



WIRELESS WORLD

R E S E A R C H F O R U M

Requirements and Proposals for Networks of the Wireless World

WWRF WG3 (CoNet) Whitepaper

Authors: Frank Pittman (Siemens), Bengt Ahlgren (SICS), Bryan Busropan (TNO), Lars Eggert (NEC), Svante Ekelin (Ericsson), Anders Eriksson (Ericsson), Jens Gebert (Alcatel), Robert Hancock (Siemens), Martin Johnsson (Ericsson), Toon Norp (KPN/TNO), Börje Ohlman (Ericsson), Nick Papadoglou (Vodafone), Christian Prehofer (DoCoMo Euro-labs), Andreas Schieder (Ericsson), Mikhail Smirnov (Fraunhofer), Wilfried Speltacker (Lucent), Stein Svaet (Telenor), Philip Eardley (BT), Irena Grgic Gjerde (Telenor), Olavi Karasti (Elisa), Ulla Killstroem (Elisa), Astrid Solem (Telenor), Peter Schoo (DoCoMo Eurolabs), Marcus Brunner (NEC), Simon Schuetz (NEC), Johan Nielsen (Ericsson), Anders Gunnar (SICS), Henrik Abrahamsson (SICS), Robert Szabo (BUTE), Simon Csaba (BUTE), Rolf Stadler (KTH), Alberto Gonzalez (KTH), Gergely Molnar (Ericsson), Jorge Andres (Telefonica), María Ángeles Callejo (Telefonica), Lawrence Cheng (UCL), Alex Galis (UCL), András Méhes (Ericsson), Göran Selander (Ericsson), Mark Priestley (Vodafone), Petteri Pöyhönen (Nokia), Ramon Aguero (Unican), Cornelia Kappler (Siemens), Jan Markendahl (KTH), Georgios P. Koudouridis (TeliaSonera), Daniel Migault (FT)

Johan Nielsen (Ericsson, editor)

Abstract— Several large, multi-year projects around the world, such as the EU IST FP6 projects Ambient Networks and Daidalos, are currently researching and investigating how networks and systems for the future wireless world will look like. This whitepaper will present the results and findings being researched and developed within the EU IST FP6 project Ambient Networks.

This document describes the architectures for future networks of the Wireless World, starting with the high-level goals of the project and continues with the identification of the main technical requirements. This document aims to capture and identify the control functions and their interactions in a common format and define the architectural style for the overall architecture itself.

A key part of this document develops fundamental aspects of the overall architecture: the various facets of the composition concept and the framework within which the individual control functions are placed. This document describes the concept of a flexible, modular, open framework for organizing the control functions, its interfaces and encapsulations.



WIRELESS WORLD

R E S E A R C H F O R U M

Table of Contents

Requirements and Proposals for Networks of the Wireless World	1
WWRF WG3 (CoNet) Whitepaper	1
1 Introduction.....	3
2 Requirements on Networks for the Wireless World	6
2.1 Heterogeneous Networks	6
2.2 Mobility.....	6
2.3 Composition	7
2.4 Security, Privacy and Dependability.....	7
2.5 Backward Compatibility and Migration.....	7
2.6 Network Robustness and Fault Tolerance	8
2.7 Quality of Service.....	8
2.8 Multi-Domain Support	8
2.9 Accountability.....	9
2.10 Context Communications	9
2.11 Extensibility of the Network Services Provided.....	9
2.12 Application Innovation	10
3 Architecture and Components of the Ambient Control Space.....	11
3.1 Ambient Interfaces.....	12
3.2 Control Space Framework: Abstractions and Components	17
3.3 Description of Control Functions.....	28
3.4 Composition	58
3.5 Business aspects of dynamic composition	69
4 Conclusion	75
Acknowledgement.....	76
Abbreviations	77
References	79



WIRELESS WORLD

R E S E A R C H F O R U M

1 Introduction

Motivation and Goals of the Architecture of the networks of the Wireless World

There are already successful standards for mobile and wireless networking that address today's markets requirements and incorporate existing air interface technologies. However, the communications environment is changing – even today – sufficiently radically that new mobile networking concepts are required as a response. The most significant change is in the business environment. As this matures, we see companies in the mobile value chain focusing on particular activities, such service creation, marketing, or infrastructure operation. A similar trend is visible in the emergence of new access networks such as WLAN hotspots, which also presents new scaling problems, as the number of individual operators is larger by some orders of magnitude compared to the cellular world. This is part of a more general trend where services are provided over a range of different access networks, bringing the additional complexity of the need to offer the same services over radically different bearer types. Finally, the mobile world is extending into the private (enterprise, home and even personal) domains. As well as the issues of scaling and heterogeneity already mentioned, these developments create further difficulties for internetworking: the relatively open and unmanaged nature of these networks and the wide variation in business models will mean that traditional forms of inter-network agreement will no longer be sufficient.

Within the constraints imposed by existing architectures, we can consider many, relatively natural, stepwise extensions to particular network functionalities. However, the strategic objectives for the Networks of the Wireless World – particularly, to expand mobile networking into new environments by enabling new types of business models and deployment concepts – are a step beyond what is possible with such an incremental approach, and current system architectures are not able to adapt at the speed that the marketplace demands. This is increasingly acknowledged also from the Internet community in recent approaches to reconsider architectural principles of the Internet (see for example [37]) that has grown up in a totally different service and business environment than that which we face today.

The Networks of the future Wireless World requires a new style of networking, which must be founded directly on the economic and social objectives of the Wireless World. Several research projects, such as Ambient Networks [1], Winner [2], Spice[3], Mobilife [4], E2R [5] and Daidalos [6], are currently addressing how these networks of the wireless world will be built and what the requirements on them are.

The requirements work of the Networks of the Wireless World is described in section 2. In section 3 we show more in detail how these requirements can be realised in a case study. This case study is based on the Ambient Networks project [1]. The overall goal of this activity was to generate a set of outputs both to establish an intuitive understanding of the scope of the problem, and also to be used as material against which the architectural proposals can be validated. The primary input was the development of a set of user-centric scenarios, using participation from the widest variety of project participants, and looking at the role future networks will play in daily life in 2015 [1]. This necessarily speculative work was complemented with a nearer-term perspective by interviews with stakeholders in current mobile networks [1]. These inputs were then distilled into twelve top-level requirements, which are discussed in section 2.



WIRELESS WORLD

RESEARCH FORUM

The architecture of the Networks of the Wireless World is described in chapter 3. This work is mainly based on input from the Ambient Networks project [1] since the contributions to this whitepaper has been made from Ambient Networks. The overall process here has been to build a framework from a deliberately minimal set of abstractions, motivated by very general engineering design principles. Although this abstract framework has been aligned with the strategic goals of the project, it is not directly derived from the user requirements themselves. The scope of the architecture is defined in terms of a set of three interfaces described in section 3.1.

The framework for the Ambient Network functionality itself is given in section 3.2. It is described in terms of a coordinated set of control functions, collectively referred to as the Ambient Control Space (ACS), and the service interface which they support (ASI) and operate on (ARI). The framework includes rules for how network elements and entities within the control space are named and addressed. For the purpose of modelling, we also introduce concepts to represent the user plane data transport capabilities visible at the ARI and ASI; these concepts are referred to as the flow and bearer respectively. Finally, the framework provides certain core components that support registration and communication between control functions, and thus allow the ACS functionality to be adapted to local needs and to accommodate future innovations without redesign.

In addition to the framework itself, it is also clearly necessary to populate it with the concrete functionality required to support our mobile networking needs. This process was carried out in two stages. Firstly, high-level technical concepts were gathered from across the project and validated against the requirements already presented here. Following this activity, the technical concepts were refined into more specific functional areas according to the component template that could then be fitted into the architectural framework. While these components continue to evolve, the current status of this work is presented in section 3.3.

The final part of the architecture story is the concept of network composition. Our expectations about future mobile scenarios indicate that internetworking will play a pivotal role – between different operators, across technologies, business environments and more. The internetworking must preserve the enhanced functionality provided by the Ambient Control Space, and must scale to complex topologies involving hundreds or thousands of networks. The basic technique for addressing this challenging goal is to consider all networks as instances of a common Ambient Network building block – they all share the same set of basic interfaces – which can be combined into larger instances of the same type. This approach, network composition, provides for scalability and universality, but has many implications for the functionality of the Ambient Control Space and the Ambient Network interfaces. Possible mechanisms to support the composition concept have been studied in detail elsewhere; in this whitepaper, the implications of the composition concept for the rest of the Ambient Networks architecture are analyzed in section 3.4. Section 3.5 describes the business aspects of Composition rather than technical aspects. The intention of section 3.5 is also to indicate the business-related issues that are important to take care of when making an agreement and why they are regarded as important.

Section 4 is the concluding section of this whitepaper. It provides an overview of the main findings of this whitepaper and gives an indication of the challenges and next steps that will be addressed in the section year of the project.



WIRELESS WORLD

R E S E A R C H F O R U M

This document was initially based on the D-1.8 deliverable [9] produced within the scope of Ambient Networks but has been extensively and significantly updated, modified and extended with contributions from the Ambient Networks project.



WIRELESS WORLD

RESEARCH FORUM

2 Requirements on Networks for the Wireless World

This paragraph gives an overview of the 12 main general requirements on Networks for a Wireless World. The general requirements are related to the problems which networks for the “Networks for the Wireless World” have to overcome. The requirements address the question "what issues do we have to solve/improve?" with respect to the needs of the users of network technology and to the needed functionalities of the network. Users of network technology are operators, end-users and service providers. Certainly, some of these requirements are similar to requirements already found in networks like GSM/3G or the Internet. However, the requirements address or outline unsolved problems in today's networks and are therefore necessary to be fulfilled for networks for the Wireless World Networks. The twelve general requirements together as a set – and not necessarily per individual requirement - describe what distinguishes networks for the Wireless World from earlier technologies and what Networks for the Wireless World intend to deliver. We also shortly list what the consequences these requirements has on our case study.

2.1 Heterogeneous Networks

The architecture shall efficiently support different kinds of technologies to provide users with an optimal connectivity based on their requirements and preferences. Networks for the Wireless World must enable application- and service-independent end-to-end reachability in the global network environment. Network services and application services shall be provisioned independently of each other.

Consequences for the case study: Although not new, heterogeneity is one of the main properties of networks for the Wireless World. Furthermore, it hides the current (radio) access technology from the application process. Beside addressing heterogeneity of access and network technologies it also addresses the business heterogeneity of the service delivery chain.

2.2 Mobility

Networks for the Wireless World must support mobility management schemes for user, service, session, terminal and network mobility.

Their mobility management mechanisms should be able to locate and update the current location of the user and to support seamless mobility. Networks for the Wireless World should be capable to support both existing and new mobility mechanisms that enable terminals and networks to move around without being closely tied to so-called "home" networks. Real-time transfer of information flows must be supported.

Consequences for the case study: Mobility across different heterogeneous networks is important and imposes some constrains in the design of the network architecture. Specifically, it must be able to offer networks the flexibility to move to different physical or logical locations at any time. This in turn has some impact on the supported naming and addressing convention. A specific control function (naming) is needed to deal with allocation, registration and if necessary translation of names as well as resolving them to physical addresses (locations, end-point IDs.)



WIRELESS WORLD

RESEARCH FORUM

2.3 Composition

The network architecture shall support mechanisms that achieve on-the-fly negotiations and agreements across different administration domains.

Consequences for the case study: Composition is a new feature introduced. The control space of a network shall be responsible for conveying and establishing the information in order for the various networks to compose (or better form) one network. With this requirement, we introduce the concept of real-time network negotiation and agreement of services. A network for the Wireless World could be formed from many such networks and look as "one" to the outside world, but without losing its identity or capability to connect to other networks with its original identity.

2.4 Security, Privacy and Dependability

Networks for the Wireless World must provide a seamless, comprehensive and flexible security scheme that operates consistently across a dynamically changing environment of constituent heterogeneous networks, component entities and services. This embedded network security shall cover a multiple network-operator/service-provider environment that is characterized by:

- user friendliness and helpfulness, while remaining as far as possible invisible to the user,
- smooth transition between different accesses and services,
- trustworthy operation,
- robustness and resilience under attack and mishap,
- ease of management,
- protection and privacy of user and network information and assets,
- protection and privacy of identity and location, and
- accountability.

Security must take regulatory and law-enforcement requirements into account. It also must contribute to the overall availability and dependability of networks and services.

Consequences for the case study: To each network in the Wireless World, feasible and suitable security procedures should be inherent that are build according to one security architecture such that all the communications and negotiation take place in a secure manner. It is also very important to establish a trust relationship between the various networks that will either communicate or compose. Three different types of trust relations have been identified as considered important and should be supported; direct trust, brokered trust and no trust at all.

2.5 Backward Compatibility and Migration

Networks for the Wireless World must support migration paths and mechanisms from existing networks and mobile terminals, e.g., reuse of infrastructure of current 2G/3G systems including their evolution as well as Internet and non-cellular access systems, such as xDSL,



WIRELESS WORLD

R E S E A R C H F O R U M

and WLAN. Legacy applications (i.e., UMTS, PLMN) must be able to run within the network environment.

Consequences for the case study: Networks for the Wireless World (WWNs) may differently use the existing (legacy) network infrastructure. As they (in general) do not provide the full functionality of WWNs, advanced features like direct composition with other WWNs is not possible. However, WWNs may feature an appropriate adaptation (abstraction) layer to provide new functionality of the network. The provisioning of services from legacy networks can be accomplished similarly. Both can be described as interoperability with the legacy network infrastructure to offer the required backward compatibility.

2.6 Network Robustness and Fault Tolerance

The network architecture and network management must allow for building Networks for the Wireless World that are scalable, cost-effective, robust, reliable, with high availability and survivability across heterogeneous networks in dynamically changing environments. It must also allow building small and affordable Networks for the Wireless World that do not possess some or any of these capabilities.

Consequences for the case study: In the design of the Wireless World Network, single point of failures should be avoided. The design should also allow partial WWNs to function even when (temporarily) isolated from the rest of the network.

2.7 Quality of Service

Networks for the Wireless World must provide the capabilities to offer multiple QoS classes for end-to-end services, across different types of network technologies and different address domains.

The QoS mechanisms employed must be independent from link-specific technologies, but provide a consistent QoS coordination across multiple access technologies.

It must also provide on-the-fly (or on-demand) negotiation for changing a QoS class either from the user or the network side.

Consequences for the case study: This requirement describes an important aspect of the formation and communication between WWNs as well as legacy networks. Therefore QoS shall be guaranteed by the WWN, even when composing with other WWNs or interfacing to legacy networks. The WWN interfaces shall be able to communicate the parameters needed at any one time for the establishment and maintenance of a service across and between any networks.

2.8 Multi-Domain Support

The network architecture must transparently support network functionality spanning multiple administrative domains (areas operated and managed by the same authority).

Networks for the Wireless World must be capable of supporting various existing and future network provisioning business models.



WIRELESS WORLD

R E S E A R C H F O R U M

Consequences for the case study: The security and trust framework within the WWN architecture shall support this requirement on demand and in real-time. It should be possible to negotiate with multiple WWNs simultaneously and form agreements for the need of one or multiple applications as well.

2.9 Accountability

The network architecture must support mechanisms that enable auditability of single entities and subsequent enforcement when appropriate.

In particular, Networks for the Wireless World must provide an efficient, reliable, and secure way to collect and manage accounting data to support the different business cases of Wireless World Networks.

Networks for the Wireless World must also be flexible to interact with legacy accounting and new compensation systems.

Consequences for the case study: When WWNs compose with other WWNs, a trust-relationship is created. This includes especially data for authentication, authorization and accounting. Accountability denotes the need for the various interfaces that the WWN supports, to be capable of conveying or collecting accounting information so that users can be made accountable for the communication they participate in and operators are enabled to compensate the used resources of that communication.

2.10 Context Communications

Networks for the Wireless World must support a common framework for context awareness across all functions in the Ambient Control Space in order to adapt service availability and delivery to heterogeneous networks and dynamically changing environments automatically. The framework shall include support for collection, processing, management, and dissemination of context information enhanced with context-level agreement negotiations and support for conflict resolution.

Consequences for the case study: User specific information, such as terminal capabilities as well as preferences shall be easily communicated across networks in order always to achieve the required result. In this respect, the controlled distribution of user information is important, so that user privacy concerns that limits the use of this information to authorised parties only and hinders re-identification of users are maintained. This holds especially for information gathered in one domain and forwarded into another domain in which the originating user has no control over the information anymore. Furthermore the network context detection and filtering mechanisms provide a means of efficiently process context information for application purposes. An appropriate service to network interface has to be part of the WWN.

2.11 Extensibility of the Network Services Provided

Networks for the Wireless World must support extensibility of the minimum functionality in order to provide advanced network services when needed. New capabilities to specifically handling multimedia communication flows have to be able to be registered and provided through a flexible service to network interface. Extensibility shall also apply for the general capability to update WWN functionality.



WIRELESS WORLD

R E S E A R C H F O R U M

Consequences for the case study: In this respect WWNs provide an evolution of the current IMS framework. Handling multimedia flows by distributed resources in the network rather than in external application servers makes sense for mass distribution of media, media adaptation to terminal and access capabilities and for media types dominating in the network traffic (like standard voice and video communications). Extensibility also supports an open ended innovation concept built into the architecture.

2.12 Application Innovation

Networks for the Wireless World shall support short innovation and deployment cycles for applications. The architecture must be able to attract application developers by offering a stable, rich, and migration friendly API.

Consequences for the case study: It is important to offer application developers the support and performance of network services they demand, from simple connectivity up to media delivery overlays. This supports application innovation, allowing application developers to stick to their area of expertise, optimising the use of resources and the adaptation of applications to context changes.



WIRELESS WORLD

RESEARCH FORUM

3 Architecture and Components of the Ambient Control Space

Based on these requirements we show in detail in this section a case study how they can be realised. Our case study is the Ambient Networks project [1].

The logical picture of the Ambient Control Space, ACS, which was already introduced in the project proposal, is depicted in Figure 1. The picture illustrates that an AN comprise three distinct components:

- Ambient Connectivity, which abstracts existing network infrastructure to which the Ambient Network functionality is added.
- Ambient Interfaces, which allow the Ambient Control Space to communicate with the connectivity resources (through the ARI), services and applications (through the ASI) and other Ambient Networks (through the ANI).
- Ambient Control Space, which can be subdivided into the actual control functions (exemplified by the boxes in the control space) and the control space framework functions, which are not explicitly shown, but assumed to implement the loop surrounding the connectivity plane. The control space framework comprises all functions necessary to allow the control functions to plug into the control space, execute their control tasks and coordinate with other functions present in the control space.

This section explains how we map the logical picture to a more concrete view of networks consisting of a set of nodes connected with different kinds of link technologies. We define the AN interfaces, a first set of functions residing within the control space framework such as a naming model and connectivity abstraction mechanisms and finally present the current status of our activity working on the definition of the network composition concept and the functions facilitating it.



WIRELESS WORLD

RESEARCH FORUM

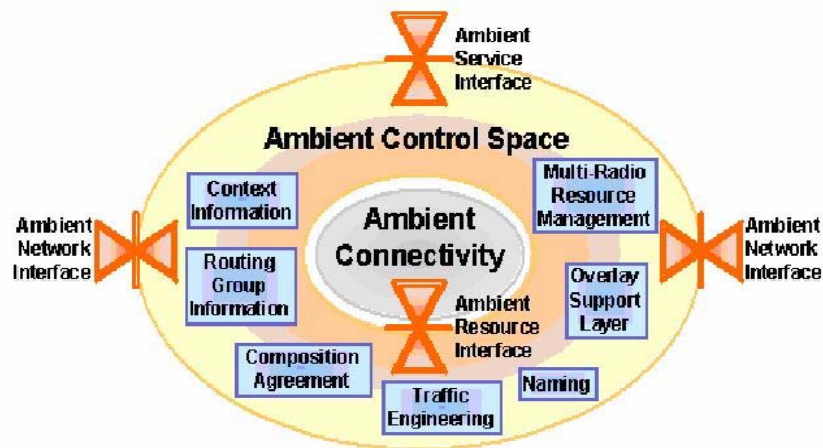


Figure 1: Illustration of the Ambient Control Space.

3.1 Ambient Interfaces

The control functionality that the Ambient Control Space provides and exposes in the Ambient Service Interface (ASI) makes it possible to implement services without having to worry about the heterogeneity of the underlying connectivity networks. Figure 2 shows an example of such a heterogeneous network environment. Each rectangle in the picture represents an AN. These ANs can communicate via the Ambient Network Interface (ANI). It is also across the ANI composition occurs. Composition is our way to simplify co-operation between networks, from the perspective of end-users, service providers as well as operators.



WIRELESS WORLD

RESEARCH FORUM

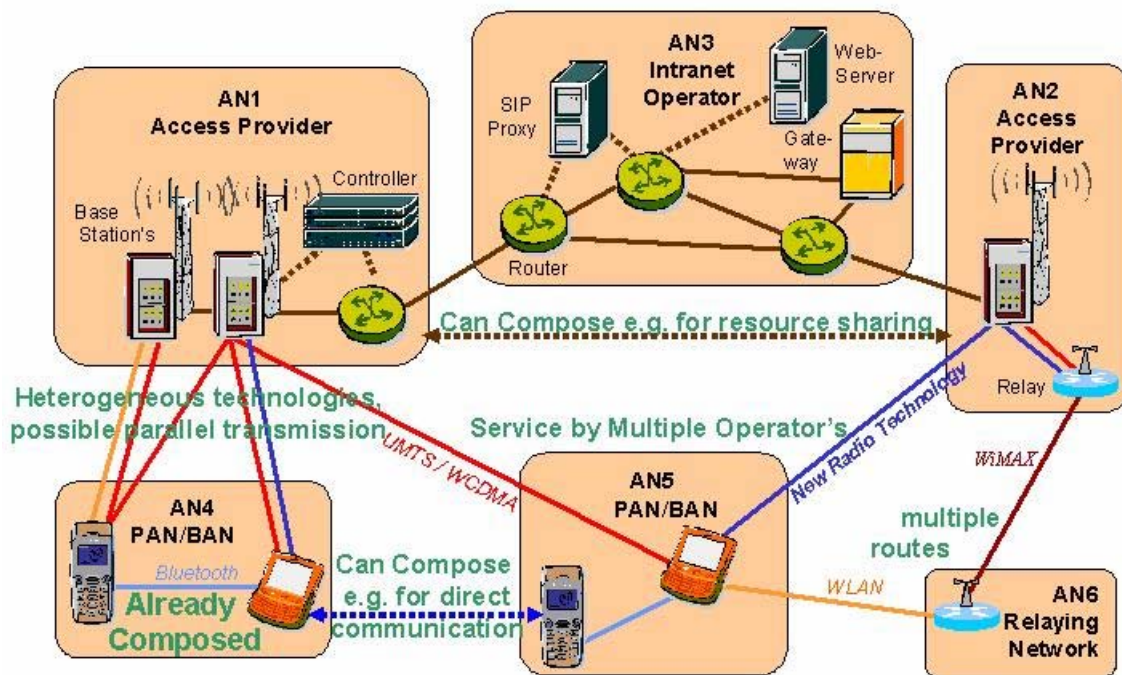


Figure 2: Physical elements of different Ambient Networks

Figure 3 shows a logical view of two ANs. It illustrates that there is one common ACS for all the nodes within an AN. The control space makes decisions on behalf of the nodes belonging to the network, and controls some aspects of the nodes operation. The control space is therefore logically present in the nodes. The AN architecture does not prescribe a certain kind of implementation of the control space. It can either be implemented in a central server or in a distributed fashion.

Nodes can implement parts of the distributed control space. For communication with other nodes in the same network, which implement other parts of the ACS, they need to implement the message passing mechanism of the control space framework. These nodes might also expose parts of the ANI in order to communicate with other nodes situated in another AN.



WIRELESS WORLD

RESEARCH FORUM

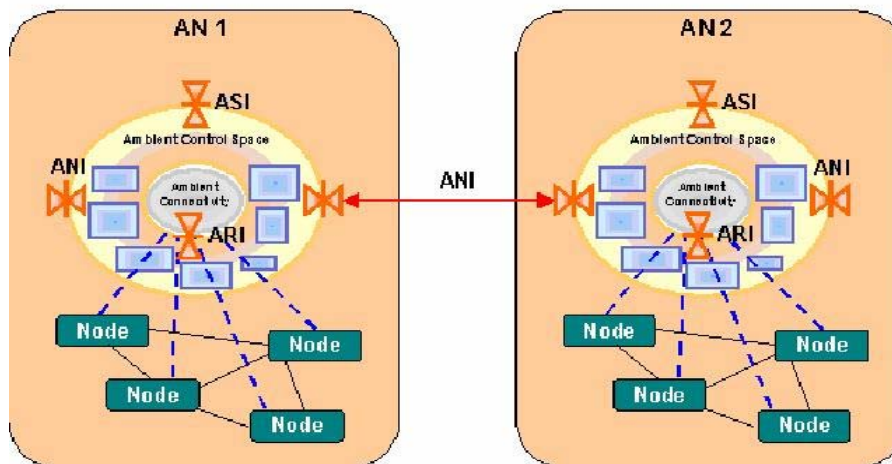


Figure 3: Interfaces inside and between two Ambient Networks

The three interfaces of the Ambient Control Space are:

- **ANI – Ambient Network Interface,** which connects the Ambient Control Spaces of different ANs. The interface is used for negotiation of network composition agreements and for transferring control information between the networks. The interface does not exist on every node of the network, but rather the nodes that collectively implement the core control space functionality.
- **ASI – Ambient Service Interface,** which is located between the ACS and the application inside a node. It allows applications and services to issue requests to the Ambient Control Space concerning the establishment, maintenance and termination of end-to-end connectivity between functional instances connecting to the ASI. The ASI also might include management capabilities and means to make network context information available to the applications.
- **ARI – Ambient Resource Interface,** which is located inside a node between the Ambient Control Space and the connectivity layer. It offers control mechanisms that the ACS can use to manage the resources residing in the connectivity plane. These resources can be routers, switches, radio elements (terminals, relays, access points) but also media transcoders, filters and proxies.



WIRELESS WORLD

RESEARCH FORUM

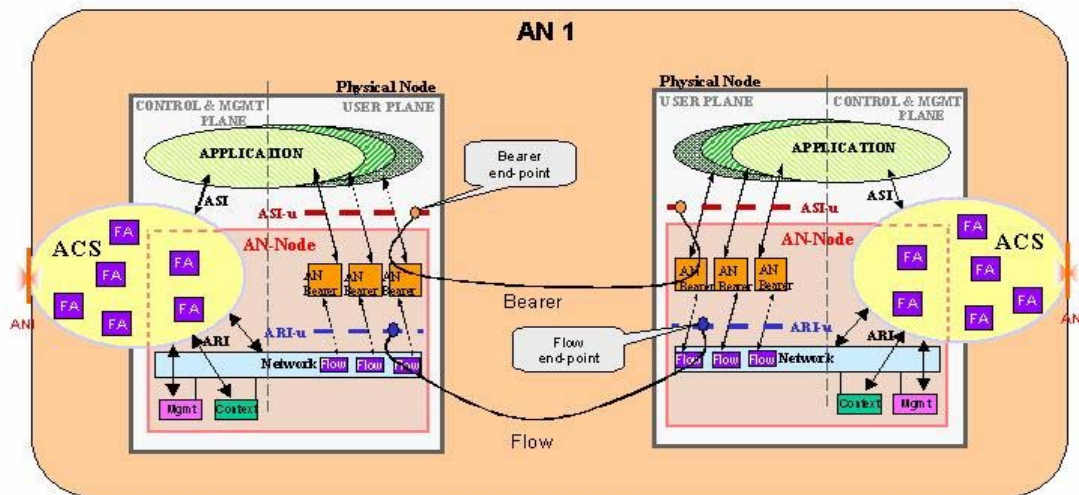


Figure 4: Example showing Ambient Network nodes and interfaces

Figure 4 illustrates an Ambient node and the relationships between the Ambient Service and Resource interfaces, the application programs and the interaction with the control space. To map these abstract control space concepts onto a physical node is not trivial.

The nodes in the picture are separated into a control and a user plane. The ACS constitutes the control plane of the AN part of the physical node. Parts of the ACS are also implemented in the node, while other parts of the ACS are implemented in other nodes.

The picture also illustrates that the ASI and ARI are node internal interfaces. There is one part of them that belongs to the user plane (-u) and one that belongs to the control plane. There is no strict separation between the user and control planes as which is which depends on from which viewpoint you look at it.

The bearer in the picture is the end-to-end data flow between applications. The AN provides these bearers that hide mobility and connectivity layer heterogeneity from the applications. These bearers are constructed from concatenations of flows, which goes between physical nodes. It is the functionality of the ACS that makes this possible.

We now describe the interface framework in more detail in the remaining part of this section.

The three interfaces of Ambient Networks – ANI, ASI and ARI – which follows the main design principles namely openness and extensibility, simplicity, and scalability. The interfaces also reflect the design of the Ambient Control Space, which consists of the Ambient Control Space Framework and control functions plugged in as modules.



WIRELESS WORLD

RESEARCH FORUM

The AN interfaces are thus structured as depicted in Figure 5. The interface framework offers basic support for the detection and negotiation of dedicated signalling protocols, which enable the information exchange for specific control purposes.

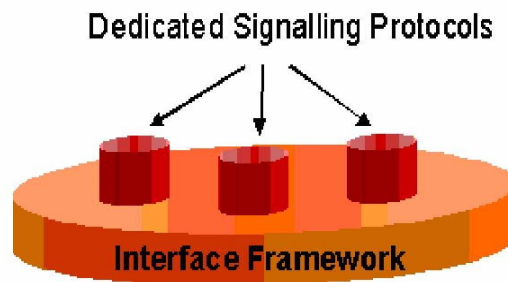


Figure 5: Common structure of the Ambient interfaces

The ANI is a horizontal interface connecting different ANs. It is typically not terminated at a single node, as the Ambient Control Space is distributed.

The ASI and the ARI are vertical interfaces bound to single nodes. This implies that a node hosting an application or service component needs to additionally implement the ASI, a minimum set of ACS functions and the ARI.

The ACS addresses network nodes taking care of the forwarding and processing of user data through the ARI. This implies that only nodes that expose this interface can be controlled directly by ACS functions. As mentioned before, the ARI is also defined as a node-internal interface. Still, controlling functions and controlled functions can reside in two different nodes. In such a case, the communication would look as depicted in Figure 6.

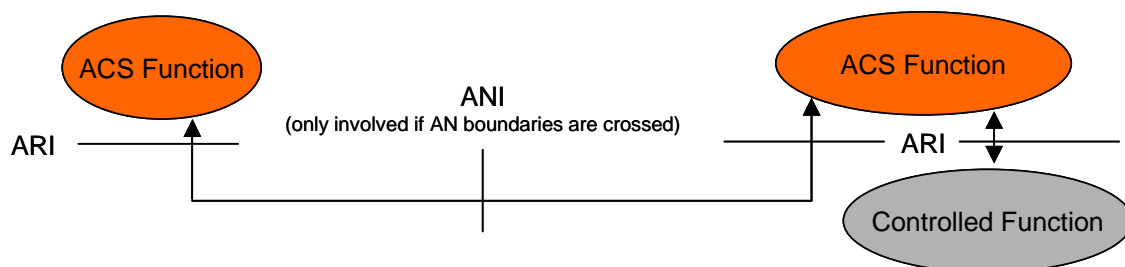


Figure 6: Scenario of an ACS function controlling a connectivity resource residing at a different node

The rest of section is organized as follows. In section 3.2 the common parts of the ACS are described. In section 3.3 specific control functions of the ACS is described. Section 3.4 gives a detailed overview of the composition concept while section 3.5 describes the business aspects that must be in place to complete a composition agreement.



WIRELESS WORLD

RESEARCH FORUM

3.2 Control Space Framework: Abstractions and Components

The control space framework consists of common functionality and abstractions that enable the specific control functions to operate together in a consistent manner. The common parts are a naming framework, connectivity abstractions, a security architecture, and functions that coordinate the specific control functions.

3.2.1 Naming Framework

Entities and identities are both real-world concepts, which exist independent of AN. A naming Framework is required for AN to provide identifiers for a particular entity in a particular context. An entity can have multiple identifiers, not necessarily of different types, and some of these identifiers can be *ephemeral* (i.e. used/valid only for a short time) to allow privacy and unlinkability.

The AN naming framework focuses on supporting four key aspects of the overall AN architecture:

1. Global reachability across different addressing domains;
2. Support for various services and end-nodes, including control of so called middleboxes;
3. Mobility of services, nodes, networks and sessions/flows;
4. Resistance to security threats (e.g. denial of service attacks).

To be able to fulfil these overall AN requirements, we have adopted a layered naming model that borrows from recent proposals: “A Layered Naming Architecture for the Internet” by Balakrishnan *et al* [36] and the Host Identity Protocol [32] as well as from Saltzer’s past wisdom [33]. The possibility of dynamic bindings at each layer enables native support for mobility of nodes and services. In the following we describe the objects that form the AN naming layers. The naming framework does at this time not prescribe that a certain *kind* of name is to be used for any of the objects.

- Application service or data object

An entity that is either a specific application service, or a specific data object. The identity of object persistence over time is not tied to the end-system hosting the service/data. Examples are SIP services and web pages.

- Application point of attachment

The point where an application program implementing (parts of) an application service can be reached by clients. This point is located at the ASI and can be compared to a standard TCP/IP socket API. A bearer connects two application points of attachment with each other.

- Host end-system

A node in the network. The identity of the host end-system is the same, regardless of its current location, and regardless of which communication interface that is used. A



WIRELESS WORLD

RESEARCH FORUM

host end-system does not necessarily mean a physical box – it may be a logical entity that can move between physical boxes. The entity “hosting” the ASI and ARI interfaces.

- Network point of attachment

Defines a location in the network. The location is identified with some kind of network address, which we below call *locator*. The locator is often dependent on network topology. This point is located at the ARI. A flow runs between two network points of attachment.

The concept of the *endpoint* which Chiappa [38] introduced is not quite the same as the just described host end-system. The endpoint notion is very interesting to the project. It is part of several of the proposals we consider in the analysis described below.

3.2.1.1 Dynamic Bindings between Levels

The purpose with defining a layered naming framework is to provide *dynamic bindings* between the levels. With dynamic bindings at multiple levels, names of objects can be made location independent and different types of mobility, for e.g., nodes and services, can be supported natively without resorting to add-on mechanisms.

It is the task of the control space to manage the bindings and to provide resolution mechanisms that map a name for an object into a lower layer object. The lower layer object is the “location” of the said object. The procedures for managing the bindings, in particular, to update them for on-going communication, are defined by the FA Handover and Locator Management in the control space.

At the current time, we have not decided whether we need dynamic bindings between all the layers described above. It is an item for further study in the project.

3.2.1.2 Indirection and Delegation

The naming framework supports the notion of **indirection** or **delegation**. It is an extension to the dynamic bindings that enable more advanced mobility schemes and the explicit control of so-called middleboxes. Network address translators (NATs), firewalls and transcoders are examples of the latter.

An object’s name can be bound not only to its own current location, but to some other location where an intermediary takes care of forwarding the communication to the object’s real location. A simple application of this mechanism enables servers to operate behind a NAT without explicit configuration.

The concept of indirection also includes the possibility to let the location of an object to be an object of the *same kind*. That is, not restricting the binding to an object one level down, but also allowing bindings horizontally within one level. One important application is to enable efficient mobility mechanisms for moving networks. A node in the moving network binds its location to a designated gateway node. Only the latter node needs to update its binding to a



WIRELESS WORLD

RESEARCH FORUM

new network location as the moving network moves. Another way of explaining horizontal bindings is to say that they provide dynamic creation of virtual tunnels in the network.

3.2.1.3 Bridging Over Multiple Address Spaces

There are two alternative methods to achieve bridging over multiple addressing (locator) domains, e.g., between IPv4 and IPv6 domains. These can be applied at different levels in the naming architecture. The methods are:

- **Translation** – The identifier used at a particular level is translated at a gateway between the two networks. NAT is an existing example of translation.
- **Common namespace** – The identifier used at a particular level is from a mutually common namespace for the two networks. Translation is therefore not needed. The extreme is if the namespace is global, which for example the case is if both use global IPv4 addresses. Note that this method corresponds to the internetworking principle.

It is currently an open question whether we need a new internetwork layer that implements a new global namespace, or whether translation is sufficient. With several layers in the architecture, it is perhaps possible to not make an exclusive choice at all levels. Note that choosing IPv6 as the new internetwork layer does not solve the problem. IPv6 has many of the same architectural shortcomings as IPv4 has. For example, they both lack native support for mobility because the same identifier is used for both node identity and location. If we take the effort to migrate to something new, we may as well migrate to a solution which solves more shortcomings than IPv6 does.

The bridging functionality raises the issue of how to handle routing *between* networks. The ACS needs to provide routing functionality controlling the translation of the common namespace. The function is similar to the Border Gateway Protocol (BGP) in today's Internet. This function requires that we can identify each Ambient Network as first class objects, also similar to the autonomous system numbers in BGP.

3.2.1.4 Cryptographic identifiers

The majority of typical identifiers in widespread use today do not come with any guarantees, e.g. IP/MAC addresses may be spoofed, usernames replaced, etc. To get some assurance from an entity presenting a particular identifier one could require the claiming entity to also present some sort of proof of ownership, typically involving cryptography.

As a basis for secure identification there is a secret associated to the identifier as well as an authentication method to prove ownership. The authentication method actually proves ownership of the secret rather than the associated identifier, but by selecting the identifier carefully, and by binding the secret to the identifier, and performing authentication appropriately, ownership is inferred to the identifier. Some obvious conditions must apply, e.g.: the secret should not be revealed by knowing only the identifier, the secret should not be revealed by performing authentication, etc. Examples of a "secure" binding between identifier and secret include tamper-resistant hardware, within which the authentication method is performed (compare with e.g. SIM cards).



WIRELESS WORLD

RESEARCH FORUM

A particularly important instance of secure identification is the use of cryptographic identifiers.

One example of cryptographic identifiers comes from public key cryptography, where a public key (the identifier) and the corresponding private key (the secret) are linked by mathematical equations, and without additional information it is not feasible to calculate the private key based on the public key, but it can be efficiently verified whether some operation was performed with one key using the other key. Cryptographic identifiers like this can be self-generated (do not require a naming authority) and statistically unique (i.e. the probability that two entities generate the same is negligible).

Although a public key (PK) can be used as a cryptographic identifier (and the corresponding private key as the associated secret), it lacks a concise representation. To alleviate this, it is possible to apply a cryptographic hash function with fixed length to the public key. The hashing is especially useful where a public key is used in some protocols that have a fixed and preferably short slot allocated for an identifier. One such example would be the Host Identity Tag (HIT) of the Host Identity Protocol where $HIT = \text{hash}(PK)$. The cryptographic identifiers considered in the AN project are mainly of this type. See for example Section 3.4.5.

3.2.1.5 Analysis of New Naming System Proposals

At the time of this writing, the project is analyzing a set of new naming schemes that have recently been proposed in the research community. The analysis is performed according to a set of criteria. They are of four kinds:

- **Namespace properties**

The structure and syntax of the used namespace. Some proposals use *flat* namespaces – what are the implications? How are flows identified in the network, and how is this identifier used? Who is intended to use these names? Are there any privacy issues raised in the solution, such as disclosing the current location of the other party?

Other possible properties of names include human readable/rememberable, topological, hierarchical, self-assigned, cryptographic, etc.

- **Name system design**

How is name resolution done, i.e., how are the dynamic bindings between the naming layers managed? Is caching used, and if so, how is consistency achieved? What is the likely performance of the name system? What transactions are needed to resolve names and set up communication? Does the proposal address denial of service?

The name system has to provide means for name assignment, naming data-base, and name resolution

Name assignment refers to the problem of assigning names to entities, while name resolution refers to resolving names one layer to a name of a lower layer, like DNS today resolved readable Internet addresses to IP addresses. Cryptographic names can be self-assigned, which is particularly useful in dynamic environment and in case many names are needed for one entity. Of course if identifiers are self generated, either a check for non-duplicated names needs to be done, or non-duplication is assumed due to e.g. randomness and the length of the ID.



WIRELESS WORLD

RESEARCH FORUM

The **Naming data base** refers to the architecture that handles assigned names. Basically, the naming database can be an ID-structured-database where entries are IDs link to another kind of information, or an ad-hoc-unstructured database where IDs are managed in an ad hoc way.

Resolution in an ID-structured-database consists of a link between IDs and other information / other IDs. This very likely today's DNS resolution mechanisms where domain names are linked to IP addresses. This can be considered as a link between two IDs, one that is human readable and another ID containing routing information, or a link between an ID and routing information without considering the IP address as an ID. Alternatively, for ad-hoc-unstructured database resolution, we can use distributed hash tables of P2P technology, which have advantages for distributed environments. In either case, each Ambient Network needs a mechanism to query the (distributed) name resolution data base. Furthermore, dynamic network topologies affects hierarchical name schemes and resolution. For network composition, this is considered in [Prehofer2005].

For name resolution in environments with legacy environments and also dynamic networks, there is a dedicated mechanism, DEEP, proposed in WP3 [D3.3]. DEEP provides unified name resolution interface for ACS entities whether it is a GANS CEP or a legacy CEP. DEEP is not tied to any specific name resolution concept/mechanism, even we have used hierarchical names in our examples.

- **Network boundary traversal**

How does the proposal provide for bridging over multiple addressing domains? What mappings are assumed at the network boundary and how is the information to support the mappings populated and managed at the network boundaries? Is there an internetworking point, and what assumptions are made about its operation?

- **AN applicability assessment**

How does the proposal address the overall AN requirements and scenarios? Maturity and migration are also considered. Are there implementations available – do they interoperate? How do we migrate to the proposal?

3.2.2 Connectivity Abstractions

This section defines the AN terminology for how the objects, or actors, described above communicate with each other. These definitions refer to things that are partly outside the scope of the project, either "above" in the application domain, or "below", in the technology providing connectivity. Parts of the definitions are therefore by necessity opaque or left open.



WIRELESS WORLD

RESEARCH FORUM

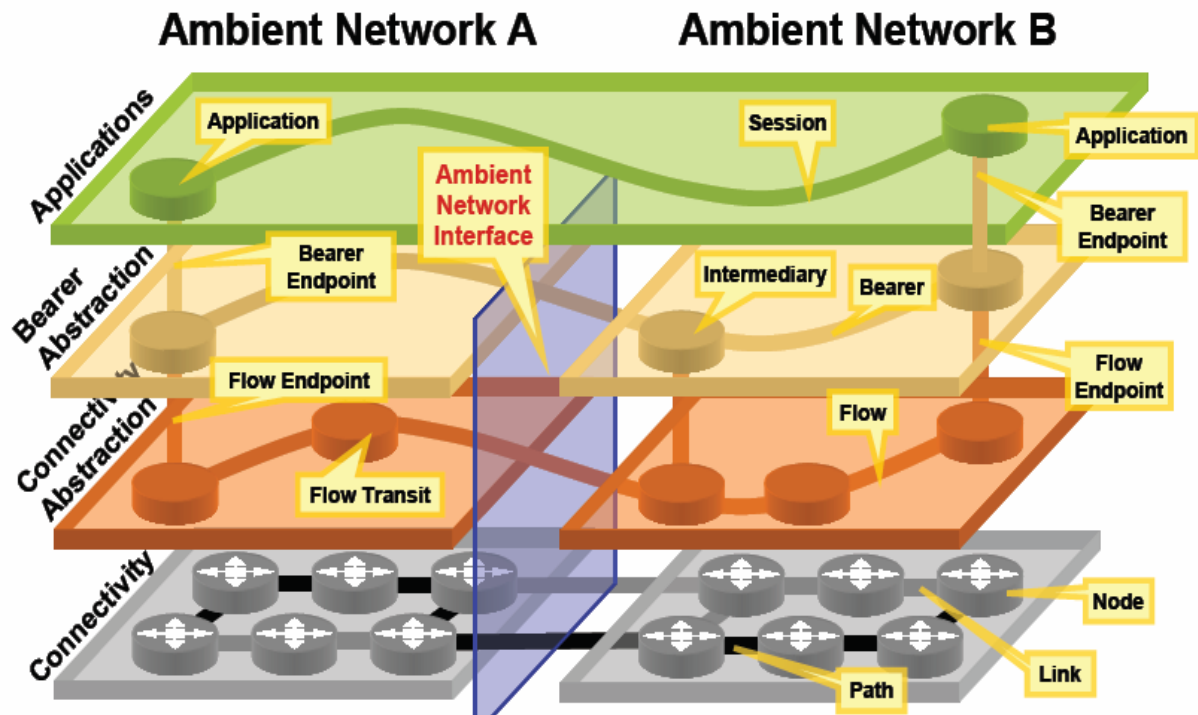


Figure 7: Connectivity abstractions

The connectivity abstractions are illustrated in Figure 7. It shows four layers from the application at the top to the connectivity provided by a specific network technology at the bottom. All nodes are visible at the lowest layer. If a node is visible at a higher layer, a low cylinder is also drawn in that layer at the same position as in the lowest layer. Starting from the top, the connectivity abstractions are:

- **Session** – An application specific notion of connectivity that we leave to the particular application to define the precise meaning of in terms of mapping to bearer(s.)
- **Bearer**¹ – The connectivity abstraction which the Ambient Network provides to the application at the ASI.
- **Flow** – An abstraction of the basic connectivity provided by the underlying network technology at the ARI.

We describe the latter two in more detail in the following two subsections.

¹ The name “bearer” for this term is currently under discussion within the project. We may choose another name for the term at a later time.



WIRELESS WORLD

RESEARCH FORUM

3.2.2.1 Flow

A flow is an abstract view of the connectivity provided by the underlying network technology. Depending on the latter, a “shim” layer may be needed in between to adapt the technology to the abstraction. A flow is constrained to a single network technology.

A flow is a *transfer of data* between two instances of the ARI, where each flow endpoint is labelled by a technology dependent locator. Flows are *unidirectional*, so a flow is associated (minimally) with a specific source locator and destination locator. For some types of network technologies, a flow may require a connection set up, but for other types that is not necessary.

A flow may pass through *intermediate resources* (“Flow transit” in Figure 7), which are not explicitly tied to the flow, but which can be controlled through the ARI. The set of intermediates may change over the lifetime of the flow without changing the flow itself. The flow may also pass other nodes not visible, and thus not controllable, through the ARI.

The flow data is transferred between successive nodes using the underlying connectivity functionality. The control space may use the control and configuration capabilities of the ARI to request certain treatment of the flow by the connectivity layer. For this reason, a flow definition may include a packet classifier that picks out a subset of the data with a given source/destination locator pair.

Flows transfer data transparently, with certain performance characteristics, which may include the level of integrity of the data. Mobility of a data transfer requires a flow to be modified (since locators are modified), or a new flow to be created and the old one deleted.

3.2.2.2 Bearer

A *bearer* runs end-to-end between application peers. It is the means for communication that an Ambient Network provides to applications at the ASI. The bearer, unlike the flow, is not bound to locators, but to a higher-level object in the naming framework. This means that the bearer can make use of the functionality provided by the control space, such as mobility, address translation and media adaptation. For the latter, the bearer has (optional) media properties that tell the data manipulation functions of the control space what things are allowed or requested to be done with it.

For certain applications, e.g., a file transfer, a bearer can be quite simple requiring very little above what a flow provides. For other applications, e.g., voice, the bearer can be quite complex involving transcoding and special media routing.

When special treatment is needed at an intermediary, the bearer is mapped to two flows – one from the source to the intermediary, and one from the intermediary to the destination. The indirection support of the naming framework described above controls this mapping of a bearer to a set of concatenated flows between the intermediaries. This feature is used by the service specific overlay network function described below in section 3.3.

Multiple bearers may be mapped to the same flow, i.e., flows can multiplex bearers between the same pair of locators.



WIRELESS WORLD

RESEARCH FORUM

3.2.3 Security Architecture

The components of the initial AN security architecture as well as general security objectives, initial requirements, and a number of specific security investigations are presented in [14].

The current results include a set of security principles to support design decisions, requirements on a security policy framework and a number of security services grouped into service areas. In this section we outline proposed security services of the AN architecture, which are detailed in section 8.2 of [14], and refine one of the groups of security services.

The outline given here reflects the current understanding of relevant security services in the scope of the AN problem space. It is for further study which services will actually remain mandatory of the Ambient Control Space Framework, which need to be integrated into specific functions of the control space, and which (if any) will result into new, self-contained security functions of control space.

The AN security services are grouped into the areas Administrative security services, Access security services, Multi-addressing security services, and Special security services (Group security and Attack resistance). Section 3.2.3.3 presents the refinement of access security services to improve network attachment mainly.

3.2.3.1 Administrative security services

Administrative security includes trust management and security policy management, security aspects of dynamic business agreements and compensation (e.g. payment) methods. These services are the pre-requisite security services for composition e.g. securing automated negotiations between business parties and bootstrapping of security credentials subsequently used to enable secure operations. This area also contains security domain management functions needed for adaptation of ANs to new services and changing environments.

3.2.3.2 Access security services

Access security services include security services related to network access, network attachment, and also link layer security. These services support the early phases of composition e.g. by securing the dynamic exchange of configuration information between ANs, and providing means for authorization for access including non-subscription based services such as micro-payments. The area also includes key management services for generic link layers, and security services for non-conventional wireless access supporting the case of terminals or relay nodes with multi-hop capability.

3.2.3.3 Basic concepts, further assumptions for access services in multitrust environments

When different types of networks, business actors, and devices can cooperate in a seamless manner to provide communication services for all then the vision of the AN project is defined. When refining the access security services and to work more tangible, some assumptions are made from the point of view of the system as well as from security perspective. The security



WIRELESS WORLD

RESEARCH FORUM

related assumptions say that cryptography is cheap, round trip time is expensive, and security should be default and automatic.

There are four security concepts identified, these are identifiers, trust relations, authorisation, and security by default. AN enabled host can have several different identifiers coming from legacy technologies but there could also be those that are AN specific. Identifiers will be needed by AN for several different purposes including, charging and accountability, and privacy and authorisation. A binding mechanism between identifiers and authorisation is useful. Another area that requires consideration is the trust relation between the AN entities. Three types of trust relations are considered to be important; these are direct trust, brokered trust and no trust at all. For each of these types suitable authentication mechanisms basically exist; however, their combination into efficient access and authentication procedures is vital. The concept of authorisation comes together with binding and credentials. Authorisation, permission to access a system resource, must be performed explicit via credentials (and not implicit with authentication). The security concept 'security by default' basically means that some default security is always used, i.e., security does not need to be switched on thus AN will have always-on-security; the issue now is whether the peers have pre-defined trust or not.

A basic set of security components is proposed: All ANs and its nodes should support cryptographically generated host identifiers that are public keys or its cryptographic hash. Membership in an AN is demonstrated by a public key certificate. An association protocol authenticates hosts or ANs based on these identifiers. The protocol allows involvement of a trusted third party in a variety of authorisation methods, and "data payload" can indicate the purpose of the association. Subsequent communication between entities is secured. Special security protocol profiles are considered for performance reasons.

Accordingly, network attachment takes a complete system view instead of per layer view as is taken in current technologies by using the concepts of cryptographic identifiers and their binding to authorisation. The interactions between ANs are studied from generic point of view and also addressing the issue of AN membership and identifiers during composition.

3.2.3.4 Multi-addressing security services

Multi-addressing security services support mobile and multi-homing services including session mobility on different layers, moving networks, handover services and multi-addressing management. These services enable security for a range of AN mobility concepts and across multiple interfaces. Examples include a general multi-addressing management framework based on addressing anchor points, identity providers and name service to protect multi-addressing signalling between the end-points, route optimization and access control within a moving network, and services to minimize the impact of security on handover performance. This service area also includes a middlebox registration service based on the Host Identity Protocol, for management and traversal of middleboxes such as firewalls and network address translators.

3.2.3.5 Special security services

In addition to the previously listed security services which target fairly well defined functions of the architecture, there are two areas of more general applicability: Group security services and



WIRELESS WORLD

R E S E A R C H F O R U M

attack resistance. Group security is about establishing and maintaining security associations for a large group of communicating parties in an efficient and scalable way. This service area supports efficient and secure signalling in dynamically changing groups such as media overlay nodes, and peers of an AN management domain. Attack resistance is about mitigation of threats to availability, such as Denial of Service attacks. In this area new intrusion detection services are begin proposed.

The security services outlined here are described in more detail in [14]. This is still work in progress. Though some of the described security services can be applied independently from others, for efficiency and even security reasons an understanding of the complete set of interacting services need to be considered when assessing the feasibility of the combination, or if in some cases different services would be needed.

These security services should be seen and understood as security components of the Ambient Control Space Framework. However, it is yet for further investigation via which AN interface these services will be provided and it needs to be detailed which information these services convey.

3.2.4 Extensible Control Space

A key feature of the overall Ambient Networks architecture is its extensible Ambient Control Space (ACS.) Based on a small set of required functionality, the ACS dynamically integrates functionality modules that provide a specific, limited set of control capabilities for the network.

This section will describe the ACS in detail, focusing on the underlying control space functionality that enables plug-and-play extensibility, namely, control communication via message passing, a common registry and consistency mechanisms.

Note that although this section describes message passing, registry and consistency control functionalities separately, these functions are interdependent. For example, consistency control is involved in concurrent updates to the registry and for some operations; direct message based-communication may be replaced with indirect communication through registry updates and queries. The details of these interdependencies will be investigated during the detailed functional specification of the architecture.

3.2.4.1 Control Communication

Different functions within the ACS communicate by exchanging messages with one another. Message-based communication among a set of participants requires a number of globally agreed-upon principles. Participants need unique identifiers to enable unambiguous message delivery. A resolution mechanism must map these identifiers into locators for the specific message delivery mechanism. Two communicating parties must agree on a specific encoding for the information they transfer. Finally, the message passing service may need to implement additional services other than best effort delivery, such as guaranteed delivery, duplication prevention, reordering protection, prioritization, subscription or flow control, to support the particular communication needs of the participants.



WIRELESS WORLD

RESEARCH FORUM

These required features for message-based communication within the ACS are extremely similar to what the Ambient Networks user plane abstraction provides (see section 3.2.2.) In some sense, the ACS can be seen as a distributed application or service implemented on top of the generic user plane. Because the ACS already implements connectivity abstractions that provide a uniform view on specific user plane technologies, using the same communication mechanism within the control space offers considerable synergies: No additional communication system on top of the user plane abstraction is needed to support the control space, leading to a relatively thin interface towards the connectivity resources (ARI.) The remainder of this section will discuss how the generic user plane supports message-based communication within the control space.

First, message-based communication within the ACS requires the dynamic allocation, de-allocation and management of unique identifiers for individual control space functions. The naming functions for the generic user plane already support these operations. Similarly, binding identifiers to topological locators is also a key characteristic of the existing naming functionality, which the ACS can leverage. However, providing plug-and-play extensibility to the ACS likely requires specific further registry functionality, as described in section 3.2.4.2.

Second, two communicating parties must agree on a specific encoding for the information they transfer. This capability is *not* part of the generic user plane abstraction. Information encoding is a service-specific issue and must hence be addressed at the control space level. Information encoding for control space messages, especially extensible mechanisms that can incorporate new types of data, is currently an open issue under investigation. However, existing encoding schemes such as MIME [31], XML [35] or ASN.1 [34] may be readily adaptable for ACS communication.

Third, if a function receives conflicting information about global data, a consistency control mechanism must resolve the conflict. For long-lived, critical information, a system-wide agreement has to be established in case of such conflicts. This functionality is not part of the generic user plane and is currently being investigated within Ambient Networks.

Finally, the generic user plane abstraction only provides a simple, best effort delivery mechanism for messages. Although this allows the connectivity abstraction to incorporate many different network technologies, for communication within the control space, best effort delivery may be too limited. A richer set of communication primitives, for example, guaranteed delivery, duplication prevention, reordering protection, prioritization, subscription or flow control, can provide improved communication mechanisms that simplify the implementation of control space functions by factoring out communication primitives into a common substrate.

3.2.4.2 Registry

The registry is an ACS-wide directory and storage service accessible by all functions. In a very general sense, it is a distributed database. Providing a unified registry simplifies many control functions by factoring out storage, discovery, lookup, sharing, distribution and access control to information into a common service. Note that although the registry is logically a single service, implementation of registry access and data storage is expected to be distributed for sizable Ambient Networks.



WIRELESS WORLD

R E S E A R C H F O R U M

One purpose of the ACS registry is storage of information about user plane entities such as network resources, services, specific hardware, links, sessions, policies and user information that are used by functions in the control space. It controls access to this information, coordinates distributed use and manages persistent storage.

A second purpose of the ACS registry is storage of information about the ACS itself. In this function, the registry supports the message passing and consistency control functionalities within the ACS. For example, the ACS registry may maintain the bindings of ACS functions to topological locators.

In addition to these typical directory services, the ACS has to provide basic resource control functions to coordinate the different ACS components. This includes

- manage access to resources which are identified in the registry. While some of the resource access control for specific entities can be provided locally by other components, some basic services will be required in the central repository. It is an item for further study which access control has to be done in an ACS wide repository.
- manage potential conflicts for the registry, e.g. if different entities aim to insert conflicting information. This issue will be discussed in the following section.

Similar to the message passing functions, data encoding is a challenge when designing the ACS registry. Due to the dynamic nature of the control space, the registry may accommodate many different kinds of information with potentially very different access characteristics.

AN WP “Context Aware Networks” is working on a context coordination function for Ambient Networks, which includes a context information base (CIB.) This database might already provide the required functionality or at least serve as a basis for the ACS registry. WP “Concepts, Architectures and Technical Coordination” is aware of the work done in WP “Context Aware Networks” and will clarify to what extent the CIB can be used to implement the registry function sketched in this subsection.

3.3 Description of Control Functions

Apart from the Control Space Framework, the Ambient Control Space contains various specific control functions, e.g. multi radio resource management, congestion control, handover management and context management. These specific control functions are specified by the various work packages in Ambient Networks and are described in more detail in their respective deliverables. To give a flavour of what these specific control functions are, this section lists short descriptions.

Note that the collection of different specific control functions does not yet comprise a complete and consistent set of Ambient Control Space functions. To find holes and solve inconsistencies among the current set of specific control functions is a challenge for the remaining part of the Ambient Networks project.



WIRELESS WORLD

RESEARCH FORUM

3.3.1 Multi Radio Access

Multi Radio Access (MRA) is a key component in Ambient Networks enabling the cooperation between heterogeneous access technologies [17][18]. The MRA as described in [19][20] includes open interfaces to provide cost effective wireless bandwidth practically everywhere and enables the selection of more than one RA for the transmission of certain user data, a mechanism called multi-radio access selection (MRAS) [21]. MRA consists of two main functional entities (i) the Multi Radio Resource Management (MRRM) [22][23] and (ii) the Generic Link Layer (GLL) [24][25]. A high-level model of the MRA architecture is shown in illustrating one communication peer is depicted in Figure 8. While MRRM is a purely control-plane function in charge of access selection in AN, GLL represents the AN L2 interface for user-plane data. MRRM maps higher level requests on services provided by GLL.

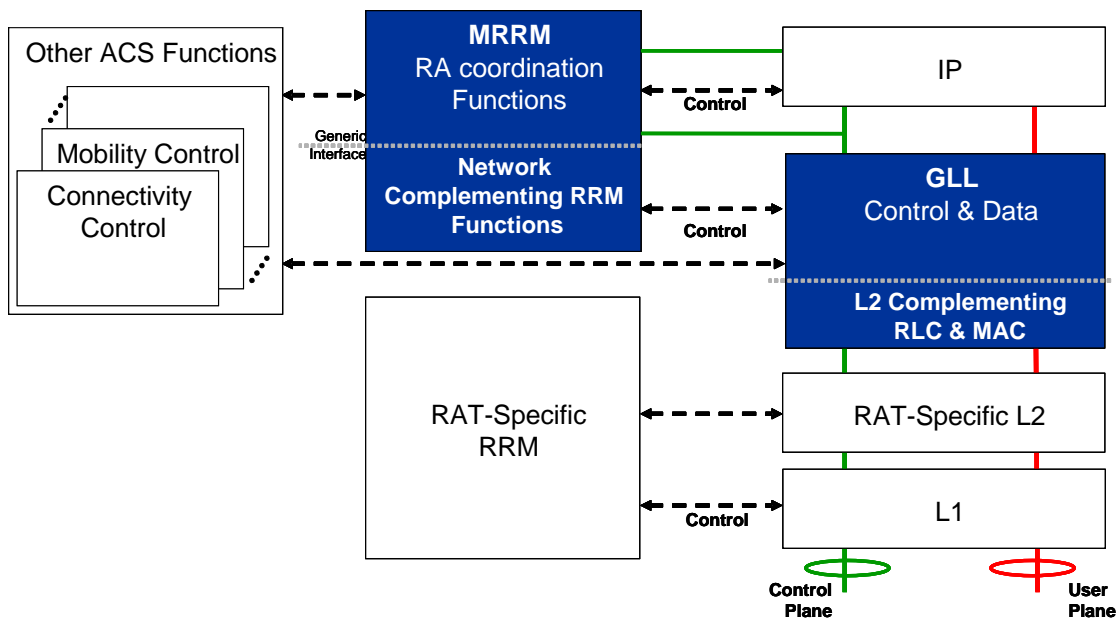


Figure 8: High-level MRA functional layer architecture

3.3.1.1 Multi Radio Functional Entities

3.3.1.1.1 Multi Radio Resource Management

Multi Radio Resource Management (MRRM) is a control space functionality to manage all available radio access resources, potentially belonging to several radio access technologies (RATs) in a coordinated manner. MRRM handles access to radio resources over both single- and multi-hop links between communicating peers. We refer to each link as “radio access” (RA), where each RA corresponds to links over distinct or possibly identical RATs and administrative entities. MRRM manages data flows and decides on the assignment of radio accesses to a flow, controlling handover between different RATs in cooperation with the “mobility” functional area. The radio resources assigned to a flow are selected so to achieve an efficient mapping of user flows’ demands to the available radio resources. For instance, to avoid congestion MRRM may redirect users to those RATs experiencing lower resource



WIRELESS WORLD

R E S E A R C H F O R U M

usage, such as lower air interface load. An important aspect is that at admission control MRRM may assign more than one radio access to a session.

In order to provide coordination between the different RATs, each one with its own RAT-specific RRM functions, MRRM consists of RA coordination and network-complementing RRM functions. The latter provide missing (or enhance inadequate) RRM functions to legacy or future networks, or act as translation layer between the RA coordination functions and RAT-specific RRM functions. The MRRM RA coordination consists of the following functions:

- RA Advertising and Discovery which advertises/discovers new access resources in different ANs and negotiate with their MRRM the terms of the access resource utilisation.
- RA Selection which selects appropriate RAs for a given data flow. It corresponds to an RA admission decision which is based on an RA Evaluation where several parameters, such as signal quality, QoS requirements, etc, are considered.
- Overall Resource Management which keeps an overall control of composed AN resources and protects established QoS agreements, for instance, by performing load sharing actions.

MRRM functions can be implemented in a centralized or decentralized way, between MRRM entities of different ANs depending on the respective roles established during network composition (e.g., master-slave or peer-to-peer relation). This allows MRRM functioning for single- and multi-hop networking (including ad-hoc networks without fixed infrastructure), as well as multicast/broadcast configurations. MRRM entities may be implemented in user devices as well as network or operator devices. Different MRRM functions may have different conflicting strategies, e.g., MRRM functions located in the user terminal (which is also an AN) may adopt a strategy to optimize battery life, whereas the MRRM functions in the access network may have a strategy to optimize capacity. Moreover, MRRM functionalities might differ also in their complexity, e.g., user equipment will normally include less functionality than infrastructure equipment.

Signalling among MRRM entities located in different ANs will use ANI. Most parts of the MRRM, like the coordination function, may be located in the Ambient Control Space above the ARI. It is currently under investigation if part of the functionality is located below the ARI. The parts of the MRRM located below the ARI may provide missing RAT-specific MRRM functionality, like admission control, congestion control or intra-RAT handover. RAT-specific functions to provide information to MRRM may also be located below the ARI. In difference to the ANI, it is assumed that MRRM is not directly accessible via the ASI. Some MRRM information may however be needed to go through ASI, e.g., when user interaction is required in order to make a final decision on a handover. In this case, MRRM may provide characteristics on the possible handover choices including network name, maximum, data rate or cost.

3.3.1.1.2 *Generic Link Layer*

The GLL amounts to a toolbox of configurable link layer functions that perform radio protocol reconfigurations and partly replaces the RA specific parts of the link layers. Its aim is to facilitate the cooperation among different RATs by providing a unified link layer processing and a unified interface to upper layers. GLL functions including access selection execution,



WIRELESS WORLD

R E S E A R C H F O R U M

To support multi-radio dynamic scheduling in Ambient Networks, two novel applications have been identified within GLL [24]:

a) Multi-Radio Transmission Diversity (MRTD) refers to the level of parallelism in the utilisation of radio access (RA) resources over a single hop. It can broadly be defined as the dynamic selection of multiple radio accesses for the transmission of data flows. Thus, depending on the re-selection rate, MRTD can be performed at different levels within L2. At this stage two levels have been considered namely, MRTD at MAC PDU level and MRTD at IP packet level, which will be referred as MRTD@MAC and MRTD@IP, respectively. “Switched MRTD” denotes the case when only one RA is used for the transmission of a single user data at any given time. Similarly, “Parallel MRTD” denotes the case when multiple RAs are used at the same time for the transmission of a data flow unit. With “Parallel MRTD” we can always choose to send multiple copies of the same data unit, for robustness, or we may send a set of subsequent data units simultaneously over the multiple RAs to increase throughput.

b) Multi-Radio Multihop (MRMH) refers to the sequential utilisation of RA resources over multiple hops characterised by the same or different RATs. To this end, GLL provides e.g. the use of an end-to-end ARQ with advanced queuing, which prioritises control messages.

The ANI will be used for the signalling between GLL instances located in different ANs. The signalling may include transfer of QoS, mobility, resource, security information (may be part of context transfer) and service negotiations. The partitioning of the GLL across the ARI is currently under investigation. One option is that the GLL-C is located in the ACS while the lower-layer functionalities of the GLL, termed GLL-D, are located within ACY.

3.3.1.2 Multi Radio Access Selection Approach and Performance



WIRELESS WORLD

RESEARCH FORUM

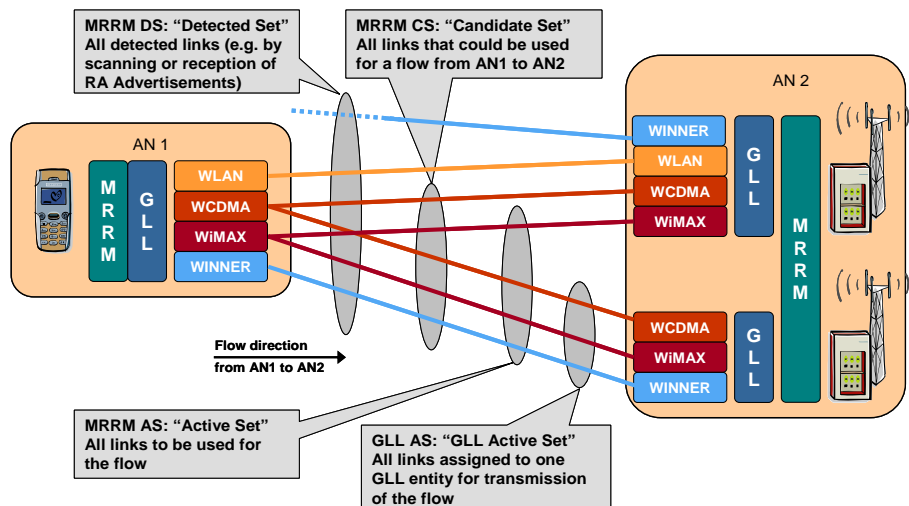


Figure 10: The Concept of Access Sets in MRAS

A user session is transmitted over the radio link via an access flow. An access flow is defined by a set of locators at the flow endpoints; it can comprise a number of consecutive links, which can be either access links, or links connecting the access to the fixed part of the network. An access flow can also include multi-hop communication via relay nodes. The radio access flows are the elements managed by MRA functionality. Managing the access flows is achieved by means of Access Sets that are established and maintained by the RA coordination functions, Figure 10:

- Detected Set (DS) is the set of all access flows detected by MRRM through e.g. scanning or reception of RA advertisements.
- Candidate Set (CS) is the bearer-specific subset of the DS with all candidate flows for assignment by MRRM access discovery function to a given active bearer.
- Active Set (AS): a subset of the CS that includes the access flows, assigned by the Access selection MRRM function, to an active bearer at a given time;
- GLL Active Set (GLL AS) is the subset of the AS assigned to a given GLL entity by MRRM to serve a given data flow at a given time, by means of multi-radio (packet) scheduling. This set is used only in cases where GLL entities control two or more tightly integrated radio accesses.

The access selection algorithm decides then which (radio) access flow(s) (among the available ones) should be used for the end-to-end session in a multi-radio access scenario. The objective of the access selection algorithm is usually to optimise a certain utility function. The utility function can be derived from one performance metric or the weighted combination of several performance metrics such as achievable user throughput, blocking or dropping probability, communication costs (in terms of resource consumption and/or price), resource utilization (load balancing), etc. In the decision process, the access selection algorithm can interact with other AN FEs, in order to take into account e.g., user specific pre-defined priority lists for preferred RATs and/or network operators, congestion in the ongoing session, changes in service requirements, cost of the active access.



WIRELESS WORLD

RESEARCH FORUM

Dynamic access selection can operate on either fast or slow timescale. The general objective of dynamic access selection is to increase the end user throughput and the capacity of the multi-radio access system. This gain can be exploited by either increasing the network capacity, or alternatively, to lower the costs in deploying a multi-radio network at a given network capacity. Fast access selection requires tightly integrated radio accesses and instantaneous radio link characteristics as input parameter (e.g., instantaneous SINR). The feasibility studies [28][29][30] present gain of fast access selection in terms of throughput and spectral efficiency (in Mbit/s/Hz) in the range of 15% to 60%. Slow access selection is based on average values of radio link characteristics, and achieves somewhat smaller gain than fast access selection. The evaluation studies presented in [25] - [30] consider both slow and fast access selection, and they report gains in system capacity or user throughput, between 10% and 70% depending on the considered scenarios. These gains are for access selection in a multi-radio access environment relative to the performance of isolated systems in the same environment. They originate from the fact that the radio access selection can consider the resources from several radio accesses (i.e. “trunking gain”), multi-radio access diversity (at not too high load levels), better match of the available resources to the geographical distribution of the traffic, etc.

In the evaluation of both fast and slow access selection, the latter has been chosen as the preferred realization. The reason is that fast access selection implies a much higher degree of complexity and required changes to existing RATs, while already with slow access selection significant gains can be achieved.

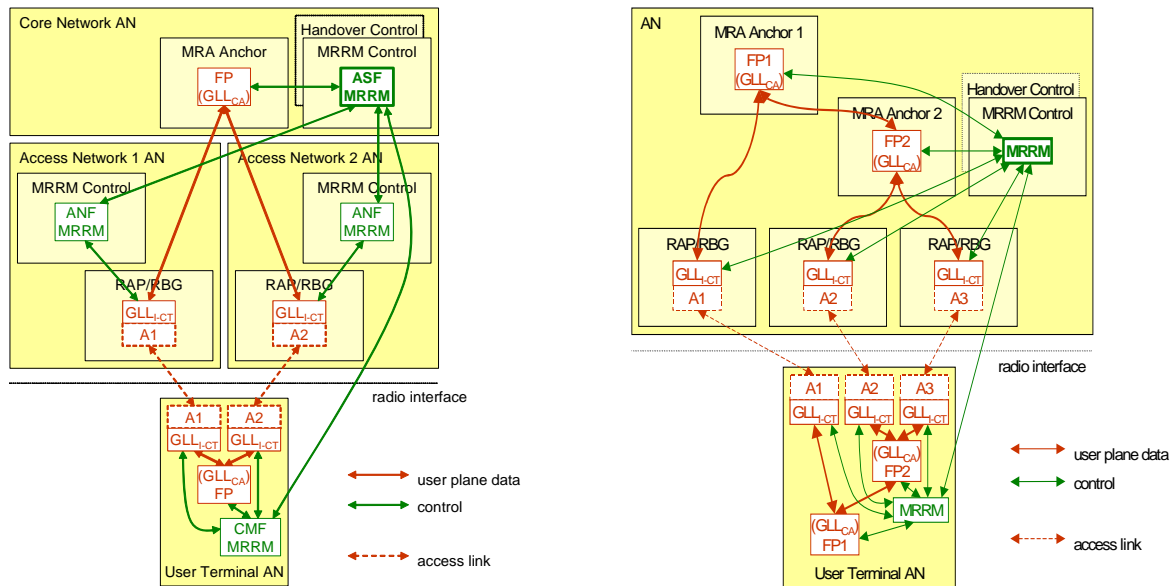
3.3.1.3 MRA Target Architecture

While the MRA FEs description refers to a layering protocol abstraction of the MRA architecture, the target MRA architecture is defined in terms of logical nodes, which corresponds to a set of function units of MRRM and GLL [20]. That is, depending on the functions deployed various logical nodes are identified. As mentioned, the MRRM complements the radio technology specific Radio Resource Management (RRM) such that the selection to activate one RAT for a user session is decided in the MRRM. The decisions are based on link state information provided by the GLL entity in the radio links as well as on other available information, e.g. requested QoS, network and cell load or terminal capabilities. However the actual execution to activate an alternative access is done by a Mobility or Handover Control (HC) function that controls the data handling in a Forwarding Point (FP) when switching over the user session to a new access flow. The FP is located in MRA Anchor point and coincides with the GLL Context Anchor (GLL_{CA}) task of MRA.



WIRELESS WORLD

RESEARCH FORUM



(a) MRA Architecture with distributed MRRM

(b) MRA Architecture with multiple MRA anchors

Figure 11: Multi-Radio Access Architecture examples

The second task of GLL is the GLL Interface and Context Transfer (GLL_{I-CT}) which provides a generic interface and support functionality for transmission over an access link. GLL_{I-CT} is located at the Radio Bearer Gateway (RBG) or Radio Access Point (RAP). Based on certain rules and thresholds (event filtering and classifications) it reports link events (triggers) to MRRM. Also, in case a flow is handed over between different GLL_{I-CT} entities, it supports link layer context transfer. The additional context transfer support is provided by the GLL_{CA} where copies of the link buffer data are kept until context transfer between GLL_{I-CT} is successful. Note, that GLL_{I-CT} and GLL_{CA} provide functionality for coordination between different RATs; transmission over the radio link is still based on RAT specific radio protocols.

The MRRM can play different roles depending on the actual coordination situation on the access selection between several MRRM entities in the network. The distribution of the MRRM is shown in Figure 11(a) with additional indication of the MRRM role. An access network control function (ANF) monitors access network related parameters, while the connection management function (CMF) monitors the access flow quality for the user terminal AN. An access selection function (ASF) is responsible for deciding on the best-suited access for user traffic. Figure 11 shows the principle of the architecture for a single hop, single operator case. In this case, the different MRRM Control entities in the network (ANF, ASF) can be merged into a single MRRM Control entity which collects the information from the different GLL_{I-CT} entities in the network as well as from the MRRM in the User Terminal (UT). The MRRM Control in the network performs the access selection and handover decisions while the handover execution takes place in the appropriate FPs via HC.

In some MRA scenarios it may be advantageous (or even necessary) to use different access selection and handover procedures for different combinations of access technologies. A reason can be that different radio accesses use different types of locators/flow identifiers. The



WIRELESS WORLD

RESEARCH FORUM

level in the network hierarchy at which different access technologies are ideally combined may also depend on the characteristics of the access technologies, e.g., their cell size. The HC function is responsible for selecting the handover procedure. To support these different ways of integrating the accesses, the MRA architecture is flexibly defined to handle multiple MRA anchor nodes. Each of the MRA anchor nodes can contain different types of FP entities; see Figure 11(b) for a case with two anchor nodes. There are three different possible access flows between the two FP1 entities in the figure. The FP2 entities map the higher-level access flows to internal access flows. The type of locators used for the flows between the two FP2 entities may be different from the ones used between the FP1 entities. MRRM may change the higher-level access flow to internal access flow mapping in the FP2 entities without affecting the state installed in the FP1 entities. Note that the FP1 and FP2 entities in the User Terminal AN may in reality be a single FP entity, e.g. when the rationale for the separation is more network related.

Finally, multi-radio access can also be provided by cooperation of different business entities operating separate networks. In the case of full cooperation, the participating FEs from different operators fully share the control over their respective resources. This level has been agreed upon during the composition process and is also configured in the MRRM functions. Effectively, this composition process transforms the mode of operation into a similar mode as for a single operator case. All *relevant* information that is required for the access selection decision is available, e.g., operator-sensitive information such as current congestion level; resource consumption per user; pricing information etc., is freely shared between the MRRM entities and could be used in the access selection decisions. The physical location of the ASF is flexible but it is not envisaged that it can be implemented directly in the RAP from one of the operators. The main motivation to locate the ASF close to the multi-radio access points is to support fast access selection (per packet), however, this is unlikely to exist in multi-operator networks due to the physical separation of the different operators' access points, which introduces long signalling delays. These multi-operator networks are likely to be operated with distributed MRRM entities.

3.3.2 AN Quality of Service

The Ambient Network Quality of Service (AN-QoS) function is responsible to provide dynamic QoS control in ubiquitous mobile environments, in a technologic independent way. The QoS function of an Ambient Network (AN) is able to set technologic independent QoS agreements, by removing the strictly coupling of Service Level Specification (SLS) to the Differentiated model, in order to extend its use to a ubiquitous environment. Moreover, the QoS function allows ANs to delegate and/or share control over their overall network resources, including the support for QoS-aware handovers. This QoS control is done in enhanced scenarios that may include multi-connected ANs and multi-paths between two ANs.

Relations to the ACS Interfaces

The AN-QoS functions of different ANs use a QoS signalling protocol to exchange QoS control information. This QoS signalling protocol is part of the Generic Ambient Signalling Protocol (GANS), which is capable of transporting different types of signalling information between ANs via an ANI.



WIRELESS WORLD

RESEARCH FORUM

The AN-QoS can use an ASI to inform applications/services/users about actual properties such as network properties, transmission characteristics or cost. AN-QoS can also use an ASI to collect QoS requirements from applications/services/users.

The QoS function can use the ARI to:

- Map the SLS to different intra-domain provisioning schemes that can be used by different providers;
- Map the QoS signalling of GANS to the different signalling approaches below the ARI;
- Query possible traffic engineer network elements such as MPLS or enhanced routing schemes.

Management, Security and Performance Considerations

Each AN needs a set of QoS policies. The QoS functional area must indicate what the consequences of violating a QoS agreement are. Moreover, SLSs must avoid the forging of negotiating entities, and Denial-of-Service vulnerability.

3.3.3 AN Congestion Control

The Ambient Networks Congestion Control (AN-CC) function is a collection of congestion control-related mechanisms, operating both in the transport plane, and in the Ambient Control Space. The function will be later further divided into well-defined sub-functions, but at present the time, it is too early to suggest such a split.

The envisaged AN-CC architecture would allow the transport plane and ACS mechanisms to obtain more information from network conditions than presently used congestion control mechanisms. At least part of this information would be obtained from related functions, especially from AN-QoS, potentially from mobility and from traffic engineering functions. Information available from AN-CC could be used in, for example, routing decisions by other functions in the ACS.

Relations to the ACS Interfaces

Any function that would benefit from having knowledge on the state of congestion in the network may access the congestion control functions through the interfaces. Examples include functions that can provide information that would be used by the congestion control mechanisms, such as AN-QoS and, most likely, mobility.

The AN-CC will feature a substantial transport plane component, which would communicate with the ACS component via ARI. Also communication with the transport plane parts of the GLL, if deemed beneficial, would take place through ARI.

Management, Security and Performance Considerations



WIRELESS WORLD

RESEARCH FORUM

The AN-CC should, to feasible extent, be immune to various strategies present-day congestion control schemes are vulnerable to. Explicit authentication mechanisms must be deployable for configuration/management access.

Critical issue in AN-CC design is the scalability of the possible inter-node communications / feedback. Therefore, AN-CC in the ACS is only involved in non-flow specific communication. That is, only “meta” information among functions is signalled (via ANI), and “per flow” signalling takes place via in-band signalling, and not involving ACS. Exceptions are possible and for further study.

3.3.4 Mobility Control Space

The Mobility Control Space consists of the following FAs:

- Mobility Triggering Management
- Handover and Locator Management
- Moving Network Support
- Reachability Management.

3.3.4.1 Mobility Triggering Management

The mobility triggering management FA is responsible for collecting and identifying triggers from different sources and processing these triggers, which may in turn initiate some mobility management actions, such as:

- Handover Decision (within Advanced Handover FA);
- Routing Group formation (within Moving Networks FA).

The Mobility Triggering Management FA is illustrated in Figure 12.



WIRELESS WORLD

RESEARCH FORUM

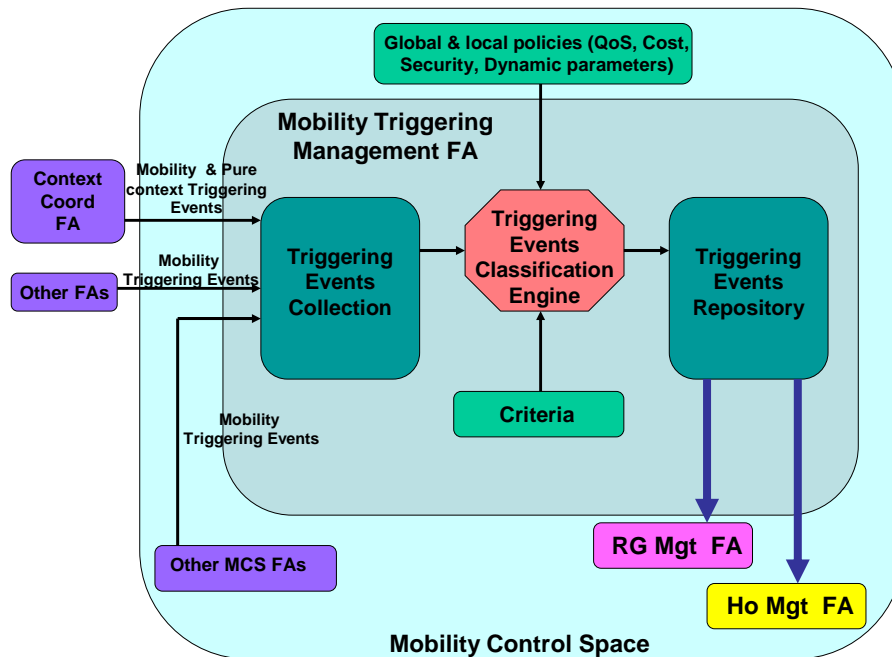


Figure 12: Mobility triggering management FA functionality view

Mobility management decisions need to be done based on various triggers, which in some cases may be conflicting. In order to take a handover decision, it is necessary to consider numerous triggers of very different types and origins. Some of the events may be seen as forcing triggers, while some might be suggesting hints, either predicting or triggering. The difference between triggering and predicting is that the latter enables anticipation of a seamless handover.

3.3.4.2 Handover and Locator Management

The Handover Management functional area aggregates all the procedures needed to perform various types of handovers to support mobility in the ANs. These include handovers between communication access points within a single radio network, between different access technologies, mobility between different IP address spaces, multiple service provider domains (i.e. network layer mobility), or application level handovers between different terminals.

HO Management is core part of the MCS, which in turn is located within the ACS, as shown in Figure 13.



WIRELESS WORLD

RESEARCH FORUM

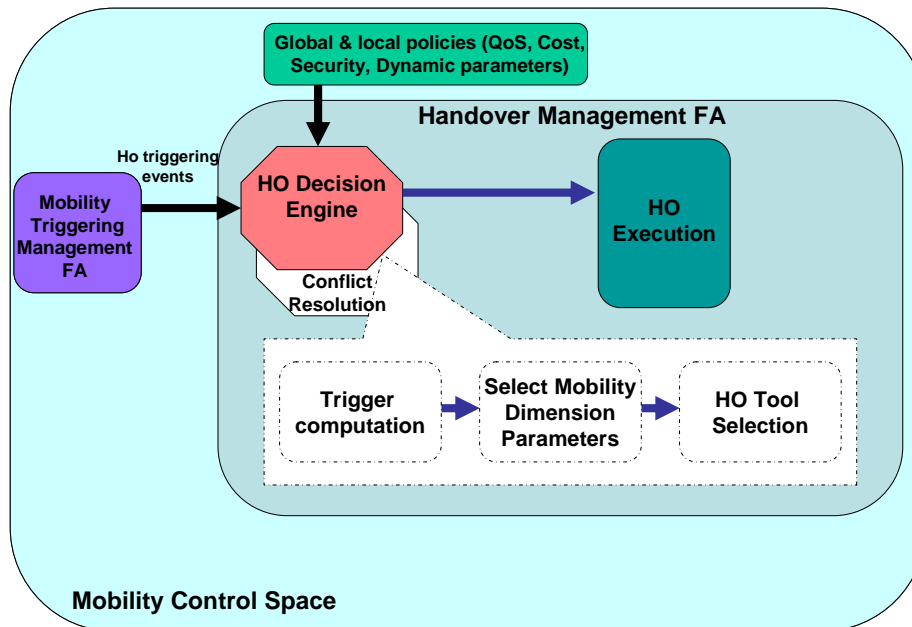


Figure 13: Handover management FA

In designing this FA the various intra (mobility) and inter (context management, multi radio resource management etc.) control space functionalities are taken into consideration in order to define a coherent Ambient Control Space. For example HO trigger input is provided by the Mobility Triggering Management FA of the MCS and this is used by the HO management FA. A description of the functionalities embedded with the HO management FA is given below.

The handover decision engine will determine by the triggers received from Mobility Triggering Management FA and the policies valid at that time, if a handover should be performed. In addition it will determine which type of mobility dimension is going to change (physical location, access technology, address space, trust domain, provider domain, and device) and how to accomplish this type of HO by using the different HO tools. Included in this is whether the HO will require a change in locator.

HO conflict resolution is an essential part of the Handover Decision Engine, that will resolve conflicts resulting from actual triggers and policies (global or local) using for example dynamic production rules to make decisions on goal basis.

A HO can require decisions at different steps. For example, some mobility events require post HO optimizations such as renegotiation of QoS, optimization of routes etc. HO Management FA would utilize mechanisms from Routing Group Formation FA (intra control space) and Context Management functions (inter control space) for providing possible optimizations in order to enhance pervasive computing within the AN architecture.



WIRELESS WORLD

RESEARCH FORUM

3.3.4.3 Moving Network Support

This FA copes with the formation, maintenance and management of Routing Groups and optimizations required for the mobility of such groups of nodes.

Figure 14 shows high level functions belonging to the FA and the information flow inside this FA and towards other FAs. Its main functionalities will be the collection of relevant inputs and hints that may be used for the formation of the RG; these should be processed in order to create the RG. Once the RG is already established, it needs to be maintained; e.g. new nodes may join, former members may leave, etc. In addition, the interconnection with external networks has to be provided by means of a Gateway that needs to be maintained continuously. All this information will be used by some optimization processes that will take advantage of the information so as to bring up improvements, both on an intra- and inter-RG level (i.e. communications inside the RG or to external entities).

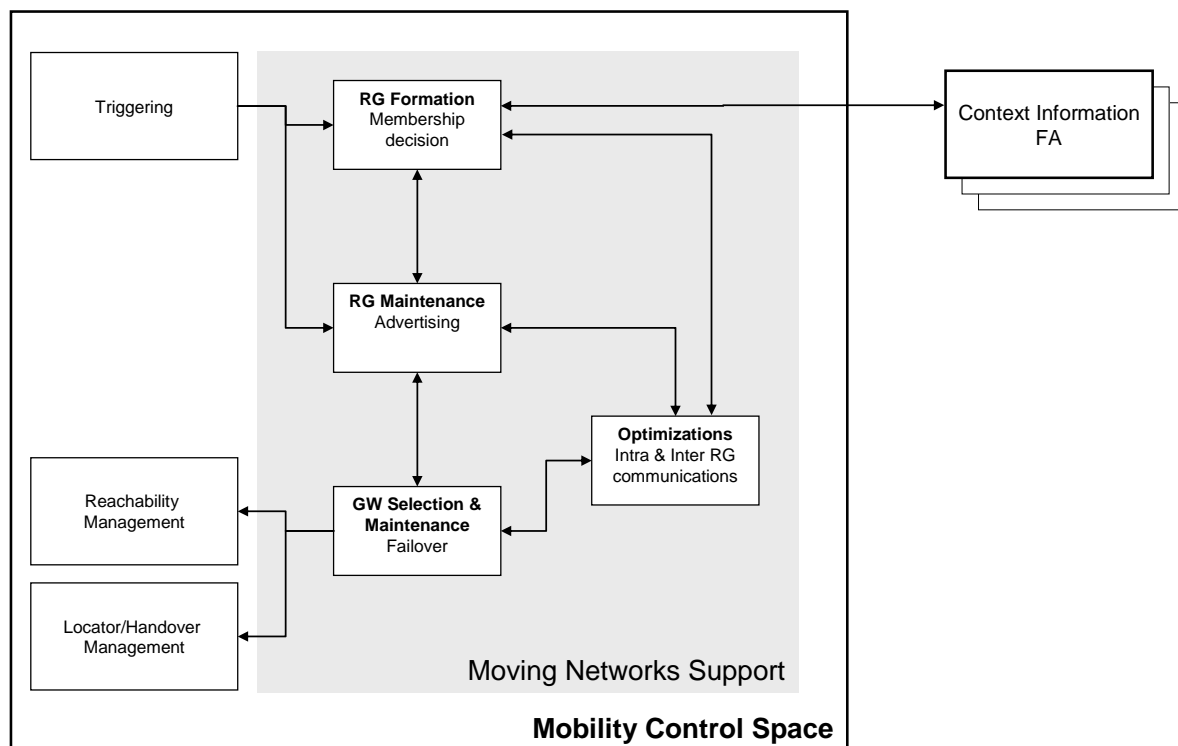


Figure 14: Moving Network Support FA

3.3.4.4 Reachability Management

This FA is responsible for enabling a CN to initiate communication with a mobility endpoint regardless of its current location. This involves providing a mechanism to allow a CN to resolve some identifier onto the current location of the ME. Examples of current techniques for supporting this type of functionality include DNS and SIP registers.



WIRELESS WORLD

RESEARCH FORUM

The ME may have multiple identities and points of presence in a multi-homed and multi-domain environment. Therefore, the ME identity may translate into different identifiers in different domains, e.g. ME's identifier in its corporate network to which it is connected over a VPN is different to the identity the same ME is using locally to access services in the visited network anonymously.

Therefore, identities used by the ME have different scopes, and each may resolve onto multiple locators. The context of the communication determines what kind of identifier should be used and the type of the identifier implies what directories or registers should be used, and how to bind the name to the lower-layer identifiers, i.e. the actual location management scheme.

For the Reachability Management FA the following functions are considered:

- **Location Registration and Maintenance**

To achieve global reachability, Mobile Entities need to register their location (reachability state) somewhere in the network to allow correspondent nodes to resolve the identifier onto the current locator for the ME. When the locator associated with the identity changes, either because the device has just initiated communication after being idle, or because of a handover event, the identifier to new locator mapping information must be updated.

This functionality provides efficient and secure means to derive locator mappings based on multiple identifiers. It supports dynamic locator and identifier mappings with varying degree of privacy requirements, i.e. anonymous operation should be possible if the local policies allow that.

Update of location information can be associated with handover of ME or other triggering events, e.g. such as paging.

- **Location Resolution**

If a CN wants to contact a ME it needs to obtain a locator to use to establish communication. To accomplish this, the CN initiates some sort of resolution procedure using the ME identifier that will ultimately lead to the data being sent to the current location of the ME. This resolution may include a simple identifier to locator resolution returned to the CN, or may utilize more complex functions such as a rendezvous mechanism where a third party node is responsible for forwarding communication requests.

Security and Performance Considerations

Security is required to protect the identifier (naming) scheme and the identifier/locator mapping. Only the nodes in the network (usually only the ME, but the ME may choose to delegate authorization to other nodes) that are authorized to update these bindings are able to access the information.



WIRELESS WORLD

RESEARCH FORUM

This functionality can be implemented as one or more directory functions in the network. Where multiple directories are used, this FA has to manage synchronization of state between directories to ensure consistent information is made available. The use of multiple directories supports redundancy and allows resolution requests to be handled quickly as locally as possible to the requesting CN.

3.3.5 Smart Multimedia Routing and Transport

A key innovation of the Smart Multimedia Routing and Transport (SMART) architecture [12] is the concept of *Service-Specific Overlay Networks (SSONs)*, which are separately deployed for every media delivery service (or group of services). This allows the configuration of appropriate high-level routing paths that meet the exact requirements of a media service on QoS, media formats, responsiveness, cost, resilience, or security). Additionally, the concept allows the transparent integration of network-side media processing capabilities (such as caching, adaptation and synchronization) into the selected end-to-end delivery paths.

Apart from the SSONs, the proposed SMART architecture includes the following components:

- **Overlay Control Space (OCS)** – The OCS is the functional area of the ACS that controls the service specific overlay networks. It manages the creation of SSONs on requests received through the ASI (e.g. from service providers, customers, etc.) and controls the re-organisation/adaptation of existing SSONs, which might become necessary due to changes in the underlying ANs (connectivity, composition, QoS, mobility, media processing functions, etc), changes in the context of a user (e.g., location, user profiles, device capabilities) or changes in the service policy/context.
- **Overlay Node (ONode)** – ONodes are specialized Ambient Network nodes that implement the functionality necessary to participate in SSONs. ONodes can implement the roles of MediaClients (MC), MediaServers (MS), and MediaPorts (MP) – or any combination of those. The MediaPorts, as special network-side functions, have the role of providing value-added functionality, such as caching or adaptation facilities, flow synchronization or special types of routing capabilities, inside the network.
- **Overlay Support Layer (OSL)** – The OSL embodies the basic overlay network functionality required in every ONode. The OSL is responsible for the packet handling in the overlay, which might include means to tunnel/un-tunnel packets between ON nodes.

Figure 15 illustrates how the SMART architecture relates to the overall Ambient Network architecture. It also shows the relation of the OCS as a Functional Area within the ACS.



WIRELESS WORLD

RESEARCH FORUM

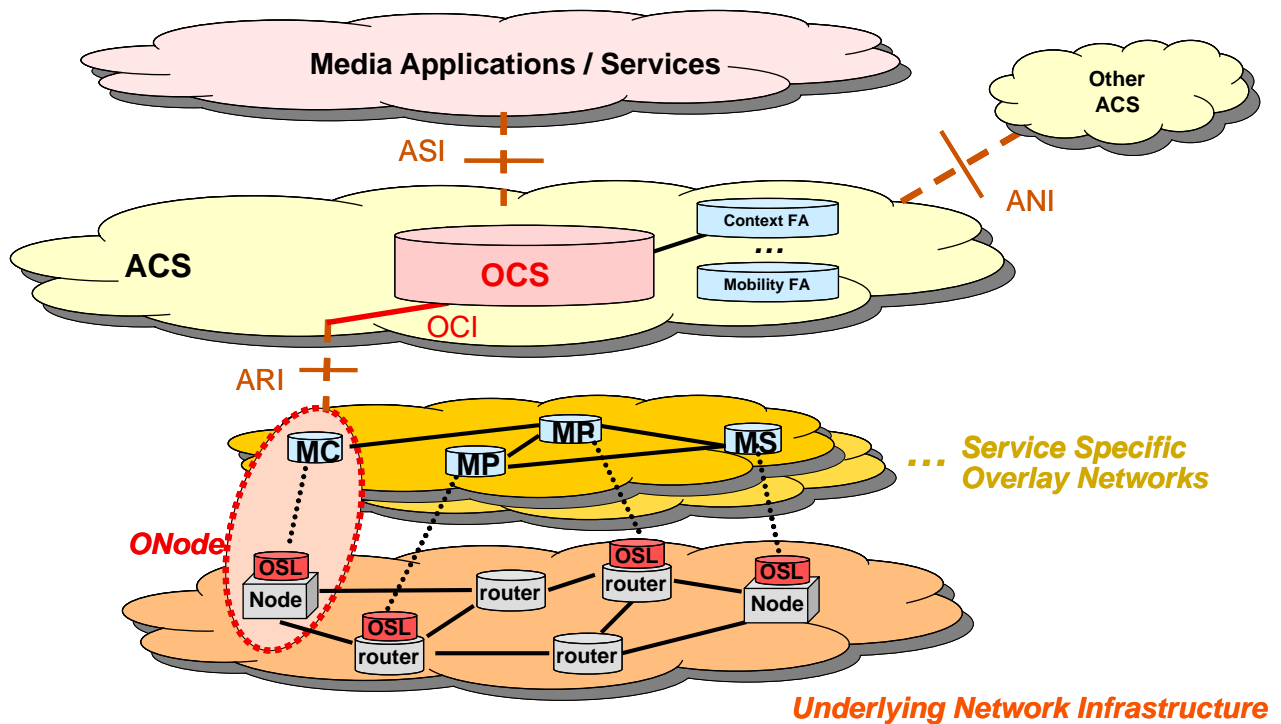


Figure 15: Smart multimedia routing and transport architecture

3.3.5.1 Overlay Control Space

The OCS is the functional area of the ACS that controls the service-specific overlay networks (SSONs) of the SMART Architecture. The idea behind service-specific overlay networks is to enable the flexible and dynamic creation of “virtual networks” (on top of the underlying network) that are tailored towards the specific needs of a particular media delivery service. Different SSONs can be created to account for different types of services, subscriptions levels or authorizations.

The OCS is responsible to manage the creation of SSONs upon requests from users of the AN (e.g., service providers or customers) and to control the reorganization or adaptation of existing SSONs, which might become necessary due to changes in the underlying ANs (for example, connectivity, composition, QoS or mobility.) This re-organization/adaptation may imply adding/removing of overlay nodes or virtual links. The OCS also controls the addressing and routing on the service-specific overlay networks.

As the OCS is implemented as part of the ACS, the OCS is able to obtain initial context information needed for the establishment of SSONs as well as updates/changes from other functional areas of the ACS, e.g., connectivity or mobility.



WIRELESS WORLD

RESEARCH FORUM

The OCS is purely a control function integrated in the ACS. As such, it has interfaces for external access/control (ASI), for control of the user plane functions (ARI) and for communication with OCS functions in other Ambient Networks (ANI.)

The part of the ARI facilitating the communication between the OACS and the user plane components of the SMART Architecture, namely the Overlay Support Layer (OSL) and the MediaClients, MediaServers and MediaPorts are referred to as OCI.

Use Cases

An example of the use of SMART multimedia functionality is a TV media-streaming provider who wants to establish a content distribution network in Europe. In order to make the whole network scale to a large subscriber base, the provider needs to deploy caches at the edge of the network. In addition, to maximize the potential users/customers, the media provider wants to supply the video streams in a large variety of classes (tailored towards end-user terminals.)

The media providers' servers contact the OCS of a composed European Ambient Network to be registered. The OCS will then setup an appropriate content distribution overlay for this particular service via the MediaServers and MediaPorts of this TV media-streaming provider.

- Discovery and selection of appropriate MediaPorts (to provide the caching and media adaptation functionality.)
- Establishment of the service-specific overlay networks.
- Configure the OSL appropriately on overlay nodes (MediaServers, MediaClients and MediaPorts.)
- Configure the virtual/overlay links between overlay nodes of this SSON.
- Configure initial routing information (SSON-level routing tables) and if necessary a dynamic routing process for the SSON.

Relations to the ACS Interfaces

The OCSs themselves communicate with functions of the local AN and with OCSs of other ANs. We expect that communication with functions of remote ANs is handled through their local representative (i.e., the identical function in the local AN.)

Media streaming services, content provider services, network provider services, third-party MediaPort services, and User applications are all expected to interact with the OCS in order to use and/or control SSONs, and in order to provide "external" information (e.g., user profiles, management information, and MediaPort information) to the OCS. Content providers and consumers use the ASI in particular to control the delivery/receipt of multimedia sessions/flows.

The OCS controls/manages the Overlay Support Layer (OSL), which provides the overlay functionality in the physical AN nodes (overlay nodes), and MediaClients, MediaServers and MediaPorts through the ARI. This part of the ARI is called the Overlay Control Interface (OCI.) The OCI is used to configure updates of routing tables at the overlay level, adaptation of media content to inform MPs about which flows need to be adapted and how this adaptation



WIRELESS WORLD

RESEARCH FORUM

should be done as well as how caching of media content is to be carried out. The OCI interface is bi-directional: the OCS controls/manages the OSL and MCs, MSs, and MPs through it; and in the reverse direction these components inform the OCS about changes or any information/updates that they acquire at the user plane.

Management, Security and Performance Considerations

Management considerations include management of SSONs and MediaClients, MediaServers, and MediaPorts as well as routing configuration/management for SSONs.

End-to-end security of multimedia data/streams is not generally desirable from a SSON point of view as it limits what can be done within the network on the flows in terms of caching, adaptation and smart routing. However, there is a tradeoff between the level of security and what you can do with to a flow within a network.

The design of the OCS might follow a centralized or distributed approach depending on the design of the ACS (see OCS description) and/on considerations regarding the SMART architecture.

3.3.6 Context Awareness

The Context Awareness architecture [13] is predicated on the existence of two main functional areas, one implementing the interface between the Context Awareness architecture and other AN functional areas and the second one implementing operations, which are internal to the Context Awareness architecture. As shown in Figure 16, these functional areas are context coordination (ConCord FA) and context management (CM FA), which are described in more detail in the following paragraph.



WIRELESS WORLD

RESEARCH FORUM

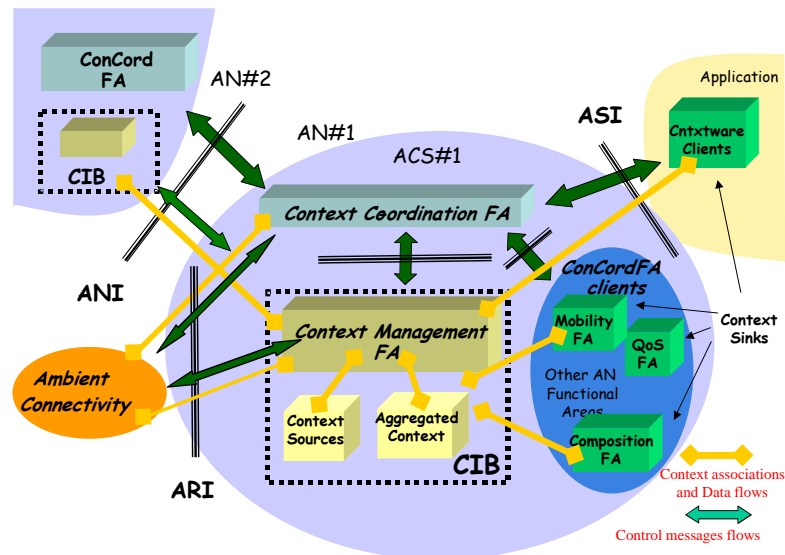


Figure 16: Overview of Context Awareness Functional Areas

3.3.6.1 Context Coordination

This functional area aims to coordinate information exchange between the different functions that are being developed in the AN project.

Earlier work in the AN project has shown that most of those functions would benefit from the availability of context information to improve their operation. Collecting the information relevant to each entity and redistributing it to the relevant entities, through the maintained CIBs, can achieve this. Each CIB contains up-to-date context information (e.g., user-related information like available devices and identities, network-related parameters such as the available media ports, available QoS and available security level.) This information is important for the operation and decision-making of the other functions (e.g., information to decide if an entity should compose with another, if it should perform handover, what types of access are available.)

The context coordination is the first point-of contact for any context client. This is where context information is requested, type and quality of context is negotiated and possible conflicts are investigated. Context coordinators also negotiate context-level agreements (CLA) between domains to enable exchange of context information across domains.

The envisaged functions implemented by the context coordination functional area are:

- Subscription Management
- Negotiation Management
- Conflict Resolution



WIRELESS WORLD

RESEARCH FORUM

Figure 17 illustrates the relationships amongst them and the functions of the context management functional area. These are described in more detail in the following three sections.

3.3.6.1.1 Subscription Management

This function takes care of establishing the right associations between context sources and context clients. This function is normally called by end-user services through the ASI. It can also be called by network services (i.e., other functions of an Ambient Network) that need to specify particular context information they are interested in. This information is processed and if the client is allowed to access the information the CM function creates an association.

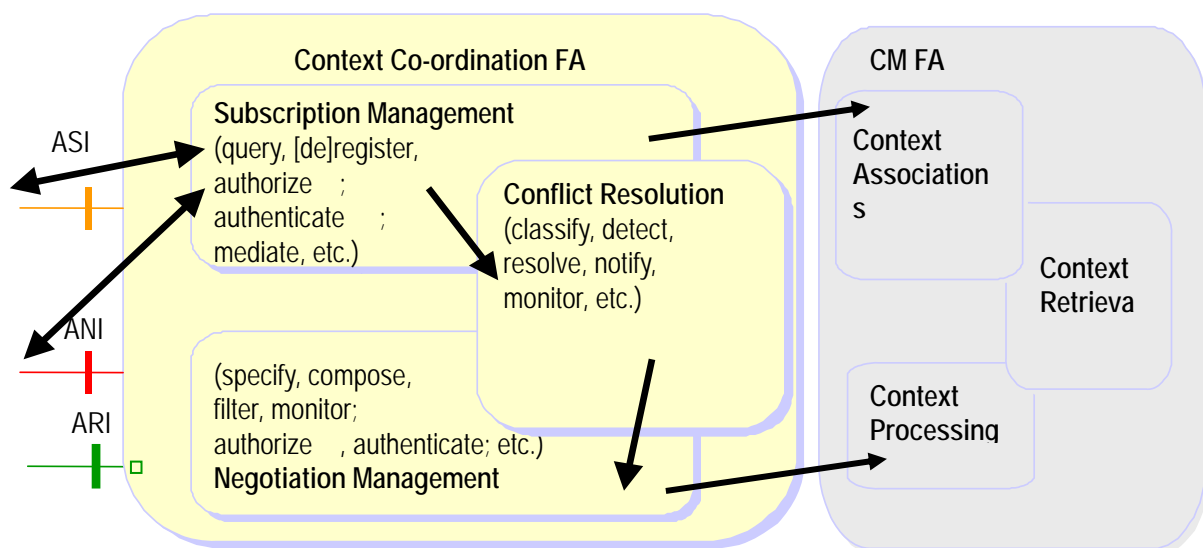


Figure 17: Context Coordination

This function calls the association management function in the CM functional area.

3.3.6.1.2 Negotiation Management

This function's main duty is to negotiate between entities requesting context info and providers of context. Negotiation might happen because of two reasons:

- The requestor is not allowed to access all the information it requests or the information requested is not available at the level of quality expected. In this case, a negotiation may take place to agree on a lower quality of context to be delivered or on a subset of the original request to be delivered or to perform some further authentication (if the problem is the missing credentials.)
- The requestor is asking for information not readily available which would possibly be created through processing of raw data available (i.e., this function would call the "context processing" and instruct it on how to create the information requested.)



WIRELESS WORLD

RESEARCH FORUM

This function calls the context processing function of the CM functional area and may be called by the “conflict resolution” function. This function may cooperate with negotiation management functions in other ANs, with the context retrieval/update functions and with negotiation management functions in other ANs through the ANI.

3.3.6.1.3 Conflict Resolution

This function's main feature is to identify and manage possible conflicts that arise in the exchange of information between administrative domains, e.g., some context information requested by some other functions may conflict with user policies or network policies which prevent that type of information from being shared.

It may call the above negotiation management function in case some negotiation needs to take place to resolve a conflict. It is called by the “subscription management” function to check that the subscription request creates no conflicts.

3.3.6.2 Context Management

The CM functional area will be devoted to the management of a set of context information bases (CIBs) within and across domains. The management of the CIB(s) will involve operations such as collection, description/modelling and dissemination of context information to the interested entities as well as managing the sharing of this information between different domains (cross-domain management.)

The CM functional area will also be responsible for scheduling interactions between context sources and context clients, monitoring of these interactions and re-allocation of interaction channels in case of context changes. Finally, it will aggregate and compose context according to clients' requirements. Context management is initiated through the context coordination functional area. The envisaged functions implemented by the context management functional area are:

- context associations management;
- context retrieval;
- context processing.

Figure 18 illustrates the relationships amongst the above functions and how they interact with the ones of the ConCord functional area. The following paragraphs add more detail to the description of these functions.



WIRELESS WORLD

RESEARCH FORUM

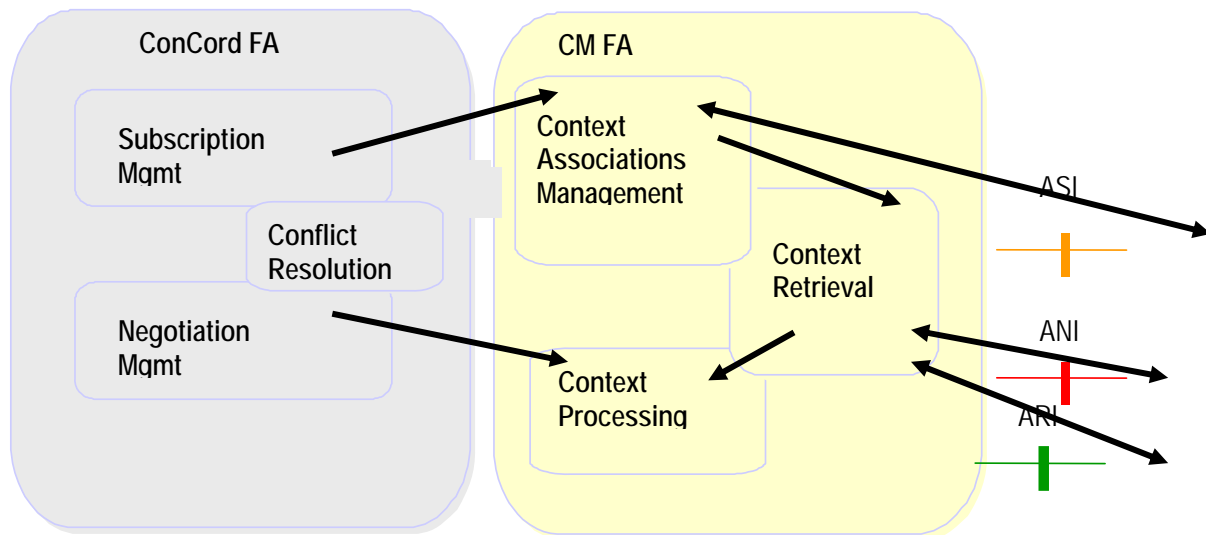


Figure 18: Context Management

3.3.6.2.1 Context Associations Manager

The purpose of this function is to manage associations between various context clients and different context information data and to notify the subscribing clients of changes. This function encompasses:

- registering entities in the AN space;
- managing association between context aware clients and context sources;
- grouping context sources associated with context aware clients;
- managing access to context information: indexing, persistent subscription and scheduling;
- publishing of context and client notification.

This function is called by the subscription management function in the ConCord functional area whenever a new context association has been agreed. It calls the context retrieval and context processing functions to fulfil the agreed context associations. It notifies context clients (other functions or services) of context changes. This function may cooperate with context association management functions in other ANs through the ANI. Modelling of context is crucial for the successful implicit notification methods. Context-sensitive publishing and advertising is an important issue since performance will depend on the correctness of information delivery and freshness of this information

3.3.6.2.2 Context Retrieval

Context varies significantly based on the situation where ANs are deployed. Thus, a powerful and efficient system for context retrieval is required in the AN space. The CM functional area includes the context retrieval function that provides the essential methods to lookup, fetch, search and index context information of the AN space.



WIRELESS WORLD

RESEARCH FORUM

Methods provided:

- monitoring of context information;
- indexing of context/network schema for context;
- network storage and back up of context;
- context usage monitoring for context managers and services;
- view management of context information.

The negotiation management calls this function via the context association manager. The context retrieval function can retrieve context information from other ANs through ANI, from context-aware network services through the ASI, from context-aware network services through the ARI, from CIB network resources and from resources that might be sources of context information. These resources include: context depots, context depot networks, QoS enforcement points and CIB database gateways. Context depots are network nodes that run as user-level processes. Depots provide context processing and storage resources to context clients and they form a context aware depot network (CDN), which is a data directory, monitoring and management system for context (i.e., the CIB realization.) The context depots form an overlay transit layer functionality built on top of the AN network. Indexing is an important issue since performance will depend on the speed at which context information is retrieved and updated.

3.3.6.2.3 Context Processing

The purpose of this function is to manipulate raw context information data, based on knowledge from the context association manager. Creating and running the appropriate algorithm for aggregating and composing context could handle requests for higher-level context aggregation. This context processing is context-association-agnostic and is invoked when needed by the context retrieval function.

Methods provided:

- aggregating context information;
- composing of context;
- filtering and semantic searching.

This function is called by context retrieval. The negotiation manager in ConCord functional area may call this function.

3.3.7 Agreement establishment and execution

The Ambient Networks project is fundamentally dealing with enabling dynamic business relationships and service/compensation mechanisms between different authorities. This is manifested in instant establishment and execution of agreements between ANs.

The AN agreements framework extends traditional trust establishment frameworks, like e.g. AAA (Authentication, Authorization and Accounting). Allowing entities to dynamically establish



WIRELESS WORLD

RESEARCH FORUM

and execute completely new services requires a set of new control functions/objects, or extensions to traditional functions.

The focus of this section is on security and trust related functions/objects related to agreement establishment and execution, for more details see [14]. It is for further study to determine whether these functions/objects constitute an “Agreements Functional Area” in itself or whether they are more appropriately allocated to other FAs.

3.3.7.1 Agreements and security domains

The draft agreement process is depicted in Figure 19, describing the phases of establishment and execution including iterations, recursions and exception handling.

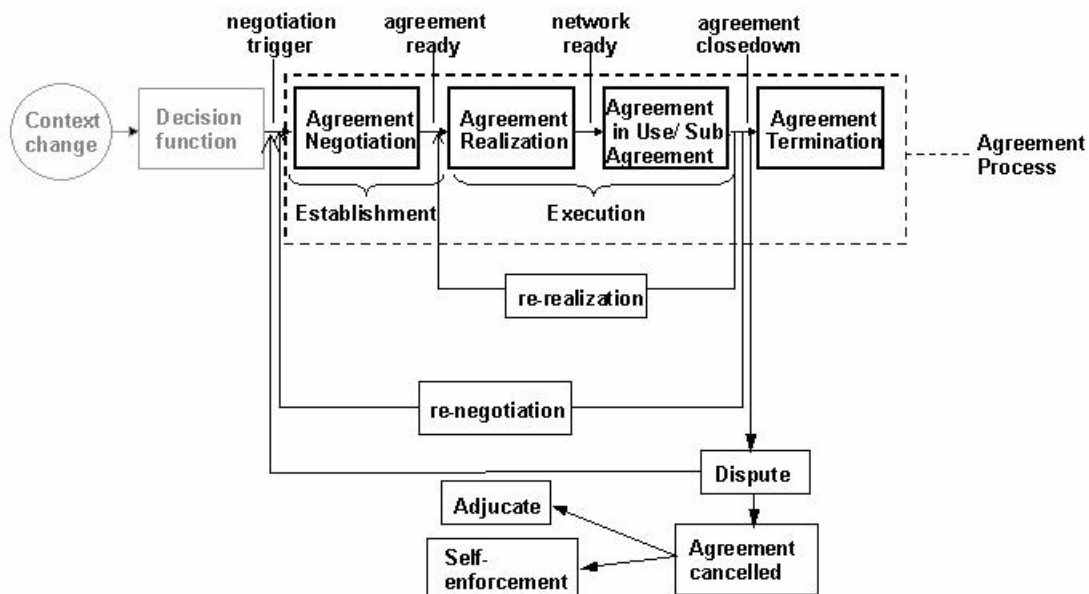


Figure 19: Flow chart representation of the agreement process

The agreement establishment phases have many similarities regardless of what is being negotiated. While the execution of an agreement depends on what this particular contract is about, some aspects of the execution are though still independent of the content of a particular agreement, e.g. the enforcement of policies associated to the contract.



WIRELESS WORLD

RESEARCH FORUM

The *AN Security Domain* is defined as one or more ANs with a common authority and a common set of security policies. There are intricate dependencies between the security policies in the security domain and those appearing as a result of a new agreement.

Figure 20 shows an example of agreements between two authorities of administrative domains and visualizes between which AN security domains the agreements are applicable.

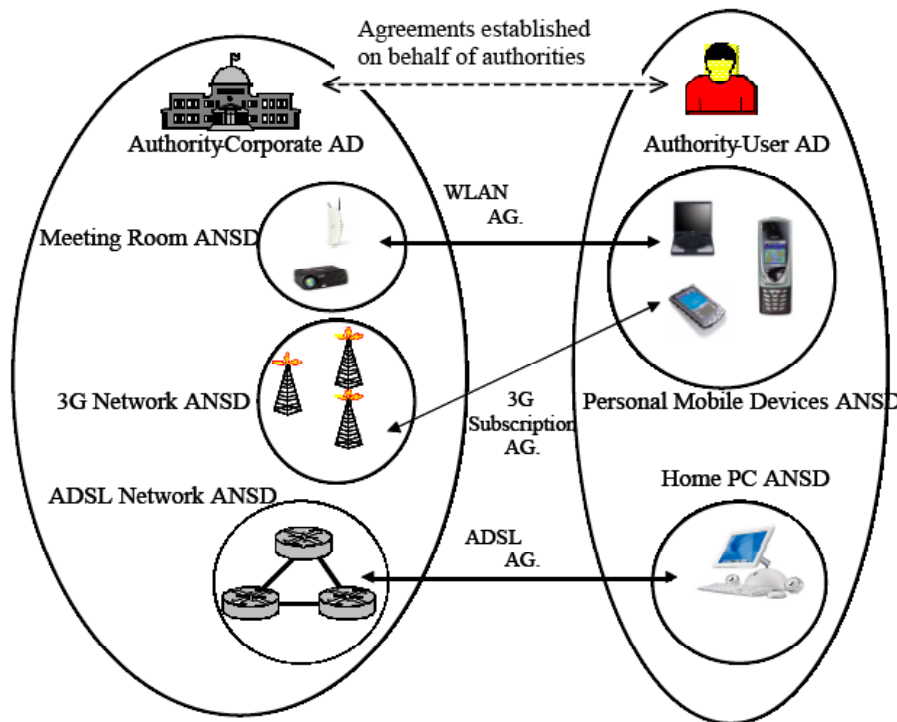


Figure 20: Agreements between AN Security Domains

We outline some important objects involved in managing the agreements between security domains, possibly distributed among the ANs in a security domain. Figure 21 shows a configuration of objects instances residing in two different AN security domains.

The authority of a security domain is represented by the *Administrative Domain Controller* (ADC). This object may offer capabilities to interact e.g. with operation personnel via a GUI or might appear to the user as menu entry on OS level, depending on the size and complexity of the systems the security domain encompasses. The ADC has control over a set of *Security Domain Managers* (SDMs), which exist in each security domain that is capable to participate in agreement establishment procedures. The role of the SDM is to manage the establishment, change and termination of agreements between security domains. For this purpose it communicates with an SDM in other domains.



WIRELESS WORLD

RESEARCH FORUM

The SDM is assumed to have the necessary information to decide if the agreement can, shall or must be accepted but delegates the task of negotiation to an *Agreement Negotiator* (AGN). This AGN will interact with the respective AGN instance in the other domain and will conclude the negotiation either positively or negatively, and the SDM is informed about the result. In case the negotiation is completed with a positive result, the SDM will take action and create an *Agreement Execution Agent* (AEA).

The main purpose of the AEA is to maintain the details of the agreement and manage and control the enforcement of the security policies that have been agreed upon.

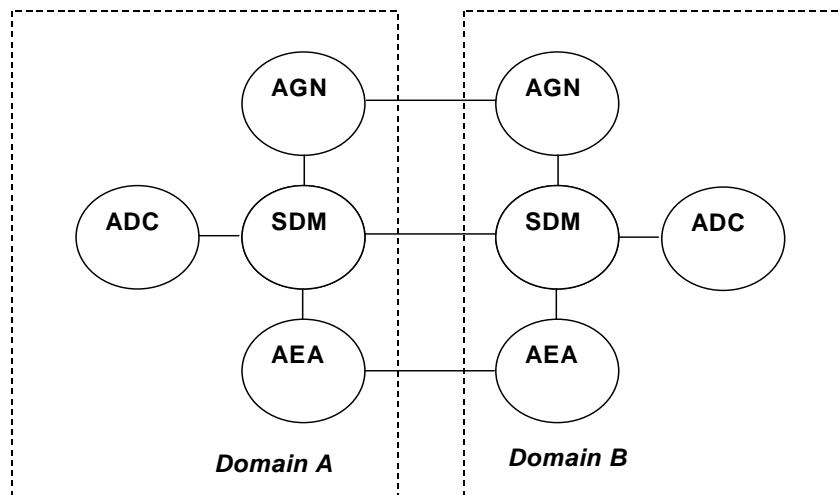


Figure 21: Object reference configuration for Agreement Establishment procedures

Relations to the ACS Interfaces

We foresee two different types of interfaces over the ANI, depending on whether the agreement is established with information from a third AN or not. The first type of interface is between the ANs negotiating an agreement. The second type of interface is between one of the interacting ANs and a third AN which can provide relevant additional information such as trust/PKI related information or previous agreements. This interface is between ANs that have a previous agreement. The detailed mapping of interfaces to the functions described above is for further study.

We believe that all requests through the ASI will first go through a resource discovery and/or some context management/decision making function.

The context management function or decision-making function could invoke the agreement negotiation function, e.g., due to input received through the ARI.



WIRELESS WORLD

RESEARCH FORUM

Management, Security and Performance Considerations

The contract resulting from the agreement is an important asset as discussed above and must be managed appropriately, e.g., it may need to be executed a long time after establishment and a garbage collection of expired contracts may be required. The security measures necessary for establishment and execution of an agreement depend on the type of agreement. Some examples of security aspects relating to agreement establishment:

- authentication of negotiating parties (though not for anonymous services, for example);
- non-repudiation of agreement;
- denial of service aspects of negotiation protocol;
- privacy aspects of negotiation information and contract.

The separation of establishment of agreement from execution of the agreement as discussed above has a performance benefit, as an agreement may be re-executed without re-negotiation (see Figure 19). For further study: an agreement established by the agreements functional area in one AN may possibly be executed by functions in another AN. There are potential scalability gains with such a construction.

3.3.8 Network Management Functions

Network Management Systems of Ambient Networks must work in an environment where heterogeneous networks compose and cooperate, on demand and transparently, without the need for manual (pre or re)-configuration or offline negotiations between network operators. To achieve these goals, ambient network management systems must become dynamic, distributed, self-managing and responsive to the network and its ambience.

3.3.8.1 Definition of AN Management Scenarios & Research Challenges

A managementware scenario has been developed around the entertainment industry's possible future use of ambient technology for the production, marketing, distribution and consumption of live and recorded content. This scenario is based on the AN Rock Express with the main focus being the arising management issues. We follow a rock band's Summer 2015 European Tour during which they use a special rock train for travel between gigs, as a concert stage and also to host exclusive interviews and present material to special guests and fans that pay to travel with the band. Multiple ANs are set up between different actors on board the trains as well as between actors on and off the train. Temporary ANs will also be set up at the concerts to facilitate information sharing and content distribution between the band and the audience and with friends not able to attend the concert. Potentially, all these ANs will be using different access technologies, and end users will be minimally affected when their connection is transferred from one access technology to another, or when new traffic is added to already restricted resources. At the same time ANs will allow for ad hoc changes in network capacity configuration with minimum human interaction.

To enable such a scenario, management systems have to become sensitive, adaptive and responsive to their ambience. That is, they have to interwork with other management systems



WIRELESS WORLD

RESEARCH FORUM

in an autonomous and dynamic way. When composing two separate networks, one crucial challenge is to join the management systems of both networks into a consistent management system for the composed network. Similarly, when a network separates its management system has to be separated as well. In order to deal with the complexity of composition and decomposition, two novel approaches are being analysed: usage of peer-to-peer technologies and pattern-based management. In addition, innovative self-management technologies need exploring in order to reduce the cost of network deployment and operation and to increase scalability and affordability of Ambient Networks. Two approaches have been developed to enable AN self-management, plug-and-play configuration at individual networking element level and closed-loop-based optimisation mechanisms at network level.

3.3.8.2 Definition and Development of AN Management Approaches

Four management approaches are being developed within the network management work, as can be found in Figure 22:

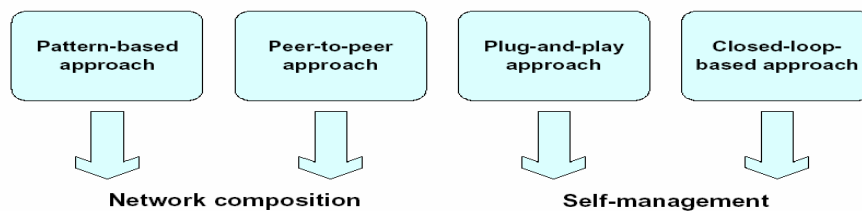


Figure 22: AN Management Application Approaches

Pattern-based Management Application Approach: Pattern-based management is a novel approach to engineering self-organizing management systems for large and dynamic environments. The paradigm makes use of generic distributed algorithms that control and coordinate the processing and aggregation of management information inside the network. A benefit of this paradigm is that such generic algorithms can be re-used for many different management tasks. For instance, an algorithm that allows decentralized polling of device variables in large environments with changing topologies can be applied to maintaining end-to-end connectivity, to dynamically re-configuring network resources for efficient operation, and to deploying services in a scalable manner.

Peer-to-Peer Management Application Approach: AN management applications for network composition perform automated creation, administration, maintenance of the network resources composition process and the resulting (de) composed ANs, for which a peer-to-peer structure is assumed. Composition process refers to the instant negotiation and enforcement of a new Service Level Agreement (SLA) between network resources under composition for the provisioning of an IP service. Two types of AN management application for network composition are under development in WP8. The first AN management application (i.e. topological resource composition) structures the network resources and their topology according to dynamic composition rules/policies. The second AN management application (i.e. service resource composition) is responsible for the provisioning of a QoS assured management service overlay network (known as the Ambient Virtual Pipe or Ambient Virtual Network), which is a network resource facing service. This service overlay network is created dynamically between AN management entities in order to provide QoS assured means of communication channels between management entities in composed ANs or across different



WIRELESS WORLD

RESEARCH FORUM

ANs. It is envisaged that a topological composition would trigger a service composition. Service composition would in some cases trigger topological reconstructions/reconfiguration of network resources

(Un)PnP Management Application Approach: PnP management is responsible for automatic and full configuration of AN elements. It also enables new AN elements to join AN domains. This includes not only the automatic configuration of end-host interfaces as known in current networks but also complete configuration of router elements when they are attached to AN domains and initialization/maintenance of a hierarchical peer structure for management purposes. AN elements may arbitrarily attach to or detach from AN domains, thus incurring dynamics in network topology. Therefore, PnP management not only has to configure newly attaching AN elements, but also to perform constant or periodic verification and optimization of current configurations. Additionally, PnP management must interact with other approaches. A new AN element may interconnect two or more different AN domains. This has to be reported to the composition component, which possibly triggers network compositions in the form of a gatewaying or absorption approach. Similarly, a newly configured AN element modifies the existing network topology. Therefore, PnP management should inform TE management, because the new element may provide additional options to increase network performance.

Traffic Engineering Management Application Approach: In order to explore robust and reactive traffic engineering methods in Ambient Networks the following key problem is identified: the large amount of network state information that is needed to balance the load in the network. In this context network state includes traffic demands, link capacities etc. To facilitate the analysis of how much state information is needed, we divide the problem in two parts: Global view and Local view. The global optimization, utilizes global information about the network state to make a coarse optimization of the routing. The state information is conveyed between nodes in the Ambient Network to perform the optimization. Since an Ambient Network is under constant change it will probably be infeasible to obtain a global view of the current traffic situation in the network. In particular, the trade-off between the accuracy of the input information and the signalling overhead is critical for the performance of the traffic engineering solution. To reduce signalling between nodes, local optimization is performed in each node to fine tune routing parameters using local information. A second key problem is also identified: the performance of constraints on inter-domain traffic engineering between and through ad-hoc networks. Today it is assumed that when different ad-hoc networks meet they merge into one new network. It is not possible for an ad-hoc network to communicate with and via other ad-hoc networks while being a separate network. During analysis of this problem we have investigated how inter-domain communication can be performed between and through ad-hoc networks. From a traffic-engineering point of view this includes the investigation and definition of a solution that performs inter-domain routing on top of ad-hoc networks, based on policies.

3.3.8.3 Definition of AN Management Interactions

A full integration of different management approaches is envisaged in the 2nd phase of the AN project. However, we already analysed how the different approaches relate to each other at a high level and how they will interwork with each other to become a network management system, as well as how this network management system will interact with other parts of the ACS Service management provides support for service management and overlay setup, when requested. Depending on the request, service management asks the plug'n'play management



WIRELESS WORLD

RESEARCH FORUM

and/or P2P management to adapt the current network configuration to the new requirements imposed on the network. Service management uses patterns to define and detect preferred routes depending on the requirements from overlays and services.

3.4 Composition

Network composition is a central theme in the Ambient Networks project. Composition describes a dynamic, uniform process that allows heterogeneous networks to work together and to possibly form larger networks.

Having networks working together is nothing new. Already since the beginnings of telegraphy we have seen networks work together to provide interconnection, allowing customers to reach the customers of other network operators. The advent of mobile telecommunications introduced another way of networks working together: roaming. With roaming, networks work together to increase the coverage for their customers by enabling them to use the networks of other operators. The new aspect that composition brings to network cooperation is the automation of this process.

In today's mobile telecommunications, establishing a roaming agreement involves operator employees travelling to have a physical meeting somewhere in order to cover the commercial negotiations on the roaming contract. Then the technical employees ensure the required network connections are in place and test whether the roaming works satisfactory for the required services. Finally, a few months after the first contacts, roaming between the two operators is in place. Currently this procedure is governed by the GSM Association (GSMA).

Within Ambient Networks we have identified the trend that there are and increasingly will be also smaller forms of networks. People have personal area networks and private residential networks. In fact, we propose that even a terminal by itself can be seen as a small individual network. With these smaller networks, we see an increasing mobility between these networks. Personal area networks, moving networks and ad-hoc networks all involve small networks that continuously change their point of attachment to other networks. It is clear that the old fashioned way of having networks cooperate together does not work for these kind of future communication environments; when an in-train moving network wants to connect to a wireless network operator – essentially a roaming agreement – that process cannot take a few months. Furthermore, it is not feasible to define a new process each time a new network type appears.

So the basic purpose of network composition is to enable networks to cooperate *automatically*. And this network cooperation can be between all kinds of networks, from individual devices in a personal area network to cooperating cellular networks.

3.4.1 Problem Statement and High-level Requirements

This section describes the different requirements that have been considered so as to refine and tune the composition process. One of the most relevant aspects is the heterogeneity of access technologies and the multitude of providers. Today's paradigm in which users do not have a large number of accesses to select from will not longer be valid in the near-future communication scenarios. Many different networks may be available, and the end user would have the freedom to select one or more of the alternatives. This implies another aspect of



WIRELESS WORLD

RESEARCH FORUM

composition; i.e. access to networks where the user (or the users home network operator) may not have any previous agreement or relation with the operator of the network in mind; this is called dynamic roaming.

The composition process framework will support a wide range of different types of co-operation. In addition to roaming, the composition process includes both configurations of Personal Area Networks (PAN's) to joint resource control of large operator networks.

Different requirements and research issues can be identified depending on the characteristics of network co-operation.

3.4.1.1 Composition support for detection of and roaming into „any“ network

Since users are not connected to the same network (operator) all the time (as today), functionality must be provided to

- Detect new networks and their service and access offers.
- Manage trust and support dynamic roaming agreements.
- Support negotiation of terms and conditions for usage of the network services and resources.
- Support for access networks with multi-hop topologies, as long as these networks allow operators to quickly extend their coverage area, see also [42].

Due to the possibly high load of a large number of "unknown" users per time unit, high requirements will be put on scalability and widely accepted schemes for naming.

In order to cope with the multi-hop requirements a hierarchical scheme to arrange composition agreements may be used.

3.4.1.2 Composition support for networks jointly providing access & services

For joint management of multiple networks, a number of requirements can be identified from the provider point of view

- Different levels of cooperation shall be possible for joint resource control
- For load balancing reasons users should be possible to "be moved" easily within composed networks

Requirements from the user perspective are

- Selection of best access according to user needs and preferences
- Continuous connectivity when moving (smooth intra-operator handover)



WIRELESS WORLD

RESEARCH FORUM

- Setup of Service-Specific Overlay Networks (SSON), to provide optimum multimedia transport;

All of these require a negotiation process, which has to be performed during the composition of networks.

3.4.1.3 Composition support for PAN's

Configuration support for PAN's will be important due to a multitude of devices, both due the different capabilities supported (different types of terminals) as well as due the multiplicity of vendors. Compared to the other cases above, scalability is not believed to be an issue since the number of devices is limited and the „compositions“, mostly will be long term. One additional challenge is to organise and manage the context data base of the user. In this respect, another AN component which has to be involved in the negotiation process is the Context Information Base (CIB), and a special functional entity, the Registry Composition Entity has been designed in order to orchestrate the CIB composition.

Regarding PAN's, we have to be able to cope with their mobility. End users will be on the move, and the composition process needs to be able to handle mobility procedures on a proper and efficient way.

Within the AN project, a quite novel and advanced Mobility Control Space has been designed [43]; within it, the most challenging issue is the management of moving networks and the impact on the composition procedure. As far as the relevance of PANs is going to be much more relevant in the near future, there will be situations in which a relatively large number of people, carrying communication devices, are travelling together; the composition process has to be light enough, not to impose a relevant overhead.

3.4.2 AN System Concepts

The logical picture of the Ambient Control Space, ACS, which was already been introduced in the project proposal, is depicted in Figure 1 above, and further detailed in [9]. The picture illustrates that an AN comprises three distinct components:

- Ambient Connectivity, which abstracts existing network infrastructure, and to which the Ambient Network functionality is added.
- Ambient Interfaces, which allow the Ambient Control Space to communicate with; connectivity resources (through the Ambient Resource Interface (ARI)), services and applications (through the Ambient Service Interface (ASI)) and other Ambient Networks (through the Ambient Network Interface (ANI)).
- The Ambient Control Space (ACS), can be subdivided into the actual control functions (exemplified by the boxes in the control space) and the control space framework functions, which are not explicitly shown, but assumed to implement the loop surrounding the connectivity plane. The control space framework comprises all functions necessary to allow the control functions to plug into the control space,



WIRELESS WORLD

RESEARCH FORUM

execute their control tasks and coordinate with other functions present in the control space.

3.4.3 Levels and Types of Composition

By definition, network composition has always a type associated with representing the level (or depth) of cooperation between the composing ANs. This turns out to be an important matter of resource management, i.e. how resources shall be managed and controlled following the composition. There are three different composition types; *network integration*, *control sharing* and *network interworking*.

In *network integration*, Figure 23, two ANs are merged to form one new AN, and thus also the two ACSs of the two ANs are merged into one resulting always in a common/virtual ACS being created with all their respective contributed resources (represented as purple in Figure 23). An example of this type of composition could be a Body Area Network (BAN) containing all users' attached devices and providing a unified view via a common/virtual ACS.

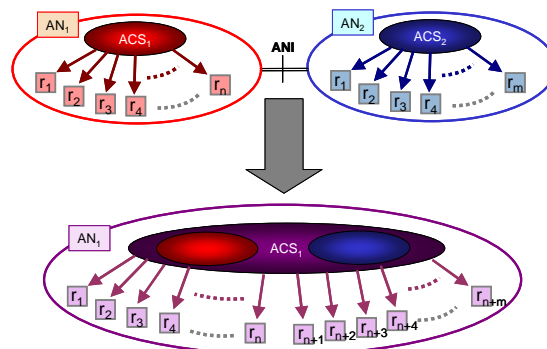


Figure 23: Network Integration.

In *control sharing*, two ANs decide to stay as separate ANs, but share their resources. If a common control of any resources is involved, then the composition is *control sharing*, Figure 24, with a new common/virtual ACS, which contains all resources under common control, represented as green in Figure 24. This new common/virtual ACS also represents a new AN „on top“ of the constituent ANs and exposes a new ANI corresponding to the newly formed AN. A Personal Area Network (PAN) could be an example of this type of composition, in which all users' devices remain to be visible to the outside after the composition and a common/virtual ACS contains all resources from the different devices under common control.

If this resource sharing does not involve a common control, then a new common/virtual ACS is not mandated, and this is called *control delegation* and is considered to be a special case of *control sharing*, Figure 25. In *control delegation*, control of some resources is delegated to another AN so that after a composition has taken place, an AN has not anymore control of delegated resources; these resources are represented inside blue and red ellipses in Figure 25. A composition between an access provider and a user could be an example, in which the control of some resources of user's device is delegated to an access network in order to support for example network- assisted functionality.



WIRELESS WORLD

RESEARCH FORUM

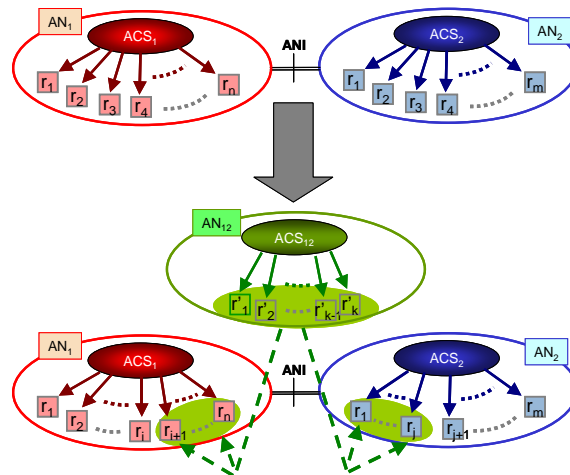


Figure 24: Control Sharing.

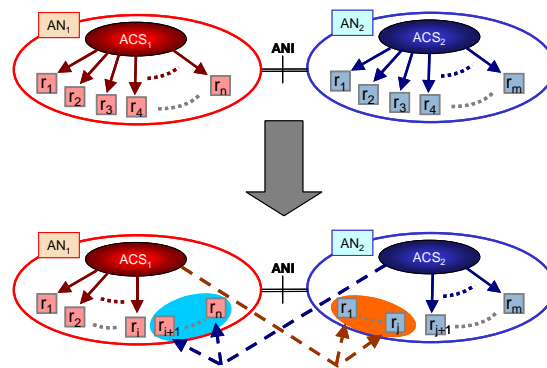


Figure 25: Control Delegation.

In network interworking, just as with control sharing, the two ANs decide to stay as separate ANs and additionally in this case, ANs maintain the control of their own resources so that the composition is transparent from resource management point of view. A dynamic roaming agreement established between operators is one example of this type of composition.

From above description, it is clear that composition is modelled as a bi-lateral process and a new common/virtual ACS is mandated if the composition type is either *network integration* or *control sharing*. However, a common/virtual ACS has an important role considering multi-lateral arrangements, and whenever multi-lateral support is preferred, a new common/virtual ACS must be created. In other words, whenever a multi-lateral support is preferred, a new common/virtual ACS needs to be created independently of the composition type.

3.4.4 Overlay types

A hierarchical P2P overlay model has been introduced in [16] to provide a scalable network architecture for composition in ANs. This overlay model maintains a separate overlay for every ACS; i.e. each ACS is represented by an overlay.



WIRELESS WORLD

RESEARCH FORUM

The basic components of this overlay model are peers, super-peers and overlays. An overlay is a set of peers belonging to a common management domain and forming a virtual network. Each overlay elects a super-peer to represent the overlay towards the outside world and therefore these super-peers also have an important role in the composition process, during which the negotiation of the super-peers of the networks is performed. Once the Composition Agreement (CA) has been successfully negotiated, it can be analyzed to detect what is the resulting composition type and what overlay type should be selected.

There are three different overlay types; *absorption*, *gatewaying* and *interworking*.

In *absorption*, one of constituent ANs ACS is discontinued and another one is kept and a relating overlay is modified according to a new common/virtual ACS. This overlay type is the only choice when the resulting composition type is *network integration*.

In *gatewaying*, both constituent ANs keep their own ACS and a new overlay is created to implement a new common/virtual ACS. This overlay type is selected for the *control sharing* and *network interworking* composition types when the creation of a new common/virtual ACS is involved.

In *interworking*, there are no overlay hierarchy changes and involved ANs keep their ACSs and related overlays. Additional configuration to enable interconnectivity between overlays might be needed. This overlay type is used when the resulting composition type is *control sharing* or *network interworking* without a new common/virtual ACS.

3.4.5 AN Identifiers & composition

To handle management and interaction of rapidly changing networks due to network composition in a secure manner, it is important to have appropriate tools for identification and key management.

Each node/peer is assumed to have a *cryptographic identifier*, which is essentially a public key (or hash thereof) identifying the node, and a unique “master”, which is the “root of authority” for the node. Just as the peer, the master is identified by a public key, and an appropriate digital signature with the corresponding private key is both necessary and sufficient for any management type operations of the node (“master commands”). The master role is not tied to a particular node, but associated to the private key and the corresponding digital signature.

A grouping of entities by means of a common controlling object is known as a *domain*. This paper focuses specifically on the concepts known as *administrative domain* and *security domain*, see further in [14] and [15]. An administrative domain is a group of network elements with a common master. Since each peer has a well-defined master, each peer is a member of precisely one administrative domain, which consists of the peers with a common master.

One administrative domain may consist of several ANs, but each AN always belongs to a single administrative domain.

A security domain is intended as a natural grouping of peers according to certain security policies, for management or to allow for secure interaction within the group or with other peers



WIRELESS WORLD

RESEARCH FORUM

(ANs) in a common way. The controlling entity of the security domain is called *manager*, to which the master has delegated management rights over some parts of the administrative domain.

It is proposed that a security domain (and its manager) is identified by a *public key*; the corresponding *private key* is in possession of the manager. To enable proof of membership, and to secure interactions between peers within or between security domains, the manager issues a public key certificate (e.g. X.509 or SPKI) wherein a member peer identifier is signed with the manager private key. These certificates can be used for authentication and to bootstrap communication security between peering nodes and networks.

3.4.5.1 Composition cases

The following examples describe some composition cases in terms of security domains. Further examples can be found in [15].

The *network integration/absorption* composition case is a scenario whereby two security domains merge, resulting in a common manager, membership and security policies.

The *network interworking* composition case is an interaction scenario whereby access to resources of one security domain is granted to peers in another security domain based on the composition agreement (see further below).

The *control sharing* composition case requires further study, but one interpretation is almost identical to network interworking, with the addition that the managers of the participating security domains also can change the policies for how resources are allowed to be used in the other domain.

3.4.6 Composition process

The composition process includes Media Sense, Discovery/Advertisement, Security and Internetworking Connectivity establishment, Composition Agreement Negotiation, and Composition Agreement Realization. These phases are not necessarily passed in a one-way fashion. E.g. after establishing a security association, more services can be advertised which are only available to certain, trusted ANs. In order to allow flexibility and efficiency, it is also possible to e.g. update the security association after determining the details of the *Composition Agreement (CA)*. Also, an established Composition Agreement can later be renegotiated. Figure 26 below shows a principal flow diagram.

3.4.6.1 Media Sense

Depending on the particular scenario, there may be different types of events, which may trigger Media Sense, for instance:

- An operator connects a new access point to its network.
- Two operator-managed networks are connected for the first time.



WIRELESS WORLD

RESEARCH FORUM

- A user device is switched on and searches for networks in its vicinity.
- A PAN needs to cooperate with a remote AN.

The very starting point is to sense a medium that would enable communication with a neighbouring node/AN. The “sensing” also includes the case of discovering a link to a remote AN (no physical vicinity). The latter case is termed “virtual composition”.

3.4.6.2 Discovery / Advertisement

Depending on the situation, Media sense is followed by either an advertisement or a discovery phase. On layer 2, these messages are broadcasted as beacons. On layer 3 (e.g. for virtual compositions) they are sent as targeted composition queries.

With active advertisements an AN can offer (network) resources and services to other ANs. The advertisement message includes the cryptographic identifier used by an AN, which is included to bind the advertisement to a particular AN, and may be authenticated and/or authorized at a later phase. The AN may alternatively listen to advertisements by other ANs, or actively discover its neighbours. The Advertisement/Discovery phase allows to select a candidate AN for composition. It allows discovering other ANs identifiers, resources, capabilities and (networks) services.

3.4.6.3 Establishment of Security and Internetworking Connectivity

When the Advertisement/Discovery phase discovered a candidate AN for composition, the two ANs need to establish basic security and Internetworking connectivity. As described in [15], for layer 2 connectivity, an efficient way of doing so is a generalization of the HIP-base exchange [32] that includes the generation of a shared session key using the Diffie-Hellmann algorithm. Cryptographic identifiers belonging to the ANs involved in the composition are used to bind the established shared key to the communicating ANs and a cryptographic puzzle is used to protect against Denial of Service.

Where the discovery phase occurs at level 3, it is assumed that existing protocols, e.g. HIP or IKEv2, could be used to establish the necessary security association between the two ANs. However, these protocols may need to be extended to carry additional payloads, e.g. AN specific credentials, purpose of composition etc.

The identities of the ANs might be authenticated and/or authorized using a Trusted Third Party. Alternatively the required trust relationship may be based on a pre-established shared secret or may even be opportunistic, e.g. the ANs make a leap of faith, trusting the unauthenticated identities.

This message exchange may piggyback further information that allows the composing ANs to establish type and purpose of the composition quickly.

When the security establishment is a layer 3 process, it is assumed the internetworking addresses associated with the cryptographic IDs of the ANs can be discovered. When it is a layer 2 process, the internetworking address exchange or internetworking address



WIRELESS WORLD

R E S E A R C H F O R U M

configuration can also be handled as part of the layer 2 exchange. It should be possible to use the security association established at layer 2 to generate a layer 3 security association.

At some point during this message exchange, or immediately afterwards, internetworking connectivity between the two ANs is established.

3.4.6.4 Composition Agreement (CA) negotiation

The next step of the composition process is the negotiation of the Composition Agreement (CA). The CA includes the policies to be followed in the composed AN, the identifier of the composed AN, how logical and physical resources are accessed, controlled and/or shared between the composing ANs etc. Where the CA includes commercial factors, the CA should be digitally signed by both ANs to provide non-repudiation.

There are two ways for negotiating a CA: centralized and distributed. In a centralized negotiation, a coordinating Composition function of the two composing ANs negotiate, each consulting with the other functions in the same AN/ACS. In the decentralized negotiation, each function negotiates independently about the control functionality it is responsible for, orchestrated by the coordinating Composition function. In this case, the negotiation process must be followed by an internal consolidation phase among functions in each AN because the partial agreements negotiated by each function may not be independent from each other. The balance between centralized versus distributed control in the composition process is further analyzed and detailed in e.g. [11].

It is possible that the process of establishing a CA may involve increasing levels of authorization, e.g. negotiation of certain resources and services may only be authorized once the two ANs have agreed the commercial aspects of the CA.

The negotiation is carried out over the ANI using the Generic Ambient Network Signalling (GANS) protocol framework [11] unless another protocol already exists for that particular purpose.

The outcome of the Composition Agreement Negotiation process depends heavily on the use case, and what roles the composing ANs have. The composition will then lead to a composition of types either network integration, control sharing or network interworking, as described above.

3.4.6.5 Composition Agreement Realization

The Composition Agreement Realization phase represents the completion of the composition. During this phase, network elements are configured to reflect the CA. Thereby, each of the composing ANs must also carry out the configuration of its own resources by updating the policies and of their control functions.

It should then also be noted that, which largely depends on the outcome and the settlement of the CA, addresses might be re-assigned and re-organised.



WIRELESS WORLD

RESEARCH FORUM

The result of the composition process is either a new AN, or an enlarged AN (i.e. one AN is absorbed into the other), or two interworking ANs.

In any case, a fundamental issue after composition is that some signalling must be exchanged through the ANI between the ANs involved in the composition, e.g. status and control information, to maintain the composition state. This could also include information that is normally exchanged during the Advertisement/Discovery phase, and which could lead to a re-iteration of the composition process or even the request to de-compose.

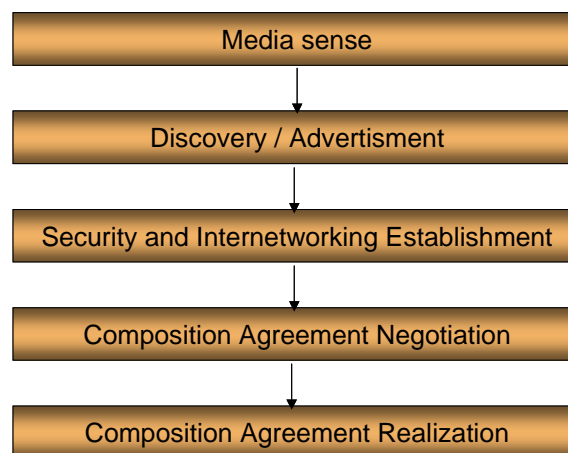


Figure 26: The principal composition process.

3.4.6.6 Decomposition process

Inside a composed AN, if one or more of the ANs decide to discontinue to share their resources (e.g. switch off of one AN, relay node leaves coverage, etc.) decomposition takes place.

A composed AN may consist of two or more ANs. The composed AN provides a set of functionalities to the outside through its ANI. The outside perceives these functionalities as being provided by a single AN, at least in case of network integration and control sharing. However, it is possible, that these functionalities are distributed among the different ANs forming the composed AN. So, if one AN decomposes, the other ANs still being composed very likely need to be reconfigured (“Composition update”).

3.4.7 Composition example

As an example, let’s consider the use case, in which our user Bob has an active connection over UMTS network that has roaming agreement with Bob’s home operator as represented in Figure 27 below.



WIRELESS WORLD RESEARCH FORUM

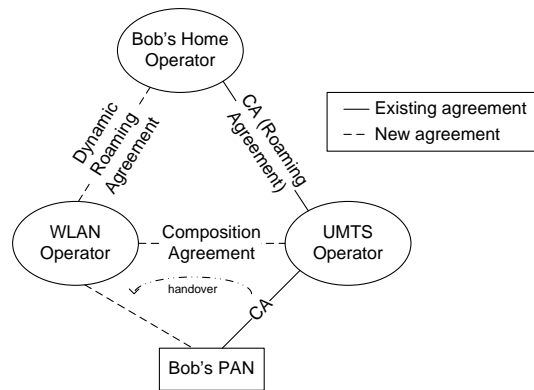


Figure 27: An example of Bob's PAN compositing with visited networks.

Bob's PAN detects a new WLAN access and the WLAN operator does not have roaming agreement with Bob's home operator and it does not know UMTS network. To be able to provide access for Bob, the WLAN operator needs to establish a roaming agreement with his home operator. In order to minimize service interruption during handover, WLAN network needs to be able to cooperate with Bob's old access network; the UMTS network, and therefore a new composition has been established between the WLAN and UMTS operator, over which handover cooperation between networks has been performed.

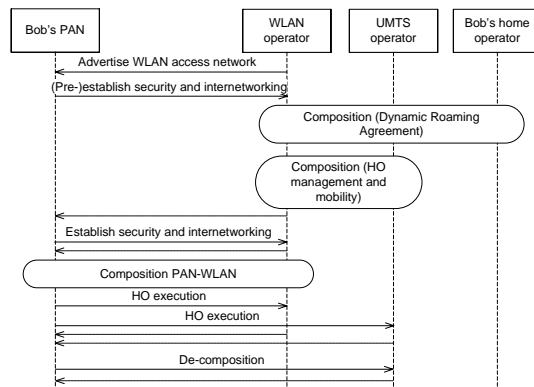


Figure 28: High level sequence chart.

In Figure 28 above, a high level sequence diagram of the example described above is illustrated. It should be noted, that many multi-access, multi-radio and mobility aspects are either simplified or omitted here to better highlight issues of dynamic triggering of the composition process and network access. Once Bob's PAN has detected a new WLAN access, it (pre-)establishes security and internetworking with WLAN network in order to exchange required security information (e.g. authentication/authorization info), which is required so that WLAN network is able to verify whether it has capability to provide access for Bob. The WLAN network detects that it has no required roaming agreement with Bob's home operator and therefore it triggers a dynamic roaming agreement. This roaming agreement is a bi-lateral, and considering the functionalities it is created for, *network interworking* composition type is used. After this, the WLAN network establishes cooperation with the UMTS network to support a (seamless) handover and mobility. This cooperation is also bi-lateral and



WIRELESS WORLD

RESEARCH FORUM

considering that both networks prefer to maintain their control of their own resources, this composition is also *network interworking* type. It is not feasible to start this composition with the UMTS operator until a roaming agreement has been established, because without it, the WLAN operator is not able to provide the access and therefore a handover is not needed. After successful verification, Bob's PAN is able to perform the access evaluation and once WLAN access has passed it, handover needs are evaluated and composition decision is done. After the composition establishment has been decided, both security and internetworking are "upgraded" between Bob's PAN and the WLAN network to enable Composition Agreement Negotiation and a new composition is established over which handover is then executed. Alternatively, the WLAN-UMTS composition execution can be postponed to be able to provide faster response to the MN, but that is subject to optimization.

Figure 29 below represents how the composition process is used during the detection of a new access (left side) and during the handover (right side).

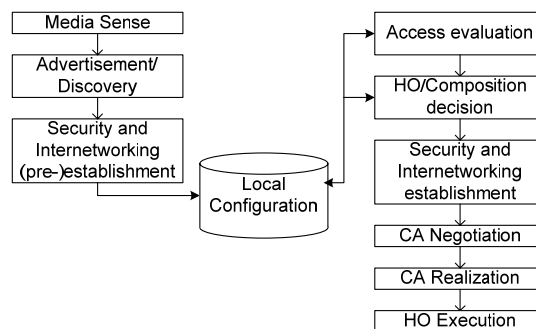


Figure 29: An example of composition process.

First, Media Sense, Advertisement/Discovery and Security and Internetworking (pre-)establishment are performed and local configuration is updated accordingly. Once local configuration is up-to-date, it is used for access evaluation and based on the evaluation results both handover and composition decisions have been carried out resulting triggering a new composition establishment. Although, and note that these three steps (Media Sense, Advertisement/Discovery, Security and Internetworking establishment) can be performed to update local configuration, without initializing the remaining steps of the composition process represented in right side.

After a new composition has been successfully established, handover is executed over it and a composition with UMTS network is removed by executing decomposition process.

3.5 Business aspects of dynamic composition

In order to make the AN composition commercially feasible, it is necessary to take care of the relevant business aspects from the very beginning. The impact of the necessary legal and economic aspects needs to be considered and reflected in the technical solution.

First, it is necessary to think about the structure a Composition Agreement (CA) made between two composing ANs. Having generic structure, given as a template, would enable



WIRELESS WORLD

R E S E A R C H F O R U M

easy automation and (re)usage of the template in any new situation between any two ANs. Here, we propose a CA template and describe its elements, and focus on the elements covering business-related issues (legal, economic, regulatory).

Next, it is important to point out that legal/economic issues are necessary to take care of when realising the composition in the commercial/business sense. Therefore, we discuss how and where the legal and economic parts of the CA will be communicated between composing ANs. It is important to keep in mind that these issues have to settle in any (commercial) CA, and our ideas are complimentary to the ideas presented in section 3.4, where the composition agreeing process is described in general along with some use cases examples.

3.5.1 Composition Agreement – template and negotiation

In a multi-service multi-provider environment, co-operating providers need to fulfil user's demands while, at the same time, compete for the same market segment. The relationships between them need to be settled efficiently. In principle, any relationship between two actors is associated with a set of expectations and obligations. These may be implicitly presumed, but in a commercial environment, it is usual to have them explicitly agreed in an agreement. The agreement helps the involved parties to e.g. find out whether the agreement was breached and what would be the compensation by pointing a reference value as a measure to decide when agreed QoS level is not delivered and when the user experienced consequences of not achieving his goal² can ask for compensation.

Generally, an agreement made between the user and the provider represents a harmonised understanding between these two parties on how they should behave (adapted from [41]). Their behaviour is described via a set of duties, rights, and obligations. It is usually expressed in a formal way and settled in a negotiation process, which is a part of the agreeing process. Different types of agreements exist, their granularity, duration, expression language may differ, they can be located between the actors positioned on various places in a value network, etc. Here, we focus on the Composition Agreement (CA), while more details on the agreements in general, various types, examples of content, structure/templates, SLA information model (and its QoS part) etc. can be found in [39][40].

Facing a composition, the composing ANs have to settle their relationship in a CA. Many technical and business-related issues related to the respective composition need to be covered in the CA.

Business issues include the legal and economic statements of the agreement, as well as the other important issues like diverse regulations, political and moral issues of relevance, etc., e.g. contractual interaction points, payment method, discount rates. Technical issues cover the technical details of the relationship, e.g. the services to be provided, its components, QoS level, money flow, management, monitoring points, interfaces/technical interaction points relevant for service delivery and assurance (e.g. ANI, ARI, and ASI), etc.

Note that business-related issues can be negotiated, implemented, executed and released independently from technical issues even though they are related to the technical issues. For

² Usually, the perception of “bad” QoS is mentioned as the argument, but since the perception is a subjective thing, not easy to measure with objective measures, it is important to have technical details to refer to if the complaint is posed.



WIRELESS WORLD

RESEARCH FORUM

instance, one can agree upon the legal issues for the certain period (e.g. agreement validity), and then re-negotiate and implement technical statements for each new session. This is an important issue in the AN environment when considering the migration path and the degrees of AN functionality presence, i.e. depending on whether the AN is partially or fully deployed.

In the following, we present a proposal for a generic CA template, where both technical and business parts are described, and we further elaborate on the above-mentioned business issues. Furthermore, we discuss the importance to consider the legal and economic issues negotiation in the overall composition process, and the necessity to reflect this in a technical solution developed in the Ambient Networks project.

3.5.2 CA template

The content of a CA would depend on the concrete situation in focus and the parties involved, but the structure would typically remain the same. Therefore, it is useful to have a template showing the generic elements that are built in the CA structure. A proposal for the elements considered in any CA (information blocks of the CA information model) is described next. The idea behind the CA information model is based on the work done originally for the SLA template, [40], and is visualised by using the UML, [41].

Roughly, two main groups of elements can be recognised – technical and business-related, though these are always highly related. Technical issues are of main concern when developing the composition architecture in the ANs, and though mentioned here, these are not the main focus in this section. Here, we focus on the details/statements covering legal and economic viewpoints.

The CA template is depicted as an information model in Figure 30.

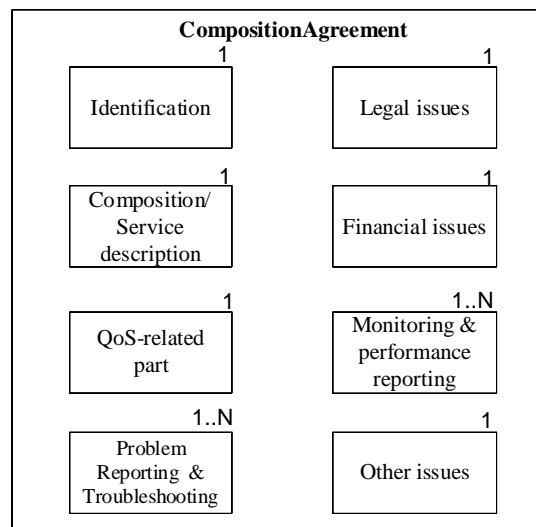


Figure 30 Composition Agreement – information model



WIRELESS WORLD

RESEARCH FORUM

The information included in the CA basically covers; 1) the unique identification of the agreement, which enables this agreement to be easily distinguished from the other CAs (*identification information block*), 2) a detailed description of the type and nature of the composition including the services to be provided (*composition/service description*), 3) QoS level to be delivered (expressed via a set of QoS parameters and their target values) and its monitoring, technical reactions if the QoS is not delivered as agreed (e.g. alarms' triggering), points of delivery/monitoring, etc. (*QoS part information block*), 4) the ways of reporting the performance (*performance reporting information block*), 5) a description of the problem reporting and troubleshooting procedures (*problem reporting and troubleshooting information block*), 6) a specification of legal terms and conditions (*legal issues information block*), 7) a description of discounts, pricing schemes, payment and billing methods (*economic issues information block*), and 8) all other relevant issues like diverse regulations, user behaviour constraints, etc. (*other issues information block*).

Last three of the above information blocks include further:

- **LEGAL ISSUES** - the scope and purpose of the agreement, definitions valid for the agreement, legal identification of the parties involved, maintenance of the agreement including the plan of responsible persons that are members of the SLA team, duration and validity of the SLA, non-disclosure agreement, force majeure situations, dispute handling, breaching procedure - the consequences and the reaction pattern for the cases when either the user or the provider did not comply with what was agreed in the SLA, legal constraints on the user behaviour wrt e.g. reselling the access capacity, etc.
- **ECONOMIC ISSUES** - tariffing policy, prices, charging schemes to be applied, penalties to be paid in case any of the events triggering the reaction pattern are detected, costs involved if the service changes and who will be charged for what, etc.
- **OTHER ISSUES** - apply to all the other issues like regulatory issues which may include references to the directives restricting further retail of the service contracted, political constraints, moral constraints, constraints on the user behaviour may be included (e.g. a specification of minimal requirements on the equipment that the user needs to experience the quality as agreed). Escape clauses may be included to define when the statements from the agreement do not apply – e.g. if a fire damaged the provider's equipment, etc.

3.5.3 Business aspects of the Composition process

The process of composition is described in Section 3.4. As already mentioned, not only technical but also business-related issues like legal/economic/regulatory need to be settled, and these issues can be negotiated/agreed/implemented/released separately. Therefore, we distinguish two situations where the composition takes place:

1. "Partially deployed AN" implies that the business-related issues of a CA are agreed in the traditional way (e.g. "hard copy", manually done). Related SLAs/SLSs which cover the issues of e.g. technical capabilities, QoS, are thereafter taken care of automatically. This solution is feasible to expect in the early phases of the AN deployment (i.e. in the first migration phases, or when AN is only partially supported in the networking environment. Here, a CA would be similar to today's situation where two large network operators agree upon a service portfolio, and where details per service are further covered by a (set of) SLAs. Parties simply agree to make business together, the



WIRELESS WORLD

RESEARCH FORUM

subject of the business (what is considered under the composition), rights and duties/obligations. Such CA is, in a way, the precondition that composition instances may take place, and the establishment of a trust relationship can directly follow it. Two variants are possible: a) the user agrees with the primary provider that he will have the access to global connectivity in the AN environment, b) an AN provider signs a “pact” where all members are trusted AN providers, and by joining them the AN provider agrees on the terms of the alliance. In the latter case it could be opening for a new business role (sort of a “trust clearing house”) that can administrate the list(s) of (un)trusted parties, grant the access, etc.

2. “Fully deployed AN”, or so-called “all-by-bits” solution. The complete CA, i.e. both technical and business-related issues, is agreed automatically via protocols. Though possible, it is important to note that this solution may be rather complex to both design and realise practically in the commercial sense, since it asks for changes in today’s legal and economic practice on several levels (e.g. nationally, globally). It implies that several laws on different levels need to be adapted to this new situation, e.g. with respect to the company registration, legislation, legal responsibility, customers organisations, customers’ interests protection laws, etc. For instance, the legislation should be covered by e.g. AN ID, which in turn needs to be reflected in the AN naming and addressing solution. Therefore, this solution may be feasible to expect in the later phases of the AN deployment where all elements of the AN concept is fully deployed.

Independent on the way the business-related statements of the CA are settled (manually, automatically), it is important to keep in mind that they have to be in place when composing in the commercial AN environment³. It is important to relate their settlement to the trust relationship establishment, and the final solution is still under development in the Ambient Networks project. Also, the sequence in which the agreement elements (business vs. technical) are negotiated is open at this stage - it is possible to first negotiate legal and economic issues and then focus on the technical issues, but it is also possible to check the technical issues before going into the formal negotiation of legal and economic issues.

The negotiation process and its elements are studied in details in the technical groups developing the Composition architecture and framework and also security solution for the AN environment. Our intention is not to override these ideas, but only to indicate the business-related issues important to take care of when making an agreement. Here, we discuss two situations where the importance of settling the CA in the legal/economic sense is highlighted:

1. Assume two ANs – AN1 (UE/end user) and AN2 (Network Operator/Service Provider) – which, after they discovered each other, want to compose. They would probably have different capabilities in their system – UE will have a simpler solution and less functionality than NO. After the details of technical capabilities are negotiated (QoS, FAs, ACS control), it is important to agree upon the rules for behaviour expected from both parties – to define and agree upon the common policy – where the constraints like “UE is not allowed to resell the access point”, and the guidelines of acting in case third AN would like to compose with their composed AN, can be included. Furthermore, legal and economic issues (like charging details) are negotiated, which results in the

³ Naturally, the CA may not be needed in cases the composition is done e.g. between buddies or people belonging to a certain network (“Net power” phenomenon), but in cases where the composition is done as a part of the business, and the money and legal responsibility is involved, the CA is needed.



WIRELESS WORLD

R E S E A R C H F O R U M

- formal CA specified, negotiated and agreed. We denote this agreement as the CA1, and it regulates the composition resulting in the ANx creation.
2. Assume that new AN – UE/AN3 – would like to compose with the ANx. This composition would require new CA, called CA2, and, in turn, it would affect the CA1 made between the ANx partners – AN1 and AN2. The issues like common policy, charging, legal issues, payment methods, reactions, etc. may need to be checked and re-negotiated.

Such situations need to be reflected in the technical solution, which should be robust and scalable enough to support all the transactions and negotiations related to the CA agreeing process. The technical solution design is aware of the above challenges and will assure that these are included in the final technical solution. Note further that the details of the proposals and ideas presented here may differ from the final solution, since this area (CA template and “all-by-bits” solution) needs further investigation and involvement of experts covering areas like contracts, law, economics, regulations etc. in addition to the technical expertise. Further step may for example include the investigation of the effects the described (full) composition process may cause in the legal/financial systems (change of laws, e.g. software agents, digital signature, etc.), and its tight incorporation in the technical solution supporting e.g. charging/billing, security, etc.



WIRELESS WORLD

R E S E A R C H F O R U M

4 Conclusion

This document describes a promising architecture for the future Networks of the Wireless World, starting with the high-level goals that lead to the development of representative scenarios for user and business perspectives and drove identification of the main technical requirements. It aimed to capture and identify the control functions and their interactions in a common format. Finally, it defined the foundations for the overall architecture itself.

A key part of this document presents fundamental aspects of the overall architecture: the various facets of the composition concept and the framework within which the individual control functions are placed. In line with the core concept of dynamic network composition, the fundamental architectural components are the 'building block' networks themselves. In the Networks of the Wireless World we have established that there should be a single type of building block, the Network itself, which can range in scale from a single terminal to a complete operator network.

Key to the architecture of the Networks of the Wireless World is the two fundamental inter-layer interfaces that bind the control functionality. The Ambient Service Interface makes the connectivity and control functions available for use by upper layer applications operating with the same Ambient Network. The Ambient Resource Interface has been developed as an abstraction of the resources provided by the underlying connectivity infrastructure. This decouples the development of Ambient Control Space (ACS) functions from any particular data transfer technology, maximizing the applicability of the results and opening the range of migration possibilities.



WIRELESS WORLD

R E S E A R C H F O R U M

Acknowledgement

This document has been produced in the context of the *Ambient Networks* project. The *Ambient Networks* project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission. All information in this document is provided "as is" and 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. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view.



WIRELESS WORLD

RESEARCH FORUM

Abbreviations

A4C	AAA + Auditing + Charging	MRA	Multi Radio Access
AAA	Authentication, Authorization and Accounting (Procedure)	MRRM	Multi-RRM
ACS	Ambient Control Space	NAT	Network Address Translation/Translator
AN	Ambient Network	OSI	Open Systems Interconnection
ANI	Ambient Network Interface	PAN	Personal Area Network (also Private Ambient Network)
ARI	Ambient Resource Interface	PDA	Personal Digital Assistant
ASI	Ambient Service Interface	PLMN	Public Land Mobile Networks
ATM	Asynchronous Transfer Mode	PSTN	Public Switched Telephony Network
BAN	Body Area Network	OCS	Overlay Control Space
BGP	Border Gateway Protocol	OSA	Open Service Access
CA	Composition Agreement	QoS	Quality of Service
CIB	Context Information Base	RAN	Radio Access Network
EID	Endpoint Identifier (ID)	RAT	Radio Access Technology
FA	Functional Area	RRM	Radio Resource Management
GANS	Generic Ambient Signalling Protocol	SIGTRAN	Signalling Transport
GCP	Gateway Control Protocol	SIP	Session Initiation Protocol
GLL	Generic Link Layer	SLA	Service-Level Agreement
HIP	Host Identity Protocol	SMART	Smart Multimedia Routing and Transport
HMIP	Hierarchical Mobile IP	SoA	State of the Art
HSDPA	High-Speed Downlink Packet Access	SS7	Signalling System 7
ID	Identifier	SSON	Service-Specific Overlay Network
IP	Internet Protocol	SW	Software
ISDN	Integrated Services Digital Network	TDM	Time Division Multiplexing
ISP	Internet Service Provider	UMTS	Universal Mobile Telecommunication System
ISUP	ISDN User Part	VoATM	Voice over ATM
L1, L2, L3	OSI Layer 1, 2, 3	VoIP	Voice over IP
LAN	Local Area Network	WAN	Wide Area Network
M2M	Machine-to-Machine		
MIP	Mobile IP		



WIRELESS WORLD

R E S E A R C H F O R U M

WLAN Wireless Local Area Network
WP Work Package

XDSL Digital Subscriber Loop (e.g.,
 ADSL)



WIRELESS WORLD

RESEARCH FORUM

References

- [1] Ambient Networks project website: <http://www.ambient-networks.org/>
- [2] Winner project website: <https://www.ist-winner.org/>
- [3] Spice project website: <http://www.ist-spice.org/>
- [4] Mobilife project website: <http://www.ist-mobilife.org/>
- [5] E2R project website: <http://e2r2.motlabs.com/>
- [6] Daidalos project website: <http://www.ist-daidalos.org/>
- [7] "D1-2: Ambient Networks Scenarios, Requirements and Draft Concepts", IST-2002-507134-AN/WP1/D02, October 2003.
- [8] "D1-3: Migration Strategies to Ambient Networks", D. Moro (*ed.*), IST-2002-507134-AN/WP1/D13, December 2004.
- [9] "D1-8: Ambient Networking: Concepts and Architecture", F. Pittman (*ed.*), IST-2002-507134-AN/WP1/D08, January 2005.
- [10] "D2.2: Draft Multi Radio Access Architecture", J. Gebert (*ed.*), IST-2002-507134-AN/WP2/D02, December 2004.
- [11] "D3-2: Connecting Ambient Networks – Architecture and Protocol Design" J.Còlas (*ed.*), IST-2002-507134-AN/WP3/D/3.2, March 2005.
- [12] "D5-1: SMART – Draft Architecture and Multimedia Routing Decision Logic", S. Schmid (*ed.*), IST-2002-507134-AN/WP5/D01, December 2004.
- [13] "D6-1: Ambient Networks ContextWare", A. Jonsson (*ed.*), IST-2002-507134-AN/WP6/D61, December 2004.
- [14] "D7-1: Ambient Networking: Concepts and Architecture", G. Selander (*ed.*), IST-2002-507134-AN/WP7/D01, December 2004.
- [15] "D7-2: Ambient Networks Security Architecture", F. Kohlmayer (*ed.*), IST-2002-507134-AN/WP7/D/02, December 2005.
- [16] "D8-1: Ambient Network Management – Technologies and Strategies", A. Galis & L. Cheng (*ed.*), IST-2002-507134-AN/ D8-1, December 2004.
- [17] J. Sachs, L. Muñoz, R. Agüero, J. Choque, G. Koudouridis, R. Karimi, L. Jorguleski, J. Gebert, F. Meago, and F. Berggren, "[Future Wireless Communication based on Multi-Radio Access.](#)" in Proc. WWRF11, Oslo, Norway, June 10-11, 2004.



WIRELESS WORLD

RESEARCH FORUM

- [18] J. Lundsjö et al., "Multi-Radio Access Architecture for Ambient Networking", IST Mobile and Wireless Communications Summit 2005
- [19] "D2.2: Draft Multi Radio Access Architecture", J. Gebert (ed.), IST-2002-507134-AN/WP2/D02, December 2004.
- [20] "D2.4: Multi Radio Access Architecture", M. Prytz (ed.), IST-2002-507134-AN/WP2/D04, December 2005.
- [21] G. P. Koudouridis, R. Agüero, E. Alexandri, M. Berg, A. Bria, J. Gebert, L. Jorguseski, H. R. Karimi, I. Karla, P. Karlsson, J. Lundsjö, P. Magnusson, F. Meago, M. Prytz, J. Sachs, "Feasibility Studies and Architecture for Multi-Radio Access in Ambient Networks", Proc. 15th Wireless World Research Forum (WWRF) Meeting, 8-9 December 2005, Paris, France.
- [22] F. Berggren, I. Karla, R. Litjens, P. Magnusson, F. Meago, R. Veronesi, H. Tang. "Multi-Radio Resource Management for Communication Networks Beyond 3G", IEEE Vehicular Technology Conference (VTC 2005) Fall, September 25-28, Dallas, Texas, USA.
- [23] R. Agüero et al "RRM Challenges for Non-Conventional and Low Cost Networks in Ambient Networks", Proceedings of WPMC '05, Aalborg, Denmark, 2005.
- [24] G.P. Koudouridis, R. Agüero, E. Alexandri, J. Choque, K. Dimou, H.R. Karimi, H. Lederer, J. Sachs, R. Sigle. "Generic Link Layer Functionality for Multi-Radio Access Networks", IST Mobile and Wireless Communications Summit 2005
- [25] K. Dimou, R. Agüero, M. Bortnik, R. Karimi, G. P. Koudouridis, S. Kaminski, H. Lederer, J. Sachs, "Generic Link Layer: A Solution For Multi-Radio Transmission Diversity in Communication Networks Beyond 3G", Proc. 62nd IEEE Semiannual Vehicular Technology Conference (VTC Fall), Dallas, Texas, USA, September 25-28, 2005.
- [26] Baraev, L. Jorguseski, R. Litjens, "Performance Evaluation of Radio Access Selection Procedures in Multi-Radio Access Systems", Proceedings of WPMC '05, Aalborg, Denmark, 2005.
- [27] J. Hultell, M. Berg, "Generalized Roaming and Access Selection in Multi-Operator Environments", In Proceedings of RadioVetenskap och Kommunikation, Linköping, Sweden, June 14 – 16, 2005.
- [28] G.P. Koudouridis, H.R. Karimi, K. Dimou, "Switched Multi-Radio Transmission Diversity in Future Access Networks", In: Proceedings of the Vehicular Technology Conference, Fall 2005, September 25-28, Dallas, Texas.
- [29] H.R. Karimi, G.P. Koudouridis, K. Dimou, "On the Spectral Efficiency Gains of Switched Multi-Radio Transmission Diversity", In: Proceedings of WPMC '05, Aalborg, Denmark.
- [30] H.R. Karimi, K. Dimou, G.P. Koudouridis, P.Karlsson, "Switched Multi-Radio Transmission Diversity for Non-Collocated Radio Accesses", In: Proceedings of the Vehicular Technology Conference, Spring 2006, May 7-10, Melbourne, Australia.



WIRELESS WORLD

R E S E A R C H F O R U M

- [31] "Multipurpose Internet Mail Extensions", RFC 2045, November 1996.
- [32] "Host Identity Protocol Architecture", Robert Moskowitz, draft-ietf -hip-arch-03 (work in progress), August 2005.
- [33] "On the naming and binding of network destinations", Jerome Saltzer, In P. Ravasio et al., editor, Local Computer Networks, pages 311-317. North-Holland Publishing Company, Amsterdam, 1982. Reprinted as RFC 1498, August 1993.
- [34] "Abstract Syntax Notation One (ASN.1) Specification of Basic Notation", ITU-T Rec. X.680, ISO/IEC 8824-1:2002, 2002.
- [35] "Extensible Markup Language (XML) 1.0 (Third Edition)", W3C Recommendation, February 4, 2004.
- [36] "A Layered Naming Architecture for the Internet", H. Balakrishnan *et al.*, Proc ACM SIGCOMM 2004, Portland, Oregon, USA, August 30 - September 3, 2004.
- [37] "Addressing Reality: An Architectural Response to Real-World Demands on the Evolving Internet." Clark, D., Sollins, K., Wroclawski, J., and Faber, T., Proc. ACM SIGCOMM FDNA 2003 Workshop, Karlsruhe, August 2003.
- [38] "Endpoints and Endpoint Names: A Proposed Enhancement to the Internet Architecture", J. N. Chiappa, Unpublished Internet Draft, '99, <http://users.exis.net/~jnc/tech/endpoints.txt>
- [39] "Agreements in IP-based Networks", Grgic I., M. Røhne. Telektronikk on Internet Traffic Engineering. Vol 97. No. 02/3.2001.
- [40] "A framework for analysing end-to-end QoS in a multi-provider environment", Gjerde I.G. PhD thesis. University of Zagreb, Croatia. 06/2003.
- [41] OMG. UML specification version 1.4. September 2001.
- [42] "RRM Challenges for Non-Conventional and Low Cost Networks in Ambient Networks", R. Agüero et al the Eighth International Symposium on Wireless Personal Multimedia Communications WPMC 2005, Aalborg, Denmark, September 18-22 2005
- [43] "Analysis of Mobility Control Functions in Ambient Networks", R. Agüero, J. Eisl, V. Typpo, S. Uno,