<table>
<thead>
<tr>
<th>Grant Agreement Number :</th>
<th>216366</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Acronym :</td>
<td>Euro-NF</td>
</tr>
<tr>
<td>Project Title :</td>
<td>Anticipating the Network of the Future – From Theory to Design</td>
</tr>
<tr>
<td>Funding Scheme :</td>
<td>Network of Excellence</td>
</tr>
<tr>
<td>Start Date of Project :</td>
<td>01 January, 2008</td>
</tr>
<tr>
<td>Duration :</td>
<td>36 months</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deliverable Number :</th>
<th>D.SEA.10.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version Number :</td>
<td>1.0</td>
</tr>
<tr>
<td>Title of Deliverable :</td>
<td>First update of the Euro-NF vision regarding the network of the future</td>
</tr>
<tr>
<td>Contractual Due Date :</td>
<td>May, 2009</td>
</tr>
<tr>
<td>Actual Date of Completion :</td>
<td>July, 2009</td>
</tr>
<tr>
<td>Workpackage contributing to the Deliverable :</td>
<td>SEA 10.1 – Euro-NF Vision</td>
</tr>
<tr>
<td>Lead Contractor for this Deliverable :</td>
<td>GET (partner 01)</td>
</tr>
<tr>
<td>Editor[s] :</td>
<td>Daniel Kofman, Jean-Paul Lefèvre</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nature of the Deliverable : (R/P/D/O)*</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination Level : (PU, PP, RE, CO)**</td>
<td>PU</td>
</tr>
</tbody>
</table>

*Nature: R-report, P-prototype, D-demonstrator, O-other
**Dissemination: PU-public, PP-restricted to programme, RE- restricted to a group, CO-confidential

Project URL: [http://www.euronf.org](http://www.euronf.org)
With contributions from the following partners:

<table>
<thead>
<tr>
<th>Partner Number</th>
<th>Partner Acronym</th>
<th>Contributor Name</th>
<th>Contributor e-mail address</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>GET</td>
<td>Daniel Kofman</td>
<td><a href="mailto:daniel.kofman@telecom-paristech.fr">daniel.kofman@telecom-paristech.fr</a></td>
</tr>
<tr>
<td>01</td>
<td>GET</td>
<td>Jean-Paul Lefèvre</td>
<td><a href="mailto:jplefevre@arches-conseil-grenoble.eu">jplefevre@arches-conseil-grenoble.eu</a></td>
</tr>
<tr>
<td>02</td>
<td>TUKL</td>
<td>Paul Müller</td>
<td><a href="mailto:pmueller@informatik.uni-kl.de">pmueller@informatik.uni-kl.de</a></td>
</tr>
<tr>
<td>04</td>
<td>UNI WIEN</td>
<td>Günter Haring</td>
<td><a href="mailto:guenter.haring@univie.ac.at">guenter.haring@univie.ac.at</a></td>
</tr>
<tr>
<td>09</td>
<td>ALF</td>
<td>Emmanuel Dotaro</td>
<td><a href="mailto:emmanuel.dotaro@alcatel.fr">emmanuel.dotaro@alcatel.fr</a></td>
</tr>
<tr>
<td>10</td>
<td>UWUERZ</td>
<td>Phuoc Tran Gia</td>
<td><a href="mailto:trangia@informatik.uni-wuerzburg.de">trangia@informatik.uni-wuerzburg.de</a></td>
</tr>
<tr>
<td>11</td>
<td>BTH</td>
<td>Markus Fiedler</td>
<td><a href="mailto:markus.fiedler@bth.se">markus.fiedler@bth.se</a></td>
</tr>
<tr>
<td>13</td>
<td>AUEB-RC</td>
<td>George Polyzos</td>
<td><a href="mailto:polyzos@aueb.gr">polyzos@aueb.gr</a></td>
</tr>
<tr>
<td>30</td>
<td>INESC-ID</td>
<td>Augusto Casaca</td>
<td><a href="mailto:augusto.casaca@inesc-id.pt">augusto.casaca@inesc-id.pt</a></td>
</tr>
<tr>
<td>34</td>
<td>AU</td>
<td>Wolfgang Kleinwächter</td>
<td><a href="mailto:wolfgang@imv.au.dk">wolfgang@imv.au.dk</a></td>
</tr>
</tbody>
</table>

**FORWARD:**

To maximize its readability, and hopefully its impact, the Euro-NF vision is foreseen with three layers:

- firstly, an executive summary presenting a set of concepts and principles which would probably be of significance for the networked world of the future;
- secondly, an overall vision introducing these concepts in a coherent way;
- and thirdly, additional details for those considered of main importance.

The present document consists of the two higher levels. The third one, more detailed, still needs significant additional work. This additional material might become in the future a supplementary deliverable.
CONTENTS

EXECUTIVE SUMMARY  4

THE EURO-NF OVERALL VISION  6

1 AN OVERVIEW OF FUTURE COMMUNICATIONS  6

1.1 A Brief History of the Internet  6

1.2 Main Trends in Communication and Information Services  7

1.2.1 Networks and personalized services ubiquity  7

1.2.2 Global mobility  8

1.2.3 Community services, spontaneous and opportunistic networking  9

1.2.4 Merging the physical and digital worlds  10

1.2.5 Towards the Internet of things and the real world Internet  10

1.2.6 Self-organization and autonomous networking  11

1.2.7 Service enablers’ overlays, Virtualization and Programmability  12

1.2.8 Home networking  12

1.2.9 Enterprise networking  12

1.3 A Macroscopic View on the Network of the Future and Related Challenges  13

1.3.1 Evolution of present infrastructure based networks  13

1.3.2 Disruption may arrive at the edge  13

1.3.3 Control and services’ overlays for the horizontal integration  13

1.3.4 Related challenges  14

1.4 Limitations of the IP Architecture and Major Networking Principles Evolution  15

1.4.1 A reminder on well known limitations  15

1.4.2 Networking principles evolution: Towards polymorphic networks  17

1.4.3 Networking principles evolution: Towards “composable” networks  18

1.4.4 Summary on networking principles evolution  19

1.5 Organization of the Following Sections  19

2 NEW NETWORKING PARADIGMS AND NETWORK ARCHITECTURES  20

3 POLYMORPHIC AND COMPOSABLE NETWORKS: AN OVERVIEW  22

3.1 The Principles  22

3.2 Knowledge and Decision Plane for Component Management  24

3.3 Identity Management  26

4 GOVERNANCE OF THE NETWORK OF THE FUTURE  27

REFERENCES  32
EXECUTIVE SUMMARY

A lot has been already written on the Internet of the future, on evolution versus disruption, on clean slate versus the need for identifying business models. As we already mentioned in the previous version of this document delivered in May 2006 [1], we believe that focusing on the Internet of the future without a larger view on the future “networked world” is too restrictive to allow a better understanding and anticipation of the changes to come. We also believe that evolution and disruption will continue to co-exist; as has been the case in the past (e.g. P2P introduced a disruption in content distribution in an environment that was evolving by increasing the capacity of the Internet and introducing a diversification of access technologies). Moreover, clean slate is required at least for benchmarking and new business models are required for paving the way towards a future that most probably no one will successfully forecast. We don’t pretend here to describe the networked world of the future; we just present a set of concepts and principles that will most probably partially shape it, this set being summarized in the remainder of this Executive Summary, then introduced in a coherent way in the second part of the document.

Summary of the Most Important Concepts and Principles

Towards a polymorphic networking environment

From the present homogeneous networking paradigm (IP networking) hiding a diversity of transport technologies we expect to move towards a service/application aware, dynamic interconnection of a wide diversity of heterogeneous networking paradigms hidden by a global superimposed architecture based on identifiers and service related semantic gateways, instead of on addresses and routers.

Towards “composable” networks

The concept of Service Oriented Architectures will apply to larger systems, encompassing the future networks. If we consider, in a loose definition, that a service component is an autonomous element that provides a function and that it has the required interfaces to be integrated with other autonomous elements in order to build a service, a network can then be considered as a service component, leading to the concept of “network as a service”. In a recursive way, the network of the future can be considered as the composition of various heterogeneous networks, each of them being considered as a service component, which itself is composed of service components of finer granularity. In particular, networks will become “dynamically programmable”.

Facing the always increasing capacity requirements for core networks

High-performance networking, including e.g., optical switching, are becoming again relevant after several years of drowsiness. Moreover, new inter-domain routing paradigms will emerge and intelligence will be introduced through concepts like semantic routing and the separation of identification and location. The combination of the new optical networking paradigms and semantic routing will reshape the present core network architectures.

Finally providing ubiquitous context-aware and composable services

Personalized, location and context aware services will become ubiquitous, accessible through a large diversity of access technologies, and globally mobile (mobility of services across any
type of borders). Service composition will become the rule. Services and network architectures will be jointly designed based on new paradigms such as publish/subscribe.

**From terminals to spontaneous and opportunistic edge networking**
Terminals are becoming networking capable devices implementing new networking paradigms. Disruption will be first introduced at the edge of the Internet; it started with solutions such as wireless mesh networks, vehicular networks, disruption tolerant networks, etc. At the edge of the infrastructure we see a ring of self-organized networks, based on heterogeneous networking paradigms, in some cases and form cooperating with the infrastructure.

**Merging with the real world**
A second ring will make the real world collide with the new generation of WSANs, RFID, etc., allowing the so talked about merging of the digital world and the real world.

**From the Internet of Communicating Things towards the Internet of Cooperating Things**
Objects will no longer be connected to the Internet, they will become the Internet. The next generation of the Internet of Things, however, will be based on coordinated and cooperative interactions among things, providing an integrated experience in the context of an ever increasing diversity of services.

**From the Internet of things towards the real world Internet**
We will no longer talk about the Internet of information, the Internet of entertainment, the Internet of communication, the Internet of things, the Internet of energy etc., but about the fusion of all of them into the real world Internet, which will be “green” (or will soon not exist anymore).

**Future services and a better integration of networks and overlays**
Functionality provided today in overlays will move into the network. Examples for the short and midterm are content distribution, support of mobility and transcoding. In general, the intelligence of the global system will be distributed in different ways between the network and the overlays and this distribution will change depending on location and time in order to achieve a global optimisation. New paradigms for content distribution will be developed.

**Mastering the complexity through self-organization**
Centralized policy based management and control will be replaced by self-organization in order to master the ever increasing complexity. Cognitive radio for advanced spectrum sharing approaches is just a first example.

**Introducing the required implementation flexibility through virtualization and programmability**
Virtualization and programmability will represent key enablers for realizing the previously introduced concepts and principles.

**Governance**
The network of the Future will go along with more complex governance challenges. Internet Governance of the future should be decentralized, diversified and adjusted according to the special needs of given issues globally or locally. Global Internet Governance of tomorrow should be a federated system where all stakeholders - governments, private sector, civil society and the technical community - will be involved in their respective roles.
THE EURO-NF OVERALL VISION

1 AN OVERVIEW OF FUTURE COMMUNICATIONS

1.1 A Brief History of the Internet

The Internet (and its precursor, the Arpanet) was conceived as a network to provide services to research labs; envisaged services were mainly limited to remote computer access, file transfer and mail. Therefore, the user population and traffic volume were quite small, the users were “friendly” (no security issues) and there were neither stringent quality requirements nor business stakes. In 1992, the Internet officially became a commercial network and the number of ISPs began to increase very rapidly, marking the start of the second phase of development. New applications, like the web and then peer-to-peer file sharing, gained widespread popularity leading to an explosion in both the number of connected hosts and the traffic they generate. A significant part of the industry effort during the nineties was devoted to dealing with this phenomenon.

Thanks to the openness of the IP protocol, we have witnessed a rapid extension in the service diversity. Following the investments in developing the Internet, the network operators better understood the advantages of the IP architecture to deal with the evolution of services. A natural consequence was that most telecommunication network operators decided to migrate their networks towards all-IP architectures capable of handling present and future applications, services and traffic structures efficiently and cost effectively. This evolution, with IP becoming the core technology of operator managed multiservice networks, can be defined as the third phase of IP networking development.

A major effort is currently being made by the industry to implement this third phase. We can in fact see a parallel deployment of “closed” IP networks tailored to specific services controlled by telecom operators (IP telephony, IPTV, triple play, quad play as an expression of fix mobile convergence, etc.) and of a ubiquitous “open” Internet that is the support for a plethora of overlay services, generally provided by third parties, some of which compete with the services commercialised by telecom operators. IP telephony is the most obvious example of this competition; one can cite Skype as a major player in this domain.

In many cases the same infrastructure is supporting the specific services controlled by telecom operators and the overlaid services, therefore raising neutrality issues that are still far from being solved.

The present evolution of the Internet is also characterized by the increasing role played by end users who are becoming content and applications’ producers and providers. As a consequence, the multimedia digital content available online is increasing very fast, leading in some cases to new business models and raising Intellectual Property issues that are pushing the regulation and legislation to evolve. Some well known applications facilitating content distribution are YouTube, DailyMotion, Facebook and Myspace, just to cite a few.

It is interesting to observe that several of the new applications and services with major social impact, like those that allowed the emergence of social networks, were designed by end-users.
Current network developments tend to further increase capacity in order notably to handle the traffic of video related services, and to improve quality of service in terms of performance and reliability, as well as manageability. Capacity is in particular being increased in mobile networks, where a billion of broadband mobile users is expected by 2011, and mobile radio interfaces of 100 Mbps are expected by 2012. These developments are taking place within the present IP and Internet architectures; they do not bring technology disruption at the IP architecture level.

Unfortunately, the present IP and Internet architectures is now attaining certain limits that are implicit to the initial design decisions. It is increasingly recognized that the architecture will be unable to satisfy the requirements of anticipated evolutions in both information and communication services and cannot adequately integrate emerging technology disruptions.

More generally, it is well understood that the Internet plays today a major socio-economic role, for which it was not designed for.

In the next section we discuss trends in future communication and information services. We then identify the limitations of the present Internet architecture before describing the main trends that are likely to guide future networking evolution.

1.2 Main Trends in Communication and Information Services

After a long period during which the evolution of network and service architectures has been driven by technology (with the consequence that received services depended on the type of terminal, access technology and operator being used), we are finally witnessing the infancy of the move towards a user-centric approach. The concept of “user-centric” is very large. It encompasses, for example, the fact that networks are becoming transparent from the user point of view. Networking is integrated in the environment of the user up to the point where it just disappears in the sense described by Marc Weiser.

The coming paragraphs present the main trends in communication and information services, starting with the present evolution towards user-centric solutions.

1.2.1 Networks and personalized services ubiquity

In a user-centric environment, the user is only aware of personalized services that can be securely accessed from anywhere, at any time and using any available device and access technology (network and personalized services ubiquity). Moreover, the personalized services dynamically adapt to provide location and context awareness when, where and however they are required.

New paradigms of services’ architectures allow for a flexible service evolution. As an example, one can cite the architectures based on the concept of services’ composition, where the basic idea is that different players provide services components that are dynamically composed in order to create new services and to answer specific client requirements. The term services’ networking is being used, in some environments, to describe this concept. These new paradigms provide new opportunities that require new types of service level agreements and even new business models.

---

1 The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it. (Mark Weiser, PARC, 1991).
1.2.2 Global mobility

A second important concept regarding the way services will be provided in the future is the ubiquity of global mobility. Indeed, mobile networks used to deal with the mobility of terminals, but not with the mobility of services. In global mobility the service follows seamless the user, even when the user changes his terminal or when his terminal crosses any technology or administrative domain border. The terminal being used can change as the user moves during a communication in order to take advantage of the best possible ergonomics in the current environment. Borders between the networks of different operators as well as borders between operated and non-operated networks can be crossed with no apparent impact on the quality of the ongoing communication. (As an example, Fix Mobile Convergence is providing today seamless mobility between Wi-Fi and cellular networks.)

Seamless mobility through different technologies is usually called vertical handover. Vertical handover is a first step in introducing what the market calls “Always Best Connected” (ABC). The number of available access technologies is growing fast (2G, 3G, 3G HSPA, LTE, 4G, Wi-Fi hotspots, WiMax, xDSL, FTTx, cable, satellite, PLC, etc.). Today, the user is aware of the technology he is using and usually gains access to one network at a time using a specific technology. The Always Best Connected concept allows a user (in a general sense: person, machine, community, network…) to be connected at any time through the best available technology and/or network. The definition of “best” is based on previously defined user preferences and can be related to quality of service, cost, robustness, trust and other metrics. Connectivity can change seamlessly during a communication when better connectivity is discovered.

In the described service mobility environment, any terminal can be your terminal (after user identification, through, for example, bio identification). After being identified in a given terminal, and based on the user preferences, some of his services will seamless move into this specific terminal.

The network via which a user is connected can also be mobile (network mobility), as in the case of embedded networks, for example. Moreover, a user can be simultaneously connected to several networks (multi-homing) in order to compose a particular service using separate components provided by different networks. Again, connectivity across various technologies and networks and service composition are transparent from the user point of view.

The following figure summarizes the ideas presented in the last two sections.
Ubiquity is provided through a diversity of access technologies. Since it is not cost effective (CAPEX and OPEX) to deploy specific aggregation networks per access technology, there is a clear trend today towards network convergence: a unique aggregation network being used to support the whole set of access technologies. Since most applications are developed today over IP, these convergent networks have to be designed to transport IP efficiently. The market is therefore moving fast into the usage of carrier class Ethernet as the transport technology for these convergent networks. A significant research effort is being carried out to design the next generation 100Gbps and beyond carrier class Ethernet networks.

1.2.3 Community services, spontaneous and opportunistic networking

The third concept we would like to introduce is related with the communities of users. Communities are generally created spontaneously as also, in some cases, are the networks that enable their communications (ad-hoc networks, vehicular networks, mesh networks, etc.).

Edge devices (terminals, customer edge router, etc.) that were just connected to the infrastructure networks have now the capability to self-discover and automatically create networks.

A ring of self-organized networks is therefore extending the coverage of the classical infrastructure networks.

Mesh networks are being used to provide wireless connectivity in cities but also at building levels. As a side remark, let us highlight that in such an environment, the last mile may no longer be under the control of the telecom operators.

One can push these ideas further: as we are surrendered by more and more electronic devices and these devices may integrate radio interfaces and networking capabilities, one can imagine a future in which the density of such devices is large enough to partially replace existing infrastructure networks. One can cite for example the research effort that has been carried out on this domain in the project Haggle.
1.2.4 Merging the physical and digital worlds

The real world and the digital world will progressively merge. The very first consequence of this merging is that the global communication and information system will be aware of the user’s environment and preferences at any time and will adapt dynamically. Services thus become context aware. A very basic example is locality awareness. Other services may depend on the user’s current activity, his environment, his health status or even his present mood.

Merging the real and digital worlds is becoming possible thanks, for example, to the development of wireless sensor networks (WSNs), which rely on devices including sensor capabilities, a radio interface and networking capabilities, that can be embedded in most types of environments and systems, including existing communication terminals, vehicles (vehicular networks), clothes and most consumer electronic appliances. WSNs allow to sense, through the network, any distant environment.

The systems will also include actuators. With wireless sensor and actuator networks (WSANs) integrated with the Internet, users (in the broad sense, including machines) will be aware of conditions in distant places and will be able to control remote objects, mechanisms and environments. WSANs will have a major impact on health, environment, and transport, just to cite a few. They will enable innovative industrial and business processes.

By providing new interfaces between users, networks and service platforms, they represent a key technology for introducing the network transparency concept presented before.

At the application level, the merging between the physical and the digital worlds will be facilitated by paradigms like augmented reality and by the more common usage of virtual reality environments together with the advent of the so called 3D Internet.

1.2.5 Towards the Internet of things and the real world Internet

Related with the merging of the physical and digital worlds introduced in the previous section, the generalization of RFID technologies will allow each and every object to carry an electronic identifier (allowing for various types of information about the object itself and his history to be obtained). New generation RFIDs will be able to locate themselves, trace their location and the contacts they have made, learn information about their environment and to actively communicate this information to other devices. Of course these capabilities will be integrated with the sensor and actuator facilities presented before. These devices will be accessible though the Internet, they will be able to create themselves opportunistic networks. New service paradigms will be developed based on these concepts, enabling the so called “Internet of Things”.

As described by Julian Bleeker when defining his “blogjet concept” (objects that blog), it is important to distinguish “things” connected to the Internet from “things” participating within the Internet, leading to the so call “Real World Internet”.

The Internet of things will permanently reshape itself, due to concepts like the “compute to fabricate” described by Neil Gershenfeld. From macro-objects self discovering and coordinating to provide integrated experiences to the users, we will move to a world where micro and nano computers/objects will self organize to build new objects and computation capacity.
In the same way that we currently use search engines to find information, the same search engines will be used in the future to locate (sense, control, reshape and even create) specific objects and mechanisms. These technologies will first impact companies supply chains (see, for example, the activities being carried out by EPCglobal). But then, **most of our day-to-day activities will be related with the network**, as is already the case today for information retrieval and processing, for communication and for some of our entertainment. However, the underlying networking capabilities will be completely invisible from the user’s perspective.

Machine-to-machine communication will become an important component of this evolution since most electronic devices will include communication interfaces. Ambient intelligence will become the rule, where the various intelligent devices of the environment will communicate and collaborate to provide the end user with an integrated experience.

1.2.6 Self-organization and autonomous networking

The set of concepts introduced in previous sections induce a permanent increase of the complexity of networks and systems. It is not longer possible to control the whole system in a centralized approach, as is usually the case in present telecommunication networks (through Network Management Centers).

We therefore see a trend towards autonomous networking. The key idea here is that the network will locally monitor its behaviour, learn critical information and take local decisions. The system is designed in such a way that the concatenation of these local decisions induces the expected global behaviour of the system (which is the basic principle of self-organization). **Self-organization and autonomic networking** will be introduced as a means both to create **new service paradigms and to reduce the operational cost of existing services**, especially when these are based on the user-centric approach described above.

Peer-to-peer applications are a typical and interesting example of self-organization at the application level. The application level may also trigger the creation of networks to support self-organized applications (like ad-hoc networks). Moreover, autonomic networking will allow terminals and networks to dynamically install required mechanisms wherever they are needed to enable a required service. This approach is thus a key element for providing user-centric services. Autonomic networking also facilitates optimisation of resources usage through the introduction of various types of monitoring.

Cognitive radio represents an example, where local decisions drive a global optimisation of the usage of the spectrum.

Application awareness represents another good example of autonomous networking. In pure IP networks, packets are forwarded based on the address of the destination. In application aware networks, the network is able to identify flows and to recognize the user and application that have generated the flow. Therefore, local decisions like prioritisation and routing (semantic routing) can be taken based on this information, enabling the optimisation of the network resources under the constraint of providing to the user the requested quality of experience. Application awareness is evolving from a nice to have functionality towards a new networking paradigm that may challenge the supremacy of IP networking.
1.2.7  Service enablers’ overlays, Virtualization and Programmability

Application awareness can be seen as a service enabler for the provision of evolved services under a control of the usage of the network resources. Other types of service enablers are content distribution networks, network storage, caching, trans-coding, peer-to-peer based streaming, network security systems, infringing content exchange detection systems, etc. Most of the time, this functionality cannot be deployed today in the network equipment and is therefore usually deployed in so called control and service enablers’ overlays. These overlays are usually designed independently from the network, leading to a lack of efficiency.

We see two main evolutions in this domain. On the one hand, interfaces will be designed between the network stratum and the services’ enabler overlays stratum to facilitate a joint design and optimisation. On the other hand, the architecture of the services overlays will implement virtualization and programmability, which introduces the flexibility for rapid evolution, sharing of the same infrastructure among different provided services, and enables the usage of self-organization paradigms.

A key question in this environment is the optimal distribution of the intelligence among the overlay, the network and the edge devices, including terminals. Indeed, services’ enablers will progressively move into the network (storage, caching, trans-coding, etc.), and virtualization and programmability will also be introduced in the network infrastructure.

1.2.8  Home networking

Home networking is a particularly important area where self-organization is critical. In this context, the residential gateway (RG) plays a role of strategic importance. It enables the control of a wide range of home services extending far beyond communication and information services to include home security, home automation or any other service provided by an intelligent household device. We face here the convergence of communication, information, entertainment, home automation, and systems for the security of persons and goods. Technology will play a significant role in the emerging competition in this area between telecom operators, suppliers of consumer electronics and software developers. Clearly the pertinent market of telecommunication companies is broadening very fast. As a consequence, we are facing the limitations of present regulation approaches.

1.2.9  Enterprise networking

The concepts presented before (M2M, WSANs, community applications, Internet of things, etc.) will impact the industrial processes as well as the business processes and will open the possibility for innovative business models in most domains of the economy. Today enterprises are buying simple services like Virtual Private Networks, which are mainly connectivity services. Tomorrow, the Information Systems of the companies will be partially integrated and will take advantage of the information services related with the electronic codes carried by all the components of their joint business processes. New business models will be defined between services providers and between service providers and clients as the network facilities will be completely embedded in most parts of the industrial and business processes.
1.3 A Macroscopic View on the Network of the Future and Related Challenges

1.3.1 Evolution of present infrastructure based networks

Future networks will see an evolution of present infrastructure based networks (core and convergent access). This evolution will allow to significantly increase the capacity and to introduce personalized services, ubiquity and global mobility.

In the core, capacity and flexibility will be introduced with new optical networking architectures (e.g. optical flow networking). These physical layer networking technologies (under IP), together with application awareness and semantic routing (over IP) may reduce the predominance of IP routing as THE network technology.

Separation of locators and identifiers will introduce scalability and flexibility.

In the metro, carrier Ethernet will remain the transport technology of choice, with an evolution towards 100Gbps and 1 Tbps carrier Ethernet networking. Large investments are being carried out in this domain (for example in Germany with public financial support). In the access, capacity will be increased based on optical technologies like Passive Optical Networks (PON) and Super-PONs (based on DWDM technologies, with an increased coverage range and therefore significantly simplifying present network architectures and central offices management and enabling a significant reduction of the number of central offices). These technologies, together with new optical fibre technologies, like plastic optical fibres, will enable deploying fibre at an affordable cost till the houses and offices (Fibre to the Home – FTTH and fibre to the Office - FTTO). The combination of plastic fibre and Free-Space-Optics will allow for the deployment of “carrier-class” home networks. High capacity, efficient, flexible and cognitive radio will also contribute to increase the capacity in the access. We expect mobile radio interfaces of 100 Mbps by 2011. These technologies have to enable an efficient usage of the spectrum and a broad coverage. The evolution described in this paragraph will be mainly based on the present IP (v4 and v6) architecture.

1.3.2 Disruption may arrive at the edge

Disruption may arrive at the edge, on a first step, with the broadening of the usage of networking capable edge devices and future opportunistic and self-organized networking solutions. We have already mentioned as an example of edge networks the impact of mesh networks, with the risk for telecom operators of losing the control of the last mile. But disruption may come from innovative networking paradigms based on edge devices as previously described in this document.

On a second step, disruption may arrive with the digital systems hitting the physical world, as also previously described, based on sensors, actuators, RFIDs and more generally on the Internet of Things. New networking paradigms will be introduced, which in the mid and long term may impact the infrastructure based networks for which possible evolutions were described in the previous section.

1.3.3 Control and services’ overlays for the horizontal integration

The large diversity of devices and network architectures will be covered by overlays that integrate facilities like virtualization and programmability and that introduce the control and
services’ enablers required for deploying the services of tomorrow and for optimising resources and reducing operation costs. On top of these overlays, new service paradigms will be deployed: we already introduced the concept of services composition, but other can be cited, like the semantic web (web 3.0) and the return to network based applications. The last point refers to future architectures on which terminals will be generic and applications and personal data will be provided on line. Overlays and networks will be jointly designed and interact through smart interfaces.

1.3.4 Related challenges

1) Technology challenges

Some of the identified technology challenges are:

- High capacity, efficient, flexible and cognitive radio. We expect mobile radio interfaces of 100 Mbps by 2011 and of 1Gbps in the next generation. These technologies have to enable an efficient usage of the spectrum and a broad coverage.
- Flexible and reconfigurable optical networking, including concepts like optical flow switching and Super-PONs.
- Energy provisioning and limited consumption. New electronic technologies, based probably on chips using reduced voltage (see recent MIT announcements) may allow for reduced consumption. Future devices may be powered by ambient energy (body movement, body heat, etc.)
- Miniaturization based on nanotechnologies for the broadening of usage of WSANs and other devices that will be embedded in our environment (robot swarms, etc.).
- Interfacing with the living world based on the convergence with biotechnologies.

2) Architectural challenges

Some of the identified architectural challenges are

- Global convergence of networks and services
- Multi-domain networking
- Network transparency
- Services evolution
- System approach for dependability, security, trust, privacy
- Cross-stratum (services-networks), cross-layer, cross-technology, cross-terminal, cross-generation (migration) design
- Design of new networking paradigms
- A global architecture flexible enough to integrate new networking paradigms

3) Economic and governance challenges

The global convergence presented in previous sections is raising the question of what is a pertinent market today in the telecommunication industry. We already highlighted this issue in the context of home networking requirements. As a second example, let’s remind that Google today is providing a large set of applications and services, they delivered a mobile operating system and they have been bidding for the UHF spectrum in the USA (even if their strategy was not really to obtain it). Supposing they would have won the bid, they would have controlled a significant part of the chain of value for the provision of services. This shows that
the pertinent markets are no longer delimited as they used to be when present regulation has been stated and this will most probably induce structural changes in regulation in the future.

Regulation is changing in various countries regarding the detection and control of infringing copyright protected content exchange and other type of infringing content exchanges. This is raising specific technical-economic problems.

A lot has been said about the governance of the Internet, but the Internet of the Future and in particular the Internet of Things is raising new governance issues even more critical as the stakes involve most aspects of our everyday life and of our economy.

New business models are being envisaged in order to integrate the increasing role of end-users (e.g. content, applications and services production and provisioning, networking facilities provisioning, etc.). New business models have also to be envisioned between service providers, and here again this raises difficult technical-economic issues, in particular related with inter-domain routing. New cost-models are required to evaluate and regulate these new business models as well as innovative billing approaches.

Corporate industrial processes, business processes and business models will evolve based on the facilities provided by the Internet of the Future, and in particular by the solutions enabled by the Internet of Things (as has been anticipated by the EPCglobal activities).

These are just a few examples of socio-economic topics requiring specific attention.

1.4 Limitations of the IP Architecture and Major Networking Principles Evolution

1.4.1 A reminder on well known limitations

This section focused on the Internet and IP architectures. To progress from the current state of the Internet towards the paradigms described in the previous sections requires the integration of a range of existing and future technologies and architectures. By integration we refer to the seamless inter-working of heterogeneous technologies (multi-technological domain) and to the creation of end-to-end services over a variety of operated and non-operated domains. It encompasses the integration of future generation RFIDs and the Internet of things, wireless sensor and actuator networks (WSANs), personal area networks, mobile ad-hoc networks, home networks, mesh networks and fixed and mobile access networks. The present IP architecture (whether IPv4 or IPv6) is not well adapted to this integration, particularly in the case of the explosion of the number and diversity of connected tiny wireless devices. We face an evolution from hundreds of thousands of wired connected devices to a few billions of wireless terminals in the short term and towards trillions of wireless devices in the midterm. A flat architecture where each device has its own IP address and is directly connected to the Internet doesn’t seem realistic even if NAT like solutions are proposed.

Moreover, the original architecture was not designed to deal with very dynamic topologies (like those of ad-hoc, mesh and wireless sensor networks), with network mobility or with constraints on the capabilities of terminals like those arising in sensors or other devices that will come into general use in the near future.

New networking paradigms are being designed and will have to inter-work with the existing IP network.
The coverage of the Internet will spread to reach any piece of electronics (including new concepts like swarm of micro-robots based on nanotechnologies) and expand to other planets (planetary networks).

Therefore, the particular concern can be summarized by saying that the present Internet architecture does not scale to expand as described. Very fundamental Internet concepts, like addressing and routing, are not adapted to this evolution. Moreover, key protocols and their related control paradigms like TCP, are also ill adapted to this integration.

Concerning addressing, the fact that the same addressing plan is used to identify end systems, flows, objects, applications, services and individuals is a critical constraint on the development of innovative applications. In particular, it significantly adds to the complexity of mobile architectures introducing a number of problems that remain unsolved today.

The external routing protocol BGP4 is a key component of the IP architecture. Its limitations currently hamper the introduction of innovative business models between operators and between customers and service providers. Moreover, it does not provide the functionalities required for end-to-end traffic engineering and offers no means for the flexible provisioning of services with controlled QoS.

There are a number of issues with current transport protocols. For instance, TCP is not well adapted to very high speed networks, the identification of TCP/UDP flows brings high complexity in the development of innovative applications and services, the congestion control algorithms of TCP are not adapted for future multiservice networks and do not perform well over wireless links or in the contexts of multi-homing and vertical handover.

The above examples demonstrate the emerging limitations of the fundamental concepts of the Internet architecture and suggest that they cannot be removed by simple incremental evolutions. This leads us to believe that it is necessary to follow the so-called green field approach to define a new network architecture unhindered by the constraint of remaining compatible with the current Internet.

The Always Best Connected concept is part of horizontal integration (although it is an extension of what the market calls the vertical handoff). Horizontal integration can be partially achieved in a centralized way, for example through an IMS²-like approach, or in a distributed way, based on peer-to-peer paradigms (or a combination of both). The concept of Mobile Service Provider can play an important role in this context but raises several technological, business related and regulation problems.

Here again, the IP architecture restrains the generalization of innovative mobility approaches. One of the main reasons for this is addressing. A clear separation between different levels of identification and addressing is required. A network address is required to reach the destination. Nevertheless, this network address is not adequate at service and application levels. For example, a user may want to communicate with another user regardless of its physical location in the network. We may wish to obtain information but don’t care on which device or devices the information is stored. We may wish to locate objects by their name or a set of descriptors and act on them regardless of where they are located at any given

---

2 IMS: IP Multimedia System as defined by the 3GPP.
time. The present strong link between application/service level addressing and network addressing is already an inconvenience for legacy applications and a hindrance to the development of new services including the generalization of innovative mobility concepts. The identities of users and objects (terminals, sensors, actuators, all types of electronic devices,...), application identifiers, flows identifiers and network addresses (locations) have to be defined independently within a global unified architectural approach. Identification management remains a critical and quite open field.

The global interconnection of operated and non-operated networks raises new security issues, as illustrated by the following examples. Autonomic networking and self-discovery require tight control mechanisms to evaluate the level to which a newly discovered component can be trusted. Content distribution over several interconnected heterogeneous systems requires the inter-working of Digital Right management (DRM) systems or other means to allow valuation of intellectual property. In the envisaged open environment, robustness becomes critical. How can complex systems with global reach be protected against attacks? What are the risks of merging the physical world and the digital one, in particular when our health relies on this merge? Security must become an integral part of network and system design with appropriate interaction with other networking mechanisms (for example, trust can be integrated as a metric in the routing protocols used in ad-hoc, mesh and wireless sensor networks).

Despite extensive research over many years, Quality of Service (QoS) remains a major requirement for the future networks we are describing. Not only does QoS remain an issue in the present Internet, but most importantly, it raises new and extremely complex problems in the context of the multi-technology network interconnections described above. New traffic engineering, traffic management and traffic control paradigms have to be designed. Since QoS is an end-to-end concept, these designs must take into account both technological solutions and the viability of implied regulation and business models. In the present Internet, not only there are no clear business incentives for the deployment of QoS but worse, there may even be a significant disincentive. If a network provider offers guaranteed quality levels, this tends to facilitate the task of any competitors who use that network to offer overlay services. Resource control and optimisation, particularly in the context of flexible radio (cognitive radio, software-defined radio, etc.), is a major concern. Lastly, new inter-domain routing paradigms have to be defined to facilitate essential end-to-end traffic engineering mechanisms and to enhance service provider business models.

The evolution process can be summarized as a migration from multiservice networks to multi-network services. The “multi-network” is more than an integration of networks. It can integrate external facilities like time and position information obtained through the Galileo satellites.

1.4.2 Networking principles evolution: Towards polymorphic networks

The first conclusion of previous section is that the network of the future will be polymorphic; it will consist on the interconnection of networks with a large degree of architectural and technological diversity (therefore the term polymorphic). IP won’t be any longer the universal network layer (the hourglass model will vanish), and as we are going to see in this section, the concept of layer will itself evolve and in some environments disappear.

We believe that disruption will be introduced without revolution; in other words, disruptive solutions, based on new (non IP based) networking paradigms, will in a first step extend the existing networks.
Since no common end-to-end networking technology will be available, the gateways that will interconnect the various heterogeneous networks will be devices that in many cases will have services related intelligence. Semantic gateways will receive services’ requests through the IP network, will interpret the request and take some actions on networks which are not IP based. The requests will be based on identifiers and not on addresses as explained before. As an example, in many applications of wireless sensor networks addressing and IP like routing are not required. Indeed, let’s think about a wireless sensor network used to monitor the level of humidity in a field, applications will not be interested in the address of a sensor (by the way most probably many different sensors will monitor the required data) but on the data itself. For distant querying of the WSN, a possible architecture will be based on a smart gateway connecting the WSN to the Internet. A request will be based on the identifier of the requested information and this identifier will be translated into the IP address of the gateway. The wireless sensor network could be based on a periodic sensing of the information being sent to the Gateway by classical networking paradigms used in this case which do not requires a routing protocol. In this example, the IP network is therefore terminated in the gateway.

We will therefore move from a “homogeneous” architecture based on the concepts of IP addressing and routing gateways to an architecture based on the concepts of identifiers and smart multi-technological gateways.

Some of the paradigms will spread into the IP networks, leading to an evolution of its architecture. As an example, from the moment that gateways have the intelligence to understand services requirements and to implement related functionality, it becomes natural to extend the basic existing IP routing to introduce semantic routing. In others words, the introduction of disruptive architectures at the edge of the existing ones will lead to the evolution of the latter.

The existing IP networks will one day lose their predominance as the core technology of the core allowing the global interconnections of all other networks to become one more network paradigm among the others to be interconnected, therefore moving towards a mesh interworking of heterogeneous networks. We will therefore move away from the hourglass paradigm.

The same as in the past IP allowed for the interconnection of lower layers islands of heterogeneous technologies, the network of the future will allow the interconnection of networks with different networking paradigms, the internetworking being based on services related semantic information instead of being based on addresses.

1.4.3 Networking principles evolution: Towards” composable” networks

We already mentioned the concept of services composition. We didn’t define what a service component is, but if we consider in a loose definition that a component is an autonomous element that provides a function and that has the required interfaces to be integrated with other autonomous elements in order to build a service, therefore a network can be considered as a service component, leading to the concept of “network as a service”. In a recursive way, the network of the future can be considered as the composition of various heterogeneous networks, each of them being considered as a service component, which is itself composed of service components of finer granularity. Therefore, a key functionality like routing can be considered as a service component.
At a first glance, this is just a new terminology to describe the systems that we already have. Nevertheless, the approach can be used to build much more flexible systems compared with what we have today. Indeed, if all these components are defined using standardized semantics, their dynamic composition becomes possible and we will move into networking architectures that will be dynamically composed to answer specific services and application requirements.

The new architecture will be flexible to introduce new networking paradigms (including those envisaged today, like delay and disruption tolerant networks, coding networks, quantic networks and others that most probably will be imagined in the future).

The future architecture has to be designed considering socio-economical issues related with governance, neutrality, privacy, intellectual property management, etc.

At network level the objectives are coverage and connectivity. In the envisioned future environment, these objectives have to be reached under new constraints: a highly dynamic network topology, composed of very heterogeneous devices some having specific limitations in terms of resources (CPU, power, etc.); a rapid growth in the number of devices and in particular an explosion of the number of wireless devices, with generalized and global mobility; a multi-domain context including operated and non-operated domains; specific requirements in terms of security and end to end quality of service, including robustness.

1.4.4 Summary on networking principles evolution

As stated before, we believe that disruption will be introduced without revolution; in other words, disruptive solutions, based on new (non IP based) networking paradigms, will in a first step extend the existing networks. We will therefore move from a “homogeneous” architecture based on the concepts of IP addressing and routing gateways to a polymorphic architecture based on the concepts of identifiers and smart multi-technological gateways.

Some of the paradigms will spread into the IP networks, leading to an evolution of the IP architecture.

Moreover, future networking architectures will be dynamically composed to answer specific services and application requirements. These new principles will provide the required flexibility to easily introduce new networking paradigms.

The future architecture has to be designed considering socio-economical issues related with governance, neutrality, privacy, intellectual property management, etc.

The concept of compassable network and services architecture will lead to a better integration between network and services strata.

The cited evolutions will pave the way towards the above presented merge of the digital and physical worlds and therefore toward the Internet of things and beyond the “Real World Internet”. When writing “Real World Internet we keep in mind Julian Bleecker view, distinguishing “things” connected to the Internet from “things” participating within the Internet; things being dynamically shaped or even created through the Internet.

1.5 Organization of the Following Sections

In the next section, some of the most important new networking paradigms and network architectures, already deployed or under consideration, will be presented. In section 3, a
detailed presentation of the two main properties introduced previously (i.e., polymorphic and composable networks) will be introduced. Indeed, section 3 introduces the basic principles Euro-NF envisions for the network of the future. Finally, section 4 discusses a shared vision concerning the governance of the network of the future.

2 NEW NETWORKING PARADIGMS AND NETWORK ARCHITECTURES

In recent years, new networking paradigms that do not follow the Internet paradigm have been developed and originated the deployment of innovative networks. These innovative networks are deployed at the Internet edge. They actually interconnect to the Internet through appropriate gateways. Most well-known examples are Ad-hoc networks, Wireless Sensor and Actuator Networks (WSAN), Networks of cooperating objects also known as Internet of Things (IoT) and Delay Tolerant Networks (DTN).

Ad-hoc networks are spontaneous organized networks established among communicating devices of the users, which use self-organization concepts for their formation and follow their own routing protocols. WSAN are sometimes considered as a subset of ad-hoc networks, but their widespread use nowadays implies that they are actually a class of networks in their own with specific functionalities and protocols. In WSAN networking, the routing protocols are also different from the Internet protocols and WSAN use their own transport protocol solutions to increase the network dependability. Also, the WSAN network structure, in which we have several sensor nodes sending information to a sink node, through a process of aggregating information and use of a multi-hop communication process, is specific of this type of network and deeply connected to their application objectives.

On the other hand, network embedded systems, as we see them today, and as they are used in application scenarios, such as automation and control, healthcare, security and surveillance, logistics and transport, commerce or environment care, could be referred to as networks of cooperating objects, with the semantics of interactions being simply communication (data exchange). The IoT, coined by industrial and commercial stakeholders inspired by identification technologies like RFID or NFC, and the possibility of linking physical objects like goods and products to data deposited “in the Internet”, is an example of this type of network. Some of the networking concepts of WSAN will apply here, but aspects linked to the challenge of managing these objects in an autonomous way, with little or no human intervention through self-organization techniques will be key to the future deployment of IoT.

Delay and Disruption Tolerant Networking (DTN) is a new networking paradigm that deals with the establishment of new communication protocols to improve the network communication in case the connectivity is intermittent and/or subject to disruptions. Delay means the end-to-end latency of the data transmission. Disruption refers to factors that are in the origin of connections to break down or even of not being established. The initial research in DTN was done for interplanetary communication, but later, the concept was generalized to include also terrestrial applications, which present similar problems, for example, in some applications of wireless sensor networks. DTN is using an overlay protocol (bundle protocol), which provides delay and disruption tolerance, providing support to the distinct DTN applications. The protocols that are used in the layers below the bundle layer might be diverse and are chosen according to the communication environment of each region.
These examples of new networking paradigms show that innovative concepts for networking are already in deployment, although most of them at the edge of the network there are some approaches addressing the core architecture itself. This perfectly fits into the architecture that we are envisioning for the Network of the Future, in which edge networks with a different paradigm from the core network (presently the Internet) can co-exist and connect to the core through an appropriate gateway. Moreover in the long run such a new paradigm can become the core of a new inter-networking architecture. Also, we should not forget that for many of the applications envisioned for these networks the identification management approach instead of the present addressing scheme, might also apply.

It has been long realized that the Internet is evolving from a network connecting pairs of end hosts to a substrate for information dissemination. Indeed, a major part of today's Internet traffic is due to content distribution applications, in most cases peer assisted applications. This means that redundant unicast transmissions of the same packets are not avoided; they are just distributed among the peers. And the actual source of this problem is the current Internet's reality of lack of support for multicast. At the same time, the end-to-end semantics of the current communication paradigm are at odds with the provision of effective mobile services. Some new concepts for new networking paradigms that are still at a research stage have already been presented. One of them is the publish and subscribe (PubSub) networking concept.

If shifting towards the publish/subscribe paradigm, multicast becomes the main routing mechanism for the delivery of an information item to the group comprised by all the item's subscribers. Hence, this missing network service is intrinsic in the new architecture, paving the way for the efficient distribution of large volumes of content around the Internet. However, since the focus is on content, which could be signed and globally identifiable, peer assisted content distribution will still be useful for asynchronously distributing very large amounts of data and the network will make use of content caching efficiently at various timescales. Moreover, the indirect and asynchronous character of the publish/subscribe communication paradigm allows mobile nodes to adapt quickly to frequent disconnections and reconnections, making it advantageous in a mobile network environment. At the same time, in view of the availability of multicast routing, multicast assisted mobility re-emerges as a promising direction for the effective and efficient support of mobility.

Besides the PubSub paradigm there is a lot of other work related to the topic future networks. Interesting clean-slate approaches which are related to the vision document can be seen in the “RoleBased Architecture” (RBA), the “Service Integration, control and Optimization” (SILO), the “Recursive Network Architectures” (RNA), the “Data Oriented (and Beyond) Network Architecture” (DONA), and the “Service oriented Architecture” (SONATE) approach. The RBA approach introduces a non-layered architecture to the design of network protocols and organizes communication in functional units referred to as “roles”. Roles are not hierarchically organized and thus may interact in many different ways. The main motivation for RBA is to address the frequent layer violations that occur in the current Internet architecture, the unexpected feature interactions that emerge as a result, and to accommodate middle boxes. The SILO approach also introduces a non-layered design based on silos of services. Furthermore it offers a more flexible header structure than the RBA approach. The overall goal of the SILO architecture is to facilitate cross-layer interactions in a manner that meets the user requirements accurately and optimizes performance. The RNA approach examines the implications of using a single, tunable protocol for different layers. RNA reuses basic protocol operations across different protocol layers, avoiding redundancy of implementation as well as encouraging cleaner cross-layer interaction. It allows protocols
and protocol stacks to adjust at runtime. This results in a more dynamic composition of services, both within stacks and in the way networks combine the stacks of individual hops into an overall network architecture. DONA takes into account that the vast majority of today's Internet usage is data retrieval and service access, whereas the architecture was designed around host-to-host applications. While the main motivation for RBA, SILO, and RNA approaches was to address the frequent layer violations and cross-layer interactions that occur in the current Internet architecture, the SONATE approach has a focus on network flexibility and evolutionary principles by utilizing principles of service-oriented architectures. This is based on a collection of autonomous services, identified by their references, with interfaces syntactically and semantically described, and processing well-defined messages. Such an approach based on horizontally distributed functionalities promises a higher degree of flexibility than other approaches.

3 POLYMORPHIC AND COMPOSABLE NETWORKS: AN OVERVIEW

3.1 The Principles

Driven by the demands of ever emerging applications and the capabilities of new communication networks present Internet has become an architectural patchwork resulting in increasing complexity and unpredictable vulnerabilities. As stated in the previous chapter, these problems are not only related to specific protocols or mechanisms but are mainly caused by the current Internet architecture, which is unable to integrate new approaches seamlessly. To address the principles of a polymorphic and composable network presented in the first chapter, we have to design a new and open network architecture based on standardized generic components/service interfaces, in which it is possible to decouple logic from implementation. This enables a simplified integration of new transport technologies and new networking paradigms and increases the flexibility of communication systems in order to be prepared for future applications.

Here we address a new and powerful solution for the design and development of distributed, open, flexible and adaptive networked systems in which components have a high degree of autonomy based on a semantic description of their capabilities. In general, such a system is built using a collection of autonomous services, identified by their references, with interfaces syntactically and semantically defined using an interface definition language, and processing well-defined messages. Thereby such an approach is an advance to the object-
oriented, procedural and data centric approaches and differs mainly in one aspect: binding. So the overall question is finding the right “glue” between application demands and network capabilities whereas the functionalities/components within the clouds are able to float depending on the capabilities of the cloud.

In the context of this vision document we want to apply the above ideas to generate a new architecture to the communication area so that components can be seamlessly used through all layers and give a holistic view of communication.

Thereby it is clear that current implementation technologies are not sufficient to implement loosely coupled components within a communication context. Nevertheless, a future network based on these ideas seems to be a promising approach due to its ability to evolve, i.e. to add, change and replace or extend functionality more easily than today. Just defining a new set of protocols for a future Internet is not sufficient, because it will be impossible to take into account all future demands. In consequence even a completely new designed future Internet will be subject to ongoing evolution. This demand cannot be achieved by a single component or protocol, but must be supported by a new architecture that defines the fundamental organization of a system, the relationship of components, and the design and evolution principles. Especially the definition of evolutionary principles allowing deliberate extensions and replacement of functionality are important to avoid the architectural patchwork appearing in today’s Internet.

Thus, applying these ideas some interesting challenges that have to be addressed are the following:

- **Remove tight coupling:** The basic idea is to free the applications from tight coupling to a certain protocol (TCP/UDP) and enable them to use loosely coupled network services. This means that applications can formulate their demands and the transport technologies (fixed, mobile networks) can offer their capabilities. A new network architecture should be able to map the demands of the applications into the capabilities of the transport networks appropriately. In such an approach all functionalities (like routing, DNS, ...) should be implemented as loosely coupled services. Loose coupling between the participating software agents can be enabled by a small set of simple and ubiquitous interfaces, descriptive messages constrained by an extensible schema delivered through the interfaces. None, or only minimal, system behavior is prescribed by messages.

- **Separation of concerns:** The challenge is to implement these ideas **even** in the lower layers of the network. The definition of interfaces between services as well as synergistic interaction of applications with the network are the focus of such an approach. Also the separation of the data plane from the control plane is a major concern. Such a separation is difficult to realize in today's Internet. This is because the network nodes are vertically integrated and content providers have no direct access to the control plane. The component based approach is based on horizontally distributed functionalities which promise more flexibility than the other approaches.

- **Dependable service architecture:** The development of an open, dependable and distributed new future network architecture based on this approach is an active area of research that is still in its infancy. A number of research challenges are
thus yet to be addressed to actually enable the dependable composition of services/components across current layers. Issues include the thorough specification of individual services and of their composition, so as to ensure the dependability of the resulting systems as well as to allow the dynamic integration and deployment of composed services. Also, associated dependability mechanisms should be devised to enable full exploitation of the dependability properties enforced by individual services and also to deal with the specifics of the systems. Another issue relates to allowing the deployment of services on various platforms, ranging from resource-constrained devices to servers.

- **Semantics**: An extremely important area of R&D is that of bringing semantics to the components/services. Like the W3C has created a working group on Semantic Web to work on the representation of data on the World Wide Web it must be possible to transfer these ideas and methods into a service-based future network architecture and especially into the lower communication layers (i.e. for service composition and service discovery).

- **Service composition**: Another important area of future research is developing rigorous methodologies supporting service composition. TLA+, among other techniques, will achieve an important role in supporting unambiguous communication between protocol engineers and implementers. This will make it possible for services to be automatically validated to detect non-conformance to the specification, while testing in productive distributed systems. This will also lead to developing a proven set of general purpose, high quality protocols that can be combined modularly to address common issues.

The translation of application requirements into specific services composition will be supported by new generation middleware based on the so called “decision plane”. Components semantics will integrate identifiers on which the global architecture will be based. The following sections introduce these key elements of the global architecture: ”decision plane” and “identification management”.

### 3.2 Knowledge and Decision Plane for Component Management

A critical pre-requisite enabling the composition of global services in benefit of various types of users (humans, enterprise, institutions, and machines) is the management of information. The information is the feed for intelligence and as such its availability, amount (exponential growth) and accuracy becomes a transverse key area in the network of the future research domain.

As per the networking history, the usual scheme was to either flood the information (i.e. link state protocols) or centralize it for management purpose (i.e. NMS limited to an administrative domain). Ubiquity is meaningless if not empowered by the sufficient level of knowledge, enabling awareness of given service components (and their refreshed status along time). We will use the so-called **Knowledge Plane** (KP) terminology to describe the set of functions related to the information management.

Within the KP, one can distinguish different types of information operation, leading each to open questions and requiring consequent research efforts.
**Discovery** is the first field where it is required to provide mechanisms searching location (even virtual) of relevant sources. Of course, breaking the flooding paradigm, networks of the future should propose efficient strategy limiting this type of operations to the minimal but relevant space (i.e. situated view) and time (refresh timer, statistics ...) domain. Example of scientific contributions may be related to Autonomous processes (adaptive behaviour), learning techniques, functional architecture and protocols allowing a smart discovery feature.

**Aggregation** stands as the next challenge as the KP should transport only the relevant and required information avoiding redundancy (or limited for robustness purpose), useless or obsolete information. Focusing on the intrinsic semantic of service components required for composition and specific operations on a given service component (including networking operations). As such, the aggregation issues are fully open and research should bring network-wide consistent and accurate methodologies: understandable formats and language, fusion, filtering, sampling, policing and context aware, for example. Last but not least, the KP will have the responsibility to **distribute** the information to the right place at the right moment. Behind the statement, sophisticated approaches embedding, learning, communication protocols (paving the way for standard interfaces) and adaptive (or even predictive) routing are required.

The applicability of the KP is an answer to the increasing amount and complexity of the information; this should not be taken as a substitute to the control plane protocols as its application scope is wider integrating service components from networking to any kind of service component supplier (human, machine, computation, storage, atomic and any intermediate multi-component service). As a specific enabler for the network of the future the KP will serve for component identification management described below.

The **Decision Plane** (DP) will perform component (i.e. service and network) management tasks with the goal of providing accountable, well-performing and safe component services for the desired communication workflows. By nature, such decisions are highly connected to the role of the component in the overall service and network context. Thus, they might address a plethora of tasks such as resource assignments, routing optimization, handover decisions, service adaptation, etc. Decisions have to be taken both in a reactive (problem solving) and a proactive manner (problem avoidance).

However, as opposed to current component- and role-specific decision structures, we foresee a generic underlying structure of a component and its decision facilities, no matter where in a communication workflow that component is to be found. Such modular management per component will allow for a flexible, straightforward and dynamic composition of overall management functions beyond concurrent stringent and static structures. In particular, different organizational models such as customer-provider, client-server or peer-to-peer will be realizable as needed.

In order to derive optimized decisions as central part of these management tasks, the DP will rely on information provided by the KP, where the direct exchange of feedback and control information between neighboring components such as customer and provider or peers plays a major role. Such a control stream will be found aside of the data stream; control data will mainly be used for service invocation, negotiation of performance, security and cost parameters, feedback of the status of the service, e.g. performance data or urgent reporting of problematic states, service modification and termination, respectively. The addressing of other components will happen through the information provided by the KP. Besides direct
interactions with other components, a component might also take context information into account. The amount of control information to be produced or consumed by components will strongly depend on the service to be provided and on the related decisions to be made. Given the enormous variety and complexity of foreseen service compositions as well as the enormous span of components’ capabilities, a major challenge is to shape the inter-component feedback as generic and lightweight as possible, targeting a minimal and generic set of communication primitives.

A major property of future service-providing components is autonomous behavior. In the context of Autonomic Computing and Networking, self-organized components are the atoms of larger self-organized workflows. Thus, it is natural that each component will apply self-management including self-diagnosis, self-healing, self-maintenance, and self-optimization. Research related to the DP will have to address amongst others: (a) identification and investigation of decision-making strategies and methods; (b) design of autonomic components, together with the required intra- and inter-component feedback; (c) investigation of the dynamicity of systems, including the identification of critical timescales; (d) design and analysis of microscopic and macroscopic control loops (spanning over a set of components), with regards to their abilities to provide customer satisfaction and (e) investigation of proactive control measures, aiming at improving service availability. These research items will need to be substantiated per component and workflow.

3.3 Identity Management

The task of Identity Management (IdM) is to provide the means to uniquely identify and address customers and components (i.e. entities producing and consuming services), with the added value of a semantic description of the component. The corresponding component identifiers (CID) are used for purposes of identification, authentication, mediation and accounting.

A component that needs a service from some other component needs to know the CID or a way how to retrieve it. Discovery, filtering and distribution of CIDs are handled by the Knowledge Plane as described above. As successful mediation between components depends on the CIDs, they need to be properly designed, treated and protected in order to avoid malfunctioning and potential misuse. Examples for related risks are unpaid service access; pollution of the component space with useless inter-component communications; Denial-of-Service attacks; disclosure and corruption. Faulty or malicious components need to be identified and black-listed in the Knowledge Plane in order to pave the way for remedies.

Research on IdM needs to address the design of identity management and CID, with focus on the ability to locate components and on trustful communication with them while being as generic, extendable and lightweight as possible. This implies the need for risk and performance evaluations of potential solutions, targeting to assess the facility to provide sufficiently strong authentication, well-working mediation and reliable accounting information. Furthermore, the aging and renewal process of information relevant to IdM needs to be studied thoroughly in order to keep the data in the Knowledge Plan as compact and consistent as possible.
4 GOVERNANCE OF THE NETWORK OF THE FUTURE

To discuss the Governance of the Network of the Future, it is important to understand, where the terminology “Internet Governance” comes from and how the concept has been evolved over the last decades.

The terminology “Internet Governance” was coined by members of the Harvard Information Infrastructure Project (HIIP) in the 1990s. It described a mechanism of the management of the borderless Internet without the direct involvement of governments. The concept of “governance without governments” was seen as the most efficient way to coordinate the political and technical administration of the critical Internet resources (CIR) like the root server system, the Internet identifiers (domain names and IP addresses) as well as Internet Protocols. Internet Governance was narrowly defined and the coordination of the management was executed primarily by the technical community.

The institutional mechanisms for Internet Governance evolved in the 1970s and 1980s and were designed and operated by the developers, providers and the users of Internet services themselves, mainly in the US. It included technical non-governmental and private sector organisations like the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Internet Architecture Board (IAB), the Internet Society (ISOC), the Internet Assigned Numbers Authority (IANA), Regional Internet Registries (RIR) like RIPE, ARIN and APNIC and the registries for ccTLDs and gTLDs as Network Solutions Inc. (NSI), which managed the .com, .org, .net and .edu domains and operated the A Root Server.

A special governance mechanism for the DNS was developed by Jon Postel. In the beginning he was the only manager of the DNS and delegated the management of Top Level Domains (TLDs) by handshake to trusted individuals. Postel also managed IANA which operated the TLD database and allocated IP address blocks to the RIRs. Some of these institutions, in particular IANA and NSI, operated under a contract with the US government which funded, first via the Department of Defence (DoD) and later via the National Science Foundation (NSF), Internet related research.

National governments or intergovernmental organisations were not involved in the governance of the Internet in these early days. Even the delegation of country code Top Level Domains (ccTLDs) took place without the involvement of the government or the parliament of the relevant country. While earlier technological innovations like the telegraph in the 19th century or radio broadcasting in the early 20th century provoked immediately a governmental regulation in form of national telecommunication and broadcasting laws – and later negotiations of international conventions and treaties - there were no similar governmental activities when the Internet emerged. The needed regulation for the borderless Internet was mainly technical by nature and done by technicians themselves or by the providers and users of the Internet [2].

A new model for “regulation” of a network was developed in the early 1970s by the so-called “Request for Comment” (RFC) procedure, proposed by Steve Crocker. The RFCs, today the “Law Book of the Internet”, is now managed by the IETF. The mainstream philosophy of the Internet pioneers in the early Internet days was that there is no need for the involvement of
governments into the governance of the network. Even more, many Internet experts explained
the outstanding success of the Internet with the absence of governmental regulation and
rejected any role of governments in the new emerging cyberspace. Dave Clark from the
Laboratory of Computer Science at the Massachusetts Institute of Technology (MIT) did set
the tone in a speech before the Internet Engineering Task Force (IETF) in 1992, titled “A
Cloudy Crystal Ball – Visions of the Future”. In his paper he formulated a principle which
became the Leitmotiv for the global Internet community: “We do not believe in kings,
presidents and voting. We believe in rough consensus, factual approach and running code” [3].

The fear within the Internet community was that governments, as soon as they would exercise
control over the Internet, would restrict individual rights and freedoms - in particular the right
to freedom of expression and the right to privacy – and would introduce time and cost
consuming procedures which would turn down the speed of innovation in the development of
new Internet services and applications. The preservation of the end-to-end principle and the
P2P communication model was seen as a guarantee for the freedom of the net. De facto,
freedom and flexibility was embedded into the architecture of the net and the Internet
architecture was defined by technical code.

Based on this Internet architecture - a multilayered system with many players – self-
governance, self-regulation, private sector leadership and bottom up policy development in an
open, transparent and inclusive manner were seen as the key elements of the proposed
network policies and relevant regulatory frameworks. With other words: The Internet
governance system was a distributed system with no single unit in charge for everything. It
was and is a “multilayer multiplayer mechanism” (M³).

In 1997, Done Heath, at this time president of the Internet Society (ISOC), said in a speech in
Geneva: “We believe that for the Internet to reach its fullest potential, it will require self-
governance. The Internet is without boundaries; it routes around barriers that are erected to
thwart its reach – barriers of all kinds: technical, political, social, and, yes, even ethical, legal
and economic. No single government can govern, regulate or otherwise control the internet,
not should it. Most governments, the enlightened ones, will say that they endorse actions by
responsible parties for efforts towards self-governance of the Internet. This does not mean that
they should not be involved, they must be involved; they just need to exercise caution so that
they don’t control and dominate by virtue of their intrinsic power” [4].

The US government supported this private sector leadership as guiding principle for Internet
Goverance and delegated in 1998 elements of policy coordination for the management of
Internet identifiers – root server, domain names, IP addresses and Internet Protocols - to a
new established private “Internet Corporation for Assigned Names and Numbers” (ICANN).
According to its Articles of Incorporation, ICANN is obliged to develop policies “for the
benefit of the Internet community as a whole”.

ICANN represents a private sector led multi-stakeholder governance model, where policy is
developed in an open and transparent way bottom by the involved and affected constituencies.
Governments are involved in an advisory capacity via the Governmental Advisory Committee
(GAC). ICANN is led by a Board of 15 Directors. The ICANN Board is composed by
individuals, representing the Internet community as a whole. Six directors are sent to the
Board by representatives of the Domain Name Industry (DNI) and the IP Address community,
eight directors are selected by a Nomination Committee (NomCom). ICANNs CEO, who is
member of the Board, is elected by the other 14 Board members. Additionally six “non voting liaisons” represent various technical communities in the ICANN Board. Governmental representatives are not eligible to the Board. Governments can send via the GAC non-binding recommendations to the Board. If the ICANN board rejects a GAC recommendation, the GAC can ask for consultations. If the consultations fail, the ICANN Board is obliged to explain to the Internet Community the reasons for the failure. ICANN is linked via a “Joint Project Agreement” (JPA) to the US Department of Commerce. The JPA expires in October 2009.

The ICANN model was challenged by numerous governments during the UN World Summit on the Information Society (2002 – 2005). It was in particular the government of the Peoples Republic of China which called for governmental leadership in Internet Governance and proposed to transfer functions of ICANN to the International Telecommunication Union (ITU), a Geneva based UN Specialized Intergovernmental Agency. The European Union proposed a “middle of road approach in form of a public private partnership, where governments would execute responsibilities on the “level of principle” while the private sector should remain responsible for the “day-to-day operations”.

To bridge the controversy between the principles of “private sector leadership” and “governmental leadership”, UN member states asked in December 2003 UN Secretary General Kofi Annan to establish an UN Working Group on Internet Governance (WGIG) with the mandate to propose a definition of Internet Governance, to identify public policy issues in Internet Governance and to define the role of the various involved stakeholders. WGIG defined Internet Governance as “the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.” [5].

A key element in this definition is that it recognizes that all stakeholders have to be involved in Internet Governance, but in “its respective role”. There is no “leadership” or “subordination”. “Respective role” means new and innovative forms of communication, coordination and collaboration (C³) among involved parties according to the specific needs of a concrete issue on equal footing. Such a new “network governance model”, which links governmental and non-governmental stakeholder “in their respective roles” on equal footing together is rather different from the traditional “hierarchical governance model” of the intergovernmental system with the sovereign nation state at the top of a decision making hierarchy.

With other words, WGIG concluded that the Internet should not be governed by one single entity top down but its management should be improved by better communication, coordination and collaboration (C³) among different organisations and stakeholder groups bottom up. WGIG rejected the idea of the establishment of an intergovernmental UN Internet Organisation (UNIO) but recommended, inter alia, to introduce a new high level discussion space for Internet Governance issues by the creation of a multistakeholder “Internet Governance Forum” (IGF) convened by the UN Secretary General. The intention was to fill “a vacuum within the context of existing structures” and to address “issues that are cross-cutting and multidimensional and that either affect more than one institution, are not dealt with by any institution or are not addressed in a coordinated manner”. Such a IGF should have no decisions making capacity but should inspire intergovernmental and non-governmental organisations, dealing with aspects of the Internet, to enhance their inter-
institutional cooperation and to make informed decisions within their constitutional competences in the light of the deliberations of the IGF. The IGF was established in 2006 and will see its 4th version in Sharlm el Sheikh (Egypt) in November 2009.

This “broad definition” proposed by WGIG, was adopted by the Heads of States during the 2nd Phase of the UN World Summit on the Information Society in Tunis (November 2005). It allowed also to develop a more diversified approach and to develop different governance models for different Internet governance issues. According to this definition, Internet related aspects of public policies as well as of technical policies can be governed in a different way taking into account the very specific nature of the individual issue.

Future Internet Governance will go beyond the ICANN model. While ICANN will continue to coordinate the management of key Internet identifiers, in particular the DNS (new gTLDs, iDNs) and parts of the IP address space (IPv6), there will be complementary governance mechanisms for the management of other components of the Internet. Some of such new mechanism may appear with the further development of the so called Internet of Things. While the present Object Naming Service (ONS) of the Internet of Things is based on top of a TLD, there is no need to base the ONS on one single root as it is the case in the DNS. Multiple roots for ONS could offer flexible governance mechanisms which would meet the special interests of the providers and users of such services. To guarantee interoperability, security and stability of this kind of services, a “federated system” could emerge where the various root operators agree on basic principle in an open, transparent and bottom up policy development process.

For other new emerging networks other governance mechanism may be developed which can take the inspiration from the WGIG definition and in particular its proposed “multistakeholder model”.

However, new governance challenges will emerge in particular when the consequences of new networks lead to new services and application which have consequences for general public policy issues like security, cybercrime, intellectual property, freedom of expression, privacy, data protection and others. The borderless nature of the Internet challenges the existing legal system which is based on the principle of national sovereignty. One and the same public policy issue are very often regulated differently in the various national jurisdictions and the level of regulatory harmonization among UN member states is low. One consequence from the evolution of the network of the future will be that governments are more challenged than ever before to broaden and deepen their intergovernmental and multistakeholder communication, coordination and cooperation to find common solutions based on a shared responsibility for what is called today the “Cybercommons”.

The complexity of the challenges was formulated by EU Commissioner Erkki Liikanen back in 2004: “It is not realistic to expect governments to take a back seat completely and leave the Internet solely to market forces. Whatever the relative merits of a government initiative might be, we will not be thanked by Internet users if any measure has the downstream effect of destabilising the Internet’s underlying architecture. The challenge for policy makers will be to find a policy approach that reinforces the Internet’s reliability without hindering its potential for further growth.” [6].

UN Secretary General Kofi Annan did put this challenge into his words: “The issues are numerous and complex. Even the definition of what mean by Internet governance is a subject
of debate. But the world has a common interest in ensuring the security and the dependability of this new medium. Equally important, we need to develop inclusive and participatory models of governance. The medium must be made accessible and responsive to the needs of all the world’s people”. And he added that “in managing, promoting and protecting (the Internet’s) presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different.” [7].

Kofi Annan’s invitation to be creative in developing governance mechanisms for the Internet is an ongoing challenge. One key point in this context is that if the technical architecture is a flat network with no single central decision making body in the center or at the top, the political architecture to deal with the network, has to mirror this reality. The proposed model of a “Multilayer Multiplayer Mechanism of Communication, Coordination and Collaboration” (MC³) reflects in the best way the challenge.

Insofar, mechanisms and networks like ICANN, the IGF or other institutions and organisations, dealing with various elements of the net, can be seen as laboratories where new forms of policy development and decision making are experimented. How far this will go what the concrete results will be and how the new mechanisms will look like remains to be seen. There is a need to intensify research on future governance of the Network. This is not a purely academic or theoretical challenge, it is a pressing practical political issue as it can be seen by efforts of the European Commission to propose new governance models both for a post JPA phase with regard to ICANN (the G 12 proposal made by EU Commissioner Vivian Reding in May 2009) [8] or for the Internet of Things (made in the EU Action Plan from June 2009) [9].

Until 2015, according to the WSIS decisions, half on mankind should be online. In 2015 we will have four billion Internet users worldwide, a mobile Internet, an Internet of Things and many other networks which allow that everybody can communicate with everybody anytime and anywhere in form of text, voice, image, video. What is going on is a technical evolution which has also to potential to change social communication and the economic process globally. Some people have called this a “silent revolution” which will change also our institutions, policies and regulatory frameworks. It has the potential to change the way how we agree on common rules and standards for our behaviour in cyberspace and how we execute these common rules and standards.
REFERENCES


