Business and Management Challenges for End-To-End Reconfiguration

Nancy Alonistioti, Zachos Boufidis, Nikos Houssos, Makis Stamatelatos [(1)],

[(1)] *Communication University of Athens, Athens, Greece*

E-mail: {nancy, boufidis, nhoussos, g.stamatelatos}@di.uoa.gr,

Abstract

Reconfiguration technologies have an increasing role in the evolution of mobile system towards heterogeneous ubiquitous infrastructures. The present contribution initially discusses business model aspects for reconfigurable systems and services. Furthermore, it elaborates on advanced reconfigurability functionality, in the form of an innovative Reconfigurability Management Plane, which addresses the coordination of the end-to-end reconfiguration process in next generation wireless networks.

1. Introduction

The convergence of the Internet, 2G/3G mobile communication systems, and wireless networks at the device, transport, and service level creates new business opportunities for incumbent business players and newcomers. Customers want operator-independence, service continuity and dynamic personalised discovery and execution of services via on-demand software download, in a ubiquitous communications environment [1]. To the end of flexible service offerings and to cope with complex systems, the need for end-to-end reconfigurable architectures, systems, and functions is emerging [2]. Business models in the mobile world seem to evolve due to such technological opportunities: in a reconfigurable context, new business actors with updated roles and relations emerge.

Reconfiguration spans across devices, network equipment, software, and services. Target reconfigurable nodes include, in the mid-term, the User Equipment (UE) and Base Stations or Access Points. Signal-processing modules in the UE as well as firmware enhancing the Hardware Abstraction Layer (HAL) can be upgraded. Operational and non-operational software can be downloadeded [3]. Service and content adaptation have already started to gain attention in the mobile world, promising on-the-fly playout adaptation via, for example, download of upgraded codecs. In the long-term, internal network nodes such as routers and switches or even (parts of) the network itself could be reconfigured, especially for large user groups requesting specialized treatment.

Within this context, the EU FP6 Integrated Project IST-E²R (End-to-End Reconfigurability) [4] aims to devise, develop and trial architectural design of reconfigurable devices and supporting system functions to offer an expanded set of operational choices to the users, application and service providers, operators, and regulators in the context of heterogeneous mobile radio systems.

End-to-end reconfiguration dictates the design and specification of a new management plane for coordinating the interactions between the involved business entities, and for enabling the decision-making and enforcement of mechanisms supporting reconfiguration in a dynamic fashion. In [5], the Reconfiguration Management Plane (RMP) is proposed, whose main task is to provide layer abstractions to applications and services on one hand, and to terminal equipment and network devices on the other. Furthermore, the RMP is responsible for the coordination of the reconfiguration process and for the provision of the required resources. In this paper, we streamline the identified plane management functional entities with layer management functions and identify key challenges for policy-based reconfiguration differentiation.

The rest of the paper is organized as follows. The business domains and actors for end-to-end reconfiguration are sketched in Section 2, and the constituent RMP functional entities are described and elaborated in Section 3. We conclude and describe future work on the evolution of business models, on

the specification of the RMP, and on accomplishing the differentiation of reconfiguration services in Section 4.

2. Business Model Domains and Actors for Reconfigurable Communication Environments

Legacy stakeholders for the provision of reconfiguration services include the regulator, the manufacturer, the telecom operator (either home or visited), the service provider, and the user. In this section, we identify the generic business roles undertaken by business actors, as well as the demarcated business domains for advanced reconfiguration services and management (Figure 1) [6][7][8].

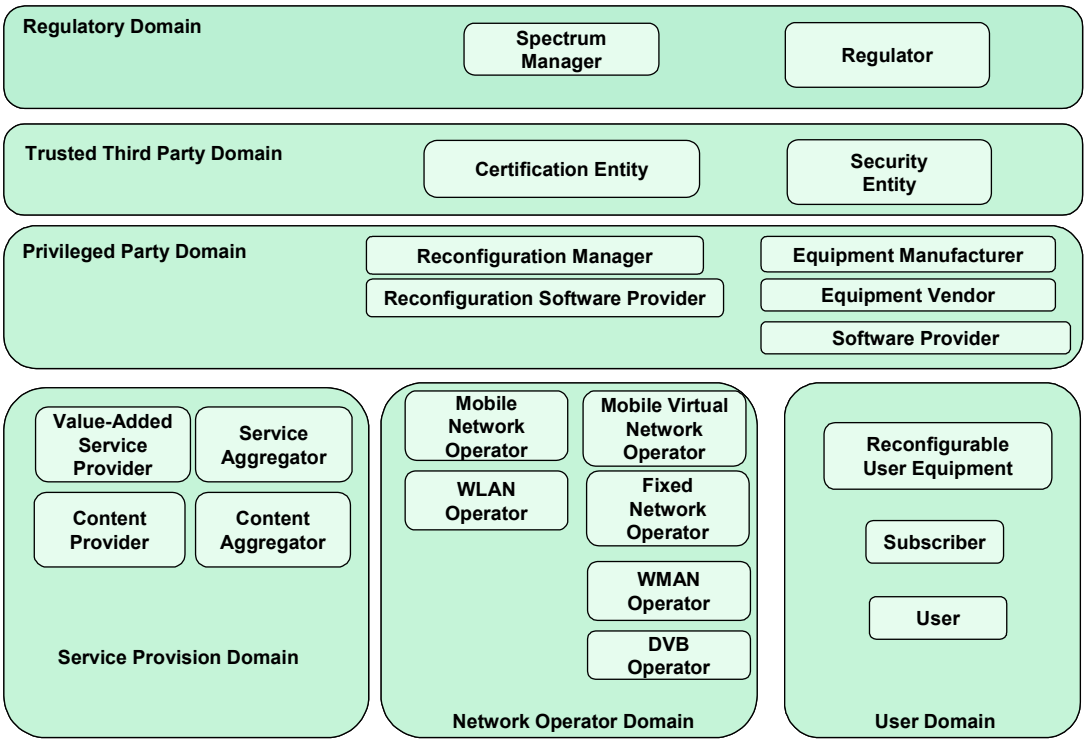

Figure 1: Generic business model domains and entities for end-to-end reconfiguration

2.1. Regulatory Domain

The Regulatory domain includes regulation and spectrum management authorities. Multiple *Regulator Entities* set the legal environment for the mobile business growing, via laws and guidelines that determine the operation of the system.

The *Spectrum Managers* coordinate the approval, allocation, exchange, sharing, and loan of spectrum. Special care should be taken for spectrum loan or leasing in case of activation of a Mobile Virtual Network Operator (MVNO).

2.2. Trusted Third Party Domain

The Trusted Third Party (TTP) domain includes trusted actors for special actions such as security and certification. The *Security Entities* guarantee the security of intended reconfiguration processes. Additionally, they guarantee overall protection against end-to-end security threats. For example, they guarantee the integrity, validation, and authenticity of origin of the downloaded software. Under the supervision of a Regulator Entity, these actors are responsible for issuing, revoking, and managing security credentials and public keys for data encryption and signing. The *Certification Entities* certify the conformance of the protocol parts to respective standards.

2.3. Privileged Party Domain

The Privileged Party domain includes providers and manufacturers targeting the reconfiguration market, as well as special-purpose entities that may not reside within the Trusted Third Party domain.

Software Providers develop and/or distribute software modules. A specialisation of this role can be defined as *Reconfiguration Software Providers* that develop and/or distribute software modules to execute on reconfigurable network elements and user equipment.

The *Equipment Manufacturers* design and manufacture the terminal equipment, base stations, etc. and supporting software for entities residing in the Service Provision, Network Operator, and User domains. In a reconfigurable system, the equipment must conform to standards developed by various bodies or to rules imposed by regulation authorities.

Equipment Vendors market and distribute the equipment (e.g., mobile terminals, base stations) that is to be used in the *Service Provision, Network Operator* and *User* domains. They can also distribute software modules for these products acting as a Reconfiguration Software Provider. This entity is envisioned for future exploration and investigation.

The *Reconfiguration Managers* are responsible for management issues related to triggering and initiation of reconfiguration actions, as well as for the coordination between multiple administrative domains where reconfiguration decisions are delivered and enforced. In addition, these entities cater for interactions between actors residing in various business-level domains, such as Service Aggregators, Certification Entities, Operators, and Equipment Manufacturers.

2.4. Service Provision Domain

The Service Provision domain encompasses Value-Added Service (VAS) Providers, Content Providers, and Service Aggregators.

The *VAS Providers* provide advanced services for which additional charges may be incurred such as web-based or downloadable services.

The *Content Providers* create the content (e.g., multimedia streaming files) and maintain repositories which are made available to VAS Providers, or to Users via VAS Providers.

Content Aggregators collect content from various sources (content providers) and aggregates/packages it in a meaningful way so that it is more conveniently discoverable and accessible or more usable for interested parties (e.g., VASPs) than the data retrieved directly from content providers.

The *Service Aggregators* mediate between VAS Providers, Mobile Network Operators, and Users keeping them aware of the available services. The Service Aggregators may also provide service profiles according to their content, localization, terminal capabilities, and subscriber profile.

2.5. Network Operator Domain

The Network Operator Domain includes actors that provide the bearer communication infrastructure for transit services, service provision, and reconfiguration capabilities.

Network Operator (NO): Represents the main actor in this domain. The NO has the responsibility for the smooth operation of the network infrastructure through which end user connectivity is accomplished. The NO is in fact an abstract class of actors. It is instantiated by specific operators for different network technologies (e.g., cellular, WLAN, DVB) as presented in the subsequent paragraphs.

Mobile Network Operator (MNO): provides radio resources, mobility management and fixed capabilities to switch, route and handle the traffic associated with the services offered to users by itself and/or by service providers.

The *Mobile Virtual Network Operator (MVNO)* may be considered a special case of Mobile Network Operator. MVNOs offer network connectivity services, but do not have their own spectrum allocation or radio access network infrastructure. To provide network access to their customers, they buy/rent network capacity belonging to a mobile network operator and usually also include additional services to their offerings. An MVNO may possess a distinct mobile network code, issue its own (U)SIM cards and operate proprietary cellular core network infrastructure. In this case, the capacity bought/rented from a mobile operator concerns only the radio access network.

The *DVB Operator* provides audio/video/data content related to video broadcasting services in terms of the stationary and portable reception of video data. Because of the increasing demand for mobile reception and the migration of communication and broadcasting, e.g. in the area of multi media communications, it is of importance for the operator to analyse the capabilities, but also the limitations of the available DVB-T/DVB-H system operated in a mobile environment.

The *Fixed Network Operator* provides telecommunications services to fixed subscribers. Its infrastructure can also be used for transport by other network operators.

The *WLAN Operator* provides its customers with high-speed wireless connectivity over WLAN networks (e.g., 802.11), typically offering them Internet access at hotspots such as hotels, airports, enterprises, exhibitions, convention centers or even coffee shops, etc.

The *WMAN Operator* provides high-speed access to wireless users in a metropolitan area through technologies such as 802.16 and LMDS.

2.6. User Domain

The user domain consists of individuals or groups that are subscribed to communication services, of users who possess account to subscribed services, and of reconfigurable equipment for accessing the offered services.

The *Subscribers* are the entities engaged in a static or dynamic subscription with one or more Fixed or Mobile Network Operators, as well as with VAS and Content Providers.

Multiple *User* accounts can be created, in which case all charges are billed to a single subscriber. Conversely, different subscribers can share the same device for short periods by exchanging their SIM cards.

The *Reconfigurable Equipment* is the reconfigurable devices used to provide access to communication services.

3. Reconfiguration Management Plane

The Reconfiguration Management Plane aims to set the grounds for integrated plane management and layer management support functions. Traditional *plane management* embraces configuration control, resource management, performance management, fault management, access and security management, and accounting management [9]. Traditional *layer management* necessitates the existence of interfaces to all protocol layers both in the control and in the user plane. Layer management handles Operation and Maintenance (O&M) functions per layer.

In reconfigurable environments, additional functional entities should be specified. As part of a new plane, RMP functional entities reside both in network elements and in the terminal equipment. The additional RMP entities are described below (Figure 2).

3.1. A. Plane Management Functions

The *Context Management* functional entity monitors, retrieves, processes, and transforms contextual information. Contextual information includes profile information as well as resource-specific information regarding the reconfiguration progress, the operational mode, state information, congestion indication, etc. Contextual information affects the service provision phase, and provides input to policy decisions and reconfiguration strategies.

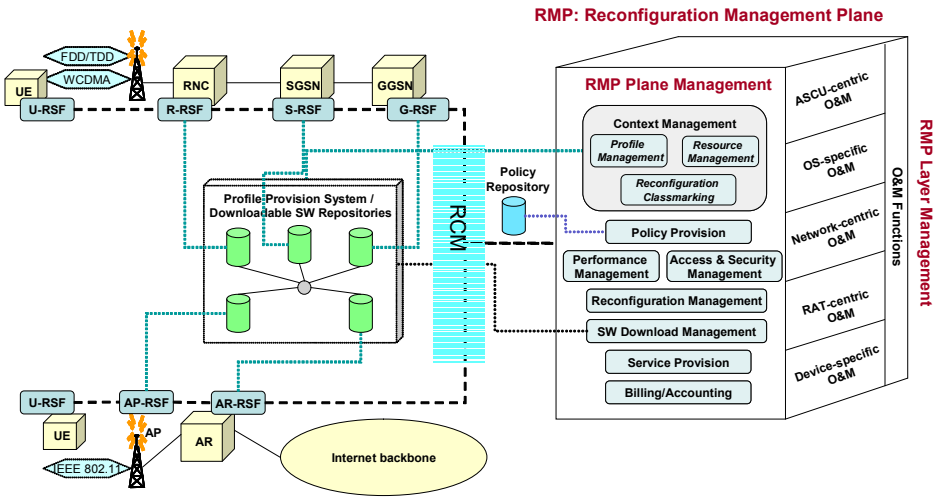

Figure 2: The Reconfiguration Management Plane in a Beyond 3G Mobile Network

Profile definition and provision is handled by a dedicated RMP functional entity, namely the *Profile Management* entity, which manages and combines the different profiles. Profile information originates from different parts of the system, and includes user profile, network profile, application/service/content profile, terminal profile (the so-called Reconfiguration Classmark), charging profile, security profile, and so on. The collection of profile repositories in a reconfigurable beyond 3G system should be viewed as a composite *Profile Provision System (PPS)*. The PPS should apply to an n-tier system capable of disseminating profile management policies into an n-layered architecture. The multi-tier architecture can be constructed based on topological considerations and/or on semantic aspects. Segmentation and distribution of profile data representation via *profile staging,* and a two-dimensional (topology-based) multi-tier (semantic-oriented) hierarchical organization of profile managers should offer performance and flexibility benefits.

The *Reconfiguration Classmarking* entity keeps track of the different nodes of the network and their state regarding reconfiguration, e.g., the protocol versions that are installed. Each terminal is assigned a *Reconfiguration Classmark*, which specifies the level of dynamism regarding reconfiguration, and the capabilities of the terminal (e.g., enhanced MExE classmark). The calculated value of the classmark depends on the type of reconfiguration requested and negotiated, on the type of software to be downloaded, on business incentives, and on individual or operational chains of stakeholders involved in the reconfiguration process.

The *Policy Provision* functional entity is the main decision-making entity for reconfiguration, by comprising the entry point for reconfiguration-related system policies. Furthermore, it exploits contextual information and redefines policy rules and reconfiguration strategies. This functional entity produces an up-to-date decision about the feasibility of a reconfiguration as well as respective actions to be triggered. In addition, the Policy Provision function caters for inter-domain issues, interacts with Policy Enforcement Points, and facilitates the mechanics for end-to-end reconfiguration differentiation.

The *Reconfiguration Management* function initiates network-originated and coordinates device-initiated configuration commands, by communicating with peer Configuration Control Modules of the terminal equipment. In order to accomplish the supervision of end-to-end reconfiguration, it incorporates the signalling logic, including *trading and negotiation* services. In the case of scheduled software download, the Reconfiguration Control function hands-over the control of the residual reconfiguration steps to the Software Download Management function.

The *Software Download Management* function is responsible for identifying, locating, and triggering the suitable protocol or software for download, as well as for controlling the different download steps prior to, during, and after download. The target software will be fetched by the appropriate repository under the control of a Reconfiguration Support Function (RSF).

The *Service Provision* functional entity is responsible for the interaction between the RMP and the application/service. This entity accepts and processes reconfiguration requests for the network in order to provide the necessary environment for an application and service to execute. In addition, it provides

feedback to the application for the feasibility of the request, and can initiate a reconfiguration command on behalf of the application. For example, it can initiate network configuration changes or selection of different settings by the users, or it can initiate mobility-related actions. In addition, the Service Provision function may trigger service adaptation actions based on network or device capability modifications, or based on updated policy conditions. Finally, roaming issues for service provisioning are also tackled by the Service Provision functional entity.

3.2. Layer Management Functions

In order to accomplish end-to-end reconfiguration, traditional layer management functions should be enhanced and collaborate with RMP plane management functions. For example, functions for O&M can be exploited for the service provision stage, and should be adapted based on input related to the definition and enforcement of reconfiguration policies. End-to-end differentiation of reconfiguration services should also take into account the outcome of reconfiguration functions for O&M, such as monitoring reports and capabilities of network elements.

O&M functions can be classified to five categories (Figure 2): Application-, Service-, Content-, and User-centric (ASCU) functions; OS-specific; Network-centric; RAT-centric; Device-specific.

Provision of customer care information is a typical example of *ASCU-centric O&M* function. Logging is an important feature, offering the history of reconfiguration actions (e.g., recent OTA upgrades), statistical information on the latest faults and alarms reported to the user, etc.

OS-specific O&M functions should coordinate the auditing, testing, and validation procedures at the Reconfigurable User Equipment.

Network-centric O&M functions address the impact of mobility and QoS on the software download process. In addition, dynamic network planning and its impact on traffic split comprise important O&M functions for reconfigurable network elements.

RAT-centric O&M functions manage RAT-specific issues for a single Radio Access Technology or guarantee efficient collaboration of multiple RATs. The *Composite Radio Environment Management* function handles stability, conflict resolution, and certification issues, and ensures proper collaboration between network infrastructure manufacturers and terminal providers. The *Radio Element Management* functional entity cooperates with the *Performance Management* RMP plane management functional entity. Analysis of RAT-specific performance data is an example of performance management, which may in turn affect real-time reconfiguration. The *Function Partitioning and Reallocation* entity coordinates coupling issues as well as distribution of functional entities for multi-RAT environments owned by a single administrative authority. Finally, the *Interworking* function verifies the correct operation of control plane functionality between radio elements owned by different operators, as well as network sharing scenarios.

Device-specific O&M functions include, for example, functions for User Equipment Management. Although security hazards exist, *remote equipment diagnosis* assists in the remote identification of equipment faults. Coordination with HAL configuration modules can also be accomplished through device-specific RMP O&M functions.

4. Conclusions

We presented an evolved business model encompassing new domains and actors for end-to-end reconfiguration. Apart from legacy stakeholders in the User, Network Operator, and Regulatory domains, we envisage new business players in the Service Provision and Network Operator domains, such as Service Aggregators and the Mobile Virtual Network Operator, respectively. We identified the necessity of Trusted Third Party entities, and in addition, we raised the importance of privileged actors that undertake part of reconfiguration and security management tasks. Future work in this area includes convergence with business models for the provision of telematics services [10] and incorporation of additional actors and roles for emerging scenarios such as in-car software download.

In order to support end-to-end reconfiguration, we proposed an integrated plane management and layer management framework, and identified and described the major required functional entities. In the next stages of our research, we will specify and model the RMP functional entities using the Specification and Description Language (SDL) or the Unified Modelling Language (UML).

Future work on differentiation of policy-based reconfiguration services includes a target switching mechanism between pure Service-Based Local Policy (SBLP) - which exploits the COPS protocol and

PDP context modification procedures -, native IP QoS signalling, and IP QoS signalling tailored to SBLP [11]. Finally, since the IETF Policy Framework [12] does not address inter-domain or end-to-end policy control, our next steps include research on collaboration of clusters of Policy Decision Points (PDPs) via a supervising entity that interfaces with the RMP Policy Provision functional entities of multiple administrative domains. An alternative distributed solution through a coordination protocol between multiple PDPs should work as well. We will analyse the advantages and disadvantages of these inter-domain policy provision options from the required business incentives viewpoint, the network management aspect, and the associated technical implications.

5. Acknowledgements

This work has been performed in the framework of the EU funded project E²R. The authors would like to acknowledge the contributions of their colleagues from E²R consortium.

References

[1] IBM, "Autonomic Computing", http://www.research.ibm.com/autonomic
[2] M. Dillinger, K. Madami, and N. Alonistioti (Editors), Software Defined Radio: Architectures, Systems and Functions, John Wiley & Sons Ltd, 2003.
[3] The Software Defined Radio (SDR) Forum, http://www.sdrforum.org/
[4] IST-2003-507995 Project E²R (End-to-End Reconfigurability), http://e2r.motlabs.com/
[5] N. Alonistioti, Z. Boufidis, A. Kaloxylos, and M. Dillinger, "Integrated Management Plane for Policy-based End-to-End Reconfiguration Services", 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004.
[6] N. Houssos, V. Gazis, A. Alonistioti, “Enabling delivery of mobile services over heterogeneous converged infrastructures”, Kluwer Information System Frontiers Journal, Special Issue on "Network convergence: Issues, Trends and Future”, Vol. 6, No. 3, 2004, pp. 189-204.
[7] M. Alvarez, C. Pedraz, and M. Dillinger", "Business models for reconfigurable communication systems", 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004.
[8] M. Stamatelatos et. al, "Business Model and Actors for End to End Reconfigurable Systems", WWRF Meeting, Oslo, Norway, June 2004.
[9] 3GPP TS 32.101, "Telecommunication management; Principles and high-level requirements (Release 6)", June 2004.
[10] H. J. Vögel, "Telematics: Serving the (Auto) Mobile Community of the 21st Century", WWRF11 Meeting, Oslo, Norway, June 2004.
[11] 3GPP TS 23.207, "End-to-end Quality of Service (QoS) concept and architecture (Release 6)", June 2004.
[12] The IETF Policy Framework Working Group, http://www.ietf.org/html.charters/policy-charter.html