Enabling efficient and operational mobility in large heterogeneous IP networks

IPv6 Cluster

Information Society Technologies

Enabling efficient and operational mobility in large heterogeneous IP networks

Enabling efficient and operational mobility in large heterogeneous IP networks

ISBN 978-84-691-0647-1

L. D. M-5808-2008

This book was made possible thanks to the cooperation and contribution of ENABLE project participants.

If you have any questions or comments or you would like to receive another copy of this book, please, visit **http://www.ist-enable.eu**

On-line PDF version also available:
(http://www.ipv6tf.org/pdf/enablebook.pdf)

Enabling efficient and operational mobility in large heterogeneous IP networks

INTRODUCTION 13

1 WHAT IS THE ENABLE PROJECT 15

2 SELECTED PAPERS RELATED TO ENABLE WORK 39

3 ABSTRACTS OF STANDARDIZATION WORK DONE IN THE ENABLE PROJECT 261

Enable

Enabling efficient and operational mobility in large heterogeneous IP networks

Enabling efficient and operational mobility in large heterogeneous IP networks

introduction

The rapid penetration of smart, portable devices creates an increasing demand for the global availability of mobility services. Consequently, there is a need to provide desirable services which surpass todays existing service capabilities and performance.

It is getting widely accepted that a key technology to achieve these objectives will be the next generation Internet protocol (IPv6), which will support the foreseen growth in the number of mobile users without breaking the end-to-end transparency of the Internet.

The goal of ENABLE has been thus, to research, develop, test, integrate and evaluate mechanisms and technologies for the deployment of efficient and operational mobility as a service in large scale IPv6 network environments, taking into account also the transition scenario from IPv4.

Specifically ENABLE has been focused on the following main areas of work:

- Enhancement of Mobile IPv6 to enable, in the medium term, the offering of transparent terminal mobility in large operational networks including multiple administrative domains, heterogeneous access technologies and a rapidly growing number of users. This activity has addressed outstanding Mobile IPv6 issues such as service authorization, autoconfiguration, interworking with IPv4, coexistence with IPv6 middle-boxes (e.g., firewalls) and protocol reliability.
- Enrichment of the basic mobility service provided by Mobile IPv6 with a set of additional features, enabling the on-demand activation and autoconfiguration of specific "premium" network features (e.g., multi-homing, QoS, fast handovers) based on the operator policies and customer profiles.
- Analysis of goals and design principles for the evolution beyond Mobile IPv6 in the long term. This activity has investigated scalability and performance issues that Mobile IPv6 might raise when the vast majority of Internet nodes become mobile, introducing the requirement for a highly efficient treatment of traffic generated on the move. Moreover, the promise of, but not yet fully understood, mobility management alternatives (e.g., Host Identity Protocol, SHIM6, etc.) have been assessed, with the objective to identify possible strategies for their smooth deployment commencing with an architecture based on Mobile IPv6.

Towards this goal, ENABLE objectives are summarized as:

1. Design an overall Mobile IPv6 service enabling architecture, including dynamic mobile IPv6 bootstrapping as a fundamental building block.
2. Develop the required technologies to enable the deployment of Mobile IPv6 in real-life environments, including IPv6 middle-boxes (e.g., firewalls, VPN gateways) and the legacy IPv4-only access infrastructures.
3. Investigate solutions to improve the reliability of Mobile IPv6 and enable an optimal usage of network resources for the deployment of Mobile IPv6 in a provider network.

4. Enrich the basic mobility service provided by Mobile IPv6 with a set of additional features, enabling the on-demand activation and autoconfiguration of specific "premium" network features (e.g., multi-homing, QoS, fast handovers) based on the operator policies and customer profiles.

5. Assess and compare the mobility management solutions that could represent viable alternatives to Mobile IPv6 in the long term, and identify a transition path for the smooth deployment of such technologies starting from the Mobile IPv6 environment.

6. Validate the results of the developed mechanisms and technologies through prototyping and laboratory testing.

7. Disseminate project results, through standardisation activities (with a focus on IETF and 3GPP), public trials and academic conferences and journals, as well as liaison and cooperation with ongoing national, European and other international projects.

Consequently ENABLE has operated in close co-operation with IETF, IRTF and other relevant standardization fora, in order to ensure that the solutions developed by the project were in line with the architectural principles devised by the Internet community and could potentially move towards standardization.

However, the objective of the ENABLE project has been not only the development of innovative mobility solutions but also the dissemination and awareness of the project work and related activities. Hence, dissemination has been an integral part of the ENABLE objectives interlinked with the rest of the project targets and should not be seen as a separate isolated activity.

The target of the project dissemination has been to promote the work developed within the ENABLE project in order to let both, end-users and organizations, to exploit the benefits of those innovations in the Information Society Technologies (IST) field. Such innovations will change both, the supply and the demand for goods and services, and are key enablers of economic growth. They might bring an expansion of new applications and services for our everyday life and work. Moreover they might contribute to the future development of a majority of engineering and science fields and have direct impact on the models for doing communications, collaboration and entertainment.

In order to adequately perform as a dissemination task, the work developed within the project and related activities, needs to be advertised to as wide a community as possible. This publication has been produced with this objective in mind, being one of the most useful tools to promote the ENABLE results to audiences that may not attend to other technical events or workshops. The booklet is structured in three chapters covering the following aspects:

- Presentation of the project and the technical issues covered over the project lifetime.
- Presentation of the most relevant technical papers written within the project in order to present innovative solutions of mobility issues.
- Presentation of the project contributions on standardization bodies such as the IETF and IRTF.

The complete work of the project is available through number of public deliverables at the project web site: **http://www.ist-enable.eu.**

WHAT IS THE ENABLE PROJECT

What is the Enable Project introduction

Over the past several years global communications networks have undergone huge growth. Additionally, the penetration of portable terminals, such as laptops, PDAs and smart phones, is generating an increasing demand for a "global" mobility service. Users are demanding to stay constantly connected, are looking for a wider variety of voice, data and multimedia services independently of their geographical location, each with performance significantly better than exists today (higher bit-rate, lower delays, etc.).

On the other hand it is becoming more widely accepted that a key technology to achieve these demands will be the mobility services offered over the next generation Internet protocol (IPv6), which, due to its "virtually" unlimited address space, will support the foreseen growth in the number of mobile devices, and users, without breaking the end-to-end transparency of the Internet. Mobility over IPv6 (MIPv6) has been standardized in the IETF but there are still some outstanding issues that make it difficult to deploy in a large scale.

The goal of ENABLE has thus been to research, develop, test, integrate and evaluate mechanisms and technologies for the deployment of efficient and operational mobility as a service in large scale IPv6 network environments, taking into account also the transition scenario from IPv4.

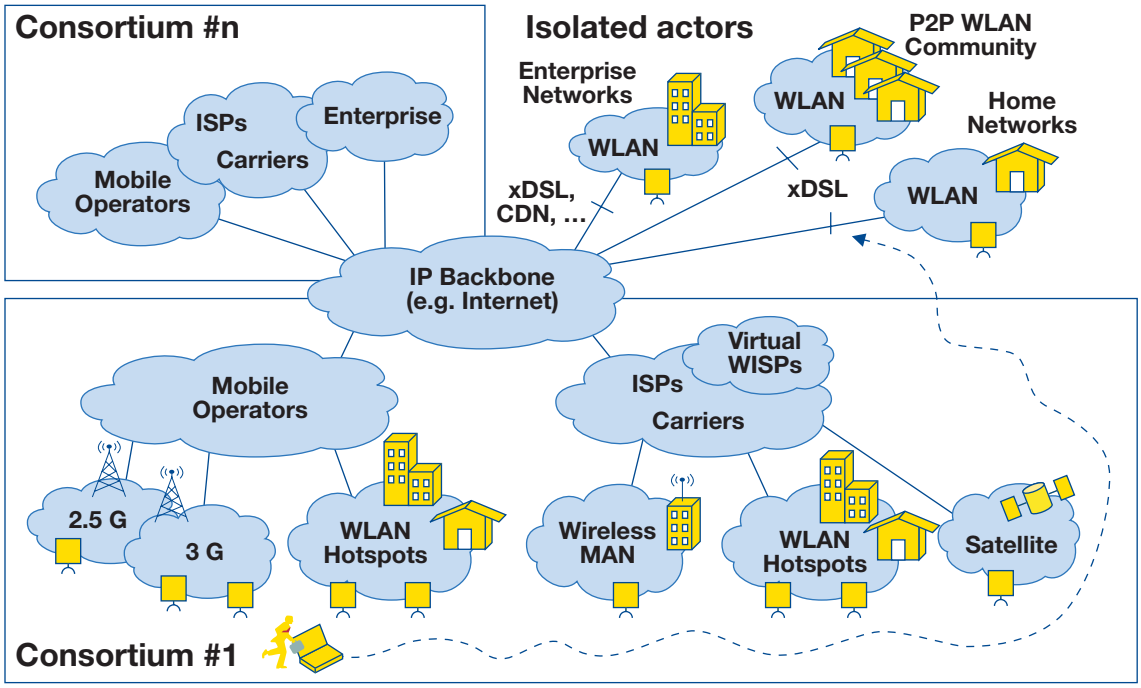
This section presents the work carried out within the project in order to achieve such objectives.

1 What is the Enable Project

1.1. THE NECESSITY FOR MOBILITY

Over the past few years, mobile operators have begun to offer data services through their existing cellular infrastructure. There are numerous technologies available that provide mobility/nomadicity with varying bit rates such as those provided by 3GPP family like GPRS and EDGE, UMTS and HSDPA. Alternative technological options available to fulfill the mobility demand of business and consumer users include satellite links, WMAN Wireless metropolitan area networks (mainly IEEE 802.16), Wireless LAN (mainly IEEE 802.11), and Wireless Personal Area Network (e.g. Bluetooth, UWB).

Figure 1.1: Mobile universe

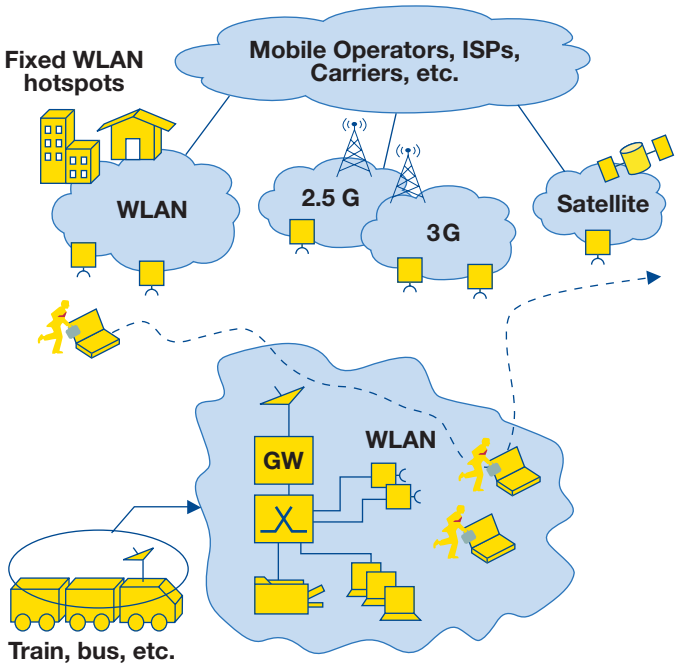


Thanks to falling equipment prices, comparable performances with respect to wired counterparts and the successful initiatives of the Wi-Fi Alliance, WLANs have proven to be an enormous market success and they currently represent the most deployed technical solution for wireless intrernet access. Furthermore, due to the usage of an unlicensed band, the technology is readily available to a wide variety of consumers, from private citizens to commercial entities.

Increasingly, there is the tendency among WLAN providers to aggregate service offerings through bi-/multi-lateral roaming agreements or through consortiums of ISP and enterprises (e.g. iPass). In this manner, an extensive service coverage area may be obtained, overcoming the fragmentation typical of public WLANs.

The resulting overall picture is inherently multi-access and multi-provider; with the user having many technology options with which to access the Internet while mobile, 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 1.2: Mobile network



Another element to be considered is the presence of on-board networks placed in trains, cars, buses or other moving vehicles. These networks (typically 802.11 WLANs) are used to offer connectivity to travellers or to exchange information between on-board devices (e.g. sensors, satellite navigation systems, etc.). An on board network can be regarded as a "mobile hotspot" and can be connected to the Internet through a variety of wireless access technologies, such as radio mobile networks or other (non mobile) hotspots.

These infrastructures combined with mobility technology, together will modify users daily life in the near future by allowing a way a life as the one described for Mr. Bart M. Watson in the Deliverable D111 "Consolidated Scenario Description" of the IST DAIDALOS project:

"Bart is having morning coffee and getting dressed while watching his personalized newscast on screens around the house - his new service follows him into every room that he enters - when a call from his boss Hector is signalled. Bart walks to the living room, as this is where external video calls are received by default and accepts Hector's call, who is urging him to come to the office prior to the briefing. He jumps up and enters his car. The vehicle automatically activates voice call. Also, the TV program he was watching is transferred but on hold during the voice call. He can resume watching it once he has finished the call - though in sound-only driver-mode. His boss informs him, that he needs to pick up customer Rosalyn Royce at the airport."

The realization of this kind of service imposes strict constraints on the network, not only because the diversity of network access technologies and portable devices but also due to the necessity of session continuity when the user is moving across different networks. Mobile IPv6 is the most promising technology being able to support this kind of new services and scenarios.

1.2. DEPLOYMENT AND OPERATIONAL ISSUES

Mobile IPv6 is the mechanism that will support future network scenarios as describe earlier. It is standardized in the [1] by the IETF and it has been proven to work. However, the basic standardized framework of Mobile IPv6 (mainly [1] and [2]) does not define viable mechanisms enabling a straightforward deployment in operational scenarios. There are other aspects not carried out in the [1] that need to be addressed if true IP mobility is going to be deployed as a production network service by a service provider. In order to aid the deployment of an efficient mobility service in large scale IP network environments, the IST ENABLE project has addressed the most outstanding issues that operators may come across in real deployment scenarios.

1.2.1. Mobile IPv6 bootstrapping

In the current Mobile IPv6 specification there is an implicit assumption that the MN is provisioned with enough information that will permit it to register successfully with its home agent. From an operational point of view, however, this requirement is challenging since in a large network which includes thousands of users and several HAs, manual/static provisioning is not feasible. The availability of dynamic solutions ("Mobile IPv6 bootstrapping") is therefore a fundamental step for enabling large scale Mobile IPv6 deployment.

This problem can be summarised as follows:

- Mobile IPv6 does not define viable mechanisms for obtaining HA and HoA dynamically
- Mobile IPv6 dictates the usage of IKEv1 but:
  - IKEv1 is unable to update the security policy database based on a dynamically assigned home address.
  - IKEv1 has no inherent integration with backend AAA which requires the mobile node to share a pre-configured trust relationship with the HA (i.e. a secret) or mandating the usage of client certificates.

While the adoption of IKEv2 [3] overcomes the above mentioned IKEv1 drawbacks, the dynamic provisioning of the HA and HoA requires the definition of ad-hoc solutions.

1.2.2. Home agent load sharing

Before being able to undertake any communication, a roaming MN has to register its current point of attachment to the Internet with a HA provided by an MSP serving the MN. This HA will be detected by and assigned to the MN within the bootstrapping phase.

An operational MIPv6 deployment would not be viable with a single HA. Firstly, this service would have no redundancy, secondly the performance of the MIPv6 service may be sub-optimal. The proper selection of the HA (e.g. using topological information) can significantly influence the performance and scalability of the overall MIPv6 service. For this reason an operational MIPv6 deployment should consider the deployment of several HAs, able to load share among them. Before assigning HA during the bootstrapping phase, first the most appropriate HA has to be selected.

1.2.3. IPv6 middlebox traversal

Middleboxes such as firewalls are an important aspect for a majority of IP networks today and the will become an indispensable means for protecting against unwanted traffic in operational IPv6 networks, especially in enterprise environments. Given the fact that Mobile IPv6 is a recent standard, most firewalls available for IPv6 networks still do not support Mobile IPv6. Unless firewalls are aware of Mobile IPv6 protocol details, they will have to either block communication traffic under Mobile IPv6, or carefully deal with - if possible - by per-user or per-connection, per-Mobile IPv6 mode, manual configuration. This could be a major impediment to the successful deployment of Mobile IPv6.

In summary, this is due to the nature of commonly used firewalls which:

1. do not understand Mobile IPv6 BU, BA, CoTI, HoTI messages and will likely drop them.
2. do not allow IPsec traffic (which is however used for Mobile IPv6 registration messages between the HA and the MN) to traverse the network.
3. do not understand data packets encapsulated in Mobile IPv6 and likely drop them.

The IST ENABLE project has been working to identify the required architectural components and interactions for firewall traversal scenarios.

1.2.4. IPv4 interworking

MIPv6 [1] supports only IPv6 nodes that are away from their IPv6 home networks. However it is foreseen that during the first stage of IPv6 deployments, mobile nodes are likely to roam in IPv4-only visited networks, which is a scenario that is not covered by [1]. That would prevent MIPv6 to work in this scenario and would represent a major impediment to its deployment.

In this context the term IPv4 interworking refers to the following two topics:

- enabling MIPv6 to work even when the access network is not IPv6 capable.
- enabling both IPv4 and IPv6 traffic being forwarded from home network to a dual-stack MN in order to allow communications with either a IPv6-CN or a IPv4-CN without falling back to MIPv4.

The IST ENABLE project has analyzed the scenarios and solutions for this MIPv6 IPv4 interworking issue.

1.2.5. Service authorisation framework

Authorisation is an often neglected problem. When a mobile node wants to use a mobile service two different topics have to be addressed. Firstly, the mobile node has to be authenticated by the mobile service provider, secondly, the request for the specific mobile service has to be authorised. The main focus of most of the existing bootstrapping architectures is to establish security associations between the involved parties. However, it is not clear whether or not a mobile node that is able to authenticate to an HA, should automatically be allowed to use the mobility service. Consider the example were the home network prohibits the use of the mobility service if the mobile node is connected to a visited network of another operator.

IST ENABLE has dealt with this issue and has proposed a framework for the mobility service authorization.

1.3. REQUIREMENTS FOR SOLUTIONS

The IST ENABLE project has identified as set of requirements intended to represent the ideal mobile service scenario. Not all of the requirements have been fully addressed during the project lifetime, due to the large spectrum of technologies that would have been needed to solve all of the involved technical issues. The following summary presents the requirements outlined by the project in order to provide a comprehensive representation of the reference service scenario.

1.3.1. Scalability

The network architecture should be flexible enough to support small-scale home networks and large-scale commercial networks. Scalability needs to be catered for in the design of the system, e.g. network size, number of terminals, number of administrative domains, etc. In particular, the system should be able to accommodate a vast and fast growing number of users and terminals in respect of addressing, routing, mobility control and deployment. Also, the network infrastructure should be easily deployable in an isolated/greenfield scenario.

1.3.2. Optimised usage of network resources

It is necessary that network resources, especially the radio spectrum, are used effectively and efficiently in order to reduce Capital Expenditure (CAPEX) and Operational Expenditure (OPEX), as well as the cost for services offered.

In order to achieve that goal, the signalling load and the overhead on data packets (e.g. tunnelling or other extension headers) should be minimised. Secondly, based on the knowledge of network and user status, such as the load of the access network/cell, congestion, cost, available QoS, terminal capabilities, service requirements and context information for a user, user profile, etc., the system should be able to offer optimised support for different applications and users, satisfying their specific requirements.

1.3.3. Minimisation of End to End transfer delay for data packets

The system should provide a mechanism to minimise end-to-end transmission delay (as well as jitter and packet loss), in order to effectively support real-time interactive applications like audio and video conferencing. Furthermore, the transmission delay should not be adversely affected by mobility management procedures, which are activated when the user moves between different networks.

1.3.4. Optimised support for always-on operation

The system should improve the user experience during the connection set-up phase, minimising the latency before the user is able to access network services. Ideally, even after a period of inactivity, the user should be able to send and receive data packets immediately with no perceivable delay. Furthermore, the system should not preclude always-on support for sensors, or other machine-to-machine equipment, which generate frequent, low bit-rate and short-lived sessions.

Scalability, optimised usage of network resources, minimisation of end-to-end transfer latency and optimised support for always-on connectivity have been identified as important high level requirements of the overall network architecture. Therefore, they have been carefully taken into account during all project activities.

1.3.5. Mobility management

The management of mobility can be done in various ways, each having its specific advantages and disadvantages. In IST ENABLE the requirements for mobility management have played an important role. These requirements come from different areas as outlined below:

- Applications can be categorised in different classes: reliable real-time, unreliable real-time, reliable near-real-time, unreliable near-real-time, unreliable non-real-time. Each one has its own, specific tolerance to packet loss during a handoff or a specific tolerance to the handoff latency. Based on these tolerances a mobility management requirement is required: seamless handover, lossless handover and session continuity.

- Requirements concerning the performance of handovers. Beyond the requirements of the different application categories, additional handover performance requirements are specified for mobility support: minimisation of signalling traffic, efficient intra-domain handovers, inter-domain handovers with session continuity and support for multiple interfaces.

- Requirements concerning the preferred way of routing data traffic. In MIPv6 the simplest mobility routing option is to route all traffic via the home network when the MN is away from home. However, it is also possible to use route optimisation and communicate directly with the corresponded node, without going through the home network. In this way the selection of the route optimisation functionality has to be optional, more precisely, the home provider should be able to inhibit route optimisation for specific user classes. The rational behind this requirement, is to provide the possibility to enable the integration of charging procedures or to enforce authorisation policies on certain traffic flows.

- Requirements on the ability to detect certain network capabilities. In order to perform efficient mobility management, a terminal would benefit from the automatic discovery of new access networks along with their specific characteristics.

Mobility management is a fundamental piece of the architecture. Nonetheless, being this a wide and complex topic, the project has mainly focused on technical solutions needed to fulfil the handover requirements of multiple types of applications (reliable/unreliable, real-time/near real-time/non real-time), minimise mobility signalling, provide seamless intra-domain handover, guarantee at least session continuity in inter-domain handovers, and ensure proper support of multi-homed terminals.

1.3.6. Security and privacy requirements

Security for mobile communications includes network access authentication, protecting user traffic on wireless links, protecting signalling messages. Without suitable protection methods, mobility management could be misused to launch severe attacks: redirecting a user's traffic could lead to denial-of-service (DoS) attacks, or simply to route the traffic of a certain user to an attacking node. Protection mechanisms of mobility management procedures rely on cryptographic material established during the mobile IP bootstrapping procedure.

Security and privacy requirements, being particularly relevant in a mobile environment, have been addressed by the project at various levels:

- The adoption of EAP as the basic authentication framework ensures compatibility with a variety of lower layers (e.g. WiFi, WiMAX). Moreover, the usage of EAP allows a decoupling of the authentication procedure and key management from the access technology, making them truly access-independent.
- In order to minimize the extra delay caused by security procedures, solutions to reduce re-authentication (and re-authorisation) delays have been studied especially in roaming scenarios, where the home AAA server may be quite far away from the location visited by the customer.
- The adoption of solutions for mutual authentication between user and network inherently reduces the chance for unauthorised users to enter and system and interfere with other customers.
- Redundancy and failover mechanisms for Mobile IPv6 HAs are expected to increase robustness against DoS attacks and equipment failure.

1.3.7. Deployment and operational issues

To work well with legacy and emerging systems and to facilitate a smooth deployment, it is necessary to design Mobile IPv6 enabling technologies to be more "environment-friendly". Therefore approaches to traverse different types of middleboxes (firewalls and Virtual Private Networks - VPNs), interworking with IPv4 networks (and terminals) and reliability features (HA load balancing and redundancy), have to be developed.

Requirements of deployment and operation issues, like support for middlebox traversal for Mobile IPv6, IPv4 interworking and network reliability, have been tackled through the design of proper extensions for the Mobile IPv6 protocol.

1.3.8. Service control

Service control refers to the ability of service provider to grant proper service access to their users. In the context of IST ENABLE, service control refers to the ability of a Mobile Service Authoriser (MSA) to ensure that the requiring MN has the correct privileges to use the services deployed by the Mobile Service Provider (MSP).

In order to enable commercial exploitation of the technology, both network access and mobility providers should be given the capability to fully control the service enjoyed by their customers. This includes the capability to assign different service profiles to the customers, the capability to explicitly bootstrap and authorise any requested service option, and the ability to disconnect, at any time a specific end user (e.g. due to credit exhaustion).

1.3.9. Charging aspects

Charging is one of the most important aspects from the service provider's point of view. It is desirable that the accounting system provides the maximum flexibility so that the provider has enough information to apply the proper billing scheme according to their policies or offers (special offerings, discounts, etc.).

Even though no specific work on charging has been carried out during the project lifetime, the adoption of a common AAA infrastructure based on RADIUS, or Diameter, which is the basis of the project reference architecture, inherently enables the exchange of accounting data between entities, both in roaming and non roaming scenarios.

1.4. THE ENABLE ARCHITECTURE FOR OPERATIONAL MOBILITY SUPPORT

In the current Mobile IPv6 specification [1], [2], the MN is provisioned with the information needed to register with its HA in a manual/static way. However, in large networks with millions of users this approach is not feasible, and dynamic solutions for Mobile IPv6 bootstrapping (i.e. assignment of the Home Agent and the Home Address to the Mobile Node and set up of Security Association between MN and HA) are needed in order to enable an effective deployment of IPv6 mobility. This is referred as the Mobile IPv6 bootstrapping problem [4]. This section describes the solutions proposed within the IST ENABLE project for the bootstrapping and control of the Mobile IPv6 service in a realistic operational deployment.

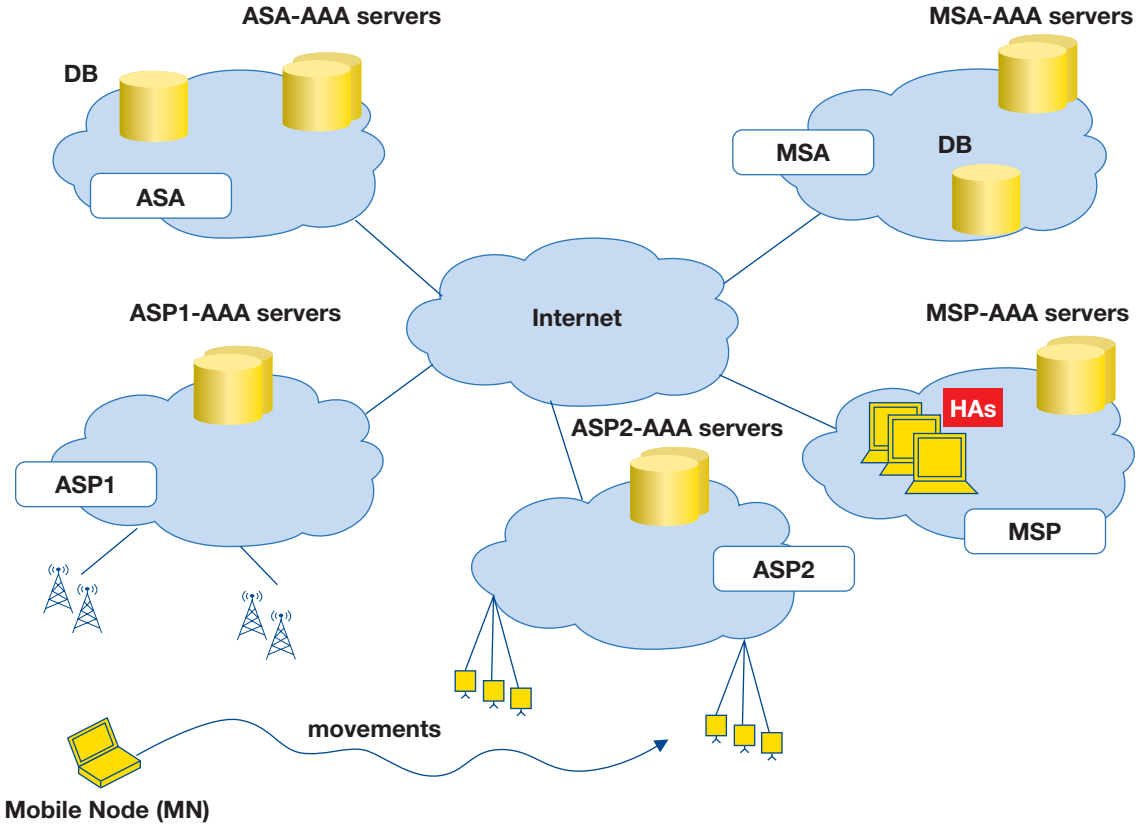
1.4.1. Overview of scenarios

The analysis of the bootstrapping problem begins with the analysis of the entities involved in the delivery of the mobility service and the relationships among them. The most relevant entities to be taken into account in the bootstrapping process are described below:

- **ASA (Access Service Authorizer):** a network operator that authenticates a mobile node and establishes the mobile node's authorization to receive an Internet service. The authentication and authorization procedures are managed by the AAA servers (ASA-AAA) of the domain. More than one AAA server may be present in each ASA for performance and reliability reasons. The ASA stores in a local database (DB) the user's profile with specific access rights and policies.
- **ASP (Access Service Provider):** a network operator that provides direct IP packet forwarding to and from the end host. Before granting access to a MN, the ASP must receive authorization from the user's ASA: for that purpose the ASP contacts the ASA via its AAA server. Once the MN has been granted access, the ASP must apply ASA service policies and may apply its own additional policies. These new policies should not be in conflict with those originally provided by the ASA, which means that the ASP should not permit to a MN what has been explicitly forbidden by the ASA.
- **MSA (Mobility Service Authorizer):** a service provider that authorizes Mobile IPv6 service. The authentication and authorization procedures are managed by the AAA servers (MSA-AAA) of the MSA domain. More than one AAA server is usually present for each MSA for performance and reliability reasons: the same MN can therefore be served by different AAA servers in different authentication/authorization sessions. The MSA stores in a common accessible database (DB) the user profile with specific access rights and policies and any needed state information for the user.

- **MSP (Mobility Service Provider):** a service provider that provides Mobile IPv6 service (i.e. Home Agents). In order to run the service, the mobile node must be authenticated and must obtain an explicit authorization. For this purpose, the MSP gets in touch with the user's MSA via its AAA infrastructure. Once the MN has been granted a mobility service, the MSP must apply MSA service policies and may apply its own additional policies.

Figure 1.3: Overview of the scenario



All these entities must trust each other and communicate in order to authenticate and authorize a user's services (i.e. network access and mobility). For this reason, it is assumed that roaming agreements are in place among the involved entities.

Based on relationships among ASA, ASP, MSA and MSP, two different scenarios can be identified:

- **Split scenario:** the Access Service Authorizer (ASA) and the Mobility Service Authorizer (MSA) are separated entities. A typical case is a mobile node that gets opportunistic connectivity from a hotspot (e.g. conference, hotel) but relies on a third party (e.g. its own home mobile operator) for global mobility. Based on relationships between the Mobility Service Authorizer (MSA) and the Mobility Service Provider (MSP) two basic sub-scenarios are to be considered:
  - MSA and MSP are the same entity.
  - MSP is a third party entity (separated from the MSA).

- **Integrated scenario:** In the integrated scenario MSA and ASA are the same entity, called MASA (Mobility and Access Service Authorizer). A common case of integrated scenario arises when the user has subscribed with a mobile operator that typically provides both network access and mobility service. The AAA server that authorizes network access may or may not be co-located with the AAA server that authorizes mobility service; this means that, in general, the AAA server that is contacted by the NAS (Network Access Server) upon a network access request may be different from the AAA server that handles the AAA request generated by the HA during the IKEv2 exchange (or MIPv6 registration) with the MN. However the assumption behind this scenario is that both servers belong to the same administrative domain (i.e. the MASA domain). Depending on the relationships among Access Service Provider (ASP), Mobility Service Provider (MSP) and MASA, different sub-scenarios can be identified:
  - ASP is the MSP, MASA is a separate entity. In this case the ASP is able to work as a MSP and the MN is allocated a local HA in the ASP network.
  - MASA is the MSP, while the ASP is a separate entity. In this case even if the ASP is available to work as a MSP, the MASA decides to deliver the mobility service by itself and the HA is allocated in the MASA network (i.e. in the "home domain").
  - ASP, MSP and MASA are separate entities (i.e. third party MSP scenario). This can happen when the ASP cannot provide MIPv6 support (e.g. because it does not own any HA) and the MASA, instead of providing the mobility service by itself, decides to redirect the MN to a third party MSP that is known to be closer to the ASP network.
  - MASA is the ASP and MSP. This is the case of a MN that is connected to the network of its own provider which also offers the mobility service. This scenario is not further analyzed in the following section, since it can be seen as a combination of the first two cases.

1.4.2. Overview of the ENABLE bootstrapping architecture

The MIPv6 bootstrapping problem has been described in IETF [4] and solutions have been proposed for both scenarios identified ([5], [6]). These solutions, however, do not consider the fact that several access networks support the EAP protocol as an access control framework (e.g. IEEE 802.11-WLAN, IEEE 802.16-WiMAX). Since these networks will probably become more and more widely available in the near future, it seems reasonable to exploit some EAP features also for the Mobile IPv6 bootstrapping purposes. The EAP protocol, indeed, can use different methods to achieve user authentication. Most of these authentication methods have been designed to offer a protected channel to the MN and the AAA server that can be used to convey bootstrapping information during the authentication phase [7]. Moreover, at the end of a successful EAP exchange a key hierarchy, shared by the MN and the EAP server of the ASA, is available: this keying material can be used to derive keys needed to bootstrap security associations with the HA. This mechanism applies independently of the mechanism used to protect MIPv6 signalling between the MN and the HA (e.g. IKEv2 or Authentication Protocol).

IST ENABLE proposes a bootstrapping architecture that takes into account and leverages the EAP protocol when available. In other cases the solutions developed in IETF are adopted. Therefore IST ENABLE encompasses three different mechanisms, which apply to different scenarios depending on the availability of the EAP protocol in the access network. More precisely:

- **Integrated scenario and EAP capable access networks.** In an integrated scenario (MSA is the same as the ASA) where the authentication for network access is carried out through EAP, the HA is provisioned to the mobile terminal directly in the EAP exchange, piggybacking suitable Type-Length-Values (TLVs) [7]. The HoA, instead, is provisioned through MN HA IKEv2 exchange as described in [5]. However, in some scenarios, most notably when the BU/BA signalling is protected by the Authentication Protocol [8], the IKEv2 exchange is not performed. In this case the HoA is directly communicated to the MN in the BA through the Home Address mobility option. The keying material to bootstrap the Authentication Protocol is derived from the EAP keying framework. A notable exception to this procedure is when the HA is assigned in the access network (MSP is the same as the ASP); since the HA selection is performed by the ASP AAA server, delivery of the HA address from the MASA AAA server to the MN would introduce excessive complexity on the MASA-ASP interface. In that case, if the MSP/ASP supports the necessary DHCPv6 extensions, the MN is informed through the EAP channel to get the HA address directly through DHCPv6 [6].
- **Integrated scenario and non EAP capable access networks.** It may happen that non-EAP-capable access networks support the DHCPv6 extensions for MIPv6 bootstrapping. In this case, before falling back to the split mechanism, the MN tries to bootstrap through DHCPv6 as described in [6].
- In **all other cases** the mobile terminal can bootstrap through the "split mechanism" described in [5], where the HA address is discovered through DNS queries and the Home Address is communicated during the MN-HA IKEv2 exchange. This mechanism is intended as a last resort when the previous mechanisms are not available.

1.4.3. GSABA architecture and components

IST ENABLE proposes the General Service Authorization Architecture (GSABA) to deploy the mobility service.

The main component is the Bootstrapping Agent (BA), which consists of the bootstrapping and service configuration function (Bootstrapping Configuration Agent - BCA) and the service authorisation function (Bootstrapping Authorisation Agent - BAA). Both functions could be co-located on the same entity or distributed. The BCA is responsible for providing necessary bootstrapping information to the Mobile Node (MN). The BAA is responsible for asserting authorisation statements. In addition, the BAA also has to authenticate the MN.

The decisions for the statements are based on the MN's profile, which is available in the authorizing domain. In the roaming case (i.e. the authorizing domain is not the same as the service providing domain), the BAA proxy located in service providing domain proxies authentication and authorization requests to the BAA of the authorizing domain. The statements and the parameters need to be conveyed to the MN. The MN communicates with the BCA to obtain bootstrapping and service authorisations. The MN performs the actual Service Protocol (SP) and thus consumes the service.

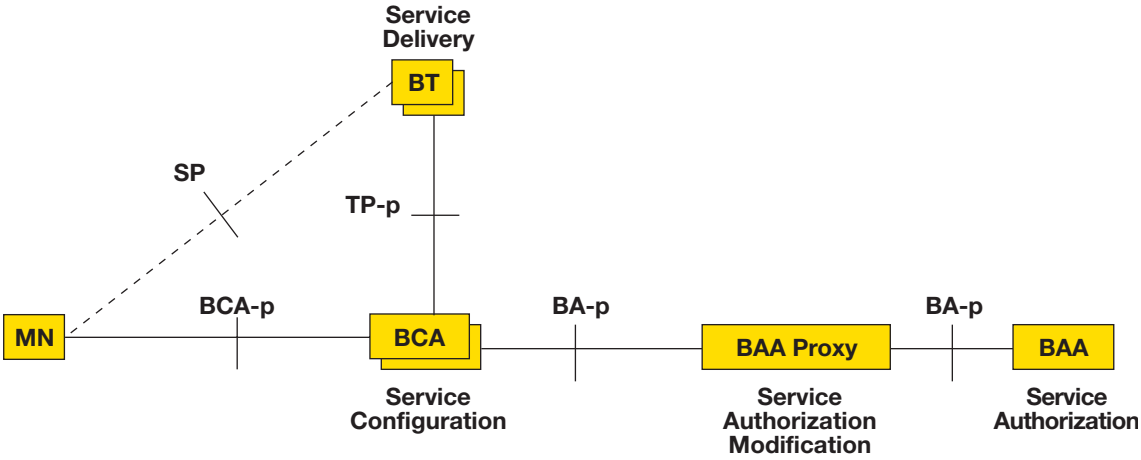
The Bootstrapping Target (BT) is a part of the service providing server. It is responsible for obtaining the service specific information and MN related information from the BCA in order to execute the service protocol and provide the service to the MN (e.g. the BT can be the Home Agent in case the service to be bootstrapped is Mobile IPv6).

The BA-p interface is the interface between the GSABA proxy and the GSABA server. The GSABA architecture does not require changes to this interface (or they will be minimal), with the exception of a new AVP (Attribute Value Pair) or a new simple application. As in the existing AAA infrastructure, the BA-p interface can encompass multiple AAA proxies which do not have to be aware of the GSABA.

The authorization decisions are taken in the GSABA server and the authorization statement will be relayed to the GSABA proxy which the MN is connected to. As introduced above, typically, this is the AAA proxy in the ASP domain. However, if the ASP is not GSABA-enabled, then the MN can also be connected to a GSABA-enabled proxy in its service authorizing domain (or in a third party domain). The authorization statement describes the authorized service (e.g. MIPv6) to the MN. It could include the authorization policies (e.g. traffic filters or QoS parameters) to be enforced on the BT. The authorization statement can be modified along the path the statement traverses. This enables the service providing domain to override the decision made by the home AAA server.

A detailed description of each interface and component as well as the message flows during the bootstrapping are described in the deliverables produced within the IST ENABLE project.

Figure 1.4: General Service Authorization Architecture



1.4.4. HA load sharing architecture

For designing a HA load sharing architecture, it is helpful to first become aware of the separate components and building blocks required. In IST ENABLE we have roughly identified the following architectural components:

- A set of HA selection parameters, which are used as basis for selecting the most appropriate HA.
  - Number of active home registrations: the closer a HA gets to its (configured) maximum number of active home registrations, the more its preference should be lowered; otherwise its performance would degenerate below an acceptable level.

- Current bandwidth availability at HA: the closer a HA gets to its maximal available bandwidth, the more its preference should be lowered. As this parameter may dynamically change, it is difficult to be accurately measured, so, most likely, a calculated average value measured over a most recent time interval will have to be used. However, if a MN has a QoS service level agreement with its provider, e.g. for supporting real-time services, this type of selection parameter may be very useful.
- Upcoming maintenance of HA: if there is a HA maintenance downtime scheduled in the "near" future, the HA should not be selected.
- Location of HA: if for performance reasons a local HA should be assigned to the MN, the HA which is closest to the MN's network point of attachment should be chosen. A local HA assignment requires that the MSP has information about the network point of attachment of the MN, that is, it requires that the MSP and ASP are the same entity.

- Distributed collection of the selection parameters from the HAs and central management components. These parameters will partly be located at the distributed HAs and partly be available at central components responsible for managing the HAs. The collection of all the selection parameters is clearly a management task, and therefore should be performed from a management entity of the respective HAs. IST ENABLE has developed its own method for collecting selection parameters.
- Selection of the most suitable HA based on the collected selection parameters. Once all the selection parameters are available, the most suitable HA to be assigned to a MN can be selected from a restricted set by calculating the load for each of the HAs, and then selecting the one with the lowest load. For calculating the load all the relevant selection parameters will be considered in a weighted manner. Each selection parameter can have a different weighting factor.
- Assignment of the selected HA. Finally the selected HA has to be assigned to the registering MN. The way this HA assignment will be done is specified within the various bootstrapping scenarios.

1.4.5. HA and MSP relocation

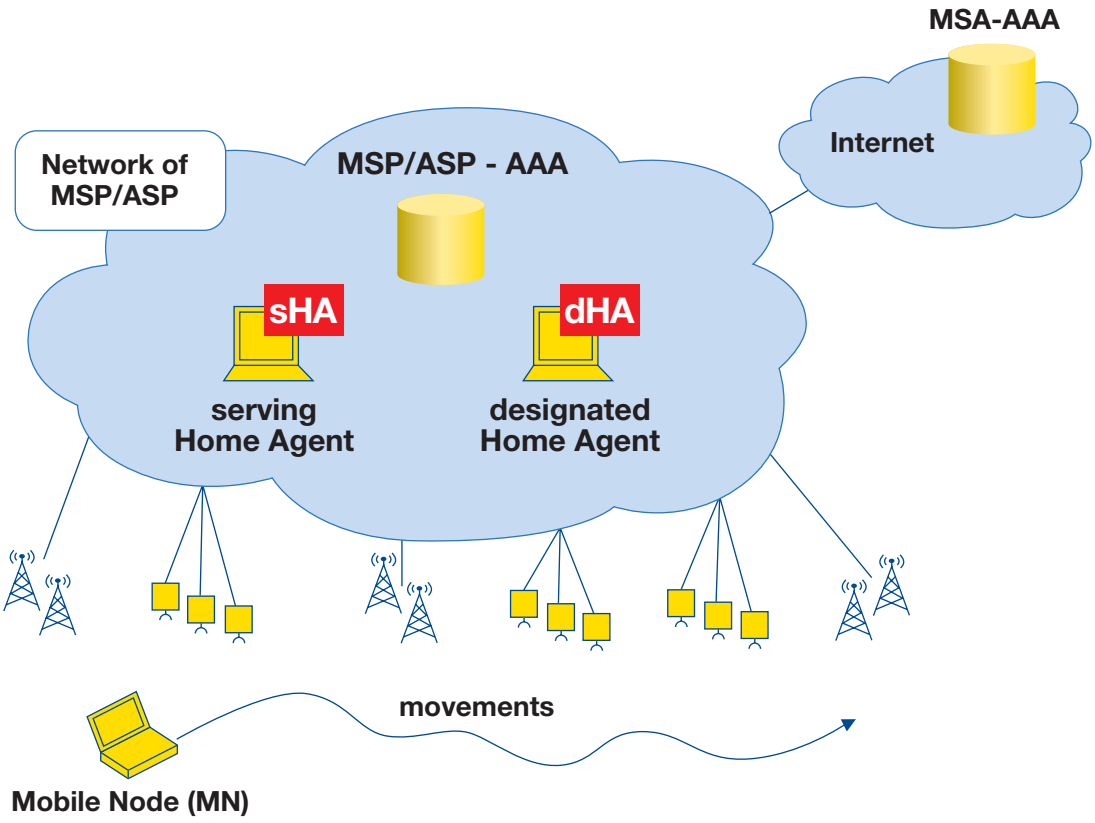
During the bootstrapping procedure one tries to assign the most suitable MSP and HA to a MN, however, in some scenarios like the split scenario this may not be possible. Even if the most suitable MSP and HA were assigned during bootstrapping, this may not be true at a later point in time, as the MN may have moved to a different location or the HA's load may have changed. Consequently mechanisms to dynamically update the MSP and HA assignments have been proposed within the IST ENABLE project.

Basically the HA relocation procedure involves four steps:

- **Relocation decision.** During a (re-)authorization event the MSP AAA server checks if relocation for a specific user applies and selects the designated HA. In general, the policies implemented for HA relocation are operator specific.
- **Authorization and notification.** The decision of the MSP AAA on relocation is notified to the user's sHA along with the information on the dHA (e.g. the IPv6 address of the dHA); in turn the sHA delivers this information to the MN.

- **Switch to the dHA.** The MN bootstraps with the dHA (i.e. gets the new HoA, if dHA and sHA are on different subnets, and establishes a new SA). From the dHA point of view the MN is a fresh bootstrapped node and no special handling is needed.
- **HoA change management.** If the HA relocation happens at a later stage and involves a HoA change, proper management of the two HoAs (i.e. old and new HoA) is needed to handle on-going sessions seamlessly.

Figure 1.5: HA relocation



A detailed description of the procedure and the architecture for HA and MSP relocation is described in the deliverables produced within the IST ENABLE project.

1.4.6. Middlebox traversal

Based on the mobility services that are to be supported, the architecture for the Mobile IPv6 firewall traversal can be summarised as follows. Firstly, the involved components are firewalls (MSP-FW and ASP-FW), MN, HA, CN, and MASA-AAA, ASP-AAA. After bootstrapping and before Mobile IPv6 messages are sent through a firewall, the nodes signal the requests for opening the corresponding firewall pinholes. The decision of opening a pinhole will be authorised by the domain ASP-AAA, and if necessary the MASA-AAA. All functional components building the architecture and the related interfaces are explained in the IST ENABLE deliverables.

IST ENABLE has identified several potential solutions to deal with the Mobile IPv6 firewall traversal problems and has investigated these solutions in detail, namely Universal Plug and Play, STUN/TURN/ICE, Application Layer Gateways, Middlebox Communication, Simple Middlebox Control, NSIS NAT/FW NSLP and Policy Based Networks. Finally, it has identified NSIS NAT/FW NSLP as the most promising IST ENABLE Mobile IPv6 firewall traversal solution.

IST ENABLE describes in detail the middlebox traversal solution based on the NSIS framework and the NAT/FW NSLP protocol. Firstly introduced is the NSIS NAT/FW protocol and a method to enable it to realize Mobile IPv6 firewall traversal. Then secondly a number of approaches to secure the NAT/FW NSLP protocol and a depiction of the messages flows including the GSABA authentication and authorization messages for IST ENABLE middlebox traversal solution based on NSIS is given. In addition, the detailed format for each firewall pinhole which needs to be installed to allow Mobile IPv6 firewall traversal is identifiied. Moreover, we explain how the NSIS Mobile IPv6 firewall traversal prototype, developed by one of the IST ENABLE partner as part of the project, has been implemented.

1.4.7. IPv4 interworking

Assuming that MN, MSP and visited ASP can be either IPv6-only, IPv4-only or Dual-Stack, the following combinations are possible from the mobility point of view[1].

Table 1.1: Interworking scenarios

	IPv6-only MSP			DS MSP		
	IPv6-only ASP	DS ASP	IPv4-only ASP	IPv6-only ASP	DS ASP	IPv4-only ASP
IPv6-only MN	MIPv6	MIPv6	Not feasible	MIPv6	MIPv6	Not feasible
DS MN	MIPv6	MIPv6	Work to be done	Work to be done[2]	Work to be done	Work to be done

The table shows where basic-MIPv6 can be applied; where work needs to be done for a MN to receive both IPv4 and IPv6 traffic from its home network, and where it is not feasible to receive such traffic when the MN is away from its home network. The IST ENABLE project has provided a solution compliant with the project requirements for the feasible scenarios.

In this regard, IST ENABLE has carried out the following tasks for addressing the MIPv6 IPv4 interworking issue:

- **Identification of scenarios for IPv4 interworking.** Taking into account that access networks and service provider networks can be either IPv4-only, IPv6-only or dual-stack, there are many combinations that define a big set of possible scenarios. However not all of them require MIPv6 IPv4 interworking, so the key objective is to present the main scenarios where MIPv6 requires IPv4 interworking.

(1) Both IPv4-only MSPs and MIPv4 in MNs are not considered because it is out the scope of the ENABLE project
(2) Denotes that MN could also be IPv4-reachable by using MIPv6 with extended capabilities and without using explicitly MIPv4

- **Analysis of alternative solutions.** The following alternatives have been analyzed in order to identify their advantages and drawbacks:
  - Tunnel based solutions
    - IETF Softwires protocol [9]
    - IETF MOBIKE protocol [10]
  - IETF Dual Stack extension for MIPv6 (DSMIPv6) [11]
- **Research on DSMIPv6.** A research activity has been made in order to solve the remaining issues of DSMIPv6 solution. These activities address the bootstrapping problem, the movement detection algorithm, and the Route Optimization mode of communication.

1.5. DEMONSTRATING THE ENABLE ARCHITECTURE

Significant effort has been done within the project towards developing software code that is able to demonstrate the IST ENABLE architecture. Specifically, the following functional components have been successfully developed:

- EAP-based MIPv6 bootstrapping
- AAA for MIPv6 bootstrapping
- Interworking with IPv4 networks
- MIPv6 firewall traversal
- HA load sharing
- Fast Mobile IPv6 (FMIPv6)

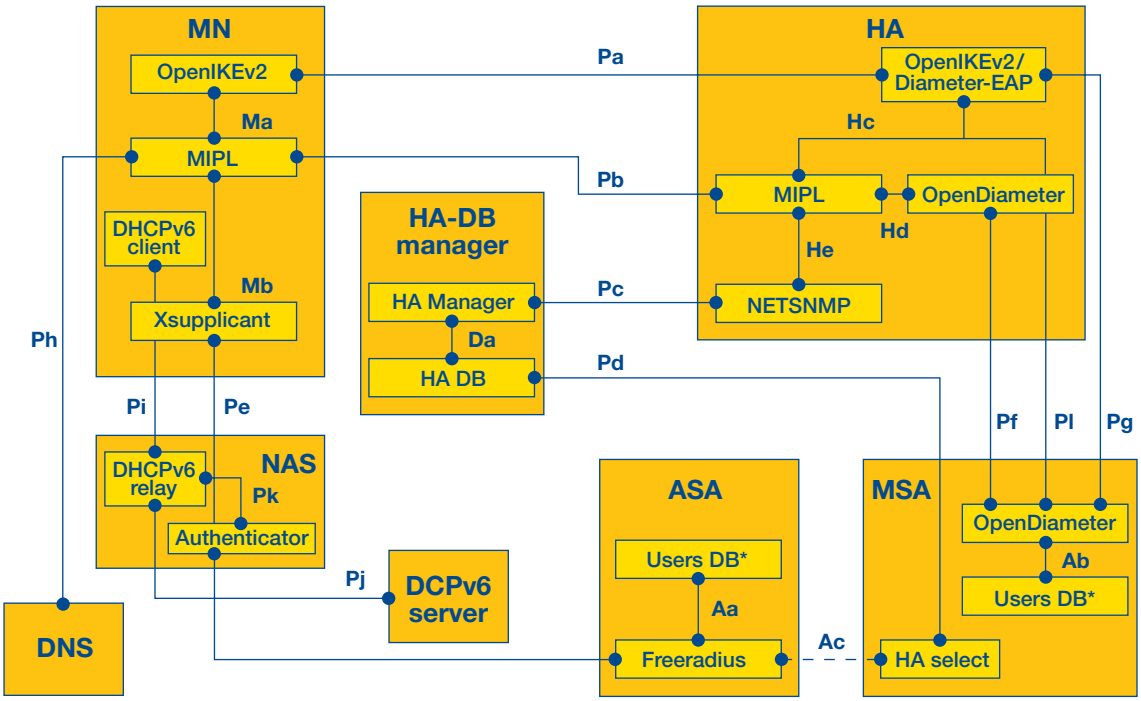
The following integrated software architecture (see Fig. 1.6) was used as a reference for all the developments with the exception of firewall traversal and FMIPv6 which were not integrated.

The yellow rectangles represent the software modules, meanwhile the main interfaces are represented with blue connectors.

The base common platform supported by the IST ENABLE consortium and used for software development was as follows:

- Linux distribution
  - Ubuntu 6.06 (Dapper)
  - Debian 3.1 (Sarge)
- MIPL Mobile IPv6 for Linux: MIPL v2.0.2
- IEEE 802.1X: Xsupplicant 1.2.4.
- AAA Platform
  - FreeRadius 1.1.1
  - Opendiameter 1.0.7-h
  - OpenSAML 1.1

Figure 1.6: Integrated Software architecture



* In an integrated scenario this two User DB could be the same one and the interface Ac is present

- SNMP: netsnmp 5.3.1
- Database: mysql-5.0

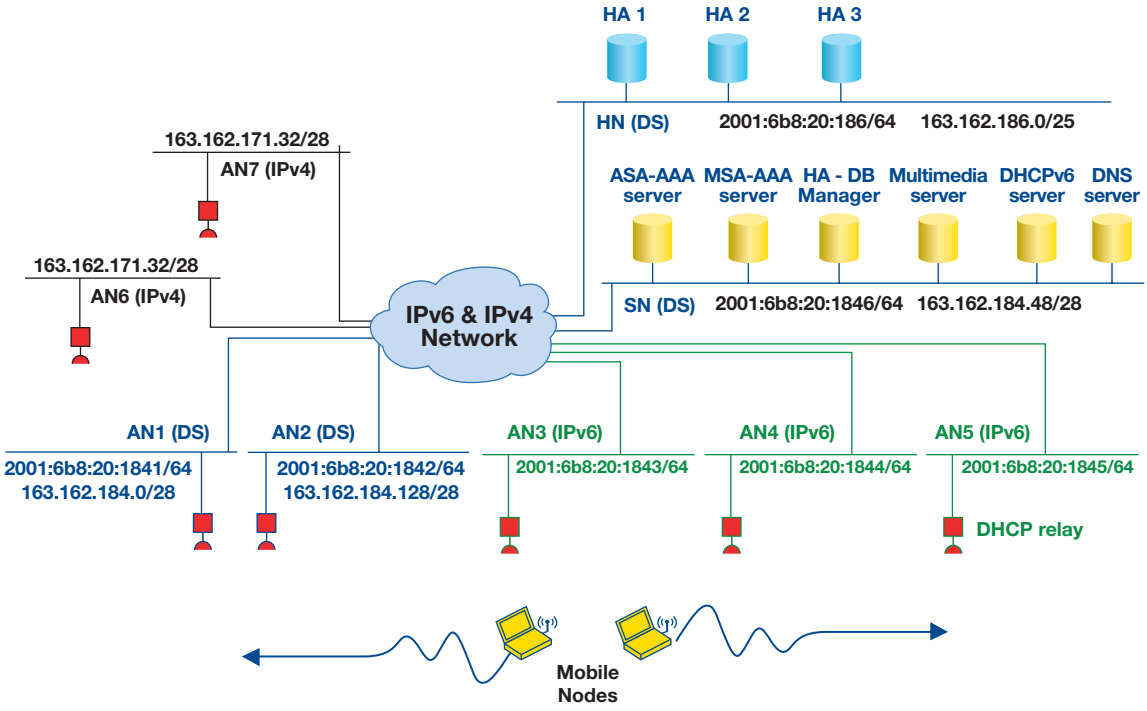
1.5.1. Test-bed for validating the developed software

Because the software has been developed in parallel by different IST ENABLE partners, it has been required to validate the individual components of the software in parallel also. To do that, the following test-bed has been designed which demonstrates the following functionalities:

- EAP-based interface for network access and MIPv6 bootstrapping.
- HA discovery through DNS.
- MIPv6 bootstrapping based on DHCPv6.
- MIPv6 authentication (and HoA provisioning) based on IKEv2.
- Diameter interface between HA and MASA AAA server.
- Realization of the interface between NETSNMP and the MIPL daemon on the HA (i.e. interface He needed for reading the number of active registrations from MIPL).

- ASP AAA server to demonstrate support for roaming scenarios.
- IPv4 extensions for MIPv6 including support for IPv6-IPv4, IPv4-IPv6 and IPv4-IPv4 movement detection and proper forwarding of traffic from and to IPv4-only networks.
- HA load-sharing.
- NSIS for Mobile IPv6 firewall traversal.

Figure 1.7: Test-Bed for validating the developed software



1.6. EMERGING MOBILITY SUPPORT TECHNOLOGIES

IST ENABLE has provided a state of the art analysis of the Mobile IPv6 alternatives under study within different standardization forums, e.g., IETF, and other experimental approaches currently published in the scientific literature, describing how these proposals could affect the future deployment of mobility and security as a service in operational environments. These experimental approaches can be considered as alternative or complementary solutions to MIPv6 approach [1] to provide a mobility service.

The identified technologies have been analyzed against a set of defined evaluation criteria. This ensures that all the relevant features of the mobility management systems are evaluated in a consistent way, and enables a straightforward comparison of the different solutions.

The analyzed technologies are the following:

- **Host Identity Protocol (HIP).** HIP is a network protocol intended to maintain shared IP-layer state between end hosts. HIP provides decoupling between the IP network address and the host identifier, and hence communication continues even on IP address changes.
- **Internet Indirection Infrastructure *(i3)* and related technologies such as FARA.** *i3* proposes an overlay-based indirection infrastructure that offers a rendezvous-based communication abstraction, decoupling the act of sending a packet from the act of receiving it. FARA is a more experimental approach, defining a new organization of network architecture concepts, but it is based on the same indirection principle.
- **Site Multihoming by IPv6 Intermediation (SHIM6).** SHIM6 is a multihoming solution for IPv6, based on the addition of a new network sub-layer. This new layer allows for the separation of the well known IP location-identifier association by managing a group of assigned IP address and providing to the upper layers a single fixed address.
- **Network-based Localized Mobility Management (NetLMM) and Proxy Mobile IPv6 (PMIPv6).** NetLMM and PMIPv6 are two alternative technologies that perform localized mobility management, allowing a MN to move from one access router to another inside the same organization in a transparent way. This kind of localized management allows for the reduction in mobility signalling traffic and the improvement of handover performance. One of the most remarkable features is that they work with unmodified (legacy) MNs.

One thing that became clear after this analysis is that the studied technologies can be classified into two different groups. On the one hand, we have technologies that are disruptive in the sense that they are, in essence, a substitute for Mobile IPv6. This is the case of all the indirection technologies (i.e. HIP, I3 and related technologies). Future deployment of these technologies is a rather difficult task, as the IETF MIPv6 is a standardized solution that will not likely be replaced by a different approach in a long time. While they are undoubtedly interesting technologies that in some cases have the potential for a great improvement over MIPv6, there may be little benefit in continuing work on them within IST ENABLE, as the chances of mid-term or even long-term deployment of these solutions are very low.

On the other hand, we find that other mobility solutions studied are conceived as a complement to Mobile IPv6, basically supporting some optimization aspects. These technologies are less disruptive and have a greater chance to be deployed. They also offer significant improvements over the existing IETF MIPv6 standard, so they are ideal candidates for further research. This applies in particular to NETLMM, PMIPv6 (due to its recent adoption by WiMAX) and SHIM6.

1.7. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, RFC3775, June 2004.

[2] J. Arkko, V. Devarapalli, F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, RFC3776, June 2004.

[3] C. Kaufman, Ed., “Internet Key Exchange (IKEv2) Protocol”, RFC4306, December 2005.

[4] A. Patel et. al., "Problem Statement for Bootstrapping Mobile IPv6", RFC 4640, September 2006..

[5] G. Giaretta, J. Kempf, V. Devarapalli, “Mobile IPv6 bootstrapping in split scenario”, draft-ietf-mip6-bootstrapping-split-03 (work in progress), October 2006.

[6] K. Chowdhury, A. Yegin, “MIP6-bootstrapping via DHCPv6 for the Integrated Scenario”, draft-ietf-mip6-bootstrapping-integrated-dhc-01 (work in progress), June 2006.

[7] G. Giaretta, I. Guardini, E. Demaria, E, J. Bournelle, M. Laurent-Maknavicius, "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-04 (work in progress), November 2006.

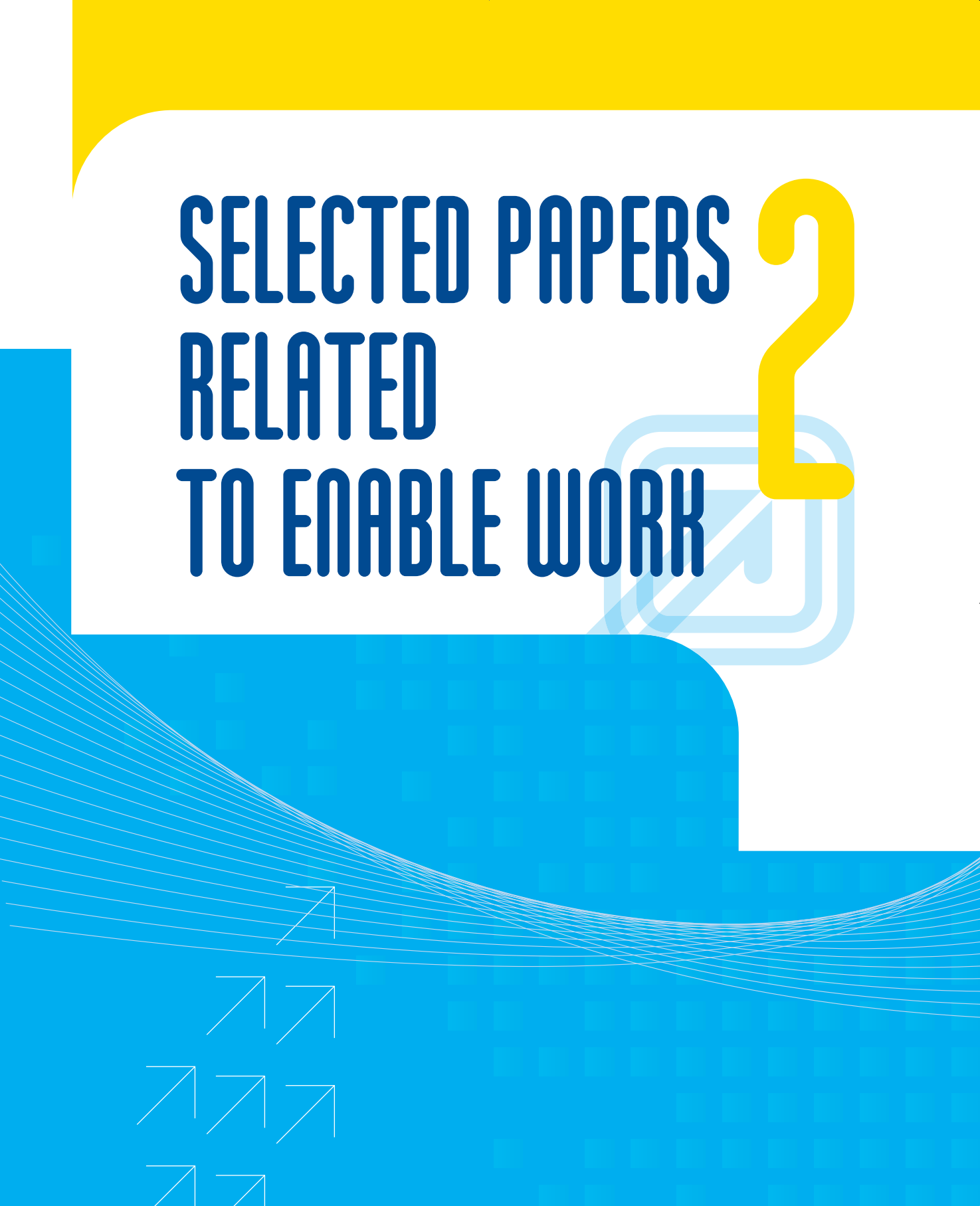
[8] A. Patel,M. Khalil,H. Akhtar, Authentication Protocol for Mobile IPv6, RFC4285, January 2006.

[9] B. Storer, C. Pignataro, M. Dos Santos, B. Stevant, J. Tremblay, “Hub & Spoke Deployment Framework with L2TPv2", draft-ietf-softwire-hs-framework-l2tpv2-07, (work in progress) September 2007.

[10] P. Eronen, Ed., “IKEv2 Mobility and Multihoming Protocol (MOBIKE)”, RFC4555, June 2006.

[11] H. Soliman, G. Tsirtsis, V. Deverapalli, J. Kempf, H. Levkowetz, P. Thubert, R. Wakikawa, “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)”, draft-ietf-mip6-nemo-v4traversal-03 (work in progress), October 2006.

SELECTED PAPERS RELATED TO ENABLE WORK



Selected papers related to enable work

introduction

As consequence of the research carried out in the ENABLE project many technical papers have been written in order to explain the technical innovations developed in the project. This section presents several of the most relevant papers covering different aspects of the outstanding issues related to the deployment of the mobility services in a large scale.

2.1 Mobile IPv6 deployment opportunities in next generation 3GPP networks

Elena Demaria, Ivano Guardini, Michele La Monaca
Telecom Italia

2.1.1. INTRODUCTION

In 3GPP the evolution of radio and core networks is now under study. In particular a new radio access, called E-UTRAN (Evolved-UTRAN) is being specified to support mobile broadband peak data rates exceeding 100 Mbps. It is based on the OFDM radio technology and it will offer a peak throughput per user of 100 Mbps Down Link and 50 Mbps Up Link (with a 20 MHz channel width).

In this context a new core network is also under study in the EPS (Evolved Packet System) specification. The goal of the work item is to have an evolved system to offer a high bandwidth and a set of services completely based on IP. The specification is expected to be completed by 2008.

To satisfy the needs of a mobile user this network will also need to interwork with legacy 3GPP accesses (i.e. GERAN, UTRAN) and non-3GPP accesses (e.g. WiFi, WiMAX).

In this context a mobility management solution is needed to guarantee session continuity when the user roams from an access segment to another.

In this paper we analyze the mobility management problem in 3GPP networks illustrating the adopted solutions and their open issues. Finally we provide an overview on possible future extensions.

2.1.2. SYSTEM ARCHITECTURE

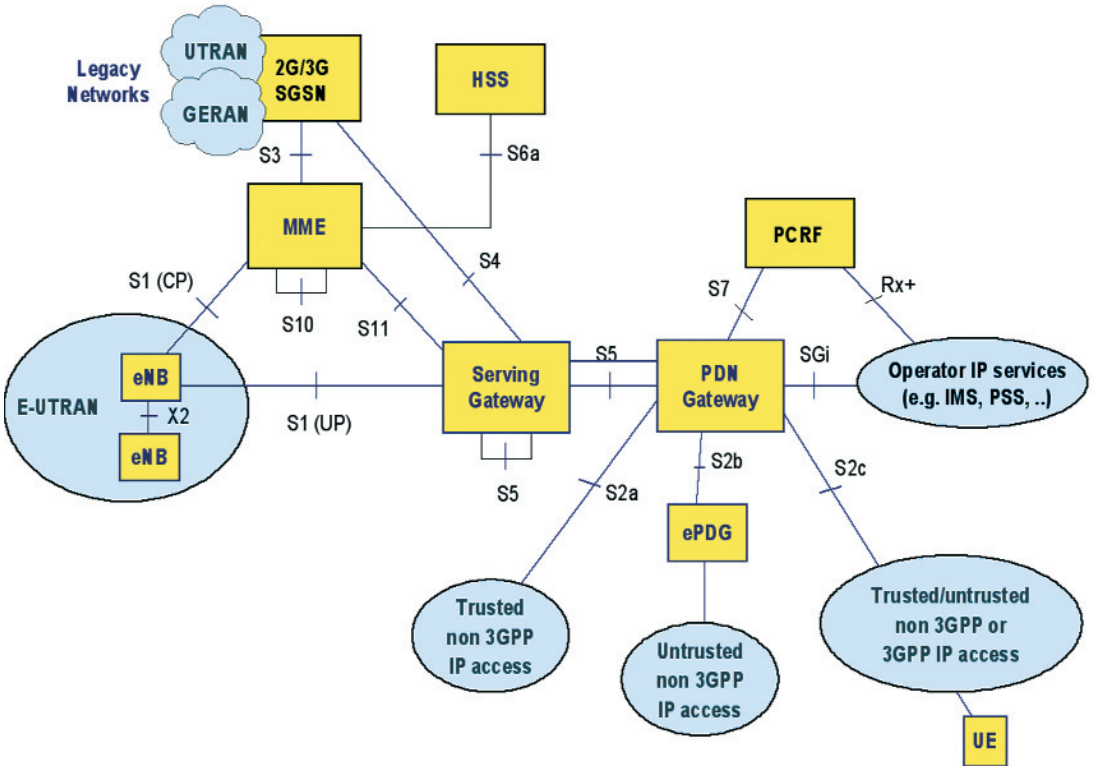
The reference architecture for the non roaming case is depicted in Figure 2.1.1.

The UE (User Equipment) is attached to an eNB (evolved Node B) that takes care of the Radio Resource Management and bearer set up procedures. The eNB also manages the inter-eNB mobility (HO decision and procedure on X2 reference point) as well as user plane ciphering and header compression.

The Control Plane of the UE is managed by the MME (Mobility Management Entity) including Authentication procedures, Idle mode UE Tracking and paging and signaling for mobility between 3GPP networks (S3 reference point).

The User Plane of the UE is managed by two gateways: the Serving GW and the PDN (Packet Data Network) GW.

Figure 2.1.1: Logical architecture: non roaming case



eNB: evolved Node B
MME: Mobility Management Entity
PDN GW: access gateway towards Packet Data Networks
SGI: interface towards Internet/Intranet

The Serving GW is the gateway which terminates the interface towards the E-UTRAN. It is the local Mobility Anchor point for inter-eNB handover and the Mobility Anchor for inter-3GPP mobility (terminating the S4 reference point and relaying the traffic between 2G/3G and PDN SAE GW).

The PDN GW is the gateway which terminates the SGi interface towards the PDN. For each UE there may be several PDN SAE GWs to support multiple PDNs. The PDN GW is responsible for enforcing QoS and/or charging policies on user plane traffic (e.g. deep packet inspection). Finally it is the user plane anchor for mobility between 3GPP and non-3GPP accesses.

The Serving GW and the PDN GW may be implemented in one physical node or separate physical nodes.

For non-3GPP accesses the system distinguishes between "trusted" and "untrusted" accesses: it is up to the operator to decide if a non 3GPP access is trusted or untrusted. The decision is not based just on the access network technology but may also depend on business considerations.

Interworking with an untrusted access is performed via an evolved PDG (ePDG) that is similar to a VPN concentrator. The UE has to establish an IPsec tunnel with the ePDG to access the operator's services.

Interworking with a trusted access is performed using a more lightweight procedure since the UE does not need to establish an IPsec tunnel with the ePDG in advance.

2.1.3. MOBILITY MANAGEMENT IN 3GPP EPS

To manage the mobility for 3GPP users different protocols have been chosen. Mobility within 3GPP accesses (E-UTRAN, UTRAN and GERAN) is managed in a network-based fashion using 3GPP-specific protocols (i.e. GTP). When connected to a 3GPP access the UE can be assumed to be at home in MIP sense.

For mobility between 3GPP and non-3GPP accesses the EPS supports both host-based and network-based mobility management solutions.

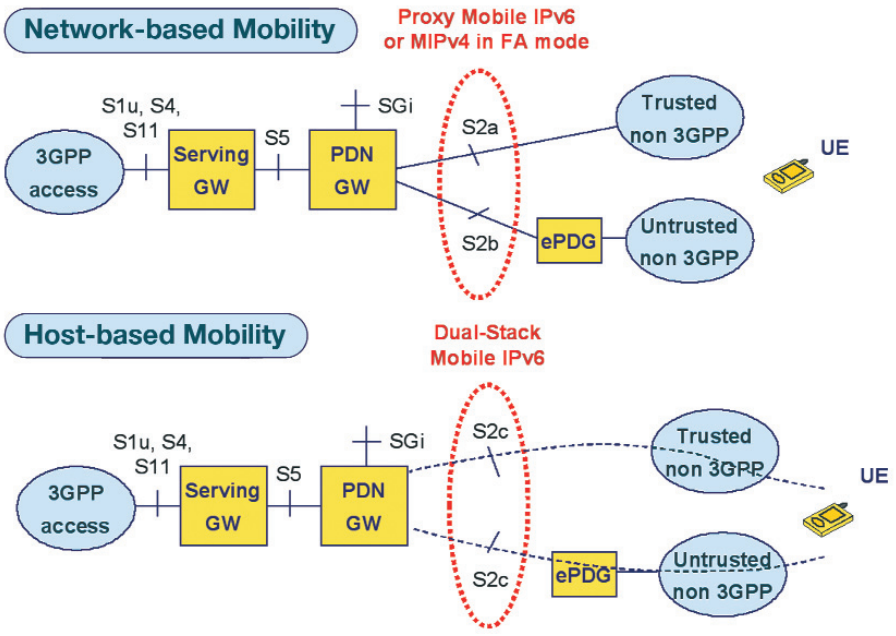
For host based solutions Dual-Stack MIPv6 [1] has been chosen for both trusted and untrusted non-3GPP accesses (S2c reference point). When the UE attaches to a trusted non-3GPP network it must be authenticated and authorized to get IP connectivity (and a local IP address) through the trusted access network. This IP Address is then used during the Security Association establishment with the PDN gateway, that works as a Home Agent (HA) and that assigns a Home Address to the UE. Once registered with the HA, the UE can start using its Home Address at the application level.

In case of untrusted non-3GPP access the UE must establish an IPsec tunnel with the ePDG and then, on top of it, the MIPv6 tunnel with the PDN GW.

For network based solutions Proxy Mobile IPv6 [2] and Mobile IPv4 in Foreign Agent mode [3] have been selected for trusted non-3GPP accesses (S2a reference point) while Proxy Mobile IPv6 with dual-stack extensions is used on untrusted non-3GPP accesses (S2b reference point). In this case the non-3GPP network (or the ePDG in case of untrusted access) receives the PDN GW address during the authentication phase and sets up the PMIP/MIPv4 tunnel.

The set of possible choices is summarized in Figure 2.1.2.

Figure 2.1.2: Interworking scenario: non roaming case



In the roaming scenario the UE attaches to a visited network (VPLMN).

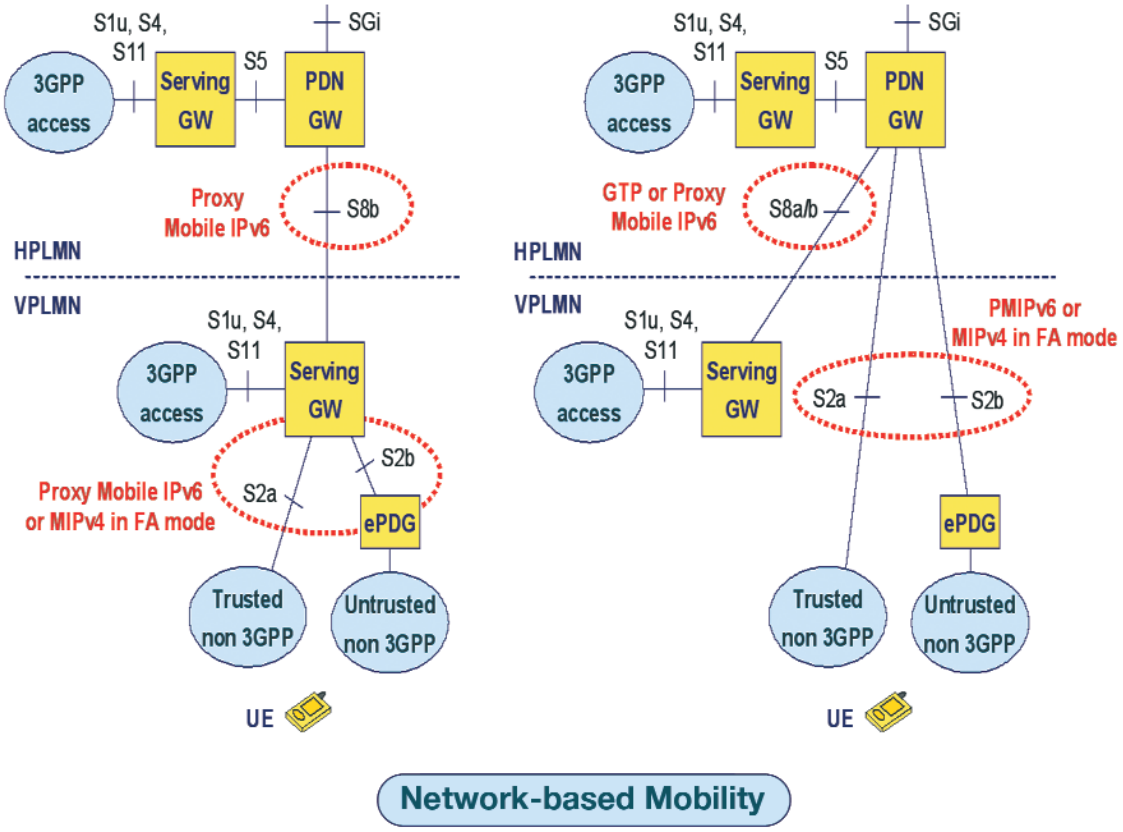
In the case of network based mobility (Figure 2.1.3) there are two possible scenarios, depending on whether the Serving GW in the visited domain is used or not as a local anchor point for 3GPP-non-3GPP mobility.

If the Serving gateway in the visited network acts as a local anchor point, the PDN GW in HPLMN needs to interface via PMIPv6 just with the anchor point in VPLMN. This simplifies the establishment of roaming agreements and the visited operator can exploit the local anchor to enforce policies on UE's data traffic.

On the other hand, if there isn't a local anchor point the HPLMN has to interface via PMIPv6 with all non 3GPP networks in VPLMN. This complicates the establishment and maintenance of roaming agreements.

In both cases the interface between the PDN gateway and the Serving gateway is based on PMIPv6 and, optionally, on GTP if the UE is attached to a 3GPP access.

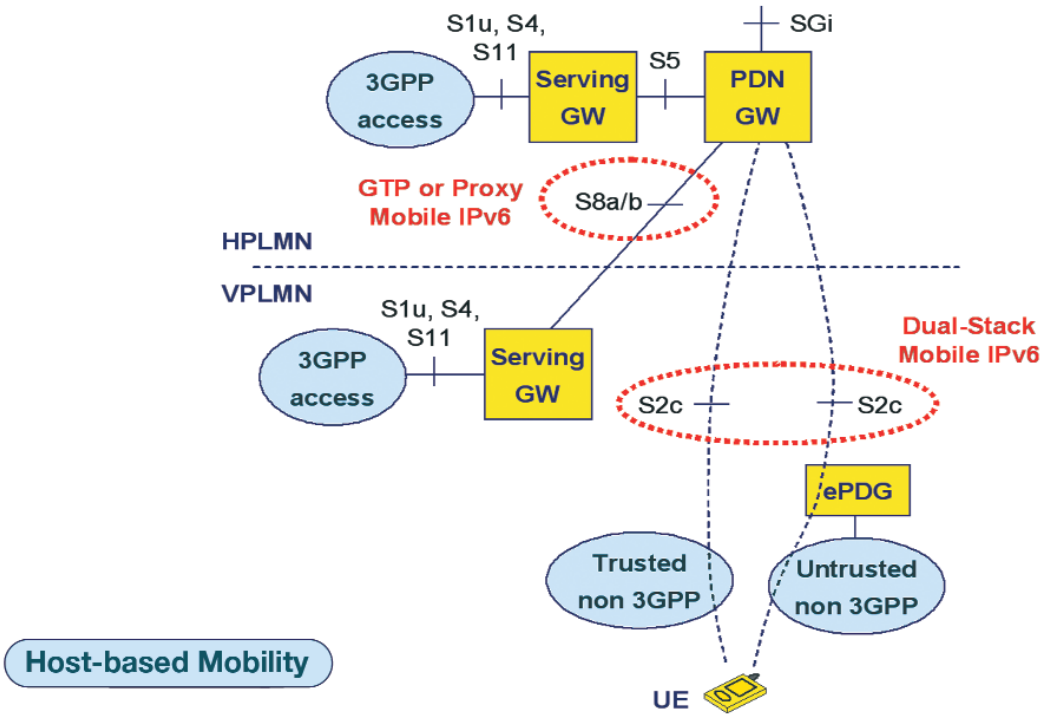
Figure 2.1.3: Network based mobility for the roaming case



On the other hand, if host based mobility is used there is only one scenario agreed for the moment (Fig. 2.1.4).

The scenario where the visited Serving GW acts as a local anchor point for host based mobility is not considered for the moment since it is not clear how to handle Serving GW relocation when the UE moves across VPLMNs.

Figure 2.1.4: Host based mobility for the roaming case



2.1.4. OPEN ISSUES

The work of 3GPP is not yet concluded: a number of issues still remain open. Among them we can cite:

- the bootstrapping problem, i.e. how to configure the user's terminal with the necessary information to start using Mobile IP (e.g. Home Address, authentication data);
- the access to multiple PDNs (Packet Data Networks). At the moment Mobile IP doesn't foresee that the Home Agent provides different services (i.e. access to multiple networks) to users. A mechanism to allow the provision of multiple services and the user to choose the desired service must be identified;
- the management of the QoS in non-3GPP networks. At the moment no standard mechanism is provided to allow the set-up of an end-to-end QoS management between 3GPP and non-3GPP networks nor a mechanism is defined to protect MIP signaling;
- the authentication mechanism used to protect MIP signaling. In the IETF two protocols have been specified for MIPv6 signaling protection: IPsec [4] and Authentication Protocol [5]. IPsec is the standard choice but it requires more computational effort while the Authentication protocol is a lighter mechanism. On the other hand the Auth Protocol needs a key management scheme to provide necessary keys and to guarantee their freshness. A complete evaluation of the two protocols is therefore necessary in order to make a choice. The analysis must take into account many aspects of the two protocols: among them we can cite the amount of resources required on the PDN GW, the signalling overhead over the air interface, support for idle mode UEs, handover latency, and interworking with non-3GPP access systems.

2.1.5. POSSIBLE FUTURE EXTENSIONS

In this context some possible ways to move forward can be identified. First of all multihoming extensions for both host and network based solutions can be studied. This could be useful when most terminals will be multi-interfaced giving the user the possibility to connect to different networks at the same time.

Another area of possible work can be the reduction of the handover latency that, for handovers between 3GPP and non-3GPP networks, still remains an issue. Optimizations in this sense can use pre-authentication mechanisms as well as some kind of context transfer between Access Routers.

Another way to optimize handovers and performance could be the use of the IEEE 802.21 standard (in progress at the moment) which will allow the use of triggers coming from different layers (e.g. layer 2) in order to optimize decision on handovers.

2.1.6. CONCLUSION

In this paper we presented the mobility management solutions adopted in the next generation 3GPP networks (Evolved Packet System). These solutions are based on Mobile IPv6 standard and will be used to manage mobility between 3GPP and non-3GPP networks. Both host based and network based solutions have been considered.

Remaining issues have been presented and analyzed and suggestions on possible future extensions and work items have been provided.

2.1.7. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, IETF RFC 3775, June 2004

[2] draft-ietf-netlmm-proxymip6-01.txt, “Proxy Mobile IPv6” work in progress

[3] IETF, RFC 3344, “Mobility Support for IPv4”

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

[5] Patel e al. “Authentication Protocol for Mobile IPv6”, RFC4285, January 2006

2.2 A Review of Mobility Support Paradigms for the Internet

Deguang Le, Xiaoming Fu, and Dieter Hogrefe
University of Göttingen

ABSTRACT

With the development of mobile communications and Internet technology, there is a strong need to provide connectivity for roaming devices to continuously communicate with other devices on the Internet - at any time and anywhere. The key issue of this vision is how to support mobility in TCP/IP networks. In this paper, we review the TCP/IP protocol stack and analyze the problems associated with it in the mobile environment. We then investigate the mobility support techniques and existing solutions for providing mobility support on the Internet. We classify the proposed solutions based on the protocol layers and present paradigms for each category of layer. We also provide a comparison of the different solutions belonging to different categories, including their advantages and disadvantages. Results have shown that there is no single solution that perfectly addresses mobility support for the Internet. Finally, we conclude this survey with a recommendation of features that ought to be met in Internet mobility support.

2.2.1. INTRODUCTION

With the rapid growth of the wireless access technologies and the increasing number of mobile computing devices, two relevant scenarios other than traditional fixed networking have arisen. Firstly, in a so-called *nomadic networking* scenario, a node requires access to the fixed network (for data or any other information services) at any time and from any location, without the need to continue the ongoing communication with their communicating peers after movements. In the second scenario, namely *mobile networking,* users require their services while roaming, preferably without interruption or the degradation of communication quality. In fact, the first scenario can be regarded as a special case of second one. Nowadays it is common that not only cellular devices, but also other types of computing devices (including PDAs, laptops) may desire to connect to the Internet in a nomadic or truly mobile fashion for various services, such as online gaming, video on demand or stock trading.

The authors are with the Institute for Informatics, University of Göttingen, Lotzestr. 16-18, 37083 Göttingen, Germany (e-mail: le,fu,hogrefe@cs.uni-goettingen.de)

As identified in Section 2.2.2, the traditional TCP/IP networks were originally designed for communication between fixed devices and there are a lot of issues that need to be resolved to support mobility. Given the importance of mobility support on the Internet in the last decade, studies that address these issues have arisen, coming up with a number of protocol proposals and IETF RFCs. Many of them have been designed, implemented and some of them are starting to be deployed. Nevertheless, as analyzed in more detail below, they demonstrate both pros and cons in dealing with mobility support in terms of efficiency, functionality and security etc. Therefore, a general comparison of different solutions is needed, including new emerging alternatives, and a review and rethinking of the architectural aspect of Internet mobility support. Among previous works, Henderson [1] reviewed three host mobility solutions, namely Mobile IP, TCP Migrate, and Host Identity Protocol (HIP) based mobility, which operate in different layers, and compared them from various aspects of performance, security, deployment, scalability, and robustness properties etc. Eddy [2] discussed the strengths and weaknesses of implementing mobility at three different layers of TCP/IP stack, suggesting that the transport layer is probably the best layer candidate to accommodate Internet mobility, and that there should be more collaboration between layers to avoid conflict and inefficiency. These exiting works did discuss some of existing and emerging mobility approaches and proposed some interesting metrics for comparison. Nonetheless, their reviews mainly focused on high layer overview, while an in-depth analysis of the underlying properties of various proposals in introducing mobility to TCP/IP architecture is still missing. At the same time, other approaches are not considered at all. The objective of this paper is to investigate and compare existing Internet mobility support paradigms as comprehensively as possible, and to discuss what could be potentially deployable in terms of functionality, performance and changes to existing systems, etc. Interestingly, INFOCOM 2005 organized a panel discussion session on Internet mobility [3], and a number of issues discussed in this paper have also been elaborated in the panel.

This paper is organized as follows. In Section 2.2.2, we review the traditional TCP/IP stack, and present some general goals for any solution to mobility support for the Internet. In particular, we describe characteristics of communications in the mobile environment, the performance requirements for Internet mobility support, and why the traditional TCP/IP network is unable to support mobility. Section 2.2.3 presents a detailed set of mobility support paradigms, each representing some specific changes to the existing protocol layer, and studies the possible effect and impact, especially the integration of different mobile support paradigms. In Section 2.2.4, we summarize the advantages and disadvantages introduced by these different paradigms, and indicate that all existing solutions have different implications to their application scenarios. There is no single perfect solution so far; mobility support may require some rethinking of the Internet architecture, and there should be some general design considerations for any Internet mobility support solution. Finally, we present our conclusion in Section 2.2.5, which recommends features that ought to be provided for Internet mobility support.

2.2.2. THE TCP/IP STACK AND WHY MOBILITY SUPPORT IS DIFFICULT

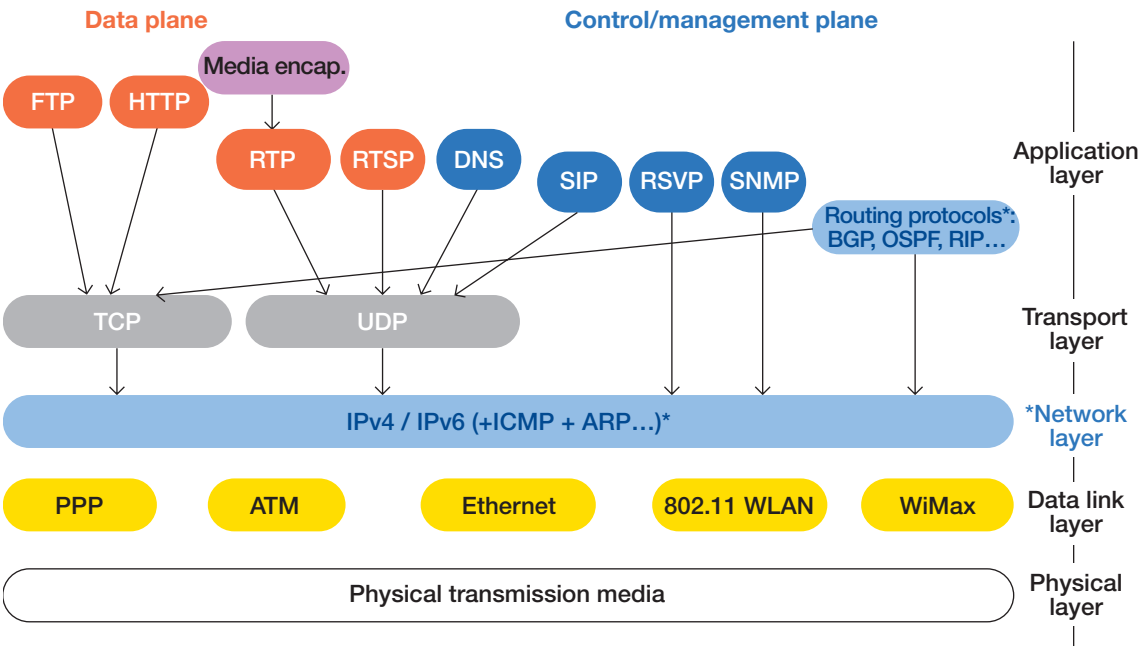
In this section, starting with a review of the traditional TCP/IP, we describe the requirements, general goals for introducing mobility support and problems in this stack.

2.2.2.1. TCP/IP Stack: a Review

For Internet communications, a number of protocols have to run in both end hosts and routers, utilizing a five-layer architecture (which is depicted in Fig. 2.2.1), where the Transmission Control Protocol (TCP),

the User Datagram Protocol (UDP) and the Internet Protocol (IP) make up fundamental elements of the architecture, known as the TCP/IP stack.

Figure 2.2.1: TCP/IP Stack



In the TCP/IP stack, whereas most lower layer (up to transport layer) functions are implemented in hardware devices and OS kernels, the application layer protocols are implemented as user application daemon programs, interfacing with the transport layer to use the network service. The transport layer provides an end-to-end delivery service: TCP provides a connection-oriented service which allows for reliability, fragmentation, flow control, and congestion control, whereas User Datagram Protocol (UDP) provides an unreliable datagram service that enhances basic network functions. The network layer is responsible for the routing and delivery of data from a source node towards a destination node across the same or different types of networks. The data link layer handles issues concerning the physical addressing, network topology, error notification, sequencing of frames, and flow control between neighboring nodes; link layer protocols are typically specified by organizations like IEEE, not the Internet community. The physical layer deals with the electrical/digital characteristics which is actually not part of the TCP/IP stack (it is referred in the stack merely for compatibility with the OSI reference model).

2.2.2.2. Basic Functional Requirements for Internet Mobility Support

Here, the term "Internet mobility support" refers to keeping ongoing communications continuity when an IP-based device moves (i.e., changes its topological point of attachment) to different networks. We exclude the case where the device just moves within a single network (or, data link layer mobility). In order to provide such support, a number of fundamental issues arise, which can be summarized as the following requirements for Internet mobility support.

Handover Management: The most important function needed to support mobility is to maintain the ongoing communication alive while a Mobile Node (MN) moves and changes its point of attachment to the Internet. In order to continue to communicate, a core technology called handover management is required. The main objective of handover management is to minimize service disruption during handover.

Location Management: Another important function needed to support mobility is the reliable and timely notification of MN's current location to those other nodes that need it. The technique to track the desired MN is called location management. Location management involves identifying the current location of the MN and also keeping track of their location changes as it moves on.

Multihoming: With a wide range of wireless access techniques such as GPRS, WCDMA/UMTS, IEEE 802.11x etc. being introduced to provide access to Internet, the future mobile environment will be characterized by diverse wireless access networks, and the MN will be equipped with multiple interfaces supporting different wireless techniques. So it is necessary to require for multihoming support by which the MN can gain access to the Internet through multiple links simultaneously and select, switch dynamic links while moving.

Applications: Internet mobility should also support current services and applications. That is to say, the mobility management mechanism is transparent and without requiring changes to current services and applications.

Security: Any mobility solution must protect itself against misuse of the mobility features and mechanism, for example, from stealing of legitimate addresses or flooding a node with large amount of unwanted traffic. Security therefore is an important concern in providing Internet mobility support.

Motivated by these requirements, we argue that a complete and useful Internet mobility should address these requirements as much as possible. In addition, there are performance requirements for mobile environments as identified as below.

2.2.2.3. Performance Requirements for Internet Mobility Support

While developing an Internet mobility solution, the performance metrics also deserve special attention. [4] discusses the various subnetwork design issues that the authors consider relevant to efficient IP support in a general sense. In this subsection we discuss some performance metrics which are the most relevant for Internet mobility.

- Handover Latency refers to the elapsed time from the last packet received via the old network to the arrival of the first packet along the new network during a handover.
- Packet Loss is defined as the number of packets lost while maintaining communication during a handover.
- Signaling Overhead is defined as the number of messages for the handover and location procedures.
- Throughput is the amount of data transmitted over a mobile Internet in a given period of time.

2.2.2.4. Deployment Requirements for Internet Mobility Support

In addition to functional and performance requirements, there are some considerations that one should take into account to successfully deploy a mobility mechanism in the Internet. Below is a summary of those which seem most prominent ones:

- Minimum changes to the applications. It is desirable not having to change every application when the mobility mechanism is applied in the Internet.
- Avoid adding third-party. Adding a third-party device into the network usually incurs additional management overhead and security vulnerabilities, thus this should be avoided if possible.
- Easily integration into the existing infrastructure. Changes to allow integration into the existing infrastructure should be kept simple, as a well-deployed infrastructure implies a significant amount of investment, operational and administrative/maintenance efforts if requiring new updates for software or hardware in routers.

2.2.2.5. Limitation of Traditional TCP/IP for Internet Mobility

The traditional TCP/IP was designed for fixed computer networks. This subsection will analyze some of the limitations of TCP/IP for Internet mobility.

1) **Limitation of Link Layer:** To its maximal possibility, wireless access techniques only provide the mobility of homogeneous networks at the link layer [5], which is not appropriate for Internet mobility across heterogeneous networks. In general the nature of network heterogeneity requires mobility support functions provided in higher layers. Besides, in mobile environments, the data link layer is based on the wireless access technologies (such as 3G, WLAN etc.), which are characterized by low bandwidth, high bit error rates, faded and interfered signal with radio channel etc. These wireless link features are encountered by the moving terminals, which may degrade the transport performance of high layers.
2) **Limitation of IP address:** The IP address of network layer plays both roles of locator and identifier. In the mobile environment, the IP address of the MN has to be changed to represent the change of its point of attachment to the network when it moves from one to another network. In traditional TCP/IP, a change of the IP address makes it impossible for other devices to contact the device using a constant IP address. In addition, even if the device is able to obtain a new IP address dynamically, the transport connections established in the previous network will be broken after the change of IP address.
3) **Lack of Cross-Layer Awareness and Corporation:** For example, the design of traditional transport layer protocol relies on the services provided by the network layer, and does not consider wireless link properties and mobility. Thus, the congestion control of TCP [6] does not distinguish the packet loss caused by handover of mobility and wireless link properties from the normal packet loss in wired network, which degrades transport performance [7]. Besides, TCP congestion control is based on the assumption that the end-to-end path of a connection is relatively stable after connection establishment.

   In the mobile environment, the MN will change its access point of Internet attachment without notifying TCP moving, and thus the existing end-to-end connection path has to be changed accordingly, which may violate this assumption and cause TCP to make congestion control decisions based on invalid information [8].
4) **Limitation of Applications:** Many applications based on traditional TCP/IP architecture are also limited in use in the mobile environment. For example, in Domain Name System (DNS), the Fully Qualified Domain Name (FQDN) is usually statically bound to a node's IP address. Thus the tight binding between FQDN and IP address will be invalid because of the dynamic change of IP addresses of the MN.

2.2.3. EXTENDING TCP/IP TO SUPPORT MOBILITY

As mentioned in the previous section, the traditional TCP/IP is not appropriate for Internet mobility. Therefore, various solutions have been developed to address it. Among them, those representing the network layer are Mobile IPv4 (MIPv4) [9], Mobile IPv6 (MIPv6) [10] and Location Independent Network Architecture for IPv6 (LIN6) [11]. In the transport layer, a wide range of studies have been undertaken to provide mobility support for TCP [12]-[18], the Stream Control Transmission Protocol (SCTP) [21], and the Datagram Congestion Control Protocol (DCCP) [22]. Session Initiation Protocol (SIP) [23], Dynamic DNS (DDNS) [24] and IKEv2 Mobility and Multihoming (MOBIKE) [25], [26] provide mobility support in the application layer.

Some researchers were interested in introducing a new protocol layer between the classic network layer and transport layer to provide Internet mobility, such as Host Identity Protocol (HIP) [27] based mobility [28], and Multiple Address Service for Transport (MAST) [29].

In this section, we investigate the solutions for improving mobility of TCP/IP in more details.

2.2.3.1. Mobility Support in Network Layer

Because IP is the ubiquitous internetworking layer for the Internet, solutions that build on the existing network layer are considered a natural approach. Mobile IPv4 (MIPv4) proposed by Perkins [9], Mobile IPv6 (MIPv6) by Johnson et al. [10] and various enhancements to the performance of MIPv4/v6 proposed in [30]-[36] have represented "classic" means for supporting mobility on the Internet. The Location Independent Network Architecture for IPv6 (LIN6) proposed by Teraoka et al. [11] provides an alternative to mobility support to MIPv6. These protocols apply techniques such as proxy, tunneling [37] and separating [38] to deal with mobility.

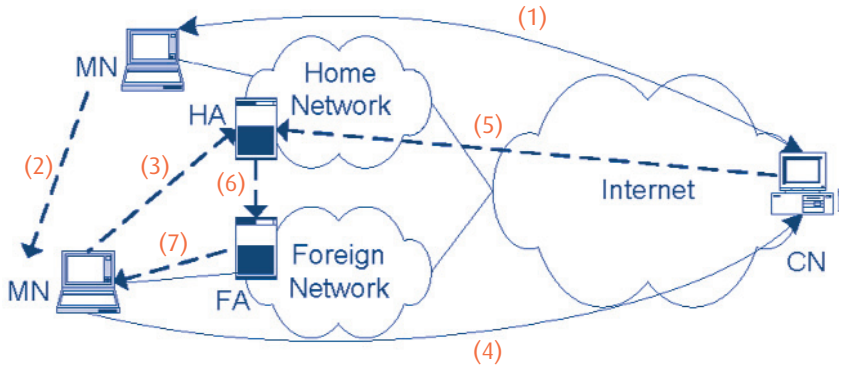
2.2.3.1.1. Mobile IPv4/IPv6 and Its Enhancement

MIPv4 defines a home network where the MN is assigned a permanent IP address called home address which identifies the MN; and it also defines foreign networks that the MN visits. It introduces two new entities, namely the Home Agent (HA) and the Foreign Agent (FA) to relay the packets between the MN and Correspondent Node (CN).

In MIPv4, when the MN is on its home network, it acts like any other Fixed Node (FN) of that network and requires no special mobile IP features. Each time when it moves out of its home network and gains access to a foreign network, it obtains a Care of Address (CoA) e.g., through Dynamic Host Configuration Protocol (DHCP) [39], and informs its HA of the new address by sending a Registration Request message to the HA. Upon the HA receiving the Registration Request message, it replies to the MN with a Registration Reply message. The HA then assumes the MN and once packets destined to the MN arrive at the home network, the HA intercepts these packets by using Proxy Address Resolution Protocol (ARP) [40], [41] and forwards them to the MN with the CoA via a tunneling technique. When the FA receives packets, it removes the IP encapsulation of the packets and delivers them to the MN. When the MN wishes to send packets back to the CN, the packets are routed directly from the MN to the destination, where the MN uses the FA as its default router. Figure 2.2.2 shows the MIPv4 architecture and its operations.

Packets of MIPv4 to the MN travel via the HA, whereas the packets from the MN are routed directly to the destination, which incurs triangular routing. MIPv4 registration clearly takes a long time, which increases handover latency greatly. In addition, since packets destined for the MN are not delivered until registration is completed at the HA. This interruption may cause packet loss. Furthermore, the Agent Advertisement

Figure 2.2.2: MIPv4 Architecture and its Operations



1. Normal communication between MN and CN
2. MN moves from home to a foreign network
3. MN registers its CoA
4. MN sends packets to CN directly
5. CN sends packets to MN's Home Address
6. HA tunnels the packets to MN's FA
7. FA delivers the received packets to MN

messages and Registration messages during the node traverses also introduce overload over the Internet. Especially, as the number of wireless users grows, the signaling overhead will increase. To avoid these drawbacks, a number of techniques such as the routing optimization technique [42], anticipation technique [31], hierarchical technique [30] and paging technique [43] etc. have been developed to enhance the basic protocol. In specific environments where a MN changes its point of attachment to the network frequently and the number of mobile users grow simultaneously, a number of micro-based mobility protocols (such as regional registration [30], Low Latency Handover in MIPv4 [31], Hawaii [32] and Cellular IP [33]) have been proposed to improve the performance of MIPv4.

Security Considerations for MIPv4: Firstly, the MN may suffer from the router's ingress filtering. Foreign network protected by a firewall may reject the packets when the MN sends the packet directly to the CN using its home address as the source address. Ingress filtering can be avoided by using reverse tunneling. Secondly, a major risk is associated with the authentication of the MN. If a bogus CoA was registered with the HA, it could prevent all connections to the MN, or even worse, cause all packets to be redirected to some attacker. To prevent this, the registration messages must be authenticated. Therefore, RFC 3344 [9] specifies the authentication extensions which is supplied with MIPv4 registration messages. The authentication extension contains the Type, Length, Security Parameter Index (SPI) and a "message digest", which is calculated using HMAC-MD5 [44] (and keyed MD5 [45] for the backward compatibility with older MIPv4 implementations). Thirdly, without replay protection, the attacker could perform valid but unwanted operations afterwards by resending old registration messages. Therefore, MIPv4 proposes to add some information (e.g., timestamps) to the registration messages by the message sender, and then the receiver can check the validity of the message. To avoid the latency and clock resynchronization issues, an optional nonce based replay-protection approach is also suggested [9].

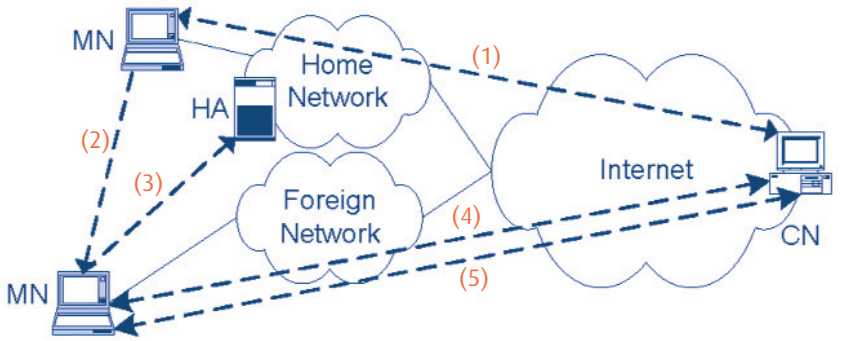
Because the traditional IP protocol has a variety of limitations for the next generation Internet [46], the IETF has defined a new network layer protocol, i.e. IPv6, to replace the current IP protocol. IPv6 is inherent in supporting Internet mobility management via MIPv6 [10]. MIPv6 follows the same basic principles as MIPv4,

including home address, CoA, HA and tunneling. The main difference is that an FA no longer exists and the security aspect has been improved. In addition, route optimization has also been incorporated into MIPv6.

In MIPv6, when the MN moves to another network, it acquires the CoA through either stateful [47] or stateless [48] address auto-configuration. After obtaining a new CoA, the MN registers to the HA and also to the CN with Binding Update messages (BUs). The HA and the CN record this binding in its binding cache. After this, packets from the CN can be routed directly to the CoA of the MN with the CN's home address in the Routing header. Similarly, the MN sends all packets to the CN directly using the Home Address Destination option, which eliminates the triangle routing. In the event that the CN wants to communicate to the MN for the first time, the first packet is tunneled through the HA like MIPv4. The HA intercepts any packets addressed to the MN's home address and tunnels them to the MN's CoA using IPv6 encapsulation. For discovering the HA, MIPv6 defines the Dynamic Home Agent Address Discovery (DHAAD) mechanism [10]. Figure 2.2.3 shows the MIPv6 architecture and its operations.

Because BUs are transferred between the MN and the CN, as well as the HA, this incurs extra overhead, especially when the MNs move quickly or increase proportionally. Thus, the IETF developed the Hierarchical Mobile IPv6 (HMIPv6) [34] protocol to reduce overload and improve handover speed by separating the mobility management local mobility from global mobility. HMIPv6 proposes a multi-level hierarchical network architecture and defines a site as any level of the hierarchical architecture. Inside the visited - or foreign - network, a new entity called a Mobility Anchor Point (MAP) is introduced. It acts like a local HA. When the MN moves within the foreign network, it shall only register its new local CoA to the MAP. The local mobility can be completely hidden from all nodes outside the site. When the MN moves between inter-sites, the mobility shall be handled by MIPv6.

Figure 2.2.3: MIPv4 Architecture and its Operations



1. MN (at home) communicates with CN
2. MN moves
3. MN registers its CoA with HA
4. Binding update/acknowledgement
5. MN communicates with CN directly

Fast Handovers for Mobile IPv6 (FMIPv6) [35] is another proposal aiming at optimization for MIPv6. The main idea of FMIPv6 attempts to acquire information that is needed to join a new link before disconnecting communication at the old link. It utilizes co-operating access routers which can request information from other access routers that are possible candidates for a handover. This is done by establishing a tunnel between the two access routers that allows the MN to send packets as if it was connected to its old access point

while it is completing its handover signaling at its new access router. Therefore, it reduces the procedure time of movement detection, new CoA configuration and binding updates etc. during handover, and eliminates packet loss. Jung et al. [36] propose a combination of both approaches of HMIPv6 and FMIPv6, which is designed to add up the advantages of both and provide additional improvements to reduce signaling overload, packet loss and handover latency.

Security Considerations for MIPv6: In MIPv6, the security features are integrated and provided as an extension to headers. The traffic can be protected by the IP security protocol (IPsec) [49] Authentication Header (AH) [51] and Encapsulating Security Payload (ESP) [50] extension headers. Furthermore, IPsec is also suggested to protect MIPv6 BUs and BAs between the MN and the HA from forgery of the data originator and replay attacks. The MN and the HA are required to establish an IPsec security association (SA) either by manual configuration or automatic key management protocols. BUs and BAs between the two entities can then be protected using the IPsec ESP in transport mode or the AH extension headers. For the protection of the registration messages of BUs and BAs between the MN and the CN, MIPv6 uses the return routability procedure to assure that the right MN is sending the messages. The detailed procedure is specified in [10], based on the idea of relying of the routing infrastructure to check that the MN is reachable both at its claimed home address and its claimed CoA. The advantage of the method is that it limits the potential attackers to those having an access to one specific path on the Internet, and avoids forged BUs from anywhere else on the Internet. The weakness of the method is that it does not defend against attackers who can monitor the path between the home network and the correspondent node. The return routability procedure is therefore subject to active attacks like the Man-in-the-Middle attack etc. launched by such attackers. This weakness has been investigated and some improvements have been proposed [52]-[54]. In addition, MIPv6 develops the route optimization as an alternative to the reverse tunneling. The MN uses home address in a packet with Home Address Destination option. MN uses its CoA as source address in the IP header and sends the packet directly to the CN, so it can avoid ingress filtering and pass through a firewall. Unfortunately, there have not been enough security considerations for HMIPv6 and FMIPv6, and further security and operational issues with regards to MIPv6 and its extensions are still not yet addressed, for example interacting with the AAA infrastructure, bootstrapping, and general stateful packet firewall traversal. Some of these issues have been discussed in recent IETF proposals and research investigations (e.g., [55]-[58]).

2.2.3.1.2. LIN6

LIN6 proposes an alternative Internet mobility solution for the IPv6 protocol. Its basic idea is separating the identifier and locator in the IPv6 address. LIN6 introduces the LIN6 ID for each node as the node identifier so that each node can be identified by its LIN6 ID no matter where the node is connected and no matter how many interfaces the node has. In addition, it defines two types of network addresses: the LIN6 generalized ID and LIN6 address. The LIN6 generalized ID is formed by concatenating a constant value called the LIN6 prefix before the LIN6 ID. It is used in the transport layer to identity the connection. The LIN6 address is formed by concatenating the network prefix and LIN6 ID. It is used to route packet over the network layer. The network prefix will then change according to the network where the MN attaches. Figure 2.2.4 illustrates the LIN6 architecture.

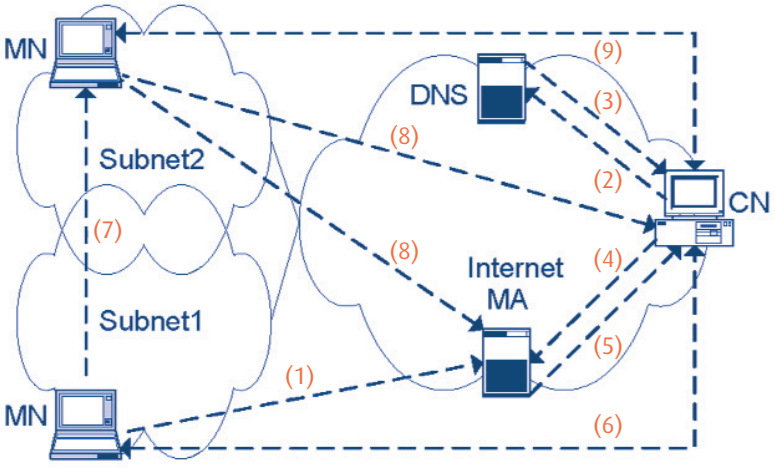
Figure 2.2.4: LIN6 Architecture

Application layer
Transport layer: <LIN6 generalized ID, port> pair
Network layer: Translation between LIN6 generalized ID & LIN6 IP address
Data link layer

In LIN6, on packet transmission, the network layer extracts the LIN6 ID from the LIN6 generalized ID and concatenates the network prefix and LIN6 ID to create the LIN6 address of destination node. On packet reception, the network layer removes the network prefix part of the LIN6 address, and then attaches the LIN6 prefix to create the LIN6 generalized ID of source node. When the MN moves to another network and obtains the network prefix of the new network, the MN updates its location with the CN in one of two ways: if the MN has a security association, it sends the Mapping Update Request message to the CN. In this case, the Mapping Update Request message must include the Authentication Header. If the MN has no security association, the MN sends the Mapping Refresh message to the CN to inform the CN of the event that the MN has moved. As a result, the CN re-queries the Mapping Agent (MA) to obtain the new network prefix of the MN. The MN also sends Mapping Update Request message to the MA to inform the current network prefix.

In order to track the current location of the MN, LIN6 employs the MA to maintain the mapping of the LIN6 ID and the network prefix, and makes use of DNS to locate the MAs of the MN. Each MA shall be assigned a predefined 64-bit value called MA IFID as the interface identifier. When the MN is powered on and attaches to a network for the first time, it registers its current location with its MAs. When the CN wants to communicate with the MN for the first time, the CN sends a query to the DNS sever and obtains the Authentication, Authorization, Accounting and Auditing (AAAA) record which consists of the network prefix of the MA and the LIN6 ID of the MN. Then the CN generates the IPv6 address of the MA by concatenating the upper 64 bits of AAAA record and the MA IFID, which is used as the lower 64 bits of IP address. Then it queries the MN's MA the network prefix of the MN and gets the IP address of the MN. When the MN moves to a new network, it registers the new network prefix with the MA and the CN by sending Mapping Update messages (MUs) with the Authentication Header or Mapping Refresh message. Figure 2.2.5 shows the LIN6 network architecture and its operations.

Figure 2.2.5: LIN6 Mobility and its Operations



1. Register MN network prefix <->LIN6 ID at bootstrap
2. Query MN FQDN
3. Response MA network prefix+LIN6 ID
4. Query MN LIN6 ID
5. Response MN network prefix
6. Establish connection and start data transfer
7. Move
8. Update the mapping of LIN6 ID<->MN network prefix
9. Go on communication

Security Considerations: In LIN6, location registration with the DNS/MA is authenticated by IPsec or exchanged cookies. Thus, the security level is almost the same as MIPv6.

2.2.3.1.3. Analysis of Network Layer Mobility

MIPv4 provides network layer mobility and transparency to the higher layers. However, there are a number of problems associated with it, such as that triangular routing introduces higher latency and extra overhead to the network. In addition, all packets to MNs pass through the HA, which induces heavy load for the HA, and in the event of an HA failure, all the desired traffic for MNs using that HA will be interrupted. Thus, MIPv4 is vulnerable to single point of failure. Although many enhanced techniques and micro-mobility protocols can improve MIPv4 performance, MIPv4 still has the weakness in terms of efficiency and complexity. MIPv6 has the advantages of inherent mobility, security support and routing optimization compared to MIPv4. BUs and Binding Acknowledgment messages (BAs) are authenticated using IPsec AH and ESP. The CN learns the MN's CoA dynamically and sends packets directly to the MN by using IPv6 routing header. However, like MIPv4, MIPv6 has the same problem of third device, which increases failure probability of communication. And it has additional header overhead. The enhancements of HMIPv6, FMIPv6, and their combination improve the performance by minimizing signaling overhead, packet loss, and handover latency, but their scalability and complexity are a concern.

In comparison with MIPv4/MIPv6, LIN6 is more tolerant of defects/errors because the HA in MIPv4/MIPv6 cannot be replicated to the subnet other than the home link, while the MA introduced in LIN6 can be replicated anywhere on the Internet. And LIN6 has less overhead due to its avoidance of the extension header and tunneling. That is, LIN6 does not use any packet interceptor or forwarder such as the HA, so its routing is the same as traditional IP-based routing. Conceptually, LIN6 adds a transient "presence" service to DNS lookup for dynamic locator mapping (from this sense, LIN6 can also be considered as the introduction of a new layer), but it is only limited to IPv6.

2.2.3.2. Mobility Support in Transport Layer

Because the transport layer is subject to the impact of mobility, a lot of work on TCP performance improvement and mobility enhancement has been carried out over the past years [12]-[18]. There were efforts on enhancing UDP for mobile environments (e.g., [19]). Recently, the mobility support for the new transport layer protocols of SCTP and DCCP has been proposed. The basic idea of enabling transport layer mobility is to remove network layer dependences by using indirection, migration, tunneling or multihoming techniques etc.

2.2.3.2.1. Extending TCP

Much focus has been placed on the TCP as it is the most widely used transport layer protocol. We classify the different proposals into two categories: Improving TCP performance for the mobile Internet and TCP mobility support extension.

Improving TCP Performance for the Mobile Internet: TCP is a reliable transport protocol tuned to perform well in traditional wired networks where network congestion is the primary factor of packet loss. However networks with wireless links and mobile hosts induce significant increase in losses due to high bit error rates, temporary disconnection and limited bandwidth etc., which violate many of the assumptions made by traditional TCP, causing TCP not adapt well to these environments. A number of researchers therefore have aimed to improve TCP performance for the mobile Internet. Indirect TCP (I-TCP) [12] and Mobile TCP (MTCP) [13] focus on the Bit Error Rate (BER) problem of wireless link. In ITCP and MTCP, a TCP connection between the MN and the FN is split in two with a device called Mobile Support Station (MSS) and the connection between the MSS and MH is optimized for the wireless link. Both I-TCP and MTCP achieve better

throughput than standard TCP. Caceres and Iftode used a fast retransmission mechanism [14] to address the problem of short disconnections during handover. Haas developed an asymmetric transport layer protocol so-called Mobile-TCP [15] to minimize communication overhead on the MN. In Mobile-TCP, functions through algorithms and procedures are implemented with the lower complexity on the MN than the FN without sacrificing performance and features. To avoid the invalid TCP congestion control, decisions incurred by the change of TCP connection path in the mobile environment, Y. Swami et al. [8] implement a Lightweight Mobility Detection and Response (LMDR) TCP option that allows the MN to inform the CN when it detects the location change which can be assisted by other layers such as the neighbor discovery of MIPv6. Based on the notification, the proper congestion control behavior can take place and react to correct the performance.

The above proposals optimize the transport performance of TCP over networks with wireless links. Although they can not support the real mobile networking, they provide the mobility enhancement for the nomadic networking scenario.

Mobility Extension to TCP: Other researchers have considered the issue of how to maintain the ongoing TCP connection when an interruption occurs due to a change in the IP address.

Funato [16] develops a simple and secure redirection mechanism called TCP Redirection (TCP-R) to maintain active TCP connections. The concept of TCP-R is to revise the pair of addresses in the ongoing TCP connection when the IP address associated to TCP connection is changed by TCP redirection options extension. In TCP-R, when the MN initiates a new connection, it shall ascertain if the CN is TCP-R aware or not, and then may perform a redirection operation. When the MN moves and is assigned a new IP address, it sends a Redirect message with RDREQ option to the CN. Upon the CN receiving the message, it validates the connection authenticator with ATREQ and ATREP. If correct, it revises the pair of addresses of the ongoing TCP connection with the new MN's IP address. Simultaneously, the MN also revises its own pair of IP addresses. Finally, they resume to communicating with the revised TCP connection.

Snoeren and Balakrishnan [17] propose an end-to-end approach to support TCP mobility through a migrating technique. TCP Migrate is similar to TCP-R. It differentiates from TCP-R through its different implementations by specifying different TCP migrate options.

MSOCKS [18] presents an alternative TCP mobility support by split-proxy mechanism and extension to SOCKS [59]. In MSOCKS, when the MN changes the IP address that a TCP connection uses to communication with the MSOCKS proxy, it opens a new connection to the proxy and sends a RECONNECT message with the connection identifier of the existing connection. Upon receiving the RECONNECT message, the proxy separates the old connection between MN and Proxy (MN-Proxy) from the connection between the Proxy and the CN (Proxy-CN); and then concatenates the new MNProxy connection to the Proxy-CN connection in place of the old MN-Proxy connection. Finally the proxy closes the old connection. Once the concatenation is setup, the proxy sends an OK message to the MN.

As TCP is one of the primary protocols in the TCP/IP stack, the performance of TCP over a mobile environment is still a hot topic today after almost ten years of study. For example, Elaarag surveyed and compared different approaches done to improve the performance of TCP over mobile wireless networks in his paper [7]. Jaiswal and Nandi [60] evaluated the impact of MIPv6 on TCP variants. These researchers give some new guidance for improving TCP performance in the mobile environment or mobility enhancement by itself.

2.2.3.2.2. M-UDP

Since wireless links tend to be susceptible to BERs and UDP will also sustain a large percent of packet loss. Thus, Brown and Sigh [19] proposed a Mobile UDP (M-UDP). M-UDP aims at reducing packet losses in wireless

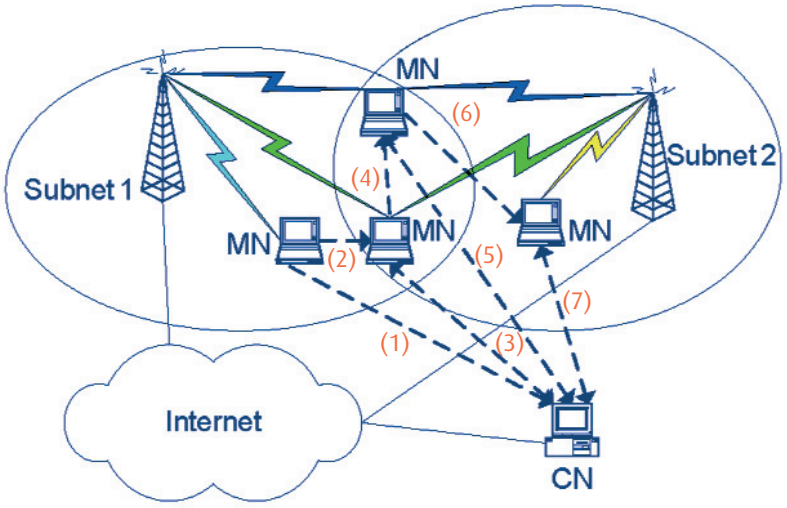
links. The idea is similar to I-TCP and M-TCP, namely, to split UDP connections in two at some node close to the mobile user. This node (named as "Supervisor Host", or SH) attempts to use any free bandwidth to retransmit packets lost during a fade thus ensuring that the number of lost packets is kept small. Every UDP packet is buffered at the SH; the SH discards a packet if it has run out of buffer space or if it has been observed to have been transmitted a certain amount of times. This approach is simply a straight-forward solution and does not consider security in the first place. Further details are described in [19], [20].

2.2.3.2.3. MSCTP

A recently developed IETF transport layer protocol, the Stream Control Transmission Protocol (SCTP) [21], provides another potential for mobility support due to its multihoming feature. Using SCTP's ADDIP extension [61], Mobile SCTP (MSCTP) has been proposed [62].

In MSCTP, the MN initiates an SCTP association with the CN by negotiating a list of IP addresses. Among these addresses, one is chosen as the primary path for normal transmission, and the other addresses are specified as active IP addresses. When the MN reaches a new network and obtains a new IP address, it sends an Address Configuration Change (ASCONF) Chunk with an Add IP Address parameter to inform the CN of the new IP address. On receiving the ASCONF, the CN adds the new IP address to the list of association addresses and returns the ASCONF-ACK Chunk to the MN. While the MN is moving, it may change the primary path to the new IP address via the path management function [21]. The SCTP association, therefore, can continue data transmission while moving to the new network. The MN also informs the CN to delete the IP address of the previous network from the address list by sending an ASCONF Chunk with a Delete IP Address parameter when it confirms that the previous network link has permanently failed. Figure 2.2.6 illustrates the operations of MSCTP.

Figure 2.2.6: MSCTP Mobility and its Operations



1. Initiate an association through subnet 1
2. Move
3. Add IP into the association
4. Move
5. Change the primary Path
6. Move
7. Delete IP from the association

Security Considerations: Unlike TCP, SCTP uses a four step negotiation process to initiate an association, which can prevent the Denial of Service (DoS) attacks such as an SYN attack. IPsec is then used to secure the SCTP communication.

The Addition/Deletion of an IP address to an existing association during mobility does provide an opportunity in which existing associations can be hijacked. The attacker is then able to intercept and alter the packets sent and received in the association. For this reason, MSCTP suggests using IPsec or Transport Layer Security (TLS) [63], [64] to protect against this insecure/threatening environment.

2.2.3.2.4. DCCP

The Datagram Congestion Control Protocol (DCCP) [22] provides integrated mobility and multihoming support by defining a DCCP-Move packet type and two new DCCP features: Mobility Capable feature and Mobility ID feature. DCCP specifies the mobility support as optional and default to be off, therefore DCCP nodes must enable mobility support by Mobility Capable feature.

Firstly, the MN sends a Change L option of Mobility Capable feature to inform the CN that it would like to enable changing its address during connection. Then the CN sends a Change R option to confirm with the MN. After that, the MN sends a value of Mobility ID feature that is used to identify a connection. The value of a Mobility ID feature is selected randomly for security reasons, and a new value is chosen after each move of the MN. The CN confirms the value of the Mobility ID feature by sending a Conform L option. When the MN reaches a new network and obtains the new IP address, it sends a DCCP-Move packet containing a Mobility ID value that was chosen for connection identification. Upon receiving a DCCP-Move packet, the CN sends a DCCP-Sync message to the MN, and changes its connection state, using the new MN address.

Security Considerations: DCCP does not provide cryptographic security guarantees. Nevertheless, by sequence number validity checks, DCCP can protect against some attacks. For example, attackers cannot hijack a DCCP connection unless they can guess valid sequence numbers, which are randomly chosen according to the guidelines in [65].

2.2.3.2.5. Analysis of Transport Layer Mobility

The TCP extensions proposed for improving transport performance on the mobile Internet cannot deal with mobility well on their own. Their main purpose is merely to minimize degradation of the transport performance. The mobility enhancements of TCPR, TCP Migrate and MSOCKS to TCP can handle mobility and keep all features of the standard TCP. Their operations are done in a secure way.

MSCTP provides an alternative solution in the transport layer. It can support seamless handover and improve transport performance. However, the current MSCTP proposal only illustrates the basic requirements for Internet mobility. Some essential issues, such as when and by which criteria the primary path is changed, or the addition and deletion of the IP addresses mapped to the SCTP association should occur during handover, are open to further study. Moreover, MSCTP by itself does not handle location management, thus a proposal on reusing MIP for location management in MSCTP is proposed in [66].

Similarly, the current specification of DCCP is at its primitive stage. There are many problems unsolved. For example, DCCP has no support for simultaneous movements of both communicating endpoints, i.e. DCCP supports mobility of only one endpoint, while the other one remains stationary.

2.2.3.3. Providing Mobility Support in a New Layer

Traditional TCP/IP protocols are already heavily loaded down with functionalities that have been added over the years. Optimization and adding new functionalities to support mobility are very difficult. A new idea has therefore emerged for Internet mobility which supports introducing a new layer, such as HIP and MAST, where Internet mobility is deployed.

2.2.3.3.1. HIP

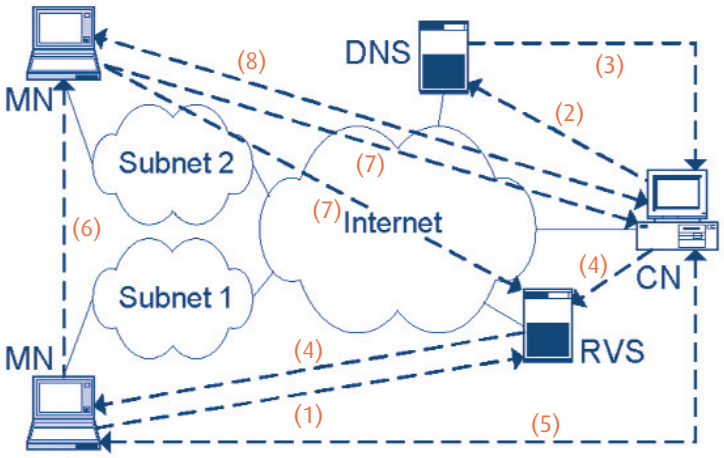
The Host Identity Protocol (HIP) [67] is being designed by the IETF to establish secure communication and to provide continuity of communication. Similar to LIN6, HIP is based on the idea of separating location from identity by an interposed host identity protocol layer that operates between network and transport layers (cf. Figure 2.2.7). HIP introduces a new host identity namespace called Host Identifier (HI), which is a public key. The transport layer connection is bound to HI instead of the IP address, and the IP address becomes a pure routing message. The HI is dynamic, mapped to one or more IP addresses in the HIP layer. In practice, HIP uses a Host Identifier Tag (HIT) to represent HI. The HIT can be obtained by taking the output of a hash function over the HI, and truncated to the IPv6 address size.

Figure 2.2.7: Introducing HIP into the TCP/IP stack

Application layer
Transport layer: <HI, Port> pairs
Host Identity layer: Translation between HI and IP address
Network layer
Data link layer

In HIP, the dynamic binding between HI and IP address is achieved by using the Update packet with HIP Readdress Packets (REA) parameter. In addition, HIP employs the Rendezvous Sever (RVS) to provide location management. On HIP initiation, the initiator retrieves the RVS IP address by looking up the domain name of the peer from DNS with a HIP RVS Resource Record (RR), and sends I1 with destination HIT packet to the RVS. The RVS then forwards the initial HIP packet to the peer at its current location. After receiving I1, the peer completes HIP initiation directly without the help of RVS. Throughout ongoing communication, the MN moves and acquires a new IP address, sending an HIP Update packet with REA to inform the CN of the new IP address, and the CN responds to the ACK. Due to security concerns, the CN may verify that the MN is available through the new IP address. Once the CN has successfully verified this, the new IP address becomes active and the old address is removed, so that the CN can communicate through the new IP address. Figure 2.2.8 illustrates the operations of HIP.

Figure 2.2.8: MSCTP Mobility and its Operations



1. Register MN HI<->IP
2. MN FQDN
3. MN HI, RVS IP
4. I1
5. Remainder data
6. Move
7. Update the binding of HI<->IP
8. Go on communication

Security Considerations: In HIP, the connection establishment procedure includes four steps instead of the traditional three of TCP: This prevents DoS attacks. Communications are bound to the public keys of the HI, as opposed to IP addresses, and are encrypted with ESP, so the hijack attempt would also be unable to reveal the contents of communications. The REA message is also signed with the sender's public key, so it is impossible to hijack communications through the use of REA message.

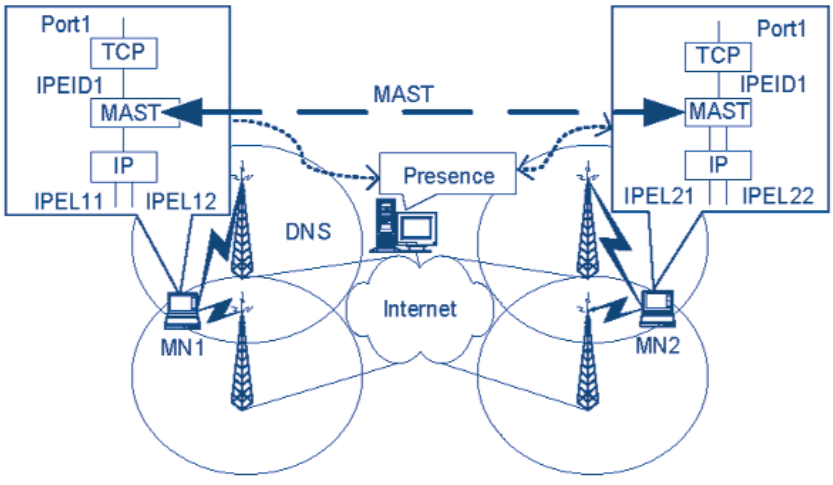
2.2.3.3.2. MAST

Multiple Address Service for Transport (MAST) was proposed by Crocker [29] for Internet mobility and multihoming. Like HIP, MAST defines a layer between the network and transport layers without creating new namespace by using the existing IP addresses, in which the initial IP address assigned for the transport layer connection/association is used for the identifier of the MN, and other IP addresses added dynamically while moving is used for the locator of the MN. Thus the basic idea of MAST in providing mobility is simple: it maps different IP addresses to the single initial IP address.

MAST defines a mechanism that supports multiple IP address association. The MAST association is manipulated with Request/Response messages, which are used to initially establish the MAST association, update the set of valid IP addresses, query association status, convey error information and terminate the association etc.

In MAST, when the MN moves across the Internet, the IP addresses of the MN locator may be added and removed, while the initial IP address continues to be bound to the transport layer. Other addresses of the MN locator are mapped to that initial IP address of the MN identifier by MAST control exchange. Over the life of the association, the different MN locator addresses might be active at different times. To find the MN, MAST uses DNS to provide the information of dynamic presence service relating to the MN. The DNS SRV [68] record is defined to reference a dynamic presence service through which an endpoint can register its current set of IP addresses. MAST specifies that the MN registers its current address with dynamic presence service available through the Extensible Messaging and Presence Protocol (XMPP) [69]. Figure 2.2.9 illustrates the MAST-based approach for mobility management.

Figure 2.2.9: MAST-based Approach for Mobility Management



Security Considerations: To resist the attacks of hijacking an association, MAST uses association-specific weak authentication [70], which ensures that later packets come from the same source as the initial packet. In addition, IPsec or TLS is also suggested for other security issues like spoofing and redirection etc.

2.2.3.3.3. Analysis of New Layer Mobility

HIP supports multihoming by dynamic mapping from one HI to multiple IP addresses. It also resolves the problem of simultaneous movement of endpoints by resending the HIP Readdress message to the RVS if no reply is received. However, the RVS also changes the basic property by replacing the IP addresses of their client nodes in the DNS with their own. The IP address in the DNS entry therefore no longer directly designates the endpoint. It suffers from failures because the I1 packet must be relayed by the RVS when initializing a connection. In addition, the applications that have followed the structure of traditional layers have to be modified to it.

MAST does not define any new namespace or addressing structure, and requires no change to IP modules or transport modules. And it has no additional packet header overhead and minimal additional packet-processing overhead. Hence MAST has a low barrier to adoption and use. However as its development is still in its preliminary stage there are many open issues to be resolved. For example, the optimal locator selection can imply some design difficulties.

2.2.3.4. Mobility Support in Application Layer

Attempts have also been made to support Internet mobility in conjunction with the application layer. This section discusses Internet mobility support using SIP, DDNS and MOBIKE in the application layer.

2.2.3.4.1. SIP

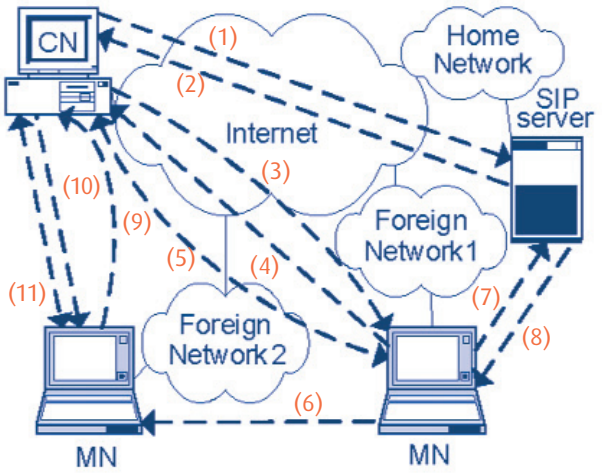
The Session Initiation Protocol [23] was initially developed by the IETF as an application layer multimedia signaling protocol. Nonetheless, it demonstrates potential capabilities for Internet mobility through its ability to define a number of specific entities and specify SIP messages. In SIP, the main entities are a user agent, redirect server and proxy server. Generally, the user agent is the only element where media and signaling converge. It identifies incoming SIP messages from the user and tracks SIP messages according to user actions. The redirect server receives SIP messages and identifies the current location of the node. The proxy server relays SIP messages. Both the redirect and proxy servers can be used for location management. They accept location registrations from users. Typically, the SIP server denotes both the redirect and proxy server. The SIP messages defined in SIP include INVITE, ACK, BYE, OPTIONS, CANCEL and REGISTER etc.

In recent years, there have been several proposals for SIP mobility support [71]-[76]. The basic idea can be summarized as follows. When the CN initiates a session with the MN, it sends an INVITE message. The SIP server in the home network of the MN has current information about the MN's location and redirects the INVITE message there. Then the normal SIP signaling procedure is performed to establish the session. If the MN accesses a new network and obtains a new IP address via DHCP while the session is ongoing, it will send a RE-INVITE message with an updated session description. This maintains the same Call-ID of the existing session but replaces the Contact field of the SIP header with the new IP address to inform the CN where it wants to receive future SIP messages, as well as replaces the c field of Session Description Protocol (SDP) [77] header with the new IP address to redirect the packets to its new location. After receiving the RE-INVITE message, if the CN runs a session over UDP, it will send packets directly to the MN's new IP address. However, if the CN runs a session over TCP, it shall send packets to the MN by a tunneling technique [74]. When the MN receives the encapsulated packets, it in turn removes them from IP encapsulation. Similarly, the MN also tunnels packets to the CN. Finally, the MN sends a REGISTER message to the home SIP server to update the location information stored there, so that the new call can be correctly redirected. Figure 2.2.10 illustrates the SIP mobility and its operations.

Generally, the handover procedure using SIP may introduce handover latency for signaling messages procedure and overhead for IP encapsulation [71], [78]. To improve SIP mobility performances, Dutta [78] optimizes

SIP mobility management by using the intra-domain solution, which limits the movement indication to within the domain to reduce handover latency and minimize packet loss. Kim et al. [73] proposes a mechanism of Predictive Address Reservation with SIP (PAR-SIP), which reduces handover latency by proactively processing the address allocation and session update using link layer information of wireless networks.

Figure 2.2.10: MSCTP Mobility and its Operations



1. SIP INVITE
2. SIP 302 moved temporarily
3. SIP INVITE
4. SIP OK
5. DATA
6. MOVE
7. SIP REGISTER
8. SIP OK
9. SIP INVITE
10. IP OK
11. DATA

Security Considerations: In SIP, there is support for both authentication and encryption of SIP messages, using either challenge-response or private/public key cryptography.

2.2.3.4.2. DDNS

As mentioned in Section 2.2.2, traditional DNS is restricted in the mobile Internet. To resolve the problem, Vixie et al. [24] propose a method for dynamically updating RRs or RRsets from a specified zone by specifying the UPDATE messages. Because most applications ubiquitously resolve FQDN to an IP address at the beginning of communication, DDNS can be considered for the location management in the mobile environment where the MN acts as a server and other nodes actively originate communication with the MN.

To locate the MN as it moves to a new network, the MN dynamically registers and updates its FQDN-to-IP entry with the new IP address to DNS servers by sending DNS UPDATE messages. Then whenever the CN wants to communicate with the MN, it will query the DNS sever with the FQDN of the MN, and the DNS sever responds with the current IP address of the MN. Finally, the CN can initiate and establish communication with the MN directly. Figure 2.2.11 illustrates the location management of DDNS in the mobile Internet.

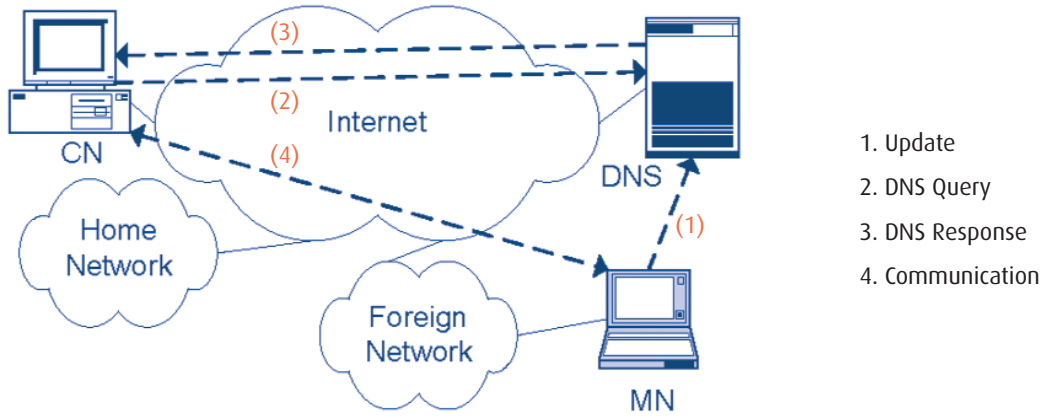
Security Considerations: The dynamic UPDATE messages are based on authenticated requests [79] and transactions are used to provide authorization by Secret Key Transaction Authentication for DNS (TSIG) [80] or DNS Request and Transaction Signatures (SIG(0)) [81], [82]. Only authorized sources are allowed to make changes to a zone's contents.

2.2.3.4.3. MOBIKE

The Internet Key Exchange version 2 (IKEv2) [83] signaling protocol is part of IPsec. In IPsec, the IKE Security Association (SA) and IPsec SA are established between the IP address pair and maintained by IKEv2. The IP address pair is tied to the IKE SA and IPsec SA. Therefore, in the mobile environment, when devices move and IP addresses change during IPsec communication, the existing IKE SA and IPsec SA become invalid and

have to be rekeyed. Rekeying the SAs for user interaction and the authentication process often occurs too slowly [26]. To deal with these mobility challenges, IKEv2 is being extended by the MOBIKE working group of the IETF for mobility extension called MOBIKE, which aims to keep the established IKE SA and IPsec SA alive throughout a session so that there is no need to rerun the initial IKEv2 exchange. In this sense MOBIKE can also be regarded as a network layer solution, although it operates based on a procedure located in the higher layer. MOBIKE provides mechanisms to detect dead peer for connectivity check, and updates the IP address stored with IKE SA and IPsec SA by specifying message exchange of the IP address update notification.

Figure 2.2.11: DDNS Location Management



In MOBIKE, multihoming support is integrated by allowing a peer address set to be stored in IKE SA during initial IKEv2 exchange. In addition, MOBIKE uses Vendor ID Payload or Notify payload during initial IKEv2 exchange to signal the support for MOBIKE. This ensures that a MOBIKE capable node knows whether its peer supports MOBIKE or not. When the MN moves to another network, MOBIKE uses the IKEv2 Dead Peer Detection (DPD) mechanism for connectivity test between address pairs. Once the MN detects dead address/path, it then sends an authenticated address update notification with a different preferred address. Changing the preferred address also has an impact for IPsec SAs. To allow the IPsec protected data traffic to travel along the same path as the MOBIKE packets, the outer tunnel header addresses ought to be modified according to the preferred address pair. MOBIKE suggests two ways by which the IPsec SAs are changed to use the new address pair. One is that when the IKE SA address is changed, it automatically moves all IPsec SAs associated with it to the new address pair. Another option is to have separate exchange to move the IPsec SAs separately.

Security Considerations: In MOBIKE, all the messages are already authenticated by the IKEv2, so there is no problem that any attackers would modify the actual contents of the packets. However, the IP addresses in the IP header of the packets are not authenticated, thus raising the vulnerability to remote redirection.

2.2.3.4.4. Analysis of Application Layer Mobility

SIP provides Internet mobility support without any modifications of lower layer protocols, which are then easily deployed. Because it functions independently of IP addresses, this makes SIP appropriate for use with a heterogeneous network. Nonetheless, it is adverse to real time applications since considerable handover latency and overload occur with certain procedures, such as the acquisition of DHCP IP address renewal, location registration, and the transmission of the RE-INVITE message from the MN to the CN. In addition, overload also occurs through the IP encapsulation of TCP connections.

DDNS utilizes existing DNS for location management, which does not require special servers, such as MIP. However, The DNS registration delay needs to be optimized. In addition, as DDNS cannot maintain ongoing communication within the mobile Internet, it is used for location management along with other solutions as a candidate approaches.

With MOBIKE, when an IP address changes due to mobility, the IP source and destination address obtained via the configuration payloads within IKEv2 and used inside the IPsec tunnel remains unaffected, i.e., applications do not detect any change at all. However, MOBIKE cannot deal with the rendezvous problem, in which both peers move and obtain the new IP address at the same time without being able to communicate this to one another.

2.2.4. COMPARISON OF DIFFERENT PARADIGMS FOR INTERNET MOBILITY SUPPORT

In this section we will qualitatively evaluate the mobility solutions on the layer category level summarized above from three aspects of functional requirements, performance metrics, and required changes of existing systems. We would like to emphasize that the comparison is not complete for solutions in question but the main issues are discussed according to comparative approaches.

2.2.4.1. Functional Aspects

Firstly, we summarize and compare the mobility support solutions based on requirements for handover management, location management, multihoming, applications and security. Table 2.2.1 summarizes how the requirements are supported by the solutions presented above. From the table, we can conclude that none of these solutions fulfill all requirements. Network layer does not yet support multihoming. The new layer solution of HIP must define a new API for the HI, which requires modification of current applications. The Transport layer by itself can not track a node, so it is short of the location management function. They depend on other layers for location management such as DDNS, MIP etc. Application layer solutions are only appropriate for specific applications, such as SIP for real time multimedia, DDNS for location management and MOBIKE for higher layer protocols and applications using IPsec. For the security issue, most paradigms (except M-UDP) address it to some degree. Some paradigms like MIP and MOBIKE etc. specified some potential threats, however the security considerations of some paradigms are still primitive. For example, in the transport layer, the MSCTP suggested using IPsec or TLS to prevent attack of hijacking, but similar to most paradigms developed so far, it does not specify the security mechanism in detail. DCCP selects the value of Mobility ID feature randomly to protect against attacker, which is not secure enough in fact because it does not specify how to guarantee the randomicity of the value of Mobility ID feature. Moreover, DCCP also does not provide cryptographic security guarantees.

2.2.4.2. Performance Aspects

With the above functional comparison it is easy to derive qualitatively the performance of different layer solutions based on metrics of handover latency, packet loss, signaling overhead and throughput. The handover mechanism of network layer suffers from large handover latency and considerable packet loss caused by proxy and no support of multihoming, although many techniques such as make-before-break or anticipated

Table 2.2.1: **FUNCTIONS OF PROPOSED PARADIGMS: A COMPARISON**

Category	Network	layer		Transport	layer		A new	layer		Application	layer
	MIP	LIN6	TCP	UDP	SCTP	DCCP	HIP	MAST	SIP	DDNS	MOBIKE
Handover	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Location	✔	✔					✔	✔	✔	✔	
Multihoming					✔	✔	✔	✔	✔		✔
Applications	✔	✔	✔	✔	✔	✔				✔	
Security	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔

handovers [84] have been developed to address the problems. Advantages to transport layer mobility include inherent route optimization, no dependence on the third device, and multihoming support etc. which make seamless handover and minimization of packet loss possible with the ability to pause transmissions in expectation of a mobility-induced temporary disconnection. The new layer like HIP employs RVS/DNS for location management, which might take quite some time to query and update a node's current IP address by which time it may result in handover latency and packet loss. In the application layer, the resigning of an entire zone of DDNS whenever the IP addresses of one entry changes, places a high cost to globally converge the DNS server which also impacts on the handover latency and packet loss.

A mobility solution in the network layer also involves signaling overhead problems caused by tunneling and extension headers etc. The transport layer solution seems to alleviate the problem because they manage mobility by negotiating and switching connections directly between endpoints. In the new layer, the updates of the MN's interface status must be signaled to the CN like HIP using REA etc. Similarly, the solutions of the application layer also suffer from signaling overhead for IP address updating or redirecting etc.

Besides, considering the impact of throughput in the mobile environment, transport layer mobility improves the performance of throughput effectively by implementing policies that reset congestion control after reattachment. Other layers' solutions by themselves can not guarantee that the efficiency of transport connections is maintained and can not handle the degradation of throughput caused by congestion control.

Table 2.2.2: **REQUIRED CHANGES TO EXISTING SYSTEMS: A COMPARISON**

Category	Network	layer		Transport	layer		A new	layer		Application	layer
	MIP	LIN6	TCP	UDP	SCTP	DCCP	HIP	MAST	SIP	DDNS	MOBIKE
Host	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Routers	✔	✔					✔	✔	✔	✔	
Third device					✔	✔	✔	✔	✔		✔
TCP/IP layering	✔	✔	✔	✔	✔	✔				✔	

2.2.4.3. Required Changes to Existing Systems

In order to maintain backward compatibility, the network and protocol infrastructure concern is another important factor in deployment including required changes to endpoint, intermediate router and addition of third entities such as proxy, agents etc., for network infrastructure, as well as change to protocol infrastructure.

Table 2.2.2 illustrates the required changes comparison for different solutions. Network layer solutions are based on routing mechanism, so they require changes to the endpoint and router for address binding. In addition, they need a third device of agents for packet forwarding and location management. Because transport layer solutions are based on the end to end model, they require no change to intermediate routers. And they are absent from location management by themselves, so there is not deployment of a third device. Therefore, the transport layer solutions require very little infrastructure change. New layer solutions need modification to the endpoint. And it employs RVS/DNS for location management, so they also need the addition of a third device. In addition, the introduction of new protocol layer also destroys the traditional TCP/IP infrastructure. Similarly, the application solution of SIP employs proxy server to relay flows and redirect server to locate the MN, it needs to add a third device and change to the endpoint.

2.2.5. CONCLUSION

In this paper, we analyzed the problems of the traditional TCP/IP stack caused by the mobility of nodes and their wireless links, illustrated many layers of the TCP/IP stack that have a negative effect on the Internet mobility issue. And we presented a survey of different mobility support paradigms for the Internet. From our comparisons and the discussion of the advantages and disadvantages of each paradigm, we concluded that current mobility solutions do not solve all general problems related to Internet mobility and it is hard to dictate which one is most suitable: individual layer contributes to Internet mobility; while the technology is important, the market will decide. Link layer mobility support is fundamental in a mobile Internet, but it constrains within a limited domain and can not preserve higher layer connections. Although the network layer solutions can handle most of requirements, it has slow deployment in practice as it is ineffective and complex. Transport layer solutions can fulfill handover management efficiently, but they lack the ability of location management by themselves. New layer solutions violate the traditional TCP/IP structure which has been deployed widely in reality, so it is difficult to deploy or modify the current infrastructure of the Internet. Application layer approaches are on the other hand restricted in specific applications.

To provide an effective solution with the issues of basic functional requirements, performance requirements and deployment for Internet mobility support in mind, we conclude with the features that need to be satisfied in the mobile Internet:

1) Can efficiently deal with handover. For example, using anticipating technique of radio trigger etc. to detect handover and perform routing/path update and location registration process in advance.

2) Can handle various mobile scenarios of the endpoints, including client-server scenario where the MN only originates the sessions and the point-to-point scenario where the sessions may be originated at either one endpoint of communicating peers, by enhance location management such as DDNS etc.

3) Provide end-to-end mobility and avoid third party entities or tunneling mechanisms which invoke the complexity and reduce the performance of mobility.

4) Take advantage of multihoming, which can make for seamless handover and improving performance of mobility with its redundancy and load share etc. features simultaneously.

5) Avoid erroneously triggering congestion control mechanisms - which could arise from handover of mobility, the wireless link characteristics (e.g., lossy and bursty high BER) and communication path change - in the transport layer, e.g., by extending TCP mobility support feature like LMDR TCP option and enhancing signaling mechanism between transport layer and other layers such as link layer, network layer etc.

6) Preferably provide compatibility (and thus allowing easier market adoption). That is, the solution does not require a change or impact in applications, network architecture, TCP/IP structure, or add additional entities.

7) Take account of security aspect in mobile environments.

The efficient Internet mobility management is a more challenging issue. In order to satisfy these features recommended above, it needs all the layers' participation in a highly cooperative way. Therefore, we anticipate a multi-layer architecture for advanced mobility support and we suggest the transport layer as the main candidate assisted with other layers together for Internet mobility support.

2.2.6. ACKNOWLEDGMENTS

The authors would like to thank Wesley Eddy, Hannes Tschofenig and Antonio Skarmeta for their insightful comments. In addition, anonymous reviewers, as well as Martin Reisslein, Editor-of-Chief of IEEE Communication Surveys and Tutorials, provided constructive suggestions for improvements and clarifications of the paper.

2.2.7. REFERENCES

[1] T.R. Henderson, "Host mobility for IP networks: a comparison", IEEE Network, Nov. 2003, pp. 18-26.

[2] W.M. Eddy, "At what layer does mobility belong?", IEEE Communications Magazine, Oct. 2004, pp. 155-159.

[3] INFOCOM 2005 Mobility Panel "How does mobility fit into the Internet layering scheme?", Mar. 2005. [Online]. Available: http://roland.grc.nasa.gov/~weddy/papers/mobility-panel.html

[4] P. Karn, C. Bormann, G. Fairhurst, et al., "Advice for Internet Subnetwork Designers", RFC 3819, July 2004.

[5] K. Kuladinithi, A. Konsgen, S. Aust, et al., "Mobility management for an integrated network platform", Proc. IEEE MWCN 2002, pp. 621-625.

[6] M. Allman, V. Paxson, and W. Stevens, "TCP Congestion Control", RFC 2581, Apr. 1999.

[7] H. Elaarag, "Improving TCP performance over mobile networks", ACM Computing Surveys, Sep. 2002, pp. 357-374.

[8] Y. Swami, K. Le, and W. Eddy, "Lightweight Mobility Detection and Response (LMDR) Algorithm for TCP", Internet draft (work in progress), draft-swami-tcp-lmdr-06, Aug. 2005.

[9] C. Perkins. "IP Mobility Support for IPv4", RFC 3344, Aug. 2002.

[10] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[11] F. Teraoka, M. Ishiyama, and M. Kunishi, "LIN6: A Solution to Multihoming and Mobility in IPv6", Internet draft (work in progress), draft-teraoka-multi6-lin6-00, Dec. 2003.

[12] A. Bakre and B. R. Badrinath, "I-TCP: Indirect TCP for Mobile Hosts", Proc. of ICDCS'05, Vancouver, Canada, June 1995, pp. 136-143.

[13] R. Yavatkar and N. Bhagawat, "Improving End-to-End Performance of TCP over Mobile Internetworks", Proc. of IEEE WMCSA'94, Santa Cruz, CA, 1994.

[14] R. Caceres and L. Iftode, "Improving the performance of reliable transport protocols in mobile computing environments", IEEE Journal on Selected Areas in Communications, 1995, pp. 850-857.

[15] Z.J. Haas, "Mobile-TCP: An Asymmetric Transport Protocol Design for Mobile Systems", IEEE ICC'97, Montreal, Canada, 1997.

[16] D. Funato, K. Yasuda, and H. Tokuda. "TCP-R: TCP mobility support for continuous operation", Proc. ICNP 1997, pp. 229-236.

[17] A. C. Snoeren and H. Balakrishnan, "An End-to-End Approach to Host Mobility", MOBICOM 2000.

[18] D.A. Maltz and P. Bhagwat, "MSOCKS: An Architecture for Transport Layer Mobility", INFOCOM 1998.

[19] K. Brown and S. Singh, "M-UDP: UDP for Mobile Networks", ACM SIGCOMM Computer Communications Review, pp. 60-78, Oct. 1996.

[20] K. Brown and S. Singh, "A Network Architecture for Mobile Computing", INFOCOM 1996.

[21] R. Stewart, Q. Xie, and K. Morneault, "Stream Control Transmission Protocol", RFC 2960, Oct. 2000.

[22] E. Kohler, "Datagram Congestion Control Protocol Mobility and Multihoming", Internet draft (work in progress), draft-kohler-dccp-mobility-00, July 2004.

[23] J. Rosenberg, H. Schulzrinne, G. Gamarillo, et al., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[24] P. Vixie, S. Thomson, Y. Rekhter, et al., "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, Apr. 1997.

[25] T. Kivinen and H. Tschofenig, "Design of the MOBIKE Protocol", Internet draft (work in progress), draft-ietf-mobike-design-04, Oct 2005.

[26] P. Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", Internet draft (work in progress), draft-ietf-mobike-protocol-04, Oct 2005.

[27] R. Moskowitz and P. Nikander, "Host Identity Protocol Architecture", Internet draft (work in progress), draft-ietf-hip-arch-03, Aug. 2004.

[28] T. Henderson, "End-Host Mobility and Multihoming with the Host Identity Protocol", Internet draft (work in progress), draft-ietf-hip-mm-02, July 2005.

[29] D. Crocker, "Multiple Address Service for Transport (MAST): an Extended Proposal", Internet draft (work in progress), draft-crockermast-proposal-01, Sep. 2003.

[30] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP Regional Registration", Internet draft (work in progress), draft-ietf-mip4-reg-tunnel-00, Nov. 2004.

[31] K. Malki, "Low Latency Handoffs in Mobile IPv4", Internet draft (work in progress), draft-ietf-mobileip-lowlatency-handoffs-v4-11, Oct 2005.

[32] R. Ramjee, T. La Porta, S. Thuel, et al., "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks", ICNP 1999.

[33] A. Valko, "Cellular IP: A New Approach to Internet Host Mobility", ACM SIGCOMM Computer Communication Review, Jan. 1999, pp. 50-65.

[34] H. Soliman, C. Castelluccia, K. El-Malki, L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", RFC 4140, Aug. 2005.

[35] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[36] H.Y. Jung, S.J. Koh, H. Soliman, et al., "Fast Handover for Hierarchical MIPv6 (F-HMIPv6)", Internet draft (work in progress), draft-jung mobileip-fastho-hmipv6-04, June 2004.

[37] C. Perkins, "IP Encapsulation within IP", RFC 2003, Oct. 1996.

[38] B. Aboba, "IAB Considerations for the Split of Identifiers and Locators", Internet draft (work in progress), draft-iab-id-locsplit-00, Mar. 2004.

[39] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, Mar. 1997.

[40] D. Plummer, "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, Nov. 1982.

[41] J. Postel, "Multi-LAN Address Resolution", RFC 925, Oct. 1984.

[42] D.B. Johnson and C. Perkins, "Route Optimization in Mobile IP", Internet draft (work in progress), draft-ietf-mobileip-optim-11, Sep. 2001.

[43] J. Kempf, "Dormant Mode Host Alerting ('IP Paging') Problem Statement", RFC 3132, June 2001.

[44] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, Feb. 1997.

[45] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, Apr. 1992.

[46] S. Deering and R. Hinden, "Internet Protocol, Version 6(IPv6) Specification", RFC 2460, Dec. 1998.

[47] R. Droms, J. Bound, B. Volz, et al., "IPv6 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[48] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Dec. 1998.

[49] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Nov. 1998.

[50] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, Nov. 1998.

[51] S. Kent and R. Atkinson, "IP Authentication Header"; RFC 2402, Nov. 1998.

[52] H. Zhu, F. Bao, and R.H. Deng, "Securing return routability protocol against active attack", VTC 2004-Fall, Los Angles, California, Sep. 2004.

[53] F. Zhao, J. Zhou, and S. Jung, "Improvement on Security and Performance of MIP6 Return Routability Test", Internet draft (work in progress), draft-zhao-mobopts-rr-ext-00, July 2005.

[54] F. Dupont and J-M. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes", Internet draft (work in progress), draft-ietfmip6-cn-ipsec-01, June 2005.

[55] F. Le, S. Faccin, B. Patil, and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem statement", Internet draft (work in progress), draftietf-mip6-firewalls-03, Oct 2005.

[56] X. Fu, H. Tschofenig, S. Thiruvengadam, and W. Yao, "Enabling Mobile IPv6 in Operational Environments", Proceedings of the 10th IFIP International Conference on Personal Wireless Communications (PWC 2005), Colmar, France, Aug. 2005.

[57] G. Giaretta, J. Kempf and V. Devarapalli, "Mobile IPv6 bootstrapping in split scenario", Internet draft (work in progress), draft-ietf-mip6-bootstrapping-split-01, Oct 2005.

[58] W. Haddade and S. Krishnan, "Combining Cryptographically Generated Address and Crypto-Based Identifiers to Secure HMIPv6", Internet draft (work in progress), draft-haddad-mipshop-hmipv6-security-00, Oct 2005.

[59] M. Leech, M. Ganis, Y. Lee, et al., "SOCKS protocol version 5", RFC 1928, Apr. 1996.

[60] S. Jaiswal and S. Nandi, "Simulation-based performance comparison of TCP-variants over Mobile IPv6-based mobility management schemes", 29th Annual IEEE International Conference on Local Computer Networks, Nov. 2004, pp. 284-291.

[61] R. Stewart, M. Ramalho, et al., "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", Internet draft (work in progress), draft-ietf-tsvwg-addip-sctp-12, June 2005.

[62] M. Riegel and M. Tuexen, "Mobile SCTP", Internet draft (work in progress), draft-riegel-tuexen-mobile-sctp-05, July 2005.

[63] T. Dierks and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, Jan. 1999.

[64] A. Jungmaier, E. Rescorla, and M. Tuexen, "Transport Layer Security over Stream Control Transmission Protocol", RFC 3436, Dec. 2002.

[65] D. Eastlake, S. Crocker, and J. Schiller, "Randomness Recommendations for Security", RFC 1750, Dec. 1994.

[66] S.J. Koh and Q. Xie, "Mobile SCTP with Mobile IP for Transport Layer Mobility", Internet draft (work in progress), draft-sjkoh-mobilesctp-mobileip-04, June 2004.

[67] P. Nikander, J. Ylitalo, and J. Wall, "Integrating Security, Mobility, and Multihoming in a HIP Way", Proc. NDSS'03, San Diego, CA, Feb. 2003, pp. 87-99.

[68] A. Gulbrandsen, P. Vixie, and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, Feb. 2000.

[69] P. Saint-Andre and J. Miller, "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 3920, Oct. 2004.

[70] J. Arkko and P. Nikander, "Weak Authentication: How to Authenticate Unknown Principals without Trusted Parties", Proc. of Security Protocols Workshop 2002, Cambridge, UK, Apr. 2002, pp. 5-19.

[71] E. Wedlund and H. Schulzrinne, "Mobility Support using SIP", Proc. of the 2nd ACM International Workshop on Wireless Mobile Multimedia, Aug. 1999, pp.76-82.

[72] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session Initiation Protocol (SIP) Session Mobility", Internet draft (work in progress), draft-shacham-sipping-session-mobility-01, July 2005.

[73] W. Kim, M. Kim, K. Lee, C. Yu, and B. L. Link. "Layer Assisted Mobility Support Using SIP for Real-time Multimedia Communications", ACM MobiWac 2004.

[74] F. Vakil, A. Dutta, and J-C. Chen et al., "Supporting Mobility for TCP with SIP", Internet draft (work in progress), draft-itsumo-sippingmobility-tcp-00, June 2001.

[75] F. Vakil, A. Dutta, and J-C. Chen, "Supporting Mobility for Multimedia with SIP", Internet draft (work in progress), draft-itsumo-sippingmobility-multimedia-01, July 2001.

[76] N. Banerjee, S.K. Das, and A. Acharya, "SIP-Based Mobility Architectgure for Next Generation Wireless Networks", Proc. of IEEE International Conference of Pervasive Computing and Communications (PerCom 2005), pp. 181-190, Mar. 2005.

[77] M. Handley and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, Apr. 1998.

[78] A. Dutta, et al., "Implementing a Testbed for Mobile Multimedia", Proc. GLOBECOM 2001, pp.25-29.

[79] B. Wellington, "Secure Domain Name System (DNS) Dynamic", RFC 3007, Nov. 2000.

[80] P. Vixie, O. Gudmundsson, and D. Eastlake et al., "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[81] D. Eastlake, "DNS Request and Transaction Signatures (SIG(0)s)", RFC 2931, Sep. 2000.

[82] D. Eastlake, "Domain Name System Security Extensions", RFC 2535, Mar. 1999.

[83] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", Internet draft (work in progress), draft-ietf-IPsec-ikev2-17, Sep. 2004.

[84] R. Bless, M. Zitterbart, J. Hillebrand, and C. Prehofer, "Quality of Service Signaling in Wireless IP-based Mobile Networks", VTC 2003-Fall, Orlando, FL, Oct 2003.

2.3 GSABA: A Generic Service Authorization Architecture

Florian Kohlmayer, Hannes Tschofenig, Rainer Falk
Corporate Technology, Siemens AG

Rafael Marín López, Santiago Zapata Hernández,
Pedro García Segura, Antonio F. Gómez Skarmeta
University of Murcia

ABSTRACT

Bootstrapping refers to the process of creating state (typically security associations, configuration and authorisation information) between two or more entities based on a trust relationship between a trusted third party and two or more entities. The term bootstrapping has been recently introduced to denote solutions to configuration problems, such as those present in Mobile IP. This paper describes a novel service authorisation and bootstrapping architecture in order to distribute keying material, to perform authorisation and to make configuration information available.

Categories and Subject Descriptors

C.2.0 *[**Computer-Communications Networks**]:* Security and Protection.

General Terms

Security, Management, Design.

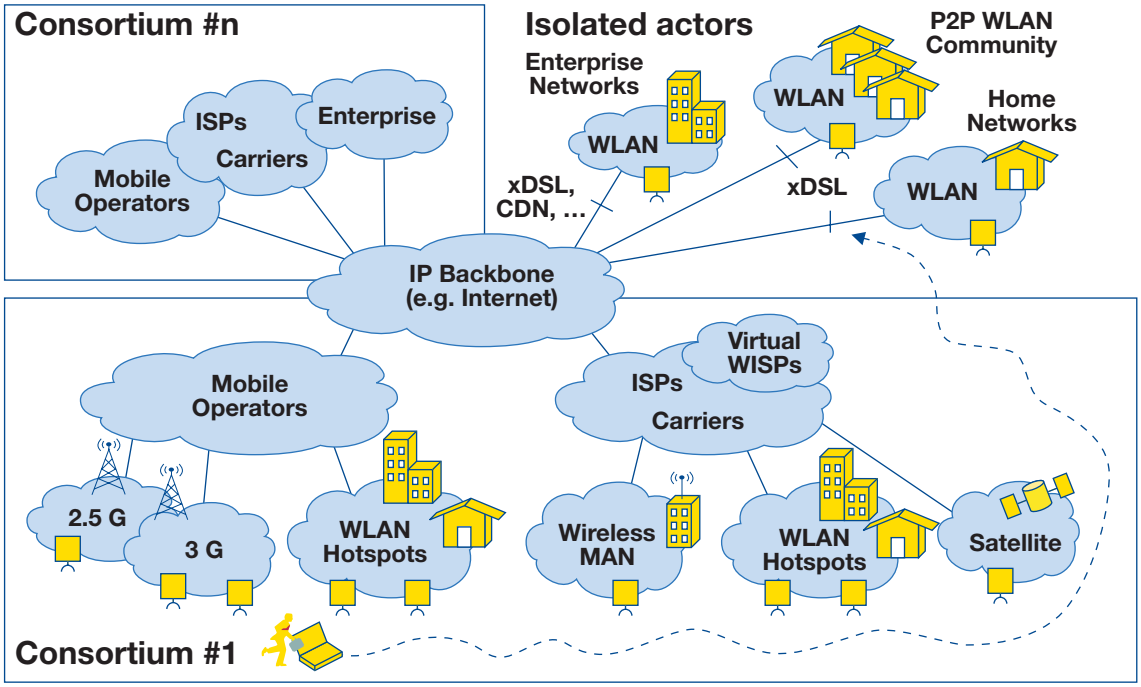
Keywords

Mobile IP, Security, AAA, Service authorisation, Enable.

2.3.1. INTRODUCTION

Future mobile networks will integrate multiple access technologies and various entities providing network access. The user will have different technology options to access the Internet while mobile. In the future market there will be ISPs (fixed and mobile), in some cases joined in consortiums, which will co-exist with much smaller and often unmanaged entities (e.g., private or home WLANs), see Figure 2.3.1.

Figure 2.3.1: The ENABLE "Universe"



The EU-funded project ENABLE (Enabling Efficient and Operational Mobility in Large Scale Heterogeneous IPv6 Networks) aims to enable efficient and operational mobility in large heterogeneous IP networks [1]. This also comprises the enrichment of the basic mobility service provided by Mobile IPv6 with a set of additional features, enabling the on-demand activation and auto-configuration of specific "premium" network features (e.g., multi-homing, fast handovers) based on the operator policies and customers profiles. The number of protocols executed between the end host and the network has grown continually and will continue to grow in the previously described future mobile network vision. In addition to the network access authentication and DHC protocols these are for example mobility, Quality of Service, NAT/Firewall, Network Discovery and Selection (e.g., Media Independent Handover protocols) and various application layer protocols (e.g., SIP).

Classically, network access authentication procedures provide strong, inter-domain security mechanisms that allow roaming users to establish a security context between the end host and some node in the access network (e.g., with the access point where the end host is attached). The protocols that are executed after the network access authentication procedure also need a security context since the end points are different. Furthermore, a different authorisation decision might be necessary for different protocols. Consider, for example, an end host that interacts with a streaming server to download a video. This streaming server might be located in the access network and an additional authorisation step from the user's home domain might be required in order to ensure that the user is authorised to obtain the video and to start credit control and accounting.

Since network providers do not want to end as a bit-pipe they are very interested in introducing additional services in their network. With an increased service deployment, the pressure for a faster time-to-market and the need to reduce operational expenses prevents operators from making static configurations at network

entities per service for individual end hosts. Even worse, static configuration at end hosts increases deployment costs considerably and leads to slower innovation. Hence, the goal is to develop a mechanism to dynamically and securely provide the end host with the necessary information for service access based on some long-term credential. Using the long-term credential, which is typically a shared secret, password or a X.509 certificate, it should be possible for a client to carry out a process that distributes necessary information for service access. This procedure typically creates a state between client and service based on a trust relationship between these two parties and a trusted third party that controls and manages the service. We call this process bootstrapping.

The challenge with bootstrapping is twofold. Firstly, there is a key distribution problem to ensure secure service access (i.e., creating a security association between client and service). Secondly, the authorisation problem must be solved since it plays an important role in real world deployments. That is, even when client possesses credentials, it is necessary to verify whether the client is authorised for service access.

As an example, let us consider Mobile IPv6 as a service. In order to use Mobile IPv6 it is necessary for the mobile node (MN) to share a pre-shared key with the Home Agent (HA) to setup an IPsec Security Association as one deployment option. This is necessary to protect Mobile IPv6 signaling messages. Possessing the shared secret does not imply that the MN is authorized to access the Mobile IPv6 service. The MIP6 WG has produced a problem statement [2] document that describes the particularities of the bootstrapping problem in the context of Mobile IPv6. In addition to the previously mentioned key distribution problem, the Mobile Node (MN) needs to be provisioned with a set of parameters. The bootstrapping process allows the MN to obtain enough information so that the mobile node can successfully register with a dedicated HA. Specifically, this means obtaining the home agent address and the home address, and for the MN and the HA to share a secret. The references [3] and [4] describe solutions to bootstrap Mobile IP in the integrated and the split scenario. These two scenarios are differentiated by the fact that the mobility service and the network access service are authorised by the same operator (integrated scenario) or not (split scenario).

Other examples can be found with DHCP RFC 3118 [5] security association bootstrapping using EAP/PANA in [6] and in [7]. A proposal to bootstrap a Kerberos Ticket Granting Ticket based on a successful EAP protocol exchange is provided in [8]. Additionally, two further contributions [9] and [10] were published that aim to reuse EAP/PANA for the purpose of MIPv6 bootstrapping information.

Besides the IETF, other standardisation bodies are currently investigating bootstrapping solutions, for example the 3GPP with their Generic Bootstrapping Architecture (GBA) [13].

The on-going work related with future mobile network architecture in the ENABLE project have led to the design of a new generic service authorisation architecture to enable the different services envisioned within ENABLE project. Bootstrapping is useful for mobility services, which represents the core of the ENABLE project, but also for other services supporting or benefiting from a mobility architecture.

This paper proposes a generic service authorisation architecture that is able to bootstrap mobility, network and application layer services independently of their functionality. In Section 2.3.2 the architecture and its components are described, Section 2.3.3 provides details including message flows. Section 2.3.4 illustrates an example. Finally, Section 2.3.5 provides a conclusion and hints to future work.

2.3.2. SERVICE AUTHORISATION ARCHITECTURE

The proposed architecture is composed of a set of basic entities. These entities or components provide specific functions and they can be instantiated in a variety of ways providing a flexible deployment.

2.3.2.1. Overview

In this section we point to two logical entities, namely the Bootstrapping Configuration Agent (BCA) and the Bootstrapping Authorisation Agent (BAA). These two entities can be co-located on the same physical box or distributed. The BCA is responsible for providing necessary bootstrapping information to the mobile node (MN). For example, with Fast Mobile IP (FMIP) [18] the home address, the HA address and the new access router address is provided; with Hierarchical Mobile IP (HMIP) [17] the Mobility Anchor Point (MAP) address and a regional Care-of Address (RCoA) is configured. The BAA is responsible for asserting authorisation statements. The decisions for the statements are based on the mobile node's profile, which is available in the authorising domain. The statements and the parameters need to be conveyed to the MN. Additionally, the BCA must be able to authenticate the MN and the bootstrapping target (BT). The BT is also known as the 'service providing' entity, i.e., the entity that offers the requested service (e.g., the HA). Note that the service may be provided by a single BT or on the contrary, multiple BTs may be involved in service provision. Examples are HMIP where the service is mobility and the BTs are the ARs, MAPs and HAs. In case of FMIP the BTs are ARs. Another required architectural element in the roaming scenario is the BAA proxy, which is responsible for forwarding and maybe modifying the policies asserted from the BAA.

Figure 2.3.2: Stationary Architecture

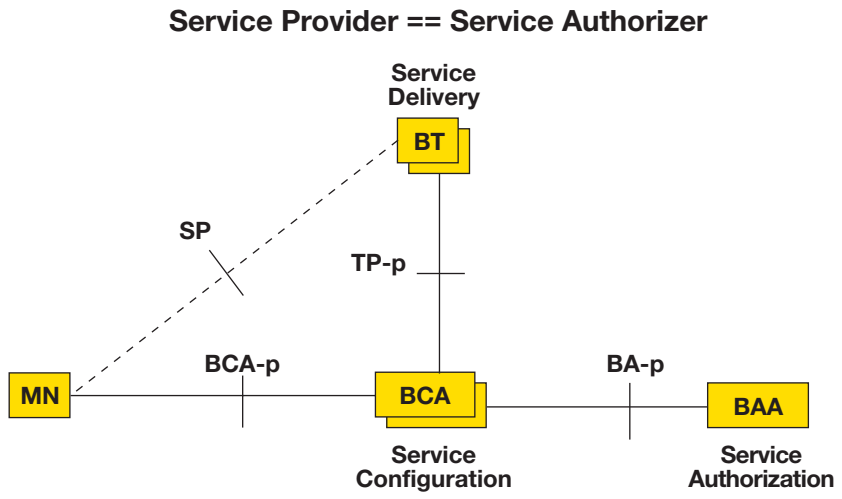
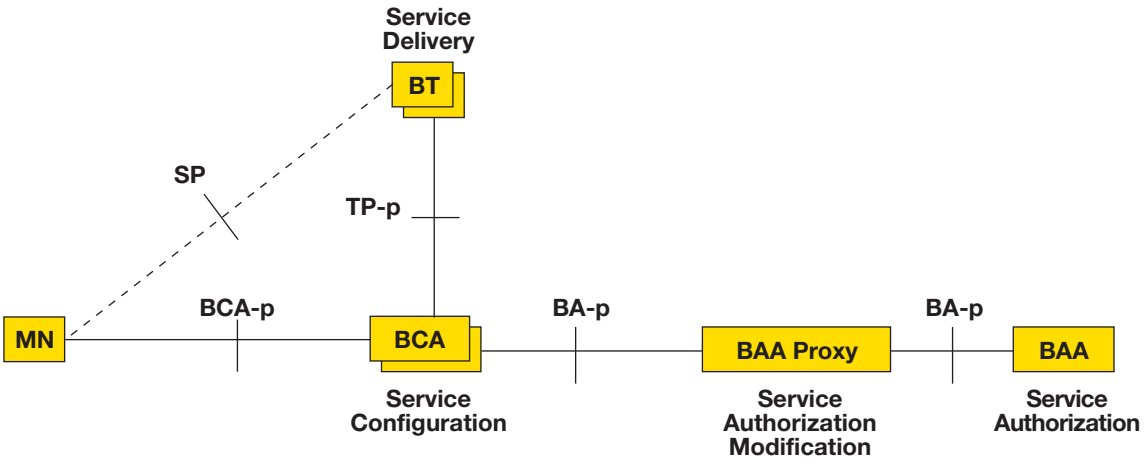


Figure 2.3.2 depicts the architecture in the stationary case by showing the placement of the various entities in the simplest deployment case. That is, when the BT, the BCA, the BAA and the MN are located in the same administrative domain (intra-domain case). In a roaming scenario, depicted in Figure 2.3.3, the entities are arranged in a different fashion: the domain boundary may be located, for example, between the BAA proxy and the BAA or between the BT and the BCA.

Figure 2.3.3: Roaming Architecture



Four main interfaces are depicted in Figure 2.3.3:

- **The bootstrapping target protocol (TP-p):** This protocol runs between the BT and the BCA. The purpose is to exchange service related information and to authorise the BT to provide service to the mobile node. The information could be encoded either in Attribute Value Pairs (AVPs) [15] or in XML.
- **The bootstrapping protocol (BCA-p):** This protocol runs between the MN and the BCA. The purpose of this protocol is to convey bootstrapping information to the MN and to inform the MN of the authorisation decision taken by the BAA and the BAA proxy. The information could be encoded either in AVPs or in XML. Candidate transport protocols are EAP/PANA, DHCP, SIP, HTTP or SOAP (over HTTP).
- **The bootstrapping agent protocol (BA-p):** This protocol runs between the BAA proxy and the BAA. If the BCA and the BAA (proxy) are not co-located then the BA-p is also used between the BCA and the BAA (proxy). The purpose of this interface is to allow information exchange needed for the BAA entities to base the decision on and to deliver these decisions to the BCA. The information could be encoded either in AVPs or in XML.
- **The service related protocol (SP):** This protocol runs between the MN and the BT. Ideally, this service specific protocol should be left largely unmodified. This interface is therefore indicated in the figure as a dashed line.

2.3.2.2. Integration in AAA Infrastructure: GSABA.

Today, most Telecommunication Operators and Internet Service Providers make use of the Authentication, Authorisation and Accounting (AAA) infrastructure for their services [14]. To support roaming AAA broker services have been deployed to accomplish peering of various providers. These peering agreements represent business relationships and have an impact on the routing of the AAA messages. To leverage the existing infrastructure and to reduce the deployment cost, we show how to integrate our Generic Service Authorisation architecture with an underlying AAA infrastructure. This section presents the mapping of the logical functions presented before to the AAA infrastructure. This mapping is intended for the real deployment of our proposed architecture.

Figure 2.3.4: Instantiation of GSABA in the AAA Architecture

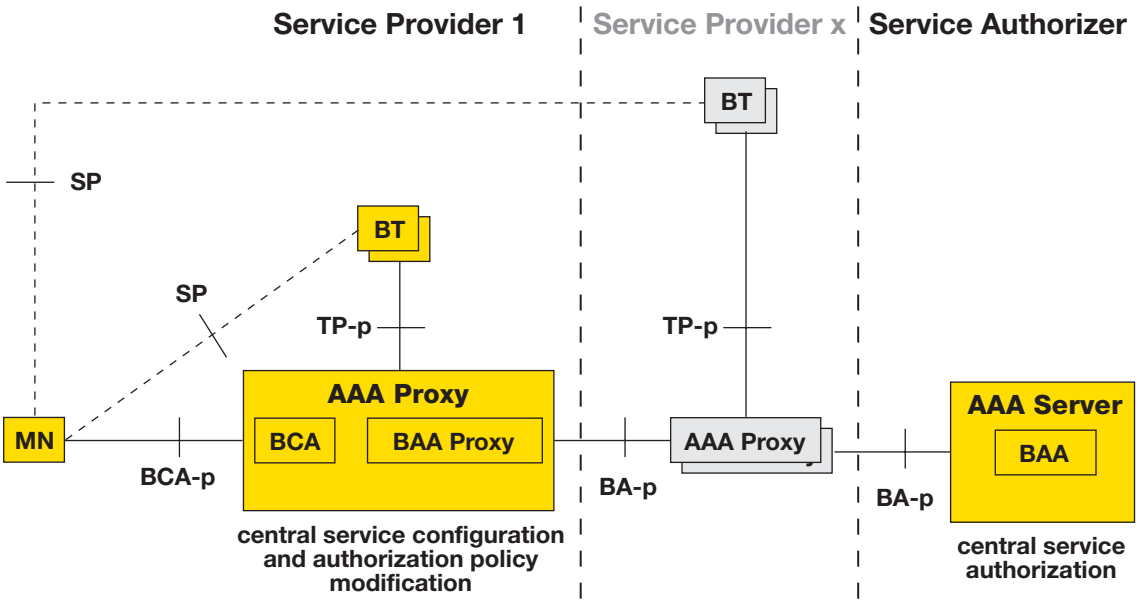


Figure 2.3.4 depicts this mapping whereby the BCA and the BAA proxy functionalities are co-located in an AAA proxy in the service providing domain (SP), and the BAA is located at the AAA server in the service authorising domain (SA). The BA-p interface provides an interaction between the AAA proxy and the AAA server. The GSABA architecture requires only extensions that are in scope of the AAA extensibility framework. As in the existing AAA infrastructures, the BA-p interface can encompass multiple AAA proxies, which may be agnostic of the GSABA functionality. This simplifies the deployment. The authorisation decisions are taken from the AAA server and are relayed to the GSABA AAA proxy with whom the MN interacts. Typically, this is the AAA proxy in the network access service provider (ASP) domain. However, if the ASP is not GSABA-enabled, then the MN can also be connected to a GSABA-enabled proxy in its service authoriser domain as it might be required in a transition period. The authorisation statements can be modified along the AAA path by proxies as envisioned with the Diameter design [15]. This enables the service providing domain to modify the decision made by the home AAA server.

The GSABA architecture is based on the following assumptions:

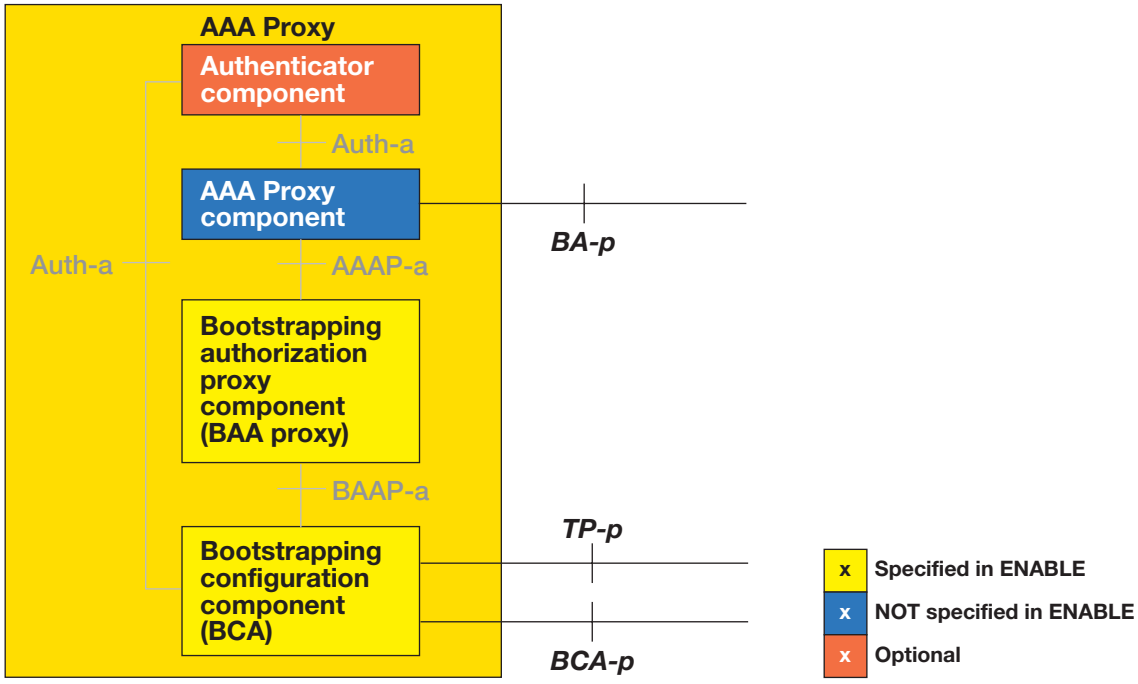
- The BT and the GSABA AAA proxy are located in the same domain.
- The service authorisation decisions are taken by the AAA server in the service authorising domain and can be modified along the AAA path by AAA proxies to the service providing domain if the service provider is different than the service authoriser.
- The service authoriser is assumed to be the "home domain", i.e., the domain with which the MN has a relationship (e.g., a subscription based on a contract). This home domain serves as a central service authoriser for various services.
- The MN needs to interact only with a single GSABA AAA proxy, either in the ASP or, if the ASP is not GSABA enabled, with the AAA proxy in the SA domain.

Taking these assumptions into account, we present how the entities involved in our architecture interact with each other through different interfaces.

2.3.2.2.1. Mobile Node

The mobile node obtains the configuration parameter and authorisation statements for the services from the GSABA AAA proxy and uses this information for consuming the services. The MN consists of the service client component and the bootstrapping client component. The service client is connected via the SP interface to the bootstrapping targets (BT).

Figure 2.3.5: GSABA AAA proxy



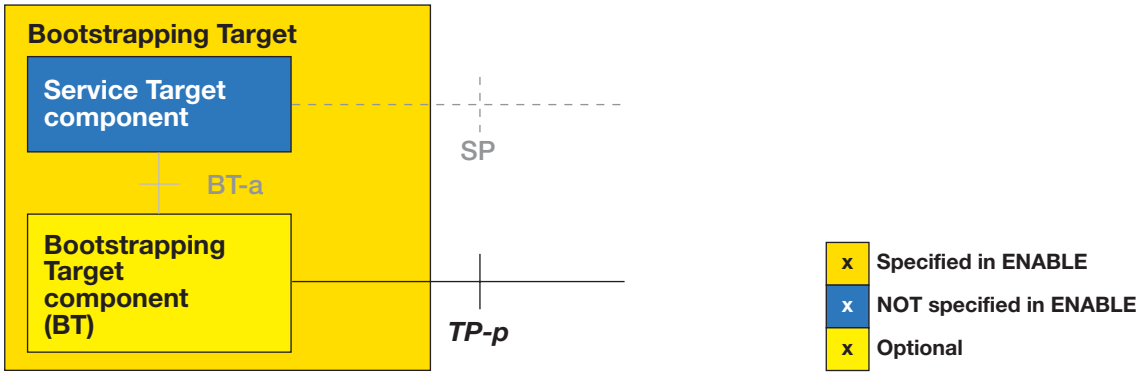
2.3.2.2.2. GSABA AAA Proxy

The GSABA AAA proxy (see Figure 2.3.5) obtains the authorization statements for specific services from the home AAA server where the BAA is co-located and processes (modifies) them. Finally, it delivers these statements together with the needed parameters to the MN and the BTs. The modified AAA proxy consists of the Authenticator, the AAA proxy, the Bootstrapping authorization proxy and the Bootstrapping configuration component. The AAA proxy component obtains the service authorization statements from the AAA server and hands it over to the Bootstrapping authorisation proxy component. The Bootstrapping authorisation proxy component processes the authorisation decision statement (e.g., modifies the decision or adds new authorisation statements). After this processing the statements are handed over to the Bootstrapping configuration component. This component adds the needed configuration parameters (according to the services provided in his domain) and delivers this information to the MN over the BCA-p interface (if the AAA proxy is an intermediate proxy it can also send this information via the BA-p interface to the next AAA proxy). If the AAA proxy is also in charge of authenticating, the MN can authenticate himself through an authenticator component located at the AAA proxy via EAP. If the AAA proxy gets a service request for a service not provided in its domain it forwards the request to the adequate entity. This mechanism is described more in detail in the next section.

2.3.2.2.3. Bootstrapping Target

The Bootstrapping Target (see Figure 2.3.6) consists of the service target component and the bootstrapping target component. The service target component is the main component of the Bootstrapping Target and is actually responsible for providing the service to the MN. The bootstrapping target component is connected via the TP-p interface to the GSABA-enabled AAA proxy and obtains via this interface the configuration and authorisation information related to a specific MN.

Figure 2.3.6: Bootstrapping Target components



2.3.2.2.4. AAA Server

The AAA server is responsible for making authorisation decisions and authenticates the MN. The AAA server needs to be aware of the services it needs to authorise. The bootstrapping authorisation component could be added to the AAA server, in order to enable the delivery of the MN profile to the AAA proxy instead of only dedicated authorisation statements.

2.3.3. HIGH LEVEL MESSAGE CHART

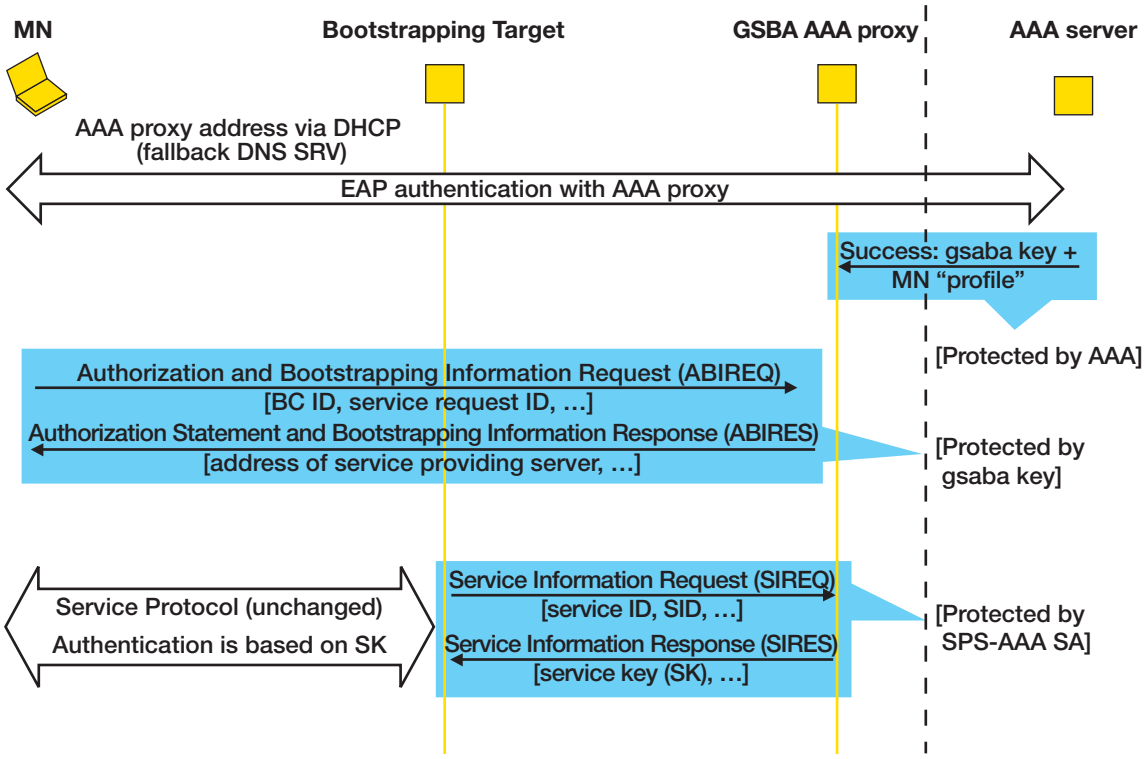
Following a message sequence chart is presented in Figure 2.3.7. It aims to show about how the different entities interact to provide service access in our architecture.

As a first step the MN discovers the address of the GSABA AAA proxy. This address discovery can be performed in various ways. For example, the address could be assigned via DHCP or the address could be discovered using a DNS query by using SRV records [12]. Then, the MN needs to be authenticated by the GSABA AAA proxy. This can be achieved in two different ways;

(a) Directly by using an EAP based authentication with the MN as the supplicant, the AAA proxy as the authenticator and the service authoriser with the backend authentication server [11].

(b) Indirectly by coupling it to the initial network access. This is possible if the GSABA AAA proxy is located in the ASP.

Figure 2.3.7: GSABA Message Chart



As a result, in both cases a new key is generated by the MN and the AAA server, called GSABA key that might be derived from EMSK generated after a successful EAP method authentication (some guidelines for further key derivation by using EMSK as a root key can be found in [16]). Finally, the fresh and unique GSABA key is delivered to the GSABA AAA proxy. In addition to the key, the MN's profile is also delivered to the GSABA AAA proxy (if the user's privacy preference allows it). This profile contains the service authorisation information for all authorised services. Once the MN's profile is available to the GSABA AAA proxy it is able to generate the authorisation decision locally and does not need to contact the backend AAA server for each service request. After successful authentication the MN and the GSABA AAA proxy have the new GSABA key. This key is used for the protection of the communication between the MN and the GSABA AAA proxy (i.e., the BCA-p interface). Additionally, a new identifier is generated by the MN and the GSABA AAA proxy with which the GSABA key (and therefore indirectly the MN) is identified (called BCID for "Bootstrapping Client IDentifier"). Now, the MN can request services. This is done via the ABIREQ (Authorisation and Bootstrapping Information REQuest) message. The minimum set of parameters included in the ABIREQ is the BCID, the identifier of the service that the MN wants to use (Service Request ID - SRID), and the corresponding identifier intended to be used on the SP interface (Service ID - SID). The SRID could either be a service name alone or, additionally a bootstrapping target address if known by the MN. The GSABA AAA proxy then sends an ABIRES (authorisation and bootstrapping information response) to the client containing the needed and requested parameters. The minimum information conveyed to the MN is the address (this could be an IP address or a FQDN) of the bootstrapping target, which could be the same as in the ABIREQ from the MN. The ABIRES can additionally include a key and an identifier (SID) to be used for accessing

the service. Furthermore, it contains the authorisation decision statements for the service. In the general case, the ABIREQ can contain a request for multiple services and also the ABIRES can contain information for multiple services. This optimisation is introduced to save roundtrips. After the MN obtained the needed information for accessing the service, it can start to execute the service protocol with the bootstrapping target. After the bootstrapping target gets the service request and can not match the SID used in the service protocol to any of its locally present SIDs it contacts the GSABA AAA proxy and asks for information about this specific ID (SKREQ - Service Key REQuest). The minimal information in this request is the bootstrapping target ID and the used ID in the service protocol (i.e., the SID). The GSABA AAA proxy answers this request with a SKRES (Service Key RESponse). This SKRES contains the key and the authorisation information to be used for the verification of the service protocol.

2.3.3.1. GSABA AAA Proxies Interworking

The GSABA architecture is designed to support GSABA AAA proxies other than the one that interact with the user (called the first GSABA AAA proxy). This is needed for cases where the bootstrapping targets are located in a different domain as the domain the user is currently attached to. Hence, these GSABA AAA proxies are in charge of managing services that are not controlled by the first GSABA AAA proxy. A specific GSABA AAA proxy (called the second GSABA AAA proxy) should be asked by the first GSABA AAA proxy because it received a request for a service which provides a domain managed by the second GSABA AAA proxy.

Figure 2.3.8: Interworking GSABA AAA proxies

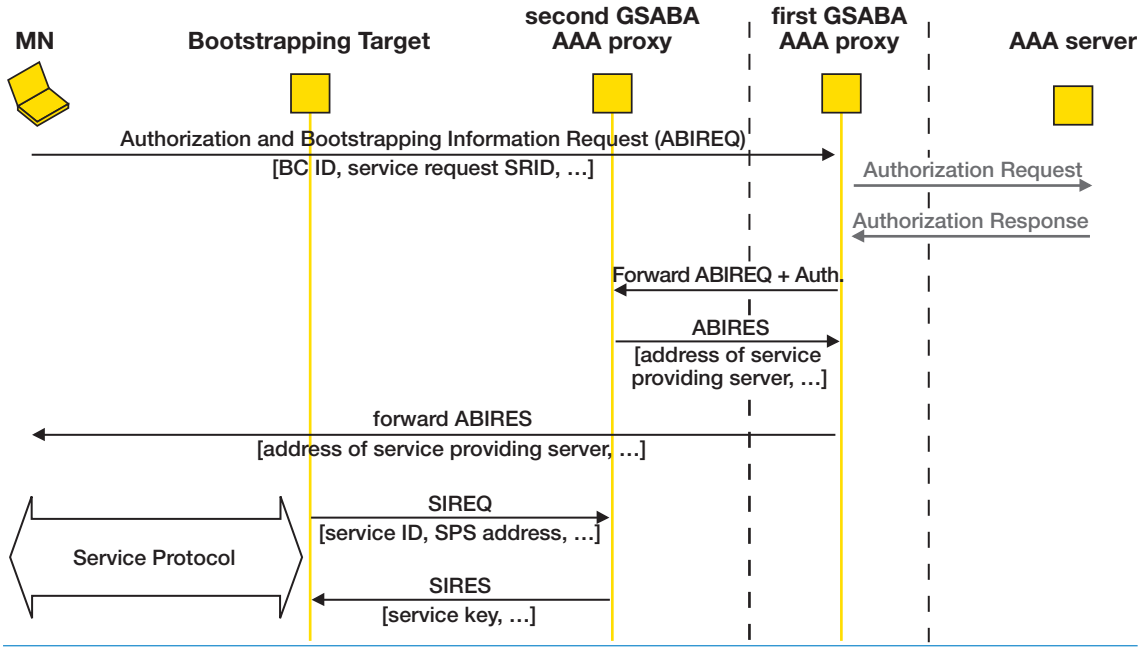


Figure 2.3.8 depicts the message chart. After receiving an ABIREQ from the user for a service not provided by the first GSABA AAA proxy, the first GSABA AAA proxy asks the second GSABA AAA proxy about service specific information by forwarding the ABIREQ message. Beside that the first GSABA AAA proxy asks the AAA server for authorisation information if the MN's profile isn't locally available. The second GSABA AAA proxy answers with an ABIRES, which is then, after possible modifications, forwarded to the MN. Now the MN has the needed information to access the requested service.

The interworking of both GSABA AAA proxies is splitting the responsibility of each one:

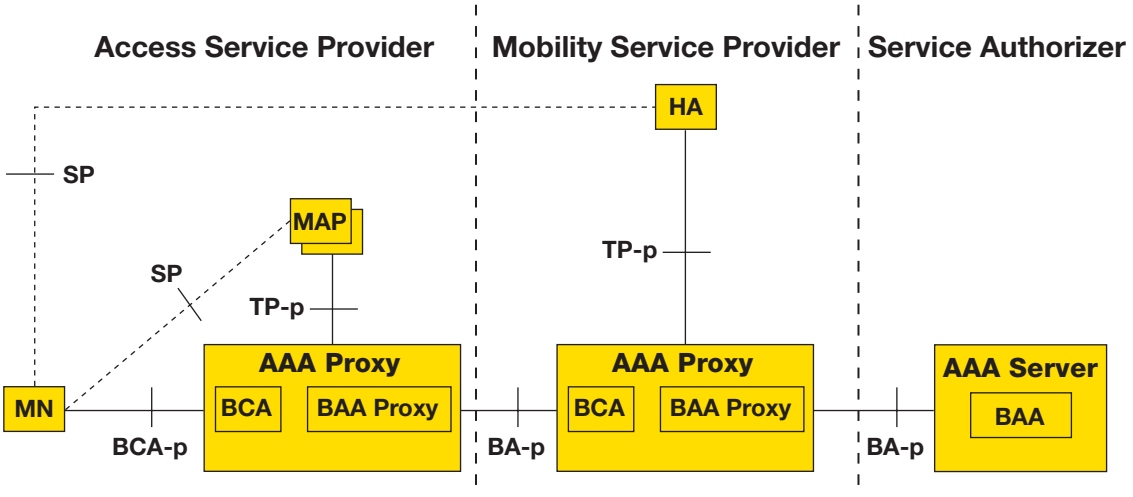
- The first GSABA AAA proxy is in charge of interacting with the user, asking the AAA server for authorisation information, and contacting the second GSABA AAA proxy for asking for servic information and for providing authorisation information.
- The second GSABA AAA proxy is in charge of selecting and configuring the actual bootstrapping target, establishing authorisation decision, and providing the service information to the first GSABA AAA proxy.

In that way, the first GSABA AAA proxy would be in charge of managing the user and AAA server interactions and the second GSABA AAA proxy would be in charge of managing the BTs.

2.3.4. APPLICABILITY EXAMPLE: MAPPING TO HMIPV6

This section describes one concrete application of the GSABA architecture by applying it to HMIPv6 [17] service. The HA and the MAP are both bootstrapping targets. The challenge is that they are quite likely located in different domains. The HA would be at the domain providing mobility service (Mobility Service Provider or MSP) and the MAP would be in the ASP domain. This implies that there are two different GSABA AAA proxies involved in the bootstrapping process. The MAP would be bootstrapped via the ASP's GSABA proxy where the MN is attached to. The HA would be bootstrapped via its MSP's GSABA AAA proxy. After the MN requests HMIPv6 service, the ASP GSABA AAA proxy forwards this request to the MSP's GSABA AAA proxy, which responds with the needed information (e.g. among others with Home Address, Home Agent Address); to this information the ASP's GSABA AAA proxy adds afterwards the parameter for the MAP (e.g. among others the MAP address and RCoA) and delivers it to the MN. Upon service execution the HA and MAP respectively requests the needed parameters from their respective GSABA AAA proxies (e.g. keying material). Similar mappings can be thought of for FMIPv6, where at the beginning already several access routers are bootstrapped at the MN. Figure 2.3.9 shows how this mapping is achieved.

Figure 2.3.9: HMIPv6 service bootstrapped by GSABA architecture



2.3.5. CONCLUSIONS AND FUTURE WORK

This paper proposes a generic service authorisation and bootstrapping architecture. The need for authorisation and the design goals have been presented followed by a description of the logical entities and the involved interfaces. One approach for integrating the proposed architecture into the AAA framework was presented that is attractive due to the large deployment base offered by the AAA architecture. As a next step, the authors plan to apply the presented architecture to different services, to provide a detailed specification of the various interfaces and to start prototyping activities including performance investigations.

2.3.6. ACKNOWLEDGMENTS

This document is a by-product of the ENABLE Project, partially funded by the European Commission under its Sixth Framework Program. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ENABLE Project or the European Commission.

2.3.7. REFERENCES

[1] ENABLE, http://www.ist-enable.org/
[2] A. Patel, Ed, "Problem Statement for bootstrapping Mobile IPv6", I-D draft-ietf-mip6-bootstrap-ps-05, May 2006.
[3] K. Chowdhury, Ed., "MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", I-D draft-ietf-mip6-bootstrapping-integrated-dhc-01.txt, June 2006.
[4] G. Giaretta, Ed., "Mobile IPv6 bootstrapping in split scenario", I-D draft-ietf-mip6-bootstrapping-split-02.txt, March 2006.
[5] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.
[6] Yegin, A., Tschofenig, H. and D. Forsberg, "Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication", Internet-Draft draft-yegin-eap-boot-rfc3118-01, January 2005.
[7] Tschofenig, H., "Bootstrapping RFC3118 Delayed authentication using PANA", Internet-Draft draft-tschofenig-pana-bootstrap-rfc3118-01, October 2003.
[8] Tschofenig, H., "Bootstrapping Kerberos", Internet-Draft draft-tschofenig-pana-bootstrap-kerberos-00, July 2004.
[9] G. Giaretta, "MIPv6 Authorization and Configuration based on EAP", I-D draft-giaretta-mip6-authorization-eap-03.txt, March 2006.
[10] Jee, J., "Diameter Mobile IPv6 Bootstrapping Application using PANA", Internet-Draft draft-jee-mip6-bootstrap-pana-00, October 2004.
[11] Aboba, B, et al., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
[12] A. Gulbrandsen, et al, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.
[13] 3rd Generation Partnership Project, "Generic bootstrapping architecture", Release 7.4, June 2006.
[14] C. de Laat, et al., "Generic AAA Architecture", RFC2903, August 2000.
[15] P.Calhoun et al., "Diameter Base Protocol", RFC3588, September 2003.
[16] Salowey et al. "Specification for the Derivation of Usage Specific Root Keys (USRK) from an Extended Master Session Key (EMSK)", June 2006.
[17] Soliman et al. "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC4140, August 2005.
[18] R. Koodli, Ed. "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

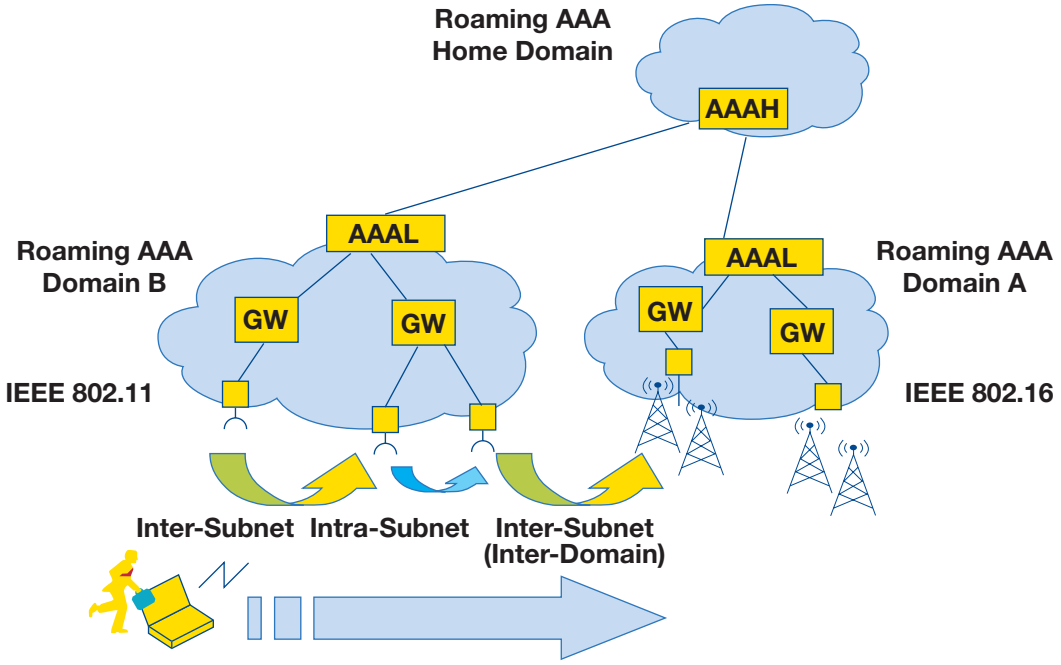
2.4 Analysis of Fast Authentication alternatives in EAP-based wireless networks

Rafael Marín López, Pedro García Segura,
Antonio F. Gómez Skarmeta
University of Murcia

2.4.1. INTRODUCTION

Facing an increasing user demand for new communication and network services, telecommunication operators (TELCOS) are providing network access through different technologies. In fact, the next generations of wireless communications are expected to integrate a huge set of different wireless technologies in order to provide universal wireless access with seamless mobility [1].

Figure 2.4.1: General Handover Scenario



Additionally, and independent of access technology, the operators need to adapt their mechanisms, protocols and infrastructures for managing and controlling subscribers. This is usually achieved through an authenticated network access with the support of Authentication, Authorization and Accounting [2] infrastructures as depicted in Figure 2.4.1. The figure highlights that network services can be accessed through different domains (visited domains) other than the user is subscribed to (home domain), thanks to roaming agreements between them. These agreements are enforced thanks to the deployed AAA infrastructures (AAAV, AAAH) in each domain.

Due to the large number of deployed technologies, and due to the fact that network access control is usually a time-consuming process, operators have to face the difficulty of providing a fast seamless mobility between different technologies, with the inclusion of an authentication process which may produce high delays in on-going communications. A flexible way to carry out this authentication process is based on the use of the Extensible Authentication Protocol (EAP) [3], which allows the use of different authentication mechanisms through the so-called EAP authentication methods. These are performed between an EAP peer (the mobile) and an EAP server (usually co-located with a AAA server) through an EAP authenticator that forwards EAP packets between these both entities. The EAP packets are transported through an EAP lower-layer between EAP peer and EAP authenticator. Between EAP authenticator and EAP server however, an AAA protocol is used. Some of these methods can derive keying material between the mobile and its home domain where the mobile has a subscription. This cryptographic material is subsequently provided to the EAP lower-layer at both peer and authenticator and used for establishing security associations between them. To carry out the EAP authentication, an EAP peer (co-located with the mobile) and EAP server authenticate each other through an EAP authenticator, which is assumed co-located with the Network Access Server (NAS) (e.g. an access router or access point). Basically, the EAP authenticator is in charge of forwarding EAP packets back and forth between EAP peer and EAP server. Although it is possible that EAP server can be co-located at the EAP authenticator, EAP server is typically placed together with the AAA server. However, the current EAP Key Management Framework [4] has shown some drawbacks when mobile and wireless networks are taken into consideration. In particular, an EAP authentication is usually a time-consuming process [5] and it is normally expected to be performed each time the mobile moves to a new EAP authenticator, regardless of whether it has been authenticated recently and owns unexpired keying material. Additionally, the home domain is contacted each time the mobile node is authenticated and this may introduce some additional delay when the home domain is distant. In fact, the home domain is expected to send keys to the access devices (e.g. access points, access routers) within the visited domain which can be particularly problematic in real scenarios [6]. These issues produce undesirable delays during handover process on the on-going communications.

Within the IETF, several alternatives have been proposed to reduce the handover delay when EAP authentication is required. In particular, the HOKEY WG has been designated for this task [7]. In this paper, we survey and analyse the different approaches that allow a secure and fast handover by leveraging cryptographic material generated during an initial EAP authentication. We also pay attention on the bootstrapping of handover keying information.

The remainder of the paper is organized as follows: in section 2.4.2 we analyse the different approaches to reduce the latency introduced for EAP authentication which are being currently discussed within the HOKEY WG. In section 2.4.3, we describe the bootstrapping problem and explain a relevant approach. Finally, in section 2.4.4 we outline some conclusions.

2.4.2. FAST HANDOVER IN EAP

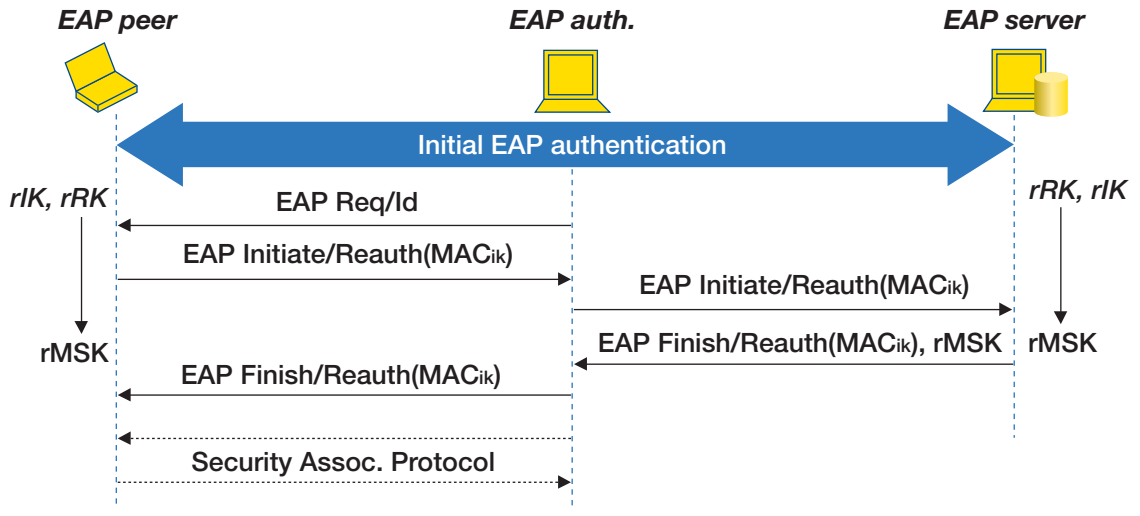
Currently, three main approaches have been proposed within HOKEY WG. The first approach is EAP-ER and it is based on a 2-party model for key distribution. The second and third approach are related. In particular, in section 2.4.2.2 we describe a general approach, currently relevant in HOKEY WG, for handover keying based on 3-party protocol for securely distributing keys in a handover solution. Section 2.4.2.3 describes EAP-HR which basically tries to implement the 3-party party model discussed in section 2.4.2.2.

2.4.2.1. EAP-ER

EAP-ER [8] describes a set of extensions to EAP that enable efficient re-authentication for a peer that has previously performed a full EAP authentication, and maintains valid and unexpired keying material that was derived during this initial process. These extensions include modifications to the protocol, with the inclusion of two new messages, as well as the definition of the required key hierarchy.

Figure 2.4.2 illustrates the protocol exchanges for an EAP re-authentication based on EAP-ER. First, the peer performs a full EAP authentication with the EAP server and both entities derive the MSK, which is then conveyed to the EAP authenticator over the AAA transport protocol. In addition to the MSK, the peer and the authentication server derive a Re-authentication Root Key (rRK). The rRK is the root of the EAP-ER key hierarchy, and from it a Re-authentication Integrity Key (rIK) is derived. This key is used by the peer to provide proof of possession later on, during the re-authentication process. Note that neither the rRK nor the rIK are disclosed to any entities other than the ones that originally generated them.

Figure 2.4.2: EAP-ER



When the peer moves to an authenticator that supports EAP-ER, it sends an Initiate Re-auth message that is integrity protected with the rIK. This message includes a peer-id, an optional temporary NAI based on the rIK name and a sequence number to provide replay protection. If the NAI is included, the message is routed to the authentication server using standard NAI-based routing. Alternatively, EAP-ER offers bootstrapping capabilities to obtain a server-id that can be included in the Initiate Re-auth message to ensure that the

re-authentication exchanges are routed back to the server that derived the keys during the initial full EAP authentication. However, strangely, this bootstrapping mechanism is performed after the initial EAP authentication. We consider the bootstrapping should be done before any handover, that is during the initial EAP authentication. This vision is reflected in section 2.4.3.

Upon reception of the Initiate Re-auth message, the server verifies the proof of possession of the rIK and the freshness of the message. If the credentials are valid, the server generates a Re-Authentication MSK (rMSK) from the rK, the peer-id and the sequence number, and replies with a EAP Finish Re-auth message that is also integrity protected with the rIK. This message transports the rMSK to the authenticator. When the peer receives the Initiate Re-auth message, it verifies the replay protection, computes the rMSK locally and runs the specific security association protocol to establish a secure association with the authenticator.

The EAP-ER solution is able to perform the re-authentication process in a single roundtrip between the authenticator and the server, which has a significant impact in the reduction of the handover latency. Additionally, the bootstrapping capabilities address the need of obtaining a server-id (or a session identifier) at the end of a successful full EAP exchange. This feature allows the peer to ensure that the re-authentication messages are routed back to the server that stored the keying material generated during the initial authentication.

The major drawback of this solution is that it involves major changes in the EAP state machines of all the entities. In particular, it requires support for the protocol on the authenticators, that must be able to understand the new EAP messages. This implies that every authenticator deployed in the network must be modified to support EAP-ER, unless some fallback mechanism is defined.

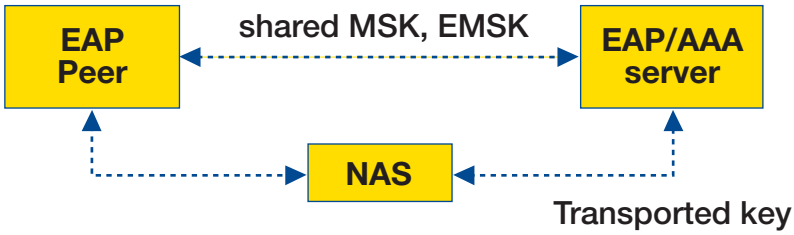
2.4.2.2. Three Party Protocol Approach

Originally, EAP-based network access authentication and authorization has been based on a 2-party trust model where the peer and the authentication server shared long term credentials that they used to authenticate mutually. Eventually, network access authentication was extended to be more scalable by separating the authentication engine from the NAS, moving it to a centralized AAA server, as illustrated in Figure 2.4.3. This extension was transparent to the peer and, although it introduced a third entity, it was argued that the two-party trust model was still in place, since the NAS has no part in determining the result of the authentication.

Figure 2.4.3: 2-party EAP model

However, the extension of the EAP authentication framework to include key management capabilities introduced some new challenges. In this case, the EAP peer and the EAP server derive keying material (MSK and EMSK) after a successful mutual authentication. Since the NAS has no part in this authentication process, it cannot generate the same keying material, which means that one of the original two parties must transfer a key to this new entity, as illustrated in Figure 2.4.4. Clearly this key distribution mechanism is now involving three parties, which invalidates the original assumptions of the original 2-party EAP model.

Figure 2.4.4: 3-party EAP model



Handover keying involves the transmission of keying material in a protocol that involves three parties [9]: the peer that wants to access the network, an entity called HOKEY server that distributes keys between the EAP authenticators, and the authenticator to which the handover will be performed. When the HOKEY server does not have a key (i.e. in a roaming scenario) the three main parties involved are the EAP peer in the visited domain, the EAP server in the home domain and the HOKEY server in the visited domain. Once the HOKEY server owns a key, the three main parties are the EAP peer, the HOKEY server and the EAP authenticator.

2.4.2.3. EAP-HR

EAP-HR [10] describes a solution to arrive to a key hierarchy that provides a solution for fast re-authentication with the HOKEY server. This hierarchy is based on a handover root key (HRK) that is derived from the EMSK, and the proposed solution is able to provision handover security by generating and delivering per authenticator keys (MDMSK) to the authenticators. EAP-HR takes into account the fact that EAP authentication is based on a 2-party protocol, so additional measures are taken to ensure that the keys are properly used in a 3-party key management scenario. The solution proposes a slight modification to the 3-party protocol described in [9] to carry the MDMSK from the HOKEY server to the authenticators, though its security properties have not been verified yet.

Figure 2.4.5: EAP-HR

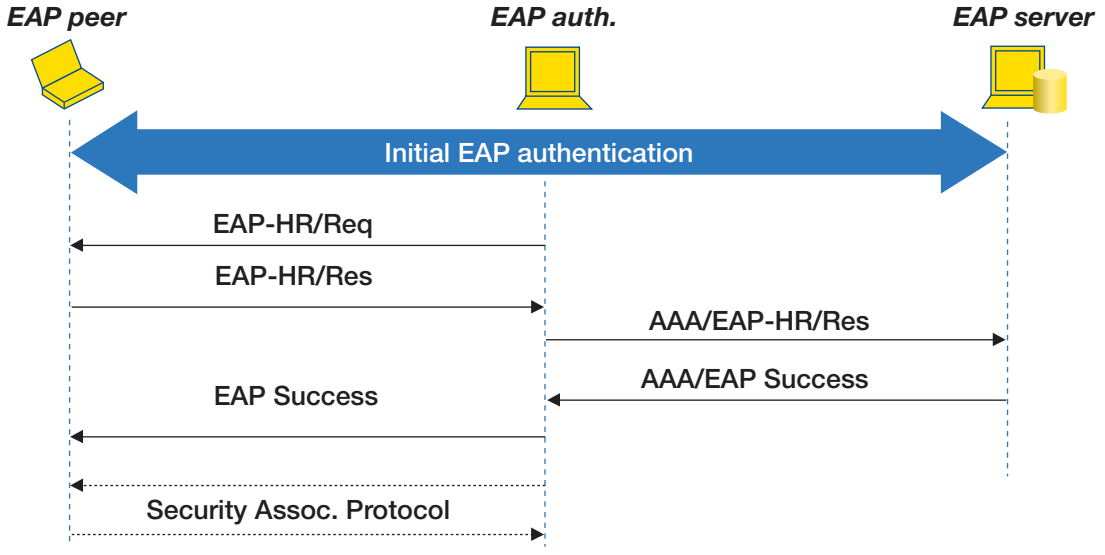


Figure 2.4.5 shows an example message exchange using EAP-HR in a re-authentication scenario. While the described 3-party protocol is, in principle, generic and thus independent of the underlying transport (e.g. EAP), the assumption is that the 3 party protocol data is carried out within EAP messages. For this purpose, a new EAP method, called EAP Handover and Re-authentication (EAP-HR) is proposed. The EAP-HR request and response messages are defined as new EAP types, and the 3-party protocol data is carried out as part of the type data. In addition to these new types, the EAP success message must be modified to carry the additional protocol data. The interface between the authenticator and the server is assumed to be a AAA protocol, so the 3-party protocol data is transported inside new AVPs specifically designed for this purpose.

The re-authentication process can be completed in a single roundtrip in the cases where the EAP-HR request is originated by the authenticator. Note that in this case the additional roundtrip between the peer and the authenticator does not add significant latency to the process. This does not apply, however, when the EAP-HR request is started by the server, but this is a more unusual scenario.

The EAP-HR approach seems have lower impact in the existing EAP implementations, since the EAP state machines does not have to be as heavily modified as in the EAP-ER. However, the implementation of the 3-party protocol implies modifications in the authenticators, peers and server.

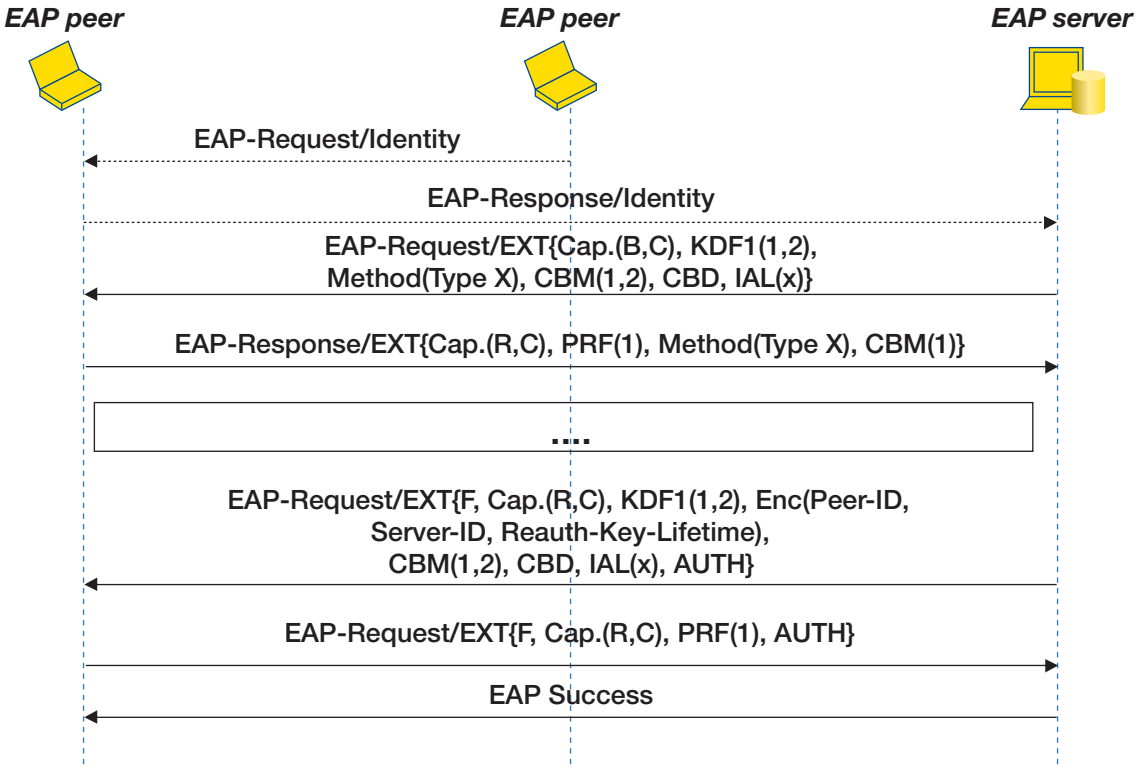
2.4.3. BOOTSTRAPPING SOLUTION: EAP-EXT

The different alternatives shown in section 2.4.2 happen once the EAP peer gets network access after an initial EAP authentication. That initial EAP authentication assumes the execution of a complete EAP method. This is not problematic under handover standpoint since it only happens the first time EAP peer accesses to the network. However, during this initial authentication, it is possible to provide the EAP peer with relevant information related with handover keying information. For example, EAP peer can be informed about the IP address of the HOKEY server in charge of handover keying distribution. In order to this, the recently designed EAP-EXT [11] method turns out a proper solution.

EAP-EXT is an EAP method which is used to provide extensions to the basic functionality of the EAP protocol. Some of this extended functionality may include support for providing HOKEY related information, as well as channel binding capabilities. In addition to this, EAP-EXT also allows sequencing multiple EAP methods within itself, and it can generate MSK and EMSK in cases where the inner EAP method/s generate MSK but do not generate EMSK. EAP-EXT does not modify the EAP protocol, unlike EAP-ER or EAP-HR, since it is based on the usage of a specific EAP method. This means that the protocol can be deployed in the existing access infrastructure, without any modification.

Figure 2.4.6 shows an EAP-EXT message exchange. After the inner EAP method generates keying material, the following EAP-EXT exchanges are protected by an AUTH TLV and encrypted TLVs. These messages can then be used to bootstrap information related to network access and fast re-authentication, such as the server-id, in a clean and secure way.

Figure 2.4.6: EAP-EXT



2.4.4. CONCLUSION

Reducing time spent on authentication (in particular EAP based) is very important for a smooth and seamless handover. IETF through HOKEY WG is working on a solution and several proposals are on the table: EAP-ER, 3-party key distribution approach and EAP-HR.

Under security perspective, the tendency should lead to solutions based on 3-party model which avoids a less impact on current EAP design. In ENABLE, we are putting our effort on designing a secure 3-party protocol, which is able to provide a secure key distribution in fast secure handover in the context of HOKEY. Our intention is to use formal tools to verify the security properties of the 3-party protocol. For bootstrapping purposes, we have chosen EAP-EXT and we are implementing a prototype.

2.4.5. REFERENCES

[1] N. Nasser, A. Hasswa and H. Hassanein, `Handoffs in Fourth Generation Heterogeneous Networks,'' IEEE Commun. Mag. vol.44, no. 10, Oct. 2006, pp. 96-103.

[2] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, "Generic AAA Architecture," RFC 2903, Aug. 2000.

[3] B.~Aboba, L.~Blunk, J.~Vollbrecht, J.~Carlson, and H.~Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.

[4] B. Aboba, D. Simon, J. Arkko, P. Eronen, and H. Levkowetz, "Extensible Authentication Protocol (EAP) Key Management Framework," draft-ietf-eap-keying-15.txt, IETF Internet Draft, Oct. 2006.

[5] M. Georgiades, N. Akhtar, C. Politis and R. Tafazolli, "AAA Context Transfer for Seamless and Secure Multimedia Services," 5.th. European Wireless Conference (EW'04), Feb. 2004, Barcelona, Spain.

[6] R. Marin, J. Bournelle, M. Maknavicius-Laurent, J.M. Combes and Antonio F. Gomez Skarmeta, `Improved EAP keying framework for a secure mobility access service,'' International Conference On Communications And Mobile Computing, pp. 183-188, Vancouver, British Columbia, Canada, March 2006

[7] T. Clancy et al, "Handover Key Management and Re-authentication Problem Statement," draft-ietf-hokey-reauth-ps-01, IETF Internet Draft, Jan. 2007

[8] V.~Narayanan and L.~Dondeti, "EAP Extensions for Efficient Re-authentication," draft-vidya-eap-er-02, IETF Internet Draft, Jan. 2007.

[9] D. Harskin, Y. Ohba, M. Nakhjiri and R. Marin, "Problem Statement and Requirements on a 3-Party Key Distribution Protocol for Handover Keying," draft-ohba-hokey-3party-keydist-ps-01, IETF Internet Draft, March 2007.

[10] M. Nakhjiri, "Keying and signaling for wireless access and handover using EAP (EAP-HR)," draft-nakhjiri-hokey-hierarchy-04, IETF Internet Draft, April 2007.

[11] Y. Ohba, S. Das and R. Marin, "An EAP Method for EAP Extension (EAP-EXT)," draft-ohba-hokey-emu-eap-ext-01, IETF Internet Draft, March 2007.

2.5 Home Agent reliability for operational Mobile IPv6 deployment

Wolfgang Fritsche, Karl Mayer, **IABG**
Michele La Monaca, **Telecom Italia**
Pedro García Segura, **University of Murcia**

2.5.1. INTRODUCTION

For deploying operational MIPv6 [1] services, the HA will be allocated to a registering MN during the bootstrapping phase. Within the integrated scenario [2], that is, for the case the Access Service Authorszer is equal to the Mobilty Service Authoriser, the HA assignment usually is done by means of DHCP in the access network. Alternatively, a HA assignment can be done via means of EAP. Within the split scenario [3], that is, for the case the Access Service Authoriser is equal to the Mobilty Service Authoriser, the HA assignment will be done via DNS. In any case, a single HA will be assigned in the end to a registering MN. As the HA represents a key component for operational MIPv6 deployment, it consequently is a single point of failure. For this reason the Mobility Service Provider (MSP) has to consider appropriate reliability aspects for its HA service.

In order to achieve this objective, several HAs can be deployed on the same home link, providing backup service between each other in the case of a failure of a single HA. This backup mechanism can be realised in different ways. An architecturally very simple, but monetary costly solution would be a hardware based redundancy strategy, that is, for each HA a completely redundant additional HA is provided, which takes over the HA tasks in case a failure is detected by some failover modules. This type of solution to increase reliabilty will not be further considered in this paper.

Other solutions are based on the MN to register with more than one HA at the same time. In case the Active HAs fails, one of the Standby HAs can take over its tasks. In this area many different approaches have already been studied. For all the protocol based backup mechanisms there are still many open issues to be solved, e.g., it often is not specified how the Active and Standby HAs are selected. It is also not specified which information needs to be synchronised between the redundant HAs, or the mechanisms frequently are based on running the ICMPv6 router advertisements between HAs, which interrelates unnecessarily the stateless address autoconfiguration process configuration with the configuration of HA reliability functionality. Consequently the IETF mip6 WG established a design team for the specification of its own HA reliability mechanism.

The approach specified by the design team [4], [5] basically foresees two different modes. In one mode called the Hard Switch mode, the Standby HA, taking over the task of a failed Active HA, will request all MNs registered at the failed Active HA to switch to the Standby HA, that is, this mode is not transparent

to the MNs. In the other mode called the Virtual Switch mode, the Standby HA takes over the tasks of the failed Active HA without involving the MNs, that is, this mode is completely transparent to the MNs.

For the design of an efficient reliability mechanism in case of failures of the HA service not only the backup mechanism itself has to be optimised, but it is also important to minimise the time to detect the failure of an Active HA itself.

The following will provide an overview of the approach chosen by the IETF, enhanced by the missing functionality to be deployable in an operational scenario as envisaged by ENABLE.

2.5.2. MOTIVATION, GOALS AND DESIGN ASSUMPTIONS

Beyond providing a reliable HA service, ENABLE identified additional goals and design assumptions, which mainly are motivated from operational deployment scenarios.

For example, for economical reasons it makes no sense to assign each Active HA a dedicated Standby HA. This would be very costly and also wouldn't require any software based backup solution, a pure hardware backup would be sufficient in this case. Consequently each Standby HA need to serve multiple Active HAs.

Also, in an operational requirement one can assume that HAs are all placed within a secure environment, that is, it isn't necessary to secure any control protocol used between them. This assumption is further justified by the fact that ENABLE considers Active and Standby HAs to be placed on a single link. The case of providing "Global Recovery" as foreseen by the IETF has not been taken into account, as routing updates required for having a Standby HA taking over the role of an Active HA on a different links will most likely cause a latency and consequently a service interruption, which is unacceptable in operational scenarios.

Having Active and Standby HAs all placed on a single link further allows us to make use of IP Multicast for exchanging control information between them.

Finally, ENABLE considers Active and Standby HAs to be comparable in terms of processor performance, storing capacity and bandwidth availability. Therefore, there is no requirement for a failed and repaired Active HA to take back its originally registered MNs. These can be left on the new Active HA, while the repaired old Active HA will serve as the Standby HA.

2.5.3. HA RELIABILITY ARCHITECTURE

2.5.3.1. Overview of Building Blocks

In order to design a deployable HA reliability architecture, one needs to firstly identify the respective building blocks required, which are outlined in the following:

- Composition of the HA redundancy set: For each HA serving MNs, in future called Active HA, one needs one or more Standby HAs, which would be available for taking over the tasks of an Active HA in case of failure. Active HAs and Standby HAs comprise the so called HA redundancy set. It is important to specify

how this HA redundancy set should be composed, that is for example, if one or more Standby HAs will be assigned to a single Active HA, if a Standby HA can serve multiple Active HAs, or if a Standby HA could also act itself as an Active HA.

- HA Failure Detection: A mechanism is required which allows the Standby HAs to timely detect the failure of the Active HA.
- HA State Synchronisation: In order to take over the role of an Active HA, the Standby HAs need to synchronise some state information with the Active HA.
- Informing MNs about HA redundancy set: The Standby HA has to request all MNs registered at a failed Active HA to switch to the Standby HA for service continuation. In order to rely on this information, the MN needs a Security Association to all possible Standby HAs. In order to establish this Security Association, the MN has to be informed about all available Standby HAs during bootstrapping.
- Switching the HA at the MN: In the Hard Switch mode the Standby HA has to request all MNs registered at a failed Active HA to switch to the Standby HA for service continuation. An appropriate mechanism is required for this purpose.
- Informing the MSP AAA about HA Switch: The MSP AAA is responsible for HA assignment during bootstrapping, and also later for any HA relocation procedures. Consequently the MSP AAA needs to be informed about any HA switch that has taken place due to reliability issues.

In the following these building blocks will be described in more detail.

2.5.3.2. Composition of the HA redundancy set

From a general point of view, a redundancy set (RS) can be defined as set of HAs implementing some reliability protocol in order that if one (or more, depending on the type) of them fails, the continuity of the mobility service is guaranteed for the users served by the HAs in the redundancy set.

More technically a redundancy set is compound of N Active HAs and M Standby HAs (with M≤N for efficiency reasons). The case of a HA acting as Active and Standby HA at the same time has been deprecated since no clear advantages are foreseen at the expense of more complexity. Furthermore, HA behaving both roles may require more resources (i.e. it will be more expensive) compared to single-role HAs.

The notation RS(N, M) denotes a RS with N active HAs and M Standby HAs. Since the probability of triple failures is negligible, the interest for redundancy sets with M>2 is mostly theoretical; RS(N, 1) and RS(N, 2) are therefore the most interesting sets from an operational point of view.

Having the choice of M restricted to 1 or 2, one may wonder how to choose N. The three main parameters are efficiency, reliability and cost. Efficiency *(e)* for a redundancy set is defined as the number of users that can be served "reliably" divided by the numbers of users that can be served without implementing reliability for a given set of HAs.

$$e[RS(N,M)] = \frac{N}{N+M} = \frac{N/M}{1+N/M}$$

Clearly, being efficiency asymptotically tends to 1 at the growth of N. Economical reasons (the cost of the HA) prevent the arbitrary growth of N and imposes a limit on the efficiency that can be obtained. Another factor that limits the number of active HA in a redundancy set is that the probability of a failure increases as the number of active HA does (i.e. reliability decreases as N increases with M fixed). Furthermore, the resources needed for synchronisation (e.g. bandwidth, processing) depends at least linearly on the number N of active HAs with which stand-by HAs must synchronise.

2.5.3.3. HA Failure Detection

For having the Standby HAs detecting a failure of the Active HA in a timely manner, a kind of keep-alive mechanism is required. One possibility here could be to make use of the already existing ICMPv6 Router Advertisement messages exchanged already between the HAs of a certain HA redundancy set on a specific link. However, using Router Advertisements for this purpose has various drawbacks:

- In case the HA software fails, but the ICMPv6 software still keeps running, the usage of Router Advertisements would not detect the HA failure. As the HA software usually runs in part in the application space, while ICMPv6 usually runs in the kernel space, such a situation may easily happen.
- While the ICMPv6 process may be fine with having Router Advertisements not sent too frequently, the HA Failure Detection process may require a much more frequent exchange. In order to not load the ICMPv6 process too much due to a HA Failure Detection functionality, both these mechanisms are better kept separately.

For this reason a new keep-alive mechanism has been specified for HA Failure Detection, which makes use of a new Mobility Header representing a HA Hello Message. These HA Hello Messages can be sent unsolicited by all Active and Standby HAs of a certain HA redundancy set, or solicited. The latter case allows a new Standby HA joining a certain HA redundancy set to quickly detect all HAs present in the HA redundancy set.

Within the HA Hello Message the Active HA sets a flag indicating its role as Active HA. This way the Standby HAs can identify exactly the Active HA of a certain HA redundancy set, and monitor it for any kind of failure.

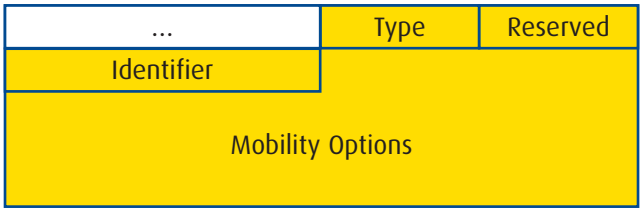
2.5.3.4. HA State Synchronisation

In order to provide appropriate redundancy the HAs have to synchronise various state information between each other. For the Hard Switch Mode it is sufficient for a Standby Home Agent to know which MNs have been registered at the failed Active HA. Having this information a Standby HA could then contact all MNs registered at the failed Active HA and request them to switch to the Standby HA for service continuation. For this reason the state information to be exchanged between Standby and Active HA can be limited to the Binding Cache information of the Active HA.

Within the Virtual Switch Mode the Standby HA has to take over the task of the Active HA in a way, which is completely transparent to the MN. Consequently any kind of state information related to HA service provisioning has to be exchanged. Besides the Binding Cache information of the Active HA this also comprises AAA and security state information, where the latter one could be either IPsec or Authentication Protocol [6] state information.

In order to synchronise the respective state information the new generic Mobility Header outlined in Figure 2.5.1 has been specified by the HA reliability design team. The specific state information itself will then be included as Mobility Option within the new state synchronisation Message.

Figure 2.5.1: State Synchronisation Message Format



2.5.3.4.1. Synchronising the Binding Cache

The following information is usually contained in a Binding Cache entry of a MN and consequently needs to be synchronised:

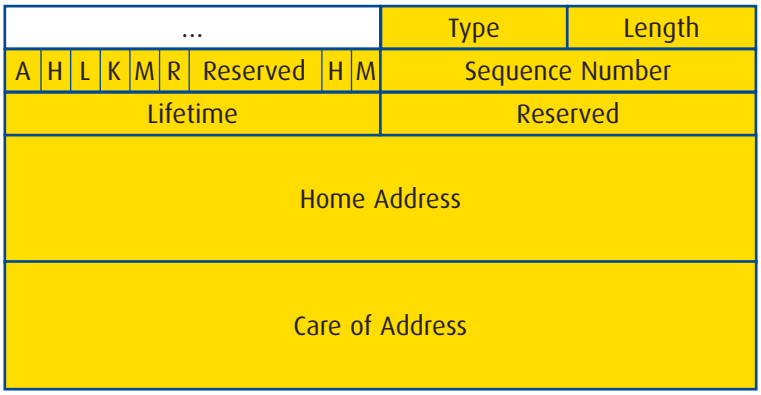
- Home Address of the registered MNs
- Care-of Address corresponding to a registered MN's Home Address
- A lifetime value, which indicates the remaining lifetime of the respective Binding Cache entry
- A flag, which indicates whether the Binding Cache entry represents a home registration
- The maximum Sequence Number received within the last Binding Update sent by the registered MN, allowing to assess the actuality of Bus
- Other flags, which are used for key management or requesting Binding Acknowledgements

Additionally, there might be some information about the usage of the Binding Cache, that is, e.g. which policy should be applied for removing Binding Cache entries. However, it is assumed that Active and all Standby HAs are pre-configured with the identical policy, that is, this policy doesn't need to be exchanged between them as part of the synchronisation information.

However, ENABLE additionally specified HA and Mobility Service Provider relocation procedures. In this context the MN can signal within Binding Updates its support for this advanced functionality, setting the appropriate flags. These flags also need to be synchronised between Active and Standby HAs.

Figure 2.5.2 illustrates the format of a new Mobility Option, which can be used to synchronise the Binding Cache information. The H and M flags behind the Reserved field refer to the signaling of support for the HA and MSP relocation functionality.

Figure 2.5.2: Mobility option for synchronising the Binding Cache state information



Based on this format, for each event causing a modification of a Binding Cache entry within the Active HA 42 octets would need to be synchronised.

2.5.3.4.2. Synchronising AAA information

In principle, the AAA information that must be synchronised is composed of the relevant AVPs from the Diameter MIP6 Authorisation Application defined by the DIME workgroup, as well as the extensions for HA/MSP relocation envisaged by ENABLE. However, further research points to the fact that the AAA synchronisation problem may not be as simple as identifying a number of needed AVPs. This is why this section will focus on the issues that have been detected during the investigation carried out within the ENABLE project.

An ideal approach for the synchronisation of AAA state would be that HA failures are completely transparent to the AAA server. This could be accomplished if the Standby HA takes over the IP address of the failed Active HA not only from the MN's perspective, but also from the AAA server point of view. In order to do this, we must ensure that the existing connection between the HA and the AAA server survives the failure of the Active HA and the subsequent takeover that is performed by the Standby HA. In order to verify the feasibility of this approach, we need to take a look at the characteristics of the Diameter transport. In Diameter a connection is a transport level connection between two peers, used to send and receive Diameter messages, and a session is a logical concept at the application layer, shared between an access device and a server, and identified via the Session-Id AVP. There is no relationship between a connection and a session, and messages for multiple sessions are all multiplexed through a single connection. All Diameter clients must support either TCP or SCTP for the transport of their connections, and it is stated that future versions of the specification may mandate that clients support SCTP. Additionally, all the messages should be protected using IPsec or TLS. In order to survive HA failures in a completely transparent way, at least per-packet TCP and IPsec state would have to be synchronised among all HAs belonging to the same redundancy set, and depending on the particular implementation, maybe also SCTP and TLS state. This amount of synchronisation overhead does not seem acceptable, so an alternative solution might be deploying an administrative entity that detects the failure of the Active HA and triggers the re-creation of the transport connection, which would now be established with the Standby HA. Note, that from the point of view of the AAA server, the HA has not changed, since in the Virtual Switch mode the Standby HA has taken over the IP address of the failed Active HA. Since in Diameter the re-establishment of the transport connection does not affect the active user sessions, the AAA server will resume operation as normal, retransmitting any queued messages.

Regarding the format of the synchronisation information, [5] suggests the use of AVPs to carry the data. This is a valid option, although it is very likely that not only Diameter AVPs, but also information from the Diameter header (e.g. the hop-by-hop identifier) must be synchronised. While using AVPs would allow to select the minimal amount of needed information (as opposed to synchronising the whole Diameter packet) it seems that in any case the amount of data to be synchronised for mobility authorisation will not cause significant overhead in the home link. Some initial calculations, assuming an average Diameter packet size of 250 octets, an authorisation lifetime of 2 hours and 100.000 MNs being served by the active HA, show that the average signalling traffic for AAA state synchronisation would be around 55kbps, which indicates that the synchronisation should be feasible at least for Mobile IPv6 authorisation exchanges.

However, this scenario gets much more complicated when accounting and credit control applications enter the picture. Due to its role in traffic forwarding, the HA is very likely to perform offline accounting procedures,

as well as real-time accounting using the Diameter Credit Control application. This is a very complex application and a deep study would have to be carried out in order to identify a way of synchronising data for features such as direct debiting, tariff switching, mutiple services, resource pools, quotas, etc. Synchronising all this information is a delicate matter, because usually network operators are very sensitive about the reliability of the accounting procedures. Further research is required in order to assess the feasiblity of performing state synchronisation for AAA, but our initial conclusion is that it is certainly a complex issue and it can present a significant drawback to the usage of the Virtual Switch mode in operational scenarios where accounting procedures are mandatory.

2.5.3.4.3. Synchronising information required for the Authentication Protocol

Basically, the information that needs to be synchronised for the Authentication Protocol is the data associated with the shared-key-based mobility Security Associations between Mobile Nodes and the Home Agents. This means that for each MN the following pieces of information must be synchronised:

- SPI (4 octets)
- MN-HA key and the corresponding lifetime (16 + 4 octets)
- Algorithms for authentication and replay protection (1 octet)
  - 1 bit specifying the replay protection mechanism (i.e. BU timestamps versa BU sequence numbers)
  - 7 bits specifying the selected authentication algorithm

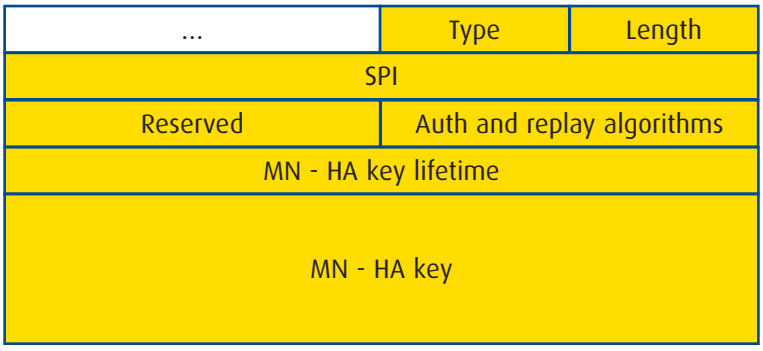
This information must be (re-)synchronised in response to one of these three events:

- a MN bootstraps
- a MN is relocated
- a MN-HA key expires.

Since these are relatively rare events and considering that each synchronisation event requires approximately 25 bytes, the bandwidth consumption due to synchronisation may be assumed negligible. For example in a redundancy set of 10 Active HAs each of them undergoing one synchronisation event per second the overall bandwidth consumption would be 0.25 kbps.

Figure 2.5.3 illustrates a new Mobility Option defined to exchange the Authentication Protocol synchronisation data among Active HAs and Standby HA(s).

Figure 2.5.3: Mobility option for synchronising the Authentication Protocol state information



Since traffic load is not an issue and no other processing other than read & copy operations is performed by the HAs, the overall overhead to synchronise the Authentication Protocol state in a HA redundancy set may be assumed negligible for both Active and Standby HAs.

2.5.3.4.4. Synchronising information required for IPsec (UMU)

A considerable amount of information must be synchronised in order to maintain the IPsec state consistent among all HAs that belong to the same redundancy set. This information can be coarsely divided into two categories: static information that does not change over time and only needs to be synchronised once (e.g. the traffic selectors when a new security association is created); and dynamic information that must be refreshed periodically or when a specific event occurs. The information that must be synchronised is the following:

- **Security Policy Database (SPD) and traffic selectors.** Most of the SPD data is static, and must only be synchronised upon the creation of the Security Policy (SP). This data includes: traffic selectors, endpoint addresses, IPsec mode, policy direction and the lifetime of the SP. However, in order to keep track of the lifetime of a SP some additional information may have to be synchronised (e.g. the number of transferred bytes or packets).
- **Security Association Database (SAD).** The SAD contains an amount of dynamic information that must be updated on a per-packet basis, that is, every time a new IPsec packet is transferred between the MN and the Active HA. In particular, the sequence number, which is modified with every sent or received IPsec packet. If anti-replay protection is enabled, the status of the replay windows must also be synchronised for every new packet. In addition to this variable information, there is also a considerable amount of static information that must be synchronised upon creation of a new SA: SPI value, IPsec mode, algorithms, keying material, traffic selectors, endpoint addresses, lifetime, etc.
- **IKEv2.** When the IKEv2 protocol is used to negotiate and maintain the SAs, the synchronisation mechanism must also take care of keeping consistent IKEv2 state among the HAs. This state includes information that must be updated for every sent or received IKEv2 message, such as the lifetime of the IKEv2 SA, message IDs, etc.

We have identified four basic events that would trigger a synchronisation exchange among the HAs of the redundancy set. The first one is the bootstrapping of the mobility service, which implies an IKEv2 negotiation exchange and the creation of SPs and SAs to protect Mobile IPv6 signaling and optionally data traffic. Second, the reception or transmission of an IPsec-protected packet between the MN and the Active HA, which should trigger an update of the sequence numbers and other dynamic information. Here, one could use IPsec only for protecting Mobile IPv6 signaling information, or more extensive to protect also data packets between MN and Active HA. The third one is the update of the IKEv2 SA, when a rekeying is performed to refresh the keying material, or when the IKEv2 SA is deleted because the MN has stopped using the mobility service. Lastly, the update of the IPsec SAs also for rekeying purposes or for deletion.

The bootstrapping and rekeying events are performed just a few times during the lifetime of the MN's mobility session, so they do not add a significant overhead to the synchronisation process. The bottleneck in this case is the synchronisation exchanges that are needed for every IPsec packet. This will likely restrict the usage of IPsec to the protection of Mobile IPv6 signaling, because the synchronisation of IPsec state in case encryption of data traffic is provided between MN and Active HA would add an unacceptable overhead to the traffic processing and consume a significant part of the home link bandwidth.

2.5.3.5. Informing MNs about HA redundancy set

As briefly mentioned above, in the Hard Switch mode the Standby HA in case of a failure of the Active HA will request a MN to switch to it for service continuation. In order to avoid that a malicious HA could pretend to be a Standby HA and cause a MN to switch to it, a trust relationship is required between MN and any potential Standby HAs. For this purpose the MN will establish during bootstrapping also a security association to all Standby HAs of a HA redundancy set. In order to do this, the MN has to become aware about all the HAs belonging to a certain HA redundancy set, as well as about the one to be used as Active HA.

In the integrated scenario for this purpose the Home Network Information Option of DHCP needs to carry all HA addresses of the HA redundancy set. Additionally, it has to carry a preference value for each of the HAs, indicating to the MN to select the one with the highest preference as Active HA. In case a MN intentionally or accidentally would select a different HA as Active HA, the MSP would trigger a HA relocation process during MIPv6 service authorisation.

In the split scenario DNS is used for HA address identification. In order to be able to inform about multiple HA addresses, the MN performs a DNS lookup by service name. This way DNS is able to return the addresses of all the HAs belonging to a certain HA redundancy set. Note, also in this case preference values have to be assigned to the HAs and obtained by DNS in order to allow the MN to identify the Active HA.

2.5.3.6. Switching the HA at the MN

Within the Hard Switch mode a Standby HA detecting the failure of the Active HA will need to request all the MNs registered at the failed Active HA to switch to itself as the new Active HA. The information about which HAs have been registered at the failed Active HA was learnt by the Standby HA from synchronising the state of the Binding Cache of the Active HA.

After Failure Detection the Standby HA sends a so called HA Switch message to all MNs, requesting them to re-register themselves at the new Active HA. This HA Switch message is protected by the security association the MNs established during bootstrapping with all Standby HAs.

2.5.3.7. Informing the MSP AAA about HA Switch

The MSP is responsible for selecting and assigning the HA to a registering MN, that is, the MSP determines the Active HA of a HA redundancy set. Consequently the MSP also has to be updated in case the Active HA changes due to HA reliability mechanisms.

In the Hard Switch mode the Standby HA requests the MNs to switch after failure of the Active HA. Performing this switching causes the MNs sending a home registration by a Binding Update message to the new Active HA. This home registration at the new Active HA will trigger the procedure of MIPv6 service authorisation, which involves the AAA infrastructure of the MSP. This way the MSP is automatically informed about the change of the Active HA.

In the Virtual Switch mode the Standby HA behaves completely transparent to the MN, taking over for this purpose the IP address previously used by the Active HA, and activating all the synchronised state of the Active HA concerning Binding Cache, AAA and security information. For this reason the HA switch is not visible also to the MSP, that is, the MSP doesn't require any update information in this case.

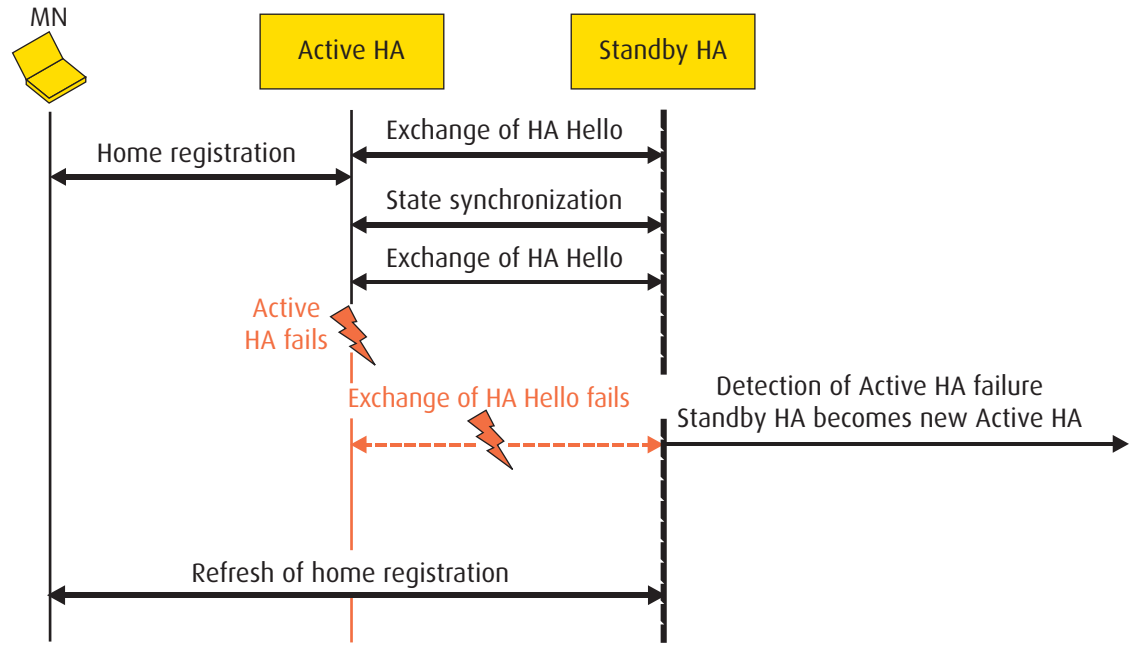
2.5.4. OPERATIONAL SCENARIOS FOR HA RELIABILITY

This chapter gives a brief overview of the message exchanges occurring in case of a HA failure. It should be noted, that not each single message is listed, but just the ones with most relevance to HA reliability.

2.5.4.1. Virtual Switch mode

Figure 2.5.4 illustrates the key message exchanges related to HA reliability for the Virtual Switch mode.

Figure 2.5.4: Message flow for HA reliability in the Virtual Switch mode



Independently from MN registration there is a periodic exchange of HA Hello messages used for Failure Detection and Active HA identification.

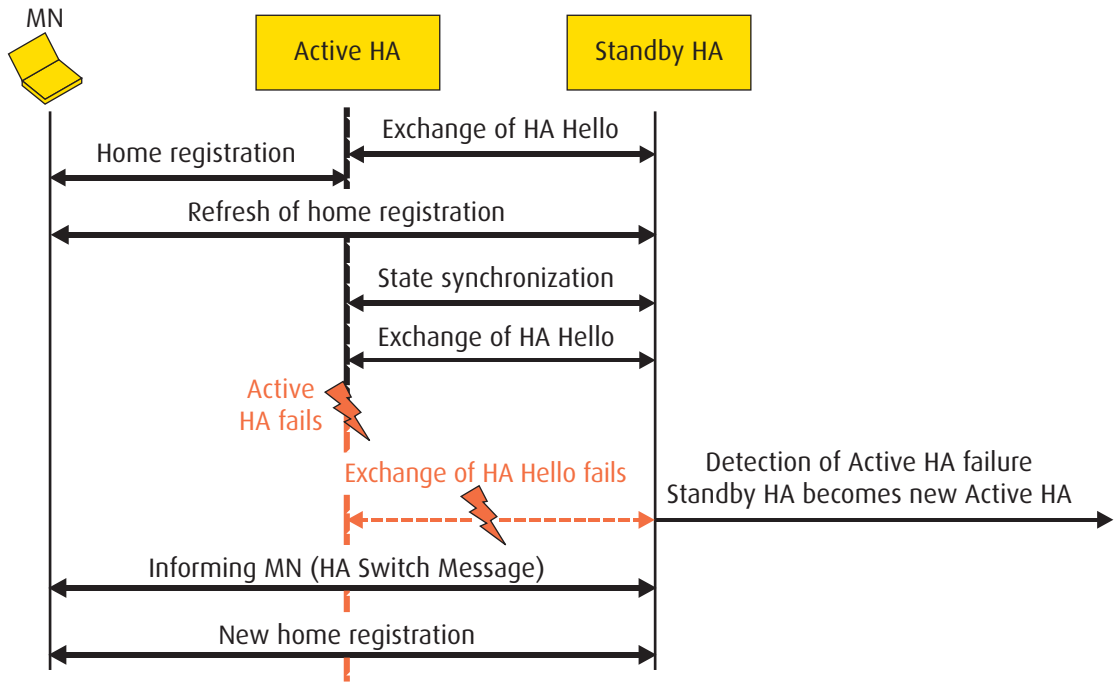
At a certain time a MN will register with the Active HA. Note, the MN has no information about Active and Standby HAs in this mode, it only sees a single HA. After the successful home registration by the MN a state synchronisation occurs between Active and Standby HA. This synchronisation will affect Binding Cache, AAA and security state information stored by the Active HA with regard to the MN's home registration, that is, the Standby HAs will obtain the complete state information the Active HA has for the MN.

At a certain time the Active HA fails, which will be recognized by the Standby HAs due to missing HA Hello messages from the Active HA. The Standby HAs have a mechanism to decide among themselves, which one should take over the role of the new Active HA. The selected one will now configure the address of the failed Active HA, activate all the synchronised state, and continue from now on to serve all the MNs previously registered with the failed Active HA. The whole process will be transparent to all registered MNs.

2.5.4.2. Hard Switch mode

Figure 2.5.5 illustrates the key message exchanges related to HA reliability for the Hard Switch mode.

Figure 2.5.5: Message flow for HA reliability in the Hard Switch mode



Similar to the Virtual Switch mode HA Hello messages are exchanged between Active and Standby HAs for Failure Detection and Active HA Identification.

During the home registration procedure of a MN in the Hard Switch mode the MN is now provided with the complete list of HAs belonging to the HA redundancy set, along with an indication of which one should be used as the Active HA. This will be done by means of DHCPv6 or DNS. After successful home registration with the Active HA, the MN additionally establishes a security association with each Standby HA of the HA redundancy set.

Again, after home registration, state information is exchanged between the Active and the Standby HAs, however, this time it affects only the Binding Cache state information.

For the Virtual Switch mode the failure of the Active HA is detected by the Standby HAs due to missing HA Hello messages from the Active HA. However, this time the selected Standby HA will not take over the role of the failed Active HA transparently for the MNs, but will actively request all MNs previously registered with the failed Active HA to re-register with itself as the new Active HA. This request is sent to the MNs in the form of a HA Switch message. The HA Switch message will then trigger a home registration from the MNs to the new Active HA using a Binding Update. In the process of performing a MIPv6 service authorisation after receiving the Binding Updates from MNs the MSP AAA is informed about the HA switch.

2.5.5. CONCLUSION

For operational deployment of MIPv6 the HA represents a critical component, consequently the provision of the HA service has to be done in a reliable way. This can be achieved by adding redundancy, that is, by assigning one or multiple Standby HAs to the Active HAs which can take over the Active HA's role in case of failures.

Two modes have been identified to provide HA reliability. The Virtual Switch mode is transparent to the MNs, and for this reason attractive from an operational point of view. However, due to the amount on information to be exchanged in some deployment constellations it might not be scalable. For example, if accounting state would need to be exchanged for each data packet, or if the IPsec based security association between MN and Active HA is also used for data encryption, and consequently would also need to be synchronised, a large scale deployment seems impossible.

The Hard Switch mode on the contrary is much more scalable from a synchronisation point of view. Its drawback is the requirement of having the MN establishing security association to all Standby HAs, which may never be used in case the Active HA never fails. However, for a limited number of Standby HAs this seems to be acceptable from an operational point of view, even if the security association is done via the air interface.

2.5.6. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] J. Korhonen, J. Bournelle, H. Tschofenig, K. Chowdhury, C. Perkins: "The NAS - HAAA Interface for MIPv6 Bootstrapping", draft-ietf-dime-mip6-integrated-04 (work in progress), May 2007.

[3] J. Bournelle, G. Giaretta, H. Tschofenig, M. Nakhjiri, "Diameter Mobile IPv6: HA-to-AAAH support", draft-ietf-dime-mip6-split-03 (work in progress), June 2007.

[4] R. Wakikawa, "Home Agent Reliability Protocol", draft-ietf-mip6-hareliability-01.txt (work in progress), March 2007.

[5] B. Haley, V. Devarapalli, H. Deng, J. Kempf, "Mobility Header Home Agent Switch Message", draft-ietf-mip6-ha-switch-03 (work in progress), March 2007.

[6] A. Patel, K. Leung, M. Khalil, A. Akhtar, K. Chowdhury, "Authentication Protocol for Mobile IPv6, RFC 4285, January 2006.

2.6 Deploying Home Agent Load Sharing in Operational Mobile IPv6 Networks

Wolfgang Fritsche, **IABG**
Ivano Guardini, **Telecom Italia**

ABSTRACT

Mobile IPv6 (MIPv6) is a protocol standardised by the Internet Engineering Task Force (IETF) in order to provide mobility support for roaming host systems. A key component within the MIPv6 functionality is the Home Agent (HA), a system at which roaming Mobile Nodes (MNs) register their current point of attachment to the Internet. In order to provide this mobility service to a high number of MNs, multiple HAs are likely to be deployed. However, for other reasons more HAs might also be useful, such as in order to select one close to the MN's location, or to continue the service even if one HA fails.

This paper describes the rational for sharing the load between the different HAs. It discusses the requirements for HA load sharing, introduces the components required for this, presents a proposal for a HA load sharing architecture and shows how this interworks with the currently investigated MIPv6 bootstrapping approaches.

The paper therefore addresses multiple architectural aspects of the MobiArch 2006 workshop, such as "Mobility impact on the Internet architecture", "Architectures and protocols for mobility support", as well as "Load Sharing".

Categories and Subject Descriptors

C.2.2 ***[Computer-Communications Networks]:*** Network Protocols - Protocol architecture
C.2.6 ***[Computer-Communications Networks]:*** Internetworking - Standards *(e.g., TCP/IP)*

General Terms

Algorithms, Design, Standardization

Keywords

IPv6, mobility, bootstrapping, load sharing

2.6.1. OPERATIONAL USE OF MIPV6

MIPv6 is a protocol standardised by the IETF in order to provide mobility support for roaming host systems in a way that is transparent to applications and users. To provide this within MIPv6 each MN owns a static IPv6 address, the so called Home Address (HoA). Additionally each MN has assigned a temporary IPv6 address, the so called Care-of Address (CoA), which is only valid at its current point of attachment to the Internet. The HA represents a system at the MN's home network, at which the MN registers in a secure way the mapping between its HoA and CoA, and therefore its current location. With this information the HA is able to forward any packets addressed to the MN arriving at the home network to the MN's current location.

In order to deploy MIPv6 operationally, a Mobility Service Provider (MSP) has a list of additional requirements, which are not addressed by the MIPv6 core functionality [5]. The main ones are the following:

- The usage of the mobility service has to be authorised by a Mobility Service Authoriser (MSA) based on the service profile of the end user; only this way appropriate accounting concepts can be realised.
- An automatic HoA assignment has to be supported.
- The signaling information exchanged between MN and HA has to be secured. For this purpose [5] specifies the use of an IPsec Security Association (SA) between MN and HA. For an operational deployment the security parameters for setting up this SA between MN and HA need to be generated and configured in an automatic way.
- A MIPv6 service should work in legacy environments, that is, work with currently deployed IPv4 networks.
- A MIPv6 service should work with currently deployed middleboxes, such as firewalls and NAT boxes.
- On request and if authorised by the MSA an optimised mobility support should be provided, such as route optimisation based on Return Routability as specified in [5], Hierarchical Mobile IPv6 (HMIPv6) [7], Fast Handovers for Mobile IPv6 (FMIPv6) [6], or general QoS support.
- Last but not least, for reasons of scalability and reliability the deployment of several HAs has to be supported, with the capability to share the load between them in an efficient way.

2.6.2. RATIONALE FOR HOME AGENT LOAD SHARING

An operational MIPv6 deployment would be difficult with a single HA.

Firstly, quite obvious this single HA would need to serve all the MNs and could therefore quickly run out of resources with regard to bandwidth, memory or processor capacity. Consequently, the number of MNs to be supported and therefore the scalability of the service would be very limited.

Beyond that, with a single HA the MIPv6 service would have no redundancy in case this single HA fails. However, it is not only the accidental failure one needs to consider here, but also the case a HA is going to be intentionally taken out of service for reasons such as upgrade or maintenance for example. A different HA could take over the mobility support for the registered MNs, thus ensuring uninterrupted service for all of them.

Finally, deploying several HAs also allows to distribute them within the network, therefore being able to always assign a HA in close proximity to the MN, and limit this way the signaling overhead and delay.

Having, for the reasons outlined above, multiple HAs available for assignment requires a process for selecting the most appropriate one. There are many reasons why a certain HA should not be assigned to a MN; it may already be serving too many other MNs and consequently has no more resources available; it might know that it has to go down in the near future for a scheduled maintenance, or its location is too far away from the MN and there are other HAs closer to the MN. The process of always selecting the most appropriate HA for a certain MN leads to an efficient HA Load Sharing.

Naturally the selection of the most appropriate HA for a MN needs to be done when the MN registers the first time with a HA. That is, HA Load Sharing mainly happens during the bootstrapping phase. After that it may be required to relocate the HA. For example if a HA fails or the MN moves away from one HA and gets closer to another one.

2.6.3. BOOTSTRAPPING SCENARIOS

As stated above, the assignment of HAs to MNs and therefore the HA Load Sharing process mainly happens during the bootstrapping phase. For this reason the fundamentals of MIPv6 bootstrapping will be briefly explained.

Basically, bootstrapping should configure a MN with enough information that it can register itself at an assigned HA without human intervention. This requires that the MN is informed during the bootstrapping phase about which HA it should use, and which HoA it should configure. Additionally, both MN and HA need to configure the respective security credentials to allow the establishment of a SA and the secure exchange of MIPv6 signaling information between them. This could either be an IPsec SA or a SA for the Authentication Protocol for MIPv6 as specified in [10].

This bootstrapping could mainly happen within two deployment scenarios. More details about the issues involved with bootstrapping and the two deployment scenarios can be found in [9].

2.6.3.1. Integrated Scenario

The first deployment scenario for bootstrapping is called the integrated scenario. In the integrated scenario the entity responsible for authorising the network access service, the so called Access Service Authoriser (ASA), is the same as the entity authorising the mobility service, the so called Mobility Service Authoriser (MSA), and will be called Mobility and Access Service Authoriser (MASA). Basically, in the integrated scenario, HA assignment happens by using DHCPv6 in the access network. This DHCPv6 service either returns a HA provided by the MSA during mobility service authorisation, or a HA provided by the local access network.

More details about how bootstrapping works in the integrated scenario are given in [1].

2.6.3.2. Split Scenario

The second deployment scenario for bootstrapping is called the split scenario. In the split scenario the ASA is a different entity as the MSA. Contrary to the integrated scenario the MN learns about the HA to be used for registration from the DNS, that is, the MN either has the Fully Qualified Domain Name (FQDN) of the HA or a service name for the mobility service pre-configured. In the latter case the DNS will return within the DNS SRV record all available HAs, from which the MN then has to choose from.

More details about how bootstrapping works in the split scenario is given in [3].

2.6.4. REQUIREMENTS FOR HA LOAD SHARING

Concerning the design of a Home Agent Load Sharing approach several requirements should be addressed. The main ones used as basis for this work are the following:

- Generally the designed approach should not depend on any specific hardware or software.
- The Home Agent Load Sharing approach must not introduce any new security issues.
- The Home Agent Load Sharing approach must integrate with the bootstrapping mechanisms used for the split and integrated scenario. This is very important as load sharing mainly will apply during the initial HA assignment in the bootstrapping phase.
- The approach should allow a HA relocation at a later point in time if required. This way an update of the most suitable local HA or a replacement of a failed HA would be possible.
- The MSP actually owns the HAs and therefore is responsible for the mobility support service provision. Consequently the MSP should finally decide about the selection of the most appropriate HA.
- The Home Agent Load Sharing should be transparent to MNs.
- The designed approach should try to limit the additionally required signaling as much as possible, especially if the signaling would need to cross a wireless link.
- The designed approach should try to limit the additional time caused by Home Agent Load Sharing during the bootstrapping process as much as possible.

2.6.5. HA LOAD SHARING ARCHITECTURE

For designing a Home Agent Load Sharing Architecture, which is able to fulfill the requirements outlined above, one first needs to identify the various components or building blocks needed. In this context we roughly identify the following architectural components:

- Set of selection parameters used for selection of the most suitable HA.
- Mechanism to collect the partly distributed selection parameters.
- Algorithm to perform the HA selection based on the selection parameters.
- Mechanism to assign the selected HA to a registering MN.

Different approaches for addressing part or all of these architectural components have been proposed so far, however, each of them has properties which conflict with the requirements for Home Agent Load Sharing as outlined in section 2.6.4. For example [5] specifies the possibility of using the Dynamic Home Agent Address Discovery (DHAAD) mechanism for registering with the most preferred HA, but this alternative won't fit architecturally to the bootstrapping proposals for the integrated and split scenarios, which don't consider the use of DHAAD for HA assignment. Furthermore, for this approach all HAs would need to be located in the same subnet, which may not be the case for local HA deployment. Using extensions to the Virtual Router Redundancy Protocol [4] for exchanging selection parameters between the HAs or the mechanisms described in "Load Balance for Distributed Home Agents in Mobile IPv6" [2] also would only

work if all HAs are located in a single subnet. Deploying the HA to HA (HAHA) protocol as specified in [8] would again require the usage of DHAAD by the MN. Furthermore no details are provided how Home Agent Load Sharing should exactly work.

For these reasons it has been decided to provide our own specification of the components required for a HA Load Sharing architecture.

2.6.5.1. Set of selection parameters

As a first step, one needs to identify the selection parameters, that is, the kind of information which one needs for selecting the most appropriate HA to be assigned to a registering MN in order to provide the most efficient mobility support service. These selection parameters could be seen as input for the Home Agent Load Sharing algorithm. In theory this could be a single selection parameter, however, for various reasons it is beneficial to support a set of selection parameters. This allows more flexibility and granularity for satisfying the MN's specific needs, but even more importantly the MSP's need's with respect to the most efficient assignment of its HA resources. For example a MN could have a preference for always getting the 'closest' HA allocated, while a MSP could have a preference to share the load on its HAs as equally as possible and avoid assignment of HAs which face an upcoming maintenance period. For an initial architecture the following selection parameters are considered:

- Number of active home registrations: if a HA gets closer to an administratively configurable maximal number of supported active home registrations, its preference should be lowered, otherwise its performance to provide the mobility support service is likely to go below a minimum service level. Having the maximum number of active home registration administratively configurable for a specific HA, different HA platforms with different performance aspects can then be integrated in the load sharing scheme.
- Current bandwidth consumption of HA: if the currently consumed bandwidth of a HA on its interface to the home network gets closer to an administratively configurable maximal available bandwidth, its preference should be lowered, otherwise its mobility support service performance will suffer. This parameter has to be used carefully as it will dynamically change. Instead of having highly frequent measurements, one alternative may also be to collect a calculated average value of the consumed bandwidth measured over a recent time interval. However, even if this parameter has to be carefully used, in case a MN has a QoS service level agreement with its provider, e.g. for supporting real-time services, this type of selection parameter could be very useful.
- Upcoming maintenance of HA: if there is an upcoming maintenance period scheduled for the HA, during which it cannot provide any mobility support service, the HA should not be selected.
- Location of the HA: in order to minimise signaling overhead and delay, the assignment of a HA close to a MN may be a valuable approach. For example, each HA could be administratively assigned to a network region. If the MN connects to this network region, only those HAs residing in the respective region may be considered during the HA selection process.

This list of selection parameters should not be seen as exhaustive, but will be open for further additions. This may also support the possibility to include manufacturer specific parameters. However, in this case the Home Agent Load Sharing architecture needs to make sure that manufacturer dependent parameters can also be left out for HA selection in case equipment of different manufacturers is combined for service provision.

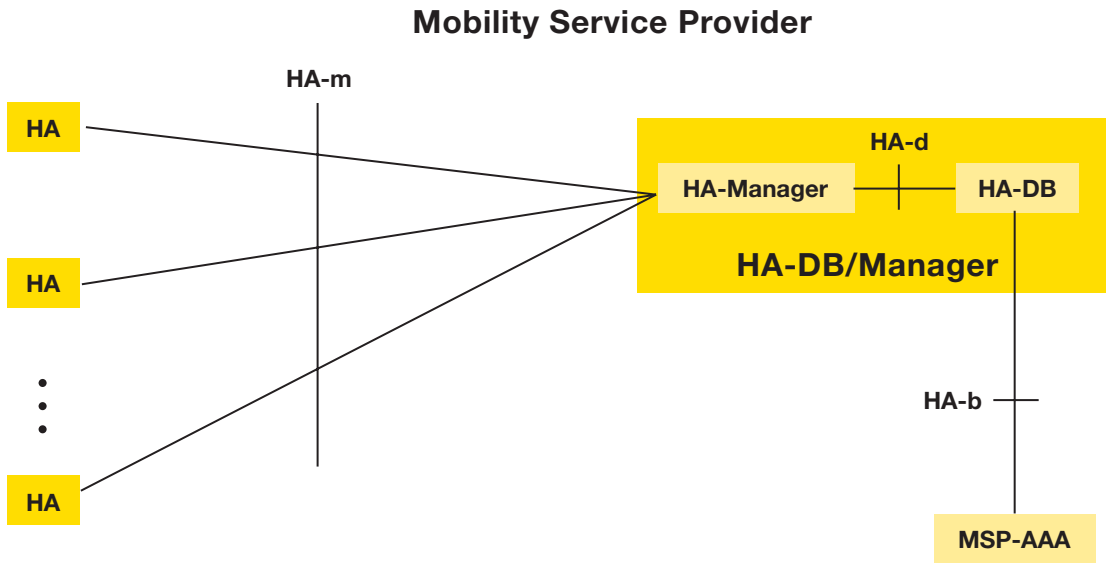
Also it has to be noted that some of the selection parameters will have to be collected from the HAs, such as the number of active home registrations, while other parameters will be available from the management entity of the HAs such as an upcoming maintenance period for the HAs. Furthermore, part of the selection parameters will change dynamically, such as the currently consumed bandwidth of a HA, while others are likely to be static, such as the network region in which a HA is located.

2.6.5.2. Mechanism to collect distributed selection parameters

In the second step one now needs to dynamically collect the required selection parameters, which are distributed between the various HAs and their management entities. In this context only the dynamically changing parameters need to be collected dynamically, while for static parameters it is sufficient to read them once. This collection is clearly a management task, and therefore should be performed from a management entity responsible for the HAs.

The approach proposed here is to have a management entity, called the HA-Manager, collecting the distributed selection parameters. Part of these selection parameters can be assumed to be already locally available on the HA-Manager, like the network region the various HAs are located in information about an upcoming maintenance of a HA. Another part of the selection parameters will need to be retrieved from the HAs, such as the number of active home registrations of certain HAs. In operational deployment most likely a management interface from the HA-Manager to the different HAs will exist anyway, it is proposed to make use of this interface marked as HA-m interface in Figure 2.6.1 also for collecting the selection parameters. This interface could be realized for example by using SNMPv3 [13][14]. Via this interface a HA-Manager could collect the required selection parameters either periodically, or on demand, e.g. when a MN is registering an awaiting HA assignment.

Figure 2.6.1: General HA Load Sharing Architecture



Having collected the selection parameters via the HA-m interface, these will be stored on a HA database (HA-DB) together with the selection parameters which had been already locally available on the HA-Manager. If this database is hosted on the same physical entity as the HA-Manager or on a different one is up to the MSP's decision. However, any communication between HA-Manager and HA-DB, outlined as interface HA-d in Figure 2.6.1, can be done using usual database mechanisms, such as SQL or LDAPv3 [12].

Finally, the selection parameters have to be provided to the entity which is responsible for HA assignment. Looking at the bootstrapping mechanism for the integrated scenario, this is clearly the Authentication, Authorisation, Accounting (AAA) instance of the MSP, outlined as MSP-AAA in Figure 2.6.1. Via a similar database interface HA-b, which uses again mechanisms such as SQL or LDAPv3, the MSP-AAA will get access to the stored selection parameters on HA-DB.

In order to secure the collection of distributed selection parameters, the security mechanisms built in SNMPv3 and in database access mechanisms should be used. Alternatively an IPsec SA could be established between HA and HA-Manager, HA-Manager and HA-DB as well as HA-DB and MSP-AAA. As all these components belong to the MSP, an exchange of the required security credentials should be no major issue.

2.6.5.3. Algorithm to perform HA selection

Once all the selection parameters are available, the most suitable HA to be assigned to a MN has to be selected. This will be done by computing the load for each of the HAs, and then selecting the one with the lowest load. For calculating the load the selection parameters will be used, but in different ways. Part of the selection parameters, such as the location of a HA, will be used in order to limit the number of HAs considered for load computation. For example, for local HA assignment a MSP could request for a registering MN to only consider HAs located in region A, as in this region A the MN has attached to the network.

The other part of the selection parameters are then used to really compute the load of a HA. This load computation happens in a weighted fashion:

$$load_{HA} = a * x + b * y + c * z + \ldots \quad (1)$$

where

x, y, z, ... are the selection parameters, and

a, b, c, ... are the weighting factors.

The weighting factors are set by the MSP for the respective selection parameters. Consequently the selection parameters can be implemented by an equipment manufacturer independent from any MSP deployment issues. Setting the weighting factors each MSP is then able to implement its own specific HA load sharing policy, which best fits its operational needs. For example if a MSP has no interest in considering the selection parameter 'y' for HA load sharing, it just has to set the respective weighting factor 'b' to zero when calculating the load for each of its HAs.

In order to achieve the weighting really by the weighting factors, the different selection parameters have to be normalised before computing the load, e.g. to have values only in the interval [0;1].

2.6.5.4. Mechanism for assigning selected HAs

Finally the selected HA has to be assigned to the registering MN. The way a HA assignment will be done is specified within the various bootstrapping scenarios, which is further described in section 2.6.6.

2.6.6. INTEGRATION OF HA LOAD SHARING WITH MIPV6 BOOTSTRAPPING

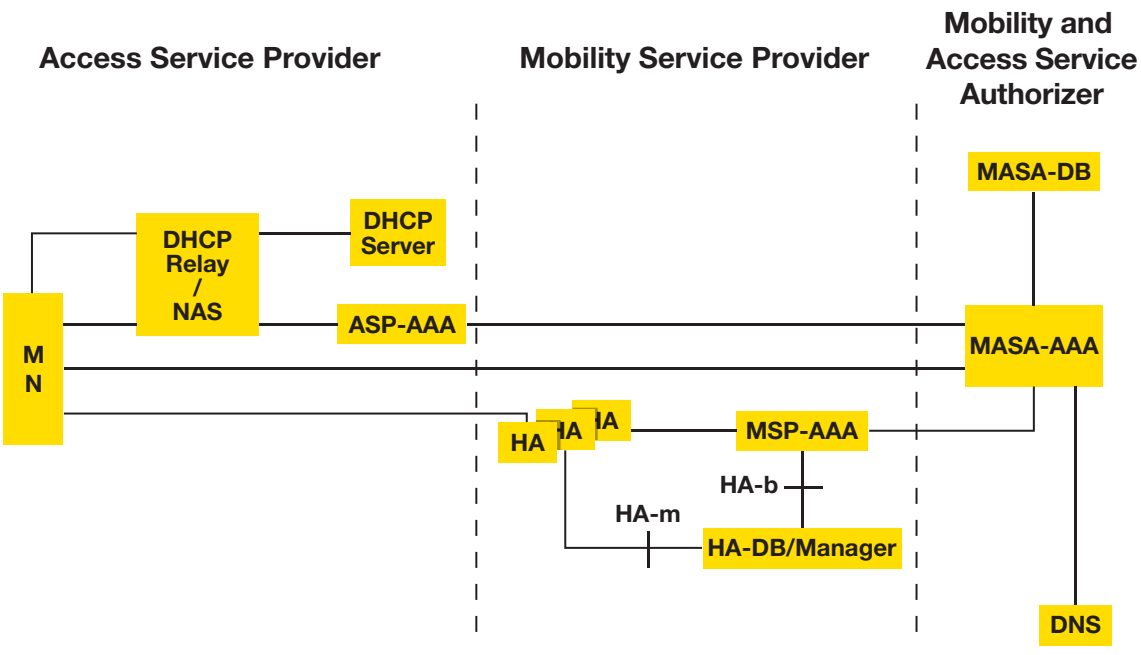
2.6.6.1. HA Load Sharing in the Integrated Scenario

In the integrated scenario [1], in which the ASA is the same entity as the MSA, the HA assignment can be done by the MASA-AAA via DHCPv6. Alternatively if an approach based on the Extensible Authentication Protocol (EAP) is considered for the integrated scenario [16], a new Type-Length-Value (TLV) field could be added to the EAP exchange and used for HA assignment. Making use of the latter alternative clearly requires EAP support in the access network. However, the HA selection will always be done by the entity operating the HAs, that is, by the MSP.

Figure 2.6.2 shows the architecture for HA load sharing in the integrated scenario. A MSP operates a set of HAs, which can be assigned to MNs registering from any Access Service Provider (ASP) network. From these HAs a HA-Manager collects the selection parameters. The collected parameters will then be stored in a HA database (HA-DB). Both collection of the selection parameters and storage in the HA database will be performed by the management entity of the MSP. For reasons of simplicity both components are also referred to as HA-DB/Manager.

From the HA database the stored parameters for each HA can be read by the MSP-AAA, which will then finally perform the computation of the load for each HA by weighting the respective selection parameters as described in section 2.6.5.3.

Figure 2.6.2: HA Load Sharing in the Integrated Scenario



When now a MN connects to any access network, it first needs to get the mobility support authorised from the Mobility Service Authoriser. In this case co-located with the Access Service Authorizer, and therefore named MASA. During this AAA exchange the MASA also selects the MSP to be used for HA service provision, and contacts the MSP-AAA for the best HA to be assigned to the registering MN. Having obtained this HA, the MASA-AAA sends back the selected HA to the ASP-AAA, which will then assign it to the MN using DHCPv6. Alternatively, the MASA-AAA could deliver the HA address directly to the MN using EAP [16], if it is supported in the access network.

Obviously, if the MASA is the same entity as the MSP, that is, the mobility service authorisation is done by the same entity as the mobility service provision, MASA-AAA and MSP-AAA are the same and don't need to communicate with each other.

Furthermore, a notable scenario is when the MSP is the same entity as the ASP, that is, the mobility service and the network access service are provided by the same entity. In this case there is no need for the MASA-AAA to poll the MSP-AAA to collect the address of the best HA. Instead, since ASA-AAA and MSP-AAA are the same, the address of the selected HA can be delivered to the NAS, and in turn to the DHCPv6 server, directly by the MSP-AAA, piggybacking it in the AAA exchange carried out by the MN for network access authentication.

2.6.6.2. HA Load Sharing in the Split Scenario

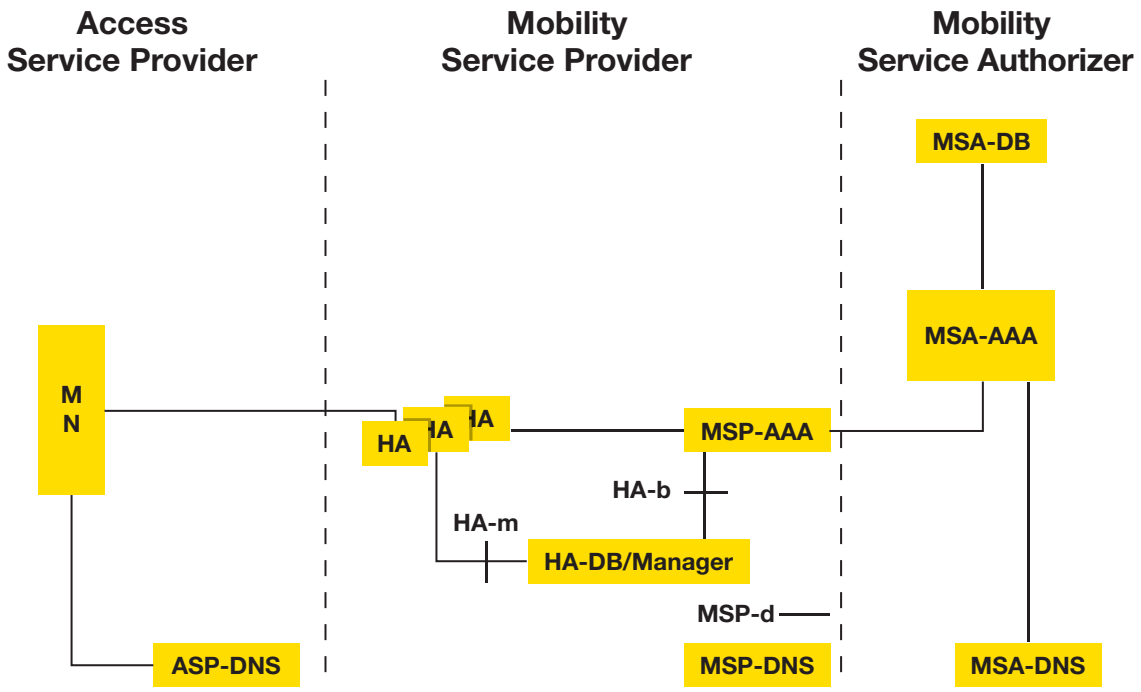
In the split scenario, in which the ASA is a different entity than the MSA, the MN performs initial HA discovery relying on the DNS. For this purpose [3] specifies two alternatives:

- DNS lookup by HA name: using this alternative the MN is configured with the FQDN of the HA. Querying the DNS for this FQDN, the MN will be provided with the IPv6 address of the HA.
- DNS lookup by mobility service name: using this alternative the MN is configured with a DNS entry for the mobility service, using the DNS service resource record (SRV record). Querying the DNS for this mobility service, the MN will be provided with a list of FQDNs of available HAs, from which the MN then could select one and ask for its IPv6 address.

Since in the split scenario the HA is independently discovered by the MN through the DNS and not explicitly assigned by the MSP, HA load sharing is much more difficult to achieve. There is the possibility to dynamically update the DNS entries for the HA FQDNs or the mobility service SRV record, which could be done by the MSP as responsible entity for the HAs. However this comes with certain side-aspects. Firstly, frequent updates of the DNS system would not scale. Furthermore, DNS is affected by a caching latency, that is, until a changed DNS entry gets distributed in the global DNS systems, several hours could easily elapse. Consequently DNS updates intended to reflect a temporary situation on the MSP's HAs make no sense, as until the DNS updates have been distributed, the temporary situation may have changed again, thus the DNS is again 'out of date' concerning the most suitable HA. Therefore DNS updates make only sense for reflecting longer lasting situations on HAs. For example if the MSP plans some maintenance service on a specific HA, this HA could be removed from DNS in advance to avoid new MNs registering with it.

Nevertheless, there is still a possibility to make use of the Home Agent Load Sharing architecture as outlined in section 2.6.5 for the split scenario. In this case the load sharing doesn't happen during the initial assignment of a HA, which is done by means of DNS, but during the later authorisation of the mobility service. For this purpose the proposed Home Agent Load Sharing architecture can be integrated in the split scenario as shown in Figure 2.6.3.

Figure 2.6.3: HA Load Sharing in the Split Scenario



The collection of the selection parameters, the storage of them in the HA database, and the execution of a HA selection algorithm by the MSP-AAA happens identically as within the integrated scenario. The result of the HA load computation could then for example also be used to update the DNS entries from time to time. This could happen via the interface MSP-d, which would run DNS updates as specified in [11].

When now a MN connects to any access network, it first discovers an initial HA based on DNS, and starts then setting up an IKEv2 session with this HA. At this point in time the MN has to authenticate with the HA, which will involve the MSP-AAA. Knowing now the Care-of Address of the registering MN (i.e. the MN's position within the network) and the selected HA, the MSP-AAA can trigger a HA relocation in case this is considered useful to provide better performance to the MN. For this HA relocation a Home Agent Load Sharing as outlined in section 2.6.5 can be used. Alternatively, if instead of IKEv2 an authentication protocol for Mobile IPv6 as specified in [10] is used, the above mentioned optimisation of HA relocation could be done based on this authentication protocol. Within so called HA Switch messages, the existing HA informs the MN about a new, optimized HA it should use in future.

Additionally the authentication of the MN with the HA will also involve the MSA-AAA, which holds the identity and the corresponding service profile of the MN. During this step the MSA-AAA could even decide to select a MSP different from the one initially preconfigured as DNS name on the MN. In this case the MN would be required to repeat the Mobile IPv6 bootstrapping phase with the newly selected MSP, that again could run Home Agent Load Sharing as outlined in section 2.6.5.

Further work will be required in investigating details of these optimisation possibilities for HA relocation with efficient Home Agent Load Sharing support.

2.6.7. CONCLUSION

In order to provide a MIPv6 service in operational networks, the deployment of several HAs along with performing an efficient load sharing between them is one of the key factors. The presented approach fulfills the main requirements listed in chapter 4. The load sharing is under control of the MSP, it is transparent to the MNs, it is independent from any manufacturer while still allowing the integration of manufacturer specific parameters, it doesn't introduce new security issues and its signaling overhead could be adapted to a specific environment by tuning the collection intervals for the selection parameters. The integration with the bootstrapping approach for the integrated scenario can be done in an efficient way. Instead, for making use of the load sharing approach in the split scenario the possibility to perform HA relocation during the mobility service authorisation has been introduced, that is, in the split scenario a HA most likely needs to be assigned twice for load sharing, an initial HA provided by DNS, and possibly a more suitable HA provided during mobility service authorisation. This could be seen as one reason for preferring the integrated scenario. Additionally, the HA Load Sharing approach may also be useful for HA relocation in the integrated scenario, assumed that the MSP-AAA will be involved in the HA relocation process. Here it should be noted, that the topic of HA relocation in general still needs more investigation.

Finally one may need to consider the standardisation of certain selection parameters within an update of the MIPv6 Management Information Base as specified in [15]. The number of active home registrations of a HA will be one candidate for this. Additionally the interfaces between HA and MSP-AAA [17], as well as between MSP-AAA and MSA-AAA may need to be extended in order to transmit the information about the most appropriate HA.

2.6.8. ACKNOWLEDGMENTS

Writing this paper has been partially supported by the European Commission FP6 IST ENABLE project.

2.6.9. REFERENCES

[1] K. Chowdhury, A. Yegin: MIP6-bootstrapping via DHCPv6 for the Integrated Scenario, IETF draft-mip6-bootstrapping-integrated-dhc-01.txt (work in pro-gress), June 2006.

[2] H. Deng, B. Haley, X. Duan, R. Zhang, K. Zhang: Load Balance for Distributed Home Agents in Mobile IPv6, IETF draft-deng-mip6-ha-loadbalance-02.txt (work in progress), October 2004.

[3] G. Giaretta, J. Kempf, V. Devarapalli: Mobile IPv6 bootstrapping in split sce-nario, IETF draft-ietf-mip6-bootstrapping-split-02.txt (work in progress), March 2006.

[4] R. Hinden: Virtual Router Redundancy Protocol for IPv6, IETF draft-ietf-vrrp-ipv6-spec-07.txt (work in progress), September 2004.

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

[6] R. Koodli: Fast Handovers for Mobile IPv6, IETF RFC 4068, July 2005.

[7] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier: Hierarchical Mobile IPv6 Mobility Management (HMIPv6), IETF RFC 4140, August 2005.

[8] R. Wakikawa, P. Thubert, V. Devarapalli: Inter Home Agents Protocol Specifi-cation, IETF draft-wakikawa-mip6-nemo-haha-spec-01.txt (work in progress), March 2006.

[9] A. Patel, G. Giaretta : Problem Statement for bootstrapping Mobile IPv6, IETF draft-ietf-mip6-bootstrap-ps-05.txt (work in progress), May 2006.

[10] A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury: Authentication Protocol for Mobile IPv6, IETF RFC 4285, January 2006.

[11] P. Vixie, S. Thomson, Y. Rekhter, J. Bound: Dynamic Updates in the Domain Name System , IETF RFC 2136, April 1997

[12] J. Hodges, R. Morgan: Lightweight Directory Access Protocol (v3): Technical Specification, IETF RFC 3377, September 2002

[13] J. Case, R. Mundy, D. Partain, B. Steward: Introduction and Applicability Statements for Internet Standard Management Framework, IETF RFC 3410, December 2002

[14] D. Harrington, R. Presuhn, B. Wijnen: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, IETF RFC 3411, December 2002

[15] G. Keeni, K. Koide, K. Nagami, S. Gundavelli: Mobile IPv6 Management Information Base, IETF RFC 4295, June 2006

[16] G. Giaretta, I. Guardini, E. Demaria, J. Bournelle, "MIPv6 authorization and configuration based on EAP", IETF draft-giaretta-mip6-authorization-eap-03.txt (work in progress), March 2006.

[17] G. Giaretta, I. Guardini, E. Demaria, J. Bournelle, R. Lopez, "AAA Goals for Mobile IPv6", IETF draft-ietf-mip6-aaa-ha-goals-03.txt (work in progress), September 2006

2.7 Home Agent and MSP Relocation in operational Mobile IPv6 networks

Wolfgang Fritsche, **IABG**

Michele La Monaca, Ivano Guardini, Elena Demaria
Telecom Italia

ABSTRACT

In the deployment of Mobile IPv6 (MIPv6) in a large mobile operator network, several Home Agents (HAs) may be present and the selection of the "optimal" HA can significantly influence the performance and scalability of the overall MIPv6 service. In this regard, in some scenarios, the efficiency of the MIPv6 service may be improved if the HA currently assigned to a MN is replaced by a more suitable one upon wide area movements of the Mobile Node. The new HA could belong to the same Mobility Service Provider (MSP) of the previous one or to a different one. This paper describes the motivations and scenarios for HA and MSP relocation, and introduces solutions to realise them.

Index Terms: HA Relocation, MSP Relocation, Mobile IPv6

2.7.1. INTRODUCTION

The conditions which determine the quality of mobility service being provided to customers may change over time. For example, a Mobile Node (MN) might bootstrap with an HA in close proximity to its point of attachment and then move far away from there, experiencing higher handover latency and increased delay for traffic transmitted in bi-directional tunneling. As another example, the serving HA might suffer unexpected resource exhaustion due to the failure of one of its interfaces. In order to handle these circumstances, a mechanism to dynamically switch a terminal from one HA to another seems necessary (HA relocation). The new HA may belong to the same or to a different Mobility Service Provider (MSP). The latter case is more precisely referred as "MSP relocation".

The relocation scenario includes different key entities: the Mobile Node (MN), the Mobility Service Authoriser (MSA), the Mobility Service Provider (MSP), the Access Service Authoriser (ASA) and the Access Service Provider (ASP). The roles of these entities are described in [2]. Based on relationships between ASA and MSA two different scenarios can be identified: "split" and "integrated". In case of a split scenario

the ASA and the MSA are separated entities. A typical case is a mobile node that gets opportunistic connectivity from a hotspot but relies on a third party for global mobility. In an integrated scenario, MSA and ASA are the same entity, called MASA (Mobility and Access Service Authorizer). A common case of integrated scenario arises when the user has subscribed with a mobile operator that typically provides both network access and mobility service. [3] and [4] describe in more detail these scenarios, with a focus on the bootstrapping phase. Any HA and MSP relocation mechanism has to fit with both these bootstrapping scenarios. In the following sections we analyse the motivations and scenarios for HA and MSP relocation and provide a solution suitable for both.

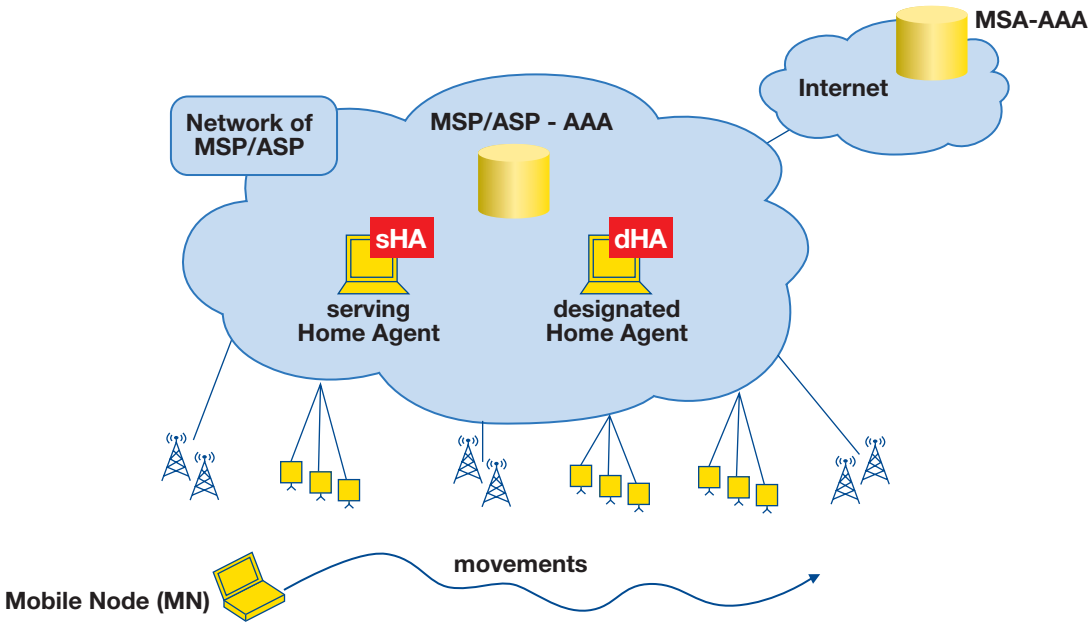
2.7.2. HA RELOCATION

2.7.2.1. Definition and motivations

Technically, HA relocation is a set of procedures intended to allow a MN to dynamically switch from one HA to another. The motivations behind such operation can be different, the most obvious being better usage of MSP resources (e.g. through load balancing), smooth handling of HAs maintenance, provisioning of a more "favorable" HA to the MN. Furthermore, each MSP can implement its own set of policies and rules for decisions when relocating a MN.

Probably, one of the most useful applications of HA relocation occurs when the MSP is also acting as Access Service Provider (ASP). In this case, the MSP AAA server has a clear knowledge about the location of the MN in relation to the location of available HAs and therefore can decide when HA relocation can provide relevant benefits based on topological considerations (see Figure 2.7.1).

Figure 2.7.1: HA relocation



In the HA relocation procedure two HAs are involved: the HA that already serves the MN, named serving HA (sHA), and the new HA to be assigned to the MN, named designated HA (dHA). The two HAs can be located in the same IP subnet or may serve different IP subnets. The former case allows the MN to maintain its already configured Home Address (HoA) also after registering with the designated HA.

HA relocation can be decided and undertaken at any moment. Nevertheless, it is useful to treat the relocation performed at bootstrap time separately since it is somewhat a special case and applies only to selected scenarios. Therefore we distinguish two kinds of relocation:

1. **HA relocation at initial state.** The MSP decides to relocate a MN before it starts using the first allocated HA. This kind of relocation applies only to the split scenario, where the HA obtained at bootstrap time may turn out to be sub-optimal, being discovered by the MN via DNS and not explicitly assigned by the MSP. In the split scenario the HA relocation procedure allows us to achieve fine grained HA selection by redirecting the MN to an alternative HA that is more convenient than the one initially discovered via DNS by the MN itself.
2. **HA relocation at a later state.** The MSP decides to relocate a MN which already has registered with a HA and possibly has active connections routed through that HA.

2.7.2.2. Relocation triggers and scenarios

The entity which controls HA relocation is the MSP since only the MSP knows the status of the mobility service being offered and can therefore properly decide whether or not to redirect the MN to a "better" HA. The envisioned factors which may trigger a relocation procedure are the following:

- Assignment of a closer HA. When working also as ASP, the MSP may decide to move a certain MN to a HA topologically closer to its current point of attachment.
- Assignment of a QoS enabled HA. An operator may want to reallocate a MN asking for real-time services, like voice for example, to QoS aware HAs.
- Assignment of a less loaded HA. The MSP may decide to redirect a MN to a less loaded HA in case the serving HA gets overloaded (e.g. the bandwidth consumption on the HA goes beyond a certain threshold).
- Upcoming maintenance of the serving HA. The MSP may stop assigning newly bootstrapped MNs to an HA scheduled for maintenance and gradually move all the already registered MNs to one or more alternative HAs.

It should be noted that each trigger may only be relevant for specific scenarios. For example, since the load-sharing mechanisms implemented by the MSP and applied during bootstrapping should prevent HAs to get overloaded, the load of a HA may not be a frequently used trigger at a later state.

2.7.2.3. Description of the solution

In the design of the solution, the basic assumption has been that the initiator of the HA relocation procedure is the AAA server of the MSP, that is responsible for deciding if HA relocation is actually necessary. Although this check can be performed at any time, as a design choice the actual relocation procedure takes place during MIPv6 authorisation and re-authorisation events, that is, when the HA actually asks the MSA-AAA server for authorisation to provide the mobility service. For that reason, an operator has to carefully choose re-authorisation timeouts since excessive authorisation lifetimes would undermine the usefulness of relocation as the actual execution of the relocation might face long delays.

The algorithms used to verify the opportunity of a HA relocation and the selection of the proper dHA may be cumbersome, especially if they take into account the load of any single HA in the network. Based on this consideration, it is useful to split the relocation algorithm in two parts. The first part runs asynchronously with respect to bootstrapping and re-authorisation events, estimates the load of each HA and caches the results. The second part is executed by the MSP-AAA server at any re-authorisation event, to decide if HA relocation for a specific MN is convenient based on the topological position of the MN and the status of the network as stored in the local cache. This procedure reducing the computation time, making it actually feasible to perform the relocation check during re-authorisation events, taking into account both the HA load and the MN's position.

Basically the HA relocation procedure involves four steps:

1. **Relocation decision.** During a MIPv6 (re-)authorisation event the MSP-AAA server checks if relocation for a specific user applies and picks the designated HA.
2. **Authorisation and notification.** The decision of the MSP-AAA server on relocation is notified to the user's sHA along with the information on the dHA (e.g. the IPv6 address); the sHA delivers this information to the MN.
3. **Switch to the dHA.** The MN bootstraps with the dHA, i.e. it gets the new HoA (if dHA and sHA are on different subnets) and establishes a new Security Association (SA). From the dHA point of view the MN is a fresh bootstrapped node and no special handling is needed.
4. **HoA change management.** If the HA relocation happens at a later state and involves a HoA change, proper management of the two HoAs is needed to handle on-going sessions seamlessly (see section 2.7.4).

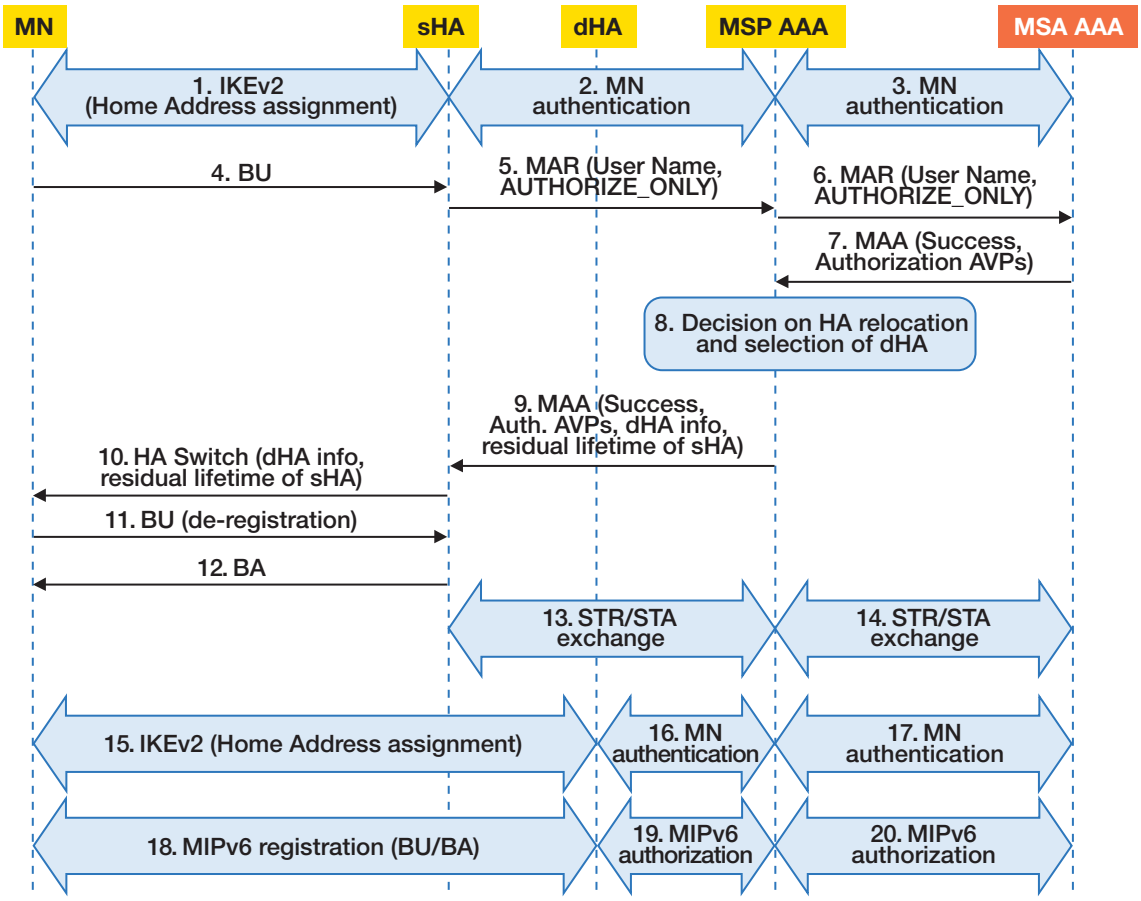
Besides the typical messages used during bootstrapping phase, HA relocation mainly requires that the MSP-AAA server delivers additional parameters to HA and MN. This is done through the MIP6 Diameter Application [7] and the HA Switch message [5] specified by the HA reliability design team of the IETF MIP6 working group. The detailed message exchange occurring during HA relocation at initial state* is depicted in Figure 2.7.2 and described in the following:

- **Steps 1-3.** MN authenticates with sHA and receives an HoA during the IKEv2 exchange.
- **Step 4.** MN sends the first BU to the sHA.
- **Steps 5, 6.** To verify if the MN is actually authorised to run the mobility service, the HA sends a MIPv6 Authorisation Request (MAR), that is routed to the MSA-AAA server through the MSP-AAA server.
- **Steps 7, 8.** At the reception of a successful MIPv6 Authorisation Answer (MAA), the MSP-AAA server verifies if HA relocation is necessary.
- **Step 9.** If HA relocation applies, the MSP-AAA server inserts the dHA address (or FQDN) in the MAA message forwarded to the sHA. Furthermore, another parameter is inserted to notify the residual lifetime of the sHA. It represents the maximum period of time during which the MN is authorised to remain registered with sHA. Since in the example HA relocation happens at initial state this lifetime is set to zero, thus forcing the MN to immediately release the sHA.

* The message exchange regarding the relocation at a later state is quite similar. The main difference is that the MN is allowed to register with both dHA and sHA for some time (specified in an appropriate parameter). Section 2.7.4 describes the management of the two HoA.

- **Steps 10 to 12.** sHA sends an HA Switch message [5] to the MN with the residual lifetime set to zero. The MN confirms the reception of such message replying with a de-registration BU. The HA acknowledges the BU with a BA.
- **Steps 13, 14.** The exchange of Session Termination Request (STR) and Session Termination Answer (STA) messages is triggered by the sHA to notify that the user session is terminated.
- **Steps 15 to 20.** MN starts the mobility service with new dHA in the usual way.

Figure 2.7.2: HA relocation procedure at initial state



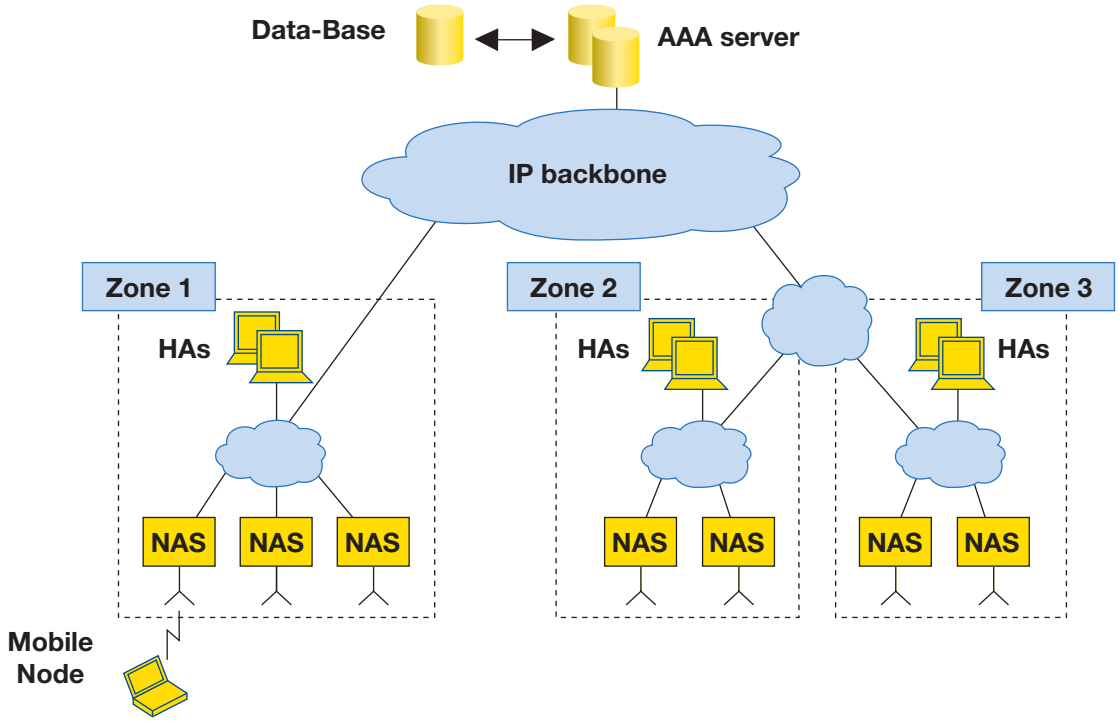
The HA switch message in step 10 is used by the HA both to signal to the MN that it must undergo a HA relocation and to deliver the information on the dHA. An alternative method to deliver this information could be based on IKEv2.

2.7.2.4 Relocation Policies

As already pointed out, the policies implemented for HA relocation are operator specific. Nevertheless, it is worth providing examples of how such policies may look like. In this section, as an example, a decision algorithm based on topological distance is provided. Decisions based on other parameters are also possible.

When acting also as ASP, the MSP has a clear knowledge about the location of the MN in relation to the location of available HAs. In this scenario the MSP-AAA server has the possibility to combine these two kinds of information in order to provide a closer HA to the MN. For that purpose, the access network is split in "zones", with each HA and each NAS being assigned to one of such zones (Figure 2.7.3).

Figure 2.7.3: HA relocation procedure at initial state



Furthermore, an administrative metric, namely the inter-zone metric (izm), is defined between zones. A symmetric matrix can be used to describe this metric as shown in Figure 2.7.4.

If $Zone_{visited}$ denotes the network zone visited by MN and $Zone_{HA}$ the zone in which the sHA of the MN is located, then, based on the distance between $Zone_{visited}$ and $Zone_{HA}$, a decision algorithm (1) could be defined as follows:

$$izm\ (Zone_{visited} - Zone_{HA}) = \begin{cases} 2 \Rightarrow \text{mandator} \\ 1 \Rightarrow \text{opcional} \\ 0 \Rightarrow \text{not needed} \end{cases}$$

In case of optional relocation the decision can be based on other parameters (e.g. load of the HA).

Figure 2.7.4: Inter-zone metric

Zone ID	1	2	3
1	0	1	2
2	1	0	1
3	2	1	0

In order to implement this kind of policy, the ASP/MSP must be able to track the topological position within the access network of any MN registered with one of its HAs. This can be easily done based on the knowledge of the MN's CoA, from which the MSP AAA can derive the identity of the NAS that is currently serving the MN. For that purpose, the HA must notify to the MSP-AAA server the MN's CoA, inserting this information in the MIPv6 Authorisation Requests (MAR). However, a movement (i.e. change of CoA) must not trigger a MAR/MAA exchange, since that would affect handover latency negatively. Instead, MAR messages are delivered at the expiration of the authorisation lifetime as usual.

An alternative approach, applicable only in the integrated scenario, is that the ASP/MSP AAA server derives the location of the MN (i.e. the NAS) from network access authentication or re-authentication events. This requires that the MN uses the same identity when authenticating for network access and mobility service. However, when a user is roaming, it might want to hide its real identity for privacy reasons making use of different pseudonyms for different services. To make the ASP/MSP always able to link MN's identities it suffices that the MASA, when authenticating a user on an HA, delivers to the ASP/MSP AAA server the pseudonym used for network access. In this way, the two identities can be easily correlated and it can be decided if relocation is needed.

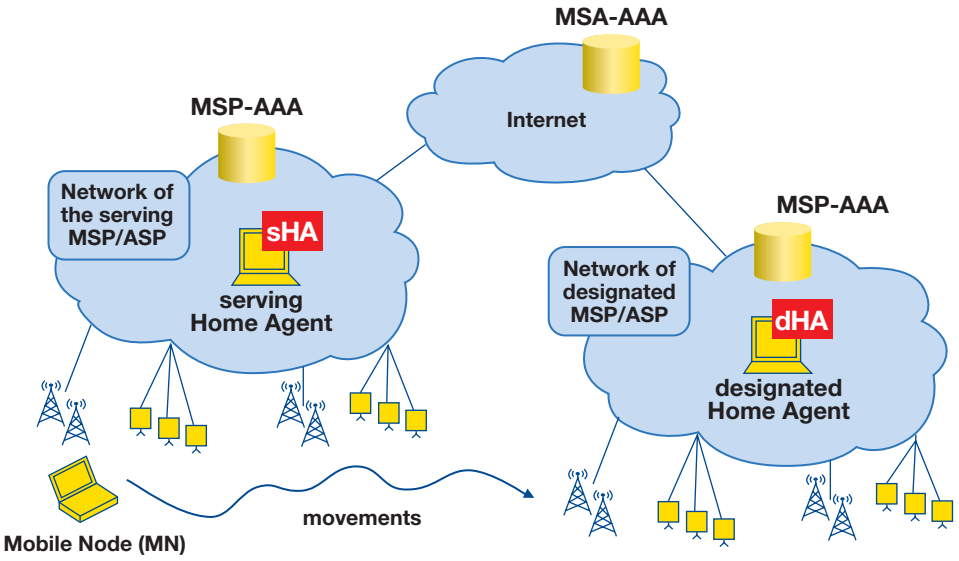
2.7.3. MSP RELOCATION

2.7.3.1. Definition and motivations

MSPs relocation is the process of assigning a new MSP to a MN. The reason for this usually is that a new, designated MSP (dMSP) is better suited to serve a certain MN than the currently serving MSP (sMSP). The most notable reason for performing MSP relocation is certainly to assign a MSP closer to the MN's point of attachment, that is, to assign the MSP role for a certain MN to the MN's ASP. With this approach local HAs in the access network can be assigned to the MN, which brings the benefit of having a local mobility anchor, and consequently avoids sending signaling information throughout the whole network and thereby causing unwanted delay during handover. Figure 2.7.5 illustrates the process of MSP relocation.

As the MSA handles MN subscription profile, it is also up to the MSA to decide if MSP relocation should be performed, and which new MSP should be assigned to the MN. The MSA needs to maintain a peering to each third party MSP it is assigning to the MN in the process of MSP relocation.

Figure 2.7.5: MSP relocation



Obviously MSP relocation causes automatically also a HA relocation. However, during HA relocation sHA and dHA belong to the same MSP, during MSP relocation sHA and dHA belong to different MSPs, precisely to sMSP and dMSP. Nonetheless, and also in this case it is necessary that the HA relocation is performed as smooth as possible for the MN. Consequently during MSP relocation the MN is also allowed to keep two sets of HA/HoA for a restricted time.

For the unlikely case that a MSP relocation happens simultaneously with a HA relocation, the MSP relocation controlled by the MSA will overrule the HA relocation. This means that first the assignment of a new MSP will be completed and after that the new MSP may decide to perform HA relocation.

2.7.3.2. Relocation triggers and scenarios

As already outlined above, the motivation for MSP relocation is the assignment of local HAs. Based on this, a MSP relocation scenario comprises the following phases:

- First the MN has to detect that it has moved into a new ASP's network.
- The ASP then signals to the MSA its ability to act as MSP, providing its own local HAs to the MN.
- The MSA has to decide whether the HAs provided by the new ASP are closer to the MN than the HAs provided by the previous ASP. Usually this should be the case.
- If this is the case, the MSA will initiate HA provision by the new ASP, and thereby relocate the MSP functionality.

In order to detect that the MN has moved into a new access network, the MSA also has to act as ASA, that is, an integrated scenario must be deployed. Furthermore, local HA assignment at initial state can be done as part of the usual bootstrapping process, so MSP relocation is only required to provide local HA assignment at later state within the integrated scenario.

2.7.3.3. Description of the solution

Contrary to HA relocation, the MSA-AAA server is responsible for deciding if MSP relocation is actually necessary. This decision is performed during network access authentication events, as this is the only time a MN can roam to a new ASP.

Basically, the MSP relocation procedure involves the same four functional steps as described already for HA relocation; however, the detailed messages and the signalling paths are different:

1. Relocation decision. During a network access authorisation event the MSA-AAA server decides if relocation for a specific MN applies and selects the designated MSP.

2. Authorisation and notification. The MSA-AAA server's decision about the MSP relocation has to be notified to the MN. This happens via the MN's sHA, this delivers DNS information about the designated MSP (dMSP) and the remaining time the sHA at the sMSP can be continued to be used for existing connections. In order to notify the sHA, the MSA will use a new AAA message, the MIPv6-Authorisation-Change-Request. In order to notify the MN, the sHA will use the existing HA Switch message. Through a Binding Update, the MN confirms the successful receipt of the HA Switch message. This is further confirmed back to the MSA within a new AAA message, the MIPv6-Authorisation-Change-Answer.

3. Switch to the dHA. The MN needs to bootstrap with the dHA. Information about the dHA is obtained by the MN by performing a DNS lookup for the dMSP's FQDN provided as part of the HA Switch message. From the dHA point of view the MN is a fresh bootstrapped node and no special handling is needed. This illustrates again how MSP relocation naturally causes also a HA relocation.

4. HoA change management. As with MSP relocation obviously sHA and dHA are located in different subnets, it consequently involves a HoA change at the MN. Therefore, proper management of the two HoAs, as described in section 2.7.4 is needed in order not to disrupt on-going sessions.

2.7.3.4. Relocation Policies

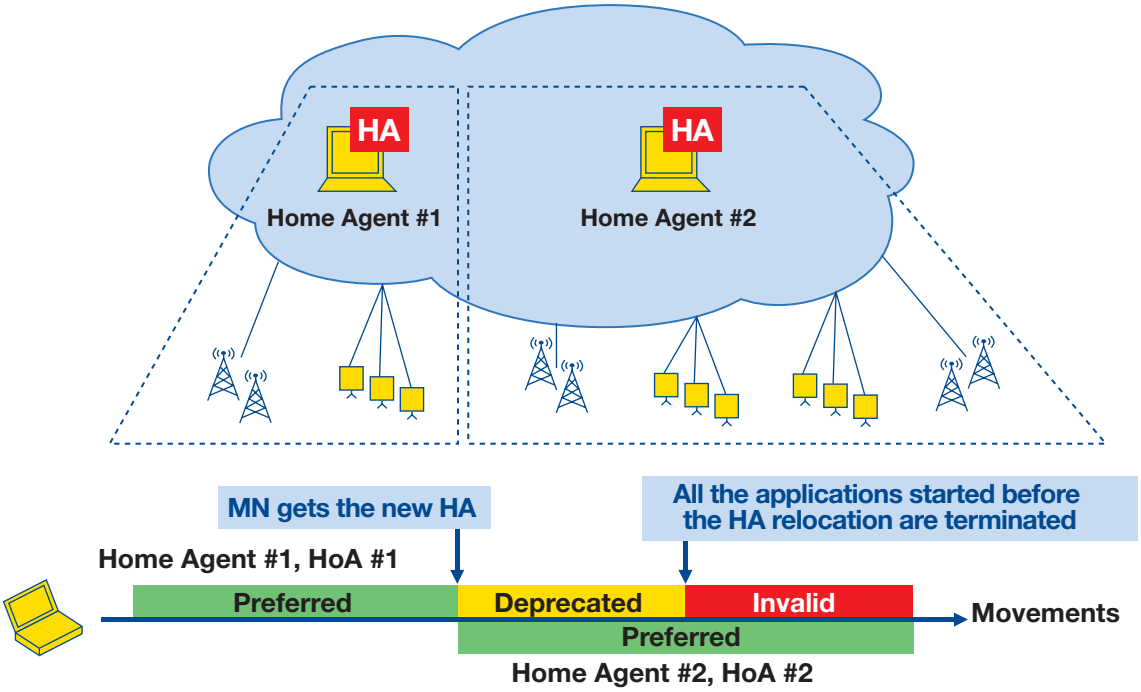
As already stated, MSP relocation is only triggered for ensuring that the MN keeps a local HA even when moving across different access domains.

In case a MN now moves into a new ASP network, which also would offer mobility services as MSP, but the sHA for the MN remains located within the old ASP's network, a local HA assignment is no longer given. Therefore, at the time the MN undertakes authentication of the network access service, the MSA will recognise that the new ASP is a different entity as the old ASP, and that it could provide also the mobility support service. Consequently the MSA could decide for performing MSP relocation.

2.7.4. MANAGEMENT OF HoA CHANGES

When relocation happens at a later state, MNs are likely to have active sessions bound to the old HoA. In order to avoid dropping these communications abruptly, MNs are allowed to maintain the old HoA for some time (i.e. residual lifetime of sHA). This mechanism, depicted in Figure 2.7.6, is similar to the one described in [6] which gracefully handles the expiration of address lifetimes.

Figure 2.7.6: HoA change management



After a MN registers with a new HA (#2) and configures a new HoA (#2), HoA #1 should become deprecated, and therefore shouldn't be further used for new communications. After the expiration of the residual lifetime, HoA #1 should become invalid and definitely released by the MN.

2.7.5. SUPPORT FOR LEGACY TERMINALS

HA and MSP relocations are optional features that may not be supported by legacy terminals; therefore if a terminal does not implement such feature, it should not be forced in a relocation procedure, which eventually would break its mobility service. A couple of approaches are possible (not mutually exclusive):

- Proactive. The mobile terminal explicitly notifies HA/MSP relocation support, inserting a new mobility option in the BUs. Legacy terminals, that don't notify this support, are then not forced to relocate.
- Reactive. Since the MN is informed of the HA/MSP relocation through a new mobility header type, a Binding Error [1] will be issued by the MN to the HA if it doesn't support HA/MSP relocation and hence doesn't recognise the header. This approach implies that at least one HA/MSP relocation procedure will be tried.

In both cases, the HA must accordingly inform the MSP-AAA server, otherwise the server would uselessly run instances of the relocation decision algorithm.

2.7.6. CONCLUSION

HA and MSP relocation are important features to increase the efficiency of the mobility support service. Both of them cause a MN being assigned to a new designated HA, which is either administrated by the same MSP as the old serving HA (HA relocation) or by a new MSP (MSP relocation).

The relocation can be triggered due to different motivations; one of them is definitely the assignment of local HAs. While HA relocation will be initiated by the MSP, MSP relocation will be initiated by the MN's MSA. In the unlikely case that HA and MSP relocation happens simultaneously, MSP relocation will overrule HA relocation.

The solutions for HA and MSP relocation presented in this paper makes mainly use of extensions to the MIP6 Diameter Application and of the HA Switch message specified by the HA reliability design team of the MIP6 working group. The solutions are designed in a way that legacy terminals without HA and MSP relocation support are not affected.

2.7.7. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, IETF RFC 3775, June 2004.

[2] Patel et. al., "Problem Statement for Bootstrapping Mobile IPv6", RFC 4640, September 2006.

[3] G. Giaretta, J. Kempf, V. Devarapalli, Mobile IPv6 bootstrapping in split scenario, draft-ietf-mip6-bootstrapping-split-04 (work in progress), December 2006.

[4] K. Chowdhury, A. Yegin, “MIP6-bootstrapping via DHCPv6 for the Integrated Scenario”, draft-ietf-mip6-bootstrapping-integrated-dhc-01 (work in progress), June 2006.

[5] B. Haley, V. Devarapalli, H. Deng, J. Kempf, “Mobility Header Home Agent Switch Message”, draft-ietf-mip6-ha-switch-02 (work in progress), December 2006.

[6] S. Thomson, T. Narten, " IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[7] J. Bournelle, G. Giaretta, H. Tschofenig, M. Nakhjiri, “Diameter Mobile IPv6: HA-to-AAAH support”, draft-ietf-dime-mip6-split-01 (work in progress), October 2006.

2.8 E²T: End-to-End Tunnelling Extension to Mobile IPv6

Deguang Le, Xiaoming Fu, and Dieter Hogrefe
University of Göttingen

ABSTRACT

In the standard Mobile IPv6 (MIPv6), bidirectional tunnelling through the home agent or route optimization show inefficiency in per-packet routing, especially when both communicating endpoints are mobile. To be scalable and compatible, mobile devices' packets should be routed efficiently with minimal changes to the network infrastructure. However, the current solutions do not provide any means for the end systems to perform optimized packet routing during the operation of the mobile devices. In this paper, we present an end-to-end tunnelling extension to MIPv6 (E²T) for mobile routing packets, which reduces the per-packet routing cost for the communications of mobile devices through the lower packet routing overhead. Besides, our approach requires little change to MIPv6, but allows the more efficient routing behavior with the shorter end-to-end transmission latency between communicating endpoints. The simulation results show our approach is suitable for real-time multimedia applications.

2.8.1. INTRODUCTION

With the fast evolution of mobile communication and Internet technology, there is a strong need to provide connectivity for moving devices to communicate with other devices on the Internet. Internet mobility support has been a hot topic in the past decade, and studies that address this issue have arisen, coming up with a number of protocol proposals and schemes [1]. Among them, MIPv6 [2] as the most mature solution has been supported and adopted by mobile devices and network equipment vendors [3], and some of the network providers are even starting to deploy MIPv6 networks [4].

MIPv6 allows a Mobile Node (MN) to communicate with a Correspondent Node (CN) at any time and any place. Fundamentally, MIPv6 consists of four functional blocks [2]: movement detection, Care of Address (CoA) configuration, (home or correspondent) registration, and packet routing. In [5], [6], [7], several enhancement schemes have been proposed for the former 3 aspects. However, to the best of our knowledge, there is little effort in improving the efficiency of mobile routing for the MN's data packets. We believe that

efficient mobile routing is necessary to fully exploit the potential of mobility enabled on the future Internet. At the network layer, the traditional mobile routing mechanism is realized by employing tunnelling [8], the so called Bidirectional Tunnelling (BT) [2] in MIPv6. However, the BT forces all packets for a MN to be routed through its Home Agent (HA). Thus, packets to the MN are often routed along paths that are significantly longer than optimal ones [9]. Hence, the Route Optimization (RO) [2] was developed beside the traditional BT. The RO enables routing packets directly to the MN's CoA, which allows the shortest communication path to be used. It also eliminates the congestion at the MN's home link and HA. However, in the RO, the MN needs to not only register its CoA to the HA, but also update binding to the CN, which suffers from greater control traffic. In addition, it relies on the Routing and Destination Option extension headers for packet routing, which is an extra overhead.

Some improvements have been suggested to the standard RO mechanism. Vogt proposed proactive tests in [10], where the procedure of address tests in the standard RO can be done proactively. Perkins [11] presented a RO security enhancement mechanism between the MN and CN by pre-configuring data useful for precomputing a binding management key that can subsequently be used for authorizing binding updates. In [12], Bao et al. suggested that one of the HA's functions act as security proxy for its mobile nodes. The authentication is based on the HA's certificate and the secret session keys are generated by strong cryptosystems, which avoids many security obstacles in the return routability mechanism. These proposals focus on the security enhancements to the return routability and correspondent registration procedures based on the RO, but the issue of signaling optimization for efficient packet routing is still not tackled. This will however be covered in our work.

Moreover, the prosperous development of mobile Internet together with the enormous growth of mobile users has resulted in a strong trend that there are more and more communicating endpoints, both of which are mobile on the Internet [13]. The scenario of communications between mobile users directly will be ubiquitous on the future mobile Internet. Therefore, in this paper, we investigate the performance of mobility routing mechanisms in more common mobile scenario, where communicating endpoints are mobile, and point out their strengths and weaknesses. In terms of the perspective of routing performance in mobile environments, we provide an alternative routing enhancement mechanism based on an end-to-end tunnelling extension to MIPv6 (E^2T) for data packet routing. The approach has the advantages of the optimal end-to-end traffic delay as well as the reduced overhead. The simulation evaluation shows our approach has better routing performance against the current routing mechanisms, especially for real-time multimedia applications.

The remaining part of this paper is organized as follows: In Section 2.8.2, we describe the mobile routing mechanisms as specified in MIPv6 and formulize the problems of the standard routing mechanisms. Then, the objectives for routing enhancement are discussed. Section 2.8.3 presents our approach, including the E^2T protocol architecture, adaptive tunnel setup, data packet routing and security considerations. The evaluation of the proposed E^2T mechanism is given in Section 2.8.4. Finally we draw our conclusions and the future work in Section 2.8.5.

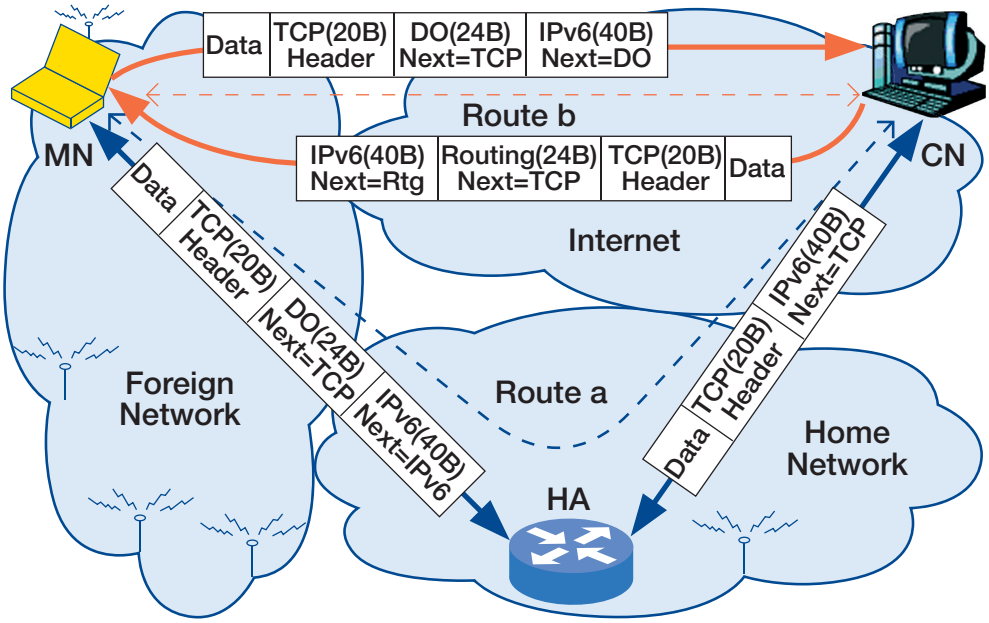
2.8.2. STANDARD MIPV6 ROUTING MECHANISMS AND THEIR PROBLEMS

In this Section, starting with a presentation of the standard MIPv6 routing mechanisms, we reveal their problems. Then, we discuss the objectives for routing enhancement.

2.8.2.1 Mobile Packet Routing Mechanisms in MIPv6

In order for communicating endpoints (i.e. the MN and CN) to trace and route packets to each other continuously even while moving, MIPv6 specifies two mobile routing mechanisms for packet transmission between the MN and CN: the BT and RO. Figure 2.8.1 illustrates the mobile routing mechanisms in MIPv6.

Figure 2.8.1: The mobile packet routing mechanisms in MIPv6



In the BT, packets from the CN to MN are routed to the home address of the MN, the HA shall use the proxy neighbour discovery [14] to intercept any IPv6 packets addressed to the MN's home address on the home network. Each intercepted packet is tunnelled to the MN's current CoA [8]. Packets to the CN are tunnelled from the MN to the HA, which is called the reverse tunnelling [15], and then routed normally from the home network to the CN (see figure 2.8.1, Route a).

In the RO, the HA no longer exclusively deals with the address mapping, but each CN can have its own binding cache. In the direction from the MN to CN, packets sent by the MN are delivered to the CN with the Home Address option in the Destination Option Extension header when the MN is away from its home network. In this case, the MN sets the IPv6 header's source address to its CoA and adds a Home Address option with the MN's home address to the IPv6 header. In the opposite direction, when sending packets to the MN, the CN checks its cached bindings for an entry for the packets' destination address. If a cached binding entry for this destination address is found, the CN uses the Type 2 Routing header to route packets to the MN by specifying the CoA as the destination address in the IPv6 header and the MN's home address as the final destination in the Type 2 Routing header (see figure 2.8.1, Route b).

2.8.2.2 Problems of Standard Routing Mechanisms

As described in the previous subsection, the RO as well as BT specifies messages and extension headers to the basic protocol for mobile packet routing between the MN and CN. This subsection will investigate the effect of the standard MIPv6 routing mechanisms on performance.

The overhead is a critical issue in wireless environments, where the spectrum is a scarce resource and must be used with care. In the RO, when the MN wishes to let the CN communicate directly with it in its visiting location, the CN sends the packet with a Type 2 Routing header. The corresponding packet from the MN to CN utilizes a Home Address option. When both the MN and CN are away from their home networks, packets delivered between the MN and CN need additional messages of both the Type 2 Routing header and the Destination Option extension header for correct functioning of routing. Therefore, the use of this direct data path incurs the cost of both Routing header and Home Address options in each direction, whereas the BT employs the tunnel header for packet forwarding between the MN and the HA, which suffers from the overhead of tunnel header [16].

The end-to-end traffic delay is also directly affected by the MIPv6 routing mechanisms. We assume that the two routing mechanisms are applied under the same Internet status including the same process time of routers and the same delay of link etc., so the traffic delay between two endpoints that are on the Internet mainly depends on the delivery distance. Then, from figure 2.8.1, we can see that the distance between the MN and HA plus the distance between the HA and CN is longer than the distance between the MN and CN. Therefore, the end-to-end traffic delay with the RO is reduced compared to the case using the BT.

2.8.2.3 Objectives for Routing Enhancement

The motivation behind the enhancement of the mobile routing mechanisms is to improve the delivery of IP-based multimedia data over MIPv6, which requires properties of the low transmission delay, the high wireless bandwidth utilization and the scalability. In recent years, multimedia applications like Voice over IP (VoIP), video conferencing and networked music are gaining momentum on the mobile Internet. Its traffic mix is subject to dramatic changes due to the ever-increasing proportion of packetswitch multimedia contents. Such applications are well recognized as delay sensitive and resource demanding. Therefore, any efforts that help to reduce the delay at any point from end to end will be much appreciated. Besides, since in wireless environments, the radio link is typically constrained in bandwidth, a better mobile routing approach with less overhead is obviously critical to the high bandwidth utilization and scalability, in particular, with the increase of the traffic volume.

Therefore, the need of the optimal end-to-end traffic delay as well as routing overhead turns out to be increasingly important, which is thus the objectives for routing enhancement in this paper.

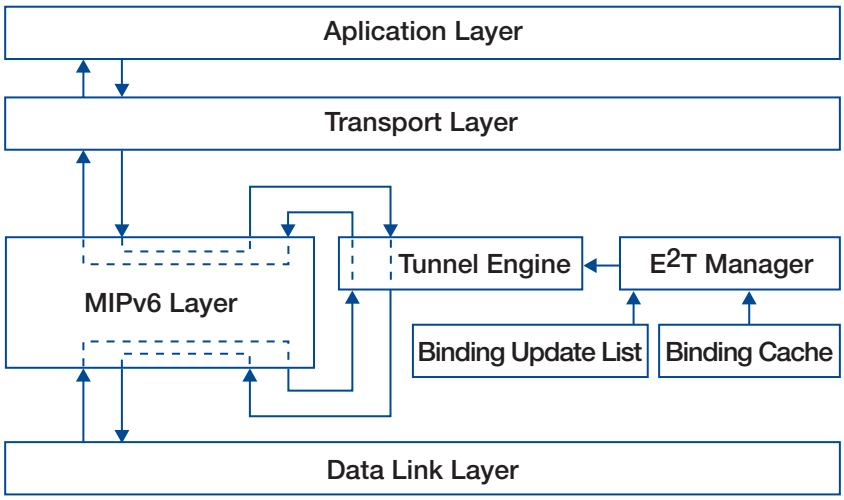
2.8.3. E²T: END-TO-END TUNNELLING EXTENSION TO MOBILE IPV6

Motivated by these objectives, we present an E²T mechanism between the MN and CN. We propose to use a tunnel header to replace the Home Address option and Type 2 Routing header when both of the MN and CN are in the foreign networks.

2.8.3.1 Protocol Architecture for E²T at Endpoints

To support the use of the E²T mechanism, IPv6 encapsulation must be implemented at the MN and CN, namely they both act as the tunnel endpoints (i.e. the tunnel entry-endpoint and tunnel exit-endpoint). In addition, we extend the IPv6 tunnel engine [8] with a E²T manager. Figure 2.8.2 shows the architecture for E²T at the endpoints.

Figure 2.8.2: The architecture for E²T at the endpoints



Here, the E²T Manager module implements the configured tunnel depending on the information of Binding Update List (BUL) and Binding Cache (BC) and invokes the tunnel engine based on the configured tunnel. The Tunnel Engine module processes the data packets by performing the encapsulation or decapsulation according to the configured tunnel [8].

2.8.3.2 Adaptive Tunnel Setup

Because the proposed E²T is an extension to MIPv6 and acts as an alternative beside the current routing mechanisms (i.e. the BT and RO), especially for the scenario where the communicating endpoints are mobile, for compatibility and adaptability, the endpoints should distinguish the standard routing mechanisms from the E²T, so that it can adaptively decide whether to route packets to the CoA directly by the standard routing mechanisms or to use the E²T, depending on the moving scenarios.

For adaptive tunnel setup, before the entry-endpoint sends any packet, the E²T examines the BUL and BC for an entry for the destination address, to which the packet is being sent. If the entryendpoint has both a BC entry and a BUL entry for this destination address, it configures the CoA of the destination address in the entry as the tunnel exit-endpoint address and enables the tunnel engine perform the encapsulation procedure. Otherwise, if the entry-endpoint has no a BUL entry or BC entry for the destination address, the entry-endpoint does not create a tunnel exit-endpoint at the entry-endpoint, and the entry-endpoint simply sends the packet normally, with standard routing mechanisms.

2.8.3.3 Data Packets Routing

After establishing a configured tunnel between the MN and CN, data packets sent between the MN and CN will be routed through the "virtual route" represented by the configured tunnel using the IPv6 encapsulation/decapsulation [8].

IPv6 encapsulation consists of prepending an IPv6 header to the original packet, which is called tunnel IPv6 header. The encapsulation takes place in an IPv6 tunnel entry-endpoint, as the result of an original packet being forwarded into the "virtual route". The original packet is processed during forwarding by decrementing the IPv6 original header hop limit by one.

When the MN encapsulates the packet for delivery to the CN, the MN sets the source address field in the new tunnel IPv6 header to the MN's CoA and sets the destination address field in the tunnel IPv6 header to the CN's CoA (see Figure 2.8.3). When the packet is received at the CN, the encapsulation will be stripped away, yielding the original IP packet, whose payload is then delivered to the upper layer protocols of the CN, and finally processed by the upper layer protocols as if it had been routed to the CN's home address.

Figure 2.8.3: The IPv6 headers in E^{2}T tunneled packets

Similarly, at the CN, in order to send the packet to the MN, the source field of the tunnel IPv6 header is filled with the CN's CoA and the destination field with the MN's CoA for encapsulation. Subsequently, the tunnel packet resulting from encapsulation is routed towards the MN. Upon receiving a packet destined to the MN, the tunnel protocol engine discards the tunnel header and passes the resulting original packet to the IPv6 protocol layer for further processing.

2.8.3.4 Security Considerations

The extension proposed in this paper is subject to the security considerations presented in MIPv6 [2]. For authenticity, the endpoint needs to insure that the encapsulating packet comes from an authentically identified, trusted source. The authenticity of the source could be obtained by the return routability check.

By using the CoA as the source address in the tunnel header, with the MN's home address instead in the original packet header, the packet will be able to safely pass through any router implementing ingress filtering [17].

Besides, for a secure IPv6 tunnel, an E^{2}T tunnel itself can be secured by securing the IPv6 path between the tunnel endpoints (i.e the MN and CN) based on [18], [19], [20]. The degree of integrity, authentication, confidentiality, and the security processing performed on a tunnel packet at the MN and CN of a secure E^{2}T tunnel depend on the type of security headers: the Authentication Header (AH) [18] or the Encapsulating Security Payload (ESP) [19] header, and parameters configured in the Security Association (SA) [20] for the tunnel. There is no dependency or interaction between the security level and mechanisms applied to the tunnel packets.

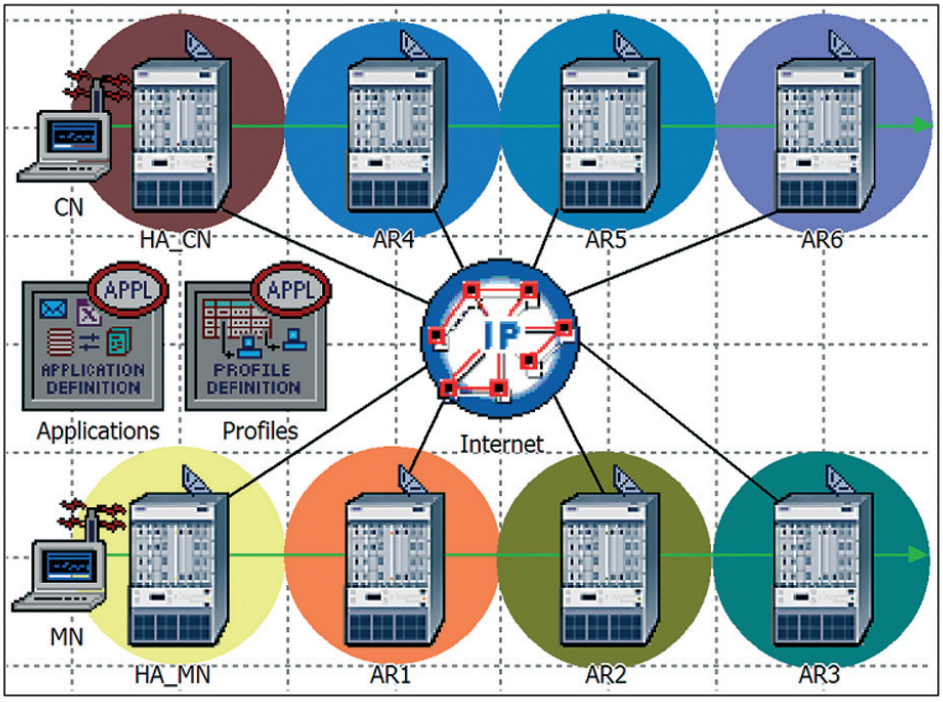
2.8.4. SIMULATIONS AND EVALUATIONS

In this section, we evaluate the performance of the proposed routing mechanism through simulation using the OPNET simulator [21]. The simulation models are built by incorporating the proposed routing mechanism into the standard MIPv6 model [22]. The simulation results demonstrate how the enhancement of routing performance can be achieved in our approach.

2.8.4.1 Simulation Setup

Without loss of generality, we design the scenario, where the communicating endpoints on the mobile Internet are point to point. That is to say, the connection may be originated at any one endpoint to another, and either can be mobile. The simulation network model, depicted in figure 2.8.4, is composed of the IP cloud model, Access Routers (ARs), and communicating endpoints (i.e the MN and CN). The IP cloud model represents the Internet, through which the IP traffic can be modelled. ARs represent wireless access networks, among which the ARs of the HA (i.e. HAMN and HACN) act as the home networks with home agent function and other ARs (i.e. AR1-AR6) act as foreign networks. Each AR consists of two interfaces, among which the wireless interface supporting IEEE 802.11b [23] provides Internet access for mobile endpoints and the wired interface is connected to the Internet IP model through wired 100Mbps duplex link with 10ms delay. The AR provides a coverage area with a radius of approximately 300 meters. The MN and CN are mobile and they move within the coverage area of the ARs.

Figure 2.8.4: The simulation network model



2.8.4.2 Simulation Results and Evaluations

In this subsection, we evaluate our approach through measuring the performance metrics of the overhead and end-to-end traffic delay.

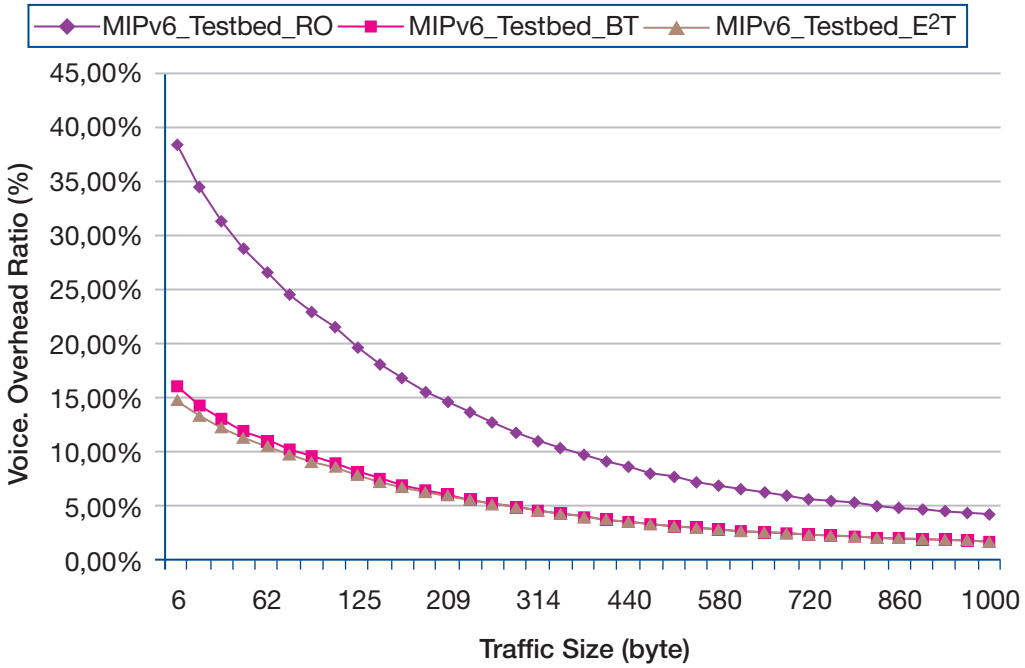
In order to evaluate the introduced overhead due to different MIPv6 routing mechanisms, we measure the overhead ratio by simulating the real-time voice application with different packet sizes. We define the performance metric of overhead ratio as follows:

$$\text{Overhead\_Ratio} = \frac{\text{Mobility\_Addition\_Size}}{\text{Original\_Packet\_Size}}$$

In this simulation, the CN and MN establish the voice sessions while they both roam in the range of ARs, the MN starts out from its home network (HAMN), and moves to the AR1, AR2 and AR3 in the deterministic path with the velocity of 10m/sec; the CN begins at its home network (HACN), and passes one by one through the AR4, AR5, AR6 in the deterministic direction with the velocity of 20m/sec (see figure 2.8.4). This case allows for full control of the mobility and handover rate of the concerned nodes.

Figure 2.8.5 shows the traffic overhead ratio versus the packet sizes of traffic for different MIPv6 routing mechanisms, namely RO, BT and E^{2}T. In this figure, MIPv6TestbedRO represents the traffic overhead ratio due to the addition of the IPv6 extension headers when routing data traffic using the MIPv6 RO mechanism. The MIPv6TestbedBT represents the traffic overhead ratio due to the additional tunnel header when routing data traffic through the MIPv6 BT mechanism. The MIPv6TestbedE^{2}T represents the traffic overhead ratio due to the tunnel header encapsulation with the proposed E^{2}T mechanism.

Figure 2.8.5: The simulation network model

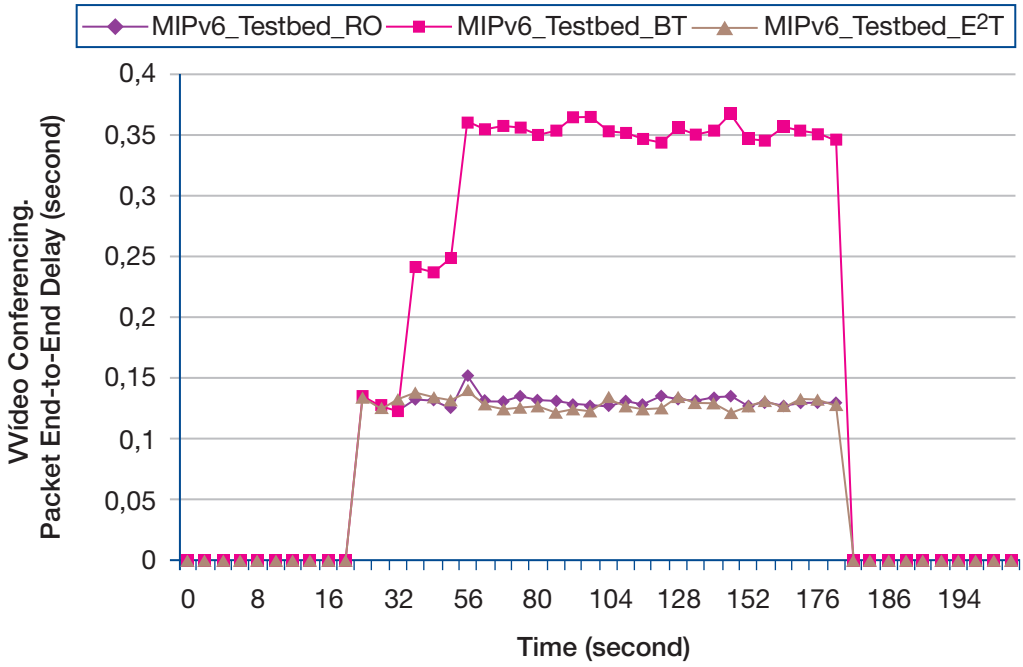


It can be observed from the above figure that when the traffic packet sizes are 1000 bytes, the overhead ratios of above routing mechanisms (i.e. RO, BT and E^{2}T) are 4.32%, 1.79%, 1.79% respectively; when the traffic packet sizes are 10 bytes, the overhead ratios of above routing mechanisms are 38.36%, 15.89%, 14.98% respectively. Although the overhead ratios of all routing mechanisms increase along with the decrease of traffic packet sizes, the RO mechanism shows significantly higher overhead than the BT and E^{2}T, especially when small traffic packet sizes are used. The BT and E^{2}T introduce the same overhead since they both employ the tunnelling technique for packet routing and have the same mobility addition messages of tunnel header. As many realtime applications have very small packets sizes, for example, the packet size is only 32 bytes in VoIP with G.711 encoder [24], so the optimization of overhead shows more important.

We also study the differences in the end-to-end traffic delay. We measure the packet end-to-end delay between the MN and CN by running a video conferencing application. It provides constant traffic over UDP for a constant bit rate. In this simulation, the incoming packet frame sizes and the outgoing packet frame size of the individual encoded video frames were configured with the constant value of 1024 bytes as input for the real time video traffic application. In order to emulate Internet conditions, we specify the IP cloud with the packet delay, which randomly varies between 90 ms and 100 ms, and the links and devices in the network model were all configured with background traffic of G.711 Voice. We set the same mobility pattern as that used in the previous simulation scenario.

Figure 2.8.6 shows the end-to-end traffic delay with the RO, BT and E^{2}T, where the horizontal axis indicates the time in seconds (sec) in which the video conferencing traffic is being transmitted between mobile devices while they are moving and the vertical axis indicates the packet end-to-end delay in seconds (sec).

Figure 2.8.6: The end-to-end delays of video conferencing traffic



As illustrated in this figure, from 20 sec to 34 sec when both the MN and CN move within the home network, the end-to-end transmissions with all above routing mechanisms have the similar delays (i.e. about 0.12 sec); from 34 sec to 52 sec when the CN has moved into the foreign network while the MN still moves within the home network, the average end-to-end traffic delay for the BT rises up to about two times (i.e. about 0.25 sec) of its previous values whereas the average end-to-end traffic delays for the RO and E^2T do not increase significantly. This is because in the case of BT, the end-to-end traffic delay will mainly be produced by two times the delay that the data packets pass through the Internet, and in case of the RO and E^2T, the end-to-end traffic delay will mainly be produced only when the data packets pass through the Internet. Similarly, from time 54 sec to 180 sec, when both the MN and CN move out of their home networks, the average end-to-end traffic delays for the RO and E^2T are only about one third of that for the BT.

2.8.5. CONCLUSIONS AND FUTURE WORK

In this paper, we analyzed the standard routing mechanisms in MIPv6 on their pros and cons. Based on this, we proposed the E^2T, an alternative routing mechanism as an extension to MIPv6 routing mechanisms for routing packet when the MN and CN are away from the home networks. The proposed E^2T combines the less overhead of BT with the low transmission delay of RO. Simulation results show that our approach is optimal for both the traffic overhead and routing delay, which is suitable for real-time multimedia applications for mobile communicating endpoints. In the future, we will study its impact on other mobility optimization approaches, and consider the minimal encapsulation for further optimization and the tradeoff between performance and complexity.

2.8.6. ACKNOWLEDGMENTS

This work is partially supported by the EC FP6 IST ENABLE project. The use of OPNET Modeler in the research was facilitated through OPNET's university program.

2.8.7. REFERENCES

[1] D. Le, X. Fu, and D. Hogrefe, "A review of mobility support paradigms for the internet," IEEE Communications Surveys and Tutorials, vol. 8, no. 1, pp. 2-15, 2006.

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, IETF, 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt

[3] S. J. Vaughan-Nichols, "Mobile ipv6 and the future of wireless internet access," IEEE Computer, vol. 36, no. 2, pp. 18 - 20, February 2003.

[4] M. Samad and R. Ishak, "Deployment of Wireless Mobile IPv6 in Malaysia," in Proceedings of RF and Microwave Conference (RFM'04), 2004, pp. 256-259.

[5] J. Choi, D. Shin, and W. Haddad, "Fast Router Discovery with L2 support," Internet Draft (work in progress), IETF, 2006. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-dna-frd-02.txt

[6] N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6," RFC 4429, IETF, 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4429.txt

[7] K. E. Malki and H. Soliman, "Simultaneous Bindings for Mobile IPv6 Fast Handovers," Internet Draft (work in progress), IETF, 2005. [Online].
Available: http://www.ietf.org/internet-drafts/ draft-elmalki-mobileip-bicasting-v6-06.txt

[8] A. Conta and S. Deering, "Generic Packet tunneling in IPv6 Specification," RFC 2473, IETF, 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2473. txt

[9] C. Perkins and D. B. Johnson, "Route Optimization in Mobile IP," Internet Draft (work in progress), IETF, 2001. [Online].
Available: http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-mobileip-optim- 11.txt

[10] C. Vogt, R. Bless, M. Doll, and T. Kuefner, "Early Binding Updates for Mobile IPv6," in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'05), vol. 3, 2005, pp. 1440 - 1445.

[11] C. E. Perkins, "Securing Mobile IPv6 Route Optimization Using a Static Shared Key," RFC 4449, IETF, 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4449.txt

[12] F. Bao, R. Deng, Y. Qiu, and J. Zhou, "Certificate-based Binding Update Protocol (CBU)," Internet Draft (work in progress), IETF, 2005. [Online].
Available: http://www.ietf.org/internet-drafts/ draft-qiu-mip6-certificated-binding-update-03.txt

[13] S. Trumpy and M. Gagnaire, "Evolution of internet technologies," Proceedings of the IEEE, vol. 92, no. 9, pp. 1355 - 1359, September 2004.

[14] R. Hinden and D. Thaler, "IPv6 Host-to-Router Load Sharing," RFC 4311, IETF, 2005. [Online].
Available: http://www.ietf.org/rfc/rfc4311.txt

[15] G. Montenegro, "Reverse Tunneling for Mobile IP (revised)," RFC 3024, IETF, 2001. [Online].
Available: http://www.ietf.org/rfc/rfc3024.txt

[16] G. Daley, E. Wu, A. Sekercioglu, and S. Narayanan, "Packet Tunneling for Route Optimization in MN-to-MN Communications," Internet Draft (work in progress), 2005. [Online].
Available: http://ftp.apnic.net/ietf/internet-drafts/ draft-ewu-mip6-mn-mn-tunnel-00.txt

[17] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, IETF, May 2000. [Online].
Available: http://www.ietf.org/rfc/rfc2827.txt

[18] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, IETF, 1998. [Online].
Available: http://www.ietf.org/rfc/rfc2402.txt

[19] S.Kent and R. Atkinson, "IP Encapsulation Security Payload (ESP)," RFC 2406, IETF, 1998. [Online].
Available: http://www.ietf.org/rfc/rfc2406.txt

[20] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, IETF, 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2401.txt

[21] OPNET Modeler, OPNET Technologies, Inc., OPNET Modeler, 2006. [Online]. Available: http://www.opnet.com/products/modeler/home.html

[22] D. Le, X. Fu, and D. Hogrefe, "Evaluation of Mobile IPv6 Based on an OPNET Model," in Proceedings of The 8th International Conference for Young Computer Scientists (ICYCS'05), 2005, pp. 238 - 244.

[23] IEEE Std. 802.1 1b, "Supplement to IEEE standard for information technology telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 2: higher-speed physical layer (PHY) extension in the 2.4 GHz band," 1999.

[24] "ITU-T Recommendation G.711," Pulse Code modulation (PCM) of voice frequencies, ITU-T, 1988.

2.9 An NSIS-based Approach for Firewall Traversal in Mobile IPv6 Networks

Niklas Steinleitner, Xiaoming Fu, Dieter Hogrefe
University of Göttingen
Thomas Schreck, **University of Applied Sciences Landshut**
Hannes Tschofenig, **Nokia Siemens Networks**

ABSTRACT

Firewalls have been successfully deployed in todays network infrastructure in various environments and will also be used in IPv6 networks. However, most of the current firewalls do not support Mobile IPv6, the best known standardized solution for mobility support in IPv6. As a result, Mobile IPv6 traffic will be most likely dropped when used without an appropriate firewall traversal solution.

This paper describes the problems and impacts of having firewalls in Mobile IPv6 environments, and presents a firewall traversal solution based on the IETF's Next Steps In Signaling framework to address these issues. Compared with other candidates such as STUN, TURN, ICE, ALG, MIDCOM and COPS, this approach does not rely on specific firewall placements and can be applied in various operational modes without additional introducing entities. In this paper we also explore security aspects since they are typically difficult to handle.

2.9.1. INTRODUCTION

Middleboxes, such as firewalls, are an important aspect for a majority of IP networks today. Current IP networks are predominantly based on IPv4 technology, and hence various firewalls (as well as Network Address Translators (NATs) have been originally designed for these networks. Deployment of IPv6 networks is currently work in progress. However, some firewall products for IPv6 networks are already available. It is foreseen that firewalls will become an indispensable means for protecting against unwanted traffic in operational IPv6 networks, especially in enterprise environments.

Given the fact that Mobile IPv6 [1] is a recent standard, most firewalls available for IPv6 networks still do

not support Mobile IPv6. Unless firewalls are aware of Mobile IPv6 protocol details, they will have to either block Mobile IPv6 communication traffic, or carefully deal with the traffic on a per-user or per-connection basis, or to allow Mobile IPv6 traffic in general, through manual pre-configuration. This could be a major impediment to the successful deployment of Mobile IPv6.

Some existing firewall traversal solutions, such as STUN [2], TURN [3], ICE [4], Application Layer Gateways (ALGs), Middlebox Communication [5], COPS [6] or policy-based solutions potentially can be extended to enable firewall and middlebox traversal even in mobile networks. However, some of them require prior knowledge of the existence of firewalls and most do not address the issue of discovering firewalls. Furthermore, they do not support the node mobility case and thus may require significant effort to be extended for use in Mobile IPv6 networks.

A recent initiative within the IETF, Next Steps in Signaling (NSIS) [7], has developed a signaling protocol for firewall and NAT traversal, the NAT/Firewall NSLP (NAT/FW NSLP) [8]. NSIS utilizes a two-layer signaling paradigm, which defines a lower layer for general extensible IP signaling and an upper layer for various signaling applications such as signaling for NAT/Firewall traversal. Since its initial design, NSIS has been considering node mobility as a potential usability scenario. However, how the NSIS firewall/NAT traversal signaling protocol supports IPv6 mobility is not specified.

This paper will give an overview of the problems when firewalls are placed in Mobile IPv6 networks, identify potential approaches and present how to use NSIS to address the Mobile IPv6 firewall traversal issues.

The paper is structured as follows. In Section 2.9.2 we shortly describe the problems and impacts of having firewalls in Mobile IPv6 environments, as described in RFC 4487 [9], and identify potential state-of-the-art solutions. In Section 2.9.3 we present a middlebox traversal solution based on the NSIS signaling layer protocol for NAT/firewall traversal [8] and show how it can be used for firewall traversal in Mobile IPv6. Section 2.9.4 provides an analysis of potential authorization solutions and Section 2.9.5 discusses open issues and further work. Section 2.9.6 summarizes this paper.

2.9.2. PROBLEM STATEMENT

To study how firewall traversal can be achieved in Mobile IPv6 environments, it is necessary to understand the problems and impacts of having firewalls in such environments.

Mobile IPv6 [1,10] introduces several new types of messages, which can be categorized into registration messages (Binding Update(BU), Binding Acknowledgements(BA)), Home/Care-of-testing messages (Home-of-Test-Init (HoTI), Home-of-Test (HoT), Care-of-Test-Init (CoTI), Care-of-Test (CoT)) and data traffic. Also, a new mobility header is introduced, and all messages between the mobile node (MN) and the home agent (HA) are IPsec ESP [10] encapsulated.

When a user moves to a visited network, a firewall - no matter whether it is located in the home network, the visited network, or the access network of the corresponding node - will affect the Mobile IPv6 signaling and data messages. For instance, route optimization, an integral part of Mobile IPv6 specification, does not work with the state-of-the-art firewalls that utilize stateful packet filtering (SPF). This set of extensions is a fundamental part of the protocol, enabling optimized routing of packets between a mobile node and its correspondent node, thus providing optimized communication performance. However, firewall technologies

do not support Mobile IPv6 or are not even aware of IPv6 mobility extension headers. Since most networks in the current business environment deploy firewalls, this may prevent future large-scale deployment of Mobile IPv6. Secondly, another mode of communication in Mobile IPv6, namely bi-directional tunneling, does not work under some scenarios, e.g., when a firewall is placed in the access network or the home network. In addition, it is difficult for the Mobile IPv6 binding update packets (encapsulated using IPsec ESP) to traverse firewalls. In summary, these deployment issues with firewalls occur due to the characteristics that commonly used firewalls possesses [9]:

- they do not understand Mobile IPv6 mobility header,
- they do not allow IPsec - which is used for Mobile IPv6 registration messages between MN and HA - traffic to traverse,
- they do not understand data packets encapsulated in Mobile IPv6 and, most likely drop them.

In the following subsections, we first explore these problems in detail from both operational and technical aspects regarding some relevant scenarios.

2.9.2.1. Scenarios and issues

Without loss of generality, let us consider a typical roaming scenario, where a mobile user with a PDA (MN) is roaming outside of his or her company (hereafter, the so-called "Mobile Service Provider", or MSP) into a visited network ("Access Service Provider", or ASP) which is also a corporate network. The MN wants to communicate with his home network or it's Home Agent (HA) (in order to register its new location) and additionally with another node, the corresponding node (CN), for data communication. The visited network could, (potentially) be protected by a firewall, thus parts of the traffic to the MN may be blocked. Also, both the home network and the network of the CN may deploy firewalls. These three possible firewall placements introduce several problems, which could prevent Mobile IPv6 from operating successfully in the presence of firewalls. In all cases, pinholes have to be open on the firewalls for enabling successful communication. These problems can be differentiated under three basic scenarios.

- Firewall located at the edge of the MN's ASP,
- Firewall located at the edge of the CN's ASP,
- Firewall located at the edge of the MN's MSP.

In the following sections we investigate these three basic scenarios individually, and show how a firewall might prevent Mobile IPv6 from a successful operation.

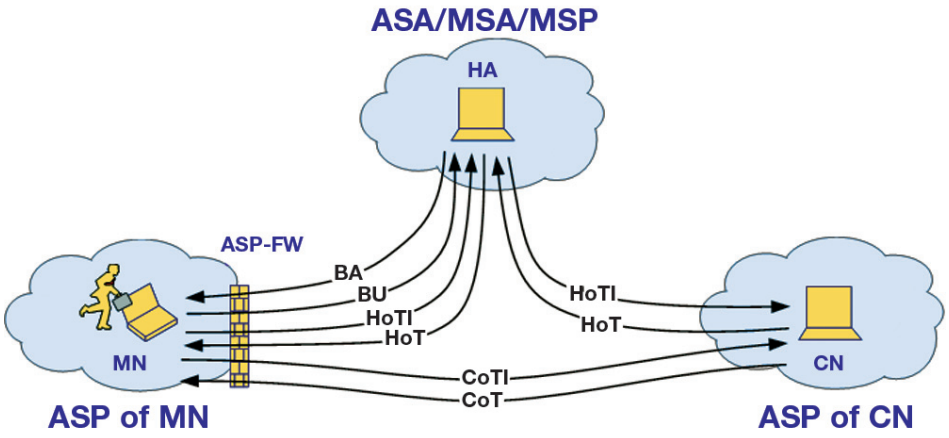
2.9.2.1.1. Firewall located at the edge of MN's ASP

The first scenario assumes that the MN roaming to another network (i.e., ASP, which deploys a firewall (ASP-FW)) wants to communicate with his company or ISP (MSA/MSP/ASA). Therefore, the MN needs to traverse the ASP-FW. Figure 2.9.1 depicts how the components are placed in this scenario. Several issues need to be considered:

- Binding Updates and Binding Acknowledgements, should be protected by IPsec ESP, but many firewalls drop IPsec ESP packets because they cannot determine whether inbound ESP packets are authorized. A possible solution might be to manually pre-configure the ASP-FW so that MIPv6 traffic is allowed to traverse it. However, not every administrator would permit IPsec traffic in general, so it must also be possible to dynamically install these firewall rules.

- The ASP-FW may drop the Home Test messages and may prevent the completion of the Return Routability Test (RRT) procedure, as the Home Test messages of the RRT are protected by IPsec ESP in the tunnel mode. Therefore, either manual pre-configuration or dynamic on-demand configuration of rules on the ASP-FW is a possible solution for this type of messages.
- If the MN successfully sends a Binding Update to it's HA and the subsequent traffic is sent from HA to MN (in bi-directional tunneling), there is also no corresponding state on the firewalls, and the firewalls drops the incoming packets. Hence, it is necessary to dynamically configure the ASP-FW to let this data traffic traverse.
- The ASP-FW may prevent correspondent nodes from establishing communications (e.g. route optimization traffic) because incoming packets are dropped since the packets do not match any existing state.
- If the MN roams and moves to another access network protected by a different firewall, all new incoming packets are dropped as they do not match any existing "allow" state.

Figure 2.9.1: Firewall located at the edge of MN's ASP

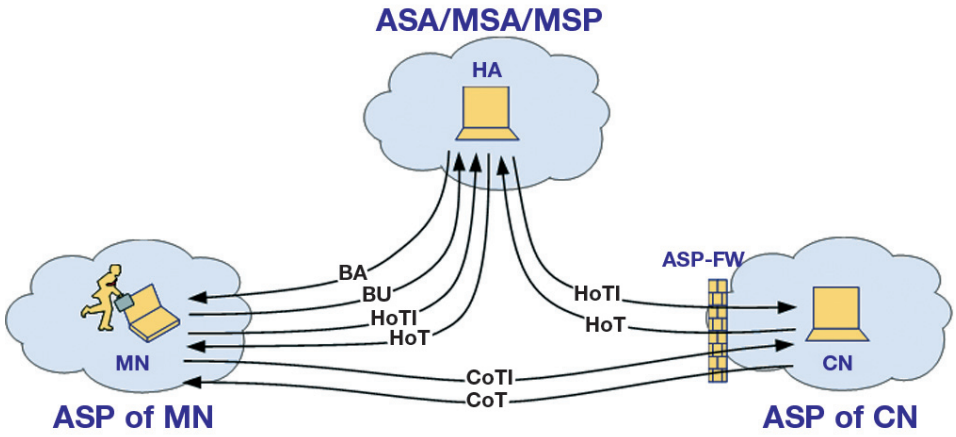


2.9.2.1.2. Firewall located at the edge of CN's ASP

Here, a MN wants to communicate with a CN that deploys a firewall. Therefore, the traffic from the MN to the CN needs to traverse the CN's ASP-FW. Figure 2.9.2 depicts how the components are placed in the second scenario. Several issues need to be considered:

- The Care-of-Test-Init message is sent using the Care-of-Address (CoA) of the MN as the source address. Such a packet does not match any entry in the protecting firewall, as the states in the firewall are bounded to the old address of the MN. The CoTI message will thus be dropped by that firewall. As a consequence, the RRT cannot be completed, and route optimization cannot be performed. Every packet has to be tunneled through the HA.
- If the BU to the CN is successful, the firewall still drops packets that are coming from the CoA, because these incoming packets are sent from the CoA and do not match any existing firewall state.

Figure 2.9.2: Firewall located at the edge of CN's ASP



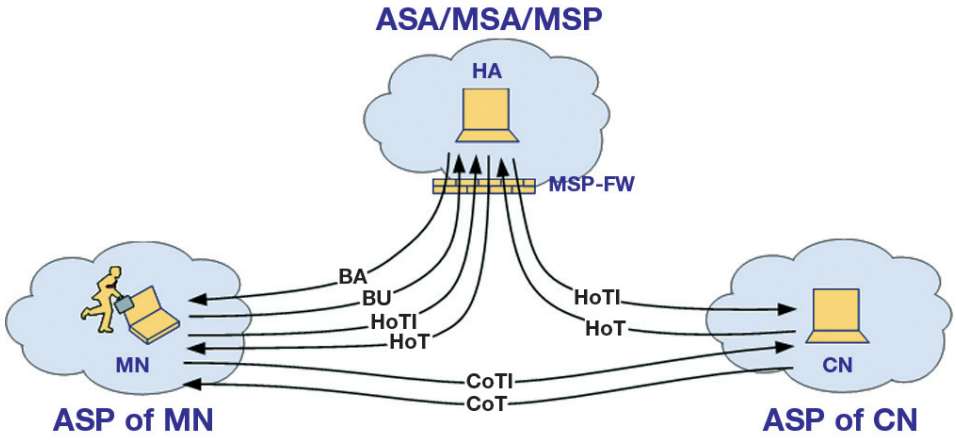
2.9.2.1.3. Firewall located at the edge of MN's MSP

In this scenario, the MN roaming to another company/ISP (i.e., ASP) wants to enjoy communicating with a CN and his own company (MSP), and the MSP deploys a firewall at its network border. The MN needs to traverse the MSP-FW to run Mobile IPv6.

Figure 2.9.3 depicts how the components are placed in third scenario. Several issues need to be considered:

- If the firewall protects the home agent by blocking ESP traffic, some of the MIPv6 signaling (e.g., Binding Update, HoTI) may be dropped at the firewall. This prevents MNs from updating their binding cache and performing Route Optimization, since the messages must be protected by IPsec ESP. Manual pre-configuration is a solution, but also has some problems as mentioned before.
- If the firewall is a stateful packet filter and protects the home agent from unsolicited incoming traffic, the firewall may drop connection setup requests from CNs, and packets from MNs.

Figure 2.9.3: Firewall located at the edge of MN's MSP



2.9.2.2. Requirements and Solution Alternatives

To get Mobile IPv6 working in these scenarios it is necessary to allow all these messages to traverse the firewall. This requires the usage of a middlebox configuration solution. In general we can distinguish between two types of middlebox configuration; the implicit and the explicit approaches. The implicit middlebox configuration is triggered by data traffic. A stateful packet filtering firewall or a NAT establishes state information based on the header information in the data traffic itself. STUN and TURN also belong in the implicit category, since these signalling protocols do not interact with the firewall itself but rather implement a hole-punching behaviour as middleboxes treats these messages as ordinary data traffic. In contrast, with an explicit approach the intention is to interact with the middlebox and therefore the middlebox has to implement additional protocols. Application Layer Gateways, MIDCOM or the NAT/Firewall NSLP are examples of this approach.

The main difference between the two approaches is flexibility regarding the pinhole creation vs. the need to enhance existing middleboxes to understand additional protocols. Implicit approaches are less flexible regarding the creation of pinholes, which often leads to the need to tunnel one protocol on top of another one. Additionally, since there is no interaction with the middlebox and the end host it is unclear how long established state is kept alive at the middlebox. As a consequence, more frequent refresh messages have to be transmitted to ensure that state information is not discarded. Finally, explicit approaches provide better security properties. However, the major disadvantage is the slow adoption of new protocols at middleboxes.

Since Mobile IPv6 networks yet have to be deployed on a wide scale there is, still, an opportunity to enhance middleboxes with additional protocols and hence we have chosen an explicit signaling approach.

Application Layer Gateways

Application Layer Gateways rely on the installation of an enhanced Firewall/NAT, called an ALG. This ALG understands the application layer protocol semantic. The ALG processes the signaling and data traffic and can modify the signaling to match the public IP addresses and ports that are used by the signaling and media traffic. The ALG is often transparent to end hosts. The ALG might be co-located with the middlebox itself or it interacts with it to setup state information, such as packet filters, or even modifies application specific payloads.

ALGs typically destroy the end-to-end semantic of a protocol and harm end-to-end security since they often modify passing payloads. These middleboxes make it more difficult to deploy new extensions since they often drop unknown extensions. Finally, there can be performance problems caused by the deep packet inspection nature of the devices. A Session Border Controller is an example of an ALG in the context of SIP.

MIDCOM

One possible alternative is to use MIDCOM [5]. The main idea of MIDCOM is to move application logic from the middlebox into a trusted third entity. There are three main entities in the MIDCOM framework: middleboxes, MIDCOM agent, and MIDCOM Policy Decision Point (PDP). MIDCOM agent is an entity performing ALG functions, which reside outside of the middlebox. It interacts with a middlebox to set up states, access control filters, extract middlebox state information, modify application specific payload, or perform other tasks necessary to enable middlebox traversal. The MIDCOM PDP acts as a policy repository, holding MIDCOM related policy profiles in order to make authorization decisions.

The decomposition in MIDCOM provides a number of advantages, including improved performance, lower

software development and maintenance costs, and easier deployment of new applications. Nevertheless some disadvantages still exist. MIDCOM assumes to have knowledge about the network topology and the middlebox has to be contacted for starting data transmission. However, for complex topologies, the task of middlebox discovery becomes a problem.

ICE/M-ICE

Another possible framework that could be used is Mobile IP Interactive Connectivity Establishment (M-ICE) [11] that builds on top of the Interactive Connectivity Establishment (ICE) [4] methodology. ICE is based on STUN [2] and TURN [3]. With M-ICE the ICE framework is applied to Mobile IPv6. M-ICE uses STUN for connectivity checks, a modified return routability procedure and UDP encapsulation of the signaling traffic as described in [12].

First, M-ICE will gather the MN's candidates and afterwards will signal them to the CN by including them in the CoTI-ICE message. When the CN receives this message it will also start gathering its candidates and provides them in the CoT-ICE message. At that time both nodes could pair these two lists of candidates up and start connectivity checks by using STUN. After this process is complete ,they both have a prioritized list of working candidate pairs.

ICE works reliably, as it is widely used for VoIP. For interacting with middleboxes an extension to STUN has been proposed that enables STUN-aware middleboxes to participate in the signaling exchange, see [13]. Authorization functionality has been proposed with [14].

2.9.3. MOBILE IPV6 FIREWALL TRAVERSAL BASED ON NSIS

This section describes how an extended NSIS [7] NAT/Firewall NSLP [8] could be utilized to compose the Mobile IPv6 firewall pinhole creation. This approach has the advantage of being a modular IETF standard protocol able to configure stateful packet filters. One particular advantage is that the NSIS NAT/FW NSLP framework relies on a soft-state approach. Therefore, established sessions will be automatically torn down after a specified timeout. This is very useful in a mobile scenario as it is not necessary to delete a session, after roaming to another network. The University of Göttingen has developed an open source implementation of NSIS protocol stack [15], including a NAT/FW NSLP implementation, which allows customized extensions for development. The following section gives an overview of the NSIS framework and the NAT/Firewall NSLP framework, developed by the IETF NSIS Working Group. It also describes how NSIS and the NAT/FW NSLP is applicable for Mobile IPv6 firewall traversal.

2.9.3.1. NSIS Introduction

The NSIS framework [7] has been developed with the goal of supporting various signalling applications, which install and manipulate certain control states in the network. Such states are meaningful for data flows and are installed and manipulated on network nodes supporting NSIS (NSIS Entities, NEs) along the data path. Not every node has to be such an NE, for instance, in the NAT/FW NSLP case, NAT/Firewall boxes need to be the NEs along the data path of a data flow as well as the end hosts. The basic protocol concept does not depend on any signaling application. This section describes the fundamental entities involved in NSIS signaling and their basic interactions. Two NSIS entities that communicate directly are said to be in a "peer relationship". Thereby, either or both NEs can store state information about the other NE, but it is not mandatory to establish a long-term signalling connection between them.

Figure 2.9.4: Simple Signaling and Data Flow Example

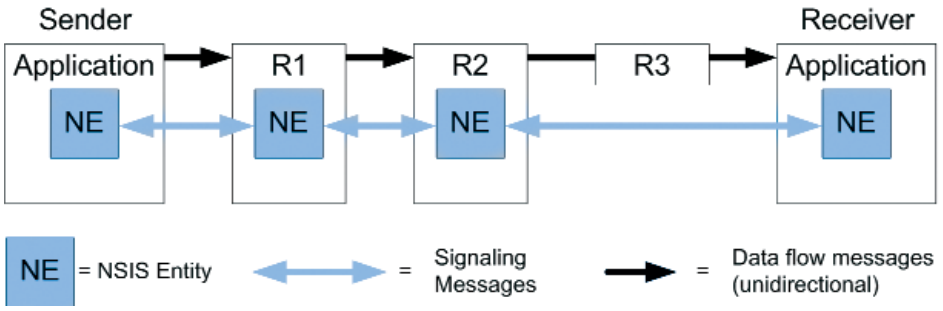


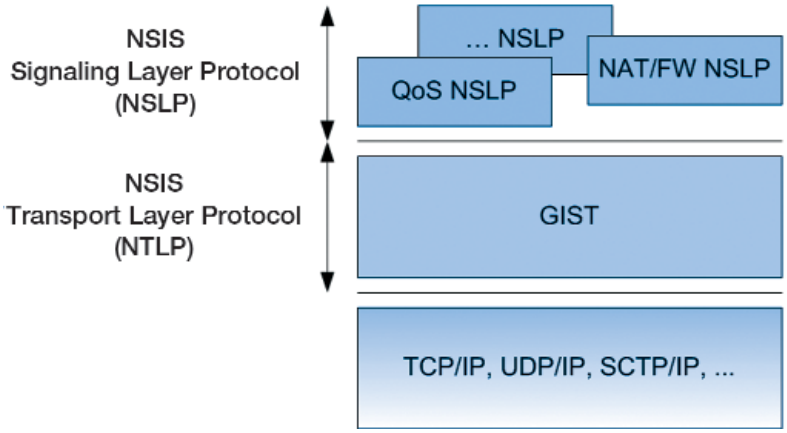
Figure 2.9.4 shows one of the simplest possible signalling configurations. A data flow is flowing from the sender via different routers to the receiver. The two end hosts and two of the routers contain NEs that exchange signalling messages about the flow. R3 does not contain an NE and forwards only the data. The signalling messages exchange is possible in both directions. Before a data flow is sent, an NSIS signalling procedure will take place along the NEs in the data path, including discovering their existence and signalling the application-specific states (e.g., firewall configurations for corresponding data traversal).

2.9.3.2. NSIS Layered Model Overview

In order to meet the modular requirements for NSIS, the NSIS protocol is structured in two layers:

- The NSIS Transport Layer Protocol (NTLP), which is responsible for moving signalling messages around and nevertheless independent from the underlying signalling application. The NTLP is implemented by GIST [15].
- The NSIS Signalling Layer Protocol (NSLP), which allows application based functionalities, such as message formats and sequences. Figure 2.9.5 illustrates this modular NSIS approach and the mutual influence between the NTLP and the NSLP.

Figure 2.9.5: The NSIS Protocol Components



Functionality within the NTLP is restricted only to transport and lower-layer operations. Other operations are relocated to the signalling application layer. A short introduction of the NTLP can be described as follows.

When an NSLP signalling message needs to be sent, the NSLP gives it over to the NTLP together with the information to which flow it belongs (so-called flow identifier). The NTLP has to care about how the message is sent to the next NE along the path. The NTLP does not need to have any knowledge about addresses, capabilities, or status of other NEs along the path, only for the NEs that it directly peers with.

Upon receipt of an NSIS message, each intermediate NTLP either directly forwards it or - if the signalling application runs locally - passes the message to the NSLP for further processing. After processing, the NSLP can use the original message or generate another message and hands it over to the NTLP. With this procedure end-to-end NSIS message delivery can be achieved. This restriction of the NTLP to peer-relationship scope simplifies the management and the complexity of the NTLP, at the cost of an increased functionality, complexity of the NSLPs and deployment complexity, as some components (e.g., middleboxes) on the path need to run NSIS.

2.9.3.3. The NAT/FW NSLP Protocol

The IETF NSIS working group is currently finalizing the NAT/Firewall NSIS Signalling Layer protocol (NAT/FW NSLP) specification [8], which describes scenarios, problems and solutions for path-coupled network address translator and firewall signalling. The NAT/FW NSLP is one of the two NSLPs that the working group has been developing. Our previous work [16] has shown that NSIS and the NAT/FW NSLP framework is able to support firewall signalling for up to tens of thousands of flows in parallel even in a low-end environment; and the overall performance bottleneck was the utilized firewall implementation, not on the signalling implementation.

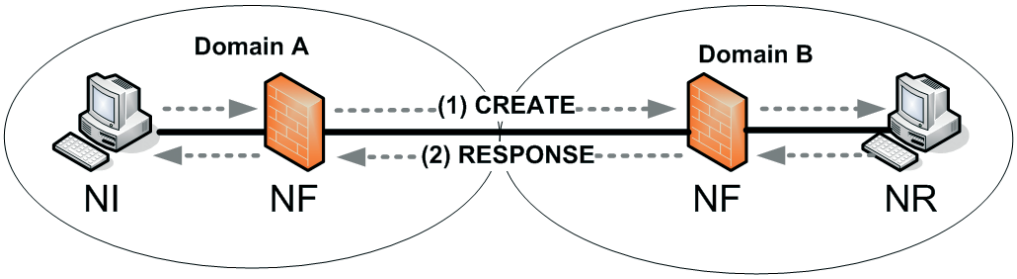
The main goal of NSIS NAT/FW signalling is to enable communications between two endpoints across different networks in case of the existence of NATs and firewall middleboxes. Firstly, it is assumed that these middleboxes will be configured in such a way that NSIS NAT/FW signalling messages can traverse them. Then, the NSIS NAT/FW NSLP protocol is used to dynamically install additional policy rules in all NAT/FW NSLP-aware middleboxes along the path. Firewalls will be configured to forward desired data packets according to the policy rules which are established by the NAT/FW NSLP signalling.

The signalling traffic of an application behind a middlebox has to traverse all middleboxes along the data path to establish communication with a corresponding application on the other end host. To achieve middlebox traversal, the application triggers the local NSIS entity to signal along the data path. If the local NSIS entity supports NAT/FW NSLP signalling, the knowledge pertaining to the application is used to establish policy rules and NAT bindings in all middleboxes along the path, which allows the data to travel from the sender to the receiver. Clearly, it is necessary for intermediate middleboxes to support NAT/FW NSLP, but not necessary for other intermediate nodes to support NAT/FW NSLP or even NSIS.

Figure 2.9.6 shows a common topology for the use of NAT/FW NSLP. This network is separated into two distinct administrative domains, namely "Domain A" and "Domain B".

The NSLP Initiator (NI) sends NSIS NAT/FW NSLP signalling messages along the data path to the NSLP Responder (NR). It is assumed that NI, NR and every intermediate middlebox implements the NAT/FW NSLP. Thereby, no knowledge about the next middlebox along the path is required; this is done by on-path next-hop discovery. The signalling messages reach different intermediate NSIS nodes (i.e., NSLP Forwarder or NF)

Figure 2.9.6: A Firewall Traversal Scenario



and every NAT/FW NSLP node processes the signalling messages and, if necessary, installs additional rules for the following data packets. The NAT/FW NSLP supports several types of signalling messages, most notably the CREATE and the EXT messages:

- The CREATE message is sent from the source address to the destination address and processed by every middlebox and forwarded to the destination.
- The EXT message is sent from the source address to an external address (e.g. the HA's address or the CN's address) and is intercepted by the edge firewall and not forwarded to the destination address. This allows signalling pinholes at the edge-firewall without introducing long end-to-end signalling delays.
- The RESPONSE message is used as a response to CREATE and EXT request messages.

Policy rules for firewalls are represented by a 5-tuple record namely the source and destination addresses, the transport protocol and the source and destination port, in addition to the rule action with the value "allow" or "deny". Such a policy rule in NAT/FW NSLP is bounded to a specified session. Different from other signalling applications where policy rules are carried in one object, the policy rules in NAT/FW NSLP are divided into an action (allow/deny), the flow identifier and further information. The message routing information (MRI) in the NTLP carries the filter specification, the additional information such as lifetime, session ID, message sequence number, authorization objects and the specified action are carried in NSLP's objects.

2.9.3.4. NSIS for Mobile IPv6 Firewall Traversal

As described in Section 2.9.2, the standard Mobile IPv6 does not work with the existence of firewalls. To tackle these issues, one approach is to utilize a signalling protocol to install some firewall rules to allow these Mobile IPv6 messages to pass through. The NSIS NAT/FW NSLP, as described in [8], allows an end system to establish, maintain and delete middlebox state (i.e., firewall rules), and as well as allows packets to traverse these boxes. This protocol thus provides a possible way to address the aforementioned problems [17]. The following subsections introduce how we could extend the NSIS NAT/FW NSLP to solve the problems.

2.9.3.4.1. Firewall located at the edge of MN's ASP

In Figure 2.9.1, the MN is protected by a firewall that employs stateful packet filtering. The external CN and the HA are also shown in the figure. The MN is located in a visited network and is expecting to communicate with the CN. If the MN initiated normal data traffic there is no problem with the SPF firewall, as the communication is initiated from internal. The following subsections explain how this approach manages the MIPv6 signalling traffic problems as described in Section 2.9.2.

Binding updates

IPsec protected binding updates cause problems in some deployment environments, as described in RFC4487 [9]. As a solution, NAT/FW NSLP can be used to dynamically configure the firewall(s) to allow the IPsec packets and associated traffic such as IKE/IKEv2 packets to traverse, before sending the binding updates. Therefore, IP Protocol ID 50 should be allowed in the filter policies in order to allow IPsec ESP and IP Protocol ID 51 to allow IPsec AH. The firewall should also allow IKE packets (to UDP port 500) to bypass, which can also be signalled beforehand.

Figure 2.9.7: Signaling for BU and BA

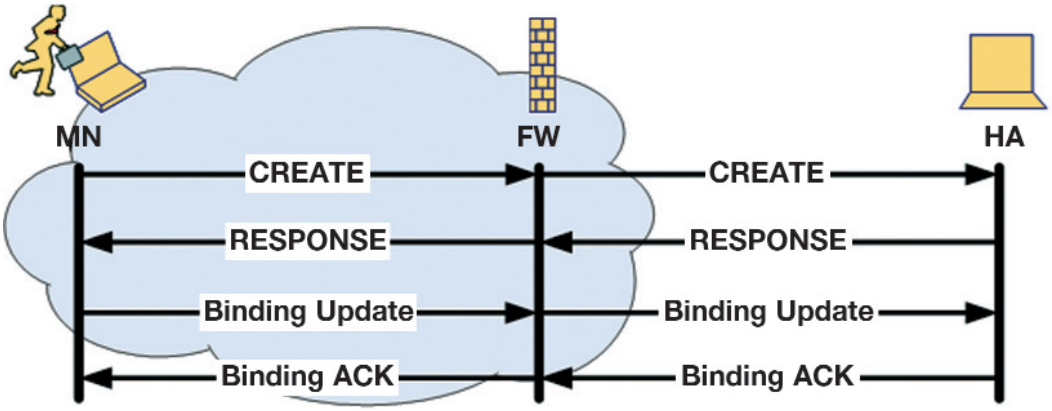


Figure 2.9.7 shows the message flow for this signalling. As the firewall is a SPF, the subsequent binding acknowledgement from the HA to the CoA can pass the firewall, as it matches an existing state in the table.

Route optimization

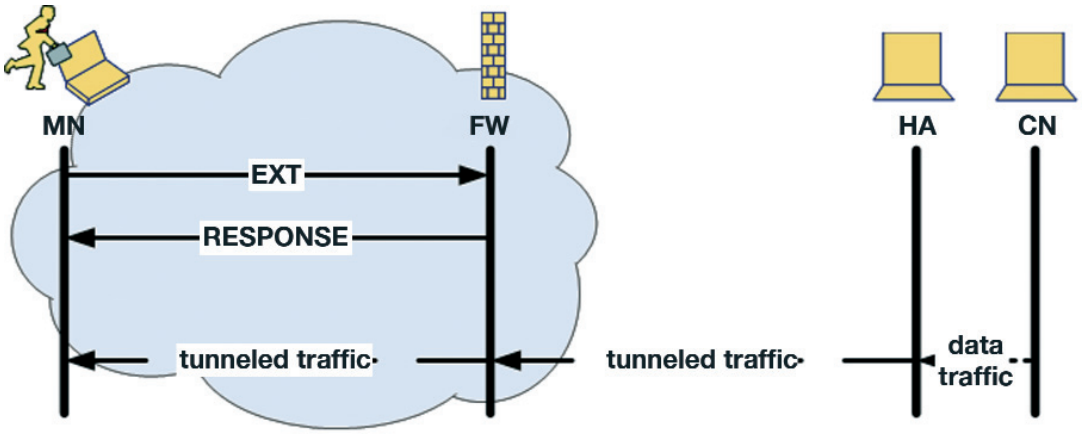
Immediately after moving into a new network, the MN acquires a new CoA, performs the pinhole creation as described previously, and runs the Binding Update to the HA. The HoTI message from the MN is IPsec encapsulated in tunnel mode and as it does not belong to the session initiated by the MN or match a previously installed rule, it will be dropped by the firewall. Using CREATE, the MN initiates NSIS signalling to the firewall and open pinholes for the HoTI message. The message flow is comparable to the flow in Figure 2.9.7, whereas the CREATE message installs different pinholes. The HoT message can re-use this pinhole and is able to reach the MN. The CoTI message and the CoT message can traverse the MN's ASP-firewall, as the CoTI message is not IPsec encapsulated and the CoT message corresponds to the state previously installed by the CoTI message.

Once the RRT is successful, the binding update message is sent to the CN. If the MN wants to continue sending data traffic, no NSIS signalling is needed at all for this scenario. However, if the CN wants to send data traffic and the previously installed rules match the addresses, the ports and the IPsec encapsulation, the relevant packet filter rules have to be installed at the firewall. If the previously installed rules only match source and destination address, the data traffic exchanged with the CN in RO-case can also traverse the firewall with no need of installing additional rules. However, this would allow all types of traffic from the CN and is rejected. Hence, the MN has to initiate sending data traffic to the CN but this happens after the RRT.

Bi-directional tunnelling

Consider the scenario where the MN is protected by a SPF. Even though the MN had earlier initiated a connection for the purpose of binding update, new filter rules have to be installed to allow the tunnelled data traffic. The message flow is shown in Figure 2.9.8. If the MN is the data sender, no signaling is necessary at all. Otherwise, the MN opens pinholes using EXT to let the data messages traverse.

Figure 2.9.8: Signalling for data traffic



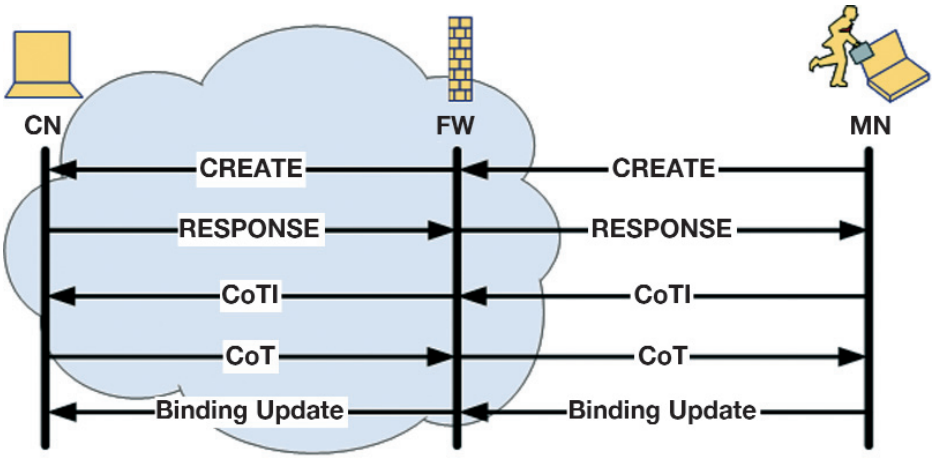
2.9.3.4.2. Firewall located at the edge of CN's ASP

Route Optimization

In Figure 2.9.2, the CN is protected by a firewall that employs the stateful packet filtering. The external MN and its associated HA are also shown in the figure. The MN communicates with the CN. If the CN initiated normal data traffic there is no problem with the SPF, as the communication is initiated from inside the firewall. The following subsections explain how this approach manages the MIPv6 signalling traffic problems as described in Section 2.9.2.

The MN moves out of its home network and has to perform the return routability test before sending the binding update to the CN. It sends a HoTI message through the HA to the CN and expects a HoT message from the CN along the same path. It also sends a CoTI message directly to the CN and expects CoT message in the same path from the CN. The SPF will only allow packets that belong to an existing session and hence both the packets (HoTI, CoTI) will be dropped as these packets are Mobile IPv6 packets and these packets have a different header structure. The existing rules at the firewall might have been installed for some other type of data traffic. As the RRT procedure cannot be executed, the firewall rules have to be modified to allow these MIPv6 messages to go through. The MN initiates the NSIS session by sending a CREATE message to the CN to install rules for the CoTI message. The NSIS signaling to allow the CoTI message is shown in Figure 2.9.9. However, such an approach where an external node is able to install filter rules in an ASP-FW clearly requires a strong authentication framework. Section 2.9.4 discusses this in more detail and presents several potential candidates.

Figure 2.9.9: Signaling for CoTI and CoT



If the MN signal as described in the previous section, the HoTI is able to reach the HA. Nevertheless, the HoTI message from the HA to the CN is not able to traverse, as it does not match any state at the CN's ASP-FW. Therefore, either the HA or the CN has to signal install rules to let the HoTI messages pass through the FW. When the MN receives both CoT and HoT messages, it performs binding update to the CN which is possible, as the BU can re-uses the previously installed rules. Note that the aforementioned signalling was only to allow the Mobile IPv6 messages.

If the CN wants to continue sending data traffic (CN is the data sender (DS)) to the new CoA, it can do so without any additional signalling. This is because the SPF will allow traffic initiated by the nodes that it protects. But if the MN wants to continue sending data traffic (MN is the DS), it has to install filter rules for data traffic. The approach of combined signalling (for control and data traffic) could be useful, but currently the NSIS NAT/FW protocol does not support installing multiple rules at the same time. This will be discussed in Section 2.9.5 in detail.

This solution works under the assumption that the firewalls will allow NSIS messages from external network to pass through, unimpeded, by applying a delayed packet filter state establishment and authorization from the CN. However, operators might be reluctant to allow NSIS message from external network as this might lead to Denial of Service (DoS) attacks. The CN might therefore be required to implicitly authorize the traversal of NSIS signalling messages to reduce unwanted traffic. To avoid this complexity, it is also possible to ask the CN to open pinholes in the firewall on behalf of the MN. However, this solution may not work in some scenarios due to routing asymmetry as explained in [8].

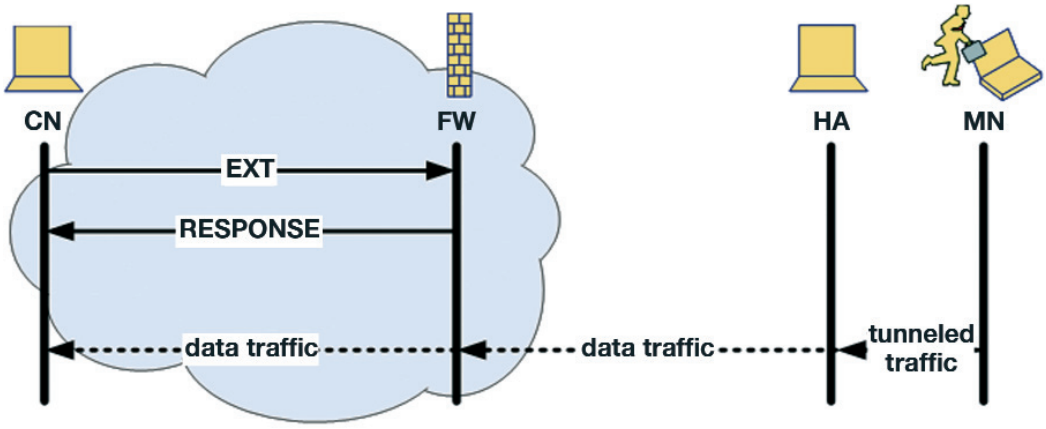
Bi-directional Tunnelling

If the CN is protected by a SPF firewall, there is no need for any signalling if the CN starts sending data traffic. The CN sends the data traffic and hence the SPF will store relevant state information and accepts packets from the reverse direction.

If the HA is the DS, then either the CN has to initiate the signalling using EXT or the HA using CREATE, in order to configure the firewall to allow the data traffic traverse from the HA to CN. To support that function, Mobile IPv6 module at the HA or CN will need to be changed so that it triggers the local MIP6-firewall-

traversal-application in the event of receiving a CoTI message from the MN. The local MIP6-firewall-traversal-application is then able to trigger the pinhole creation process. The message flow if the CN should signal for this pinhole is shown in Figure 2.9.10.

Figure 2.9.10: Signalling for data traffic



2.9.3.4.3. Firewall located at the edge of the MN's MSP

Route Optimization

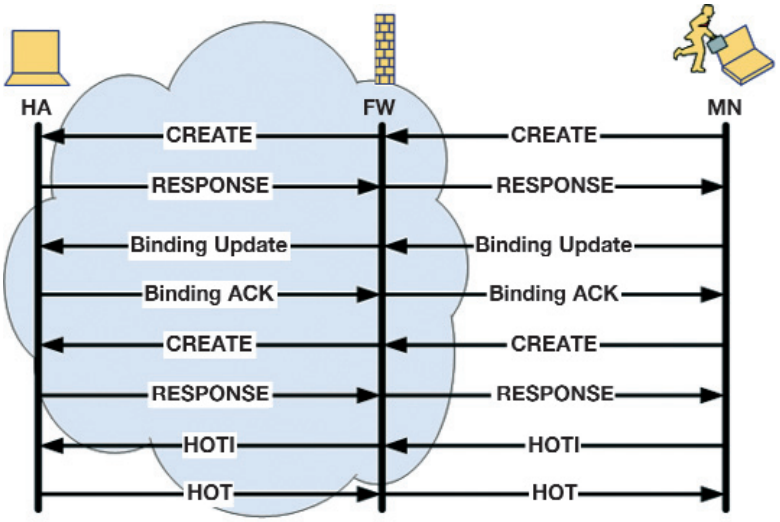
In Figure 2.9.3, the Mobile Node's MSP is protected by a firewall that employs stateful packet filtering. The MN and the CN are also shown in the figure. The MN, after entering a new network, sends a Binding Update to the HA. However, as it is initiated by the MN, the MN first has to install some filter rules in the firewall before sending the Binding Update.

The MN-HA Binding Update message is assumed to be IPsec encapsulated. This might cause problems, as some primitive firewalls do not recognize IPsec traffic and hence drop the packets because of the absence of any transport header. One approach is to use UDP encapsulation of IPsec traffic in order to overcome this problem. Another is using NSIS NAT/FW NSLP to signal the firewall to allow such traffic to traverse. The MN initiates the NSIS signalling to create rules that will allow the Binding Update messages to go through the firewall. The MN then sends the Binding Update message to the HA.

By default, the rules previously installed in the firewall will not allow the HoTI message to go through. Hence, the MN has to install a different set of rules for these signalling messages by initiating another NAT/FW NSLP signalling exchange. After that it sends the HoTI message to the HA. The HA installs rules between the HA and the CN and accordingly send the HoTI to the CN. The HoT message from the CN to the HA is also allowed by the SPF as it belongs to the session previously installed by the HA. The HoT message from the HA to the MN is also allowed as it is initiated by the HA. The RRT completes successfully. Detailed message flow between MN and HA is shown in Figure 2.9.11.

For the data traffic, there is no additional signalling as the MN sends data directly to CN and none of these networks are protected by firewalls. This is applicable for both cases when either MN or CN is the data senders.

Figure 2.9.11: Signaling for BU, BA, HoTI and HoT



Bi-directional tunnelling

Here, it is necessary that the HA opens pinholes for the data traffic from the CN using EXT. The CN is then allowed to send the data traffic through the firewall. After intercepting a packet, the HA tunnels it to the MN.

2.9.4. AUTHENTICATION, AUTHORIZATION AND KEY MANAGEMENT

An important aspect for firewall signalling is how to ensure that only authorized hosts are allowed to perform actions. This leads to the question of how to provide authentication, authorization and key management. Manner et al. [18] specifies how authorization is accomplished for the NSIS QoS and NAT/FW NSLP using an authorization token. That document reuses the authorization token format specified for RSVP and allows information to be exchanged between nodes in order to authorize access to resources. In addition to the already proposed mechanism we discuss three solutions, namely using the Generic Service Authorization Architecture (GSABA) [19], SAML assertions and TLS-EAP [21].

2.9.4.1. Generic Service Authorization Architecture

The Generic Service Authorization Architecture (GSABA) [19] is an authentication system with three parties. The goal is to give an end host the ability to access services offered by third parties and to utilize the AAA infrastructure for authentication, authorization and accounting. In this section we will give a short introduction to the GSABA and subsequently discuss a possible integration with the NSIS NAT/FW NSLP for MIPv6 usage.

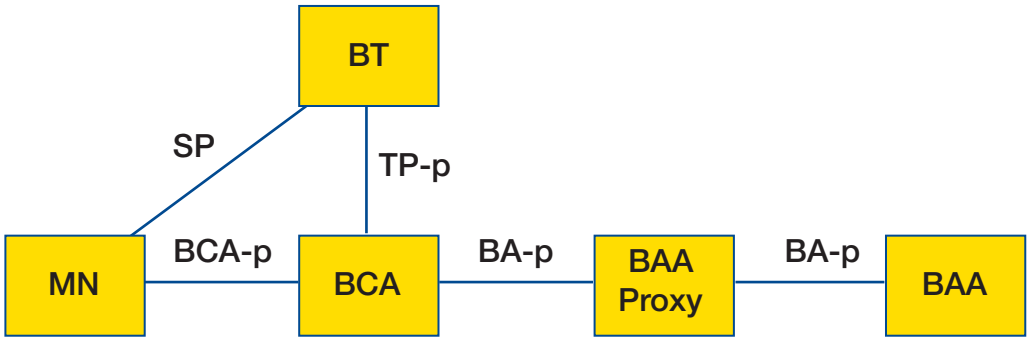
2.9.4.1.1. GSABA Architecture

Figure 2.9.12 illustrates the basic architecture elements of GSABA. The Bootstrapping target (BT) is the entity that offers the requested service. In MIPv6 case, the firewall will act as the BT. The Bootstrapping

Configuration Agent (BCA) provides necessary bootstrapping information to the MN. The Bootstrapping Authorization Agent (BAA) stores the MN's profile and acts as an Identity Provider. For roaming purposes there will be an additional architectural element, the BAA Proxy. It's function is to forward and, if necessary, to modify policies.

One important interface between the BT and the BCA is the Bootstrapping Target Protocol (TP-p) that provides the mechanism to exchange service related information. RADIUS and Diameter are example protocols for TP-p. The Bootstrapping Protocol (BCA-p) will transmit bootstrapping information to the MN and also informs it about the authorization decision taken by the BAA and BAA Proxy. HTTP is a possible candidate for the BCA-p interface. RADIUS and Diameter is again used for delivering decisions between the BAA and the BCA via the Bootstrapping Agent Protocol (BA-p). The interface between the MN and the BT is the Service Related Protocol (SP) that ideally does not need to be changed to support GSABA when certain minimum requirements are met. The latter aspect is particularly important since it allows a smooth transition for various protocols since no additional standardization work is necessary if basic security mechanisms are already specified.

Figure 2.9.12: The GSABA Architecture



2.9.4.1.2. GSABA Integration in the NSIS NAT/FW NSLP

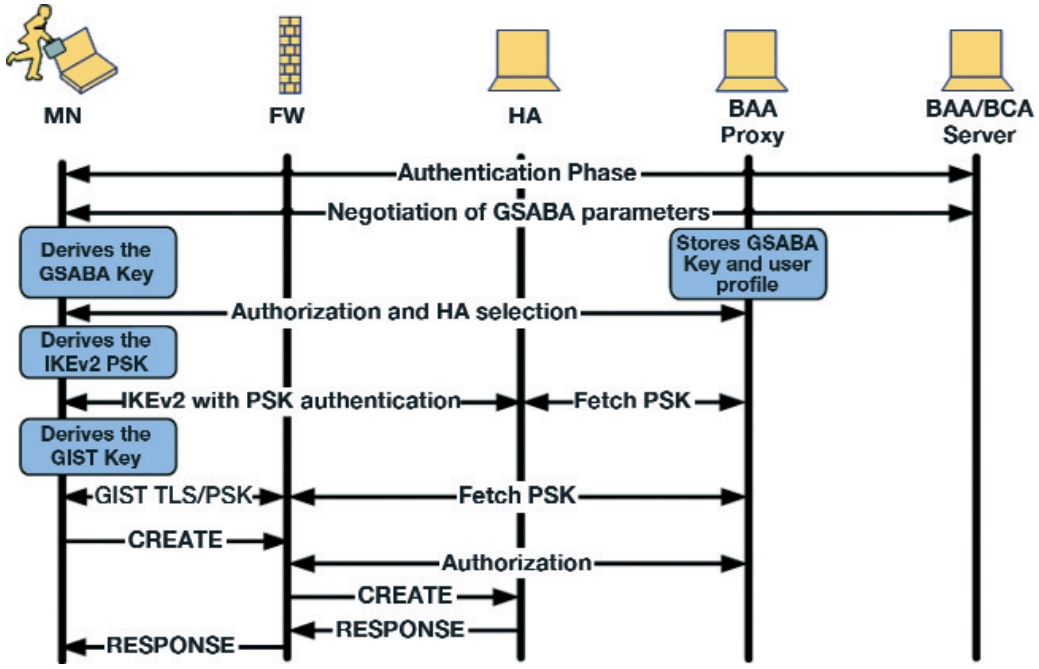
The integration of GSABA into the NSIS NAT/FW NSLP requires, in case of firewall traversal for Mobile IPv6, the investigation of the three scenarios described in Section 2.9.2.1. In all three following scenarios, the firewall acts as the BT. The first scenario additionally details bootstrapping of Mobile IP via the same infrastructure.

Firewall located at the edge of MN's ASP

When the MN wants to install rules at the firewall, it usually uses CREATE or EXT. Therefore, it has to interact with the BAA. After the MN and the BCA/BAA have mutually authenticated each other, the BAA will send the GSABA Key and the users profile to the GSABA Proxy, which will store this information locally. The MN gets the GSABA Key and is able to request HA information at the GSABA Proxy. The proxy checks whether the MN is authorized and selects a HA. Then, the MN derives the IKEv2 PSK to authenticate against the HA. The HA will fetch the PSK from the GSABA Proxy. After this step, the MN derives the GIST Key and uses it as a PSK in the TLS handshake with the firewall. At this point the firewall fetches the PSK also from the GSABA Proxy.

Now, the MN starts NSIS NAT/FW signalling, for example, by sending a CREATE message through the firewall to the HA. The firewall authorizes the CREATE message. Figure 2.9.13 shows an example message flow for the above-described procedure.

Figure 2.9.13: The GSABA message flow, Firewall located at the edge of MN's ASP



Firewall located at the edge of CN's ASP

In this scenario, the CN needs to establish a security association between the firewall and itself. When the MN wants to open pinholes at this firewall, it firstly signals this with the CREATE message. As there is no authorization at this point, the firewall responses with a error message including it's domain name. The MN now derives a NSLP Key from the GSABA Key and sends the CREATE message again. At this time, it uses the PSK in the TLS handshake with the firewall and the firewall fetches the NSLP Key from the GSABA Proxy. Hence, the firewall is able to authorize the message sent by the MN and forwards it to the CN, which replies with a RESPONSE message on the same path. The MN and the CN are now able to send the CoTI/CoT messages for route optimization.

The message flow for the HoTI message is different as the MN tunnels the HoTI message via its HA, which will then trigger a CREATE message for opening pinholes at the firewall on the CN side. The firewall can now authorize the CREATE message. The subsequent BU/BA message exchange between the MN and the CN will be able to traverse the firewall without problems.

Firewall located at the edge of MN's MSP

In this scenario, the MN first needs to be authorized against the GSABA Server to get the GSABA Key. Afterwards the MN derives the GIST Key and uses it as a PSK in the TLS handshake with the firewall. The firewall fetches the PSK from the GSABA Proxy and the MN could send a CREATE message to allow IKEv2 traffic to traverse the firewall. The firewall checks the authorization at the GSABA Server and then decides if the CREATE message can traverse the firewall. The MN derives the IKEv2 PSK to authenticate against the HA. The HA will fetch the PSK from the GSABA Proxy. The GSABA infrastructure may provide additional information to the firewall in order to pre-authorize subsequent NAT/FW messages.

2.9.4.2. Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an XML-based framework for creating and exchanging security information. In the course of making, or relying upon such assertions, SAML system entities may use SAML protocols, or other protocols, to communicate an assertion itself, or the subject of an assertion.

Thus one can employ SAML to make and encode statements such as "Alice has these profile attributes and her domain's certificate is available over there, and I'm making this statement that she is allowed to traverse firewalls within this particular domain." Then, an end host can cause such an assertion to be conveyed to some party, for example a firewall, who can then rely on it for computing an authorization decision, for example using it as input into some local policy evaluation for granting the establishment of a pinhole.

A possible approach of applying SAML for NAT/FW NSLP signalling in Mobile IPv6 environments is as follows. The MN first asks the Identity Provider (IdP) to get such an assertion before commencing signalling with the firewall. The IdP will authenticate the user or end host and will return an assertion in the case of success. When interacting with a firewall the MN will attach the SAML assertion to the message. After that the firewall verifies whether the assertion is valid and if the MN is authorized to perform the indicated action (e.g., creating a pinhole) for further communication. An error is returned in case the end host is not authorized. Despite the popularity of SAML for identity management there is also a disadvantage, namely the large size of the XML-based assertions when conveyed by value. To overcome this limitation a reference to a SAML assertion can be used instead; the firewall then has to first resolve the reference in order to obtain the assertion, for example using an HTTP lookup.

2.9.4.3. TLS using EAP Authentication

Transport Layer Security (TLS) using EAP Authentication [21] (TLS-EAP) enhances the TLS handshake with support for authorization with the Extensible Authentication Protocol (EAP). The fact that NSIS allows TLS to be used, the integration with EAP is attractive since the TLS server is able to relay EAP payloads to the existing AAA infrastructure in order to offload authentication, authorization and accounting tasks.

When TLS-EAP is used then the TLS handshake is initiated and EAP messages are exchanged between the TLS client (i.e., NAT/FW client) and the TLS server (i.e., firewall). The TLS server forwards messages to the AAA infrastructure whenever it is not able to handle authentication locally. The TLS server does not need to understand the specific EAP method and acts as a relay until the exchange is completed and the AAA server indicates the success or failure of the EAP exchange to the TLS server. Later, when the NAT/FW client requests the creation of new firewall pinholes, the firewall may need to initiate an authorization request towards the AAA server. The AAA server may either grant or deny the request and returns the decision to the firewall. The advantage of using TLS-EAP is the smooth integration with the AAA infrastructure and the simple enhancements needed for EAP integration into TLS due to the extensibility of the NSIS framework, in this particular case GIST. A weakness of using TLS-EAP is the additional message exchanges since EAP is quite chatty.

2.9.5. OPEN ISSUES AND FUTURE WORK

The firewall traversal solution based on the IETF NAT/FW NSLP presented in this paper can deal with the problems of having firewalls in Mobile IPv6 environments. However, the approach as described in this paper might not be efficient enough for some environments. As a result, the optimization of the signalling exchange

and the reduction of the signalling delay are for further study. Overall, more work on performance optimizations and scalability investigations are necessary.

Firewall traversal requires strong authentication and authorization. An initial set of security mechanisms are proposed in Section 2.9.4 but further work is needed to investigate the details in order to study the security properties, potentially including a formal analysis. For example, currently there is no SAML "profile" or "binding" defined that describes in detail how SAML assertions are carried within NSIS.

Todays infrastructure mostly supports MIPv4, rarely MIPv6. Therefore, it is necessary to investigate a MIPv6/v4 dual stack solution. We are currently finalizing a prototype implementation to prove the feasibility and usability of such a Mobile IPv6 firewall traversal approach.

2.9.6. CONCLUSION

This paper shows how the NSIS NAT/FW NSLP can address the issues caused by stateful packet filter firewalls encountered in a Mobile IPv6 network. We described the problems and impacts of having firewalls in Mobile IPv6 environments and presented a firewall traversal solution based on the IETF NSIS framework, which can handle all these issues in the different scenarios. It has to be noted that a real scenario could include a combination of some set of these cases. In contrast to other middlebox configuration solutions, the NSIS solution can offer a solution for all deployment scenarios assuming that the MN, the CN, the HA and the firewalls are NSIS NAT/FW NSLP aware.

In contrast to other explicit middlebox configuration approaches like MIDCOM, NAT/FW NSLP requires more signalling but does not require knowledge about the topology and avoids possible performance problems caused by the deep packet inspection of such approaches. M-ICE that builds on STUN is a very recent proposal that is designed based on a different security framework but conceptually similar to the NSIS NAT/FW NSLP.

Finally, this paper also outlines approaches for addressing the security aspects for NAT and firewall traversal. These approaches are based on the recently developed GSABA (a AAA-based bootstrapping framework), TLS-EAP that reuses EAP and the AAA infrastructure and SAML assertions. Further studies with respect to the aspects described in Section 2.9.5 are necessary.

2.9.7. ACKNOWLEDGMENTS

We would like to thank Ivano Guardini, Li Cai, Qin Wu, Ingo Juchem, Swen Weiland, Jan Demter and Mehmet Ersue for their contributions and insightful discussions.

This work has been partially supported by the EC FP6 IST research project ENABLE - Enabling Efficient and Operational Mobility in Large Heterogeneous IP Networks.

2.9.8. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6 ", RFC 3775, June 2004.

[2] J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[3] J. Rosenberg, R. Mahy, C. Huitema, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", I-D (draft-ietf-behave-turn-04), work in progress, July 2007.

[4] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", I-D (draft-ietf-mmusic-ice-17), work in progress, July 2007.

[5] J. Quittek, M. Stiemerling, P. Srisuresh, "Definitions of Managed Objects for Middlebox Communication", I-D (draft-ietf-midcom-mib-09), work in progress, October 2006.

[6] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[7] R. Hancock, G. Karagiannis, J. Loughney, and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

[8] M. Stiemerling, H. Tschofenig, and C. Aoun, "A NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", I-D (draft-ietf-nsis-nslp-natfw-15), work in progress, July 2007.

[9] F. Le, S. Faccin, B. Patil, and H. Tschofenig, "Mobile IPv6 and Firewalls: Problem Statement", RFC 4487, May 2006.

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

[11] H. Tschofenig, G. Bajko, "Mobile IP Interactive Connectivity Establishment (M-ICE)", I-D (draft- tschofenig-mip6-ice-01), work in progress, July 2007.

[12] H. Tschofenig, G. Bajko, "Firewall friendly Return- Routability Test (RRT) for Mobile IPv6", I-D (draft-bajko-mip6-rrtfw-02), work in progress, July 2007.

[13] D. Wing, J. Rosenberg, H. Tschofenig, "Discovering, Querying, and Controlling Firewalls and NATs using STUN)", I-D (draft-wing-behave-nat-control-stun- usage-03), work in progress, July 2007.

[14] D. Wing, "Media Session Authorization", I-D (draft-wing-session-auth-00), work in progress, January 2006.

[15] "An Implementation of the Next Steps in Signaling (NSIS) Protocol Suite at the University of Göttingen", http://user.informatik.uni-goettingen.de/nsis/.

[16] N. Steinleitner, H. Peters, H. Tschofenig, X. Fu, "Implementation and Performance Study of a New NAT/Firewall Signaling Protocol", ADSN2006, in conjunction with ICDCS 2006, Portugal, July 2006.

[17] S. Thiruvengadam, H. Tschofenig, F. Le, N. Steinleitner, X. Fu, "Mobile IPv6 - NSIS Interaction for Firewall traversal", I-D (draft-thiruvengadam-nsis-mip6-fw-06), work in progress, March 2007.

[18] J. Manner, M. Stiemerling, H. Tschofenig, "Authorization for NSIS Signaling Layer Protocols", I-D (draft-manner-nsis-nslp-auth-03), work in progress, March 2007.

[19] F. Kohlmayer, H. Tschofenig, R. Falk, R. Lopez, S. Hernandez, P. Segura, A. Skarmeta, "GSABA: A Generic Service Authorization Architecture", MobiArch'06, San Francisco, December 2006.

[20] P. Eronen, H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[21] Y. Nir, Y. Sheffer, H. Tschofenig, P. Gutmann, "TLS using EAP Authentication ", I-D (draft-nir-tls-eap-01), work in progress, July 2007.

2.10 Analysis of Options for Securing NATFW NSLP

Qin Wu, **Huawei Technology**

ABSTRACT

NSIS NATFW is a client initiated firewall traversal solution that allows hosts to signal inband (on the data path) for NATs and firewalls to be configured according to the needs of the application data flows. However, securing signals for firewall traversal is an important issue. This document investigates the different options for securing NSIS NATFW with the goal of using existing credentials, user and policy databases and other security infrastructure. Transport Layer Security (TLS) with X.509 PKI, Extensible Authentication Protocol (EAP), 3GPP Generic Bootstrapping Architecture (GBA) and authorization token among these options are examined. The advantage and drawbacks of these options is evaluated.

2.10.1. PROBLEM STATEMENT

Firewalls are an integral aspect of a majority of IPv6 networks that provide protection to network elements by enforcing access and filter policies which are used to monitor and control traffic to and from a network. The main purpose is to detect and prevent Denial of Service (DoS) attacks or unwanted traffic on a network. However most firewalls available for IPv6 networks do not support Mobile IPv6 which could prevent future large-scale deployment of the Mobile IPv6 protocol.

In order to solve NAT/firewall traversal problem, several alternative firewall traversal solutions are discussed in IETF mip6 work group. NAT/FW NSLP is one such solution to be that also supports mobility. The basic idea of NAT/FW NSLP is described as follows:

In the case where control or data packets are passing through firewall, a Mobile Node (MN) will initialize firewall traversal signalling to open pinholes through the firewall. However it brings two problems:

1. what make firewalls trust firewall traversal signalling from mobile node and establish corresponding rules?
2. Is firewall traversal signalling transported securely? i.e., is there any malicious node eavesdropping on or tampering with firewall signalling?

Since NSIS Framework consists of two layers. A message transportation layer and a signalling application layer. Security issues in both levels need to be considered in designing a firewall traversal security mechanism. One issue is the authentication mechanism in the message transportation layer, i.e., it is necessary to establish trust relationship between two peers. Generic Internet Signaling Transport (GIST) in the peer either drops a request, or delivers it to the NSLP for processing together with whatever authenticated information about the requestor can be found. Another is service authorization mechanism in the signalling application layer, i.e., one authorization entity is needed to make authorization decisions whether an entity can be authorized and what resources that entity is allowed to access according to their authentication identifier, e.g., the NSLP can, somehow, look up this identity from an access control list of some sort in order to find out what kind of rules it is allowed to create. Authenticating a particular identity (identifier) may not be always needed if the identifier is not actually used in making the authorization decision.

2.10.2. EXISTING SECURITY INFRASTRUCTURE OPTIONS IN SECURING NSIS COMMUNICATION

NSIS protocol is similiar to the RSVP protocol. It enables message transportation between two neighbouring peers in a more universal network deployment scenario. Thus authentication between peers in message transportation layer is required. Until now there are several existing security mechanisms that can be used to secure NSIS communication, e.g., TLS, EAP, GBA, Authorization Token, etc. However, each security infrastructure makes certain technical assumptions, has certain constraints and may only be applied in certain situation. As a result, a single solution is unlikely to be appropriate for all usage scenarios. Thus we examine several security infrastructure options.

1 Transport Layer Security with X.509 PKI

2 Extensible Authentication Protocol

3 Generic Bootstrapping Architecture

4 GSABA

5 Authorization Token

2.10.2.1. Transport Layer Security (TLS) with X.509 PKI

TLS [1] is one of the most popular security mechanisms for protecting application-layer protocols. TLS supports authenticating the parties using public-key certificates [1], pre-shared keys [2], and Kerberos [3], and also includes an "anonymous" Diffie-Hellman key exchange that does not authenticate the parties. TLS is usually run over TCP or SCTP, but datagram TLS [4] also allows the use of unreliable transports such as UDP.

Here we consider how TLS authenticated using certificates can be used to protect GIST messaging over TCP. TLS is usually used with X.509 PKI. The detailed authentication procedure is exemplified as follows:

1. When a NSLP is started, it must at least configure the key/certificate for establishing and accepting messaging associations protected with TLS.

2. Peer A's NSLP sends a message and Peer A's GIST notices that a new messaging association is needed, and initiates Query/Response with Peer B

3. Peer A establishes a TCP connection to IP_B:PORT_B, and begins the TLS handshake

4. Peer A verify certificate from Peer B

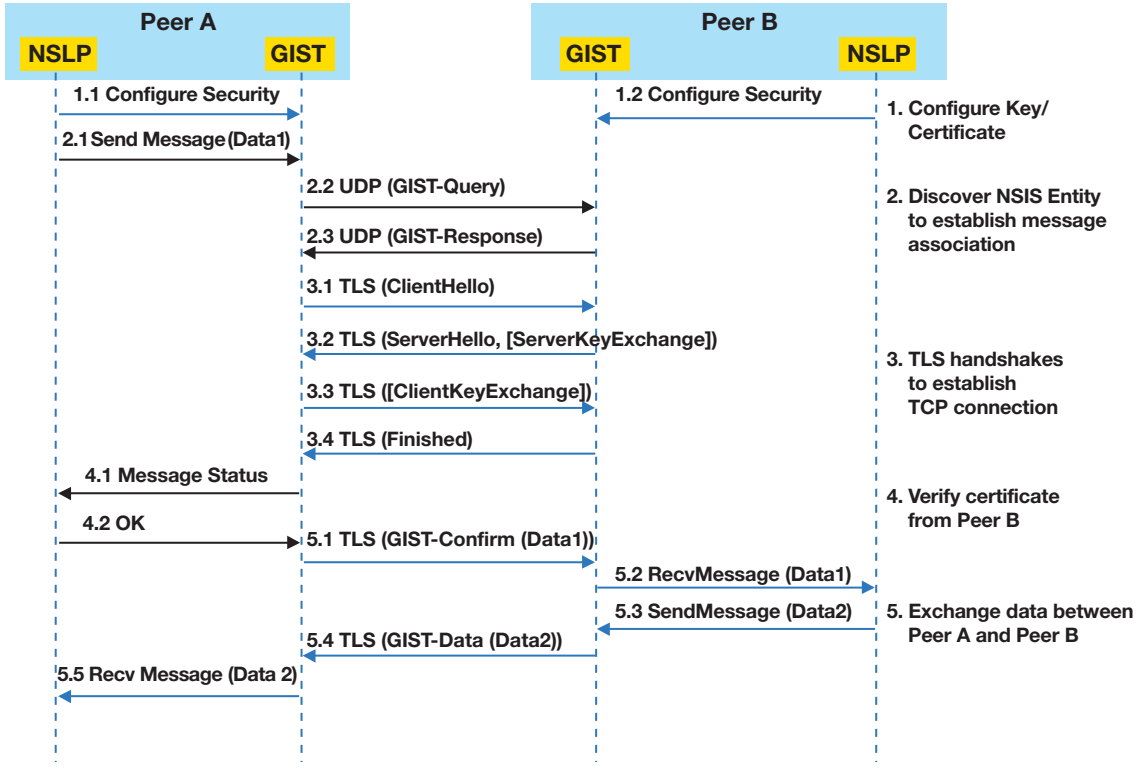
5. Exchange data between Peer A and Peer B.

From above authentication procedure, it is apparent that TLS depends on certificates to derive key materials and it is difficult to integrate TLS using a X.509 PKI with an AAA infrastructure. This approach is suitable when an existing authentication infrastructure based on X.509 certificates is present. This clearly does not cover all possible scenarios for NSIS: for instance, assuming that all users have X.509 certificates has proven to be unrealistic in many environments.

However, we do allow flexibility in what kind of semantics the certificates have. X.509 certificates bind together one or more identifiers and a public key, but sometimes they have additional authorization semantics: the certificate either implicitly or explicitly grants of permission to do 'something' (that is not simply an identifier uniquely identifying the subject).

This approach can be used to implement authentication between two neighbouring peers. But it is not appropriate for access authentication in foreign network for the simple reason that not all access routers install certificates.

Figure 2.10.1: TLS with X.509 PKI



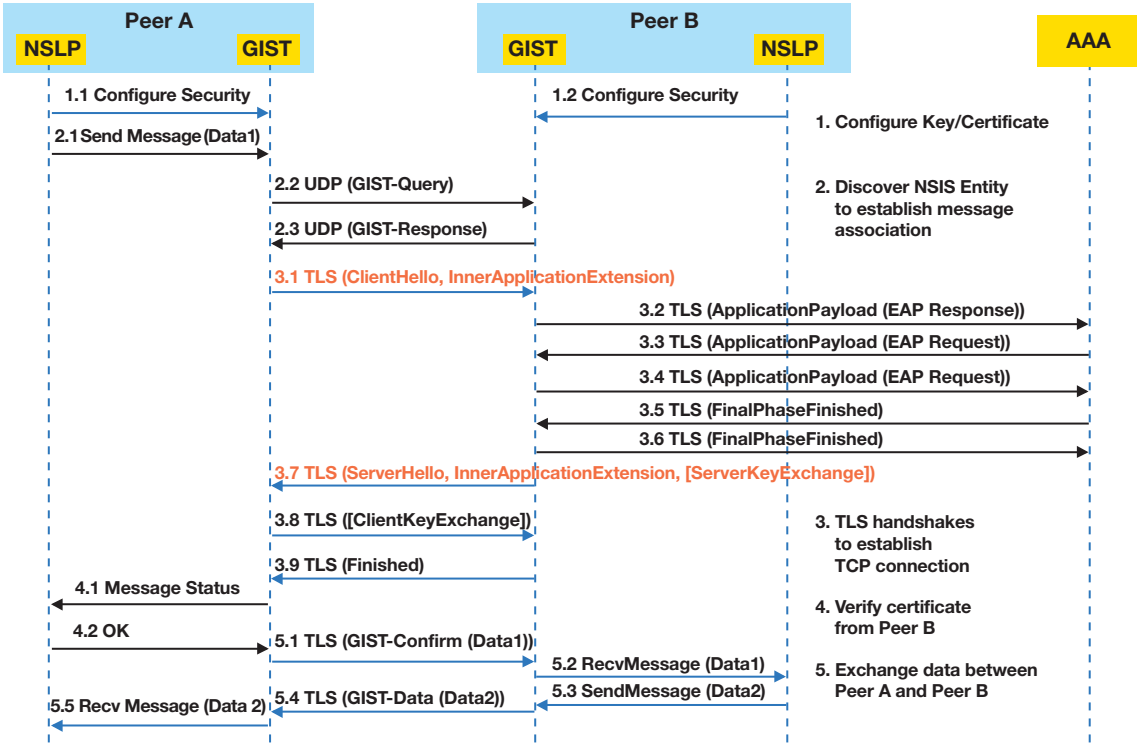
2.10.2.2. Extensible Authentication Protocol (EAP)

In order to support different deployment scenarios, NSIS signalling should have flexible authentication and authorization capabilities. This can be achieved by interacting with the AAA infrastructure for computing the authorization decision of various NSLP requests. To support existing credentials and the large number of different usage scenarios, the Extensible Authentication Protocol (EAP) might be reused. EAP provides the following capabilities:

1. Flexible support for authentication and key exchange protocols.
2. Ability to reuse existing long-term credentials and already deployed authentication and key exchange protocols (for example, the UMTS-AKA)
3. Integration into the existing AAA infrastructure, namely RADIUS [5] and Diameter [6].
4. Ability to execute the authorization decision at the user's home network based on the capabilities of protocols like RADIUS and Diameter.

Here we first consider how EAP authenticated in TLS exchange can be used to protect GIST message over TCP. The authentication procedure of TLS/IA is exemplified as follows:

Figure 2.10.2: TLS/IA

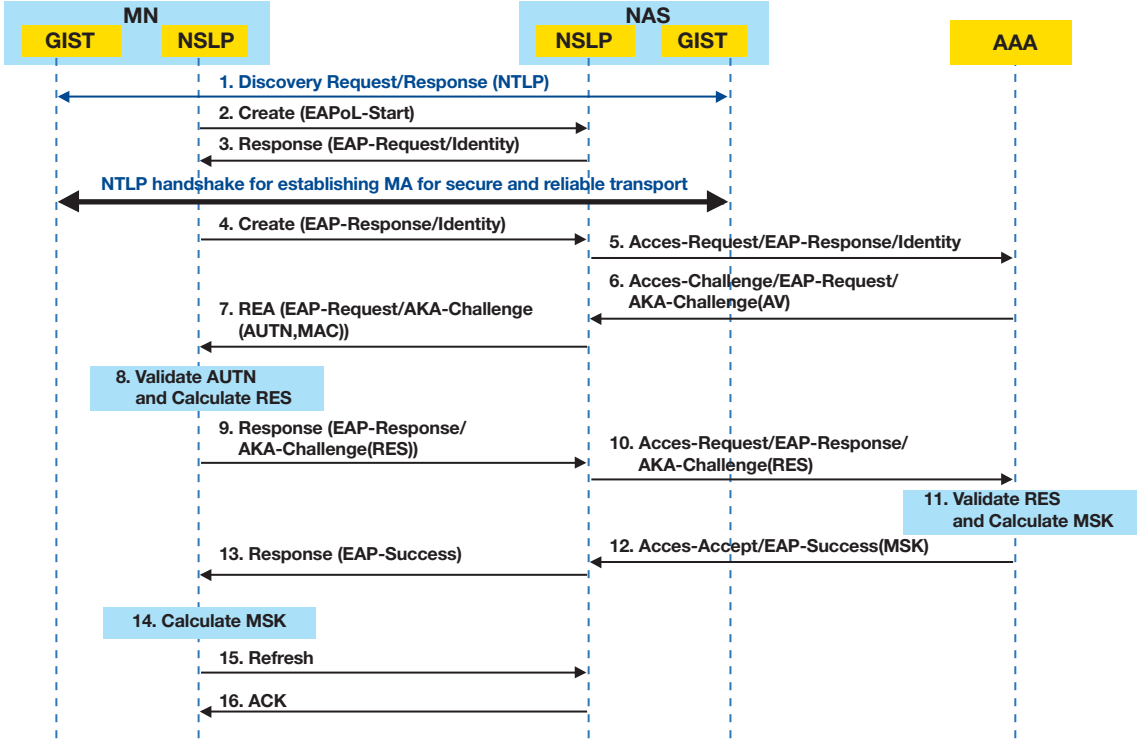


1. When a NSLP is started, it must at least configure the key/certificate for establishing and accepting messaging associations protected with TLS.
2. Peer A's NSLP sends a message and Peer A's GIST notices that a new messaging association is needed, and initiates Query/Response with Peer B
3. Peer A establishes a TCP connection to IP_B:PORT_B, and starts the TLS handshake with Peer B in which Peer B initiates EAP process with AAA infrastructure to obtain server key material.
4. Peer A verify certificate or key material from Peer B
5. Exchange data between Peer A and Peer B.

The main advantage of this approach is that it does not require modifications for the NSIS protocol suite since the EAP exchange is encapsulated within the TLS Handshake exchange. The AAA interaction triggered as part of the TLS I/A (and the EAP method processing) performs only authentication which, of course, requires a third party to provide keying material. When authentication and key exchange is provided with TLS I/A (and therefore the embedded EAP exchange) then the specific NSLP payloads are not yet processed. Hence, authorizing the specific NSLP operation (such as a request for reserving a certain amount of bandwidth) can only be provided at the NAT/FW NSLP layer, i.e., key establishment and a separate exchange might be required at the NSLP.

Then we give another example to consider how EAP integration into NSLP can be used to protect NSLP. The authentication procedure of EAP in NSLP is as follows:

Figure 2.10.3: EAP in NSLP



1. MN sends create message with EAPoL-Start option included.
2. NAS replies with response message with EAP-Request option for MN's Identity.
3. MN sends create message with EAP-Response option, MN's identity included.
4. NAS forwards EAP-Response option to AAA in Access Request.
5. AAA initializes Access Challenge with AKA challenge to MN.
6. NAS forwards AKA challenge in notify message to MN.
7. MN validate authentication token and calculate RES.
8. MN replies with response message, AKA-challenge included in EAP-Response option.
9. NAS forwards EAP-Response to AAA.
10. AAA validates RES in AKA challenge and calculate MSK.
11. AAA replies with Access-Accept message, EAP-success option included.
12. NAS forwards EAP-Success in notify message to MN and MN calculate MSK.

The advantage of this approach is that it allows a seamless inter-working between EAP and

NAT/FW NSLP protocols, with a proper encapsulation of the EAP payloads into NAT/FW NSLP Create/Notify/Response messages. However EAP methods should deal with fragmentation, reliability and re-transmission of the EAP data into the NAT/FW NSLP messages. For integrating EAP into a NSLP application, a new NSLP payload object should be defined to carry the EAP packets. The EAP session will be established between a NAT/FW-NSLP initiator, a NAT/FW-NSLP policy aware node, and an Authorizing entity. A NAT/FW policy aware node should be authenticated and authorized to be one side in an AAA NAT/FW Authorization session In addition, the authorization decision is based not only on an authenticated identity, but also on the description of requested NAT/FW parameters, which would clearly identify the type of the requested service.

Until recently, engineers and scientists thought that running one authentication and exchange protocol on top of another increases the security of the entire exchange. Running these two exchanges in isolation may allow for Man-In-The-Middle (MITM) attacks, for the NSIS case, the transport layer is secured by TLS and additional authentication and authorization is provided at the signalling layer, Hence, additional security attributes need to be exchanged through the API between the transport and the signalling layer.

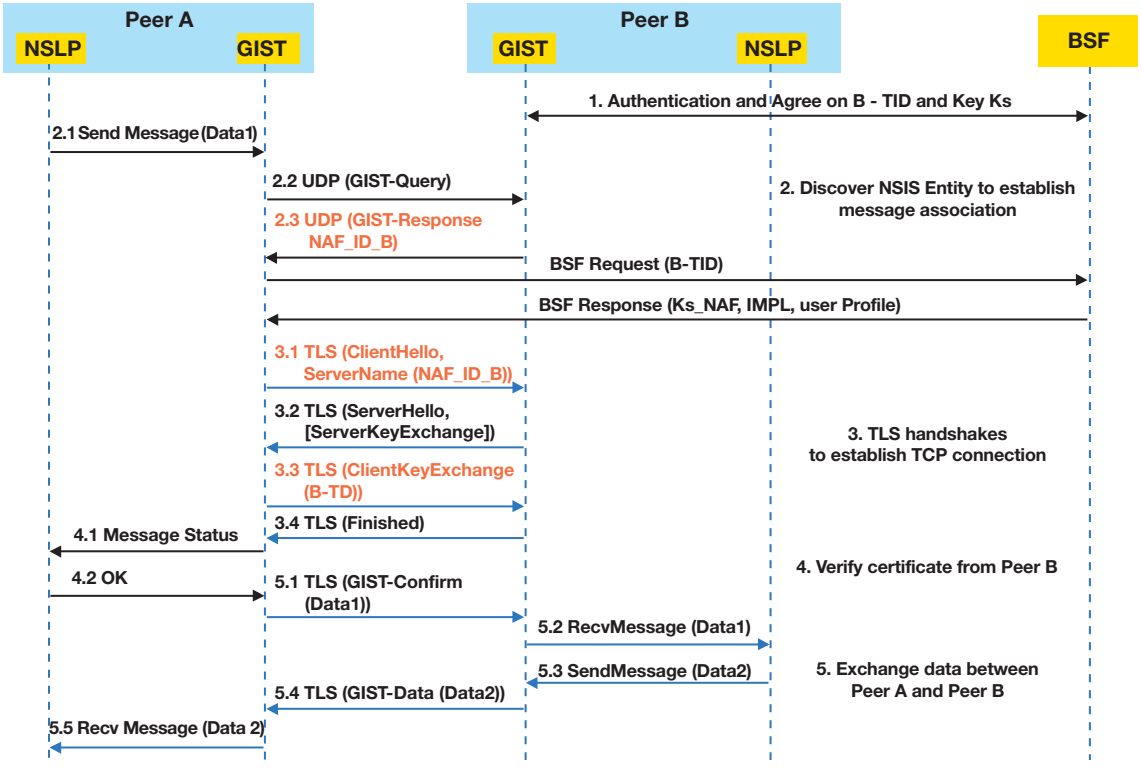
The above two authentication procedures both build trust relationship between two neighbouring peers. The difference between them is that EAP is carried in a different layer. For EAP in NSLP, EAP procedure can be used to generate session credentials that secure NSLP signalling from being tampered by other malicious nodes, while for TLS/IA, key materials can not be easily obtained from GIST layer to secure NSLP signalling.

2.10.2.3. 3GPP Generic Bootstrapping Architecture (GBA)

The 3GPP Generic Bootstrapping Architecture (GBA), specified in [7], is an authentication system with three parties: a trusted third party (called Bootstrapping Server Function or BSF), is involved in authentication and key exchange between two other nodes, a client (called User Equipment or UE) and a server (called Network Application Function or NAF).

The goal of the architecture is to isolate knowledge of long-term secrets and credentials to a single trusted node, the BSF. The actual servers (NAFs) do not have access to the clients' long-term credentials, and indeed, do not have to know the type of credentials (such as smart cards) that were used between the client and the BSF. Here we consider how 3GPP Generic Bootstrapping Architecture (GBA) can be used to protect GIST messages.

Figure 2.10.4: GBA Architecture



1. Peer B is authenticated by BSF in advance and B-TID and Key Ks are agreed between Peer B and BSF.
2. Peer A's NSLP sends a message and Peer A's GIST notices that a new messaging association is needed, and initiates Query/Response with Peer B
3. Peer A's GIST B-TID to the BSF, and gets back a server-specific key (Ks_NAF), the user's permanent identity (IP Multimedia Private Identity or IMPI) and the application-specific parts of the user profile.
4. Peer A establishes a TCP connection to IP_B:PORT_B, and starts the TLS handshake
5. Peer A verify certificate from Peer B
6. Exchange of data between Peer A and Peer B.

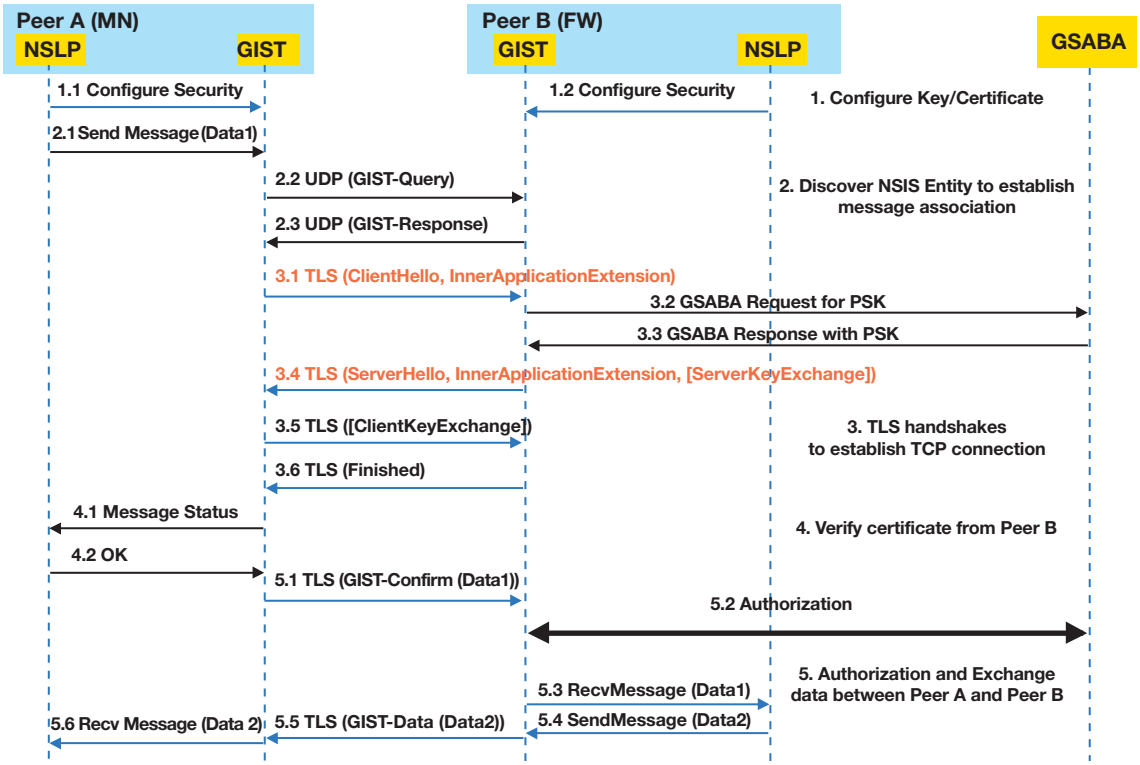
This approach uses an authentication entity identifier to request key material from the AAA.

Infrastructure and establish trust relationship with an authenticated entity. It appears to use mechanisms similar to the GAA HTTPS services. The difference is that GAA HTTPS knows the FQDN of the responding node beforehand, while this approach can obtain FQDN through GIST exchange message.

2.10.2.4. GSABA

GSABA provides a generic service authorization and bootstrapping framework that leverages the use of the AAA infrastructure, extending it but without requiring additional credentials. This approach is attractive due to the large deployment base offered by the AAA architecture. GSABA is able to bootstrap mobility, network and application layer services independently of network access authentication. Challenges remain with regard to security and privacy, authorization complexity and performance. Here we give one example to explain how GSABA can be used to protect NSLP.

Figure 2.10.5: GSABA Architecture



1. When a NSLP is started, it must at least configure the key/certificate for establishing and accepting messaging associations protected with TLS.
2. Peer A's NSLP sends a message and Peer A's GIST notices that a new messaging association is needed, and initiates Query/Response with Peer B
3. Peer A establishes a TCP connection to IP_B:PORT_B, and starts the TLS handshake with Peer B in which Peer B initiates AAA exchange with GSABA infrastructure to obtain PSK.
4. Peer A verify certificate or key material from Peer B
5. Authorization and Exchange data between Peer A and Peer B.

From the above procedure, GSABA approach is same like TLS/IA approach. The difference between them is that communication between Peer B and AAA architecture is not based on TLS but AAA protocol. Also authorization process is introduced to make service authorization decision.

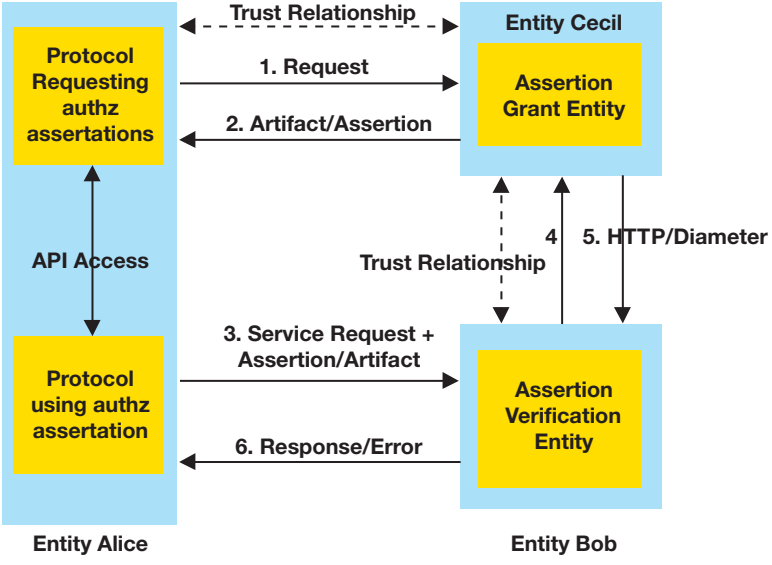
2.10.2.5. Authorization Token

Cryptographic computations are expensive and computing authorization decisions may require a lot of time and may also require multiple messages between the entity enforcing the decisions and the entity computing the authorization decision. To add complexity, in a mobile environment these entities are physically separated - or not even in the same administrative domain. Accordingly, the notion of "authorization token" is one potential application of authorization assertions, and trait-based authorization - a user is authenticated and authorized through one protocol, and can reuse the resulting authorization assertion in other, unrelated protocol exchanges.

An Authorization Token based security mechanism is usually used to complete authentication and authorization with the other security infrastructures mentioned above. Here we consider a basic authorization framework based on authorization token and the authorization procedure is described as follows:

1. A Client requests authorization token from the grant entity
2. The grant entity replies to the client with the corresponding token
3. The Client sends authorization request to assertion verification entity with client's token
4. The Assertion verification entity exchange message with the third grant entity to validate token
5. In the case of a valid token, the assertion verification entity responds to client with an authorization result.

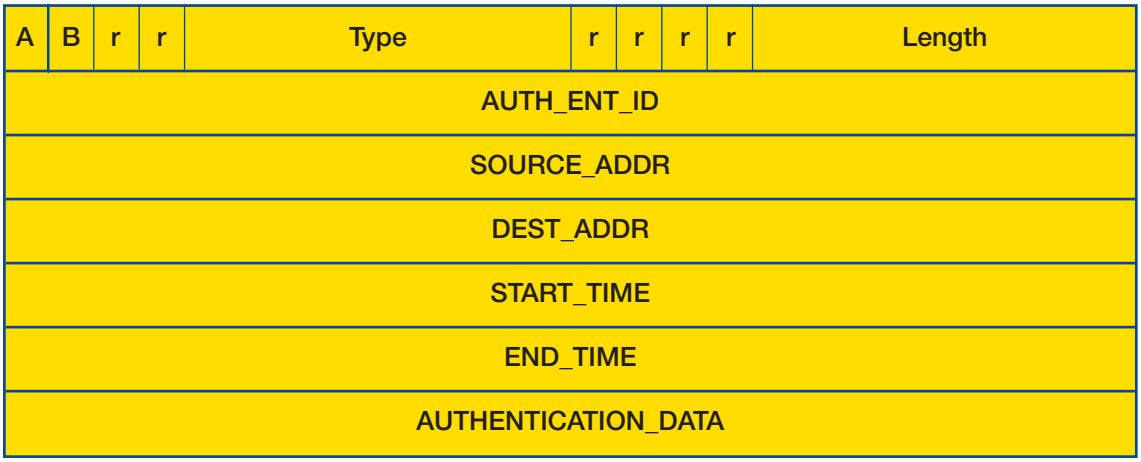
Figure 2.10.6: Authorization Framework based on authorization token



With authorization token, it is beneficial for the third party to compute authorization decision about what entity can be authorized and what resource that entity is allowed to access.

Subsequently according to [8], the authorization token format is defined as follows. Authorization token mainly consist of authorization identifier, source address, destination address, session start time, end time and authentication data. and policy element of session is included in authentication data.

Figure 2.10.7: Authorization Token Format



It should be noted that different authentication mechanism have different formats of authorization token. Here we consider two type of authorization token format, one is symmetric share key based authorization token, and another is a public key based authorization token. The main difference between two types of token is that different key environment has different AUTH_ENT_ID. In a symmetric share key environment, a token may be used with a AAA infrastructure, AUTH_ENT_ID is usually a IPv4 address, IPv6 address or FQDN,NAI. While in public key environment, a token may be used with digital certificates, AUTH_ENT_ID is usually X509_V3_CERT or PGP_CERT.

2.10.3. Comparison among existing security infrastructure options

Comparing the above security infrastructures, each security mechanism has its advantage and disadvantage. Here we present the following table to evaluate the characteristics of each mechanism.

	TLS+X.509	EAP	GBA	GSABA
Source for Key Materials	X.509	AAA	AAA	AAA

	TLS+X.509	EAP	GBA	GSABA
Authorization Token	Not necessary	Not necessary	Not necessary	Needed
Layer to establish trust relationship	GIST Layer	GIST Layer or NSLP layer	GIST Layer	GIST Layer and NSLP layer
Integration with AAA	Hard	Easy	Easy	Easy
Authentication signaling overhead	small	large	small	small

2.10.4. CONCLUSION

NAT/FW NSLP can be used to realize mobile ipv6 firewall traversal. However for security consideration, it needs to establish a secure tunnel between any two neighbouring peers before delivering a NSLP message. Furthermore a firewall needs to authenticate an NSLP message before allowing NSLP message to pass through. Using the existing security infrastructure options, a trust relationship between peers can be established in two layers. TLS with PKI X.509 is suitable when an existing authentication infrastructure based on X.509 certificates is present. This clearly does not cover all possible scenarios for NSIS. EAP and GBA approaches are appropriate for establishing trust relationship between GIST layers or between NSLP layers, however the exchanges taking place in each layer are completely isolated, this can potentially lead to Man-In-The-Middle (MITM) attacks. For GSABA approach, the transport layer is secured by TLS in message transportation layer and additional service authorization based on authorization token can be provided at the signalling layer. It provides a generic service authorization and bootstrapping framework. As a result, GSABA would be our more favoured approach for securing NAT/FW NSLP.

2.10.5. REFERENCES

[1] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[2] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279.

[3] A. Medvinsky, M. Hur, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)", RFC2712, October 1999.

[4] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[5] C. Rigney, W. Willats, P. Calhoun, "RADIUS Extensions", RFC2869, June 2000.

[6] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[7] 3rd Generation Partnership Project (3GPP), "Generic Authentication Architecture (GAA); Generic bootstrapping architecture (Release 6)", 3GPP TS 33.220 V6.5.0, June 2005.

[8] J. Manner, M. Stiemerling, H. Tschofenig, "Authorization for NSIS Signaling Layer Protocols", draft-manner-nsis-nslp-auth-02, October 23, 2006.

2.11 Mobility in the Integration of Mobile Ad-hoc Networks

S. Sargento, R. Sarrô, **Instituto de Telecomunicações, Univ. Aveiro**

R. Duarte, **INESC Porto**

P. Stupar, **NEC Network Laboratories, Heidelberg**

ABSTRACT

There is an increasing requirement for ubiquitous access for users, enabling seamless support for different networks, with different technologies, and also with different types, such as moving networks and ad-hoc networks.

This paper describes the Ad-hoc network integration architecture and its mobility support, being developed inside the IST project Daidalos II. The main purpose of this architecture is to seamlessly support the movement of nodes between ad-hoc and infrastructure networks, maintaining in the ad-hoc networks all the features being supported in the infrastructure. The architecture makes use of IEEE 802.21 and NetLMM IETF concepts for mobility support and integration, and multihoming procedures for multiple gateways support.

2.11.1. INTRODUCTION

Daidalos II [1] is defining a network architecture to provide ubiquitous access integrating heterogeneous access networks and providing seamless movement among them. The architecture will also support the following features:

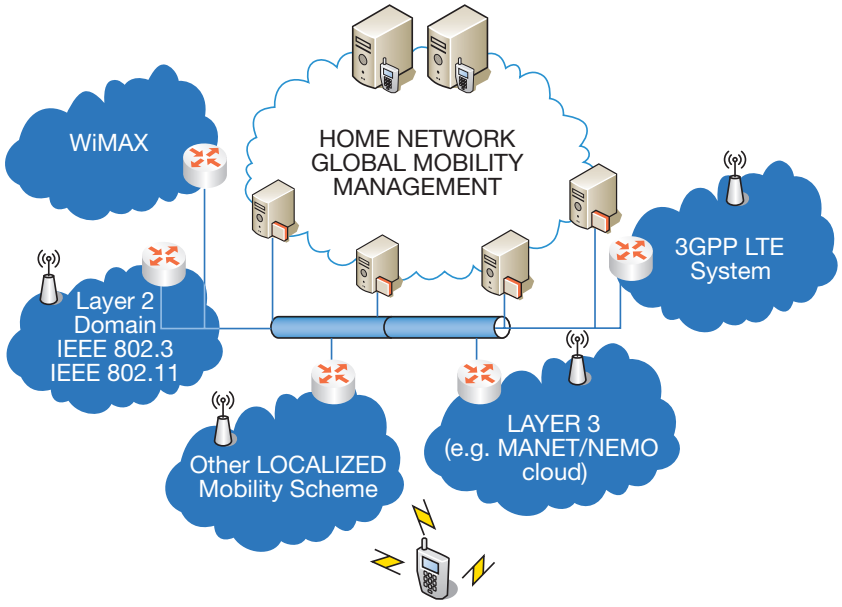
(1) mobility management is split between local and global domains;
(2) it explores an identity based mobility management solution through the independent and general management of identities;
(3) it integrates MANETs and NEMOs in the mobility architecture;
(4) it supports host multihoming, where the host owns multiple physical network interfaces and concurrently gets access through them;
(5) it integrates ubiquitous and pervasiveness concepts for customized services to the users.

This paper addresses the support of MANETs integration developed under the framework of Daidalos II. This architecture aims at seamlessly support nodes moving between infrastructure and ad-hoc networks, maintaining its access to the Internet with the same quality.

The proposed architecture (Figure 2.11.1) recognizes the current trend in networks towards a heterogeneous landscape of access providers. In such environment it is important to give to access providers (e.g. ISP or NAP) the flexibility of managing users mobility inside their own domain without requiring an interaction with the global mobile operator domain. Thus, it is envisioned the splitting of mobility management into different levels: a global level associated with the mobile operator network and a local level associated to network access providers. This view is in line with the current trends envisioned in the NetLMM IETF Working group [2] but important extensions are proposed: integration of MANET clouds and support of multihoming both at global and local domain.

In the global domain, mobility is supported by means of a global mobility protocol (GMP), such as Mobile IPv6 (MIPv6) [3] or Host Identity Protocol (HIP) [4]. Terminal mobility within a local domain is handled via local mobility protocols (LMP), which are transparent to the core network and independent of the GMP. In this case, when a mobile node moves within a local domain, only the LMP used in that domain operates; when the node moves across domains, only GMP operates.

Figure 2.11.1: Daidalos II network architecture



The envisioned MANETs in Daidalos II are considered as multi-hop networks connected to the core network by means of one or more gateways. Therefore, since access clouds are considered as local mobility domains, the integration of MANET within the overall architecture requires the analysis of the interaction between these networks with the LMP. These interactions depend on the number of gateways supported and its location, in the same or different local domains. This has impact on the ad-hoc nodes address configuration and on the mobility management.

Mobile terminals (MTs) equipped with multiple wireless access technologies enable the opportunity for multihoming. The control plane of such technology can be implemented at global level where the mobile operator owns the functionalities for multiple bindings or locally keeping this transparent outside the local domain. MTs can be therefore multihomed without the mobile operator knowing users' settings.

2.11.2. MANET SUPPORT FOR MOBILITY

2.11.2.1. Local Mobility

The local mobility protocol used is similar to the one in development in the NetLMM IETF WG [2]. Local mobility management scheme introduces a new entity in the network, called the Local Mobility Anchor point (LMA). The LMA will register and update the location of the mobile node inside the Localised Mobility Domain (LMD). The LMA works in close cooperation with the Access Routers (AR), since they will signal the LMA when a node moves (from one AR to another), so its location can be updated.

The local mobility management concept requires that the ARs of the network detect the nodes movement (nodes attachment and detachment to the network). In regular 802.11 WLAN networks, the ARs can easily detect new nodes recurring to standard IPv6 protocol operation (such as ICMPv6 neighbor discovery and router solicitation). However, since MANET is a multi-hop network, the ARs cannot detect the nodes presence when they are more that one hop away from them.

The adaptation needed for the MANET to work in a LMD relates to the gateway's ability to detect the nodes movement, This can only be done if the MT explicitly notifies the gateway about its new location; therefore, when a MT arrives to a new network, it signals the gateway so that the local mobility protocol can be triggered. This solution accomplishes two purposes: the movement detection by the local mobility protocol, and the start of the bootstrapping procedure, described in the next section. Once the AR (or gateway) detects the node presence, the local mobility protocol can operate in the same way than in infrastructure network.

2.11.2.2. IEEE 802.21 support in MANET

The IEEE 802.21 Media Independent Handover (MIH) services [5] is a working draft in development in the IEEE that aims to provide an 802 independent mechanism to perform handover between heterogeneous 802 systems, and between 802 systems and cellular systems. The great advantage of this protocol is that it provides a standard way of performing the signaling and control of the handover process independently of the 802 technologies being used underneath. The 802.21 MIH protocol requires that an abstraction layer is added between the 802 drivers and the upper layers, in order to provide the desired technology independency; this layer is called MIH Function (MIHF). The MIHF receives events and information from the drivers and processes it before sending it to the upper layers.

The advantages of the 802.21 protocol resides on the gained independency in the technology chosen, and thus seamlessly support of all 802 technologies, and the fact that it provides to the nodes and the network a generic way to detect events that have occurred in the terminal itself, as well as in the network.

A problem exists, however, with the way the 802.21 information (commands, information and events) is exchanged between the MT and the point of access to the network (PoA). The 802.21 is created for infrastructure networks, in where the MT and the PoA are always one link away from each other, which is

not true in ad-hoc networks. The solution found to solve this issue is to expose the MANET as a new technology to the MIHF that only supports information transport with L3 messages. This solution guarantees that the MIHF will be capable of sending and receiving 802.21 messages without requiring explicit support for multi-hop in the protocol. Another problem concerns with the integration of 802.21 in ad-hoc networks in terms of its events. The events, that are part of the 802.21 Event Service, are generated by the drivers and sent to the MIHF inside the MT. In the standard form, all events generated by the driver are sent to the MIHF, but as the MANET is now presented as an L3 technology, these L2 events are not meaningful. The events that are of interest to the decision making and handover controlling modules are generated based on L3 information (like route errors from the routing protocols or lost of connectivity with the gateway from the auto-configuration protocol). To solve this issue, a new module is added to the architecture of the terminal, between the driver and the MIHF. This module, the MANET Wrapper, has the responsibility to generate the 802.21 events from the L3, using information from the routing protocols and auto-configuration, emulating a virtual link (with one hop) between the MT and the gateway.

2.11.2.3. Handover candidates discovery

Before performing any handover, it is needed to know where to perform the handover. The handover target can be obtained by performing an active scanning of the wireless medium, followed by a validation of the results obtained. Using active scanning the MT will only consider as handover targets the networks that it can reach, since they are the results of the scanning.

The scan for surrounding networks is a normal 802.11 scan, in where the driver returns a list of available networks, containing both ad-hoc and infrastructure networks. The results corresponding to ad-hoc networks have to be then validated. The validation is required because the MAC layer of the driver does not contain information on whether the ad-hoc network has a gateway that provides connectivity to the core network and its services. The gateway presence is provided by the auto-configuration protocol. To perform validation, the MT has to associate to each found ad-hoc network and receive an auto-configuration message. Receiving one of these messages will ensure that the MANET is in fact connected to one gateway. In addition, the auto-configuration message will also have information about the gateway, such as its address, which is needed later to perform handover. Since the handover candidate discovery is also a part of the 802.21 protocol, this task will also be performed in the MANET by the MANET Wrapper. Upon reception of a scan request command sent by the MIHF, the MANET Wrapper will take control of the process, first performing the network scan, and then the results validation. Once the validation of all ad-hoc networks found is done, the MANET Wrapper will issue an 802.21 event towards the MIHF, one for each network, containing the MANET relevant information.

This candidate discovery process has some disadvantages. The scan, and subsequent association to each network for performing its validation, will interfere with the ongoing communications of the node, since the WLAN card will be busy validating the network. One possible way to avoid this problem is by using two wireless interfaces, one for normal communications, and other for performing scans. If two wireless interfaces are not available, then some performance drawbacks have to be expected.

2.11.2.4. IEEE 802.21 and Local Mobility

The usage of the IEEE 802.21 protocol and its full support by the MANET will bring the necessary elements to support the local mobility protocol, namely the mobile node's presence detection. Albeit not discussed in this paper, the designed architecture has support for QoS: 802.21 is used to provide signaling needed

to maintain QoS information during handovers. These 802.21 messages can then be used by the ARs in order to detect new nodes in the network, and trigger the local mobility protocol.

This mobility process also supports make-before-break handover, where the handover destination AR is informed about a new node wishing to attach to this network, before its movement. This type of handover is supported in this local mobility architecture due to the usage of the IEEE 802.21 protocol.

2.11.2.5. Bootstrapping process

Bootstrapping is the process by which the MT gets the necessary information needed to have full access to the network. In a typical infrastructure network, the MT is always one link away from its PoA, and thus can communicate directly with it. This communication is easily done by using IPv6 link-layer addresses and L2 messages. Unlike in the infrastructure, direct communication between ad-hoc nodes and the gateway may not be possible; in this scenario, L3 communication needs to be in place between the node and the gateway. However, considering that the communication is performed to the outside, this requires that a globally scoped IPv6 address is configured on the network interface. Unfortunately, a globally scoped MT address is only available after the bootstrap phase, so, some other temporary address must be used instead. For this operation, we decided to use the Unique Local IPv6 Unicast Addresses (ULA) [6]. These addresses replace the link-layer addresses for operations inside the MANET.

During the bootstrap phase, the node should only have access to the PoA, and should not be part of the routing protocol operations, because it is not fully authorized to use the network. The gateways should also drop packets proceeding from ULA. With a unique local unicast address, the node is only allowed to have bi-directional connectivity to the gateway. The bootstrap operation consists of the MT sending its credentials, and then the gateway sending the prefix assigned to it.

The knowledge of the gateway and its address is given by the Jelger auto-configuration protocol [7], which spreads the information in the network, and builds a tree with all nodes in the network (any node can reach the gateway through simple forwarding). To enhance performance, limit the access to the network and minimize the awareness of the entrance of a new node, a simplification of a routing protocol such as AODV can be used. A node entering the network generates its address through auto-configuration and sends a Route Reply, addressed to the gateway, reachable using the path created by gateway discovery. This message creates a temporary bi-directional link between the node and the gateway. The gateway then communicates with the network and verifies if the node is allowed to use it. In the case where the node is authorized, the gateway sends the prefix assigned by the network to the node's ULA. The node generates a valid global address, based on the received prefix, and starts the fully functional ad-hoc routing protocol.

2.11.3. MOBILITY EXECUTION

To fully explore the MIH functionality in the MANET, as discussed in section 2.11.2.2, it is necessary for the ad-hoc network to be presented to the MIH Layer as a different technology, even if the real technology used is 802.11. The MIH-LINK-SAP (Service Access Point) abstract interface must be implemented by the ad-hoc modules, using not only information and operations provided by ad-hoc auto-configuration and routing protocols, but also from the 802.11 L2 events provided by the driver. Because the same card can be used for infrastructure and ad-hoc connectivity, our MANET module presented to MIHF must keep the 802.11 functionalities of the original 802.11 module (WLAN-Radio Access Layer - RAL), and extending it with the MANET information.

To transparently use the same module in ad-hoc and infrastructure mode, we introduce the MANET Wrapper between WLAN-RAL and the MIHF. The wrapper communicates with both 802.11 RAL and ad-hoc modules, and generates meaningful messages to the MIH. The events are processed by the wrapper in a way that they have relevance in the context of the MANET. Commands from the MIHF can trigger operations on the MANET modules and on the 802.11 RAL as well.

MIH manages a collection of information regarding available PoA for each technology. MANET wrapper introduces the ad-hoc PoAs to the framework. The metrics that characterize the quality of the PoA will relate to the virtual link. Information about the Virtual Links is provided by an ad-hoc auto-configuration protocol that informs the MT about the connectivity towards the gateway, and provides a metric that characterizes the path to it, that is updated hop-by-hop.

MANET is supported at a lower level inside the MIH architecture, and the MIH-Users (eg: handover controllers) will interact with the MANET using the abstract interface they use for the other technologies. They still have to be MANET aware, so that they can take decisions on what PoA to use and implement policies.

By introducing the wrapper, the ad-hoc handover operations are managed in a seamless way as in the infrastructure. If a new 802.11 PoA (adhoc or not) is selected, three different handover scenarios are possible. On the first one, the node is connected to infrastructure and requests a handover to an ad-hoc PoA. On the second one, the MT is part of a MANET and connects to infrastructure. The third scenario is the one where the node is requesting a handover from one ad-hoc PoA to another.

Figure 2.11.2: Handover from Ad-hoc to infrastructure

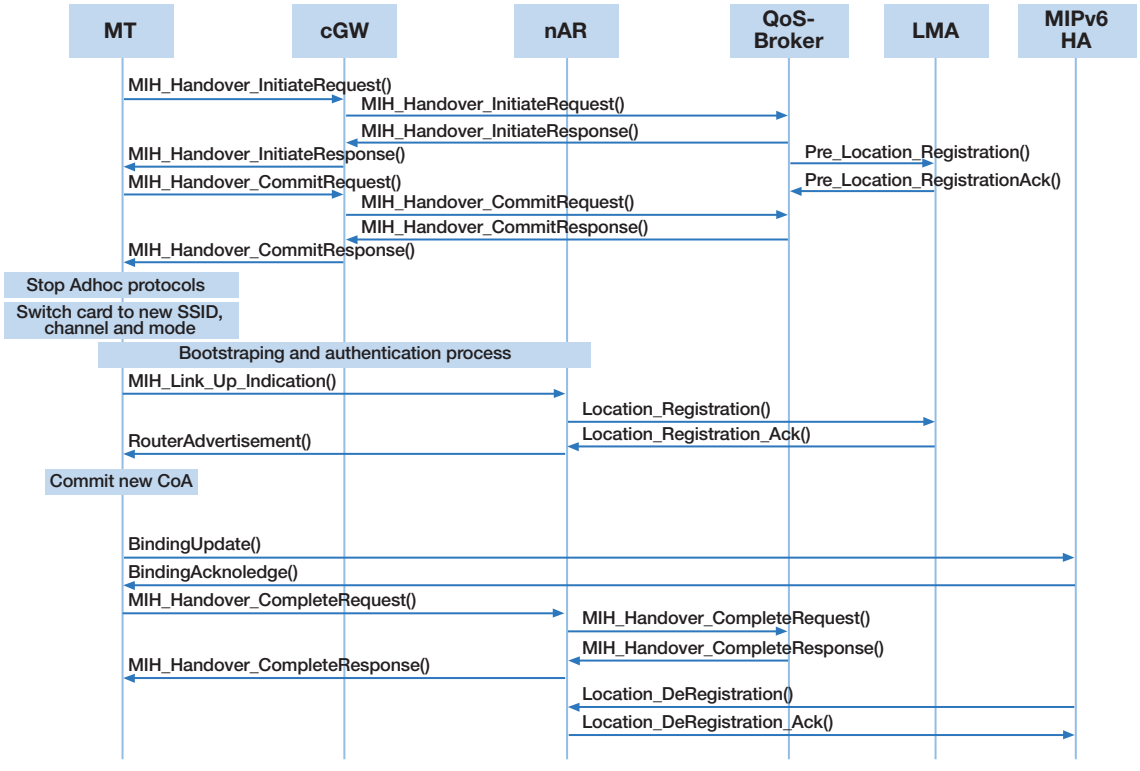
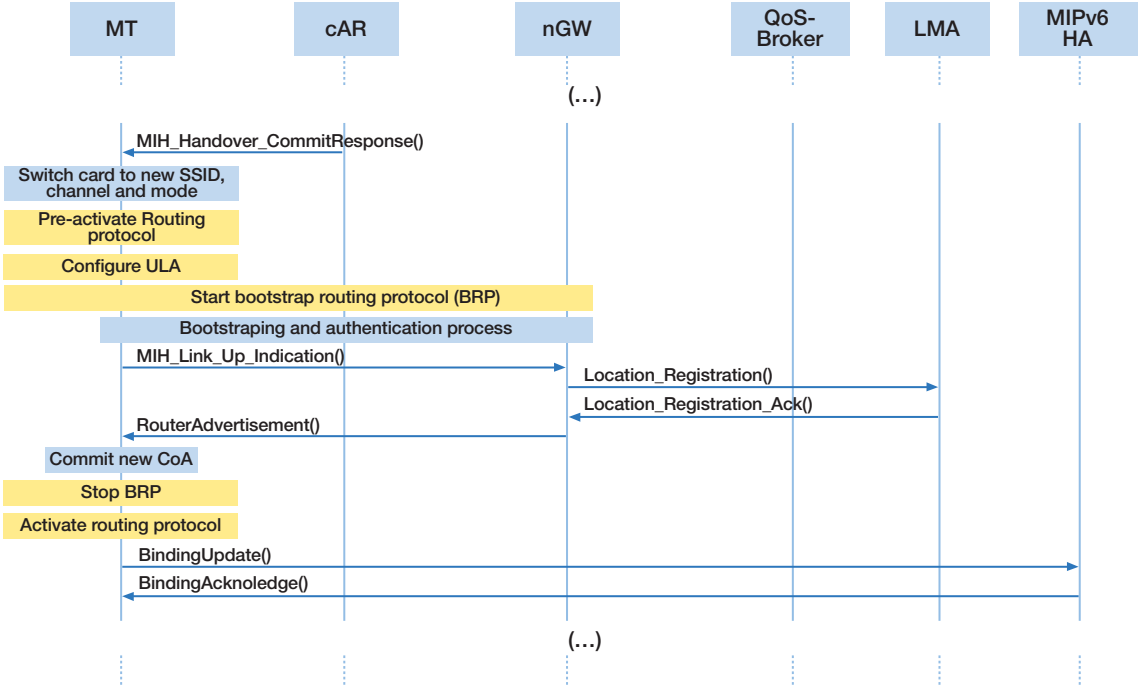


Fig. 2.11.2 shows the handover process for the first scenario. MT_MIHF forwards the *MIH_Handover_InitiateRequest* to the current gateway MIHF, which forwards it to a QoS-Broker to get permission to perform the switch. An answer is sent back to the MT using the same path as the request message. In parallel, QoS-Broker orders the reservation of resources in the new AR (these messages are not listed). The MT then issues a *MIH_Handover_CommitRequest* to the QoS-Broker signalling that the resources should be allocated, and instructs the nAR to activate the already allocated resources. MT then switches to the new SSID and channel, and sends a *MIH_Link_Up_Indication*() to the nAR. This event reaches the the LMP Engine in the nAR which uses the LocationRegistration message to register the new terminal's location with the LMA. The answer triggers a *RouterAdvertisment* (RA) from the LMP Engine towards the MT. The MT then triggers a MIPv6 *BindingUpdate* in order to register the new address with the *HomeAgent*. Then, a *MIH_Handover_CompleteRequest* is sent to free the resources in the ad-hoc network. The last step in the process is the deregistration of the old CoA issued by the LMA Engine to the ad-hoc gateway which confirms it.

The second and third scenarios use a similar MIH signalling between the MT and the network entities, but differs on the way the *MIH_Link_Switch* messages gets processed. Besides connecting to the L2 ad-hoc network, MANET Wrapper also signals the auto-configuration module to configure an ULA address and activate the bootstrap routing protocol, so that MT can reach the gateway to get authenticated, and to send the Link-Up message and receive the RA message. The RA message will be addressed to ULA, instead of the link-local address.

As MANET Wrapper acts as a radio access layer for both ad-hoc and 802.11 infrastructure PoAs, and fully implements MIH-LINK-SAP interface, it is also possible for a node to handover from ad-hoc to PoAs of all the supported technologies (UMTS, DVB, 802.11e) in a transparent way. In this case, there is a slight variation of the message sequences, because the old link while the new one is not fully setup (Figure 2.11.3).

Figure 2.11.3: Handover from infrastructure to Ad-hoc



The *MIH_CommitRequest/Response* phase precedes the *MIH_Link_Switch* to the new PoA, and after handover is complete, the old link is switched off. The MT is aware of the type of handover (inter or intra-technology), and generates the correct message sequence accordingly.

2.11.3.1. Multihoming

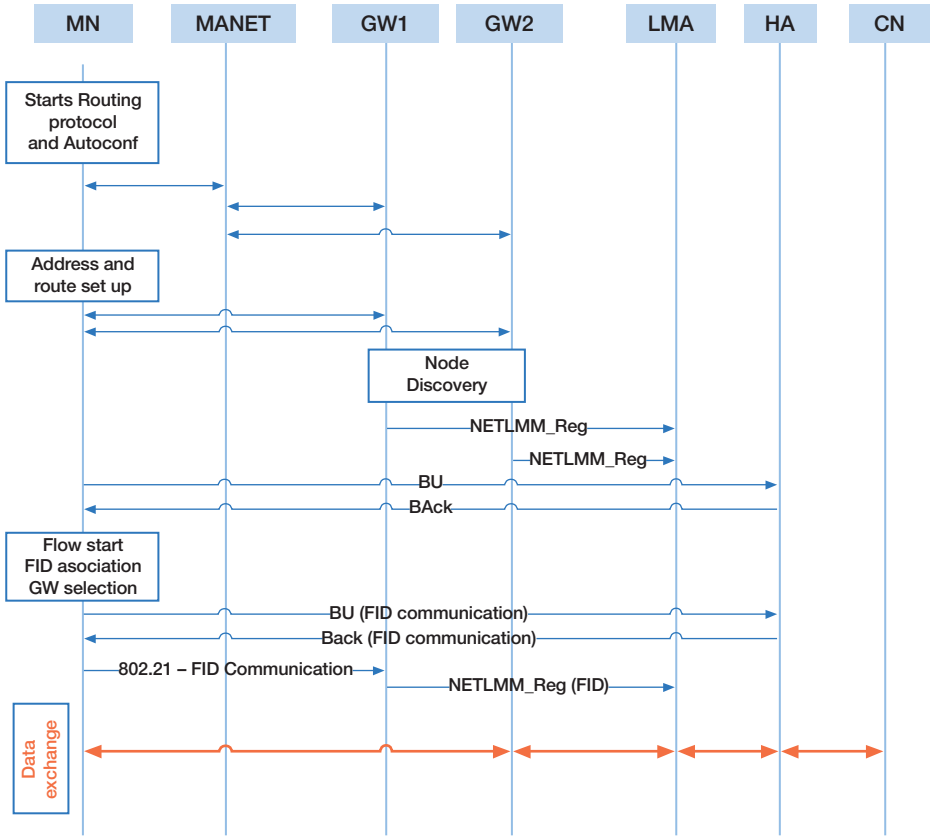
Ad-hoc networks are characterized by unpredictable topologies determined by degree of mobility of the nodes. Indeed it may happen that a MANET is connected to an external network by means of several gateways, i.e. a node can exploit several ingress/egress points to exchange traffic with hosts located outside the MANET it is connected to. The plurality of gateways can be exploited to achieve redundancy and load balancing. Redundancy is an inherent feature of multiple gateways MANET but attention must be paid to the operations executed to replace or change the gateway. The considered approach is the enhancement of routing protocols proactively announcing topology information: nodes periodically transmit OLSR MID messages containing all the usable global addresses; if AODV is used, a Gratuitous Route Reply is sent to each gateway with the global address associated to the gateway itself. When the node changes the gateway used to exchange packets, the MANET already knows the required routing information to deliver packets destined to the node. Since session maintenance is a fundamental requirement nowadays, multihoming in MANET is fitted within mobility infrastructure, both global and local. Global mobility copes with multihoming when different gateways announce different prefixes: this implies that a node can use several CoAs to communicate. All the set of available addresses have to be registered with the mobility anchor, e.g. Home Agent in case MIP is used. MIPv6 framework will be extended with multiple CoAs (bound with the same HoA) support and will be MANET unaware (i.e. Binding Updates messages are the same as those used for standard MIPv6 multiple registration). Policy management handling distribution of flows among available gateway is performed by using flow identifier extensions of MIPv6: each flow is identified by a 5-uple that is identified by a Flow ID (FID) which is communicated to home agent or correspondent node if route optimization is performed. FIDs are then bound with CoAs associated to the gateway through which that particular flow has to be exchanged: data packets of a specific flow will be transmitted to the CoA bound to that flow and therefore will be routed to the gateway announcing the prefix of that CoA. OLSR MID messages and AODV Gratuitous Replies cope with the set-up of routing information to deliver packets destined to the CoAs of the node. Uplink traffic distribution is achieved by means of IPv6 routing header, including the address of chosen gateway as the first destination.

If multihoming is performed at LMD level, some additional extensions have to be provided. Indeed, a node connected to multiple gateways belonging to the same LMD will receive only one prefix which will be handled by all the gateways. This implies that an additional data is required to handle downlink packets distribution. The proposed solution exploits FID used by MIPv6 to identify flows for routing purposes. If it has been established that a certain flow has to be exchanged to a gateway A, then the node communicates the FID of the flow to gateway A by using 802.21 messages. Gateway A, in turn, registers the triple made by such FID, node CoA and gateway identifier with LMA through NETLMM extended messages. Our solution requires the insertion of FIDs into the IPv6 Flow label field of outer IPv6 header of packets transmitted to the node: such operation is executed by home agent or correspondent node (when route optimization is run).

It may happen that a MANET is endowed with multiple gateways (GMD) which can be split into multiple subsets of gateways belonging to the same LMD. This scenario implies a hierarchical approach: multihoming at GMD level handles distribution of flows among the subsets of gateway belonging to the same LMD, and multihoming at LMD level controls the delivery of the traffic to the chosen gateway. No changes to the previously described approaches have to be performed.

Figure 2.11.4 describes the sequence of operations performed by a MANET node connected to an ad-hoc network endowed with multiple gateways. After entering the cloud, the node starts running routing protocol and auto-configuration in order to discover routes and available prefixes. After routes and prefix discovery, the node has set up its global address and routes to the gateways: some specific signaling (depending on the used routing protocol) is now required to inform gateways about the global addresses. The reception of such information triggers gateways to register the node with the LMA, in order to set up IP data plane in the LMD (NETLMM Reg message). Concurrently, the node will register with the Home Agent the CoA (BU-BA message exchange) to be globally reachable.

Figure 2.11.4: Support of Multihoming



So far, the IP plane has been set-up but the exploitation of both gateways can not be performed as there are no routing policies installed. Such operation is performed on demand when applications are started, through the assignment of an FID the decision about the gateway to use to exchange that flow. The next step is the communication of the routing decision: this must be performed in two steps, one for the LMD and the other for the GMD. The first one requires the node to send a 802.21 message to inform the chosen gateway about the taken decision (802.21 FID communication): the gateway will then send a NetLMM message to the LMA containing the FID of the flow (NETLMM_Reg (FID)). This message enables the LMA to route all the packets labeled with that FID to the proper gateway. The routing decision communication step for the GMD requires the exchange of BU-BA messages containing the FID and the 5-tuple.

Only after this message exchanges have been performed the flow can be route to the node through the proper gateway. Indeed, the HA will tunnel packet towards the MANET node labeling outer IP header with the corresponding FID, and LMA will route packets to the chosen gateway by examining the FID, which finally will deliver packets to the node.

2.11.4. CONCLUSION

This paper described the Ad-hoc network integration architecture being developed inside the IST project Daidalos II, mainly in terms of its functionalities and interactions to efficiently support the mobility between ad-hoc networks and infrastructure. The proposed architecture is able to efficiently integrate ad-hoc and infrastructure networks, enabling a node to be using one of the networks or both (through multihoming), and to seamless move between ad-hoc and infrastructure networks. The ad-hoc architecture is designed in such a way that the mobility process is independent of the type of network in place.

2.11.5. REFERENCES

[1] IST FP6 Integrated Project Daidalos II: http://www.ist-daidalos.org

[2] J. Kempf, et al, "Goals for Network-based Localized Mobility Management (NETLMM)", draft-ietf-netlmm-nohosts-req-03, 2006.

[3] D. Johnson, C. Perkins, J. Arkko. Mobility Support in IPv6, IEFT RFC 2775, June 2004.

[4] R. Moskowitz, et al, "Host Identity Protocol", draft-ietf-hip-base-06, June 2006.

[5] Draft Standard for Local and Metropolitan Area Networks: Media Independent Handovers Services (Draft .01). IEEE, March 2006.

[6] R. Hinden, B. Haberman., "Unique Local IPv6 Unicast Address", IETF RFC 4193, October 2005.

[7] C. Jelger, T. Noel, "Gateway and address autoconfiguration for IPv6 adhoc networks", IETF Internet Draft, draft-jelger-manet-gateway-autoconf-v6-02.txt, April 2004.

2.12

MoAR: Mobile Access Router. Providing Security and Localised Mobility support for Mobile Networks

Carlos J. Bernardos, Ignacio Soto, **Universidad Carlos III de Madrid**
Santiago Zapata, Francisco J. Galera, **Universidad de Murcia**

ABSTRACT

Nowadays, users do not only expect to have Internet access from fixed locations (e.g., at home, work, or through hotspots deployed in airports, hotels or cafes), but also from mobile platforms, such as trains or buses. Host mobility support in IP networks was a first step towards achieving such a ubiquitous Internet environment. Nevertheless, supporting the movement of a complete network that changes its point of attachment to the fixed infrastructure, without requiring the intervention of the nodes attached to the network, also presents some advantages. Additionally, access to this kind of public Internet access networks must be secured and authenticated, in order to avoid unauthorised users to gain connectivity. A third issue that needs to be tackled is the performance of the mobility management solutions deployed in these scenarios, since handover latencies should be small enough to enable the deployment of real-time applications (e.g., VoIP). The use of Localised Mobility Management mechanisms aims at improving this performance, while reducing the overall system signalling overhead.

This paper proposes an architecture that integrates Network Mobility, Security and Localised Mobility management mechanisms, minimising the changes required on the network infrastructure and analysing relevant scenarios where this integration is required.

Index Terms

Network Mobility, Authentication, Security,
Localised Mobility Management, Mobile Router, Mobile IPv6, PANA.

2.12.1. INTRODUCTION

Users demand Internet access not only from fixed locations (e.g., at home, at work, in hotels, cafeterias, universities, etc.) but also in public transportation systems (e.g., planes, trains and buses). In order to satisfy such demands, the technical community worked on the design of the required protocols to provide Network Mobility support. The Internet Engineering Task Force[1] (IETF) has standardised the Network Mobility (NEMO) Basic Support protocol [1], which enables mobile networks to change their point of attachment while maintaining the sessions that the nodes of these networks may have established.

The NEMO Basic Support protocol solves the very basic problem of network mobility support, but current use case scenarios pose additional challenges, mainly triggered by users' requirements and deployment issues. As an example, users demand seamless connectivity, no matter how they attach to the network or where they are located. This imposes additional challenges, such as the need of optimising the path followed by data packets (the so-called Route Optimisation problem [4]) or the minimisation of the delays/service disruptions due to handovers. Additionally, today's networks must be secure and access from unauthorised users must not be permitted, hence security and authentication should also be taken into account.

This paper presents an architecture that combines enhanced Network Mobility mechanisms - to provide transparent and route optimised mobility support for roaming networks - with localised mobility management solutions - to improve the handover performance and reduce signalling overhead -, and with a security framework, based on Protocol for Carrying Authentication for Network Access (PANA), to provide the designed architecture with security and authentication mechanisms.

The paper is structured as follows. Section 2.12.2 introduces some of the basic technologies and protocols that are integrated into the proposed architecture. Some relevant use case scenarios and the motivation to this work are described in Section 2.12.3, while the proposed solution is detailed in Section 2.12.4. Finally, Section 2.12.5 concludes the paper.

2.12.2. BACKGROUND

2.12.2.1. Network Mobility

To address the requirement of transparent Internet access from mobile platforms, the IETF standardised the NEMO Basic Support protocol [1], which defines a Mobile Network (or Network that Moves, NEMO) as a network whose attachment point to the Internet varies with time. The router within the NEMO that connects to the Internet is called the Mobile Router (MR). It is assumed that the NEMO has a Home Network where it resides when it is not moving. Since the NEMO is part of the Home Network, the Mobile Network has configured addresses belonging to one or more address blocks assigned to the Home Network: the Mobile Network Prefixes (MNPs). These addresses remain assigned to the NEMO when it is away from home. Of course, these addresses only have topological meaning when the NEMO is at home. When the NEMO is away from home, packets addressed to the Mobile Network Nodes (MNNs) will still be routed to the Home Network. Additionally, when the NEMO is away from home, i.e. it is in a visited network, the MR acquires

(1) http://www.ietf.org/

an address from the visited network, called the Care-of Address (CoA), where the routing infrastructure can deliver packets without additional mechanisms.

The basic solution for network mobility support is quite similar to the solution proposed for host mobility (Mobile IPv6 [3]) and essentially creates a bi-directional tunnel between a special node located in the Home Network of the NEMO (the Home Agent, HA), and the CoA of the MR.

The NEMO Basic Support protocol has several performance limitations, namely: it forces suboptimal routing (i.e. packets are always forwarded through the HA). It introduces non-negligible packet overhead and the HA becomes a bottleneck for the communication as well as a potential single point of failure. Because of these limitations, it is highly desirable to provide what has been called Route Optimisation (RO) support for NEMO [9], to enable direct packet exchange between a Correspondent Node (CN) and a MNN, avoiding traversing the Home Network. MIRON [2] is a proposal of a solution for Route Optimisation that does not require upgrades in CNs, MNNs, or HAs.

2.12.2.2. Localised Mobility management

The idea of Localised Mobility Management (LMM) is not new. Early in the development of mobility solutions in IP networks, it was recognised that Mobile IP alone was not sufficient and improvements were needed to provide adequate performance when a Mobile Node (MN) roamed across access networks far from its home network. Some of the proposals to deal with this issue were based on the idea of managing the local mobility differently from the global mobility.

Initial proposals had as main objectives to reduce signalling outside the local domain, and improve efficiency by managing the local mobility closer to the MN (reducing the time needed for the mobility signalling and improving handover latency). These early proposals (such as Hierarchical Mobile IPv6 - HMIPv6 [4]) were host based, i.e. hosts were active elements in the mobility process, taking care of the signalling needed to manage the local mobility, and being aware of the local and global solutions, thus acting accordingly.

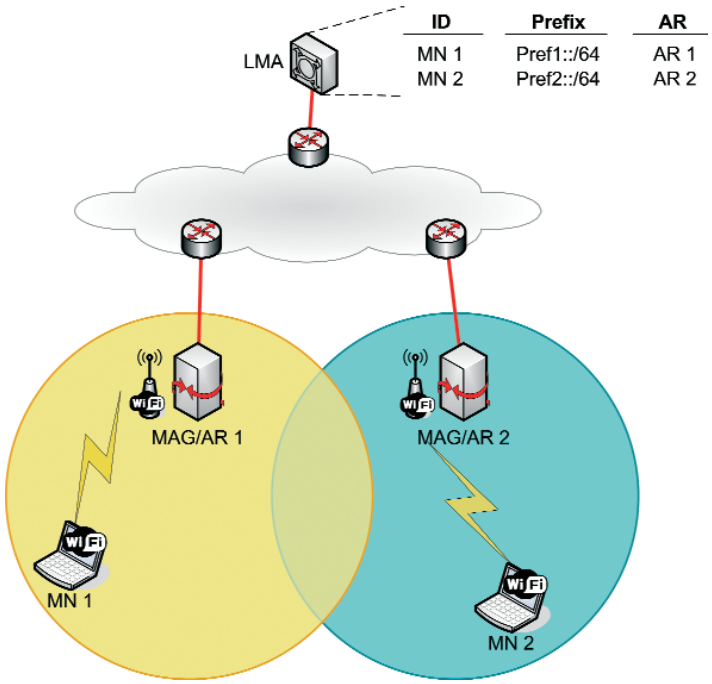
Unlike host-based mobility, such as Mobile IPv6, where mobile terminals signal a location change to the network to maintain routing states and to achieve reach ability, Network LMM (NetLMM) [5][8] approaches relocate relevant functionality for mobility management from the mobile terminal to the network. In the localised mobility domain, the network learns through standard terminal operation, such as router and neighbour discovery or by means of link-layer support, about a terminal's movement and coordinates routing state update without any mobility specific support from the terminal. While moving inside the Localised Mobility Domain (LMD), the MN keeps its IP address, and the network is in charge of updating its location in an efficient manner. Such an approach allows hierarchical mobility management on one hand, where mobile terminals signal location update to a global mobility anchor only when they change the localised mobility domain, and mobility within a localised domain for terminals without any support for mobility management at all on the other hand. NetLMM complements host-based global mobility management by means of introducing local edge domains.

The LMM solution defined in the EU DAIDALOS II project is based on [5]. It basically defines a Localised Mobility Domain as a network domain where Localised Mobility Management support is provided. To do so, two new network entities are defined (see Figure 2.12.1):

- Mobile Access Gateway (MAG). This entity is also referred to as Access Router, so we will use both terms along the paper. It is a router that a mobile node is attached to as the first hop router in the LMM infrastructure. There are multiple MAGs/ARs in an LMD.

- Local Mobility Anchor (LMA). It is a router that maintains reachability to a Mobile Node's address while the Mobile Node moves around within the same LMD. It is responsible for assigning IPv6 addresses/prefixes to Mobile Nodes within the LMD, and maintaining forwarding information for the Mobile Nodes which includes a set of mappings to associate Mobile Nodes by their identifiers with their address information, associating the mobile nodes with their serving MAGs/ARs and the relationship between the LMA and the MAGs/ARs. There may be one or more LMAs in a same LMD.

Figure 2.12.1: Daidalos II LMM solution



2.12.2.3. Security and authentication in access networks

Access Networks require the provision of access to them in a secure way, but only for authorised users. This requirement implies the existence of a suitable authentication process which is able to supply other mechanisms with cryptographic material for providing the security into this network. This is especially important in mobile scenarios in which the user is visiting a foreign network, and there is not a direct way to provide access to the network without a previous authentication process.

A solution based on Protocol for Carrying Authentication for Network Access (PANA) [6] and IPsec has been designed within the framework of the EU DAIDALOS II project. In this case, PANA is in charge of the authentication process by carrying the Extensible Authentication Protocol (EAP) [7] packets from PANA Client (PaC, in the MN) to PANA Agent (PAA, in the Access Router - AR) which is acting as an EAP Authenticator. On the other hand, the transport of authentication packets into the core network requires the deployment of an Authentication, Authorisation and Accounting (AAA) infrastructure. Once the MN is authenticated, the PAA transfers keying material derived by the EAP method to the Access Point (AP) to which the MN is attached. In that way, the AP is sharing a Security Association (SA) with the MN.

This solution can be adapted to NEMO scenarios in the most possible transparent way, by splitting the global procedure in three phases:

- Authentication of MR. At this point, the MR authenticates itself in the network like a normal MN does, so it requires to deploy into the MR the modules in charge of authentication (mainly PANA Client).
- Establishment of Security Associations between the MR and the network. This is done to allow MNN's authentication and mobility management. For example, a PANA Agent should be located in the MR and should re-establish its SA with the corresponding AAA Server.
- MNN's authentication. The MNNs start authentication process with the PAA located in the MR like they did in authentication This is why it is required to deploy a PAA also in the MR.

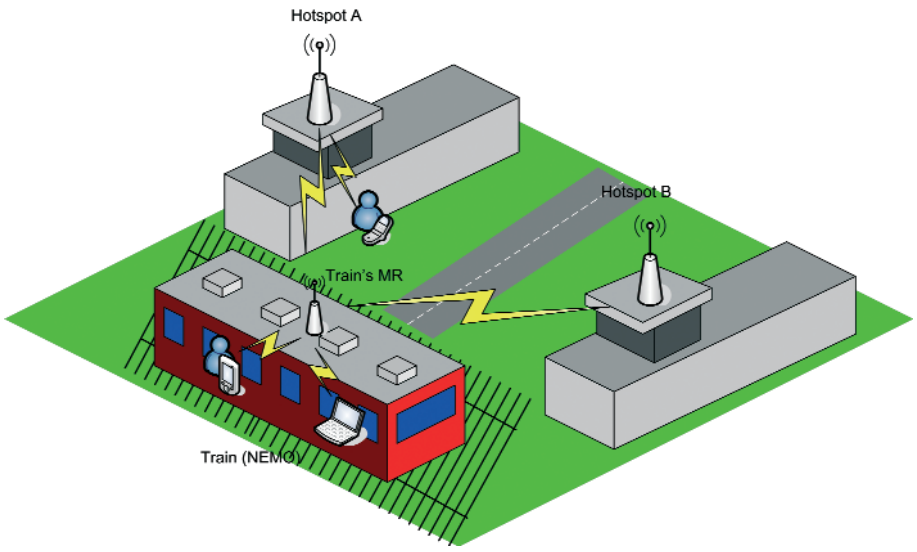
2.12.3. USE CASES SCENARIOS AND MOTIVATION

There are several potential scenarios where a secure combination of Host and Network mobility with Localised Mobility management solutions is required. Next, some of these scenarios are introduced.

2.12.3.1. Airport scenario

A possible scenario could be found when a user is connected via WLAN to a hotspot located in an airport's terminal, where it is already authenticated. At some moment, the user takes a train to commute to another terminal. A Mobile Network is deployed within the train, and therefore the user keeps its Internet connectivity, by performing a handover to the train's NEMO.

Figure 2.12.2: Airport scenario



While connected to the train, the MN does not deal with any mobility issue, since it is the MR deployed on the train the one managing the mobility of the whole train. As soon as the train arrives to the new terminal, the MN should perform another handover to the fixed infrastructure, in order to maintain its connectivity.

This scenario implies that the train's MR hand offs from hotspot in terminal A to hotspot in terminal B, and users using the train's NEMO hand off from the hotspot in terminal A to train's NEMO, and from train's NEMO to the hotspot in terminal B. Nevertheless, all the handovers are performed within the same administrative domain (airport), so Localised Mobility Management could enable the MN to keep its address, which can be exploited in order to provide seamless handovers.

New mechanisms need to be designed and integrated to enable Moving Networks belong to the same Localised Mobility domain that the fixed infrastructure.

2.12.3.2. Bus scenario

Another interesting scenario is the one in which a user is connected via WLAN to a hotspot in a bus station, while waiting a bus.

The bus provides connectivity - by having a NEMO deployed inside - while it is moving, and users keep their connectivity when they hand off from the bus to the fixed hotspots available at the stations. This connectivity is maintained while the bus is travelling and moving (potentially moving from an administrative domain to another), in a transparent way to the users.

In this case, a Localised Mobility Management solution can not be exploited when the bus moves from an administrative domain to another, but it can while the bus is connected into the same administrative domain.

2.12.3.3. Motivation

As pointed out in previous sections, the integration of Network Mobility and Localised Mobility solutions brings several interesting advantages, mainly the reduction in the required signalling (which in NEMO can be significant when a Route Optimisation solution is used) and the gain in the performance. However, this integration presents several challenges, depending on the type of nodes that are connected to the NEMO:

- Local Fixed Nodes (LFNs). Since mobility is hidden from the LFNs, a localised mobility management solution is transparent to them. An MR will configure an address belonging to the LMM domain (exactly as an MN would do) - this is the CoA for the MR - that can be registered in the HA by using the NEMO Basic Support protocol. The MR-HA tunnelled traffic will transparently traverse the LMA-AR tunnel in the LMM domain. The advantage of using an LMM solution is that when the MR moves from one AR to another inside the LMD, this does not require to send signalling to the HA. The infrastructure will use the same method to detect the movement of the MR as it uses for any MN, in fact it will not be able to notice the difference.
  The situation when the MR is using an RO solution as **MIRON** is the same. In MIRON, the CoA of the MR is not only registered in the HA of the MR, but also in the CNs that are communicating to LFNs of the NEMO. In this case the LMM provides an additional advantage in the intra-LMM handover, all the signalling to the HA and the CNs after a handover is avoided.
- **VMN** and nested NEMOs support with Route Optimisation: Supporting VMNs and nested NEMOs is somehow more difficult. VMNs require addresses topologically correct in the infrastructure that the NEMO is visiting to be able to perform Route Optimisation in an efficient way. The more challenging issue is how to manage an MN's handover between the fixed infrastructure and a NEMO (attached to the same LMD), in such a way that the MN does not require to change its IP address. This paper proposes a mechanism that solves this issue.

2.12.4. SOLUTION ARCHITECTURE

2.12.4.1. Overview

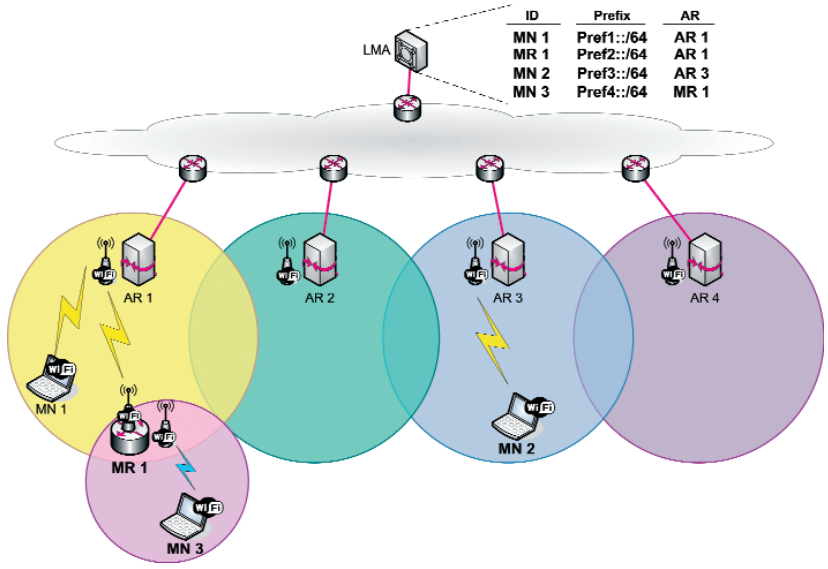
In order to extend an LMD with attached Mobile Networks, we propose an architecture in which the role of a Mobile Router is two-folded:

1. On one hand, the Mobile Router behaves as a Mobile Node (normal Mobile Router operation over its egress interface), so it obtains an IPv6 address/prefix from the LMA when it first enters the LMD and then keeps that address while roaming within the same LMD.
2. On the other hand, the Mobile Router behaves as a MAG/AR - that is why we call it Mobile Access Router (MoAR). It extends the LMD by providing IP addresses/prefixes to attached VMNs and forwarding/receiving packets to/from the LMA.

The basic operation of a MoAR is as follows. When an MR attaches to an Access Router belonging to an LMD, this Access Router informs its LMA about this event, providing it with the MR's identity. The LMA delegates an IP address/prefix to the MR and creates a binding, associating the MR's identity, the delegated address/prefix and the AR to which the MR is attached. This is the standard behaviour when a normal MN connects to an AR of an LMD. If the MR moves to another AR within the same LMD, the LMA updates the binding with the new AR's information.

If the MR is authorised (i.e. it has the required security relationship/trust with the LMA) to behave as a MoAR within the LMD, the MR also plays the role of a normal Access Router for VMNs that get attached to it. When a VMN attaches to an MR, the MR informs the LMA and gets an IPv6 address/prefix for the VMN. The LMA adds a new binding entry, associating the VMN's ID with the delegated address/prefix and the Access Router to which it is attached (i.e. the MR).

Figure 2.12.3: Solution overview

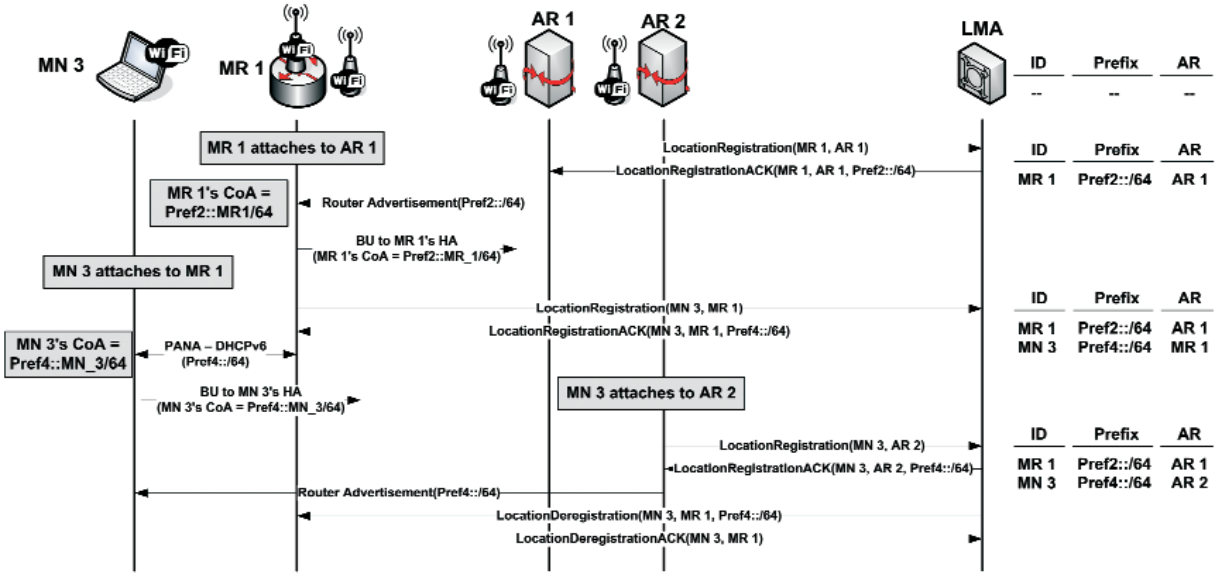


A change in the normal operation of the LMA is introduced to support MoARs. Basically, the LMA will need to recursively look into is binding table to find out how to deliver packets addressed to a VMN attached to connected MoARs. In a first look-up, the LMA obtains the MR to which the VMN is attached. After that, the LMA looks for the MR in its table and finds the associated Access Router. With this information, the LMA is able to encapsulate the received packet towards the Mobile Router, through the appropriate Access Router. The MR is then able to forward data packers from/to the VMN.

The MR also plays a double role in the security framework proposed:

1. Mobile Router must authenticate itself when it arrives to a visited network such a Mobile Node does. This authentication is required because the Mobile Router is an unknown entity in the visited network, and Access Routers need to trust the Mobile Router.
2. On the other hand, the Mobile Router plays the authentication agent role for attached Mobile Network Nodes.

Figure 2.12.4: Detailed operation signalling



Both MRs and MNNs authentication processes use PANA as the protocol in charge of carrying the EAP packets from PANA Client to PANA Agent. Then, the PANA Agent is forwarding the EAP packets for authentication purposes to AAA Server. The protocol used for exchanging these packets between PANA Agent and AAA server is the AAA protocol named DIAMETER [10]. For this interface, the PAA should act like a Diameter Client node asking for authentication/authorization to Diameter Server node.

It is important to notice that in order to allow MRs to behave as MoARs within the LMD, an association procedure between the MoAR and the LMA is required. Thus, MRs send a Association Request to the LMA for setting up the control and data plane between them, similarly as done between MAGs and LMA. The mechanism used by LMA to check if MAGs and MoARs are authorized to act as access routers is out of the scope of this paper.

2.12.4.2. Detailed Operation

This section describes in more detail the operation of our proposed architecture, using the network scenario that appears in Figure 2.12.3 and the Message Sequence Chart (MSC) depicted in Figure 2.12.4.

Let's assume that the network is bootstrapped, so there is no state in any network entity (that is, LMAs and Access Routers of the LMD). When a Mobile Router - MR 1 - attaches to AR 1, this event is detected by AR 1 and reported to its serving LMA, by means of a *LocationRegistration* message. Because there is no existing entry for MR 1 in the binding table of the LMA, a new entry is created, including the information of the IPv6 assigned prefix (Pref2::/64) and the AR to which the new arrived node (MR 1) is attached to (AR 1). The LMA then replies with a *LocationRegistrationACK* message, that includes the IPv6 prefix assigned to MR 1. With this information, AR 1 unicasts a Router Advertisement message to MR 1, so it can form a Care-of Address from the assigned prefix. At this stage, the MR is able to register/update its location with its Home Agent and start sending/receiving traffic. While the MR moves within the same domain, its CoA does not change.

When an MN - MN 3 - attaches to MR 1 (that is, MN 3 is a VMN), MR 1 sends a *LocationRegistration* message towards the LMA, which creates a new entry for MN 3 and informs MR 1 about the assigned prefix (Pref4::/64). MR 1 can then inform MN 3 about the IPv6 address it has to use (if we assume that MR 1 is using MIRON as Route Optimisation solution, it will use PANA-DHCPv6 signalling to make MN 3 obtain this address, as specified in [2]).

Figure 2.12.5: Packet encapsulation

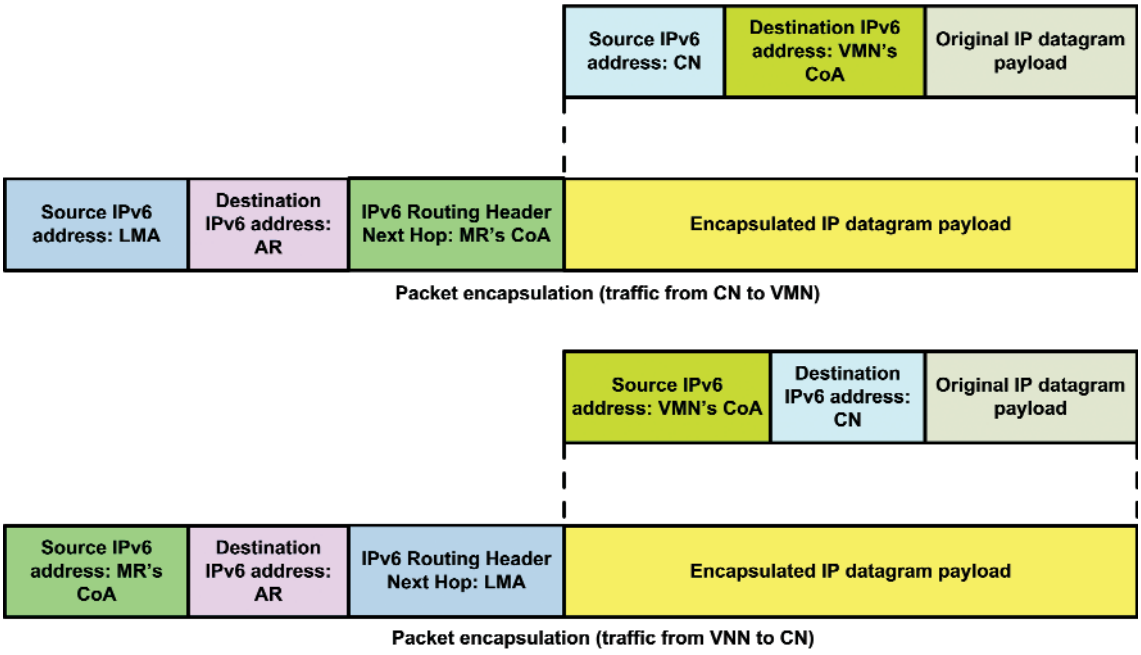


Figure 2.12.5 details the packet encapsulation performed by the LMA and MoAR while forwarding data traffic. Data packets from a CN are received by the LMA, which will look-up at its binding table which is the Access Router to which it has to forward packets received. This look-up is performed recursively until an infrastructure-Access Router (i.e. a non-MoAR) is found. Following our example, if the LMA receives a packet

from a CN addressed to MN 3, it will find that MN 3 is attached to MR 1. Since MR 1 is a MoAR, it will perform a second look-up at its table, searching for the Access Router to which MR 1 is attached to. Once that the LMA has found out that MN 3 is attached to MR 1, which is attached to AR 1, the LMA is able to forward data packets towards MR 1. To do that, LMA encapsulates each data packet in a new IPv6 packet towards MR 1, but using an IPv6 routing header[2], that ensures that the packet traverses AR 1 in the path towards MR 1 (the packet sent by the LMA has AR 1 as its destination address, and the Routing Header has only one hop, set to the MR 1's CoA). MR 1 decapsulates the packet, by removing the extra IPv6 header and delivers the packet to MN 3. In the reverse direction, MR 3 operates analogously, encapsulating data traffic sent by MN 3 towards the LMA.

If MN 3 performs an intra-LMD handover from MR 1 to AR 2, AR 2 informs the LMA, so it can update its binding table accordingly (now MN 3 is attached to AR 2, instead of to MR 1), which also informs MR 1 about the handover of MN 3.

The proposed architecture enables intra-LMD NEMO-to-infrastructure handovers. Roaming MNs keep their IPv6 addresses while moving within the same LMD, therefore reducing the mobility signalling outside the LMD, and improving the overall handover performance.

2.12.4.3. Security considerations

The whole authentication process is based on the introduction of PANA/AAA architecture into NEMO scenarios, which imply to satisfy several requirements:

- All MNNs should be provided with PANA Client (PaC) support (also LFNs).
- PANA Client (PaC) for authenticating the MR and PANA Agent (PAA) for authenticating MNNs must be located in the MR.
- Internal NEMO AAA architecture will consider the moving network as if the MR was physically located at MR's home domain, so NEMO management should be in charge of sending the AAA messages to the corresponding home domain.
- The PANA Agent located in MR should maintain a Security Association (SA) with AAA server in MR's home domain. This is required to enable the Diameter peers (PAA in MR, and AAA server in home domain) be connected in a secure way. However, this is not an extra requirement, because the MR will be a PAA when the MR is attached at home, and so, it should maintain this SA.

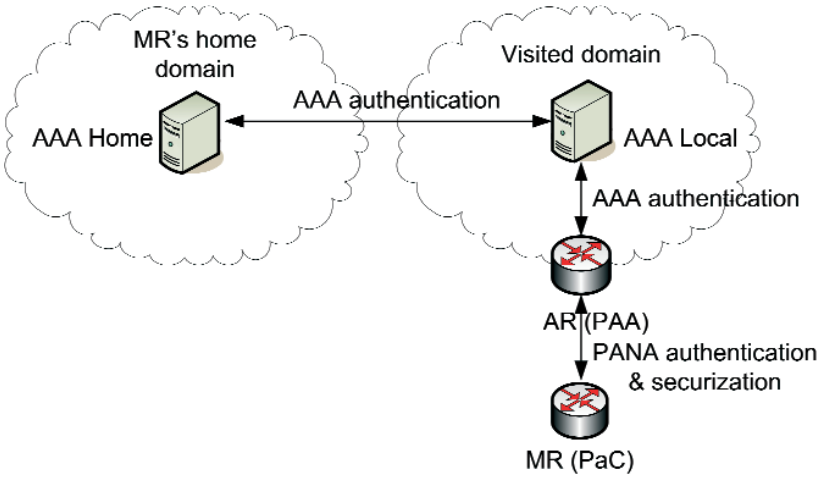
As already explained in the previous sections, the authentication process of a Mobile Network can be split in three phases:

1. Authentication of MR into the visited network

An MR arriving to a visited domain must authenticate itself within this domain before having access to the network, just like another MN arriving to this network. For this purpose, it uses PANA protocol to interact with the AR in the visited domain. Once the new AR is detected, the PaC in the MR starts the PANA/AAA authentication process. The PaC will interact with the PAA in the AR of visited domain. This interaction will be the normal authentication for a node arriving to the visited domain. AAA messages will be forwarded from AAA local server to AAA home server in MR's home domain (because this is the one having the authentication/authorization information for this MR). Figure 2.12.6 shows this process.

(2) A new type of Routing Header should be defined, with a new semantic that improves the security of the solution, by restricting in which situations it can be used.

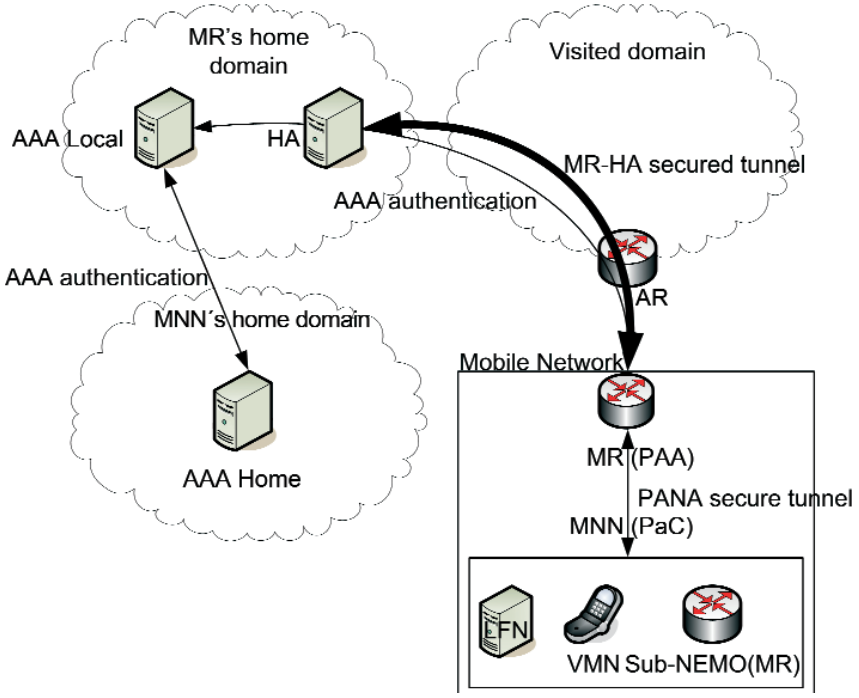
Figure 2.12.6: MR's authentication in the visited domain



2. Establishment of Security Associations

After receiving a successful notification of the MR authentication process, the AR and MR establish a secure tunnel for future communications. At this moment, the MR is able to get an IPv6 address and to establish the secured tunnel to its HA. Once the MR is authenticated and the Security Associations between MR and the network have been established, the bootstrapping process detailed in the previous section can be initiated.

Figure 2.12.7: MNN authentication into the NEMO



3. Authentication of the MNNs into the NEMO

Arriving MNNs must be authenticated into the NEMO. For this purpose, the PAA module is deployed into MR. This module is maintaining a secure connection with AAA server in MR's home network, so all the AAA messages will be forwarded through this server (this is the way also in which the AAA server can control the authorization information deployed into its MR by AAA servers of MNNs). This phase is depicted in Figure 2.12.7.

2.12.5. CONCLUSIONS

In this paper, we have proposed an architecture that provides localised mobility support for mobile networks in a secure way. We have identified and described several interesting real-life scenarios where this integration is needed and would improve users' connectivity.

The proposed architecture is based on a new network entity: the Mobile Access Router (MoAR), which is a NEMO (RFC 3963) Mobile Router extended to behave also as an LMM Access Router. Besides this, only the LMA is required to be extended to fully support our solution. Access Routers in the infrastructure of a Local Mobility Domain are not modified, therefore making easier the deployment of the solution.

The solution described in this paper integrates NEMO with one of the solutions for Localised Mobility Management that have been proposed at the IETF NetLMM WG. We are currently working on a solution that integrates NEMO and Proxy Mobile IPv6 (PMIPv6) [8], since this is the solution currently being adopted by the IETF. Another issue, not addressed in this work, in which we are currently working on, is the simulation of the proposed architecture and the evaluation of its performance under different network loads and scenarios.

2.12.6. ACKNOWLEDGMENTS

The work described in this paper is based on results of the IST FP6 Integrated Project DAIDALOS II. DAIDALOS II receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Carlos J. Bernardos and Ignacio Soto are also partially sponsored by the Spanish Government under the POSEIDON Project (TSI2006-12507-C03-01).

2.12.7. REFERENCES

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," IETF, RFC 3963, January 2005.

[2] María Calderón, Carlos J. Bernardos, Marcelo Bagnulo, Ignacio Soto, and Antonio de la Oliva, "Design and Experimental Evaluation of a Route Optimization Solution for NEMO", IEEE Journal on Selected Areas in Communications (J-SAC), issue on Mobile Routers and Network Mobility, Volume 24, Number 9, September 2006, pp. 1702-1716.

[3] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF, RFC 3775, June 2004.

[4] H. Soliman, C. Catelluccia, K. E. Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," IETF, RFC 4140, August 2005.

[5] H. Levkowetz, Ed., "The NetLMM Protocol", draft-giaretta-netlmm-dt-protocol-02.txt, IETF Internet-Draft (work-in-progress), October 2006.

[6] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-13.txt, IETF Internet-Draft (work-in-progress), December 2006.

[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[8] S. Gundavelli et al., "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-01.txt, IETF Internet-Draft (work-in-progress), June 2007.

[9] C.-W. Ng, P. Thubert, M. Watari, F. Zhao, "Network Mobility Route Optimization Problem Statement", draft-ietf-nemo-ro-problem-statement-03.txt, IETF Internet-Draft (work-in-progress) (September 2006).

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

2.13 Optimized FMIPv6 using IEEE802.21 MIH Services in Vehicular Networks

Qazi Bouland Mussabbir, Wenbing Yao, Zeyun Niu
Brunel University

Xiaoming Fu, **University of Göttingen**

ABSTRACT

In this paper, we optimize the handover procedure in Fast Handover for Mobile IPv6 (FMIPv6) protocol by using IEEE 802.21 Media Independent Handover (MIH) services. FMIPv6 is used to enhance the performance of handovers in Mobile IPv6 (MIPv6) and its basic extension for Network Mobility (NEMO), the fundamental mobility management protocols used in vehicular networks. With the aid of the lower three layers' information of the mobile node/router (MN/MR) and the neighboring access networks, we tackle the radio access discovery and candidate Access Router (AR) discovery issues of FMIPv6. We introduce an 'Information Element Container' to store static and dynamic Layer 2 (L2) and Layer 3 (L3) information of neighboring access networks, and propose to use a special cache maintained by the MN/MR to reduce the anticipation time in FMIPv6, thus increasing the probability of the predictive mode of FMIPv6 operation. Furthermore, we propose a cross-layer mechanism for making intelligent handover decisions in FMIPv6. Lower layer information of the available links obtained by MIH services as well as the higher layer information such as quality of service parameter requirements of the applications are used by a Policy Engine (PE) to make intelligent handover decision. We will show through analysis and simulations of the signaling procedure that the overall expected handover (both L2 and L3) latency in FMIPv6 can be significantly reduced in the proposed mechanism.

Index Terms

Cross-layer Design, FMIPv6, IEEE802.21, Mobility Management, NEMO

2.13.1. INTRODUCTION

The provisioning of seamless mobility to vehicles across heterogeneous access networks is essential for the next generation's vehicular communication networks. A variety of access network technologies (e.g. 802.11a/b/g WiFi, 802.11p WAVE, 802.16 WiMAX, GPRS and UMTS networks) are converging their core network infrastructure to the Internet Protocol (IPv4/6) [1] [2] suite. While IPv6 is being chosen as an underlying convergence protocol for vehicle networking, the introduction of high speed Wireless Access in Vehicular Environments (WAVE) necessitates the support of 'breakthrough' safety and commercial applications in Intelligent Transportation Systems (ITS). In particular, the new emerging 'infotainment' applications call for the vehicular networks to support multimedia and real-time services.

In order to enable Mobile Nodes (MNs) and networked vehicles to seamlessly roam across heterogeneous networks while enjoying the plethora of 'all-IP-based' services, there are many challenges arising from inter-technology 'vertical' handovers. A number of network layer mobility solutions have been proposed or discussed in the Internet Engineering Task Force (IETF). Amongst them, Mobile IPv6 [3] (MIPv6) is one of the few solutions that has been widely accepted in the academic world and industry. Since MIPv6 is designed for supporting the mobility of single mobile hosts, the IETF NEMO [4] (Network Mobility) Working Group (WG) has extended it for supporting the mobility of moving networks.

As an extension to the Mobile IPv6 protocol, the NEMO Basic Support [5], is concerned with the mobility of an entire network which dynamically changes its Point-of-Attachment (PoA) (i.e. Access Points, Base Stations) and thus its reachability in the Internet. Its main objective is to maintain session continuity between the Mobile Network Nodes (MNNs) and Corresponding Nodes (CNs) while the Mobile Router (MR) changes its PoA. The MNNs behind the MR are IPv6 nodes and do not need to register or bind their home addresses with the Home Agent (HA) individually. The MR, acting as a gateway between the inter-vehicle network and the network infrastructure, updates its change in IP subnets at the HA by sending a prefix-scope Binding Update (BU) message that associates its Care-of-Address (CoA) with the Mobile Network Prefix (MNP) used by MNNs.

CALM (Continuous Air interface for Long and Medium range) is a family of umbrella protocols being developed in ISO/TC204/WG16 ("Wide Area ITS Communications") in order *"to provide a uniform environment for vehicle data communications that allows vehicles to stay connected using the best communications technology available both in the vehicle and in the infrastructure wherever the vehicle is located"* [6]. In fact, under CALM, MIPv6 and NEMO are selected as two options for supporting host mobility and network mobility in vehicular communications.

Handover performance plays a crucial role in the Quality of Service (QoS) provisioning for real-time services in heterogeneous networks. The period during which the MN/MR loses connectivity with its current link till the time it receives the first IP packet after connecting to the new link is known as the *handover latency.* The overall handover latency in NEMO and MIPv6 consists of Layer 2 (L2) latency and Layer 3 (L3) latency. The L2 handover latency is the period when the MN/MR is disconnected from the air-link of the current Access Router (AR) till the time it successfully accesses the air-link of the new AR. The L3 handover latency comprises of the latencies incurred during the IP layer movement detection, network re-authentication, Care-of-Address (CoA) configuration and BU. With the help of L2 triggers, the Fast Handover for Mobile IPv6 (FMIPv6) protocol [7] developed within the IETF MIPSHOP (Mobility for IP: Performance, Signaling and Handoff Optimization) WG can reduce handover delays in MIPv6.

FMIPv6 reduces the handover delay by exploiting various L2 triggers to prepare a New CoA (NCoA) at the new AR (nAR) while being connected to the link of the old AR (oAR). It relies on the oAR to resolve the network prefix of the nAR based on the L2 identifier reported by the link layer triggers in the MN. Note that, although FMIPv6 is originally designed for improving the handover delay in MIPv6, it can also be used to support NEMO after minor extensions. The idea is very simple: the traffic addressed to MNNs in a Mobile Network would need to be tunneled to the MR's CoA; the MR here will be treated like a MN by FMIPv6 for traffic redirection between oAR and nAR using the binding of the Previous CoA (PCoA) and the NCoA maintained at the oAR. The overall handover process (i.e. handover message signaling) would be identical to the procedure described in the original FMIPv6 RFC [7] with minor extensions. We will discuss the details about the extensions later in Section 2.13.3.2.

The IEEE802.21, namely the Media Independent Handover (MIH) Standard WG [8] officially formed in 2004, is developing a standard that provides generic link layer intelligence and other network related information to upper layers to optimize handovers between different heterogeneous media, such as 3GPP/3GPP2, and both wired and wireless media of the IEEE802.21 family. Considering the overlap of work in IEEE802.21 and CALM in the handover area, a liaison between these two is being discussed. The IETF MIPSHOP WG has liaised with IEEE802.21 WG to investigate the delivery and security issues of transporting MIH services over IP [9-12, 22].

In this paper, we investigate the potential of applying FMIPv6 in vehicular environments, and optimize the handover procedure of the FMIPv6 protocol in vehicular environments by using IEEE802.21 Media Independent Handover (MIH) services. With the aid of the lower three layers' information of the MN/MR and the neighboring access networks, we tackle the radio access discovery and candidate AR discovery issues of FMIPv6. We designed an 'Information Element Container' to store static and dynamic L2 and L3 information of neighboring access networks, and propose to use a special cache maintained by the MN/MR to reduce the anticipation time in FMIPv6, thus increasing the probability of the predictive mode of operation. Furthermore, we propose a cross-layer mechanism for making intelligent handover decisions in FMIPv6. Lower layer information of the available links obtained by MIH services as well as the higher layer information such as Quality of Service (QoS) parameter requirements of the applications are used by a Policy Engine (PE) to make intelligent handover decisions. We will show through analysis and simulations of the signaling process that the overall expected handover (both L2 and L3) latency in FMIPv6 can be reduced in the proposed mechanism.

The rest of the paper is organized as follows. Section 2.13.2 introduces the related works, where the issues of FMIPv6 in vehicular environments, IEEE802.21 MIH Function and its related services will be introduced. Section 2.13.3 provides an overview of the proposed mechanism and the extension of FMIPv6 for NEMO. Section 2.13.4 introduces the detailed handover procedure in the proposed mechanism. Mathematical and numerical evaluations of the handover performance of the proposed mechanism are given in Section 2.13.5, and Section 2.13.6 concludes the paper and discusses the future work.

2.13.2. RELATED WORKS

2.13.2.1. FMIPv6: Overview and Problem Statement

FMIPv6 concentrates on the protocol operation and does not consider issues such as radio access network discovery and candidate AR discovery (i.e. how the ARs could map the network prefix with the corresponding L2 identifier). Although the anticipation mechanism specified by FMIPv6 is useful, it also introduces additional problems.

Neighbouring access network discovery: The FMIPv6 does not address any radio access network discovery mechanism. Discovering the available PoAs by actively scanning all the channels provided by the neighbouring networks takes a considerable amount of time, which has significant contribution to the overall handover latency. For example, in 802.11b, the L2 scanning can take 400ms to 800ms [18].

Information exchange with neighbouring ARs: How neighbouring ARs exchange information to construct PrRtAdv messages is not specified in the RFC of FMIPv6. The IETF SEAMOBY WG has developed the Candidate Access Router Discovery (CARD) protocol [19][21] to address this issue. However, it does not support the sharing of L2 information between the ARs.

The cost of anticipation: There are three FMIPv6 signaling messages involved in the anticipation phase: *Router Solicitation for Proxy Advertisement* (RtSolPr), *Proxy Router Advertisement* (PrRtAdv) and *Fast Binding Update* (FBU). These messages are used for assisting IP movement detection and NCoA configuration. In FMIPv6, the L2 handover is triggered by the degraded link condition. It is likely that the MN will not be connected to the oAR long enough to send and receive all FMIPv6 messages. When anticipation is used, the MN may not have sufficient time to update the oAR with the FBU. As a result, if the MN has already lost connection with oAR, the MN will then be forced to operate in the reactive mode and the handover latency will increase consequently.

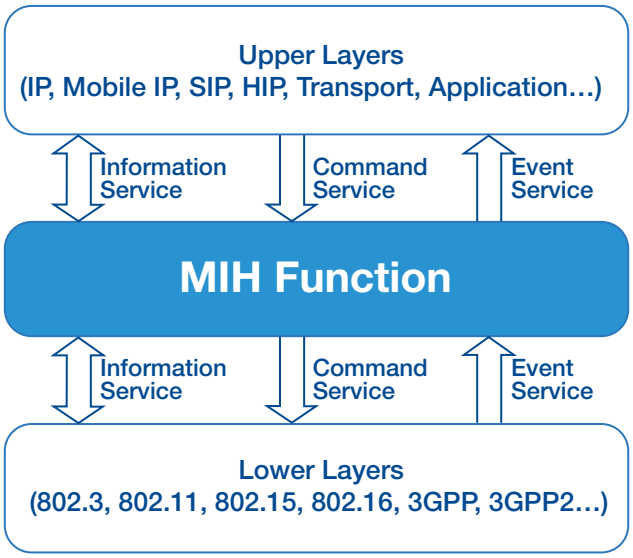
2.13.2.2. IEEE 802.21 Media Independent Handover Function

In the mobility management protocol stack of both the MN and network element, the IEEE802.21 Media Independent Handover Function (MIHF) is logically defined as a shim layer between the L2 data link layer and L3 network layer [8]. The upper layers are provided services by the MIH function through a unified interface. The services exposed by the unified interface are independent of access technologies. This unified interface is known as MIH_SAP. The lower layer protocols communicate with the MIHF via media dependent SAPs (i.e. Link_SAP).

MIHF defines three main services that facilitate handovers between heterogeneous networks: MIH Event Services (MIES), MIH Command Services (MICS) and MIH Information Services (MIIS). Figure 2.13.1 shows the MIH Framework. Detailed discussions of each of the services is given below.

Media Independent Event Service (MIES) provides event reporting, event filtering and event classification service corresponding to the dynamic changes in link characteristics, link quality and link status. The MIES report both local and remote events to the upper layers. Some of the events that have been specified by IEEE 802.21 are "Link Up", "Link Down", "Link Detect"," "Link Parameter Reports" and "Link Going Down". Mobility management protocols can use some of these events, for example, Link Down or Link Going Down as handover triggers. Together with the QoS requirements from the application layer, the reported link status, quality and characteristics will also be very useful for the mobility management entity to make handover

Figure 2.13.1: IEEE 802.21 Media Independent Handover Framework [8]



decisions, i.e. to decide which network and PoA within several available networks and PoAs the MN should switch to, and when the MN should make the handover.

Media Independent Command Service (MICS) uses the MIHF primitives to send commands from higher layers (e.g. Policy Engines, Mobility protocols) to lower layers. The MICS commands are utilized to determine the status of the connected links and also to execute mobility and connectivity decisions of the higher layers to the lower layers. For example, the mobility management protocol can use MICS to inform the link layer to get ready before the actual handover happens, and to give the command to the link layer to switch from one network interface to another. It also allows the mobility management protocols to enquire about the link layer's status before the handover decision making.

Media Independent Information Service (MIIS) provides a framework and mechanism for an MIHF entity to discover available neighbouring network information within a geographical area to facilitate the handover process. The primary idea is that, in order to represent the information across different access technologies, the MIIS specifies a common way of representing this information by using a standard format such as XML (Extensible Markup Language), ASN.1 (Abstract Syntax Notation One), or TLV (Type Length Value), and this information can be obtained through a certain query/response mechanism. Both static and dynamic information is provided by the MIIS. Examples of static information include the names of service providers, MAC addresses, channel information of the MN's current network neighbourhood. Dynamic information includes link layer parameters such as, data rate, throughput, and other higher layer service information to make intelligent handover decision.

In the current 802.21 MIIS specification, a MN gets the heterogeneous neighbourhood information by requesting Information Elements (IEs) from the Information Server (IS). It also allows the neighbourhood information to be delivered to the MN by using pre-defined Information Reports/IE Containers to effectively represent the heterogeneous neighbourhood information in TLV format. In IEEE 802.21 draft, the defined IEs provide mostly static L2 information.

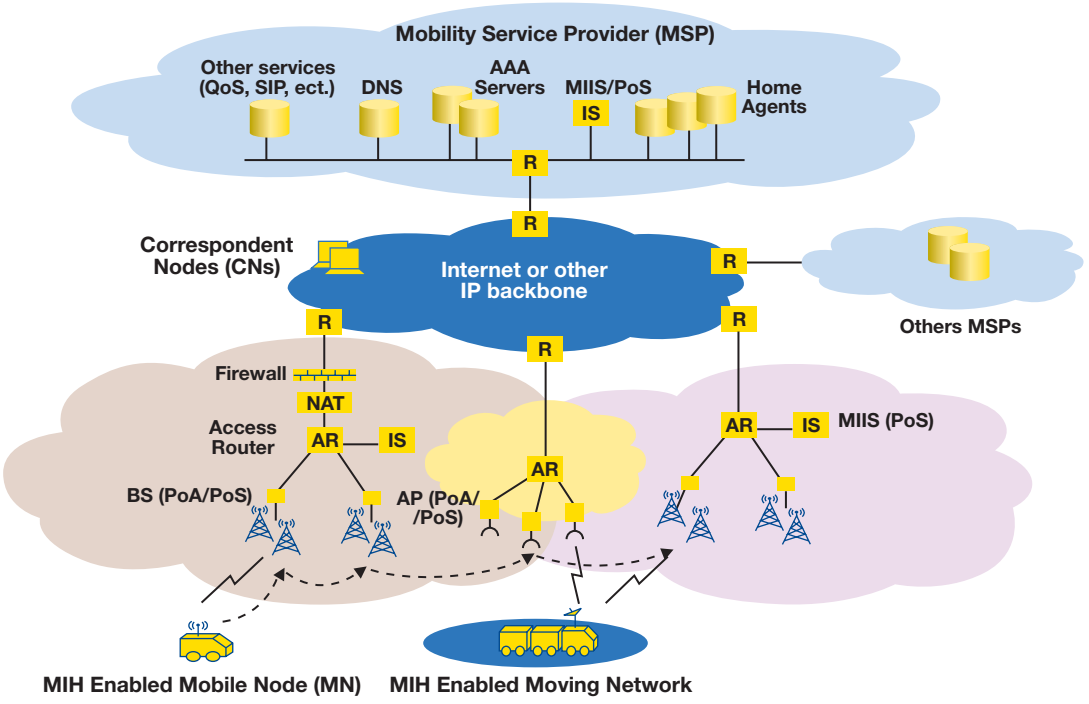
In [9], a problem statement is defined in transporting the MIH services over IP. Some usage scenarios and models for MIH Event, Command and Information services are outlined in [10] and [11]. The security considerations of MIH services are also discussed in these papers. In [12] a UDP-based mechanism for the transport of MIH services between network nodes is defined.

The network requirement of IPv6 based vehicular communication systems are investigated in [13]. The use of IEEE802.21 reference model for appropriate network selection in vehicle-to-infrastructure systems is discussed in [14] and [15] respectively. An optimized solution for reducing the handover latency in Nested NEMO is provided in [16]. Works have also been done on using MIH services as a way to reduce the handover latencies in [17] and [18], however, they did not address the vehicular networking environment.

2.13.3. IMPROVING FMIPV6 WITH IEEE 802.21 SERVICES IN VEHICULAR NETWORKS

Figure 2.13.2 illustrates the network architecture considered in this paper. The MN/MR could be an MIH enabled multi-mode mobile device. The MIH enabled PoA that the MN is currently attached to is the serving Point of Service (PoS), whilst the other MIH enabled PoAs are candidate PoSs. The IS also serves as a MIH PoS which could be located in either the access network or the core network. The IS could be considered as a data reservoir for storing and managing the knowledge of neighbouring networks.

Figure 2.13.2: An Overview of the Considered Network Architecture



MIIS: Media Independent Information Server | **PoS:** MIH Point of Service (PoS) | **PoA:** Point of Attachement

2.13.3.1. Extending FMIPv6 to Support Network Mobility Solution - NEMO

As mentioned in Section 2.13.1, FMIPv6 could be used to support network mobility, but needs minor extensions. The necessary extensions will include extending the FBU, HI, HAck and FBack messages specified in the NEMO Basic Support [5]:

The FBU message - A new Flag Option(R) will be needed in the original FBU message to distinguish the message sender - whether it is a single MN or a MR of a mobile network. We set R to be 0 for a MN, and 1 for a MR. A new Mobility Header Option will be needed for carrying Mobile Network Prefix (MNP). Upon receiving a FBU message, the oAR will first check the R flag. If R is 0, i.e. the FBU is sent from a MN, and the FMIPv6 will operate as it is originally defined. If R is 1, the oAR will understand that, the FBU is send from a MR of a mobile network and it needs to forward incoming packets that are destined to the mobile network to the MR. The oAR will then find out the MNP from the Mobile Header option and tunnel the packets with this MNP (destined to the MNNs in the mobile network) to the nAR during handovers. Note that, the MNP only needs to be carried as a mobility options in the explicit mode [5] of NEMO operation. In the NEMO implicit mode [5], the MR does not include any MNP, the oAR can then use any mechanism to determine the route to the MNNs.

The FBack Message - A new Flag Option(R) will be needed in the original FBack message to distinguish the FBack message receiver - whether it is a single MN or a MR of a mobile network.

The HI message - The MNPs can be transmitted between the oAR and nAR using one of the "Options" fields of the HI message. Both the oAR and nAR could maintain a Prefix Table [5] for preventing the clash between a newly claimed MNP and a MNP that is being used. The mechanism for tackling duplicate MNPs is out of scope for this paper.

The HAck message - should contain new status results indicating the success or failure in accepting the MNPs maintained by the MR.

2.13.3.2. Overview of the 802.21 Assisted FMIPv6 Mechanism

In this section, we use IEEE802.21 MIH services to assist FMIPv6 to enhance the overall handover performance in vehicular environments by addressing the issues discussed in Section 2.13.2.

1) We define a Heterogeneous Network Information (HNI) Container to facilitate the storing and retrieval of the L2 & L3 static information of neighbouring networks obtained through the IEEE 802.21 MIIS. The IE known as 'Subnet Prefix' is used to provide subnet prefixes of neighbouring ARs. Alongside the L2 information, they form the proposed pre-defined Heterogeneous Network Information (HNI) container/report. The draft has defined a PoA container and an Access Network Container (ANE) [8], which include many IEs such as MAC address, channel range, Network Type, Cost, Roaming Agreements, Network Security. Instead of including all of IEs from these two containers, we select the ones which can further optimize our proposal and put them in a single IE container, which is our HNI container. Having a single predefined HNI container will be ideal in vehicular environments and help in reducing the message overheads, processing and lookup/indexing times.

   The handover latency caused by the radio access discovery in FMIPv6 will be eliminated by using the L2 link information retrieved from the MIIS. Furthermore, with the L3 information of corresponding PoAs, the MN will learn of subnet prefixes of the nAR and form the NCoA prior to handover. This eliminates the router discovery time and optimizes the L3 handover latency in FMIPv6. Note that the HNI Report maintained

by an IS will be similar to the mapping table maintained by the ARs for resolving L2 Identifiers of corresponding subnet prefixes. This could eliminate the need for ARs to exchange neighbouring information for maintaining the mapping table and thereby tackling the candidate AR discovery issue in FMIPv6.

2) In order to reduce the adverse impacts of the long anticipation time in FMIPv6, we propose to create a Neighbouring Network Report (NNR) Cache in the MN for storing and maintaining the HNI report. This would help to reduce the number of signaling messages during the anticipation phase and thereby reducing the overall anticipation time. The HNI report will be delivered to the MN through the 'MIH_Get_Information' service primitives. By reducing the anticipation time, the probability of operations in predictive mode is increased. Also the CoA configuration time can be reduced and thereby the L3 handover latency is reduced.

3) We use MICS to collect/obtain dynamic QoS link layer parameters directly from MIH enabled Candidate PoAs. Dynamic neighboring network information includes packet loss rate, average packet transfer delay, signal-to-noise ratio (SNR), available data rates, etc.

4) We define a new MICS service primitive for requesting application QoS requirements, and a new MIES for delivering the application QoS parameters to the policy engine. A cross-layer mechanism is proposed for intelligent handover decision making by using the static and dynamic information of neighboring network, the local link condition and application QoS requirements.

2.13.3.3. The IEEE 802.21 MIH Services To Be Used

We utilize a subset of existing IEEE802.21 MIH services to enhance the handover process in FMIPv6. Their corresponding primitives and parameters are listed in Table 2.13.1. In Table 2.13.2, the new MIH service primitives that we defined for the handover decision making are presented.

2.13.3.4. The Structure of HNI Report

The MIIS 'HNI' report will be delivered through a request/response mechanism and will be represented in a standard format such as XML, ASN.1 or TLV. Table 2.13.3 shows the HNI request message in TLV format by which the MN/MR can obtain the HNI_report by specifying the Link Type and Operator Identifiers as parameters. Table 2.13.4 shows the HNI response message. The HNI report containing the IEs will be produced and stored in an IS.

2.13.4. DETAILED HANDOVER PROCEDURE OF THE 802.21 ASSISTED FMIPV6

2.13.4.1. Events Subscription

At the very beginning, when a MN is switched on, the FMIPv6 protocol in the MN will register for MIES notifications (i.e. L2 triggers) within its local stack. This will be done via MIH Event Subscription service primitives [8] that are listed in Table 2.13.1.

Table 2.13.1: **EXISTING MIH SERVICES USED AND EXTENDED**

Primitives	Service	Parameter
MIH_Link_Going_Down	MIES	MN MAC Addr, MAC Addr of Curent PoA
MIH_Link_Up	MIES	MN MAC Addr, MAC addr of new PoA, Link ID
MIH_Link_Down	MIES	MN MAC Addr, MAC addr of new PoA, Reason Code
MIH_MN_HO_Commit	MICS	Old Link ID, New Link ID
MIH_MN_HO_Candidate_Query (extended)	MICS	SNR, Available Data Rate, number of associated user, Throughput , Packet Error Rate, CoS Minimum Packet Transfer Delay, CoS Average Packet Transfer Delay, CoS Maximum Packet Transfer Delay, CoS Packet Loss
MIH_N2N_HO_Candidate_Query	MICS	SNR, Available Data Rate, number of associated user, Throughput , Packet Error Rate, CoS Minimum Packet Transfer Delay, CoS Average Packet Transfer Delay, CoS Maximum Packet Transfer Delay, CoS Packet Loss

Table 2.13.2: **NEWLY DEFINED MIH SERVICE PRIMITIVES**

Primitives	Service	Parameters
MIH_App_Par	MIES	Required data rate, delay, jitter, priority of applications
MIH_App_req	MICS	SNR, Required data rate, throughput , jitter, delay

Table 2.13.3: **HNI REQUEST**

Type = TYPE_ IE_HNI_REPORT	Length = Variable
Type_IE_Container_HNI Report	

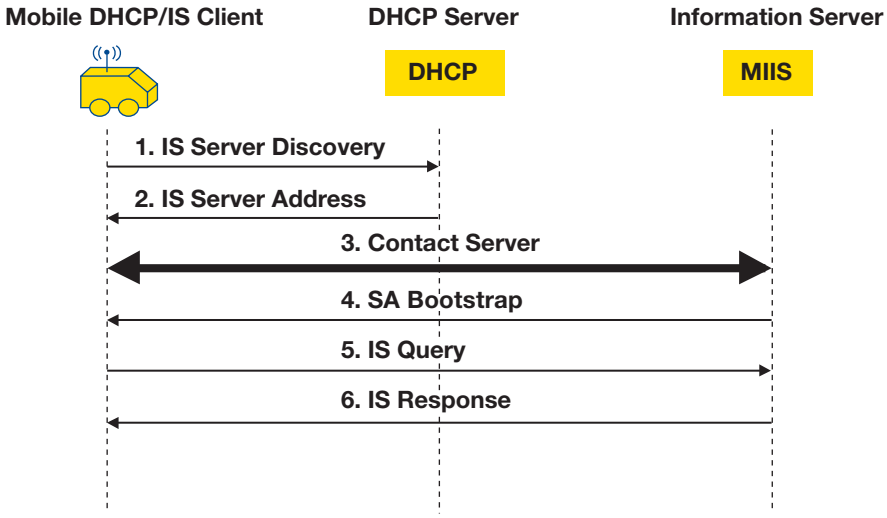
Table 2.13.4: **HNI RESPONSE**

Type = TYPE_ IE_HNI_REPORT	Length = Variable
HNI Container #1	
PoA MAC Address IE	
POA Channel Range IE	
POA MAC Type IE	
POA PHY Type IE	
PoA Subnet Prefix IE	
PoA Subnet Prefix IE	
Network Type IE	
Roaming Partners IE	
Cost IE	
Network Security IE	
HNI Container #2	
... ...	

2.13.4.2. IS Discovery and Usage

Valid ISs can be discovered through either layer 2 or layer 3 mechanisms. At the time of writing, Dynamic Host Control Protocol (DHCP) is one of the candidate solutions for discovering the IS [11, 20]. Figure 2.13.3 shows the three phases related to our MIIS usage scenario: IS Discovery, SA bootstrap, IS Query/Response. The MIIS serves the upper layer entity that implement network selection and handover algorithms, i.e. the Mobility Management Entity (MME).

Figure 2.13.3: Information Server Discovery & Message Exchange



2.13.4.3. SA Bootstrap

Before the MME can exchange any messages with the IS server, a set of Security Associations (SA) have to be established. Authentication and encryption must be provided by each SA for keeping the mobile device anonymity so as to prevent eavesdroppers. The SA negotiation mechanism depends on the used transport layer and required security services [11]. For Instance, TLS (Transport Layer Security) will be advised for use if upper layer protocols use TCP, whilst ESP (Encapsulation Security Payload) using IPSec/IKE will work in most situations without the need to worry about the upper layer protocols, as long as the IS protocol identifiers are handled by IKE [11].

2.13.4.4. Retrieval of Neighbouring Network Information from the IS

It must be noted that the communications between the MN and the IS will be handled by the MIH protocol as specified in the IEEE802.21 draft. The MIH protocol defines the frame structure for exchanging messages between MIH functional entities. The payload of the MIH message contains service specific TLVs. Details on the MIH protocol message structure is provided in [8].

After the IS discovery and SA association phase, the MN will send an MIH message that carries the 'MIH_Get_Information' request TLV as its payload to request the HNI Report from the IS. The HNI report will then be delivered in a returned MIH message from the IS to the MN in the format shown in Table 2.13.3. The contents of the report will be processed by the MN and stored in its NNR cache.

We suggest a time stamp to be maintained by the MN for periodical access to the IS. This would help the MN renew its contents and also check whether it is in the same or different IS domain.

2.13.4.5. Handover Operations

In the proposed 802.21 assisted FMIP6, we replace the RtSolPr/PrRtAdv messages with 'MIH_Get_Information' request/reply messages which are exchanged much before the L2 trigger occurs. This is different from the original FMIPv6 in which the RtSolPr/PrRtAdv only occurs after L2 triggers (i.e. when the MN senses that the signal strength of existing link is becoming too weak). Later, when the signal strength of the current PoA becomes weak, the MIES will be informed by the MAC layer of the MN. The MIES will scope and filter this link layer information against the rules set by the MIH user (FMIPv6 in this case), and then produce a 'MIH_Link_Going_Down' event indication message, and send it to network layer where FMIPv6 protocol resides.

Upon receiving this event notification, the MN checks its NNR Cache and selects an appropriate PoA to handover to. Since the MN knows the radio link information (i.e. MAC address and channel range of PoAs, etc) of the candidate access networks, the time to discover them is eliminated. In IEEE802.11 networks, for example, there will be no need to use the 'scanning' mechanism to find the neighbouring APs. In this paper, we propose to select the appropriate PoA with a cross layer mechanism.

2.13.4.6. Intelligent Handover Decision Making using Cross Layer Mechanisms

The decision to select the appropriate (i.e. optimal) network is based on a policy engine which takes into account the QoS parameter requirements from the application and matches them with the dynamic QoS link parameters from the lower layers (L2 and below) of the available networks. As mentioned before, it is clearly specified in [8] that dynamic link layer parameters (e.g. QoS Parameters such as Throughput, Average Packet Transfer delay, Packet Loss Rate, SNR etc) have to be obtained based on direct interaction with the access networks and MIIS may not to be able to help much in this regard. Such dynamic QoS link parameters will have to be delivered to the MN through the MICS. For this purpose, we extend the service primitive 'MIH_MN_HO_Candidate_Query' defined in [8] to include the list of resources shown in Table 2.13.2 as the 'Query Resource List'.

The MIH_MN_HO_Candidate_Query service primitive works in a request/reply fashion and are carried as payloads of a MIH message as service specific TLVs [8].

Upon choosing a PoA from the HNI Container/Report in the NNR solely on the grounds of the static L2 and L3 information (e.g., MAC address, channel range, subnet prefix), the PE in the MN will use the extended 'MIH_MN_HO_Candidate_ Query' service primitive via the MIHF to send a request to the serving PoA.

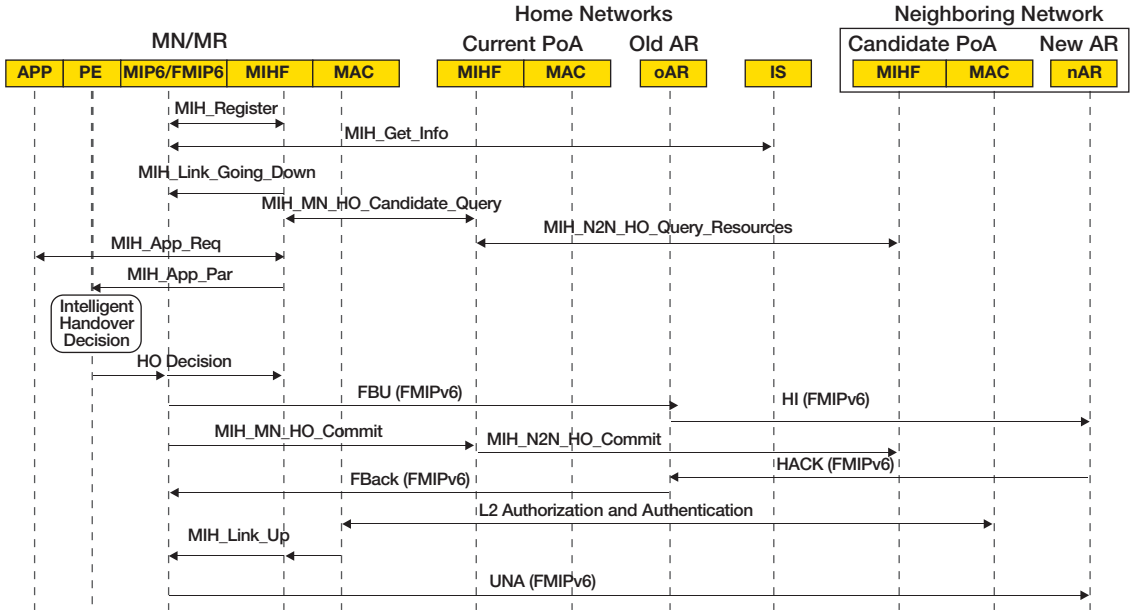
The Serving PoA will use the MIH_N2N_HO_Query_ Resources to prepare and query the available resources in the candidate Networks.

After receiving the MIH_MN_HO_Candidate_response, the PE receives the QoS requirements of the applications. Using the newly defined MICS service primitive 'MIH_App_Req', the QoS requirement parameters are delivered from the application layer to the MIH Layer. The newly defined MIES service primitive 'MIH_App_Parameter' is triggered to deliver the application QoS parameter requirements to the PE. Figure 2.13.4 illustrates how MIH service primitives help the PE in the MN/MR acquire the dyanamic QoS parameters of neighour networks.

The PE takes the application QoS parameter requirements and compares them with the dynamic QoS parameter from the lower layers of the candidate access networks. The “best” PoA to attach to can be selected according to the rules or policies input by the users. Details of such Policies is out of scope

for this paper. Note that sophisticated and complicated algorithms can be implemented in the PE to make intelligent decision. The overall cross-layer mechanism is depicted in Figure 2.13.5.

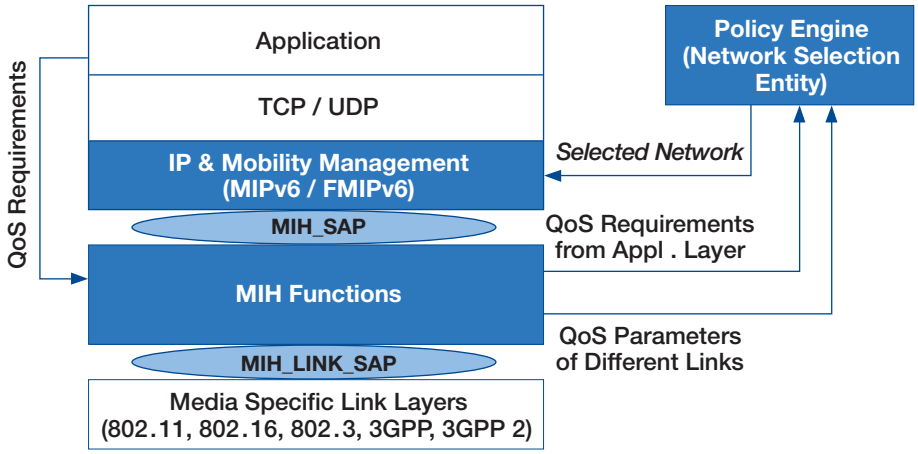
Figure 2.13.4: Message Flow in IEEE 802.21 Assisted FMIPv6 Handover Operations (Predictive Mode)



2.13.4.7. Handover Operations - Switching Link

After selecting an appropriate radio access network, the MME in the MN/MR utilizes MIHF MICS, and generates a link switch command using 'MIH_MN_HO_Commit' and MIH_N2N_HO_Commit primitives as described in [8]. The parameters are shown in Table 2.13.1. Prior to sending the 'MIH_MN_HO_Commit' command, the MN uses the L3 information, the PoA Subnet Prefix, to form a NCoA, and sends a FBU to its default AR (oAR). There is no longer any need to send the RtSolPr/PrRtAdv messages for router discovery as the candidate AR information (i.e. 'Subnet Prefix' IE) is already in the NNR Cache. The CoA address configuration procedure that is related to the candidate AR discovery or RtSolPr/PrRtAdv messages is eliminated. During the anticipation phase, only the FBU message will be sent to the oAR. As opposed to the original FMIPv6 operation, in our proposed mechanism only a single signaling overhead will be incurred during the anticipation phase. The probability of a Predictive Mode of operation in FMIP6 will be increased, and the L3 handover latency in FMIPv6 will be optimized. After receiving the FBack (Fast Binding Acknowledgement) message on the oAR's link and necessary L2 authentication and association procedure, a MIH_Link_Up event notification will be sent to inform the FMIP6 that the L2 connection with the target PoA is established. After the 'MIH_Link_Up' notification, the UNA (Unsolicited Neighbour Advertisement) message is immediately sent and the traffic starts to flow from the new link. Figure 2.13.5 shows the procedure of the cross layer mechanism in selecting the optimal network with the assistance of the newly defined the MIH services.

Figure 2.13.5: A Cross Layer Mechanism for Intelligent Handover Decision Making (MN side)



2.13.5. HANDOVER PERFORMANCE EVALUATION

As explained in Section 2.13.1, FMIPv6 can improve the handover performance of MIPv6 as well as NEMO. Our proposed 802.21 assisted FMIPv6 mechanism should also be applicable to optimize NEMO handover procedures. In this section we analyse the handover delay of the original NEMO, original FMIPv6 and the 802.21 assisted FMIPv6. The overall handover latency (both L2 and L3), i.e. the time interval between the moment the MN/MR loses connectivity with its current PoA till the moment it receive the first IP packets in the new subnet, is analysed. For this reason, we include both the L2 and L3 handover.

2.13.5.1. Handover Latency in NEMO

The handover procedure for both FMIPv6 and NEMO can be expressed by

$$d_t = D_{L2} + D_{L3} \quad (1)$$

where d_t is the overall handover latency time, including both L2 and L3 latencies. Here D_{L3} is the time period when the MN/MR is unable to send or receive any IP packets due to handover action. D_{L2} is the time period the MN/MR loses connectivity with its current air link (i.e. PoA) till the time it connects to a new PoA. The overall handover procedure in both NEMO and FMIPv6 is started when L2 handover is initiated.

The L2 handover latency in IEEE802.11 WLAN, for example, could take place in two distinct phases: the discovery phase and the re-authentication phase. During the 'discovery' phase, when the MN detects that the signal strength from the current AP is degraded to an unacceptable level, the MR/MN will start to scan available neighbouring APs and generate a list of the APs prioritized by the corresponding signal strength. The 'Re-authentication' phase involves exchanging authentication and association messages between the MN and the AP. More details of the L2 handover in IEEE802.11 can be found in [24]. The 802.11 L2 handover delay can be expressed as

$$D_{L2} = D_{Discovery} + D_{Re\text{-}authentication} \quad (2)$$

For a MR in NEMO, its first step in the L3 handover is to perform the movement detection, during which the MR sends Router Solicitation (RS) to nAR. Upon reception of the RS, the nAR sends a Router Advertisement (RA) to the MN. After receiving the RA, the MN will know that it has moved. The delays caused by movement detection can be expressed as:

$$D_{MV} = D_{RD} + D_{CoA} + D_{DAD} \quad (3)$$

where,

$$D_{RD} = D_{RS} + D_{RA} \quad (4)$$

Here D_{MV} is the time required for a MR to detect its movement and to form a new CoA. D_{RD} is the router discovery time and includes the delays caused by sending RS (i.e. D_{RS}) and RA (i.e. D_{RA}). It also includes the time the MN takes to form a new CoA (i.e. D_{CoA}) and to perform Duplicate Address Detection (DAD), i.e. D_{DAD}.

After movement detection, the MR must send BU to inform the HA and the CN of its new location, i.e. nCoA. The total handover latency can be expressed as the sum of L2 and L3 handover latency as

$$d_t = D_{HO\text{-}NEMO} = D_{L2} + D_{RD} + D_{CoA} + D_{DAD} + D_{BU\ (MN\text{-}HA)} \quad (5)$$

2.13.5.2. FMIPv6 Handover Latency in FMIPv6

The handover latency in FMIPv6 is also comprised of the L2 part and the L3 part. However, the delays associated with movement detection, new CoA configuration and DAD are eliminated in FMIPv6. The FMIPv6 has the handover initiation time to perform the CoA configuration prior to the L2 handover. After the L2 handover, the MN sends a Fast Neighbour Advertisement (FNA) message to nAR to inform its presence and then perform the BU operations.

$$D_{HO\text{-}FMIPv6} = D_{L2} + D_{MN\text{-}nAR} \quad (6)$$

In (6), $D_{MN\text{-}nAR}$ is the delay to send the FNA message from the MN to the nAR. In the reactive mode, this will take a single Round Trip Time (RTT) since the MN will have to wait for the FNAAck (FNA Acknowledgement) message after sending the FNA. The Handover Initiation (HI)/anticipation time is equal to the time required to send the RtSolPr and PrRtAdv, FBU and FBack messages. Note that it is not necessary to include the FBack in the HI time as it is not required to be received on the current link. However, for operations in predictive mode, it is mandatory for the FBack message to be received while being connected to the oAR's link. The Handover Initiation time is given below in the following equation.

$$T_{HI} = D_{PrRD} + D_{FMIPv6} = D_{RtSolPr} + D_{PrRtAdv} + D_{FBU} + D_{FBack} \quad (7)$$

Here, D_{PrRD} is the time for sending the RtSolPr and PrRtAdv messages. D_{FMIPv6} is the time it takes for sending the FBU and to receive the FBack message.

2.13.5.3. Handover Latency of the 802.21 assisted FMIPv6

In our proposed mechanism, L2 handover latency is significantly reduced by removing the radio access network discovery delay (i.e. scanning time). The handover initiation/anticipation time is reduced by removing the RtSolPr and PrRtAdv delay from D_{PrRD}.

$$T_{HI} = D_{FBU} + D_{FBack} = D_{FMIPv6} \quad (8)$$

The 'discovery' phase will be eliminated from the L2 handover time in the proposed mechanism. Therefore, the overall handover delay is:

$$D_{HO\text{-}FMIPv6} = D_{Re\text{-}authentication} + D_{MN\text{-}nAR} \quad (9)$$

Table 2.13.5 show the comparison of the handover latencies of the original NEMO, FMIPv6 and the 802.21 assisted FMIPv6.

Table 2.13.5: **COMPARISON OF HANDOVER LATENCIES OF NEMO, FMIPV6 AND THE 802.21 ASSISTED FMIPV6**

Handover Mechanism	Handover Latency	Handover Initiation Time
NEMO	$D_{Discovery} + D_{Re\text{-}authentication} + D_{RD} + + D_{CoA} + D_{DAD} + D_{BU}$	
FMIPv6 (Predictive)	$D_{Discovery} + D_{Re\text{-}authentication} + D_{MN\text{-}nAR}$	$D_{PrRD} + D_{FMIPv6}$
FMIPv6 (Reactive)	$D_{Discovery} + D_{Re\text{-}authentication} + 2D_{MN\text{-}nAR}$	$D_{PrRD} + D_{FMIPv6}$
802.21 assisted FMIPv6	$D_{Re\text{-}authentication} + D_{MN\text{-}nAR}$	D_{FMIPv6}

2.13.5.4. Simulation Results

To evaluate our proposed mechanism, we simulate a network scenario in an area of 2000 meters by 2000 meters in which one WiMAX (IEEE 802.16) cell and one IEEE 802.11b WLAN Basic Service Set (BSS) are located. The WiMAX cell has a radius of 1000 meters, whilst the coverage area of the WLAN has a radius of 50 meters. The WLAN BSS is inside the WiMAX cell. We assume that they are managed by one mobility service provider. The WiMAX network is the home domain where the HA is located. Each domain has one PoA which is connected to the core network through 100Mbps connection. A correspondent node (CN) is connected to the core network through the 100Mbps Ethernet. A WiMAX/WLAN dual mode MN/MR is communicating with while it is moving in the above area at a random speed between 5 meter/s and 25 meter/s. Each time it enters and leaves the WLAN area, handover procedures will be initiated.

Based on the FMIPv6 package we developed and the 802.21 and 802.16 NS2 extension developed by NIST [23], we carry out the simulations in NS2. We focus on evaluating the handover performance in terms of handover latency, packet loss and handover signaling.

Two types of traffic flows are transmitted between the MN and the CN. One is a video stream with a packet size of 4960 bytes and a packet rate of 100 packets/s. Another is an audio flow with a packet size of 320 bytes and a packet rate of 200 packets/s. Simulation time is set up as 200s. For each mean speed, we take the average of the results of 10 simulations.

From the simulation results presented in Figure 2.13.6, 2.13.7 and 2.13.8, we can see that obviously the handover process of FMIPv6 can be significantly improved by using the IEEE 802.21 MIH services. Unsurprisingly, the handover latency increases in both the original FMIPv6 and the 802.21 assisted FMIPv6 as the moving speed of the MN/MR increases (Figure 2.13.6). This may be due to the signaling packet loss over the deteriorated physical link, or the fact that MN/MR might not have sufficient time to complete all FMIPv6 signaling at the oAR's link. 802.21 assisted FMIPv6 can reduce almost half of the handover latency of the original FMIPv6.

Figure 2.13.7 shows that 802.21 assisted FMIPv6 loses less packets than the FMIPv6 does when speed increases. When MN/MR moves at high speed, the FMIPv6 handover process might not be completed at the oAR's link hence packets received by the oAR would be dropped. The overall signaling overhead here is the average signaling overhead (in bits) at the network and above layers during each handover interval. Figure 2.13.8 shows that the 802.21 assisted FMIPv6 has about 50% less signaling overhead than the original FMIPv6 does. This is aligned with our analysis on the proposed mechanism given in previous sections.

Figure 2.13.6: Average handover latency vs. node average speed

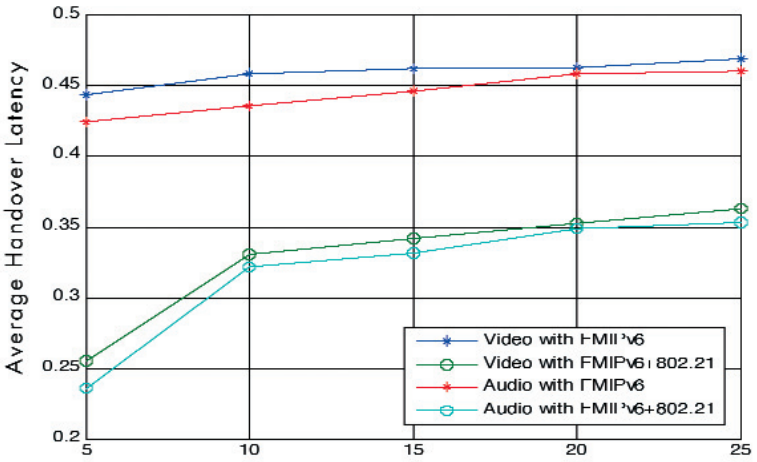


Figure 2.13.7: Average packet loss vs. node average speed

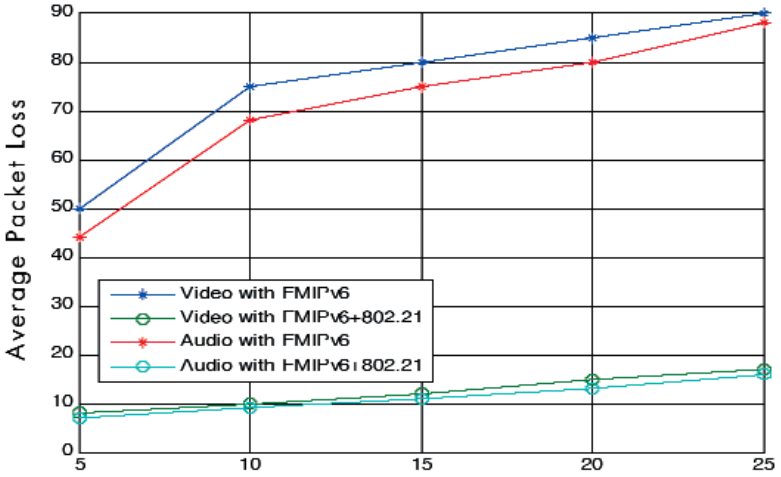
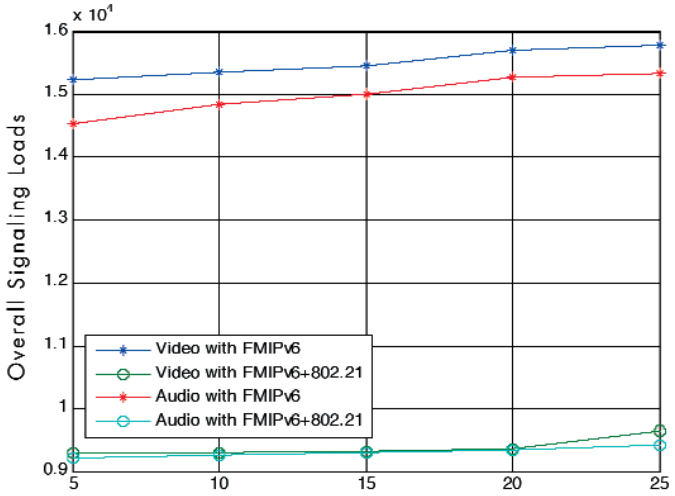


Figure 2.13.8: Overall signaling loads vs. node average speed



2.13.6. CONCLUSIONS

In this paper, we propose a mechanism which optimizes the FMIPv6 handover procedure with the assistance of IEEE802.21 MIH services for vehicular networking. To do so, we have exploited the MIH services. Most notably, we utilize the 802.21 MIIS and include L3 information of neighbouring access networks in the MIIS service. We define a new Information Report, the 'HNI Container/Report' to contain L2 and L3 information of neighbouring access networks which can help the FMIPv6 protocol to tackle issues such as radio access discovery and candidate AR discover. Moreover, we propose to store the contents of the HNI Container/Report in the NNR cache which can be maintained in the volatile memory of the MN. This eliminates the need for sending RtSolPr/PrRtAdv messages which in turn reduces signalling overheads and the long anticipation time imposed by FMIPv6. Therefore, we show through analytical and simulation results that when our proposed mechanism is applied to FMIPv6, it increases the probability predictive mode of operation and reduces overall (both L2 and L3) handover latency. The proposed mechanism outperforms the original FMIPv6 protocol and NEMO basic support.

Moreover, the handover decision is made by a policy engine where a cross-layer mechanism is adopted. New MIH service primitives are defined to support the intelligent handover decision making. The cross-layer mechanism takes into account QoS parameters requirements from the applications and compares it with the dynamic parameters of the available access networks. The parameters are then matched with pre-defined policies to optimize the handover decision.

2.13.7. REFERENCES

[1] S.Deering et al, "Internet Protocolv6 Specification", RFC 791, IETF, December 1998

[2] Marina del Rey, "Internet Protocol Specification", RFC 2460, IETF, September 1981

[3] D. Johnson et al., "Mobility Support in IPv6". RFC 3775, IETF, June 2004.

[4] Ernst, T., "Network Mobility Support Goals and Requirements", Internet Draft (work in progress), IETF, November 2006

[5] Devarapali, V., Wakikawa, R., Petrescu, A., and P.Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, IETF, January 2005.

[6] "CALM -Medium and Long Range, High Speed, Air Interfaces parameters and protocols for broadcast, point to point, vehicle to vehicle, and vehicle to point communication in the ITS sector - Networking Protocol - Complementary Element", ISO draft ISO/WD 2121 (works in progress), ISO, Technical committee 204, WG16, December 2005

[7] Koodli, et al., "Fast Handovers for Mobile IPv6", RFC 4608, IETF, April 2006

[8] Draft IEEE standards ,"IEEE802.21 Standard and Metropolitan Area Networks: Media Independent Handover Services", Draft P802.21/D00.05, March 2006

[9] T. Melia, E. Hepworth S. Sreemanthula, S. Faccin, Y. Ohba, G. Vivek, J. Korhonen, S. Xia, "Mobility Services Transport: Problem Statement", IETF Draft (work in progress), IETF, May 2007

[10] S. Sreemanthula, S. Faccin, G. Daley, E. Hepworth, S. Das, " Requirement For Handover Information Services", Internet Draft (work in progress), IETF, March 2006

[11] S. Sreemanthula, G. Daley, E. Hepworth, "Problem Statements and requirements for Event and Command Services in Media Independent Handovers", Internet Draft (work in progress), IETF, March 2006

[12] A. Rahman, U. Olvera-Hernandez, J.C. Zuniga, M. Watfa,, H.W. Kim "Transport of Media Independent Handover Messages over IP", Internet Draft (work in progress), IETF, February 2007

[13] T. Ernst, "The Information Era of the Vehicular Industry", in Proceedings of ACM SIGCOMM Computer Communication Review, volume 36, number 2, April 2006

[14] E. Weiss, G. Gehlen, S. Lukas, C. Rokitansky and B. Walke , "MYCAREVENT- Vehicular Communication Gateway for car maintenance and Remote Diagnosis, in Proceedings of ISCC, 2006

[15] G. Gehlen, E. Weiss, S. Lukas, C. Rokitansky, B. Walke, "Architecture of Vehicle Communication Gateway for Media Independent Handover", http://www.mycarevent.com, February, 2007

[16] M. Sebeur, B. Jaoaber, D. Zeghlache, "Low Latency Handoff for Nested Mobile Networks", in Proceedings of IEEE CCNC, 2006

[17] Y. Young An, B.H Yae, K.W Lee, Y.Z Cho and W.Y Jung, "Reduction of Handover Latency Using MIH Services in MIPv6", in Proceeding of AINA'06

[18] Q. B. Mussabbir and W. Yao, "Optimized FMIPv6 Handover using IEEE802.21 MIH Services", in Proceedings of the 1st ACM/IEEE International Workshop on Mobility in the Evolving Internet Architecture (MobiArch 2006).

[19] M. Liebsch, et.al, "Candidate Access Router Discovery (CARD)", RFC 4066, IETF, 2005.

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

[21] J.Zhang, H.Chen, Z. Xia, X. Duan, Z. Zhou, "AR Information for FMIPv6", draft-zhang-mipshop-fmip-arinfo-00.txt, IETF, June 2006

[22] Y Ohba, "IEEE 802.21 Basic Schema", Internet Draft, IETF, Jan 2007

[23] NIST Project- Seamless and Secure Mobility tool suits: http://www.antd.nist.gov/seamlessandsecure/doc.html, May 30, 2007

[24] H.Soliman, 'Mobile IPv6 : Mobility in Wireless Internet',Addison-Wesley, 2004

2.14 Scenarios Designed for the Verification of Mobile IPv6 Enabling Technologies

Miguel Ponce de León, **Waterford Institute of Technology**
Wenbing Yao, **Brunel University**
Miguel A. Díaz, **Consulintel**

ABSTRACT

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.

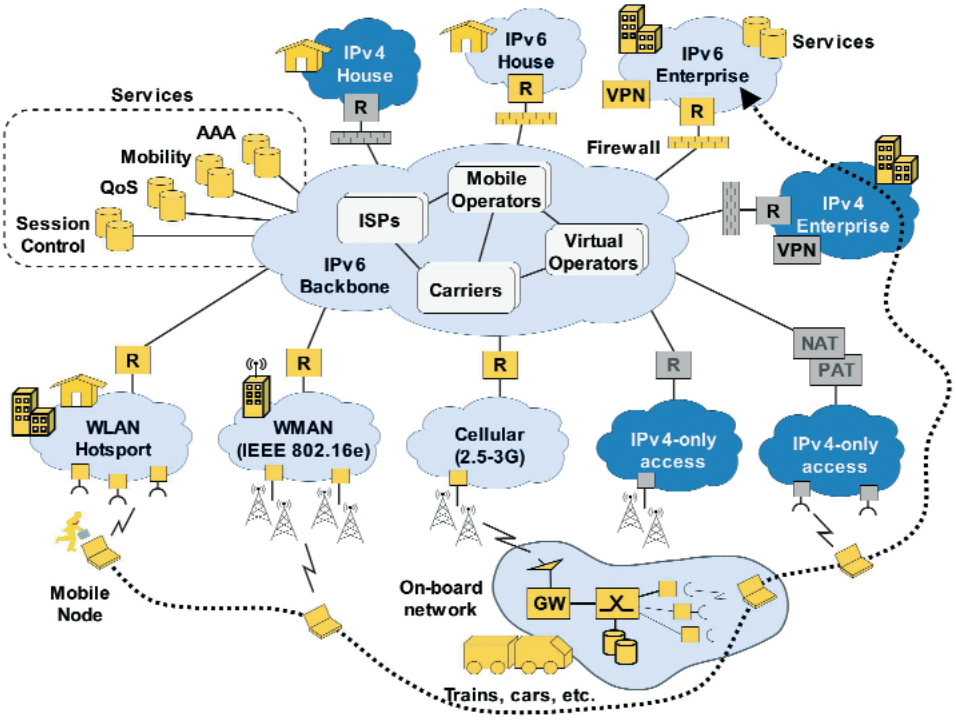
Keywords

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

2.14.1. INTRODUCTION

It is clear over the past few years, that mobile operators have been offering extensive data services through their cellular infrastructure. However, there are many other delivery options available to fulfil the mobility demand of business and consumer users, such as, 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). The rapid development of these technologies and falling equipment prices have led to an inherently multi-access and multi-provider market (Figure 2.14.1) 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 2.14.1: Multi-access and multi-provider



It is a difficult and risky excise to predict customers' needs in the fore-seeing scenario depicted in the Figure 2.14.1 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 compromising the end-to-end transparency of the Internet. Solutions based on Mobile IPv6 (MIPv6) [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 MIPv6 in large scale deployment in the domain of one network provider, and a method of validating results through prototyping and testing in a designed application scenario in laboratory environments.

2.14.2. ENABLING TECHNOLOGIES OF MIPV6

Amongst many candidate technologies, a 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) are the other two components being developed. However as they are separate mobility solutions they will not be discussed further in this paper.

2.14.2.1. 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 provided 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's 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 delivering MIPv6 service to customers. The process is known as MIPv6 bootstrapping [5] and is executed in order to obtain 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 and send an EAP Success message.

2.14.2.2. 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.

2.14.2.3. 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.

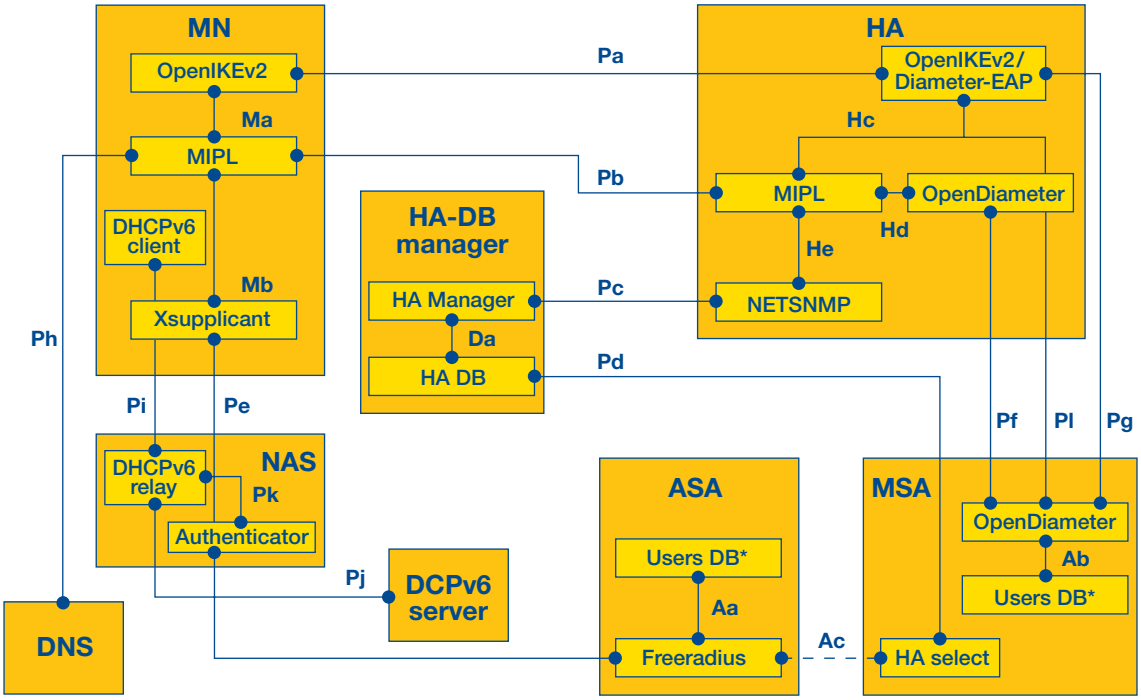
In the ENABLE solution, for HA selection, the MSP assesses the current situation of the HAs by evaluating several pre-defined selection parameters, such as, the number of home registrations (Registrations), the currently consumed bandwidth on home link (Bandwidth), announcement of upcoming maintenance (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 the 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 are normalised to have values between 0.0 and 1.0.

2.14.2.4. 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 2.14.2: ENABLE Integrated Software architecture



* In an integrated scenario this two User DB could be the same one and the interface Ac is present

Figure 2.14.2 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 Node (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 black connectors. Both software modules and interfaces are described in the IST ENABLE Deliverable D6.1 [15].

2.14.3. 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 are 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. 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 enduser perspective and are structured into different scenes. They are user driven / user focused and demonstrate how a user will handle complex future technologies 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.

2.14.3.1. 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

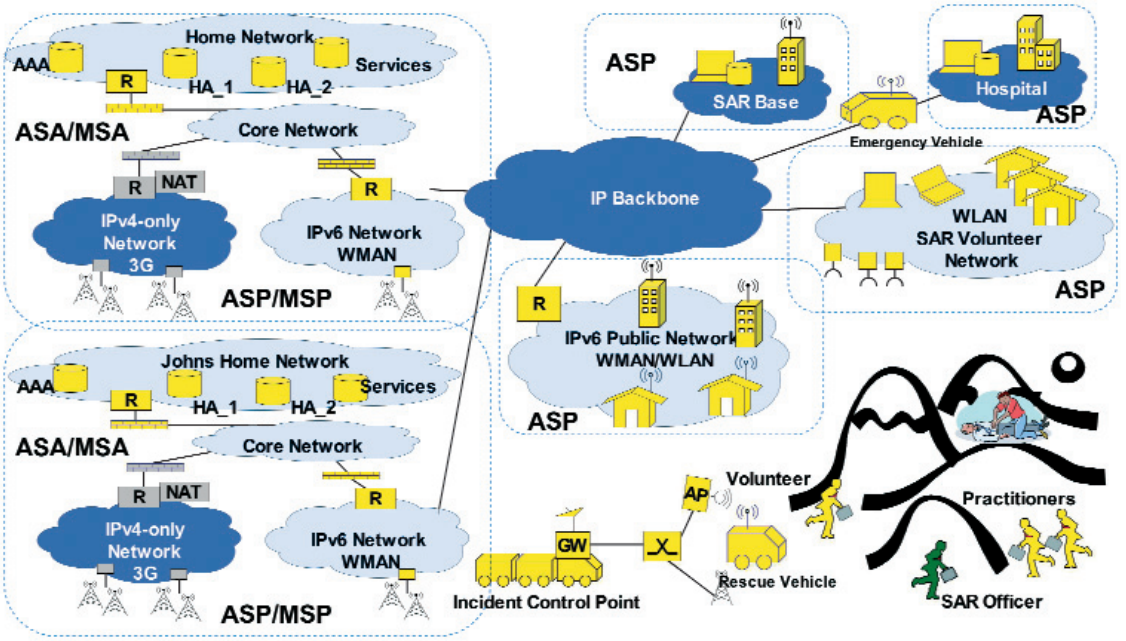
management scenario rich with application opportunities, and gave the possibility to incorporate the Location Based Services (LBS) and VoIP Application into the scenario.

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 its 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.

2.14.3.2. Implementation

Figure 2.14.3: Scene layout for the Search and Rescue (SAR)



The IST ENABLE scenario takes into account 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 required performance level. Another example would be the seamless movement across homogeneous and heterogeneous access networks, 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 mobil-ity 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 prac-titioners to access 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 per-sonnel 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 accessibility 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 2.14.3, 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 has been demonstrated and mapped to the software components, is 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.

2.14.3.3. Case Study in Detail

3a) John is one of the volunteers, called in by the search teams whenever there is a lack of resources at the search site. John has a MN with four network interfaces including WLAN/WMAN, 3G and LAN.

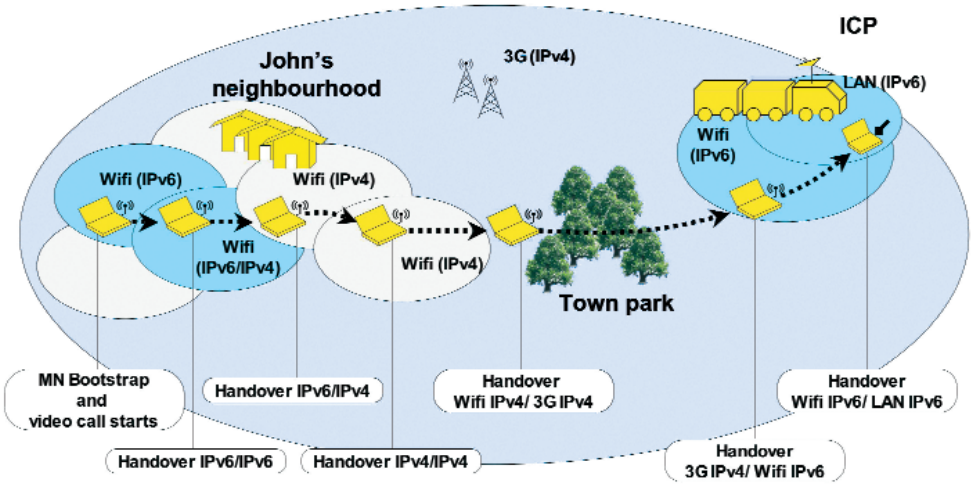
3b) John can access any of these networks over both IPv4 and IPv6 networks. When John is leaving the house he re-ceives a video call.

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 net-works. John will loose the WLAN coverage when he approaches the town park which he must go through to reach the search site. Thus 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 to 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 2.14.4 shows scene 3 case study in detail.

Figure 2.14.4: Scene 3 Case Study in Detail



2.14.3.4. 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 IPv6 network 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.

2.14.3.5. 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 the 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.

2.14.3.6. 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 during 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) to 3G Networks.

2.14.3.7. 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.

2.14.4. 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 with-out 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 imple-mented 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 stand 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.

2.14.5. 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.

2.15 Converged Multi-access Radio Networks in Beyond 3G Heterogeneous Environment

Bin XIA, Yan PENG, and Guohui Zou

ABSTRACT

In this paper, we introduce a converged radio access network concept based on heterogeneous physical layers, w/o generic L2/L3 protocols. Such network could accommodate a wide variety of the existing and future communication systems, such as Wi-Fi, GPRS, NxEV-DO, UMTS HSPA/LTE, and new radio technologies for Beyond 3G. By pushing intelligence to the network boundaries, a flexible framework with very flat architecture for different deployment scenarios and performance targets is presented. Some important aspects, such as network and resource control and management functionality, service authorization and control, mobility management with efficient traffic routing and delivery, handover, different converged modes are discussed. Finally, conclusions on cooperated converged RAN in Beyond 3G heterogeneous environment are drawn.

Index Terms

Converged RAN, very flat architecture, network and resource control, service authorization, traffic routing and delivery, handover

2.15.1. INTRODUCTION

With the rapid progress of radio technologies, there are a wide variety of commercial and unlicensed wireless and mobile communication systems deployed all around the world. These systems, e.g. Wi-Fi, GPRS, EV-DO, UMTS HSPA/LTE, are distinct in radio access technologies (RAT) and network architectures from each other. As they are originally designed for different markets, business applications and performance requirements, they have no or less capability of interworking/integration with each other at first. However, under the heterogeneous network environment [1], a mobile subscriber with multi-mode or SDR (Soft-defined Radio)

terminal would like to establish/maintain communications with correspondent nodes across several RATs. In particularly, the communications via one or several RATs could occur simultaneously. The existing mobility management and other network control functionalities merely take media-specific information into account, thus cannot deal with the existence of multi-radio access deployment imposed by Beyond 3G systems.

Beyond 3G systems are expected to provide interworking/integration with a wide variety of wireless communication systems, such as the existing 2nd generation and 3rd generation wireless systems, etc. Therefore convergence of multi-radio access technologies and broadcast technologies in heterogeneous environment is one of the important aspects of Beyond 3G systems. The main goal of Beyond 3G systems is to provide personalized, ubiquitous and trustable service access/provision anywhere at any time with any available terminals in heterogeneous environment.

To achieve the aforementioned Beyond 3G goal, some of the following challenges should be considered during the system design, such as dynamic communication adaptive to variety of communication entities, and variety of user requirements; dynamic radio resource management; efficient network discovery/selection/reselection; fast and reliable (re-)establishment of E2E network service connectivity; mobility across heterogeneous systems, including handover initialization, preparation, decision and execution, uniform identifier to upper layer with efficient addressing for underlying specific technologies, and design of advanced mobility protocols; efficient and reliable E2E communications and routing optimizations/traffic delivery, etc.

Although the interworking/integration among Wi-Fi, GPRS and UMTS has been standardized [2], that's still insufficient, as the existing solution cannot satisfy the users' requirement for ubiquitous and seamless service access. In [3]-[8] and [10], the Beyond 3G research activities and 3GPP release 8 standardization are being done to cope with some of these challenges. In [4] and [5], the convergence of different RATs is designed with completely different air interface protocols, i.e. Physical layer, L2 and L3. That means the convergence would occur at network layer. Whereas in [3], the idea is to use a common L2 and L3 protocols for varieties of radio access technologies, such as Code Division Multiple Access (CDMA), Orthogonal Frequency Division Multiple Access (OFDMA), etc. with different configuration to different application scenarios. It is applicable for the design of a total new radio access system. But considering the widely deployment of existing systems, the common L2/L3 idea could only be regarded as a complementary to the convergence at network layer in [4] and [5].

Therefore, convergence of Radio access networks at any layers may be possible according to different application and deployment scenarios. It is important to clearly figure out the concepts, requirements, overall architecture, key components, and the flexible system framework of converged radio access networks (RANs) in Beyond 3G systems. So far, many Beyond 3G researches are on the overall architecture, and individual components. Few concerns the system frameworks and protocol design. In this paper, based on the Beyond 3G concepts and requirements discussed in [11] and [12], we proposes a flexible system framework in heterogeneous radio access network environment, and the base protocol, which are used for the detailed researches on the converged control management functionalities, and to be extended with the progress of the related researches.

The paper is organized as follows. In Section 2.15.2, the converged radio access network concept with the proposed base protocol is introduced. In Section 2.15.3 converged radio access network framework, the key elements, optional elements, and the flexible framework are presented. After that, some of the network operations, such as service authorization and control, mobility management with efficient traffic routing and delivery, handover initialization and preparation considerations are discussed in Section 2.15.4. In Section 2.15.5, the loose, tight, semi-tight converged modes are considered. Finally, some open issues are presented followed by conclusions in Section 2.15.6.

2.15.2. CONVERGED RADIO ACCESS NETWORK CONCEPT

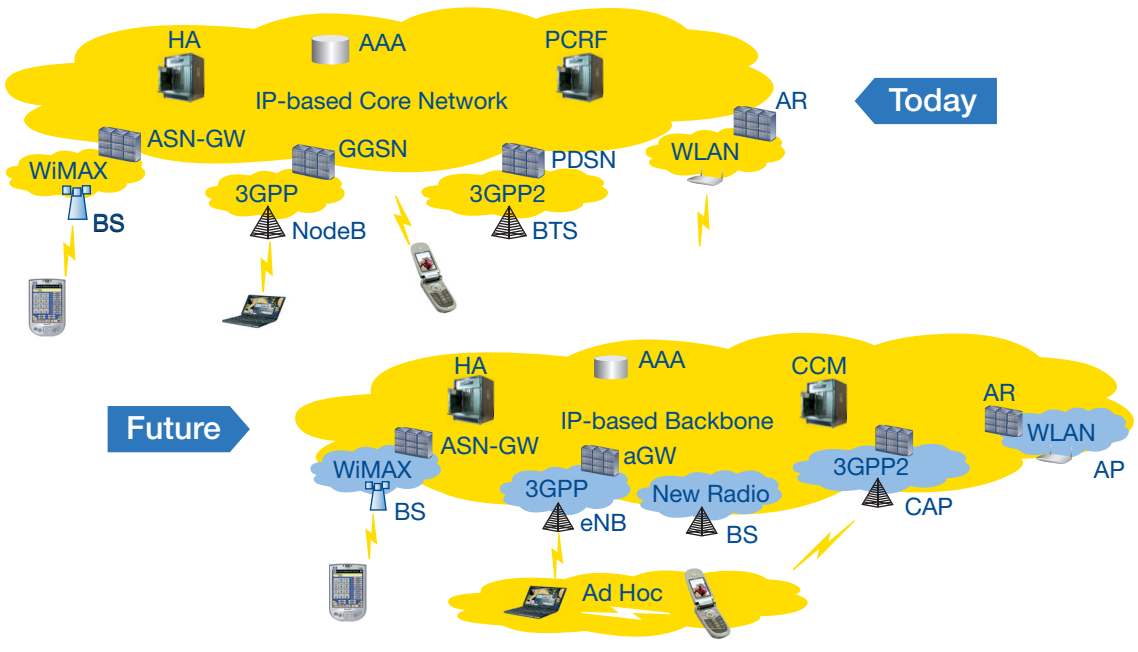
In the Beyond 3G systems, it is anticipated that it will be developed based on all IP networks, i.e. the IP-based networks bearing IP-based service [9], [10]. This requires for the development of a new RAN architecture optimized for IP transport and interoperability with pre-Beyond 3G systems. In addition, the edge of the IP network will get much closer to the terminal as shown in Figure 2.15.1. Although some of the existing wireless access systems are considering the evolution for IP-based RAN and Core network, they cannot provide seamless mobility across different RATs for today's heterogeneous environment shown in Figure 2.15.1. It is foreseen that seamless handover for IP packets across heterogeneous radio access technologies will continue to be a key technology during this rush for all-IP. The trend is to push intelligence to the network boundary without or with less concerning of media-specific transport protocols in RAN and backbone . On the other hand, it should be noted that the even in the all-IP network environment, a smooth migration and convergence of the existing RANs and their evolutions is still needed.

Considering these factors, we propose a converged link layer (CLL), a converged control management above media-specific protocol stacks in this paper.

In user plane, the CLL is to make the IP packets from the external networks more suitable for the transmission on a radio-specific bearer, and vice versa. In addition, the CLL is responsible for the packet delivery to different RATs, and packet diversity by means of transmission of the same packet on different RATs simultaneously or consequently. Also the CLL is in charge of traffic anchoring for the mobility across different RATs.

In control plane, the CCM is responsible for the QoS negotiation and management, cooperative radio resource management, security, policy control and management, mobility management in heterogeneous networks, e.g. among different RANs.

Figure 2.15.1: Trends for All IP Networks



2.15.3. CONVERGED NETWORK FRAMEWORK

2.15.3.1. Key Elements

BS: Base station
- To provide physical and MAC layer functionalities to the terminal;
- To translate IP-based traffic to media-specific packet

AR: Access router
- To act as the first hop for the terminal

RANC: Radio access network controller
- To provide RAT-specific L3 functions, e.g. RRC, intra-RAT RRM, intra-RAT Mobility management, etc.

AAA: Authentication, authorization, and accounting

CCM: Converged control management

GMA: Global mobility anchor
-To provide global seamless mobility across different RATs

2.15.3.2. Optional Elements

LMA: Local mobility anchor
- To provide seamless mobility across local RATs without the involvement of GMA within a limited region

2.15.3.3. Framework

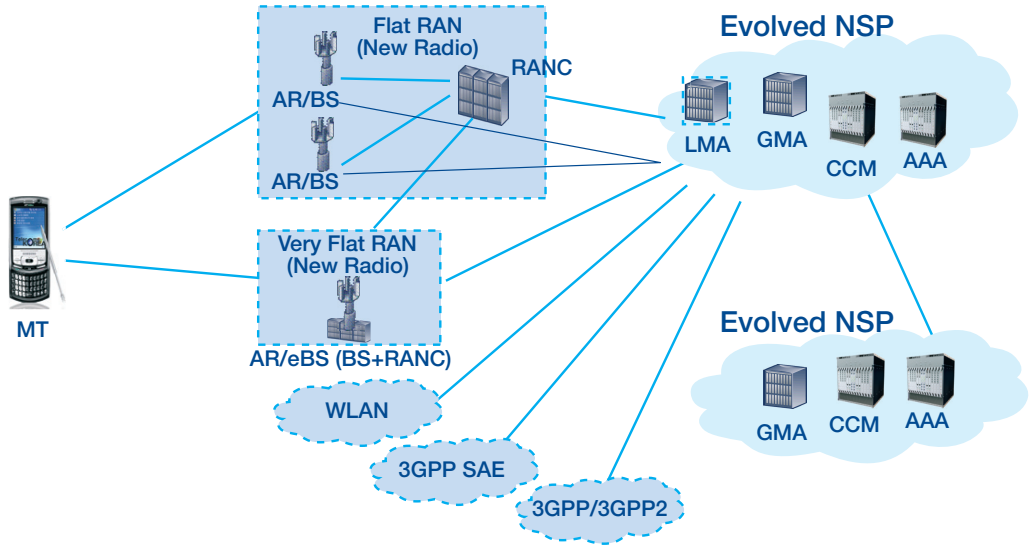
The basic framework is shown in Figure 2.15.2 where four different networks with different radio access technologies are interconnected. In general, in a loose converged environment, each network would have the following types of network functionality entities: BS, AR, RANC, AAA server, GMA. Some of them may be collocated in one physical network elements. They are linked via internet. Information exchange between different RATs is limited to user profile, authentication credentials, and accounting information, or even less. The AR and GMA support handover in a homogeneous network, and the GMA supports handover across heterogeneous networks, e.g. in 3GPP I-WLAN. One should note that these equivalent functionality entities in different systems may be different. For instance, in WiMAX, the ASN-GW (Access service network - gateway) plays the roles of AR and RANC, the HA in the CSN (Connectivity service network) acts as the GMA. Whereas in 3GPP, the SGSN and RNC act as the RANC, the GGSN acts as AR, etc.

Although the GMA could provide potential of global seamless mobility in user plane, there exist diverse media-specific network control and management functionalities to different RATs in control plane, such as mobility management and radio resource management, security management, QoS mapping, etc. Moreover the required context for different RATs may be different and not all the RATs are willing to share their context. Therefore, a CCM function entity is introduced to coordinate all involved RATs.

Whenever a mobile terminal is powered on, it looks for available networks and negotiates capabilities with candidate networks. With the help of CCM, it could find the most preferred network and attached to it.

In the following authentication procedure, the context associated with the terminal and subscribed services, which defines different parameters like QoS, user profile and filtering rules etc. Then the mobile terminal would be provided with parameters needed for their subscribed default services, so that the user would access services as soon as possible whenever he requires.

Figure 2.15.2: Framework of converged RAN



With sufficient context, the CCM would be in charge of transmission required context to a specific RAT whenever handover occurs. Therefore it is not required for the user profile acquisition, re-authentication with AAA server in home network or visited network. The user experience is improved by reducing the handover latency in control plane.

In user plane, usually the mobile terminal communicates with the correspondent node along the path of BS, AR, LMA and GMA, and visa versa. When the mobile terminal moves across different RATs, the elements along the path may be involved. Along the new path, some elements may be different from those along the old path prior to the handover, whereas some are the same. More efficient mobility management should be studied to increase the user experiences by means of reducing the signaling overhead and the connectivity re-establishment latency.

2.15.4. CONVERGED NETWORK OPERATION

2.15.4.1. Converged Control Management Overview

CCM is responsible for the QoS negotiation with different RATs and core networks, QoS mapping on specific RAT. It is also in charge of the cooperative radio resource management for load sharing, and admission control purposes, etc. In the following, some other important CCM functionalities, such as service authorization and control, mobility management in heterogeneous networks with efficient traffic delivery, and network entry and handover initialization, preparation and execution schemes are discussed in detail.

2.15.4.2. Service Authorization and Control

It requires for the network to provide users with services as fast as possible. Therefore, we should try to reduce the service setup duration. It is reasonable to deliver the parameters for default services to the service client (usually the mobile terminal) and some other involved network elements. Also it is anticipated that the service authorization and control for dynamic services should be pushed to the network boundaries, in order to reduce the signaling and traffic transmission delay.

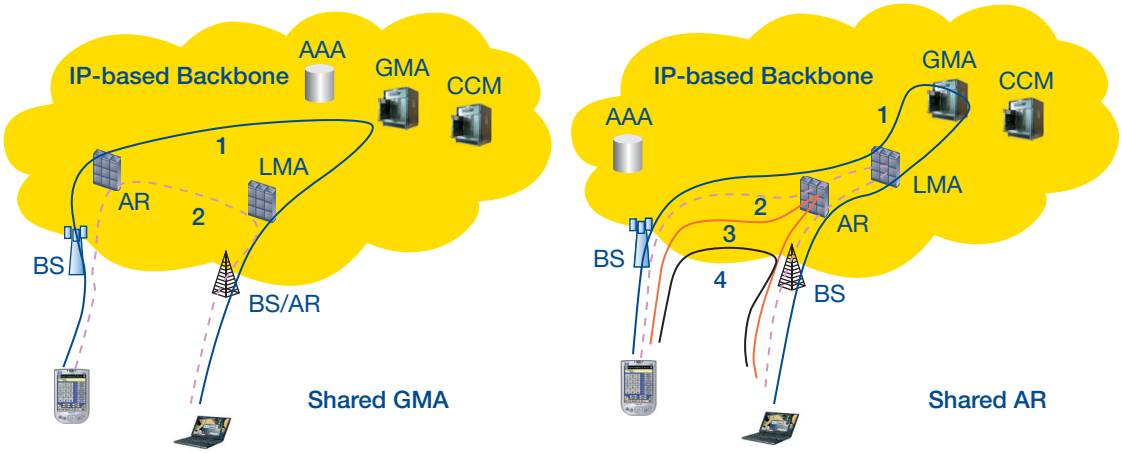
Therefore, a generic service authorization architecture is required. In the architecture, AAA may take roles of service authorization, and authorized states/information relay/forwarding; AAA or CCM may act as the configuration agent taking roles of service configuration to the service deliverer (e.g. AR, LMA, GMA, etc.); the service deliverer is responsible for the service provision and supervision. It is FFS to map these functionalities to the network elements in real wireless systems according to different services.

2.15.4.3. Enhanced Mobility Management with Efficient Traffic Routing and Delivery

Micro and macro mobility has been widely studied in [13], [14] and [15] in IETF, known as Mobile IP, Network-based local mobility management (NETLMM) and Hierarchical Mobile IP (HMIP), respectively. As shown in Figure 2.15.3, with the deployment of all or some of the above protocols on local and global mobility anchors, optimized mobility management could be achieved with reduced handover delay and data loss.

In addition, in Beyond 3G systems the user is expected to access services or be provisioned with services with lower E2E transmission delay. An efficient traffic routing and delivery scheme is required. Route optimization [13] in mobile IP could provide efficient traffic delivery by enabling direct IP communication between the mobile node and the correspondent node without the indirect routing via home agent. However, this is not sufficient as this still introduce more transmission delay in case the communication peers are under the control of the same LMA or AR. More efficient communication could be achieved as shown in Figure 2.15.3. Moreover, such premier services should be coordinated by the mobility management function entity and service authorization function entities.

Figure 2.15.3: Efficient Traffic Delivery



2.15.4.4. Network Discovery, Capability Negotiation, Network Selection/Re-selection Considerations

As we know, existing radio access networks offer a wide variety of services according to different user cases and requirements. For instance, WLAN could offer high data rate services but limited coverage area. Whereas cellular networks, such as UMTS, could provide voice and data services at a relatively low rate but higher coverage. With all the above options available, the users can choose the network to suit their specific requirements and need. They also may be overlapped in specific geography regions to satisfy different user requirements in the regions. For the user to take full advantage of seamless connectivity without disruption of service, an

efficient network discovery with less power consumption, network capability negotiation, network selection and handover decision mechanism becomes vital. To make full use of the critical radio resource, it is expected that soft handover or diversity could be avoided even though sometimes they could provide better QoS. Therefore, efficient radio resource management architecture and algorisms, and a media-independent handover mechanism are required to provide personalized ubiquitous seamless mobility services.

2.15.5. DISCUSSIONS ON OPEN ISSUES

There still some open issues to be studies, such as centralized network control vs. distributed network control, smart terminal vs. smart network; selection of user plane anchor point, support of multicast and broadcast service, etc.

As one of the most important functionalities of network control, joint radio resource management is proposed in centralized management mode in [6], [7], and a distributed management mode is proposed in [8]. As stated in [8], the drawbacks of centralized processing in multiple radio access technologies environment are mainly from the following three aspects: first, in case the RATs are owned by different providers, they would like to hide their network topologies, and they are unwilling to share the radio information. Secondly, it cannot deal with the scalability problems. The last one is the robustness problem and the computation complexity. Actually, it is not the drawbacks of the centralized joint RRM, but also of the centralized network control functionalities. In that paper, the authors highlighted that the distributed RRM, or say network control, could provide either cooperation but also competition among different RATs. The paper proposed a novel distributed intelligent Multi-Agent System (MAS), which is self-organized to solve the coexistence of multi RATs operated by different network providers. It aims to decrease the burden of heterogeneous networks with the introduction of the agent performs a macro control and management function by using control factors and validation mechanism instead of micro control handling detailed RRM decisions concerning individual users. But this architecture introduces the performance degradation due to the factor that not all information could the available for efficient radio resource management. Therefore, the location of CCM functionalities should be considered: is it collected in one network element or distributed among different RANs to make full use of distributed computation and network control?

In Internet industry, the terminal is always assumed smart, that the terminal is mainly responsible for network discovery, selection, access/service control and configuration, etc. Whereas, in telecommunication industrial, it is expected that the network should be a manageable, all service access/provision should be supervised by the network. Moreover, we should consider the support of power and memory limited terminals. As a tradeoff, the functionalities of CCM should be split and allocated to the terminal and network sides, respectively. In addition, the support of ad-hoc network should also be considered, in this case, how to keep the network manageable, and move some of the burden on the network to the terminal is still open.

2.15.6. CONCLUSION

In this paper, we present a base converged RAN framework and protocol stacks which are flexible for different scenarios. By introduction of a CCM in control plane, and a CLL in user plane, seamless mobility across different RATs could be achieved. Some important functionalities and converged RAN operations are discussed followed by open issues which are to be further studied.

2.15.7. ACKNOWLEDGMENTS

The work presented is partly supported by EU FP6 IST project ENABLE -Enabling Efficient and Operational Mobility in Large Scale Heterogeneous IPv6 Networks [16].

2.15.8. REFERENCES

[1] X. Yang, J. Bigham, L. Cuthbert, "Resource management for service providers in heterogeneous wireless networks", Proc. IEEE Wireless Communications and Networking Conference, Vol. 3, pp. 1305-1310, March 2005.

[2] 3GPP TR 23.234 v7.2.0, Technical Specification Group Service and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 7), June 2006.

[3] M.-H. Fong, T. A. Gulliver, and V. K. Bhargava, "Multi-mode Access System with Anchor Layer 2/3 Protocol for Beyond 3G Wireless Networks," Proc. IEEE VTC, Spring, 2006."

[4] C. Politis, T. Oda, S. Dixit, A. Schieder, H.-Y. Lach, M. I. Smirnov, S. Uskela, R. Tafazolli, 'Cooperative networks for the future wireless world,' IEEE Comm. Magazine, Vol. 42, Issue 9, pp.70-79, Sept. 2004.

[5] J. McNair, F. Zhu, 'Vertical handoffs in fourth-generation multinetwork environments', IEEE Wireless Comm., Vol. 11, Issue 3, pp 8-15, June 2004.

[6] J. Luo, R. Mukerjee, M. Dillinger, et al., "Investigation of radio resource scheduling in WLANs coupled with 3G cellular network," IEEE Communications Magazine, vol. 41 pp. 108-115, 2003.

[7] J. Luo, E. Mohyeldin, M. Dillinger, P. Demestichas, Kostas Tsagkaris, G. Dimitrakopoulos, and E. Schulz, "Performance Analysis of Joint Radio Resource Management for Reconfigurable Terminals with Multiclass Circuit-switched Services," WWRF 12th Meeting, WG6, Toronto, Canada, Nov., 2004.

[8] Z. Y. Feng, P. Zhang, "Cooperation Techniques and Architecture for Multi-access Radio Resource Management," Proc. IEEE VTC, Spring, 2006.

[9] 3GPP TR 23.882 v1.3.0, Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution: Report on Technical Options and Conclusions (Release 7), July 2006.

[10] 3GPP TS 22.258, Technical Specification Group Service and System Aspects; Service Requirements for the All-IP Networks (AIPN) (Release 8), Mar. 2006.

[11] Ambient Networks, http://www.ambient-networks.org/

[12] Yan Peng, Guardini Ivano, Meng Liang, Bin Xia, "Views on wireless network convergence," Proceeding of WWRF#16, April 2006

[13] Shoaib Khan, Sahibzada Ali Mahmud, Shahbaz Khan, Wenbing Yao, and Franjo Cecelja, "Generalized architecture for converged heterogeneous networks," Proceeding of WWRF#16, April 2006

[14] IETF NETLMM WG

[15] IETF MIPSHOP WG

[16] EU FP6 IST ENABLE, http://www.ist-enable.org/

2.16 IP Based Network Convergence

Yan PENG, Bin XIA, Meng LIANG, **Huawei Technologies**

Guardini Ivano, **Telecom Italia**

ABSTRACT

Currently, a variety of networks providing different services and different levels of QoS are flourishing in markets. While the user demands for enjoying multiple services anywhere and anytime have emerged and been increasing. In order to satisfy the growing user needs in a flexible and non-intrusive manner, future wireless communication networks would provide higher capacity, maximized coverage, more efficient resource usage, and richer and higher quality user experience. All these characteristics drive the various networks to converge. By analyzing of the convergence in the two dimensions (i.e. layer and degree), the possibility of network convergence on IP transport and control layer is highlighted. Some issues on IP based convergence are taken into consideration and explained in details as well. Also we propose a feasible evolution strategy of the IP based convergence in this paper.

Index Terms

Convergence, IP-based transport and control layer, evolution strategy

2.16.1. INTRODUCTION

During the past few years, the communication networks have grown tremendously. More and more technologies have been developed to provide higher transmission speed, larger coverage area, and better performance etc. Yet the user requirements have been evolving at a higher speed all along. Users would like to enjoy satisfying services "anywhere" and "anytime". This leads to the conclusion that the provision of "seamless" and "ubiquitous" services will become prominent within future mobile services. Moreover, the future wireless world communication should be user centric.

Additionally, the rapid diffusion of portable terminals, such as laptops, PDAs and smart phones, is generating an increasing demand for a "global" mobility service. Users are desiring to be always connected and looking for a wider variety of voice, data and multimedia services independently of their geographical location, with performance significantly better than today (higher bit-rate, less delays, etc.). [1]

Today there are many heterogeneous communication technologies that differ in their support of data rates, mobility, coverage, quality of service, and possible business models. Will there be a universal technology, replacing all current technologies in order to satisfy all the user requirements in any scenario in the future? Considering the diversity of user requirements and nature, additional technologies with other characteristics are expected to support new challenging networking scenarios or be suitable to solve the current problems, while not likely to replace the existing technologies.

The convergence of different access technologies would potentially yield significant gains for both providers and end-users of wireless networks. Improvements in total effective capacity, total coverage, radio resource usage efficiency, robustness, mobility support, service availability, flexibility in deployment alternatives, and cost are some examples. Perhaps convergence is the future evolutionary trend.

Research on convergence has been carried out in a number of research projects previously. [2] The convergence steps of integrating heterogeneous radio access technologies into one core network environment also have been taken into consideration by standardization bodies and commercial operators. [3, 4]

This paper considers two dimensions of convergence, namely, the layer and the degree of convergence. After comparison of different options, we focus on the converged networks on the IP based transport and control layer. Then around this choice, relative issues considered are discussed. At last a possible evolution strategy is proposed to accomplish this kind of convergence.

2.16.2. MOTIVATIONS FOR WIRELESS NETWORK CONVERGENCE

In order to understand the benefits of the wireless network convergence more clearly, one means is to identify some important motivations from different points of view: [2]

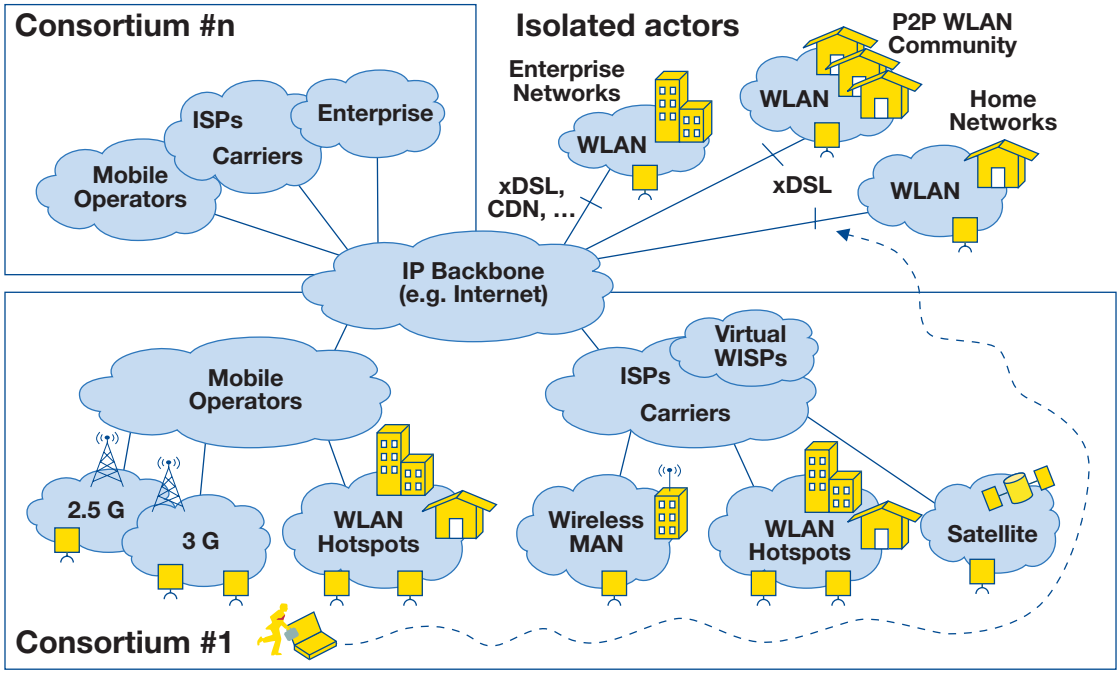
- User perspective: the user expect much of the flexibility to choose among available accesses and services according to his own needs (always the most satisfying connection) and the freedom to access "any" network without subscription to each network operator. Related to this are also mobility aspects with reliable, ubiquitous and continuous services during user movement.
- Network provider perspective: convergence which improves the network availability, reliability and capacity will result in better service and access offers for the end-users. Other drivers are the increased customer number and reduced cost for the deployment of such infrastructure and services. Finally, the demand for simple and efficient means for migration and introduction of new access technologies —with the least impact to existing network— ïs another important motivation, especially while considering the increased multitude of access technologies entering the market.
- Regulator/government perspective: Increased competition in the market for mobile services is an important benefit which network convergence will bring, e.g.,1) Lowered barriers for new players to enter the market (increased competition), 2) Increased and wider range of co-operation between providers and 3) New market rules, e.g., agreement broker between providers. More efficient utilization of spectrum is another motivation from a regulator perspective.

2.16.2.1. A few application scenarios

In this section, scenarios, which illustrate how we consider wireless network convergence can be used in future, are depicted.

The first one is about a business user moving in the wireless world. This scenario envisages a future converged wireless network, which enables secure seamless end-to-end media delivery automatically adapted to the dynamically varying conditions of the user's surroundings. As this scenario shown in figure 2.16.1, all the access technologies, such as WLAN, cellular network and satellite, work in tight harmony and cooperation to enable an enhanced user experience, especially in the overlapped area. [1]

Figure 2.16.1: User moving in wireless world



Secondly, the key problem addressed in the "Moving networks" scenario is seamless mobility of a personal/office area network. For instance, some travelers in a vehicle communicate with each other using WLAN, such as scenario in train or airplane. And the hotspot connects to Internet through a gateway and an antenna just like the left picture in the figure 2.16.2. [1] A more common scenario from technical viewpoint is that all users reside in the same network domain, e.g. ad-hoc network, but perhaps they are connected to different networks via different wireless interfaces with different requirements and QoS at the same time, based on different profiles as the right picture shown in figure 2.16.2.

Last but not least, the third scenario highlights the ability of future converged network to support virtual moving network, such as PN (Personal Network). The Personal Network (PN) consists of more than one device (terminal or server perhaps provided by different operators) under the control of one user. Although these terminals may connect to different networks via different wireless interfaces, there are connections among all of them so that the user is provided with a virtual secure network and perceives a continuous connection regardless of their relative locations and movements, as shown in figure 2.16.3.

Figure 2.16.2: Moving networks

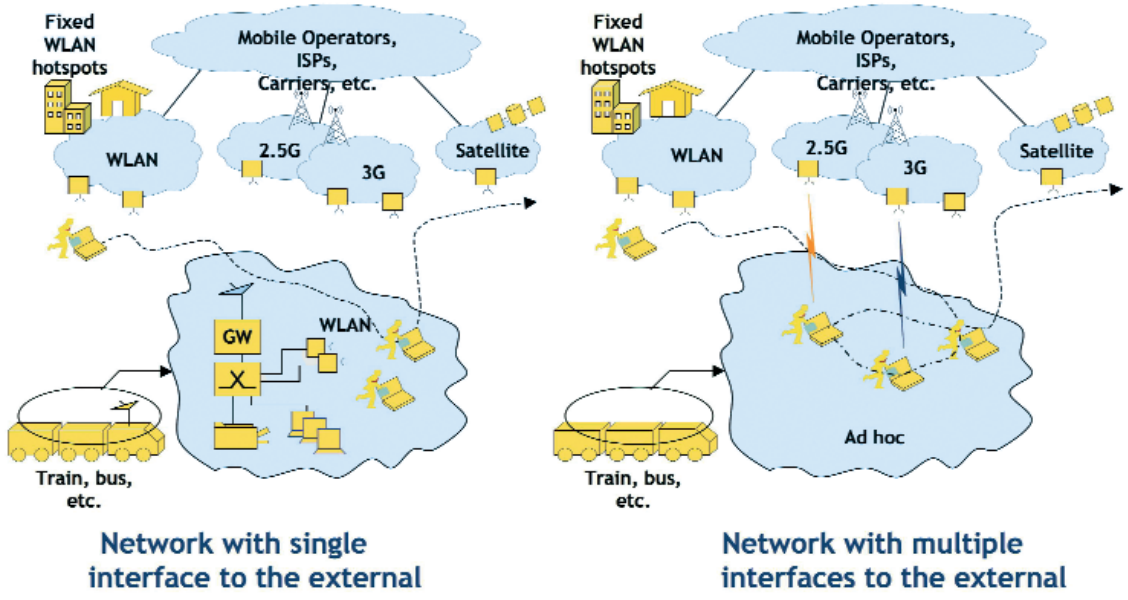
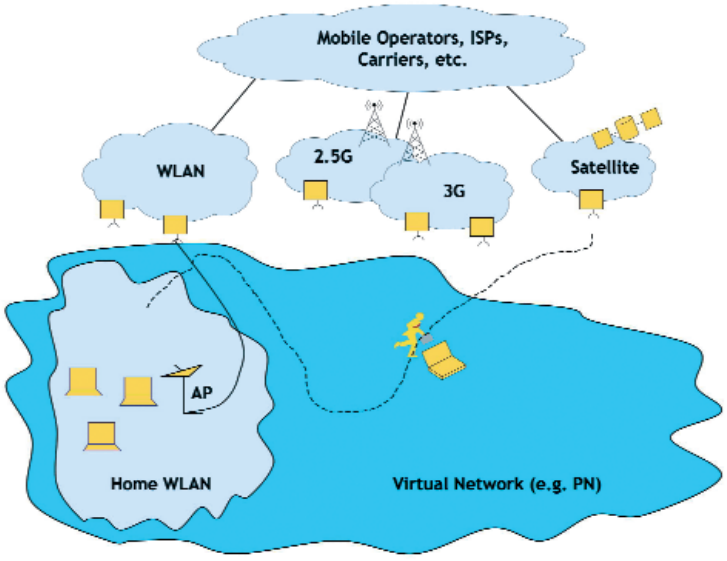


Figure 2.16.3: Virtual moving networks



2.16.2.2. Challenges and requirements

In these scenarios many features are described which are not easy or totally impossible to implement with today's technology. Some key challenges that cannot be solved with today's technology are:

- Heterogeneous network supporting. The co-existence of many technologies and network types becomes more and more complex and would require detailed study both from the potential user on how to use and access and from the operator on how to implement more efficient usage with cost reduction. Nearly all of them existing today are more or less isolated from each other. Supporting multiple access technologies and multiple administration domains is the main challenge of convergence. [5]
- Multiple service supporting. Different services have different tolerance for delay and data loss. Currently, certain technology has more advantages than the others for certain service, e.g. WLAN for file transfer and cellular network for voice conversation. Supporting multiple services with corresponding satisfying QoS according to the service feature is another main challenge.
- Seamless mobility. Mobility could be achieved up to a certain level with the current state-of-the-art standards. Nevertheless, Seamless mobility still seems to be an attractive future vision which would intensify user satisfaction and hide technology details from humans. [6]
- Ubiquitous services. It can be foreseen that in the future there will be a ubiquitous mobile communication environment in which a legal user can access all the service anywhere and anytime, no matter whether static or moving.
- Efficient traffic delivery. It's especially useful for multicasting or broadcasting multimedia service.

Analyzing high level technique requirements for wireless world convergence might help offering methods to cope with the above issues in the future. [1]

- Convergence rather than innovation. There should be minimum impact on consolidated standards already widely deployed in the network.
- High reliability. There should not be any "single-point-of-failure".
- High scalability. The system should be able to support a very high (and fast growing) number of users.
- Optimized usage of network resources. The system should minimize the overhead of both signaling (especially on the radio access) and data packets
- Minimization of e2e transfer delay for data packets. It's useful for supporting real-time interactive applications like audio and video conference.
- Optimized support for always-on operation. The system should minimize the connection set-up delay (i.e. the latency before the terminal is able to transmit or receive IP packets).

More detailed issues about technique requirements will be discussed in the latter section.

2.16.3. MOTIVATIONS FOR WIRELESS NETWORK CONVERGENCE

Convergence has a very broad scope. Research about convergence has been conducted in some projects, and convergence of digital industries has already been underway. However, it should be noted that the term "convergence" has much broader meaning with different perspectives within the various industries, and there is no single agreed-upon definition currently. Generally speaking, it includes the follows: [7]

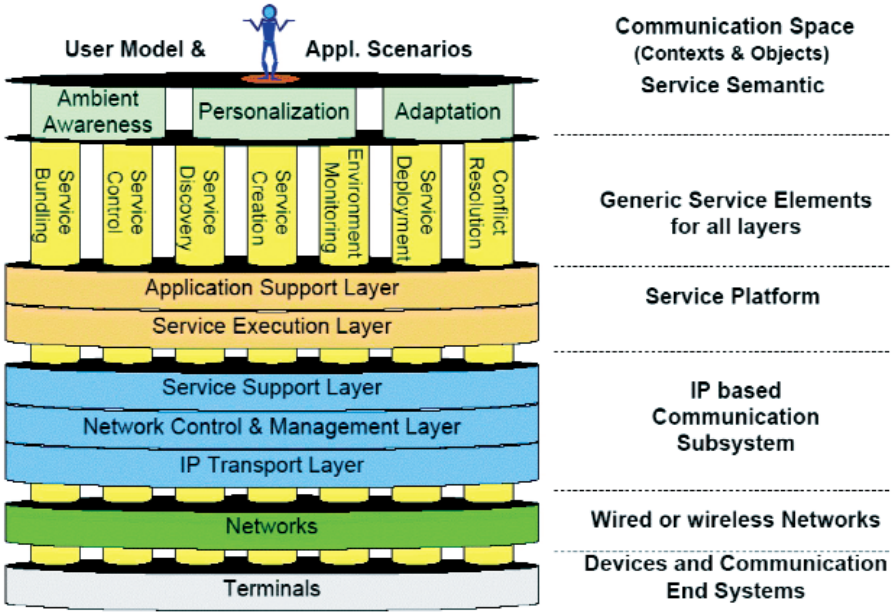
- User centric with uniform user experience

- Open and spam-free internet
- IP-based architecture in all domains
- Commercial and technical interoperability
- Open standardized interfaces
- Common platforms for software and services

But how convergence can be implemented is still under discussion. Multi-dimension convergence categories have been proposed. One study on the convergence architecture may be sliced according to the convergence on different layers, as shown in figure 2.16.4, which will be discussed in detail later. [8]

- Converged Applications
- Converged Services
- Converged Service Platform (API)
- Converged Networks
- Converged Spectrum

Figure 2.16.4: Layered convergence concept



In addition, the following issues about convergence have also been considered.

- Converged Devices
- Converged Infrastructure

Usually we pay much attention to the layered convergence, for the sake of minimum impact on consolidated standards, smooth migration roadmap and high extensibility. A further design choice is on which layer the convergence should occur.

From figure 2.16.4 it can be seen that different levels of convergence have been defined. Usually different pairs of networks may converge at different layers. The layer of convergence is motivated by design trade-offs. A major factor in determining the convergence layer is the possible time scale of operation. The lower layer where the convergence happens, the finer the time scale of operation can be. On the other hand, each kind of access technology has its own advantage and application scope, so it's not proper to converge on link layer, even if without considering the convergence cost. So convergence on IP transport layer is a good choice.

The other dimension, i.e. convergence degree may also be interesting. Will the future network be one single fully converged wireless world? Many factors affect convergence degree, such as operator's agreements, capabilities of infrastructure and terminals, etc. It's more possible that different degrees of convergence will co-exist, from loose convergence to tight convergence. They are: [4]

- Common billing and customer care
- Common access control and charging
- Services sharing
- Service continuity
- Seamless services

From our point of view, all the options or combinations are possible and worth studying, and we focus on converged networks on IP based transport and control layer at the first stage.

2.16.4. ISSUES ON IP BASED CONVERGENCE

As discussed in the previous section, convergence on IP transport layer is a good choice in theory. The concept "IP based Convergence" does not just refer to the transport protocol used within the converged network. Actually it refers to the general concept of a network based on IP and the associated technologies which provide an enhanced, integrated service set independent of the access method used. It will enable access systems and services converge into a common network. Actually, many systems set IP-based network as the future evolution object.

About IP based convergence, some issues should be considered and designed carefully.

- IP-based network control

There should be a general network control mechanism across different domains, including generic control signaling interface, conveyed on IP layer or above, and access technology agnostic. And an efficient control message transfer mechanism should be defined with minimization of signaling round trips and other overheads.

- IP-based transport

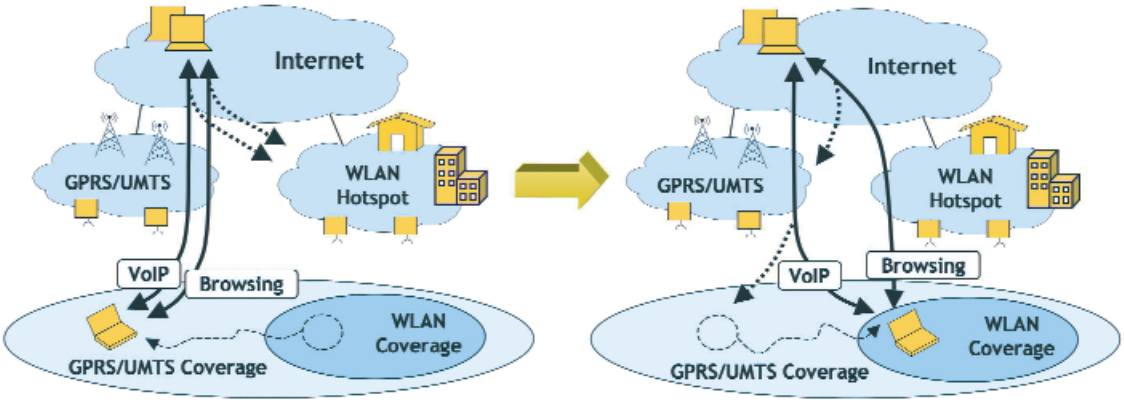
The convergence should support efficient and transparent transport traffic, across different IP versions (IPv4, IPv6, IPv4 with NAT), and across different access technologies, without users' intervention.

- IP-based routing and addressing

Conventional numbering mode, such as E.164 in the legacy telephone field will not be appropriate in converged network. The new system should be able to accommodate such a vast (and fast growing) number of users and terminals, that implementing IP addressing over heterogeneous networks is mandatory.

Optimized routing for specified service and network is another portion of this issue. The following figure 2.16.5 shows an example of optimized routing. [1] Considering a terminal with GPRS and WLAN interfaces, it was originally located in the UTMS coverage, with both of its VoIP and browsing service routed through GPRS/UTMS network. As user steps into an overlapped WLAN hotspot, the routing optimization may take place, i.e. the VoIP via GPRS/UTMS and browsing via WLAN

Figure 2.16.5: Optimized routing example



Communication Quality

Mobility should be supported based on application requirements, such as fast handoff for VoIP, lossless handoff for browsing, and seamless handoff for real-time reliable applications. The communication quality should also be flexible in offering specific QoS according to different conditions (e.g. user profile, network loading, and resource usage)

Support of IP services

The IP based converged network should have the ability to effectively handle a variety of different types of IP traffic: real-time or non-real-time, mission critical or reliable, end-to-end, end-to-multicast or multicast-to-multicast. Service based access selection should be necessary especially for efficient usage of radio resource.

Security and Privacy

Compared with traditional telecom network, IP network is vulnerable for its openness. So the enhanced security and privacy is needed to conduct IP based convergence. Different policies of different network and operators should cooperate harmoniously to keep security and privacy.

Deployment

The convergence process should be smooth enough to be backwards compatible with legacy system, and easily deployed.

2.16.5. A POSSIBLE EVOLUTION STRATEGY

The complete convergence of different networks will take a long time, potentially years. This is partly due to the difficulty in technology and business consideration. So a feasible evolution strategy is needed.

According to investigation of the previous network evolution, we believe that some themes will help a network to evolve friendly. [2]

First, business motivations are important aspects of evolution. If a technology and its infrastructure are already established on the market, it will be difficult to introduce a totally new kind of infrastructure or architecture (even if it is standardized). Because the network provider wants to protect its established investment, and the user often won't change his preference easily. Thus the evolution should be smooth enough to meet and influence the requirements of operators and users.

Second, the evolution should be carefully planned in order to minimize the number of components or component types, which shall be updated in each step. The scope of the changes required should also be restricted. For example, evolution is harder to achieve if it requires both the users and the operators to upgrade at the same time or if changes are required by different operators. An important step is to identify suitable independent functionalities, since this allows a particular functionality to be upgraded or replaced simply and easily. A stand-alone improvement can then be made, which is easier for users to understand and easier for operators to roll-out.

Last, well-defined interfaces between layers help evolution. Because the layers can evolve independently (there are further advantages). This allows the technologies associated with different layers to evolve at different speeds (e.g. typically applications evolve faster than bit transport technologies). Also different solutions can be deployed according to the changing circumstances around the user or operator. An excellent example is IP technology. One of the key reasons for its success are its clear, simple inter-layer interfaces, which have allowed service providers to innovate quickly to meet user requirements quickly (software developers can use the same sockets interface for the new services), and new lower layer transport technologies to be deployed gradually in a backward compatible manner.

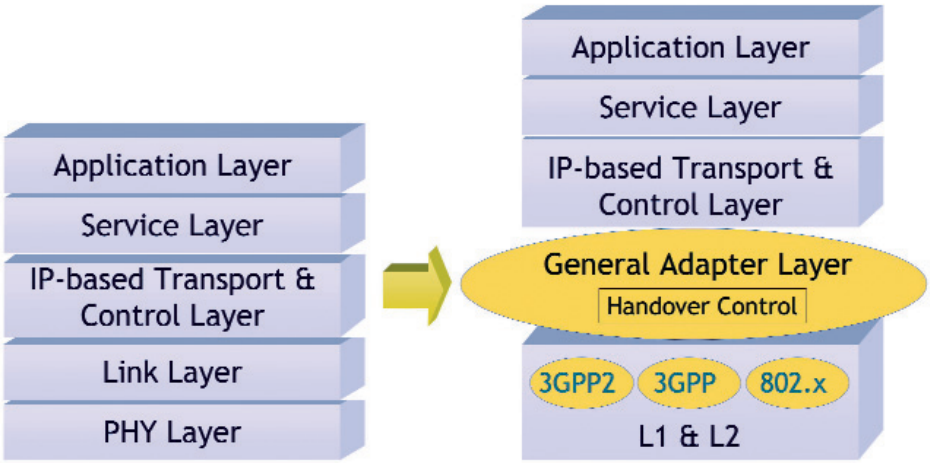
From this perspective, we can identify three phases of the evolution path towards the future converged environment. The three phases are:

1. With mobile terminal evolution, more and more terminals with multiple network interfaces appear.
As mentioned above, now that we could not unify all wireless technologies into one, it will be possible to combine them into a single terminal. For ubiquitous service, the mobile node is capable of supporting multiple interfaces at the same time. In this way, it will be possible to guarantee the maximum service availability at lower costs, and with better performance, in respect to the realization of a global mobility with a single mobile terminal. In fact, lots of multi-mode terminals have been widely used at present.

2. Implementation of an adaptation layer supports part of transport layer convergence functions, such as handover with session continuity, without affecting existing legacy networks.
As shown in figure 2.16.6, the legacy network is included via the General Adapter Layer (GAL). Between the IP-based Transport & Control Layer and lower L1 & L2 is the "vertical" interface - GAL, which aims at providing a unified interface to higher layers and facilitates efficient link layer inter-working among multiple, possibly diverse, radio accesses. The GAL is an optional abstraction layer, which may solve part of the problem, such as session continuity. Some projects (e.g. IST projects-BRAIN and MIND) and standardization bodies (e.g. IEEE802.21) have conducted much research on the “layer 2.5”. The former has proposed “IP2W” which

focuses on control functions like QoS and mobility management as well as data transport functions. The latter has proposed "MIH" which pays much attention to seamless handover.

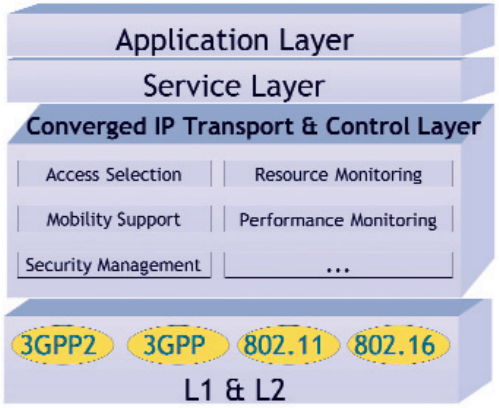
Figure 2.16.6: Evolution strategy - step2



3. Add convergence functionality to the adaptation layer, and make it mandatory to implement convergence on IP transport and control layer.

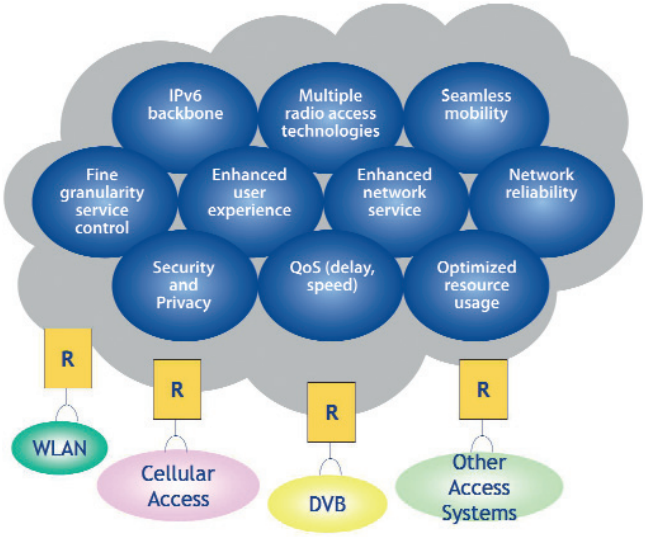
In this phase, more and more convergence functionalities being added to the adaptation layer, a fully converged IP Transport and Control Layer comes true at last (figure 2.16.7). The GAL is converged into the transport and control layer instead of acting as an independent "Layer 2.5". The new converged layer fulfils two main characteristics: on one hand, it simultaneously controls different radio interfaces over which it is configured and shields the difference between various access technologies. On the other hand, it exposes a single uniform IP interface, with a unique IP address to the upper layers. The intelligence added by convergence brings the possibility of utilizing all the available resources simultaneously (independent of wireless channels).

Figure 2.16.7: Evolution strategy - step3



But there is still a long way to go before getting to fully converged networks on IP-based communication subsystem Layer. A possible converged network example is given in figure 2.16.8.

Figure 2.16.8: A converged network example



The evolution process should be flexible enough to adapt to the needs of operator and market. Again, evolution should be business-driven other than technological-oriented. There should be a clear demand of an operator to add certain convergence functionality to his system.

2.16.6. CONCLUSION

In this paper, our aim is to sharpen the vision of "Network Convergence". At first the motivations for wireless network convergence were analyzed from different points of view, then some scenarios were depicted, which illustrated how we propose wireless network convergence might be used in future. From different convergence dimensions, the possibility of network convergence on IP transport and control layer was chosen and highlighted. Then some issues on IP based convergence were considered. At last, a possible evolution strategy was also proposed.

2.16.7. REFERENCES

[1] IST Project ENABLE, http://www.ist-enable.org/

[2] IST Project Ambient Networks, http://www.ambientnetworks.org/

[3] 3GPP TS 22.258 V7.0.0: "Service Requirements for the All-IP Network (AIPN)".

[4] 3GPP TR 22.934 v6.2.0: “Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) Interworking”.

[5] 3GPP TR 22.978 v7.1.0: “All-IP Network (AIPN) feasibility study”.

[6] IEEE 802.21, http://www.ieee802.org/21/

[7] Andy Jeffries, SIG4 Convergence of Digital Industries Inaugural Meeting, WWRF15#, 2005

[8] Mikko A. Uusitalo, The wireless world research forum - global visions of a wireless world, WWRF15#, 2005

2.17 Mobility through Heterogeneous Networks in a 4G Environment

S. Sargento, **Instituto de Telecomunicações, Aveiro**
T. Melia, **NEC Europe Ltd, Network Laboratories**
A. Banchs, I. Soto, **Universidad Carlos III Madrid**
J. Moedeker, **Fraunhofer FOKUS**
L. Marchetti, **Telecom Italia Lab**

ABSTRACT

The increased requirement of ubiquitous access for users to the requested services points towards the required integration of heterogeneous networks. Ideally, a user shall be able to access required services through different access technologies, such as WLAN, Wimax, UMTS and DVB technologies, from different network operators, and to seamlessly move between different networks with active communications sessions.

In this paper we propose a mobility architecture capable of supporting a user's ubiquitous access and seamless movement, while simultaneously bringing increased flexibility for operators of access network.

Index Terms

Broadcast, heterogeneous, local and global domains, mobility, multihoming, pervasiveness, QoS.

2.17.1. INTRODUCTION

Daidalos II [1] is an EU IST research project that is working to define and validate the network architecture of future mobile operators. A key requirement for these networks is the support of ubiquitous access. With the current evolution of technologies we envision that, to provide this ubiquitous access, users will access networks through a variety of technologies such as WLAN, WiMax, UMTS, and DVB, depending on the situation, traffic requirements, and classes of networks, be they mobile ad-hoc or moving networks.

Daidalos II is defining a network architecture to provide ubiquitous access among heterogeneous access networks. The architecture will also support the following features:

- Mobility management is split between local and global domains. As such, access network operators will have the flexibility to choose the mobility management scheme inside their networks, including layer 2, layer 3 or legacy mobile technologies.
- Daidalos II supports handovers with Quality of Service (QoS) through a common framework for mobility and QoS signalling in heterogeneous technology networks. This common framework is based on the IEEE 802.21 draft standard [2].
- It supports host multihoming - the host is equipped with multiple physical network interfaces, capable of operating concurrently.
- It explores an identity-based mobility management solution through the independent and general management of identities - an enhancement of traditional network mobility protocols with a view towards a solution for identity mobility.
- It integrates Mobile Ad-hoc Networks (MANETs) and mobile networks (NEMO) into the mobility architecture. This will allow a terminal to roam, not only among infrastructure access networks, but also through NEMOs or MANETs, keeping all the properties of the Daidalos II architecture in QoS support and security.
- Daidalos II integrates broadcast networks, with consideration for unidirectional networks without a return channel. It also supports QoS in multicast services running through broadcast networks.
- It integrates ubiquity and pervasiveness concepts for customized services to the users.

This paper presents a network architecture able to support the aforementioned functionalities. We briefly describe the challenges and the directions in order to specify the pervasive mobility architecture, supporting heterogeneous technologies (including unidirectional broadcast, local and global mobility concept, and different types of networks). We also address the challenges of the proposed architecture when considering host multihoming, virtual identities and integrated QoS support.

The following section describes how each of the mentioned features is addressed in the Daidalos II architecture. Finally, we present the most relevant conclusions in section 2.17.3, section 2.17.4 and section 2.17.5.

2.17.2. DAIDALOS II ARCHITECTURE

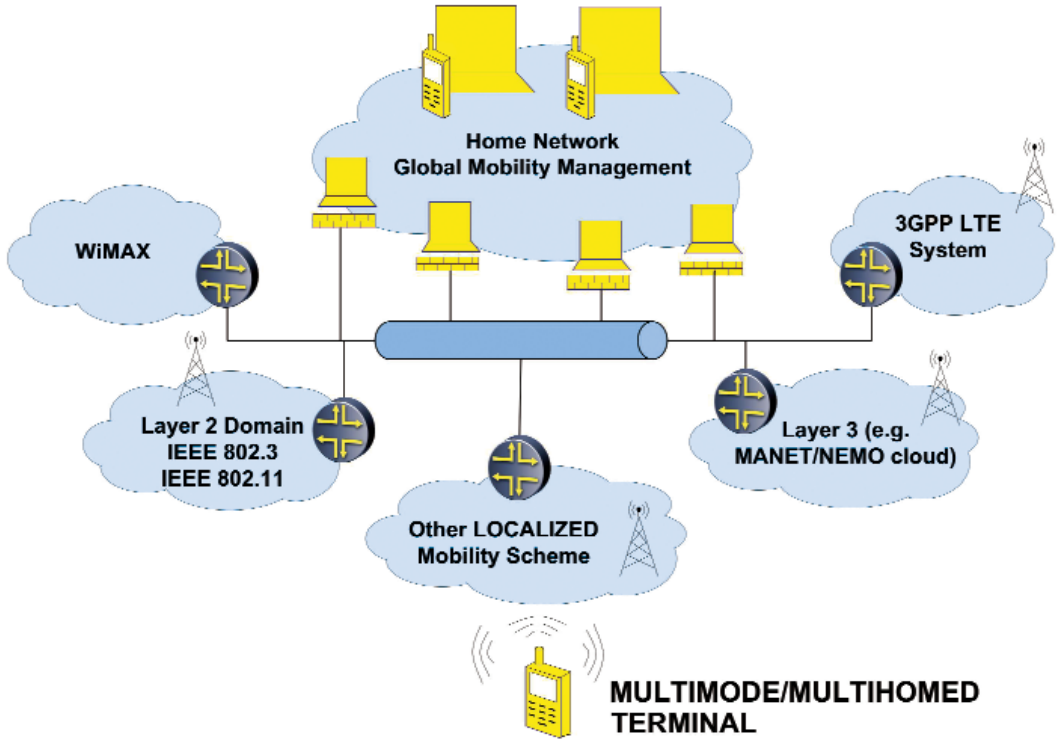
Network operators require the flexibility to manage their networks according to their requirements, technologies, and preferences. To provide this flexibility for mobility management, the Daidalos II architecture splits the mobility management into global and local domains (see Figure 2.17.1). Each of these mobility domains can belong to different operators. A global mobility domain is related to a user home network and provides user subscriptions and mobility, across different local domains. Local mobility domains are related with access networks. For simplicity, the architecture in Figure 2.17.1 restricts this view to a local domain per technology or type of network. However, we consider that a local domain is an operator network that eventually may be heterogeneous and contain several technologies. The mobility management in each of the domains is independent of the mobility management solution in other domains.

In the global domain, mobility is supported by means of a global mobility protocol (GMP), such as Mobile IPv6 (MIPv6) [3] or Host Identity Protocol (HIP) [4]. Terminal mobility within a local domain is handled via local mobility protocol operations, which are transparent to the core network and independent of the GMP. In this case, when a mobile node moves within a local domain, only the LMP used in that domain operates; when the node moves across domains, only GMP operates.

In the Daidalos II solution the terminals are not directly involved in the local mobility management: they only generate triggers that the local mobility management can use to manage the terminals' mobility. We define a framework, based on IEEE 802.21, to support this signalling and to integrate QoS concepts. IEEE 802.21 provides a standard interface between the network and the terminals in a technology independent way.

The Daidalos II mobility management view is in line with the current trends envisioned by the NetLMM IETF Working group [5]. However, many extensions need to be provided to the local mobility protocol. The support of heterogeneous domains, layer 2 domains, MANETs and NEMOs, multihoming, QoS integration, and identity based mobility management are some of the examples of shortcomings in the current NetLMM draft.

Figure 2.17.1: Daidalos II network architecture



Splitting mobility management in two domains and making both mobility management solutions independent brings a lot of flexibility to operators. For example, access operators can manage the mobility of the terminals closer to them, and thus do so more efficiently and with less overhead. Moreover, they do not have to depend on functions of an external operator to provide their own mobility services. In this sense, the access operator is free to choose any option for local mobility, including layer 2, layer 3 or legacy mobile technologies.

Also, while retaining the overall interoperation, network operations can be managed according to an access provider's or home operator's preferences, giving the opportunity for multiple wireless or wired access technologies. In addition, our architecture also relieves the terminal side of the requirement to implement a mobility function since it can provide mobility transparently within the local domain to terminals that do not implement any mobility function. To allow easy integration with the terminal side, it is envisioned the specification of a single interface, based on 802.21, abstracting the communication with the local mobility management scheme.

This solution also allows an easier integration of different legacy technologies like 3GPP Long Term Evolution (LTE) and WiMax networks that can be integrated as local mobility domain clouds. Another interesting case supported by the proposed architecture is L2 clouds that manage local mobility using L2 techniques. We are considering IEEE 802 technologies and solutions to improve mobility at L2 (e.g.: IEEE 802.11r for fast transition).

In terms of the functionalities, already mentioned, this architecture is able to provide both mobile- and network-initiated handovers, and can consider multihoming terminals and virtual identity concepts in the mobility management. It also supports networks like NEMO and MANET, and broadcast technologies with QoS support. All this integration aims at the support of a ubiquitous and pervasive environment.

Terminals roaming across different access networks, potentially implementing different wireless or wired access technologies, have the possibility to receive or send data across different access networks, possibly even simultaneously. This opens a new variety of business opportunities where users can choose the most suitable technology depending on several parameters, such as application requirements, user profiles or network conditions. However, the network is also required to implement intelligent functions to manage information systems as well as mobility, resources, and QoS. Thus, while traditional host based mobility will be maintained, more intelligent systems for network decision and network handover trigger are being investigated and developed. Mobile terminal and network initiated handovers will coexist in the same framework, being tightly integrated with the QoS support providing efficient support for handover decisions and resource management.

We also envision mobile terminals with multiple wireless access technologies that enable the opportunity for multihoming, namely the capability to receive or send data through different network devices at the same time. The control plane of such technology can be implemented at a global level, where the mobile operator owns the functionalities for multiple bindings, or locally keeping this transparent outside the local mobility domain. Terminals can be therefore multihomed without the mobile operator knowing the users' settings.

One of the Daidalos key concepts is that of virtual identity, which provides privacy to the entities using it. A user wants to be able to remain anonymous to the service provider and to neighbouring users. Service providers need not know the preferences of any given user but at the same time, they need sufficient information for charging and accounting. The virtual identity framework provides the possibility to instantiate several virtual users (which may represent only one physical user) all potentially using the same physical device or different physical devices. From the network perspective, virtual identities behave as different users, with different preferences. This may lead to a mobile terminal having simultaneous connections for different virtual identities, based on the multihoming support described in the previous section. In this sense, virtual identities affect mobility in the sense that users can move virtual identities without really moving the physical device.

In this architecture we consider local domains composed by MANETs and NEMOs, as shown in Figure 2.17.1. For both these networks, the concept of local/global mobility has a large effect on the mobility between

one of these networks and the infrastructure. We consider that NEMO can support the communication of two types of nodes: the legacy nodes (nodes without any kind of mobility support), and the visiting mobile nodes that are nodes visiting the NEMO. We have to define how to treat these nodes in the local mobility concept. The envisioned MANETs in Daidalos II are considered as multi-hop networks connected to the core network by means of one or more gateways, announcing specific prefixes within the MANET. Since access clouds are considered as local mobility domains, the integration of MANET within the overall architecture requires the analysis of the interaction between these networks with the local mobility management protocol. These interactions depend on the number of gateways supported and their locations, in the same or different local domains. This has impact on the ad-hoc nodes address configuration and on the mobility management.

The seamless integration of broadcast technologies is another key concept of the Daidalos II project. Namely, we consider the following broadcast technologies: MBMS, WiMAX, DVB-H/-T/-S and WLAN. Both MBMS and DVB networks require special actions to support them in the architecture. MBMS is a enhancement of UMTS to offer point-to-multipoint (PTM) services which enables this technology to be integrated into our project for multicast services. Therefore, we will study how to perform multicast mobility with Multimedia Broadcast Multicast Service (MBMS). There will be intra-technology handovers as well as handover to or from other network technologies considered, such as from a DVB cell to an MBMS cell. In order to have a seamless integration of the broadcast technologies, we are studying the integration of the UDLR [6] mechanism with IEEE 802.21 to support a unified interface to the upper layers.

For the support of QoS functions in the above framework, the envisioned QoS architecture is independent of the LMP/GMP specifics, and offers a common interface for all cases. The media-independent signalling part of the architecture will be based on the upcoming 802.21 standard. This standard is an ideal candidate as it aims at providing a media independent interface, which is exactly the objective of the QoS architecture. Note that to provide all the above functions, some extensions to the standard will need to be designed (in fact, these extensions were already performed [7])

Finally, one of the most relevant tuning parameters to provide mobility decisions is the availability of information from the surrounding context. Ubiquity and Pervasiveness (USP) are regarded here as a new set of triggers, which the architecture can benefit from enabling more customized set of services such as mobility. In this view, terminal mobility and related handover control can receive triggers from network related conditions events as well as from less traditional triggers, such as context information (such as location information, network coverage). This, combined with the identity management framework creates a new level of synergies giving novel functionalities to the architecture.

2.17.3. MOBILITY ARCHITECTURE

We further explore the requirements to be taken into account for the design of the mobility support. These are:

- **R1** Access Network Operators can implement their own mobility solution within their domains. The solution must be independent of external Mobility Operators (including home).
- **R2** Minimize complexity in the terminal
- **R3** Efficient use of wireless resources
- **R4** Reduce overhead signalling in the network

- **R5** The solution must be security friendly
- **R6** Seamless handover support
- **R7** Multihoming support
- **R8** Scalability for routing
- **R9** Minimize network side nodes modifications
- **R10** Support for heterogeneous networking
- **R11** The solution must be QoS friendly

It is common understanding that the Daidalos II project will address the Mobile IPv6 technology as part of the GMM problem space (although any other GMP protocol could apply) and a network based approach as part of the LMM problem space. The GMM is tightly integrated with the global identity-based mechanism described in the previous section.

The architecture can therefore support multiple LMPs. That is, the terminal should not implement LMP specific functions rather implement mechanisms for triggers to be provided to the network (see R2). It is therefore desirable to have a common interface to the access network. We envision the use of IEEE 802.21 for the common interface (extensions here might be required to meet Daidalos requirements).

One of the main goals of the mobility split is to provide a scalable solution where signalling overhead, both in the network and over the air, is minimized (see R3 and R4).

It is desirable that an LMD can (potentially) implement different wireless access technologies. We address these LMDs to be heterogeneous. Homogeneous LMDs are supported too (see R10).

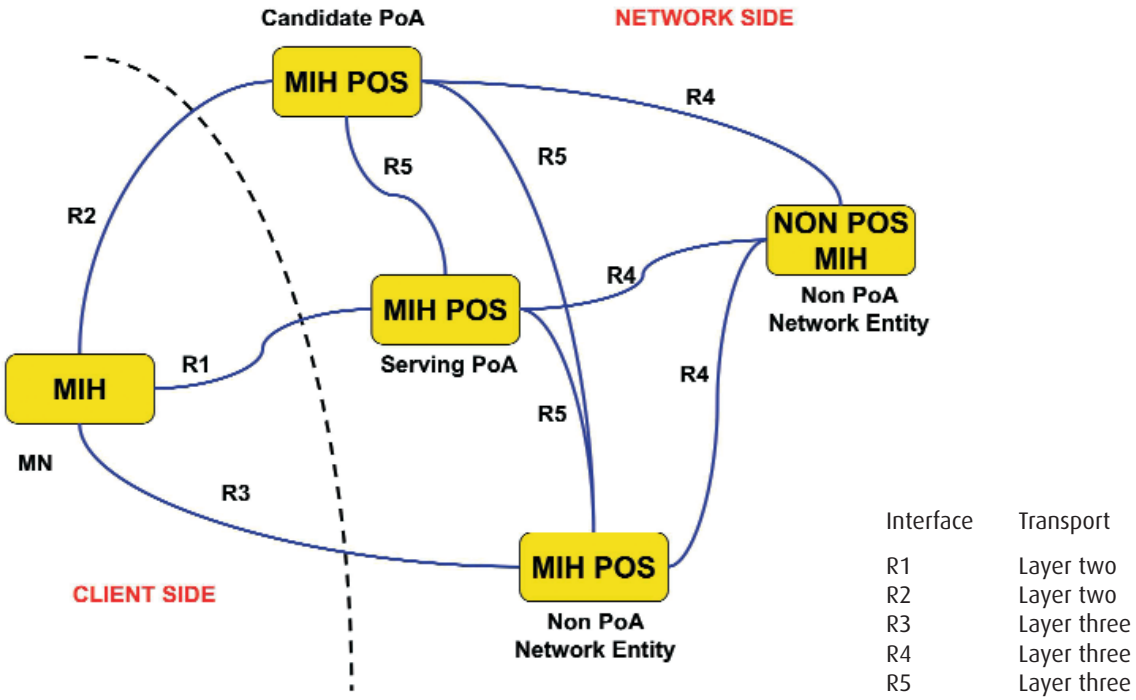
It is recommended to maintain the same IP address (Care of Address - CoA) within a single LMD. This feature looks appealing from a security point of view since LMDs can be untrusted. It avoids as well signalling to the home network for location update when performing handover (see R6, R9, R3, R4). By not changing the IP address location privacy is also provided. The level of privacy also depends on the size of the LMD (see R5).

Seamless (proactive) handover is required. The 802.21 signalling framework will provide this feature (see R6).

The IEEE 802.21 Media Independent Handover (MIH) technology enables the optimization of handovers between heterogeneous IEEE 802 systems as well as between 802 and cellular systems. The goal is to provide the means to facilitate and improve the intelligence behind handover procedures, allowing vendors and operators to develop their own strategy and handover policies. Furthermore, IEEE 802.21 is potentially usable in multiple mobility scenarios, both mobile and network initiated, and it is independent of the location of the mobility management entity.

The 802.21 standard specifies the communication model (see Figure 2.17.2) with functional entities and associated interfaces where the MIH technology is implemented in the mobile nodes and network side components, both being MIH-enabled. Network side components are classified either as Point of Attachment (PoA), where the mobile node is physically connected to, or as Point of Service (PoS). PoSs provide mobility services as defined in the specification. The transition between PoAs and its optimization is technology specific (e.g. fast BSS transition) in intra-technology handovers. However, in heterogeneous wireless access technologies scenarios, cross layer communication and handover optimizations are required, and are not trivial tasks (due, for example, to the link diversity).

Figure 2.17.2: IEEE Reference Communication Model



For this purpose, the IEEE 802.21 aims at optimizing the handover procedure between heterogeneous networks by adding a technology independent function (Media Independent Handover Function, MIHF) which improves the communication between different entities, either locally (mobile node) or remotely (network functions). The share of information and the use of common commands and events allow handover algorithms to be sufficiently intelligent to guarantee seamlessness while moving across different PoAs.

MIH defines three main mobility services. The Media Independent Event Service (MIES) provides event classification, event filtering and event reporting, associated to dynamic changes in link characteristics, link status and link quality. The Media Independent Command Service (MICS) enables MIH clients to manage and control link behavior related to handovers and mobility. It also provides the means to mandate actions

Multihoming at both GMD and LMD should be supported (see R7). So looking at the mobility management architecture, based on a logical separation of local and global mobility management, the following areas have to be considered:

- How to handle Multihoming in the Global Mobility Management (GMM);
- How to handle Multihoming in the Local Mobility Management (LMM).

Within LMM two different further possibilities have to be taken into account:

- Homogeneous Localized Mobility Domain (LMD): this implies that within a local mobility domain only one access technology is deployed; a multi-homed MT is connected to different LMDs (one for each access technology). Multihoming is only managed within the Global Mobility Domain (GMD);

- Heterogeneous LMD: a single LMD can deploy different access technologies. A multi-homed MT may be connected to two (or more) different (heterogeneous) access networks belonging to the same LMD. This implies that Multihoming (MH) could be managed within the Localized Mobility Management Protocol (LMP). Moreover, it could be the case that some other MT interfaces could belong to a different LMD; in this case Multihoming should again be managed within the Global Mobility Domain (GMD) through the Global Mobility Management Protocol (GMP).

Since the mobility is handled using two layers (GMD and/or LMD) multihoming extensions can be applied to:

- the Global Mobility Management Protocol (GMP);
- the Local(ized) Mobility Management Protocol (LMP);
- both the GMM and the LMM protocols.

In the case multihoming is managed at GMD level there is not impact on the LMD protocol. The solution for multihoming support is based on Mobile IPv6 extensions. In the case multihoming is managed at LMD level, solutions are related to the LMD protocol considered.

It is desirable to study the optimal (routing) configuration for large scale LMDs (see R8).

An operator has the flexibility to choose any LMP to handle mobility in its own network. Alternatively, a mobile operator may decide to directly use the GMP to support mobility in its own network and thus avoid installing any mobility related infrastructure. In this latter case mobility functions are supported by equipment located in other networks outside the operator's domain.

The LMD solution is based on the IETF NetLMM protocol.

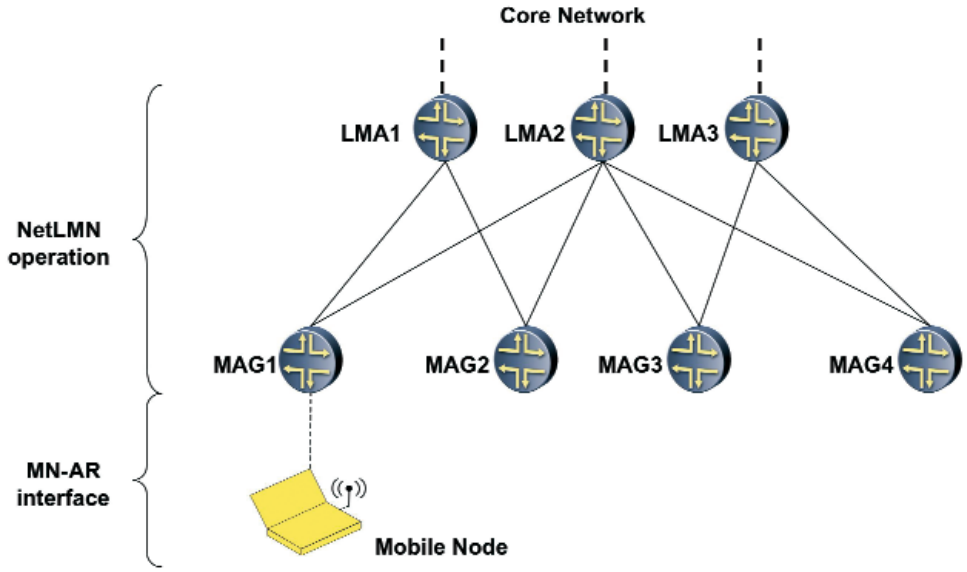
Unlike host-based mobility, such as Mobile IPv6, where mobile terminals signal a location change to the network to maintain routing states and to achieve reach ability, the NetLMM approach relocates relevant functionality for mobility management from the mobile terminal to the network. The network learns about a terminal's movement through standard terminal operation, such as router and neighbour discovery or by means of link-layer support. It then coordinates routing state update without any mobility specific support from the terminal. Such an approach allows hierarchical mobility management on one hand, where mobile terminals signal location update to a global mobility anchor only when they change the localized mobility domain, and mobility within a localized domain on the other hand. for terminals without any support for mobility management. NetLMM complements host-based global mobility management by means of introducing local edge domains. In the future, network based approaches may be also used for to achieve global mobility.

Figure 2.17.3 shows the entities involved in the localized mobility management. The entities supporting NetLMM functionalities are the Local Mobility Agent and the Mobility Access Gateway. The LMA is a router defining the edge between the NetLMM domain and the core network. If a global mobility scheme is used, it is the boundary between Global and Local Mobility domains. The MAG is the access router for the mobile node.

The NetLMM operation is located between the LMA and the MAG.

Finally, the integration of LMDs based on layer two technologies focus on the use of IEEE 802.1D (Learning Bridges). In fact, this traditional Ethernet switching technology is to be used for "routing" IEEE 802 data frames inside the L2 cloud. The choice of this technology considers factors such as the high cost/benefit ratio of Ethernet, integration with 802.11 and 802.16, and legacy considerations.

Figure 2.17.3: Netlmm protocol architecture



2.17.4. AD-HOC AND NETWORK MOBILITY

The basis for the NEMO support in Daidalos is the NEMO Basic Support protocol [3]. This standard solution has several performance limitations, and for this reason we extend it to provide also route optimization in the traffic between the nodes in the NEMO and other nodes. For providing route optimization we consider that inside a NEMO we can have two types of nodes: the legacy nodes that are nodes without any kind of mobility support, and the visiting mobile nodes that are mobile nodes visiting the NEMO. In terms of the legacy nodes, all the address configuration and mobility procedures (including route optimization) are handled by the mobile router. The mobile router acts as a proxy for the legacy nodes, detecting flows that can be optimized and generating the appropriate mobility signalling for optimizing those flows. The visiting mobile nodes, on the other hand, can manage their own mobility but they require addresses (CoAs) that are topologically correct in the infrastructure that the NEMO is visiting. In the proposed solution this is achieved using Protocol for carrying Authentication for Network Access (PANA) functionality that allows telling a node that it must change its IPv6 address and how to get a new one. The MR uses this functionality for detecting a visiting node and directs it to configure a topologically correct address in the infrastructure.

This route optimization functionality has to be combined with the localized mobility solution. A localized mobility solution can be very useful for NEMO, because it avoids the mobility signalling outside the domain in intra-domain handovers, and NEMO solutions can require significant signalling during handovers (signalling corresponding to different nodes inside the NEMO have to be sent). With the localized mobility solution, this signalling only takes place in movements between localized mobility domains.

The mobile router will protect all the addresses (CoAs) in the infrastructure, both their own address and the topologically correct addresses that are used by the mobile nodes visiting the NEMO. If the NEMO changes

Access Router (AR) inside the localized mobility domain, the Localized Mobility Anchor (LMA) will send the traffic to the new AR without any explicit mobility signalling from the mobile router or the visiting mobile nodes inside the NEMO (the corresponding CoAs do not change). When a Visiting Mobile Node (VMN) moves from the NEMO to an AR in the infrastructure inside the same localized mobility domain the NEMO is visiting, the MR will cease protecting the address of the VMN (its CoA) and the VMN can keep using this address as CoA, performing an intra-localized domain handover. The localized mobility protocol will take care of sending the packets addressed to the CoA to the new AR.

The support of NEMOs in Daidalos also provides authentication (based on PANA), integration with a AAA infrastructure, and QoS. These solutions are extensions of the solution adopted for mobile nodes. In fact, from the point of view of the infrastructure, a NEMO cannot be differentiated from a mobile terminal: the procedures are the same and there is no any new requirement to the infrastructure to support NEMOs.

2.17.5. BROADCAST AND MULTICAST

The seamless integration of broadcast is another key concept of the Daidalos II project. Namely, we consider the following broadcast technologies: MBMS, WiMAX, DVB-H/-T/-S and WLAN.

Both MBMS and DVB networks require special actions to support them in the architecture. MBMS is a enhancement of UMTS to offer PTM services which enables this technology to be integrated into our project for multicast services. Therefore, we will study how to perform multicast mobility with MBMS. There will be intra-technology handovers as well as handover to or from other network technologies considered, such as from a DVB cell to an MBMS cell.

The integration of DVB networks is a challenge since these support only unidirectional transmission. There are several modes of handling this limitation by using a second bidirectional link:

- True unidirectional mode: using the DVB link as a unidirectional link and to receive the broadcasted services without being able to react or to control them.
- Virtual bidirectional mode: permanently using a second bidirectional link for return traffic. This allows common IP services to be used.
- A composition of these modes: have only unreliable services received via DVB but control these via a bidirectional link when necessary (and possible). This intermediate mode requires quite extensive work on integration.

In order to have a seamless integration of the broadcast technologies, we are studying the integration of the UDLR [6] mechanism with IEEE 802.21 to support a unified interface to the upper layers.

The challenge of unidirectional links support becomes even greater when we consider mobility of both unidirectional and return channel, as well as the QoS and security support. As well as the common QoS and security process, the encapsulated return traffic should be treated in a similar way. Also the support of seamless handover on such links will be studied. The terminal should already know the tunnel endpoint address of the next DVB AR before the handover, otherwise long gaps of connectivity will be experienced.

To make effective use of the "one-to-many" capability of these broadcast networks, multicast based on PIM-SM and MLDv2 is used. The use of multicast in the architecture requires the integration of multicast

and the localised mobility management, as well as its integration with authentication and security mechanisms, and support for virtual identities. Since source mobility will be considered too, single source multicast (SSM) will be supported in addition to Any Source Multicast (ASM). To allow seamless forwarding for moving source and efficient routing PIM-SM will be extended by an indirection mechanism.

For seamless listener handover, there will be a context transfer mechanism used, as well for intra- and inter-domain handovers.

In our architecture, all virtual identities used on the same device will remain unlinkable in terms of multicast subscription as well as multicast transmission. Since multicast routing hides the set of receivers from potential attackers outside of the access network, the actions taken may be restricted to the access network.

To support multicast on unidirectional links with a temporary unavailable return channel an alternative group membership management system will be provided which allows subscribing for a certain time in advance. Using this system there is no need for the listener to provide MLD reports during the specified time frame.

2.17.6. CONCLUSION AND FUTURE WORK

This paper presents a mobility architecture able to seamlessly integrate heterogeneous networks with different technologies, including broadcast ones, with different network types, such as MANETs and NEMOs, and able to interoperate with legacy architectures, such as 3GPP and Wimax.

This paper briefly describes the functionalities of this architecture and some ideas on how to achieve them. The final paper will deeply explain the architecture and the mechanisms developed to support all the mentioned functionalities.

2.17.7. ACKNOWLEDGMENTS

The work described in this paper is based on results of IST FP6 Integrated Project Daidalos II. Daidalos II receives research funding from the European Community's Sixth Framework Programme. The authors wish to thank the partners of the Daidalos II Consortium, in particular partners of WP2 for their collaborative work.

2.17.8. REFERENCES

[1] The IST Daidalos Poject, http://www.ist-daidalos.org.

[2] The IEEE 802.21 Working Group, http://www.ieee802.org/21.

[3] D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775 (Proposed Standard), June 2004.

[4] R. Moskowitz. Host Identity Protocol Architecture. Internet Draft (Work in Progress), January 2005).

[5] Giaretta, G., "NetLMM Protocol", draft-giaretta-netlmm-dt-protocol-00, June 2006.

[6] E. Duros, W. Dabbous, H. Izumiyama, N. Fujii, Y. Zhang: A Link-Layer Tunneling Mechanism for Unidirectional Links, , ftp://ftp.ietf.org/rfc/rfc3077.txt.

[7] A.Vidal, T.Melia, and D. Corujo. QoS Considerations in Network Initiated Handovers. Contribution to IEEE 802.21, May 2006.

3 ABSTRACTS OF STANDARDIZATION WORK DONE IN THE ENABLE PROJECT

Abstracts of standardization work done in the enable project

introduction

The ENABLE project has operated in close co-operation with IETF and IRTF, in order to ensure that the solutions developed by the project are in line with the architectural principles devised by the Internet community and can lead towards standardization.

As a result of such work, several Internet Drafts and RFC documents have been published. This chapter summarizes the title and the abstract of those documents, which cover different aspects, related to various mobility deployment issues.

3.1 IETF

WORKING GROUP Diameter Maintenance and Extensions (dime)

TITLE Diameter Fast Mobile IPv6 Application
draft-bournelle-dime-fmip6-00

ABSTRACT

The Diameter Fast Mobile IPv6 Application is to be used in conjunction with the "Handover Keys using AAA" protocol.

TITLE Diameter MIPv6 Application for the Integrated Scenario
draft-tschofenig-dime-mip6-integrated-00

ABSTRACT

A Mobile IPv6 node requires a home agent address, a home address, and IPsec security association with its home agent before it can start utilizing Mobile IPv6 service. RFC3775 requires that some or all of these parameters are statically configured. Ongoing work aims to make this information dynamically available to the mobile node. An important aspect of the Mobile IPv6 bootstrapping solution is to support interworking with existing authentication, authorization and accounting infrastructure. This document defines a Diameter application to facilitate Mobile IPv6 bootstrapping for the integrated scenario.

TITLE Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction
draft-ietf-dime-mip6-split-05

ABSTRACT

Mobile IPv6 deployments may want to bootstrap their operations dynamically based on an interaction between the Home Agent and the Diameter server of the Mobile Service Provider (MSP). This document specifies the interaction between a Mobile IP Home Agent and the Diameter server. Several different mechanisms for authenticating a Mobile Node are supported. The usage of the Internet Key Exchange v2 (IKEv2) protocol allows different mechanisms, such as the Extensible Authentication Protocol (EAP), certificates and pre-shared secrets in IKEv2 to be used. Furthermore, another method makes use of the Mobile IPv6 Authentication protocol. In addition to authentication authorization, the configuration of Mobile IPv6 specific parameters and accounting is specified in this document.

WORKING GROUP Diameter Maintenance and Extensions (dime)

TITLE Diameter Mobile IPv6:
Support for Network Access Server to Diameter Server Interaction
draft-ietf-dime-mip6-integrated-05

ABSTRACT

A Mobile IPv6 node requires a Home Agent address, a home address, and a security association with its Home Agent before it can start utilizing Mobile IPv6. RFC3775 requires that some or all of these parameters are statically configured. Mobile IPv6 bootstrapping work aims to make this information dynamically available to the Mobile Node. An important aspect of the Mobile IPv6 bootstrapping solution is to support interworking with existing authentication, authorization and accounting infrastructure. This document describes the MIPv6 bootstrapping using the Diameter Network Access Server (NAS) to home Authentication, Authorization and Accounting server (HAAA) interface.

TITLE Diameter Quality of Service Application
draft-tschofenig-dime-diameter-qos-01

ABSTRACT

This document describes a Diameter application that performs Authentication, Authorization, and Accounting for Quality of Service (QoS) reservations. This protocol is used by elements along the path of a given application flow to authenticate a reservation request, ensure that the reservation is authorized, and to account for resources consumed during the lifetime of the application flow. Clients that implement the Diameter QoS application contact an authorizing entity/application server that is located somewhere in the network, allowing for a wide variety of flexible deployment models.

WORKING GROUP Handover Keying (hokey)

TITLE Handover Key Management and Re-authentication Problem Statement
draft-ietf-hokey-reauth-ps-04

ABSTRACT

This document describes the Handover Keying (HOKEY) problem statement. The current EAP keying framework is not designed to support re-authentication and handovers. This often cause unacceptable latency in various mobile wireless environments. HOKEY plans to address these HOKEY plans to address these problems by implementing a generic mechanism to reuse derived EAP keying material for handover.

WORKING GROUP IPv6 Operations (v6ops)

TITLE ISP IPv6 Deployment Scenarios in Broadband Access Networks
RFC4779

ABSTRACT

This document provides a detailed description of IPv6 deployment and integration methods and scenarios in today's Service Provider (SP) Broadband (BB) networks in coexistence with deployed IPv4 services. Cable/HFC, BB Ethernet, xDSL, and WLAN are the main BB technologies that are currently deployed, and discussed in this document. The emerging Broadband Power Line Communications (PLC/BPL) access technology is also discussed for completeness. In this document we will discuss main components of IPv6 BB networks, their differences from IPv4 BB networks, and how IPv6 is deployed and integrated in each of these networks using tunneling mechanisms and native IPv6.

WORKING GROUP Mobility for IP: Performance, Signaling and Handoff Optimization (mipshop)

TITLE Establishing Handover Keys using Shared Keys
draft-vidya-mipshop-handover-keys-aaa-04

ABSTRACT

This document describes a key management protocol to generate a handover key between a mobile node (MN) and an access router (AR) for the purpose of securing Fast Mobile IPv6 (FMIPv6) signaling messages. As such, it specifies a message exchange between the MN and the AR and assumptions that must hold in order for this protocol to work. The protocol itself is described here for FMIPv6 use, but is applicable to other protocols that need to establish shared keys between the MN and a network entity.

WORKING GROUP Mobility for IPv6 (mip6)

TITLE AAA Goals for Mobile IPv6
draft-ietf-mip6-aaa-ha-goals-03

ABSTRACT

In commercial deployments Mobile IPv6 can be a service offered by a Mobility Services Provider (MSP). In this case all protocol operations may need to be explicitly authorized and traced, requiring the interaction between Mobile IPv6 and the AAA infrastructure. Integrating the AAA infrastructure offers also a solution component for Mobile IPv6 bootstrapping in integrated and split scenarios. This document describes various scenarios where a AAA interface for Mobile IPv6 is actually required. Additionally, it lists design goals and requirements for such an interface.

TITLE Application Master Session Key (AMSK) for Mobile IPv6
draft-giaretta-mip6-amsk-02

ABSTRACT

The Extensible Authentication Protocol (EAP) defines an extensible framework for performing network access authentication. Most EAP authentication algorithms, also known as "methods", export keying material that can be used with lower layer ciphersuites. It can be useful to leverage this keying material to derive usage specific keys that can be used to authenticate users or protect information exchange by other applications or services. For this purpose "Specification for the Derivation of Usage Specific Root Keys (USRK) from an Extended Master Session Key (EMSK)" [draft-salowey-eap-emsk-deriv-01] proposes to derive root keys for each usage application and, then, child keys to actual be used. This document defines how to generate a Usage Specific Root Key (USRK) and a series of Application Master Session Keys (AMSKs) specific to Mobile IPv6 service. These AMSKs can be used by Mobile Node and Home Agent to bootstrap Mobile IPv6 protocol operation.

TITLE Firewall Recommendations for MIPv6
draft-krishnan-mip6-firewall-01

ABSTRACT

This document presents some recommendations for firewall administrators to help them configure their firewalls in a way that allows Mobile IPv6 signaling and data messags to pass through. This document assumes that the firewalls in question include some kind of stateful packet filtering capability.

WORKING GROUP Mobility for IPv6 (mip6)

TITLE MIP6-bootstrapping for the Integrated Scenario
draft-ietf-mip6-bootstrapping-integrated-03

ABSTRACT

The Mobile IPv6 bootstrapping problem statement describes two main scenarios. In the first scenario (i.e. the split scenario), the mobile node's mobility service is authorized by a different service authorizer than the basic network access authorizer. In the second scenario (i.e. the integrated scenario), the mobile node's mobility service is authorized by the same service authorizer as the basic network access service authorizer. This document defines a method for home agent information discovery for the integrated scenario.

TITLE MIPv6 Authorization and Configuration based on EAP
draft-giaretta-mip6-authorization-eap-04

ABSTRACT

This draft defines an architecture, and related protocols, for performing dynamic Mobile IPv6 authorization and configuration relying on a AAA infrastructure. The necessary interaction between the AAA server of the home provider and the mobile node is realized using EAP, exploiting the capability of some EAP methods to convey generic information items together with authentication data. This approach has the advantage that the access equipment acts as a simple pass-through for EAP messages and therefore does not play any active role in the Mobile IPv6 negotiation procedure, which makes the solution easier to deploy and maintain.

TITLE Mobile IP Interactive Connectivity Establishment (M-ICE)
draft-tschofenig-mip6-ice-01

ABSTRACT

This document describes how the Interactive Connectivity Establishment (ICE) methodology can be used for Mobile IP to determine whether end-to-end communication is possible. ICE makes use of the Session Traversal Utilities for NAT (STUN) protocol in addition to mechanisms for checking connectivity between peers. After running the ICE the two MIP end points will be able to communicate directly or through a relay via Network Address Translators (NATs), Network Address and Port Translators (NAPTs) and firewalls. This document addresses also the problems raised in RFC4487 "Mobile IPv6 and Firewalls: Problem Statement".

WORKING GROUP Mobility for IPv6 (mip6)

TITLE Mobile IPv6 Bootstrapping in Split Scenario
RFC5026

ABSTRACT

A Mobile IPv6 node requires a Home Agent address, a home address, and IPsec security associations with its Home Agent before it can start utilizing Mobile IPv6 service. RFC3775 requires that some or all of these are statically configured. This document defines how a Mobile IPv6 node can bootstrap this information from non-topological information and security credentials pre-configured on the Mobile Node. The solution defined in this document solves the split scenario described in the Mobile IPv6 bootstrapping problem statement in RFC4640. The split scenario refers to the case where the Mobile Node's mobility service is authorized by a different service provider than basic network access. The solution described in this document is also generically applicable to any bootstrapping case, since other scenarios are more specific realizations of the split scenario.

TITLE Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)
RFC4640

ABSTRACT

A mobile node needs at least the following information: a home address, a home agent address, and a security association with home agent to register with the home agent. The process of obtaining this information is called bootstrapping. This document discusses issues involved with how the mobile node can be bootstrapped for Mobile IPv6 (MIPv6) and various potential deployment scenarios for mobile node bootstrapping.

TITLE RADIUS Mobile IPv6 Support
draft-ietf-mip6-radius-02

ABSTRACT

A Mobile IPv6 node requires a home agent (HA) address, a home address (HOA), and IPsec security association with its HA before it can start utilizing Mobile IPv6 service. RFC3775 requires that some or all of these parameters are statically configured. Ongoing work aims to make this information dynamically available to the mobile node. An important aspect of the Mobile IPv6 bootstrapping solution is to support interworking with existing authentication, authorization and accounting (AAA) infrastructure. This document defines new attributes to facilitate Mobile IPv6 bootstrapping via a RADIUS infrastructure. This information exchange may take place as part of the initial network access authentication procedure or as part of a separate protocol exchange between the mobile node, the HA and the AAA infrastructure.

WORKING GROUP Network-based Localized Mobility Management (netlmm)

TITLE Goals for Network-Based Localized Mobility Management (NETLMM)
RFC4831

ABSTRACT

In this document, design goals for a network-based localized mobility management (NETLMM) protocol are discussed.

TITLE NetLMM Protocol
draft-giaretta-netlmm-dt-protocol-02

ABSTRACT

This document specifies an Internet protocol that allows mobile nodes to move around in a local mobility domain, changing their point of attachment within the domain, but without ever being aware at the IP layer that their point of attachment has changed, and maintaining seamless communication in the presence of such changes. It defines two protocol entities, a Mobile Access Gateway and a Local Mobility Anchor, and a set of messages between them, that together make these mobility events transparent to the mobile nodes at the IP layer, as long as they remain within the local mobility domain.

TITLE Problem Statement for Network-Based Localized Mobility Management (NETLMM)
RFC4830

ABSTRACT

Localized mobility management is a well-understood concept in the IETF, with a number of solutions already available. This document looks at the principal shortcomings of the existing solutions, all of which involve the host in mobility management, and makes a case for network-based local mobility management.

WORKING GROUP Next Steps in Signaling (nsis)

TITLE Authorization for NSIS Signaling Layer Protocols
draft-manner-nsis-nslp-auth-03

ABSTRACT

Signaling layer protocols in the NSIS working group may rely on GIST to handle authorization. Still, the signaling layer protocol itself may require separate authorization to be performed when a node receives a request for a certain kind of service or resources. This draft presents a generic model and object formats for session authorization within the NSIS Signaling Layer Protocols. The goal of session authorization is to allow the exchange of information between network elements in order to authorize the use of resources for a service and to coordinate actions between the signaling and transport planes.

TITLE Mobile IPv6 - NSIS Interaction for Firewall traversal
draft-thiruvengadam-nsis-mip6-fw-06

ABSTRACT

Most of the firewalls deployed today are Mobile IPv6 unaware. Widespread Mobile IPv6 deployment is not possible unless Mobile IPv6 messages can pass through these firewalls. One approach is to use a signaling protocol to communicate with these firewalls and instruct them to bypass these Mobile IPv6 messages. The goal of this document is to describe the interaction between NSIS and Mobile IPv6 for enabling Mobile IPv6 traversal.

WORKING GROUP Protocol for carrying Authentication for Network Access (pana)

TITLE PANA Bootstrapping IEEE 802.11 security
draft-marin-pana-ieee80211doti-00

ABSTRACT

PANA (Protocol for carrying Authentication for Network Access) is a link-layer agnostic transport for Extensible Authentication Protocol (EAP) to enable network access authentication between clients and access networks. PANA framework defines two types of security associations which can be bootstrapped as a consequence of PANA execution: IP layer security is established with IPsec by using IKE and link-layer security with WPA/IEEE 802.11i in PSK mode. This document is focused on how PANA can bootstrap link layer security through IEEE 802.11i and exposes issues which can be raised as a consequence of this interaction.

WORKING GROUP RADIUS EXTensions (radext)

TITLE RADIUS Quality of Service Support
draft-tschofenig-radext-qos-05

ABSTRACT

This document describes an extension to the RADIUS protocol that performs authentication, authorization, and accounting for Quality-of-Service reservations. The described extensions allow network elements to authenticate the initiator of a reservation request (if desired), to ensure that the reservation is authorized, and to account for established QoS resources. Flexibility is provided by offering support for different authorization models and by decoupling specific QoS attributes carried in the QoS signaling protocol from the AAA protocol. This document is the RADIUS complement to the DIAMETER QoS application.

WORKING GROUP Softwires (softwires)

TITLE Automatic Tunneling Setup for/with IPv6
draft-palet-softwire-ats6-01

ABSTRACT

This document presents the basis for a procedure that enables a host or router to automatically setup an IPvX in IPvY tunnel. Basically, the document considers several scenarios, from the most common today "dominant IPv4" networks to new "dominant IPv6" networks, which can even support the use of multicast. A basic requirement is that the host or router is a dual stack node and it will have either native IPv4-only access (dominant IPv4 network) or native IPv6-only access (dominant IPv6 network). Consequently, either IPv6 will be transported in the existing IPv4-only infrastructure, or IPv4 will be transported in the existing IPv6-only infrastructure. Other combinations are possible, such as IPv6 in IPv6 (for example to support IPv6 multicast in an IPv6-unicast-only infrastructure). The procedure follows the work from "Goals for Zero-Configuration Tunneling in 3GPP" [draft-nielsen-v6ops-3GPP-zeroconf-goals-00], "Zero-Configuration Tunneling Requirements" [draft-suryanarayanan-v6ops-zeroconf-reqs-00], "Goals for Registered Assisted Tunneling" [draft-ietf-v6ops-assisted-tunneling-requirements-01], "Goals for Tunneling Configuration" [draft-palet-v6tc-goals-tunneling-00] and mainly "Softwire Problem Statement" [draft-ietf-softwire-problem-statement-00], trying to be compliant with the requirements enumerated in those documents.

WORKING GROUP Softwires (softwires)

TITLE Software Problem Statement
RFC4925

ABSTRACT

This document captures the problem statement for the Softwires Working Group, which is developing standards for the discovery, control, and encapsulation methods for connecting IPv4 networks across IPv6-only networks as well as IPv6 networks across IPv4-only networks. The standards will encourage multiple, inter-operable vendor implementations by identifying, and extending where necessary, existing standard protocols to resolve a selected set of "IPv4/IPv6" and "IPv6/IPv4" transition problems. This document describes the specific problems ("Hubs and Spokes" and "Mesh") that will be solved by the standards developed by the Softwires Working Group. Some requirements (and non-requirements) are also identified to better describe the specific problem scope.

TITLE Softwire Security Analysis and Requirements
draft-ietf-softwire-security-requirements-03

ABSTRACT

This document describes the security Guidelines for the Softwire "Hubs and Spokes" and "Mesh" solutions. Together with the discussion of the Softwire deployment scenarios, the vulnerability to the security attacks is analyzed to provide the security protection mechanism such as authentication, integrity and confidentiality to the softwire control and data packets.

TITLE Softwires Hub & Spoke Deployment Framework with L2TPv2
draft-ietf-softwire-hs-framework-l2tpv2-07

ABSTRACT

This document describes the framework of the Softwire "Hub and Spoke" solution with Layer 2 Tunneling Protocol (L2TPv2), and the implementation details specified in this document should be followed to achieve inter-operability among different vendor implementations.

3.2 IRTF

WORKING GROUP Anonymous Identifiers (alien)

TITLE Anonymous Layers Identifiers (ALIen):
Threat Model for Mobile and Multihomed Nodes
draft-haddad-alien-threat-model-00

ABSTRACT

This memo describes privacy threats related to the MAC and IP layers identifiers in a mobile and multi-homed environment.

WORKING GROUP Host Identity Protocol Research Group (hiprg)

TITLE Interaction between SIP and HIP
draft-tschofenig-hiprg-host-identities-05

ABSTRACT

This document investigates the interworking between the Session Initiation Protocol (SIP) and the Host Identity Protocol (HIP) and the benefits that may arise from their combined operation. The aspect of exchanging Host Identities (or Host Identity Tags) in SIP/SDP for later usage with the Host Identity Protocol Protocol (HIP) is described in more detail as an example of this interworking.

WORKING GROUP Host Identity Protocol Research Group (hiprg)

TITLE Traversing HIP-aware NATs and Firewalls: Problem Statement and Requirements
draft-tschofenig-hiprg-hip-natfw-traversal-06

ABSTRACT

The Host Identity Protocol (HIP) is a signaling protocol, which supports mobility and multihoming by adding a new layer in the TCP/IP stack. By carring relevant parameters in the signaling messages, HIP can be used to establish IPsec encapsulating security payload (ESP) security associations between two hosts. Middleboxes (e.g. firewalls and network address translators) cannot inspect transport layer headers of data traffic if that traffic is sent over an IPsec ESP tunnel. However, HIP is designed to be middlebox friendly; it enables the middleboxes to inspect the signaling messages. The information that they can derive from that messages enables the middleboxes to uniquely identify the subsequent data flows, e.g. for the purposes of multiplexing and demultiplexing. A middlebox that implements the relevant mechanisms is called "HIP-aware". This document presents a problem statement and lists some requirements that are necessary for a HIP-aware middlebox traversal technique. These include authentication and authorization of signaling end-hosts by the middleboxes. Such authorization will help the middleboxes to decide whether or not an end host is allowed to traverse, and can potentially limit unwanted traffic.

TITLE Using SRTP transport format with HIP
draft-tschofenig-hiprg-hip-srtp-02

ABSTRACT

The Host Identity Protocol (HIP) is a signaling protocol which adds a new layer between the traditional Transport and the Network layer. HIP is an end-to-end authentication and key exchange protocol, which supports security and mobility in a commendable manner. The HIP base specification is generalized and purported to support different key exchange mechanisms in order to provide confidentiality protection for the subsequent user data traffic. This draft explains a mechanism to establish Secure Real Time Protocol associations, to protect the user data packets, by using HIP.

WORKING GROUP IP Mobility Optimizations (mobopts)

TITLE Link and Path Characteristic Information Delivery Analysis
draft-korhonen-mobopts-delivery-analysis-01

ABSTRACT

This document analyses capabilities and applicability of various IP Mobility, signaling and transport protocols for delivering Link and Path Characteristic Information between communicating end points.

GLOSSARY

3GPP. 3rd Generation Partnership Project. The scope of 3GPP is to make a globally applicable third generation (3G) mobile phone system specification within the scope of the ITU's IMT-2000 project. 3GPP specifications are based on evolved GSM specifications, now generally known as the UMTS system.

AAA. Authentication, Authorization and Accounting.

Access Point (AP). A wireless access point, identified by a MAC address, providing service to the wired network for wireless nodes.

Access Router (AR). The entity interconnecting the access network to the Internet or other IP-based networks. The AR provides connectivity between hosts on the access network at different customer premises. It is also used to provide security filtering, policing, and accounting of customer traffic.

Access Service Authoriser (ASA). A network operator that authenticates a mobile node and establishes the mobile node's authorisation to receive Internet service.

Access Service Provider (ASP). A network operator that provides direct IP packet forwarding to and from the end host.

Accounting. The collection of resource consumption data for the purposes of capacity and trend analysis, cost allocation, auditing, and billing. Accounting management requires that resource consumption be measured, rated, assigned, and communicated between appropriate parties.

Binding Acknoledgment (BA). The Binding Acknoledgment message is sent by the home agent in order to acknowledge the Binding Update message sent by the mobile node.

Bootstrapping Authorisation Agent (BAA). Function of the BA that is responsible for asserting authorisation statements.

Bootstrapping Client (BC). Entity that communicates with the BA in order to obtain bootstrapping and service authorisations.

Bootstrapping Configuration Agent (BCA). Function of the BA that is responsible for providing necessary bootstrapping information to the mobile node (e.g. HA address, the security association and the Home address).

Bootstrapping Target (BT). Entity that is part of the service providing server and is responsible for obtaining the service and MN related information from the BA and converting the obtained information in service target function understandable format.

Binding Update (BU). The mobile node sends the Binding Update message to the home agent in order to inform that is attached to a foreign network.

Care-of Address (CoA). A unicast routable address associated with a mobile node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix. Among the multiple care-of addresses that a mobile node may have at any given time (e.g., with different subnet prefixes), the one registered with the mobile node's home agent for a given home address is called its "primary" care-of address.

Care-of Test Init (CoTI). The mobile node sends a Care-of Test Init message to the correspondent node during the Return Routability Procedure.

Correspondent Node (CN). A node on either foreign network or home. network or other network with which the MN communicates

Designated Home Agent (dHA). In the HA relocation procedure, the dHA is the new HA assigned to the MN.

Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The Dynamic Host Configuration Protocol for IPv6 (DHCP) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes.

Domain Name System (DNS). The system used in Internet in order to find out the nodes IP address based on their Domain Names.

Dual-Stack (DS). Nodes that implements both IPv4 and IPv6 network stacks.

Denial-of-Service (DoS). It is a method to attack a node in order to prevent its regular working.

Extensible Authentication Protocol (EAP). An authentication framework which supports multiple authentication methods, typically used for wireless network access authorization.

EDGE. Enhanced Data rates for GSM Evolution. EDGE is a digital mobile phone technology which acts as an enhancement to 2G and 2.5G General Packet Radio Service (GPRS) networks.

Firewall (FW). Network device in charge of filtering undesired network traffic.

Global mobility. Global mobility roughly refers to the situation where the MN moves between two access networks. The scope of the access networks is depending on deployment considerations.

GPRS. General Packet Radio Service. It is a mobile data service available to users of GSM mobile phones.

GSM. Global System for Mobile Communications. GSM is the international digital radio standard created by the European Telecommunications Standards Institute. GSM allows users to roam freely among markets.

General Service Authorization Architecture (GSABA). The ENABLE architecture proposal for deploying the mobile service in large scale.

Home Address (HoA). A unicast routable address assigned to a mobile node, used as the permanent address of the mobile node. This address is within the mobile node's home link. Standard IP routing mechanisms will deliver packets destined for a mobile node's home address to its home link. Mobile nodes can have multiple home addresses, for instance when there are multiple home prefixes on the home link.

Home Agent (HA). A router on a mobile node's home link with which the mobile node has registered its current care-of address. While the mobile node is away from home, the home agent intercepts packets on the home link destined to the mobile node's home address, encapsulates them, and tunnels them to the mobile node's registered care-of address.

Home-of Test Init (HoTI). The Home-of Test Init message is sent by the mobile node to the home agent during the Return Routability Procedure.

Internet Key Exchange (IKEv1). Protocol to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IPsec.

Internet Key Exchange (IKEv2). Version 2 of the Internet Key Exchange (IKEv1) protocol. Version 1 and 2 do not interoperate each other.

Integrated scenario. A scenario where the mobility service and the network access service are authorized by the same entity.

Inter-domain handover. Inter-domain handover occurs when the mobile moves between two administrative domains. The mobile is also subjected to inter-subnet handover, as two different domains exclusively have two different subnets. Thus an Inter-domain handover will by-default be subjected to inter-subnet handover and in addition it may be subjected to either inter-technology or intra-technology handover.

Inter-technology handover. An inter-technology handover occurs when a mobile terminal moves between different access technologies.

Intra-domain handover. When a terminals movement is confined to movement within an administrative domain it is called intra-domain movement. An intra-domain movement may involve intra-subnet, inter-subnet, intra-technology and inter-technology as well.

Inter-link mobility. Mobility between access points belonging to different IP links. This kind of mobility involves Layer 3 mechanisms, so Inter-link mobility is also called inter-subnet mobility.

Intra-link mobility. Mobility between wireless access points within an IP link. Typically, this kind of mobility only involves Layer 2 mechanisms, so Intra-link mobility is also called intra-subnet mobility.

Intra-technology handover. An intra-technology handover is defined when a mobile moves between the same type of access technology.

IPsec. Architecture to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments.

Localised mobility. Mobility over a restricted area of the network topology. Although the area of network topology over which the MN moves may be restricted, the actual geographic area could be quite large, depending on the mapping between the network topology and the wireless coverage area.

MIPL. Mobile IP Layer.

Mobile Node (MN). A node that can change its point of attachment from one link to another, while still being reachable via its home address.

Mobility Service Authoriser (MSA). A service provider that authorises Mobile IPv6 service.

Mobility Service Provider (MSP). A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and prove authorisation to obtain the service.

Network Address Translation (NAT). It is a solution based on the address reuse to face the IP address depletion issue.

Network Access Server (NAS). A system that provides access to a network.

NETSNMP. Implementation of the SNMP protocol.

Next Steps in Signaling (NSIS). The Next Steps in Signaling framework provides protocols for signaling information about a data flow along its path in the network.

NAT/Firewall NSIS Signaling Layer Protocol (NSLP). NSLP allows hosts to signal on the data path for NATs and firewalls to be configured according to the needs of the application data flows.

PDA. Portable Digital Assistant. Generally, a PDA is a small portable device that works as an organizer.

Quality of Service (QoS). Network service framework to provide better quality parameters to specific network flows.

Roaming Broker (RB). An entity that provides (global) services for Home Entities and Hotspot Operators by operating as an intermediary and trading broadband access between them at a fixed or transactional price (buying and re-selling roaming airtime usage), and performs clearing and settlement services. Brokers may provide centralized authentication services in order to compute and validate the broadband traffic.

Serving Home Agent (sHA). In the HA relocation procedure, the sHA is the HA currently serving the MN to be replaced by the designated HA (dHA) during a HA relocation event.

SIM. Subscriber Identity Module. A SIM card is a small memory chip that is inserted into a mobile phone handset and is required for the phone to talk to the network operator. The chip contains a unique ID (known as an IMSI) that network operator uses to identify the user and the handset to the network.

Simple Network Management Protocol (SNMP). Protocol for network management.

SP. Service Protocol.

Split scenario. A scenario where mobility service and network access service are authorised by different entities. This implies that MSA is different from ASA.

Type-Length-Values (TLV). Specific attributes in a protocol message describing the type, length and value of a specific parameter. This kind of parameters are typically used in EAP.

UMTS. Universal Mobile Telecommunications System. UMTS is a next generation network for mobile communication. UMTS is a 3G network (3rd generation) and is the successor of the 2nd generation GSM.

UWB. Ultra Wide Band. UWB is a technology for transmitting information spread over a large bandwidth that should, in theory and under the right circumstances, be able to share spectrum with other users.

VPN. Virtual Private Network. It is a hardware/software solution for remote workers, providing authorised users with a data-encrypted gateway through a firewall and into a corporate network.

WMAN. Wireless Metropolitan Area Network, is used to describe a large network that covers a broad metropolitan area such as an entire major city.

xDSL. The different variations of Digital Subscriber Line (DLS).