue and addressed directly by the ENABLE project with EAP-based MIPv6 bootstrapping as one of the solutions. Some EAP methods (e.g. [6, 7]) are able to convey generic information items along with authentication data. This flexibility allows the configuration of bootstrapping parameters during the MN's authentication process when accessing the network. Upon the successful completion of the authentication phase Configuration-TLVs are exchanged to deliver the bootstrapping information. Actually, these TLVs are a mere container: LCP messages and logic [8] are used to configure service specific information. A new network control protocol (MIPv6CP) is defined for the purpose of configuring MIPv6. This approach is similar to [9] which defines a new configuration option for IPCP. Services can be bootstrapped in sequence or, more efficiently, more than one Configuration TLVs are inserted in one packet. If the terminal does not recognize the Configuration TLV, it must send a NAK TLV and consequently the AAA endpoint must immediately close this phase sending an EAP Success message.

AAA for MIPv6

Initially the MIPv6 protocol and its extensions were designed as standalone protocols. Recently researchers have started to consider the possible interactions of MIPv6 with protocols nowadays commonly used in practice for Authentication, Authorization and Accounting (AAA), such as Diameter [10] and RADIUS [11], and mechanisms like stateful dynamic address configuration (DHCPv6) [12]. In order for the providers to perform necessary service authorization and control, an interface between MIPv6 and the AAA infrastructure is required and some issues related to this problem have recently been discussed.

When bootstrapping MIPv6, the ENABLE project partners have considered two different scenarios, the "*Integrated scenario*" in which the Mobility Service Authoriser (MSA) and the Access Service Authoriser (ASA) are the same entity, and the "*Split scenario*" in which the MSA and the ASA are separated entities. In the integrated scenario, the MSA + ASA (MASA) controls the entire bootstrapping procedure, so it can provide mobility configuration parameters piggybacked on the network authentication process. In this scenario there are two different possibilities to provide the Home Agent Address (HoA) to the MN: the MASA could deliver the HoA directly within the EAP tunnel (if the access network of the MN allows it) or via DHCPv6. In the split scenario, the ASA does not know anything about mobility so the MN must discover the HoA using DNS queries.

Once the HoA is known by the MN, the rest of the bootstrapping steps are the same in both scenarios. First, the MN needs to authenticate with the HA, obtain a HoA and establish the needed security associations (SAs) to protect the mobility signalling and authorise the mobility service with the MSA. All these actions are performed through:

1. IKEv2 [13] and a Diameter EAP Application.
2. MIPv6 signalling and a newly defined Mobile IPv6 Authorization Application.

HA load-sharing

In order to provide for load sharing and reliability, a Mobility Service Provider (MSP) must operate several HAs. Each mobile node that requests mobility service is assigned one HA. For deploying MIPv6 operationally, a reliable HA service [14] allowing a flexible load balancing between HAs is required.

In the ENABLE solution, for HA selection, the MSP assesses the current situation of the HAs by evaluating several pre-defined selection parameters, such as, the number of home registrations (Registrations), the currently consumed bandwidth on home link (Bandwidth), announcement of upcoming maintenance (M_Flag), HA location (Region_ID), HA interface address (HA_IP), maximum number of possible home registrations (Max_Reg), HA polling interval (HA_Ptime). Some of these selection parameters are available on the HAs and are collected by a HA Manager periodically and stored in a database denoted as HA-DB. Beside the parameters collected from the HAs, there are parameters set by the HA administrator that have also relevance for load sharing and those are stored in HA-DB as well.

In order to perform the evaluation, the MSP-AAA periodically queries the HA-DB for its content. Upon this query by the MSP-AAA the current load of each HA is calculated and the most appropriate HA is selected. In the integrated scenario (MSA = ASA), after selection, the address of the selected HA is forwarded to the MASA entity. Since in our case MSP = MSA, in the integrated scenario MSP and MASA are the same entity. In the split scenario, HA load sharing is realized via HA relocation. After selection of the most appropriate HA, the MSP-AAA triggers HA relocation with the selected HA as new designated HA. The selection parameters for determining the "best" HA can be divided into selection parameters obtained from the HAs and selection parameters that are preconfigured and stored in the HA-DB. In order to have comparable selection parameters, all parameters were normalised to have values between 0.0 and 1.0.

Integrated software architecture

It is to be noted that this reference architecture is based on the assumption that the MSA and the MSP are co-located.

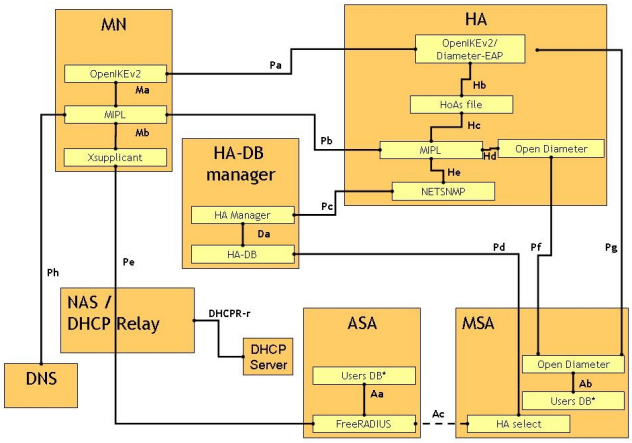

Figure 2 ENABLE Integrated Software architecture

Figure 2 shows the Integrated Software architecture for the EAP-based MIPv6 bootstrapping (with and without MIPv6 DHCPv6 extensions and DNS/IKEv2), AAA for MIPv6 bootstrapping, and HA load sharing.. The functional elements (orange rectangle) that compose this architecture are, Mobile Mode (MN), Home Agent (HA), HA-DB Manager, Network Access Server (NAS) / DHCP Relay, DHCP Server, DNS Server (DNSS), Access Service Authorizer (ASA) server, Mobility Service Authorizer (MSA) server.The yellow rectangles represent the software modules, meanwhile the main interfaces are represented with blue connectors. Both software modules and interfaces are described in the IST ENABLE Deliverable D6.1 [15].

Mobile IPv6 Deployment Scenarios

It is not easy to convey the innovations of infrastructural based technologies such as EAP-based MIPv6 bootstrapping, AAA for MIPv6 bootstrapping, and HA load sharing in regards to the deployment of Mobile IPv6. It is also not trivial to incorporate these into a realistic and demonstrable scenario, which would support the verification of the technical and business requirements of a Mobile IPv6 service environment.

However there are some hints, under the EU IST Strategic Objective (SO) “Mobile and Wireless Systems and Platforms beyond 3G” of the 6th Framework Programme, there are in excess of forty six projects, so this would be a good place to start. And specifically under the B3G System Architecture and Control cluster [16], which hosts a set of projects that have developed new network and signalling concepts for heterogeneous mobile and wireless networks based on common IP infrastructure, there is a clear body of work to review. Across four projects in this cluster, IST Ambient Networks D4.1 [17], IST Daidalos D111 [18], IST ePerSpace D1.1 [19] and IST Simplicity D2101 [20], there are 17 application scenarios described.

In deliverable D4-1 [17] of Ambient Networks, high level mobility concepts, innovative scenarios from a mobility perspective and the definition of requirements for these different mobility perspectives is given. It shows how the mobility concepts have been derived from scenarios but also from other mobility related research initiatives. There are 6 scenarios defined with the most popular scenario being the RockStar Express, in which the scenario takes place somewhere in Europe during the summer of 2015. It follows a rock band, Rusty Zigglers Travelling Hearts Club Band, while they tour Europe using a special rock train by which they travel between gigs.

The approach taken to define the scenarios, was that each scenario has a template layout which covers the following headings: Environment and assumptions, End User perspective, Operator perspective, Service Provider perspective, Network perspective, Application Developers perspective, Business relations, Roles and players, Value chain, Accounting / Compensation models, Trust/authorization relationships, Contractual responsibilities, User data privacy and/or integrity protection.

The Daidalos project as a whole, adopted a methodology of scenario-based design and in its deliverable D111 [18] it describes in detail the continuous evolution of scenarios, the generation of requirements based on several stages of the scenario development process and the flowing design of the architecture. In general the Daidalos scenarios describe the daily life in the near future from an end-user perspective and are structured into different scenes. They are user driven / user focused and demonstrate how a user will handle complex future technology and services easily and seamlessly. From this background the project defined two key scenarios which are the Automotive Mobility scenario and Mobile University scenario. As with Ambient Networks in Daidalos each scenario has a template layout which covers the following headings: General Assumptions, Short description of the scenes

that make up the scenario, Business Models, Realisation of the Scene in each WP, Used Technology & Services, Set of Use Cases for each step in each scene.

IST ENABLE approach

There were some initial hints for an application scenario which included, Location Based Services (LBS), Search and Rescue scene management (emergency applications), and a VoIP Application with HA failover & middlebox traversal. These were all mentioned as possibilities, and it was from these starting points and subsequent discussions within the consortium that the main application scenario on "Search and Rescue scene management" was investigated. The Search and Rescue scene management scenario was chosen as it allowed for enough flexibility to comply with the basic mobility scenario requirements, such as the range of access technologies, intra-subnet/inter-subnet and intra-technology/inter-technology handover and intra-domain/inter-domain mobility, as set forth in the initial IST ENABLE architecture [21].

In most cases, on the rescue scene there is limited connectivity. For this reason an assumption made is that some local volunteers can provide connectivity using their private resources (e.g. WLAN, ADSL, etc.). This connectivity, being opportunistic, is provided with no network planning, which means that mobility events that are normally unlikely might happen in this scenario. For example there might be overlapping (and independent) WLAN/WMAN coverage with no authentication required and multiple protocols supported (IPv4-only, IPv4-only with NATs, IPv6-only, dual-stack). These factors made the Search and Rescue scene management scenario rich with application opportunities, and gave the possibility to incorporate the Location Based Services (LBS) and VoIP Application into the scenario.

Given all the template scenario layouts from the different projects, it was felt that the ENABLE project could best use the format as shown in IST Ambient Networks, with it's headings of environment and assumptions, scenario story, different perspectives and business relations; we took these as the basis for the ENABLE scenarios and came to the general headings of

- Scene Story.
- Scene Challenge.
- Supported services.
- Mobility Issues.
- User experience.

Implementation

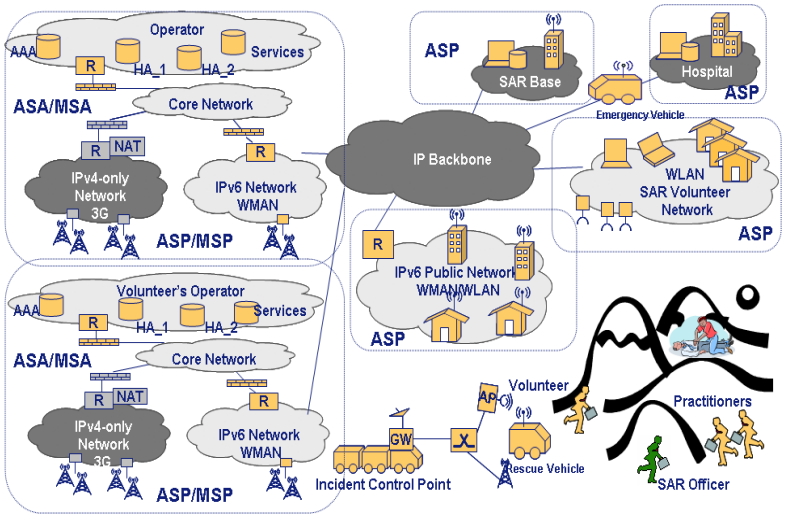

Figure 3 Scene layout for the Search and Rescue (SAR)

The IST ENABLE scenario takes into account the various access technologies ranging from Local Area Networks, to Wireless Metropolitan Area Networks to cellular networks. The end user experience is the focus of the scenario where users can get benefits from services independent from the underlying access infrastructure.. An example of some of these services would be to make available services subscribed by the user with the home provider anywhere and with the highest performance level. Another example would be the seamless movement across homogeneous and heterogeneous access technologies, with little or no disruption to ongoing applications (e.g. VoIP or video conferencing). Other issues such as performance of mobility management procedures, network capability discovery, security and service control are other technological innovative areas being considered and taken into account. This scenario consists of both fixed locations such as the Rural Location of the search / Search and Rescue Base and

mobile assets such as the Incident Control Point, SAR Ambulance, SAR Vehicle, SAR Officer and SAR Volunteer, with a combination of networks that serve these places and assets.

Throughout the SAR scenario there are multiple operators, ASPs (Access Service Providers) and mobility access points providing networking services. These are summarised in the below.

- **Mobile Operator (ASP/MSP) / (MSA/ASA)**. This is the private network operator that provides connectivity and mobility services to subscribed customers. In this scenario the customer is the SAR organisation.
- **Incident Control Point (ASP)**. The ICP is the onsite command post that contains equipment to allow rescuers and practitioners access to the network. The ICP unit will act as a bridge onto the operator's network.
- **SAR Volunteer Network (ASP)**. A closed community network, which is used by the part-time search and rescue personnel to connect with each other, and the SAR Base.
- **Public Network (ASP)**. Open community network offered by members of the public.
- **SAR Base Network (ASP)**. A closed enterprise network, which is used by the full-time professional search and rescue practitioners that are stationed permanently at the SAR Base.

The ASA is the provider that authorises the end users access to the ASP. The end user will initially subscribe to a 'home' ASP which is also the end users ASA. As the MN migrates around the search and rescue location area or urban environment, it may attach to multiple access networks being provided.

Within the search and rescue scenario, the SAR base may be considered as an ASP, where the vehicles bootstrap in the SAR base. Given the starting point as shown in Figure 3, the scenario is further developed through six individual scenes:

- Scene 1 Search and Rescue is initiated.
- Scene 2 Assets (People & vehicles) are deployed.
- Scene 3 Not enough assets on site, volunteers called in.
- Scene 4 Areas of location not covered by Private Network Operator.
- Scene 5 Rescue victim found, special emergency unit vehicle deployed.
- Scene 6 Ambulance transports the victim from rescue scene to hospital.

The main scene that was selected from the overall Search and Rescue scenario and was demonstrated and mapped to the software components, was Scene 3. This is because in scene 3 once all vehicles and people have been deployed around the search location area, further assets may be required onsite if the target area of the search location is expanded to cover a larger terrain, e.g. there are not enough SAR practitioners to cover this larger terrain. In this scenario extra volunteers may be called in to the site to aid in the searching. In addition to people, extra equipment may also be brought to the site. These additional personal called into the search will be one of the main actors played in the rescue scenario as they may move between IPv6, IPv4-only, and dual stacked networks.

Case Study in Detail

- 3a) John is an example of a volunteer, called by the search teams whenever there is a lack of resources at the search site. John has a MN with three network interfaces including WLAN/WMAN, 3G and LAN.
- 3b) John can access any of these networks over both IPv4 and IPv6 networks. When John is leaving the house he receives a video call.
- 3c) John decided that, as the search is quite close to his house, he will walk part of the way. It is presumed that when John leaves his house he has blanket WLAN coverage from his house to the town park over both IPv4 and IPv6 networks. John will loose the WLAN coverage when he approaches the town park which he must go through to reach the search site. However, he will then handover onto a 3G connection. On route to the SAR site John is continuing his video call through his MN which is fed from the SAR site.
- 3d) John reaches the site and enters the ICP. He connects his MN to the Mobile ICP with LAN cable (e.g. to download high resolution maps of the area). John on his way to the ICP area may pre authenticate himself with the mobile ICP unit before he arrives. This requires sending the correct credentials that allow John access information provided by the SAR base. However, if John is already receiving a video stream from the SAR base he may be already authenticated.

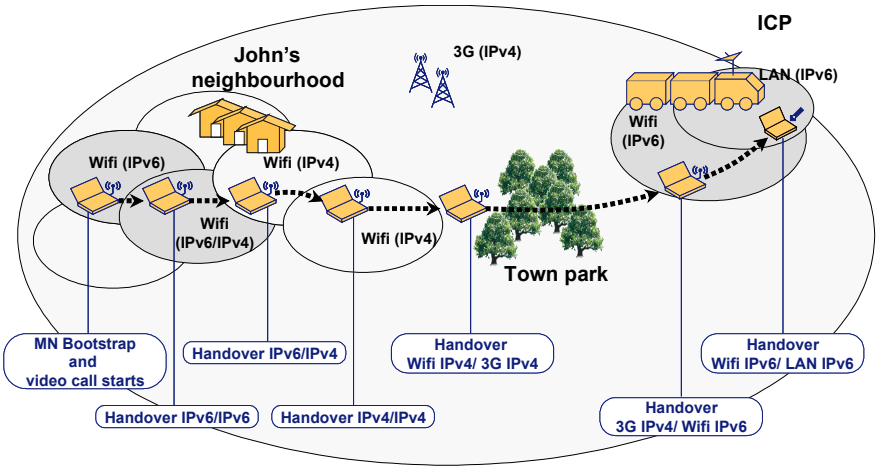

Figure 4 Scene 3 Case Study Detail

Scene Challenges

This scene presents a number of challenges for Mobile IPv6. As more volunteers are called in they may have different home providers (i.e. ASAs/MSAs). These people may also have different devices that will need to operate within the system. As the users come closer to the Mobile ICP they may connect in via WLAN/WMAN and then subsequently via a LAN connection. Direct connection to the ICP will be made via WLAN/WMAN connection. The ICP unit will be considered to be a dumb wireless bridge which will enable clients to connect. As WMAN technologies can be used here John may be able to pick up the ICP unit from greater distance and be able to avail of High Bandwidth Video that may not be possible over 3G.

As more users visit the site their devices will have to bootstrap and may need to authenticate against their respective ASA/MSA. Actors that are connected to WLAN/WMAN connection on the Mobile ICP will have their connections bridged. Therefore they will generate their own IPv6 address (Care-of Address, CoA) directly from the operator that the Mobile ICP unit is connected to. However, these actors must also have access credentials to be able to authenticate themselves successfully with the operator. As John is moving from one network that is IPv6 to another network that maybe IPv4-only an IPv4-IPv6 interworking solution must be provided as John may be receiving a video call from the site.

Mobility Issues

Bootstrapping is one of the main issues that occurs in this scene as there are many new actors that may enter the search location after initial deployment. Authentication mechanisms must support multiple users when they arrive on the site to authenticate against their home provider. As John is receiving a video call when he leaves the house, the session connection survivability is important as the SAR may be updating John on his instructions or current situation at the site. Although John has blanket coverage around his living area there may be some WLAN/WMAN operators that only operate on IPv4; therefore John will have to use IPv4 interworking methods as designed by ENABLE to overcome this problem.

User Experience

Throughout this scene session continuity is important as John will be receiving a video call from the SAR scene. John will also need to seamlessly connect to the Mobile ICP unit through authentication mechanisms, possibly through the use of a username and a password. Although not essential in the case of scene 3, maintaining an active connection through John's journey from house to SAR is important, along with the important issue of IPv6/IPv4 interoperation as John moves from WMAN/WLAN (IPv4 and IPv6) and 3G Networks.

Mapping of Scene 3 to Enabling Technologies of MIPv6

Since scene 3 in the rescue scenario has now been described in detail it is now possible to map the individual actions of the actor (played by John) onto the components that ENABLE will deploy for demonstration purposes. The following table gives the detailed actions that John will take during the journey from his house to the SAR base. It will then map the components of the ENABLE test-bed to these specific actions outlining which components are used in which step.

- **3a - before leaving his house John switches on his MN**: MN, Home Agent, ASP-AAA, ASA-AAA. MSA-AAA, MSP-AAA. NAS, DNS,

- **3b – Video call is initiated to John from the SAR base**: Home IP network contacted via HA by ICP. Video call initiated.
- **3c – John moves from one network to another**: Access points (such as FN AP2 – FN AP3) with IPv6, IPv4 or dual stack subnets, ASP- AAA. MSA/ASA-AAA In this particular scene we can demonstrate all the handover types (IPv6 -> IPv6, IPv6 -> IPv4, IPv4 -> IPv4, IPv4 -> IPv6)
- **3d – John arrives at ICP and plugs in using LAN cable**: LAN Wired Connection / IPv6 Auto-configuration.

It is clear that scenario design is an important step in the process of system integration and test bed deployment. Successful determination and support for the pre-investigation activities have effectively aided the deployment of MIPv6 in the ENABLE project..

Conclusion

The scope of this paper is to report on the design of application scenarios which will eventually highlight and facilitate the efficient and operational mobility in large heterogeneous IP networks. In approaching this task, the paper starts with an overview of four of the components being developed in the IST ENABLE project, namely, EAP-based MIPv6 bootstrapping (with and without MIPv6 DHCPv6 extensions and DNS/IKEv2), AAA for MIPv6 bootstrapping, Interworking with IPv4 networks, and HA load sharing.

The paper reviews scenarios of two EU IST FP6 projects, IST Ambient Networks and IST Daidalos. While there are in excess of seventeen high level scenarios to choose from, it was found that all the best mobility related scenarios were already being implemented by the original project. From this point of view the authors decided to continue evaluating the application scenarios as mentioned in the original description of work for the project, which included Location Based Services (LBS), Search and Rescue scene management (emergency applications), and VoIP Application with HA failover & Middlebox traversal. One positive aspect of reviewing the IST project scenarios is that two keys methodologies have been clearly identified. Firstly, the use of UML was not advisable for the project. This is mainly because a technological bottom up approach is followed in the research activities of ENABLE project, whilst the use of UML scenario based development is more suitable when a top down approach is employed. Secondly, when defining the ‘per scene’ template layout, success lessons are learned from other IST project, which lead us to having sub-section headings ‘Scene Challenge’, ‘Supported Services’, ‘Mobility Issues’, and ‘User Experience’ in each scene that helped greatly in each scene definition.

Having completed a story board of six scenes for a search and rescue scenario, two of the scenes really stood out. Scene 3 is where insufficient assets are on site so that volunteers have to be called in. Scene 6 is where the ambulance picks up the victim and is returning to hospital location. These two scenes provide specific application case studies which we believe are flexible enough to support the verification of the technical and business requirements of a Mobile IPv6 service environment. This paper has also given a more detailed description of scene 3, including the business model, and shows how the scenes are mapped to the physical nodes in the test-bed infrastructure and will be the ones that will be used to demonstrate the IST ENABLE project technological achievements..

References

[1] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 2460, December 1998.

[2] RFC3775, D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, IETF RFC 3775, June 2004.

[3] RFC3776, J. Arkko, V. Devarapalli, F. Dupont, Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, IETF RFC 3776, June 2004,

[4] IST ENABLE project, www.ist-enable.eu .

[5] A Patel, G Giaretta, Problem Statement for bootstrapping Mobile IPv6 (MIPv6), IETF RFC 4640, September 2006.

[6] Palekar, A. et al., "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-10 (work in progress), October 2004.

[7] Arkko, J. and H. Haverinen, "EAP-AKA Authentication", IETF RFC 4187, January 2006.

[8] W. Simpson, “The Point-to-Point Protocol (PPP)”, IETF RFC 1661, July 1994.

[9] J. Solomon, S. Glass, “Mobile-IPv4 Configuration Option for PPP IPCP”, IETF RFC 2290, February 1998.

[10] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, Diameter Base Protocol, IETF RFC 3588, September 2003.

[11] C. Rigney, S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865, June 2000.

[12] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), IETF RFC 3315, July 2003.

[13] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306, December 2005.

[14] J. Faizan, H. El-Rewini, and M. Khalil, "Towards Reliable Mobile IPv6" Southern Methodist University, Technical Report (04-CSE-02), November 2004.

[15] IST ENABLE, D6.1 Report on case studies and initial prototypes, December 2006.

[16] B3G System Architecture and Control cluster, http://cordis.europa.eu/ist/ct/proclu/p/mob-wireless.htm.

[17] IST Ambient Networks, D4.1, V1.0, Ambient Network Mobility Scenarios & Requirements, July 2004.

[18] IST Daidalos, D111 Consolidated Scenario Description, February 2005.

[19] IST ePerSpace, D1.1 Service Scenarios and Specifications, March 2004.

[20] IST Simplicity, D2101 Use cases, requirements and business models, July 2004.

[21] IST ENABLE, D1.1 Requirements, scenarios and initial architecture, June 2006.