Deutsche Telekom Laboratories
An-Institut der Technischen Universität Berlin

Opinion Paper on "Mobility and Quality of Experience in an IPsphere Environment"

Hans J. Einsiedler, Rui L. Aguiar, Jose Ignacio Moreno, Alexandre Brito, Rubén Gálvez Carranza, Gregorio López López,

White Paper No. 2
July 2009

Abstract and Keywords

This technical report discusses the challenge of defining the location of different kind of hand-over mechanisms (mobility) and Quality of Experience (QoE) concepts in the reference strata model of IPsphere. This reference model goes along with the current overlay architectures in standardisation (NGN, NGMN, IMS) as well as in the research communities (Daidalos). Mobility and QoE are important mechanisms to provide satisfying services in a Mobile and Future Internet. Especially mobility has different variations such as inter- and intra technology hand-over or inter- and intra-domain hand-over, device and session mobility. Mechanisms such as Mobile IP, which is located between the network layer and the transport layer in the Internet Protocol stack, can not satisfy al these variations. On the other side, the provisioning of QoE (end-to-end QoS) over a multi-provider environment is still under discussion, e.g. in the IPsphere project. A possible solution besides the IPsphere Overlay is presented in this technical report.

Index Terms: Hand-over, mobility, Quality of Service, Quality of Experience, end-to end Quality of Service, inter- and intra technology hand-over, inter- and intra-domain hand-over, device mobility, session mobility, multi-provider environment, multi-service provider environment. Three strata model, IPsphere.

Status	Participants
Public	**Not restricted.**

Disclaimer: The technical report is an opinion paper of the authors. The authors want to stimulate a discussion. This report does not claim to be exhaustive, e.g. SA4C (Security, authentication, authorisation, accounting, auditing, charging) and its combination are not part of it.

“Only connect” from E. M. Forster (1879-1970), Howards End, Epigraph

Table of contents

1 Introduction

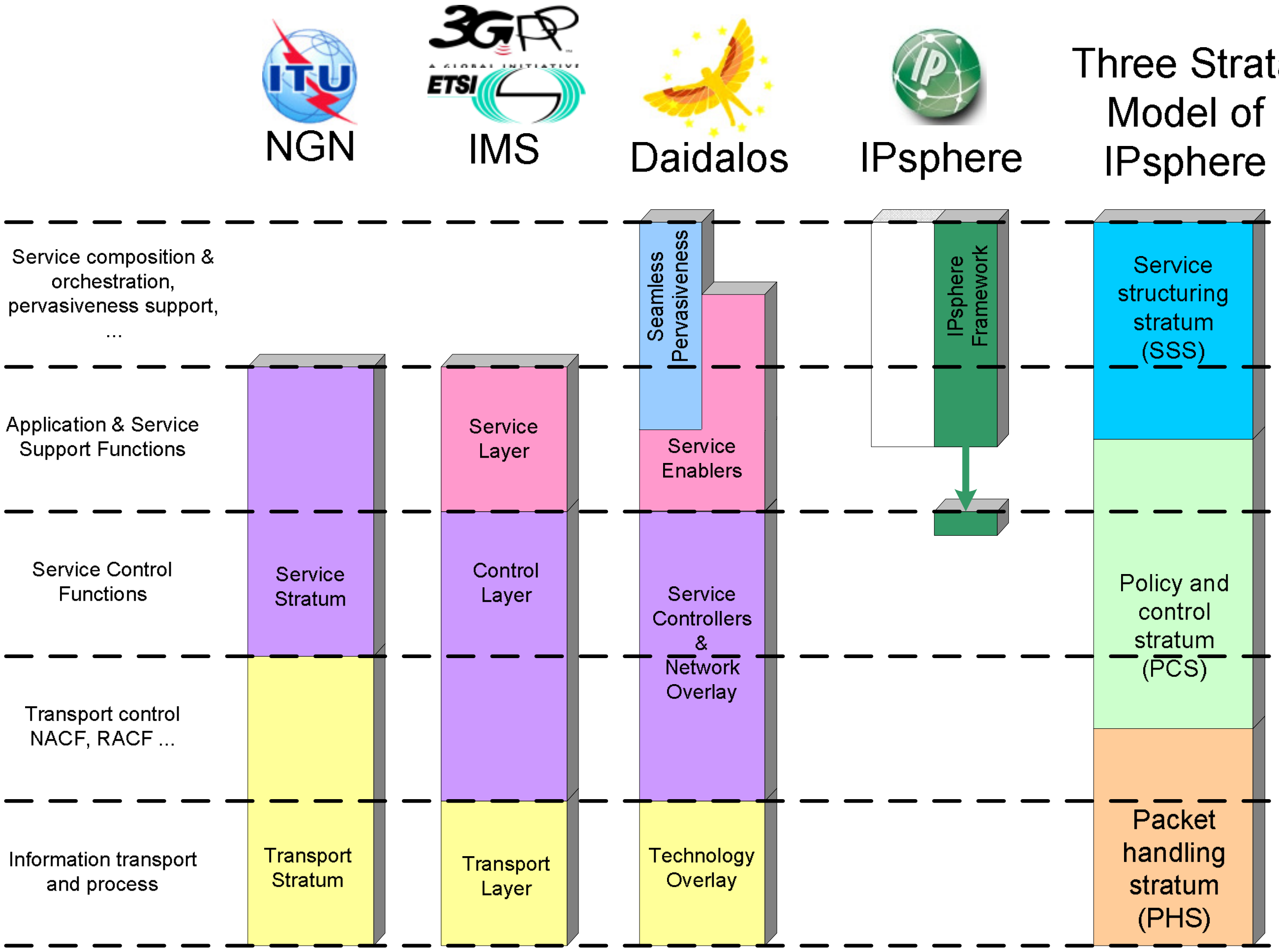

Figure 1: IPsphere Forum reference strata model in comparison to other reference architectures

Mobility and Quality of Experience are intensively discussed topics in the research world today. They are important basic blocks for the future telecommunication environment and very important for future business, costomer relationships, and competition.

This document analysis those challenges in a scenario driven approach and will highlight the difficulties, components, and technologies. The document will also provide some proposals to solve the listed challenges. Heterogeneous technologies, mobility in inter/intra domain scenarios or Quality of Experience across different operators are some of the scenarios.

Basis of the scenarios are the strata model [1] of the IPsphere Forum [2], which became a project in the Telemanagement Forum [3] framework.

The IPsphere reference architecture is related with the OSI layer model concepts but its origin is really a reflection of operational realities. In each stratum some of the OSI layers might be present. Depending on the functionality of the stratum, the strata have a certain strength or weight. There is no requirement for the three strata on two different operators to be similar – as long as the relevant inter-operator interfaces are respected.

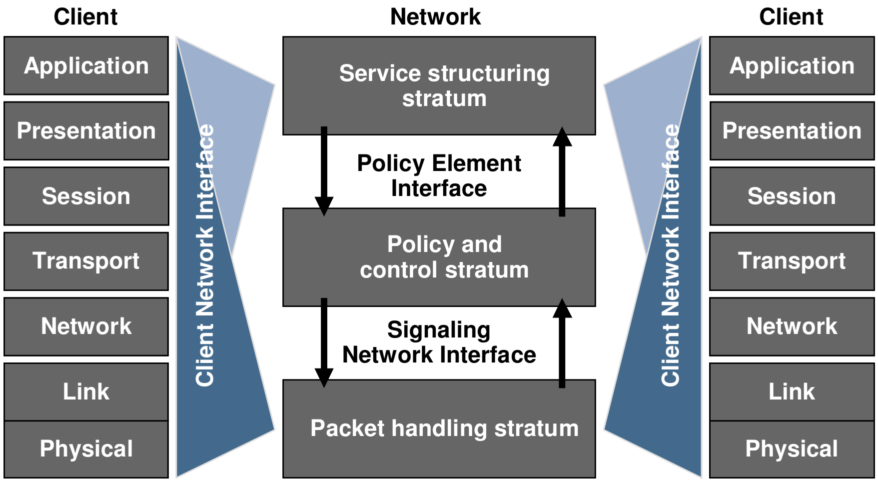

Figure 2: IPsphere Forum reference strata model and architecture

The Packet Handling Stratum (PHS) is the responsible for handling incoming and outgoing packets (routing, switching, forwarding queuing, etc.), in fact reflecting the reality that a given overlay will have some physical infrastructure support. The Policy and Control Stratum (PCS) is in charge of aspects related to resource allocation and tracking ensuring the reliability, security, and availability in the network. The specific control environment between operators is performed in the Service Structuring Stratum (SSS – originally called Service Signalling Stratum [1]). Current specification work of IPsphere is centred on this stratum, where the service abstraction and composition take place [4] in the logical overlay established across operators.

Overlays seem to operate along these lines – at least most of them act without detailed knowledge of the lower or upper layers. The IPsphere Forum reference model explored this by introducing a “Policy Element Interface” and a “Signalling Network Interface”.

The strata model can be used to identify the location of other layered overlay architectures such as the NGN [6], IMS [5], Next Generation Mobile Network (NGMN, most probably a sub-set of IMS) [7], Daidalos [8], and of course the IPsphere Forum overlay architecture.

We will continue in the Section with some basic definition and requirements. Section 3 will focus on mobility, where Section 4 will cover Quality of Experience. Finally, the document will close with a Conclusion part.

2 Definition of actions and terms

2.1 Basic definitions

Service definition: Set of functional capabilities negotiated between two or more entities/parties[1]. E.g. IPTV, VoIP, VoD.

Session definition: Single instantiation of a service in which a subscriber uses those functional capabilities. E.g. someone is watching IPTV, someone is talking with a friend using VoIP, and someone is watching a movie on demand.

2.2 Hand-Over Triggers

There are different reasons to perform a hand-over, such as:

- The terminal moves out of coverage.
- A new Point of Attachment (PoA) is found.
- A terminal is moved out of a cell because other terminals with higher priority get in the cell (Network Initiated Hand-Over).

2.3 Mobility Management

In this part, several ways to manage the mobility of the terminal among different operators will be defined. Firstly, in Figure 3 the first option is shown. In this case, as the device moves from one operator network to another, but the device communicating with it directs the data to its Home Domain (HD). The user data is forwarded from the previous operator to the one the user moves. This procedure will be repeated each time it changes the operator through which it is accessing the network, so at the end the operators will form a forwarding chain.

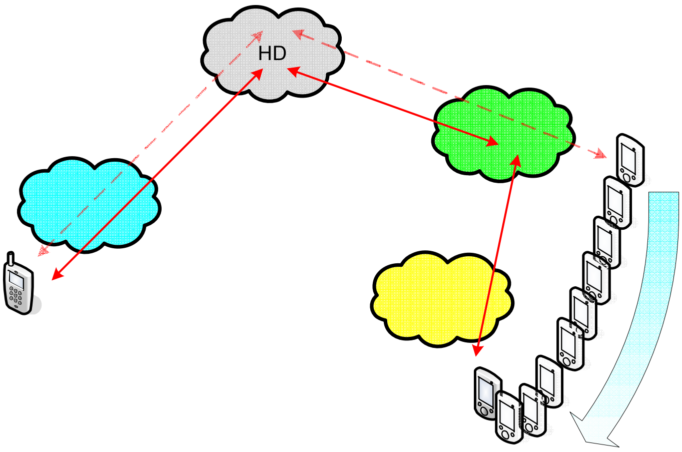

Figure 3: Mobility management type 1, forward chaining subtype.

A special case of the previous type can be considered when there is no chaining at all as depicted on Figure 4. The traffic in the reverse direction will still traverse the same path than the forward traffic. However, there will be no path reserved between the HD and another operator if the moving user is not at its network. Each time the device changes the HD will tear down the path reservation done with the previous operator and establish another one with the new domain of the moving terminal.

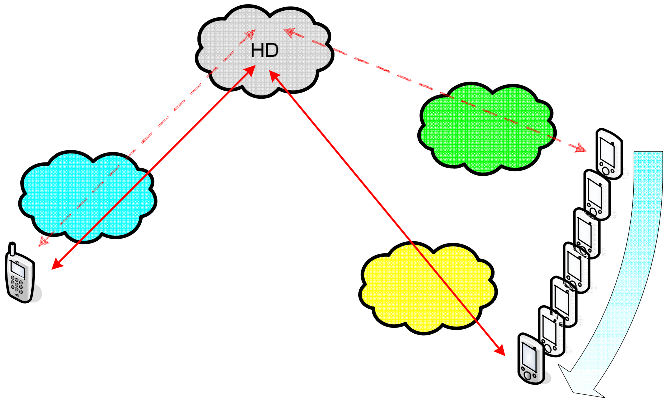

Figure 4: Mobility management type 1, not chaining subtype.

Another type comes up when considering a direct backwards communication. It will be possible as the moving terminal knows exactly where the other is, as that device was the one contacting it. In the first subtype, Figure 5, a forward path chaining will be established.

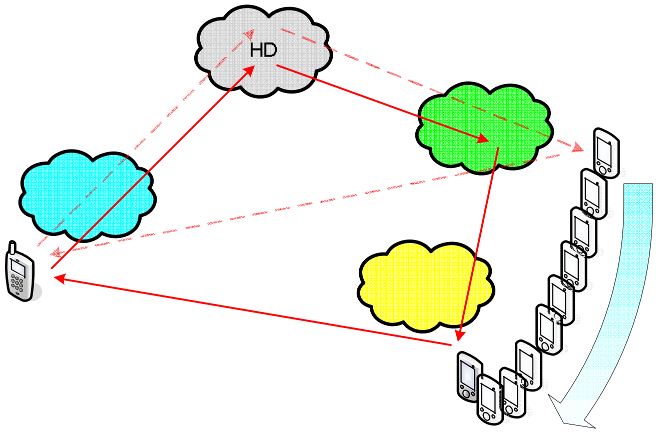

Figure 5: Mobility management type 2, forward chaining subtype.

A subtype of the previous one comes up when the path chaining is not established, but the direct backwards communication is still used as it is shown in Figure 6.

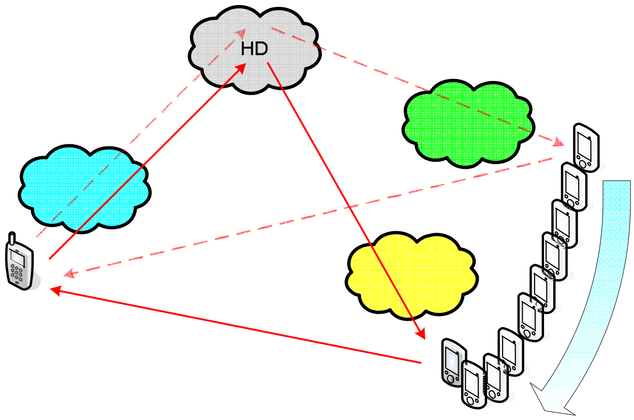

Figure 6: Mobility management type 2, not chaining subtype.

Another type of mobility can be identified when there is a direct communication between the current domains of both terminals using the “Route optimization” to remove the triangle loop, Figure 7. One of the previous types will be established initially (typically the type 2 not chaining subtype). But then, after both domains know which the other is, the direct communication can be established.

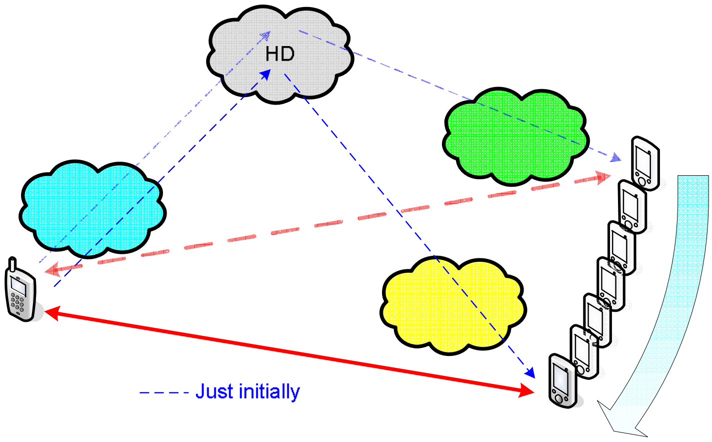

Figure 7: Mobility management type 2, not chaining subtype.

A particularly procedure should be taking into account when having a forward chaining type to avoid useless loops. When the moving terminal comes back to a previously visited domain, this domain must detect it and, to avoid those loops, it should free the previous forwarding path and deliver the data directly to the user. The operators involved in the previous chaining should be notified about this situation and must free the path as well.

3 Mobility Study

3.1 Intra-domain Scenarios

3.1.1 Scenario 1

A user terminal (device) performs a hand-over between two PoA belonging to the same technology (e.g. from a Wi-Fi PoA to another Wi-Fi PoA, from an UMTS Node-B to another UMTS Node-B).

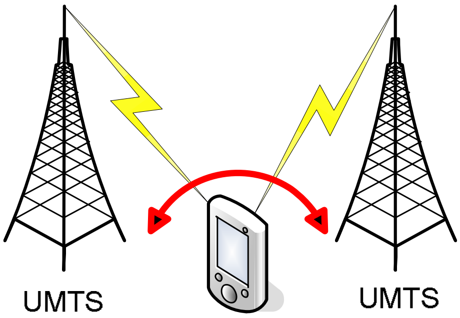

Figure 8: Intra-technology hand-over.

This will be a Layer 2 (Link-Layer) hand-over. The terminal will perform an authentication process towards the new access point because the terminal moves out of the coverage of the associated access point. In the same time the terminal enters the coverage of a new access point. After a successful authentication in the new PoA, the device will disassociate from the old one and associate to the new. The session will be moved from one PoA to the other. Then, it will de-authenticate himself from the previous PoA, and the hand-over is performed successfully.

SUMMARY:

- **Authentication of the device towards this new PoA.**
- **Session transfer from the old PoA to the new one.**
- **De-authentication from the first PoA.**
- **Disassociation of the terminal from the previous PoA.**
- **Association to the new PoA is finished.**

3.1.2 Scenario 2

A device performs a hand-over between two PoA belonging to different technologies (e.g. from a Wi-Fi PoA to an UMTS Node-B).

Strata Model Match

Mechanism	Stratum
Security Authentication	Managed entirely by the PHS
Registration	PCS
Network address allocation	PHS
Network address management	PCS
Association/Disassociation	PHS
Data transport	PHS
Session transfer	PHS

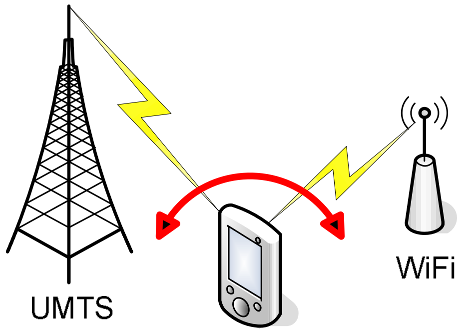

Figure 9: Inter-technology hand-over.

In this case, different technologies are involved in the hand-over processing. This will be a Layer 3 (Network-Layer) handover, because the network address may change or any action to keep the same one in a different network may be needed. The example where the network address will not change can be when using mobile IP, changing the Care-Of-Address and maintaining the Home Address. An external operator or service provider will reach the user with the same old IP address, the Home Address.

In this case, the terminal must associate firstly with the new PoA to be used. Then, it will de-authenticate from the first access network and perform an authentication in the new one. After this authentication is done, the communication will continue maybe with an interrupt or seamlessly. At this moment the network address may be changed or maintained. Finally the terminal will disassociate from the first PoA.

SUMMARY:

- **Authentication of the terminal towards the new PoA.**
- **Resource reservation and user profile storage at the new access network.**
- **The network address management mechanisms are performed.**
- **Session transfer from the old PoA to the new one.**
- **De-authentication from the first PoA.**
- **Free resources and user profile deletion in the previous access network.**
- **Disassociation of the terminal from the first PoA.**
- **Association to the new PoA is finished.**

Strata Model Match

Mechanism	Stratum
Security Registration Authentication	PCS
Network address allocation	PHS
Network address management	PCS
Association/Disassociation	PHS
Data transport	PHS
Session transfer	PCS

3.1.3 Scenario 3

A user moves the session from one device to another (e.g. a user transfers a movie from the TV to the PDA).

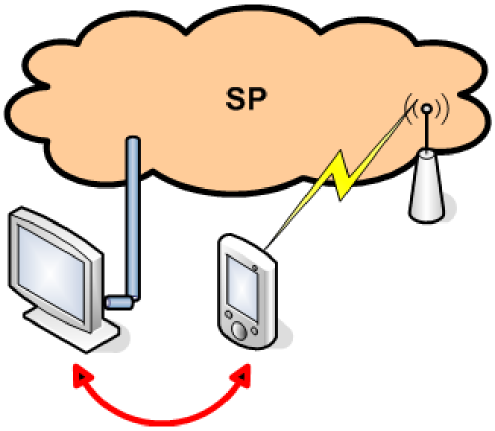

Figure 10: Service moves between devices

In this case the action of the user cannot be predicted as in the previous scenarios where the device loses signal from one PoA and gains on another, or the user is moved to another PoA due to network requirements.

Therefore, the user changes from a device to another one. Depending on whether the service parameters are affected by the change of terminal or not, the hand-over management mechanisms will reach up to the SSS level. The PHS and PCS cannot handle this type of mobility by its own, even if the access technology being used is the same, because the link layer address of the device will change, and the network address may change as well.

The user is authenticated at its first device. Any time afterwards the user will authenticate itself at another device. The user will be de-authenticated automatically at the first one. After this, the PCS will free the resources the user had until that moment at the first access network and reserve the new ones the user needs from now on in the new access network.

The PCS, through PHS, will also unbind the user from the previous link layer address and bind him to the link layer address of the new device. It will delete the user profile and information at the first Access Network (AN) and it will store it at the new AN. After this, a network address management mechanism would be triggered to allow the final mobility enforcement avoiding other relevant entities in the process to notice about the change. Now the user will continue receiving the service.

There will be only one difference with respect to the previous example if any service parameter changes: the mobility management will reach the SSS level as the service needs to be modified. In this case the SSS will modify the service properly and inform the PCS about its new characteristics in order to configure the network allowing service provision continuity. The overall management is done in the SSS because service parameters may change or the new access network is under control of another network provider.

SUMMARY

- **The user authenticates in a new device.**
- **If any service parameter needs to be modified, it will be modified and then enforced.**
- **Resource reservation and user profile storage at the new access network being used.**
- **Network address management mechanisms will perform the needed tasks to allow the mobility be enforced at the PHS level.**
- **Free resources and user profile deletion from the access network he was connected**
- **The user is automatically de-authenticated in the first device.**

Strata Model Match

Mechanism	Stratum
Security Registration Authentication	PCS
Network address allocation	PHS
Network address management	PCS
Association/Disassociation	PHS
Data transport	PHS
Session transfer	PCS
Service modification and negotiation	SSS

3.2 Classification criteria

In order to figure out what kind of mobility we have in each scenario, the following logic is used. We take into account two cases: **session** and **device**. In each scenario, we want to answer the following questions:

- What is moving?
- What is changing?

Those will be done from the **user perspective** and from the **network perspective.**

3.2.1 Scenario 1

From the **user perspective**:

- The session **is not** moving.
- The device **is** moving from one PoA to another.

From the **network perspective**:

- The session **is not** moving.
- The device **is not** moving.

The hand-over is transparent for the network, since it is handled at PHS.

3.2.2 Scenario 2

From the **user perspective**:

- The session **is not** moving.
- The device **is** moving from one PoA to another (different access technologies).

From the user perspective, this scenario is the same as Scenario 1.

From the **network perspective**:

- The session **is** moving from one technology to another. In this scenario, the network may have to perform some tasks to aid the hand-over.
- The device **is not** moving.

3.2.3 Scenario 3

From the **user perspective**:

- The session **is** moving from one device to another, i.e. the user is moving its session from a device to another.
- The device **is not** moving, but changing.

From the network perspective:

- The session is moving from one device to another. Even if both devices are using the same access technology, the network will realize that the session is moving since some parameters such as the network addresses or resource requests may change.
- The device is not moving, but changing.

3.3 Types of mobility

Taking into account the reasons described in 3, we can distinguish two different types of mobility based on what is moving.

- **Device mobility**: the device moves from one PoA to another.
- **Session mobility**: a session moves from one device to another or from one access technology to another. Since by definition a session is linked to a subscriber, this kind of mobility may be also named as User mobility (i.e. the user moves its session from one device to another).

From the **user perspective**, scenarios 1 and 2 are examples of device mobility and scenario 3 is an example of session mobility.

From the **network perspective**, scenarios 2 and 3 are examples of session mobility and there is not mobility at all in scenario 1.

3.4 Inter-domain Scenarios

3.4.1 Scenario 4. Inter-domain Device Mobility.

In this scenario, a user keeps on consuming a given service using a given device across two different telecom operators.

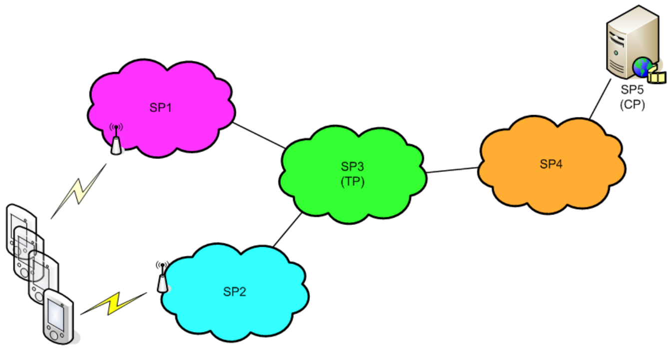

Figure 11: Inter-domain Device Mobility.

From the user perspective:

- The session **is not** moving.
- The device **is** moving from one PoA to another.

Therefore, this is an example of Device Mobility.

Let us have a look from the **network perspective**. In order to do so, some key mechanisms involved in this use-case are going to be identified and explained.

1. The device has to **authenticate** itself in the new PoA belonging to SP2. The Home Domain is SP1. First the user has to **register** in SP2, which in turn involves a **user's authentication** procedure (**security**). Therefore, SP2 has to ask SP1 for the user's credentials2 This inter-domain communication will be enabled by the SSS.

2. Since the device is moving across network operators, its network address will change. However, the terminal will be able to keep both **network addresses** associated to the same interface until the stream can be delivered through the new path. There are different solutions to manage this issue that will impact in different ways the operators' perspective (section 2.3).

   2.1. The terminal has to signal its new network address to its Home Domain. The Home Domain will redirect the stream to the new location of the user. As it is shown in Figure 12, data traffic will traverse SP3 through two different paths. The one that connects SP4 and SP1 was already allocated. However, the path that connects SP1 and SP2 has to be established. This requirement will be signalled using the SSS. SP2 will be informed about the new session through SSS as well. Within this approach, both SP1 and SP3 realize that the session is moving, for SP2 a new session is starting and for SP4 and SP5, nothing changes.

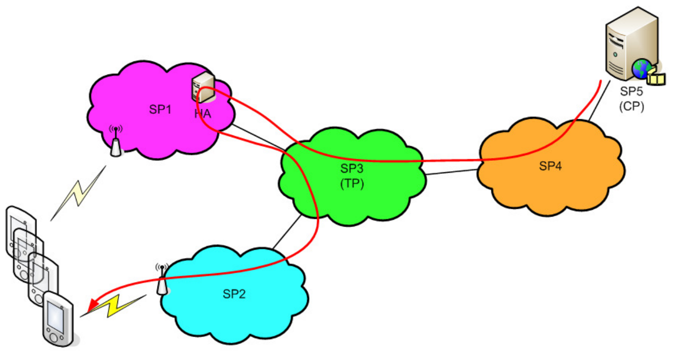

Figure 12: Communication done through Home Domain.

2.2. The device sends its new network address to the CP (end-to-end signalling). As a result, the CP (SP5) has to change the destination network address. As it is shown inFigure 13, SP3 has to set up a new path between SP4 and SP2 and tear down the one that connects SP4 and SP1. Again, this process will be enabled by the SSS. Within this approach, for SP1 the session finishes, for SP2 a new session starts, for SP3 the session moves and for SP4 and SP5, nothing changes since this movement is hidden to them by SP3.

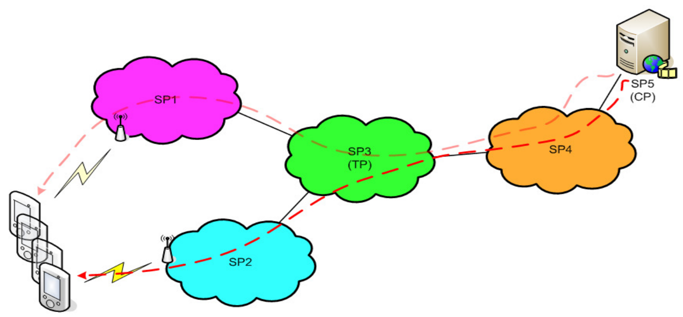

Figure 13: End-to-end signalling.

3. In all the situations explained above, resources must be allocated for the new path (**resource allocation**). These requests will be exchanged using the SSS, as it has been already mentioned.
4. Once the new path is established, the terminal has to **disassociate** from the SP1 PoA and associate to the SP2 PoA.
5. Then, it can start receiving **data** through the new connection.
6. Finally, it has to release the resources allocated for the session through the previous path (**resource deallocation**).

SUMMARY:

- **Registration in the new domain (SP2). User's Authentication and Security.**
- **Network address management**
- **Resource allocation for the new path.**
- **Disassociation from SP1 PoA.**
- **Association to SP2 PoA.**
- **Communication through the new path.**
- **Release resources associated to the previous path.**

Strata Model Match

Mechanism	Stratum
Security Registration Authentication	Enabled by SSS Performed at PCS
Network address management	Enabled by SSS Performed at PCS
Resource allocation/Deallocation	Enabled by SSS Performed at PCS Enforced at PHS
Association/Disassociation	PHS
Data transport	PHS
Accounting	PCS
Billing/Charging	SSS

3.4.2 Scenario 5. Inter-domain Session Mobility.

In this use case a user watches a movie on a smart cell phone while coming back home. At home, the user decides to keep on watching the movie on the TV.

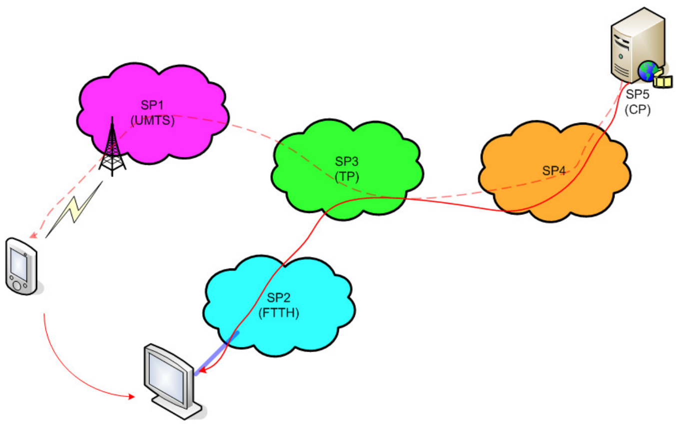

Figure 14: Inter-domain Session Mobility.

From the user perspective:

- The session **is** moving from one device to another
- The device **is not** moving, but changing.

As a result, this situation is an example of Session Mobility.

From the **network perspective**, the analysis is the same as in section 3.4.1. However, since the device is changing, some **presentation parameters** such as codecs may also change. Regarding this issue we can distinguish two different situations:

1. The required changes are included in the service definition. In this case, if the service is delivered by a SP on its own, the required operations are performed at PCS. However, in pan-provider services, these new parameters may need to be negotiated at SSS.
2. The required changes are not supported by the service. As a result, since the functional capabilities change, a new service is needed.

SUMMARY:

- **Registration in the new domain (SP2). User’s Authentication and Security.**
- **Network address management**
- **Presentation parameters negotiation.**
- **Resource allocation for the new path.**
- **Video streaming through the new path.**
- **Disassociation from SP1 PoA.**
- **Release resources associated to the previous path.**

Strata Model Match

Mechanism	**Stratum**
Security Registration Authentication	Enabled by SSS Performed at PCS
Network address management	Enabled by SSS Performed at PCS
Presentation parameters (e.g. codec)	Enabled and performed by SSS
Resource allocation/de-allocation	Enabled by SSS Performed at PCS Enforced at PHS
Association/Disassociation	PHS
Data transport	PHS
Accounting	PCS
Billing/Charging	SSS

Note that if the functional capabilities change the service change. For instance, if the user watches the movie on its PDA that does not support High Definition TV and when the user arrives at home the user wants to keep on watching the movie on her High Definition TV, the service will not be the same. In this case, a new service has to be established.

3.5 Daidalos types of mobility in our model

Interface mobility is actually device mobility.

User mobility is actually session mobility.

Scenarios 5 and 6 are examples of Daidalos service mobility. As a result, from the user perspective, **service mobility** could be mapped to device mobility or to session mobility in our model. On the other hand, from the network perspective, the analysis depends on the SP.

4 Quality of Experience Study

Quality of Experience study pretends to identify the main processes and mechanisms to perform QoS session across heterogeneous domains based on scenarios and use cases.

The study is divided in two parts:

1. Intra-domain study
2. Inter-domain study

At the end of the chapter we pretend to identify the main procedures to enable true end to end QoS across different domains and point out the main challenges.

4.1 Next Steps and Other Vision

In [1] and in [11] the current QoS challenges are well described. QoS Premium services which represent the latest years attempts to define a solution for QoS over the Internet, is now losing power and influence. The Internet2 QoS Group (http://qos.internet2.edu), which objective is to support the development and deployment of advanced network applications through the use of IP traffic differentiation, dedicated several years of research on Premium Service. In May 3, 2008, the group release an officially announcement with the results of 3 years research:

"The costs of Premium (Service) are too high relative to the perceived benefits. Moreover, even if successfully deployed, Premium (Service) fundamentally changes the Internet architecture, running contrary to the end-to-end design principle, and threatening the future scalability and flexibility of the Internet. The conclusions reached herein apply not just to Premium, but to any IP quality if service (QoS) architecture offering a service guarantee."

In today's times, a new approach is been taking in account in parallel with Premium Services solutions. The Less than Best Effort (LBE) vision pretends for users voluntarily accept QoS with no guarantees. Both perspectives are compatible with our study and impact greatly with the architecture of NGN networks.

4.2 Intra Domain Study

4.2.1 Video on Demand with QoS

In Figure 15, a simple video download with QoS enable where both end points of a session share the same domain in an inter-technology scenario.

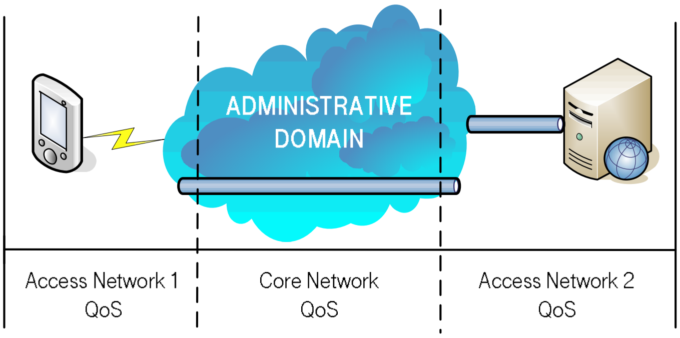

Figure 15: QoE basic intra domain scenario

In this scenario, network addresses are maintained and assigned by the network domain to both devices. The same applies in terms of QoS Classes, meaning that QoS parameters are managed by the network domain as well.

The main challenge on this scenario is to provide QoS across different Access networks. Different technologies implements different QoS mechanisms. Therefore, mapping procedures between QoS signalling and QoS enforcement differs from technology to technology as, for instance, from 802.11e (QoS on WiFi) to WiMAX. Emerging standard 802.21 enables QoS translations through heterogeneous technologies providing a suitable solution for this scenario.

When a QoS session is activated, the following occurs:

1. Application requests for specific QoS parameters
2. QoS Client at the terminal receives application QoS parameters and translates it to a QoS request accordingly to access technology
3. QoS Server at the AN translates the client QoS request to network QoS request
4. QoS negotiation for the Core Network
5. QoS enforcement at both AN and Core Network
6. Monitoring and accounting
7. Billing and charging

NSIS [13] or RSVP [14] or even SIP [15] protocols and DSCP marker field, for instance, provides QoS templates for QoS signalling and classification.

The network architecture management and control overlay provides the necessary mechanism to perform the accounting. Billing and charging are under the control of the service overlay.

4.2.2 Voice over IP Call

Figure 16 shows a VoIP call between two terminals with QoS enable.

In this intra-technology scenario, the same mechanisms are applied as the previous scenario. However, two new points must be discussed:

- Intra-technology
- Bidirectional QoS session

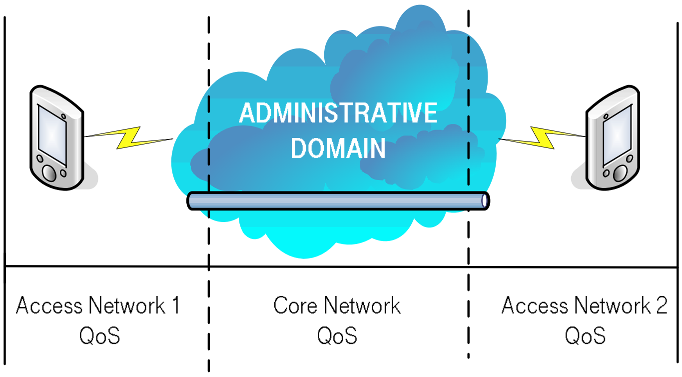

Figure 16: Both directions QoS session

Fine-grained flow specs must be translated to DSCP classes for QoS aggregation proposes. QoS parameters such as, packet loss, jitter, latency and bandwidth will be translated to corresponding class. Each session on the AN will have a specific QoS requirements (fine grained QoS) while at the CN sessions will be aggregated. The major challenge resides at the AN since they are the bottlenecks of the system. Monitoring millions of reservations at the AN is, currently, one of the key challenges to provide QoS to the size of Internet.

On the matter of the bidirectional QoS session, for instance a VoIP call, typically two reservations are established and associated. In practical terms, the network reserves two sessions while the management overlay keeps tracks of the association (two unidirectional QoS setup). This is another key challenge to provide QoS: Two unidirectional QoS under different conditions and possible different domains.

SUMMARY:

- **QoS translation**
- **QoS negotiation at AN and CN**
- **Management overlay for billing and charging**
- **Inter/intra technology is not relevant**

Strata Model Match

Mechanism	Stratum
AN QoS link parameters negotiation	Performed at PHS
CN QoS link parameters negotiation	Performed at PCS
Terminal QoS Translation	Performed at PHS
AN QoS Translation	Performed at PHS
CN QoS Translation	Performed at PCS
QoS Enforcement	Enforced at PHS
Accounting	Performed at PCS
Monitoring	Performed at PCS
Billing/Charging	Performed at SSS

4.3 Inter Domain Study

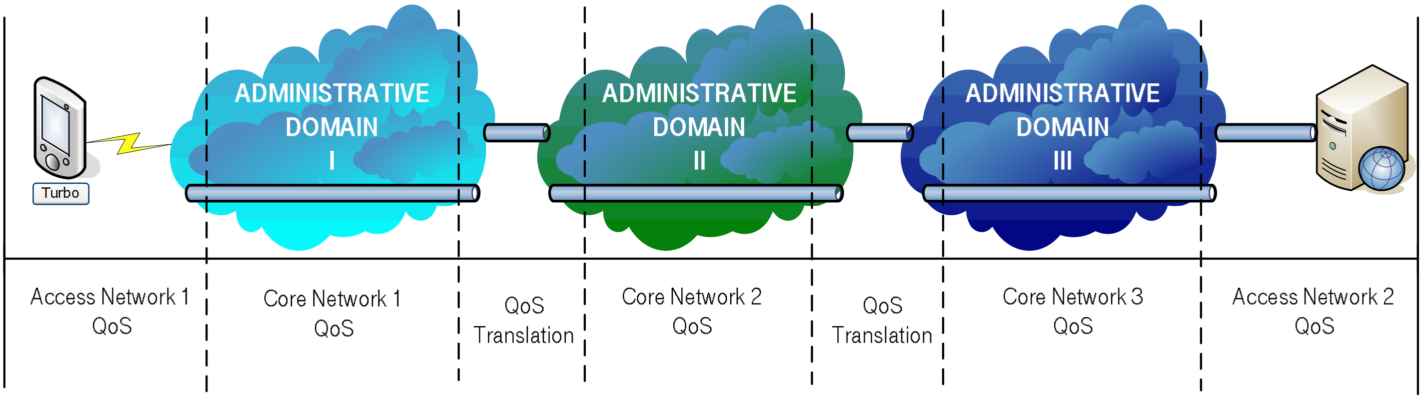

Figure 17: QoE inter domain scenario

In Figure 17it is shown a simple video download across different domains with QoS.

The scenario is similar to Figure 15 in terms of Access Networks QoS provision. However QoS translation between different domains (i.e. across different Core Networks) introduces a new challenge.

Following this description, we will now study the scenario. It is similar to the intra-domain case, however, in bold the major differences are identified.

When a QoS session is activated, the following occurs:

1. Application requests for specific QoS parameters
2. QoS Client at the terminal receives application QoS parameters and translates it to a QoS request accordingly to the access technology
3. QoS Server at the AN translates the client QoS request to network QoS request (IntServ)
4. QoS negotiation for the Core Network
5. QoS translation between different domains including server side (Access Network 2)
6. QoS negotiation between different domains including server side (Access Network 2)
7. QoS Enforcement
8. Monitoring and accounting
9. Billing and charging

Point 4 will detect an inter-domain QoS Session, triggering an inter-domain negotiation process.

Points 5 and 6 will translate and negotiate QoS parameters across different domains. Each domain is responsible for QoS provision at its own Core Network including the Access Network 2.

Point 7 installs the translated QoS at the different domains and Access Networks.

Point 8 adds validation, monitoring and accounting of the QoS installation across the different domains.

Point 9 adds billing and respective revenues for the transit domains when charging the QoS session.

4.3.1 Inter-domain challenges

The major challenges of the scenario are:

1. QoS translation between different domains
2. Provide QoS validation, monitoring, accounting and charging across different domains without relying on global trust system (domains cooperation)
3. A common QoS protocol would have to be widely implemented across all domains to enable true end2end QoS without a global negotiation framework
4. Provide QoS in a routing proof manner, which means to provide QoS able to sustain route change (and this way, not compromising the Internet routing based on destination against routing based on the source)

IPsphere Framework is working on a solution for points b) and c) and even point a), by defining a service management plane to enable service negotiation, validation, monitoring, billing and charging across different heterogeneous domains, based on simple templates. In this model, most elements of the network can be viewed as services, and QoS is a suitable example. IPSF separates network plane from service plane, by abstracting the QoS network parameters. The parameters are related to a QoS requirement template shared between different domains.

The IMS and Daidalos Frameworks addressed these issues by defining standardized templates and communications procedures to transmit QoS parameters across different domains with the same architecture, with accounting, billing and charging.

IPsphere Framework enables the possibility to implement similar solutions across different heterogeneous domains.

Point d) is still a major challenge with no consensual solutions. Routing engineering offers the possibility the manipulated traffic in function of latency, link load, jitter and any other parameter. However such technology introduces a relative amount of complexity to the network. While inter-domain path optimization is relative well research, still today it is not deploy. Its relative simpler to adjust the path costs and even if routing engineering was efficient enough to justify the investments, it would be required a global effort by the operators for the inter-domain scenarios.

SUMMARY:

- **QoS translation and negotiation between different Access Networks**
- **QoS translation and negotiation between heterogeneous domains including the Core Networks**
- **SLAs validation and activation**
- **Distributed charging (and billing)**

Strata Model Match

Mechanism	**Stratum**
AN QoS link parameters negotiation	Performed at PHS
CN QoS link parameters negotiation (SLA negotiation)	Enabled and Performed at SSS
Terminal QoS Translation	Performed at PHS
AN QoS Translation	Enabled at PCS Performed at PHS (e.g. IEEE 802.21)
CN QoS Translation	Enabled at SSS
QoS Enforcement	Enforced at PHS
Accounting	Performed at PCS
Core Network Monitoring	Performed at PCS Enabled at SSS
Billing/Charging	Performed at SSS

4.4 The Turbo Button scenario

4.4.1 Intra Domain

In the intra-domain scenario, the QoS established between the terminal and the content provider is unsatisfactory for the user. The user presses the *Turbo* button to improve the QoS session.

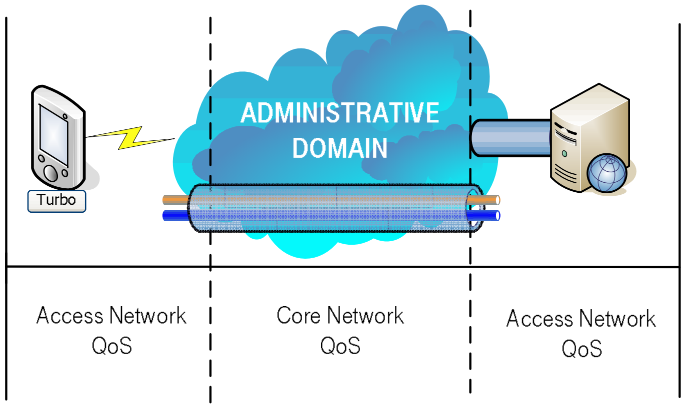

Figure 18: Turbo button in a intra domain scenario

At this point, the network must verify the conditions of the network and alter policies:

- bandwidth at the AN for the re-allocation QoS request
- bandwidth at the CN for the re-allocation QoS request
- marks packets for higher priority
  - (1) terminal/AN marks packets
  - (2) network marks packets (see 4.1)
- QoS Routing
  - (3) using the same link, but with priority queues
  - (4) different routes for different QoS (traffic engineering)

Accounting, billing and charging follow the same principles of the previous scenarios.

SUMMARY:

- **Traffic engineering and/or QoS queues change**

Strata Model Match

Mechanism	**Stratum**
Queues Change	Performed at PHS Controlled by PCS
Traffic engineering	Performed at PHS Controlled by PCS

4.4.2 Inter Domain

For the inter-domain scenario, the challenge complexity increases. The re-allocation request will trigger basically the same mechanisms as the allocation request (QoS negotiation for the Access Network, Core Network, and Inter Domain operators). However, the session must not be interrupted.

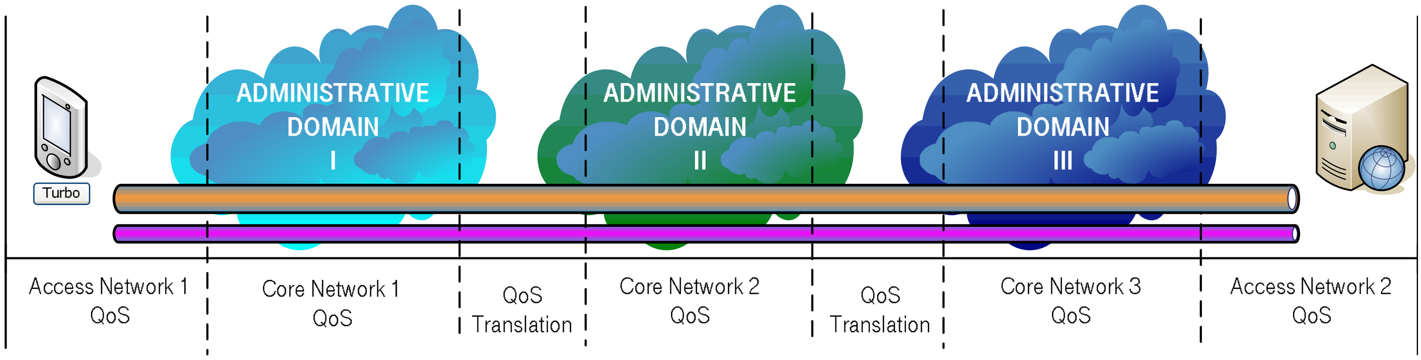

Figure 19: Turbo button in a inter-domain scenario

Two possibilities to deal with the session modification are enlisted:

1. The current session is terminated and a new session is initiated.
2. The current session is ‘upgraded’.

Point 1 implies that a current session and the new session do not necessary represent the same session. A make-before-break similar to mobility events could enable this type of QoS enhance. A management overlay (as IPSF) would prepare the trunk through the different operators and at the end of the process the ‘new’ session would be installed. Traffic/routing engineering can and should be avoided by defining different QoS queues. For the content provider application this process would not be transparent, since signalling for tear down session and new session would have to be taken into account.

In Figure 19, pink tube and orange tube represent different queues with different parameters.

Point 2 leads to a change of the queuing parameters on the fly. Similar to Point 1, traffic/routing engineering should not take place. The session would remain the same. A management overlay would still be necessary to propagate and monitor the QoS modification throughout the different domains. Since the content provider QoS application controls the QoS, it would still be aware of the change.

Other relevant issue is the QoS path resulted from the change. A QoS session can be upgraded to a better QoS class maintaining the same path, or changed to different and more appropriated path. The latter option requires routing engineering which is still a hot topic as explained on section 4.3, point 4.

SUMMARY:

- **QoS inter-domain negation**
- **Traffic engineering and/or QoS queues change**

Strata Model Match

Mechanism	Stratum
Queues Change	Performed at PHS Controlled by PCS Enable by SSS (in an abstract way)
Traffic engineering	Performed at PHS Controlled by PCS Enable by SSS

4.5 Overload Scenario

In this scenario, terminal A arrives at a saturated access network (in red) and tries to initiated a new VoIP call to terminal D. Terminal B is connect to the saturated network but is also covered by another AN (in green) while terminal C is only covered by AN in green.

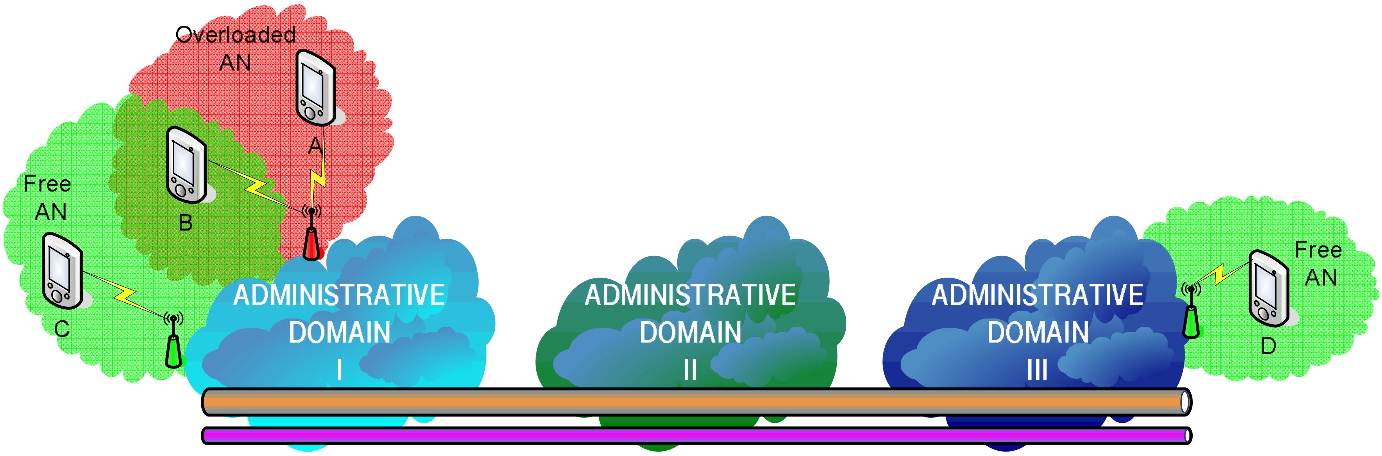

Figure 20: Overload scenario

In order for the terminal A be able to initiate a QoS session, the following actions are possible:

- A Network Initiated Handover (NIHO) would be trigger and move terminal B the other AN (terminal mobility with session refresh). Terminal B can represent best effort users or other QoS Session (as long as the new AN can also provide QoS)
- Best effort users would be dropped (possibly terminal B)

The NIHO for terminal B would be transparent for the inter-operators if an inter-domain session was ongoing.

Accounting, Billing and Charging follows the same principles of the previous scenarios.

SUMMARY:

- **Bandwidth monitoring**
- **Costomers QoS plan and QoS triggers**
- **Network Initiated Handover**

Strata Model Match

Mechanism	Stratum
Access Network monitor	Performed at PHS
Network Initiated Handover	Performed by PHS
Session termination	Performed by PHS Enabled by PCS (notification)

5 Conclusions

In this technical report we defined a structured way to discuss the issues related to the location of mobility and Quality of Experience (QoE) mechanisms and protocols in the three strata model of IPsphere. This strata model can be seen as a reference model for mapping different architectures, which currently are discussed in standardisation and research towards a Mobile Internet and Future Internet.

The discussion is needed since mobility and QoE have different flavours, e.g. mobility in a single operator environment or single technology infrastructure or in a multi-operator/service provider environment. It is not possible to define one unique mechanism or protocol, which satisfy neither mobility nor QoE. Based on the reference model of the IPsphere project – the three strata model – and scenarios, we have defined different location for the different mechanisms and protocol and sub-sets of protocols. The scenarios covered intra- and inter-technology issues, intra- and inter-domain cases, session and device mobility, as well as typical scenarios such as Video on Demand, Voice over IP, and overload situations.

For each scenario the mechanism and the location in the three strata model was defined and discussed. This report does not claim to be exhaustive since SA4C (Security, authentication, authorisation, accounting, auditing, charging) and its combination are not part of it. This is work and material for further interesting discussions.

6 References

[1] T. Nolle, “A New Business Layer for IP Networks”, July 2005 Issue of Business Comunications Review, 999 Oakmont Plaza Drive, Suite 100, Westmont, IL 60559, 630/986-1432, http://www.bcr.com/ - http://www.ipsphereforum.org/Files/A%20New%20Business%20Layer%20for%20IP%20Networks%20-%20TN1.pdf.

[2] ”IPsphere Forum – the Business of IP”, http://www.ipsphereforum.org/, http://www.tmforum.org/IPsphereFramework/.

[3] “Telemanagement Forum (TMF)”, http://www.tmforum.org/browse.aspx.

[4] IPsphere Framework Technical Specification (Release 1). IPsphere Forum. March 2007.

[5] “IMS Subscription and access scenarios – 3GPP TS 22.800”, http://www.3gpp.org/ftp/Specs/html-info/22800.htm.

[6] ITU-T NGN Management Focus Group: NGN Management Specification Roadmap v3.1. March 2007.

[7] “Next Generation Mobile Networks Alliance”, NGMN, http://www.ngmn.org/.

[8] “Daidalos: Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services”, http://www.ist-daidalos.org/.

[9] R. Aguiar, H. Einsiedler, R. Karrer, “Daidalos: The Operator's Vision of the Next-Generation Internet”, IEEE INFOCOM 2006, Barcelona, Spain, April 23-29, 2006.

[10] Cisco Whitepaper about IntServ and DiffServ - http://www.cisco.com/en/US/products/ps6610/products_white_paper09186a00800a3e2f.shtml.

[11] A Nice Way to Get Network Quality of Service - http://www.oreillynet.com/pub/a/network/2002/06/11/platform.html.

[12] Internet 2 QoS Working Group, “Why Premium IP Service Has Not Deployed (and Probably Never Will)”, May 2002.

[13] NSIS IETF draft, http://www.ietf.org/html.charters/nsis-charter.html.

[14] RSVP Standard, http://tools.ietf.org/html/rfc2205.

[15] SIP Standard, http://tools.ietf.org/html/rfc2543.

7 Annex: Service Mobility

In this situation, let imagine that a given user talks with a friend using VoIP at work. During the conversation, the user leaves work, so it has to change its profile, what means a different user from the network point of view.

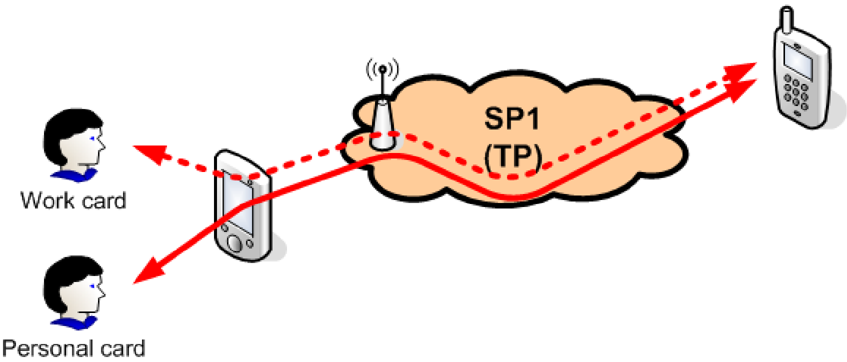

Figure 21: Service mobility scenario

- The service is moving from one user to another - Service mobility
- The session is not moving, but changing, since the user is not the same.
- The device is not moving. Eventually, it might change.

8 Table of figures

Publisher:

Deutsche Telekom AG
Laboratories
Ernst-Reuter -Platz 7
D-10587 Berlin
Telefon: +49 30 8353-58555
www.laboratories.telekom.com

Authors: Hans J. Einsiedler, Rui L. Aguiar, Jose Ignacio Moreno, Alexandre Brito, Rubén Gálvez Carranza, Gregorio López López