Future Internet

The Cross-ETP Vision Document

Contributors:

Editor: Dimitri Papadimitriou (Alcatel-Lucent)

Co-authors listed in alphabetical order:

Henrik Abramowicz (Ericsson), Stefan Arbanowski (Fraunhofer), Federico Alvarez (UPM), Ilias Andrikopoulos (Space Hellas), Alessandro Bassi (Hitachi), Pascal Bisson (Thales), Didier Bourse (Alcatel-Lucent), Vincent Boutroux (France Telecom), Brigitte Cardinael (France Telecom), Josema Cavanillas (ATOS Origin), Guillermo Cisneros (UPM), Jim Clarke (WIT), Pierre-Yves Danet (France Telecom), Francisco de La Iglesia (ATOS Origin), Gorry Fairhurst (University of Aberdeen), Daniel Gidoin (Thales), Guillermo Gil (Robotiker-Tecnalia), Wolfgang Gerteis (SAP), Juanjo Hierro (Telefonica), Elmar Hussmann (IBM), Hans-Peter Huth (Siemens), Paul Jenkins (BT), Terje Jensen (Telenor), Jose Jimenez (Telefonica), David Kennedy (Eurescom), Konstantions Liolis (Space Hellas), Roberto Martinez (UPM), Saverio Mascolo (Politecnico di Bari), Enrique Menduina (Telefonica), Jean-Dominique Meunier (Thomson), Werner Mohr (Nokia Siemens Networks), Andrew Oliphant (BBC), Stefano de Panfilis (Engineering), Dimitri Papadimitriou (Alcatel-Lucent), Jean-Charles Point (JCP Consult), Jorge Posada (Vicomtech), Johannes Riedl (Siemens), Jukka Salo (Nokia Siemens Networks), Michael Smirnov (Fraunhofer), Fiona Williams (Ericsson), Tanja Zseby (Fraunhofer).

Editor and co-authors acknowledge and thank the contribution and reviews of their colleagues from organizations and from ETPs.

Disclaimer: The contents of this document are the consolidated ideas of many individuals and may not be taken as the definitive opinions of any those people exclusively, their employers, or the European commission. This paper, and the opinions expressed within, should be considered as part of the emerging consensus in Europe on the opportunities for significant technical, economic and social advancement enabled by the Future Internet.

Executive Summary

The international race to invent the future of the Internet is well under way. Europe can build on its strong technological capability to position itself in the new world Internet order. Society is undergoing a paradigm shift, the evolution of the society and the Internet being now tightly interconnected. With over 1.5 billion users worldwide, the current Internet is a great success in terms of connecting people and communities and increasingly forms the support for the functioning of both economy and society. Daily life increasingly relies on the Internet in the developed world and is bringing economic development of emerging economies.

However, today's Internet was designed in the 1970s to support communication between computing systems for communities of technically expert users. The paradigm shift in society and the opportunities enabled by new technological advances in devices, place completely new requirements on the evolution of today's Internet. Future Internet will enable a multitude of new application sectors leading to the development of new markets.

Considerable effort has already been devoted to defining options and concepts which could form the basis of Future Internet to support a sustainable society. The dimensions of the Internet by and for People, the Internet of Contents, the Internet of Services and the Internet of Things supported by Network Infrastructure will form the Future Internet. European organizations, can if given the right opportunity, significantly contribute to the shaping of the Future Internet, by building notably on the strongholds of Europe as well as on a long tradition in R&D collaboration. Such a collaborative effort can bring about a greater effectiveness on R&D spending while spurring innovation and hence contributing to the Lisbon strategy for growth and jobs. Recent turmoil in the financial markets has changed the context of R&D investment for the coming decade. The potential shortage of investment finance is driving a new level of focus on return for investment. Europe must invest now to simply be at the competition edge in the coming years.

We, industrialists and academics, involved in several European Technology Platforms, have come together to devise a strategy and action plan that will make the Future Internet an industrial, economic and societal success for Europe. We strongly recommend to the EU Commission, Members States and European Parliament to actively support our efforts to make the Future Internet a reality driven by European interests.

We will act to:

- Identify achievable business models based on the current ecosystem and based on disruptions brought by the Future Internet developments,
- Develop a dynamic roadmap for the key research challenges to be tackled, and establish a road map ensuring the take-up of the research results,
- Explore different R&D evolutionary and disruptive approaches, covering classical, clean-slate, and experimentally-driven,
- Further develop the cross-domain research fertilization covered by the set of projects working together in the Future Internet Assembly.

We however call on the European Union to:

- Provide the financial resources allowing for the strengthening of the industrial/public partnerships in R&D,
- Develop appropriate multi-disciplinary teaching and life-long training programs to ensure sustainable knowledge and skills acquisition facilitating innovation,
- Develop the an integrated and structured approach between National and European R&D programs so as to overcome the current fragmentation of efforts,
- Develop and implement the so-called push-pull model: Large investment in R&D accompanied by a solid and homogenous policy of leading edge markets development and public procurements,

- Stimulate a pan-European coordinated approach on matters relating to standardization and the single market,
- Provide the means to ensure global coordination of concepts and plans for the Future Internet to address industrial perspective,
- Raise awareness of all European citizens about the clear and visible benefit of the outcome of the investment in Future Internet development.

In conclusion, we consider that a European coordinated approach to the Future Internet, will allow us to fully address the multiple technological challenges which are ahead. Turning these challenges into opportunities requires that bold steps are taken at European level. Our ambition to meet the societal needs ahead in terms of economic growth, sustainable environment and quality of life, can only be realized, if the European Union provides its full support to our vision.

Table of Content

1. Introduction

In the past 50 years, the world experienced the most important changes and evolutions in centuries. Social, economical and political development has brought the world to new paradigms of living, education and social interaction. The expansion of the Internet, worldwide network of interconnected computer networks based on the TCP/IP standard communication protocol, was driven over last 30 years by the exchange of data between hosts such as server platforms and personal computers (PCs). Today, the Internet has become essential for enabling data information flow exchanges all over the world enabling in turn a wide range of applications and services. Indeed, the concept of "computer networks" inherited from the 1970s considered only fixed networked computing machines. Today's, "computer networks" in reality comprise devices characterized by autonomous information processing capabilities, not limited to PCs, laptops, or palmtops. Networked collaborative enterprises and digital manufacturing are already a reality, and e-business is developing fast. Our societies and culture are inevitably becoming digital. Sooner or later, all human activities will evolve towards their digital era. This concerns all fields of our lives: health, transport, knowledge, culture, and more. Internet evolution has been characterized [Dutton] by the transition from "sharing" in Web1.0 (Web) to "contributing" in Web2.0 (user-generated content) to "co-creating" in Web3.0 (collaborative production, semantic Web). This has been accompanied by convergence of telephony, video/TV and other multimedia content, all now delivered via the Internet.

Internet is today the most important information exchange means that is providing to the society the mechanisms to create new forms of social, political and economical intercourse, which is now today designing the society of the 21st Century. Internet will be the key enabler for the free movement of knowledge in addition to the free movement of persons, capital, services and goods [EC140308]. As such the Internet plays a crucial role in the ability of humans to communicate but at the same time opens new challenging problems. As the current Internet grows beyond its original expectations (a result of increasing demand for performance, availability, security, and reliability) and beyond its original design objectives, it progressively reaches a set of fundamental technological limits and is impacted by operational limitations imposed by its architecture.

To address the Future Internet and its related challenges, ICT ETPs (eMobility, NEM, NESSi, ISI, and EPOSS) have set up a common workgroup (Cross-ETPs Future Internet) with the objective to define a vision and provide recommendations to the European research for the following 10 years. The 5 ETPs represent most of the European and European-based organizations (more than 1000 members: Manufacturers, Operators, SMEs, Academics) and bring competencies on networks, devices, content and services which embrace most of the aspects of the Future Internet. The work has been organized around 3 main aspects: definition of the vision and the ambition, identification of the key research challenges and finally description of the research topics that future projects need to address in order to achieve the overall goal.

The aim of this vision document is to draw the attention of decision makers, of the utmost importance for Europe to actively drive the global definition of the Future Internet. Section 2 explains the overall objectives and ambitions of the Future Internet, identifying the trends and limitation of the current Internet, then defining the high-level objectives of the Future Internet. It describes the clustered approach proposed by the workgroup, built on ***four key pillars*** (the Internet by and for People, the Internet of Contents and Knowledge, the Internet of Services and the Internet of Things) and the foundation (Network Infrastructure). These pillars are under-pinned by a common foundation of ***Future Internet networking technology***. The key technological challenges are summarized in this section, additional details being available in the "Technological Challenges – Working Document", to be further broken down inside the Strategic Research Agenda (SRA)[1].

[1] First draft version of the SRA will be made available during December 2008.

Section 3 identifies the key opportunities for Europe, and the impacts on ethical, societal, legal, regulatory, standardization, operational, industrial, economical and environmental domains. Finally, Section 4 exposes the ambitions that the Cross-ETPs workgroup pursues and the proposed recommendations to be taken into account for a successful definition of the Future Internet outlined in the "Architectural Vision - Working document".

2. Overall Objectives and Ambitions

This section describes the overall objectives and ambitions underlying the trend towards the Future Internet.

2.1 Trends and Motivations

The growth of the communication infrastructure in Europe and globally has resulted in a significant impact on business processes, and quality of life. The Internet has become the core communication environment not only for business relations but also for social and human interaction. As such the Internet plays a crucial role in the ability of humans to communicate but at the same time opens new challenging problems. Indeed, as the current Internet grows beyond its original expectations (resulting from an increasing demand for performance, availability, and reliability) and beyond its original design objectives, it progressively reaches some of fundamental technological limits and is impacted by operational limitations imposed by its architecture.

Fifteen years ago nobody would have envisaged the Internet as it is today as well as its various applications. Some remarkable cases can be outlined such as i) the Web, which processes 100 billion clicks per day and offers 55 trillion links between Web pages, ii) the exchange of 2 million of emails per second and iii) instance messengers with 1 million instant messages per second. Also, there is a growing penetration of Internet connectivity in terms of geographical size and the number of connected users and the fact that users go from occasionally connected to always connected, the Internet infrastructure is also growing in geographical distribution, number of network elements and heterogeneity of physical connectivity (optical fiber, twisted pair, co-axial cable, wireless, etc.). It is expected that, by 2011, about 3 billion hosts (devices that use the communications infrastructure including mobile and other type of handheld devices) will be connected to the Internet from the 570M of hosts connected in July 2008. In addition, the Internet traffic is expected to grow by a factor of 3-3.5 (see Figure 1) compared to 2007[2]. ***The key point from this perspective is whether the use of the Internet as a common communication infrastructure*** for computing systems, but also for any other device that will be equipped with an networking communication stack, ***will impart or not a serious motion departure to these growth curves***. Concerning the traffic growths estimation, it remains to be seen how much additional traffic would really result from this trend. Early assessment (see Figure 1) shows that most of the traffic increase would be generated by the generalization of the exchange of digital media content over the Internet. Another factor showing the growth of the Internet is the increasing number of Autonomous Systems (AS) in particular at the periphery of the Internet that are also the source of most of the instabilities in the current routing system.

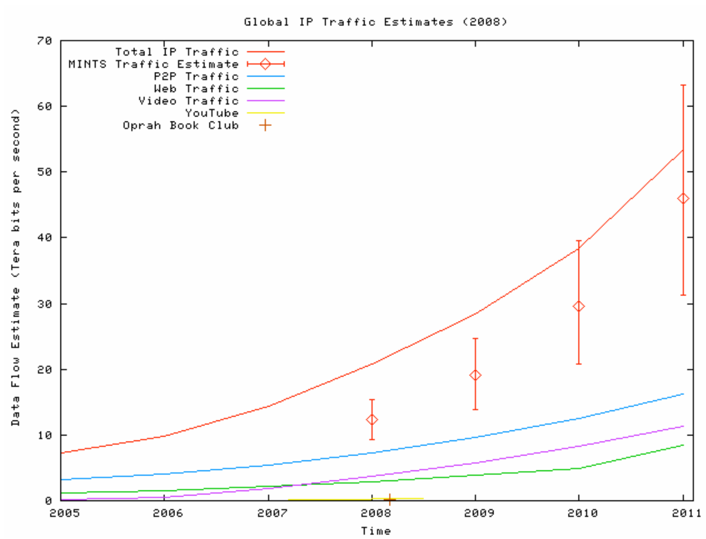
Today, with over 1.5 billion users worldwide[3], the current Internet is a great success in terms of connecting people and communities. However, today's Internet was designed in the 1970s for purposes quite unlike today's heterogeneous application needs and user expectations. Though the Internet infrastructure has evolved with changing applications, its underlying architecture has to

---

[2] Traffic growth rates is driven by the empirical Nielsen law: 50% access bandwidth increase per year, traffic growth resulting from the Minnesota Internet Traffic Studies (MINTS) also show an average growth rate ranging between 50-60%).

[3] The ratio between the number of users and the number of hosts is about 3.

date slowly evolved. This underlying architecture was not created to function as a global critical infrastructure, and it has a number of fundamental limitations. Moreover, the piecemeal growth and addition of functionality has created a set of structural anomalies. Today's Internet works - but 'only just' - whereas tomorrow's applications will attract more users to new applications needing greater mobility, security, wider bandwidth, and enhanced interactivity.



Source: AmericaFree.TV LLC, March 2008

Fig.1. Forecasted Traffic Growth to 2011

The Internet architecture has been successful so far in allowing a worldwide scale global internetwork, being an heterogeneous collection of interconnected systems that can be used for communication of many different types between any interested parties connected to it. However, as detailed in the "Technological Challenges - Working document", the Internet architecture is progressively ***losing its original simplicity and transparency.*** One of the main cause is the emergence of new classes of applications, additional operational and management requirements, variety of business models, security mechanisms and scalability enablers that give rise to point solutions that extend the architecture without regard to the original key design principles. While it is necessary to operate the Internet under current economical, technical and social conditions, the combination of these mechanisms has significantly reduced the potential for incremental evolution of the Internet architecture. This loss of flexibility is already being felt as the number of Internet nodes grows another order of magnitude. Indeed, the Internet nowadays size and scope render the deployment of new network technologies difficult while experiencing increasing demand in terms of connectivity and capacity.

Even though the current Internet continues to work and is capable of fulfilling its current missions, it also suffers from a relative “ossification”, a condition where technological innovation meets natural resistance, as exemplified by the lack of wide deployment of technologies such as multicast or Internet Protocol version 6 (IPv6). As a result of the Internet growth and the increasing communication requirements, many ***piece-meal solutions have been progressively developed and deployed*** to allow the Internet to cope with the increasing demand in terms of user connectivity and capacity. Examples are firewalls to cope with end-user/site security and NAT to cope with the exhaustion of IPv4 address space. There is, however, a growing consensus among the scientific and technical community that the methodology of continuously “patching” the Internet technology will not be able to sustain its continuing growth and cope with it at an acceptable cost and speed. Thus, something has to change.

Although the design principles of the Internet remain valuable, there also is growing evidence that the current architecture and resulting components, as defined today, face certain objective limits (in particular, in terms of security an scalability). Indeed, with an increasing reliance on the Internet infrastructure for economic and social activities the impact of network-wide threat in the form of worms or viruses is also increasing. Improving the security and accountability of the Internet is thus of the utmost importance. On the other hand, certain objectives of the Internet are not sufficiently addressed to cope with the users' new expectations and behaviors (in particular, in terms of availability and reliability). In other terms, the ***current Internet architecture is progressively reaching a saturation point in meeting increasing user's expectations and behaviors as well as progressively showing inability to efficiently respond to new technological challenges*** *(in terms of security, scalability, mobility, availability, and manageability)* ***but also socio-economical challenges***.

Even worse, misguided attempts over recent years to sustain the Internet growth lead to the ***erosion of the end-to-end principle*** that has resulted in decreasing the availability, deteriorating the robustness, as well as reducing the scalability of the Internet. Moreover, this erosion combined with the Internet infrastructure growth makes its manageability and configurability increasingly complex. It is thus expected that the operating cost of the Internet technology will start to increase more than proportionally to the number of nodes resulting from a) the additional patches that will have to be developed, deployed and operated, b) the growth of the infrastructure (in terms of number of autonomous systems, routers and routes), c) the increase in both the number of connected users and their activity (in terms of time, location and traffic) and d) the heterogeneity in application needs. This results in an increasing complexity and decreasing maintainability of user's satisfaction while keeping an openly accessible, neutral, and generic Internet infrastructure. In addition to underlying architectural limitations of the infrastructure itself, the way services are offered today to citizens suffers clear limitations on their overall adaptability to context where this includes devices, situations, cultures and time. These demands will put the overall architecture from the underlying infrastructure up to the offering to citizens under greater stress. We need a more trustable (secure, dependable, and reliable), flexible, evolvable, and scalable Internet. If we do nothing, standards of service for today's applications may decline substantially. And future applications that would benefit Europe's economy and enhance the lives of its citizens will be limited by today's technology.

2.2 High Level Objectives and Ambitions

The Future Internet should offer all users a secure, efficient, trusted and reliable environment. In turn, this environment, should allow open, dynamic and decentralized access to the network connectivity service and information, as well as being scalable, flexible and adapt its performance to the user needs and context.

We firmly believe that an extensive research on Future Internet can only be effective if we follow an holistic approach where all the components and challenges are addressed in a synchronized way. According to this holistic principle the development of Future Internet needs to address the following high-level main objectives:

1. *To accommodate unanticipated user expectations together with its continuous empowerment.*
2. *To become the common and global information exchange of human knowledge.*
3. *To leverage and evolve information and communication technologies and capabilities and services to fulfill increased quantity and quality of Internet use (considering the requirements from an increasingly heterogeneous set of applications such as, e.g., manufacturing, multimedia, healthcare, and power distribution).*

4. *To be scalable to provide cultural, scientific and technological exchange among different regions and cultures, and within single communities.*
5. *To be ubiquitously accessible (from physical, to connectivity and informational level), and open.*
6. *To be secure, accountable, and reliable without impeding user privacy, dignity, and self-arbitration.*
7. *To support mobility, have widespread ubiquitous coverage, and be capable of assisting society in emergency situations.*
8. *To support means for various performance adaptability features based on context, content, etc.*
9. *To support the innovative business models that are emerging (and may emerge in the future) to allow for more entities (including businesses, SMEs, and individuals) to be involved in providing any particular instance of a service.*
10. *To be carbon neutral and energetically sustainable.*

In the Future Internet, access to the network will be made available ubiquitously and connectivity will become a fundamental service that communities use and rely upon. Currently, access to the Internet is mainly based on DSL (Digital Subscriber Line) connections and coaxial cable/Hybrid Fiber Coax (HFC). Further technologies in the access network will also include optical fiber connections up to close to the last mile, terrestrial radio technologies (cellular mobile communications, broadband wireless access) but also satellite communications (extending coverage, and decreasing time to deploy services). The transmission technologies and access networks will increasingly be designed and deployed for horizontal integration and service-agnostic platforms, as addressed under the "technology neutrality" paradigm where services can be provided through different networks and different technologies, that can ultimately be carried flexibly in the spectrum when wireless. This is one the major precondition for consistent network architecture resulting in a reduction of Opex and Capex. Resulting from the cost reduction and ease of access to knowledge shall in turn allow the creation of new markets and new labor expectations where coopetition[4] will shift toward a model where small businesses and even individual professionals can compete with greater equality in large markets.

It is important that the Future Internet is ***designed to accommodate conflicting interests*** (the so called "tussle networking" introduced D.Clark) such as conflicting policies, traffic patterns and compensation modes. It is fundamental to recognize the powerful capability of the current Internet to accommodate new applications developed by an increasing user community. It is thus essential to keep the entry barrier as low as possible and design the Future Internet so as to allow and steer open and innovative application development without impeding the Internet genericity, evolvability, openness and accessibility. The Future Internet shall thus cultivate the opportunity for new players to take benefit of the infrastructure foundation but also the pillars of the Future Internet without sacrificing on its global architecture objectives and principles. Moreover, additions and extensions to the network architecture should be facilitated without rigorous standardization processes but also without replacement of the infrastructure equipment. Also, the Future Internet should be able to accommodate and sustain evolvability of its stakeholder (see Section 3) needs in terms of e.g. forwarding and processing capacity.

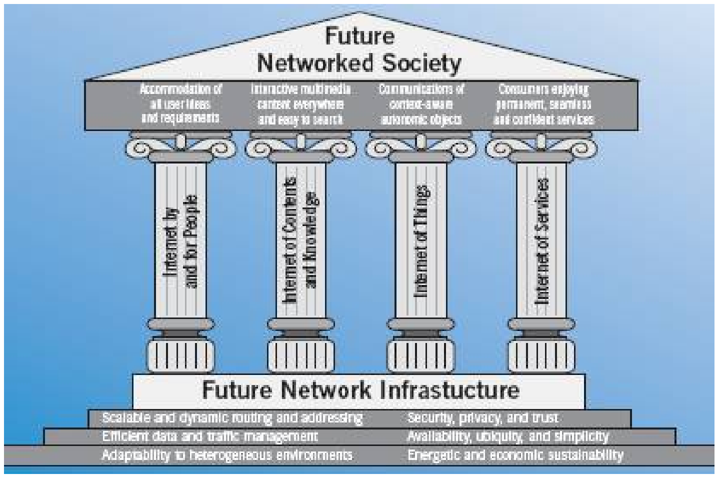
2.3 Future Internet Pillars and Foundation

The main vectors of growth of the Future Internet referred to as pillars are: (1) Internet by and for people, (2) Internet of Contents and Knowledge, (3) Internet of Things and (4) Internet of Services. These pillars are supported by the Network infrastructure foundation as depicted in Figure 2. To

[4] the result of competing antagonistic actions by parties implicitly cooperating but whose global return is negative.

support and sustain growth of these pillars, the Network infrastructure foundation must itself be the object of specific research resulting from large set of technological challenges associated to the network infrastructure (see Section 2.4 and Section 1 of Working Document: Technological Challenges).

This document also recognizes the existence of generic technological challenges such as security and accountability covering all pillars and network infrastructure foundation. The following sub-sections are detailing each pillar, and network infrastructure foundation.



Fig,2. Future Internet Overview

2.3.1 Internet by and for People

By breaking the digital divide, the future Internet should be able to interconnect growing population over time. The FI shall be capable to meet new and common people (Internet users) expectations and needs while promoting their continuous empowerment, preserving their self-arbitration (control over their online activities) and sustaining free exchanges of ideas. The FI shall also provide the means to i) facilitate everyday life of people, communities and organizations, ii) allow the creation of any type of business regardless of their size, domain and technology, and iii) break the barriers/boundaries between information producer and information consumer. The latter will foster the emergence of prosumers: people/communities will be part of the creative flow of content and process, and not just consumers. Indeed, content creation no longer requires professional expertise and content submission has been tremendously facilitated by a broad variety of tools which enable users to create high-quality content within minutes and at almost no expense. Distributed knowledge can thus be shared easily and opinions can be made public in almost real-time. Complemented with Social Networks, which allows establishing and maintaining personal networks beyond any frontier, humankind is offered an unprecedented level of interactivity. This trend combined with the evolution of the Web has induced a new phenomenon: formation of virtual communities and access to their wisdom that allows users to become part of the application development life cycle. In Web 3.0, semantic technologies, knowledge exchange, processing and generation by machines are substantial for the Future Internet. Such intelligent methods for knowledge collection processing and presentation is mandatory for being able to handle and benefit from the huge amount of information being available now or in future. This immediately leads to the second pillar, the Internet of Contents and Knowledge.

2.3.2 Internet of Contents and Knowledge

With the evolving role(s) of digital communication, a cognitive society goes beyond information and content accumulation and consumerism by involving conscious intellectual activity (as thinking, learning, reasoning, or remembering). For this purpose, the Internet should support mechanisms for knowledge dissemination both at local and global level. In this perspective, the way of managing the networked knowledge needs to be revised to meet user expectations. Knowledge and culture must be diffused worldwide to breakdown barriers and to promote dissemination and learning.

In practice, this means that in order to achieve real social progress, the Future Internet shall provide beyond information access, adequate processing means and involve conscious intellectual activity. As digitalization of data progresses, it is now expected that the majority of new media will arrive in digital form, with the analogue form being the exception. For instance, digital videos will not only increase in number, but also in size, due to increases in resolution and the ease of creation and manipulation. The increase of number of digital videos and their distribution over increasing number of locations creates the need for specific multimedia search engines. Progress in network multimedia communication is also leading to 3D videos. Several means with which to easily share these news forms of digital media continue to appear (YouTube for asynchronous video content being one of the well known pioneers in this space). Digital TV channels are also progressively penetrating the Internet space, Zattoo and Joost, for real time/streaming video content being pioneers in this space.

Web evolution to Web 3.0, will introduce cognitive intelligence, enabling Web applications not only to provide but also to intelligently process information. Semantically tagged information is the foundation for this new form of intelligent capabilities: deriving knowledge from mere information and making knowledge accessible for humans and machines including the objects of the Internet of Things. The general capabilities of semantic descriptions also cover functional and none-functional properties of services. The Future Internet will not only support intelligent content and provide tools for processing information intelligently; it will probably most importantly render it intelligibly (have it easy understood and accessible by human beings).

2.3.3 Internet of Things

The expression “Internet of Things” (IoT) recalls scenarios from science fiction, where objects will become “living beings” and have identifiable behaviors and actions. In the foreseeable future, we can expect that any object will have a unique way of identification; not only, as today, computers, printers, actuators, mobile phones, but literally any thing around us, anywhere, at any time, creating an universally addressable continuum. Having the capacity of addressing each other and verifying their identities, all these objects will be able to exchange and, if necessary, actively process information according to predefined schemes, which may or may not be deterministic. In the definition of “Internet of Things”, the term “Thing” refers to “an object not precisely identifiable". Hence, the “Internet of Things” can be defined as “a world-wide network of uniquely addressable and interconnected objects, based on standard communication protocols”.

While the current Internet is a collection of rather uniform devices, though heterogeneous in some capabilities but very similar for what concerns purpose and properties, it is to be expected that the IoT will exhibit a much higher level of heterogeneity, as objects of totally different in terms of functionality, technology and application fields will belong to the same communication environment. Semantics of messages will also play a central role: not all objects will have “something to say” to other objects. As the communication means will be the same, novel protocols based on the semantic of the language must be developed, if the IoT will have to scale to the zillions of objects around us.

Already today, the variety of devices equipped with Internet access ranges from items like vehicles, home appliances over consumer goods to any type of industrial machinery. The sheer ubiquity of these devices will create a whole set of novel applications where for instance sensors and Radio-frequency Identification (RFID) playing a central role. As far as our knowledge goes, the combination of RFID and sensors enables a cost-effective and robust system of item identification and context awareness, changing the current Internet usage completely from a request-and-retrieve to a push-and-process paradigm.

Dynamic business processes can be digitally seized and autonomously controlled by embedding "smart objects" which establish communication on demand in order to execute coordinated activities. Complex industrial control tasks can be realized like the operation of the future power grid satisfying all its decentralized aspects, or the control of advanced manufacturing coping with its extremely sophisticated logistical processes. New innovative applications will emerge from this social and technological context exploiting the connectivity and accessibility of everything. Some can easily be identified: there will be intelligent buildings, robots, cars, and cities facilitating and assisting our daily lives and thereby increasing our quality of life; social networks will deepen and transcend physical boundaries, and global communities will emerge; medicine can make giant step forward, by giving the possibilities of more precise, personalized, pro-active health care. Smart fabric will sense our body temperature and humidity, not only allowing an interaction with the air conditioning system to have the highest possible comfort, but also being able to detect early the insurgence of illnesses, such as flu. Smart books will interact with the entertainment module, creating a multi-dimensional, multimedia hypertext: while reading a page, the monitor will show more information on the topic we are reading in real time.

Moreover, humans can integrate seamlessly into such a smart environment and become active part in the definition of their instantaneous context, which, for example, closes the digital patient-physician loop enabling novel applications in the future healthcare industry (including ageing). Finally, any object connected either offers a service or requires the existence of one or many services. Hence, there is a natural and close relation to the other novel view of the Future Internet, the Internet of Services.

2.3.4 Internet of Services

The term Internet of Services is an umbrella term to describe several interacting phenomena that will shape the future of how services are provided and operated on the Internet. The Internet of Services also comprises the various sets of Internet Applications including pervasive/immersive/ ambient, industrial/manufacturing, vehicular/logistics, financial/ePayment/eBusiness, power network control/eEnergy, eHealth, and eGovernment applications.

Three major domains of development are the emergence of Internet-scale service oriented computing, the contextualized and proactive services and service orchestration.

The emergence of *Internet-scale service oriented computing*: Service oriented computing has gained increasing attention in recent years as the next evolutionary step after component-based software. Translated towards the Internet, it is has the potential to radically change the way Internet applications are engineered, executed and maintained. Also, it may lead to new categories of applications. An important concept in that context is that of "loose coupling". Whereas electronic interaction in the Internet is mostly based on the use of tight properties – like IP addresses of physical machines or data sources – a service-oriented Internet would allow the access to complex physical compute resources, data or software functionality in the form of services. Consider as one example the "cloud-computing" approach to infrastructure services, where large-scale data centers provide virtual execution environments as Internet services with the same functionalities to physical machines but far greater flexibility and scalability. The analogy of a "cloud" is based on the effect that the user doesn't need to worry where tasks are currently executed or where data is currently physically located – it is just "somewhere in the cloud" with the precise functionality of a 24h fully scalable data center.

Contextualized, proactive, and personalized access to services: The Internet of Services will allow proactive and not only reactive services as currently enabled on today's Internet. At the same time, it will empower people to personalize their experience. A number of key concepts underlie this. The fist key concept is "context-awareness" meaning that interaction will become fully personalized and suited to the context in its widest meaning (including user preferences, usage history or the social networks users belong to and the delivery context, which in turn comprises access device description, location and time). This links to the technical possibilities of "loose coupling", as services can be flexibly detected and invoked based e.g. on semantically rich inference rules relying on properties describing context. Another key concept is "seamless" meaning that interaction covers a much broader and interoperating variety of user interface service types, which span diverse/heterogeneous networks, organizations and computing platforms/devices. In this new context, users would be able, for instance, to dynamically select the most appropriate mode of interaction for their current needs, while enabling developers to provide an effective user interface for whichever modes the user selects. This is possible, as functions of a user interface may also be decoupled from underlying services e.g. a service that provides a certain type of information. For instance, multi-modal interaction offers usability benefits over unimodal interaction when hands free operation is needed, for mobile devices with limited keypads, and for controlling other devices when a traditional desktop computer is unavailable. Users could also interactively provide input via speech, handwriting, and keystrokes, with output presented via displays, pre-recorded and synthetic speech, audio, and so on. A translation service might be coupled to an information service etc. Two last key concepts also belong to this area, which are both related to some of the main principles in Web 2.0 than will be imported to the applications/services space, namely "end user empowerment" and "collaboration". With the first one we refer to the fact that it will be more easy for users to design their own orchestration of services as well as to configure their own service front-end web access to services by means of self-servicing and mashing up service front-end resources published in catalogues/stores available on the Internet. With the second we refer to the ability of users to share their knowledge (e.g., by collaboratively tagging service front-end resources) or export the applications/services they design (e.g., by exporting mash-ups or service orchestration scripts) therefore becoming actual prosumers.

Service orchestration and the rise of core services: Already in the current Internet we are using some core services – such as search engines. Others, e.g., to provide geo-information, people search or social networking have seen tremendous growth in recent years. Mostly we are using these services in isolation from each other, e.g., via independent websites and user interfaces. Some services – like search – are starting to become integrated but here a significant increase can be expected. This is even more the case in business scenarios where complex services from different providers are combined, e.g., to link the management of customer data to advanced data mining, geo-economic information, sales reporting, and life market trends. As a consequence of this stronger linkage of services, some services will become fundamental and shared by many derived services. The Internet of Services will therefore emerge in several layers of services, from fundamental infrastructure services – like those provided by clouds to specific, data-, information-, application-like and user interfacing services.

Despite the strong interactivity of services – the business landscape of the Internet of Services will be heterogeneous. Some services will be highly specialized and probably be provided by SME type of companies. Others will address fundamental service needs and relate to significant business opportunities. The emergence of the multi-layered Internet of Services holds therefore the potential to re-shape fundamentally the Internet business landscape. The enormous investments that companies like Google are making into test-driving new Internet services provide an early indicator of the strategic importance of the Internet of Service for the ICT industry.

2.3.5 Infrastructure Foundation

To reach the architectural vision detailed in Section 1 of the Working Document "Future Internet - Architectural Vision", there are a core set of technological challenges ahead that needs to be addressed. These challenges are specific to the network infrastructure/substrate (referred to as foundation) such that it supports the pillars (outlined in Sections 2.3.1 to 2.3.4) and sustains the resulting capacity and performance requirements that Future Internet will have to provide. It is expected that by meeting these challenges, no application making use of the Future Internet will be badly influenced by some - currently - missing capacities. Based on the pure data forwarding, i.e., connectivity service provided by the communication infrastructure, various kinds of advanced network services will be established.

The main domains of improvement for the network infrastructure relate to its ***functionality*** (in particular, in terms of accountability, security/privacy/trust, manageability and diagnosability, availability, as well as mobility) and its ***architectural properties*** (in particular the flexibility, evolvability. resiliency/survivability, and routing system scalability), We acknowledge that such improvements requires in-depth investigation of the underlying Internet design principles and components.

The main drivers here are the use of the ***Internet as a common infrastructure*** for interconnecting more than computing machines e.g. sensor networks will push connectivity needs that have now reached the limit of the original design. Indeed, IPv4 addressing is running out of space (predictions shows today this may happen as early as 2011), notably showing that the original design estimates of but most notably the number of devices that would connect to the Internet has been exceeded many times over. Mobile devices have outnumbered fixed devices such as PCs with an expectation to have about 3 billion devices in less than 5 to 7 years. A further increase in the number of devices will come through the developments in wearable, in sensors, and also in the fact that each person will likely own more than one of such device in the future.

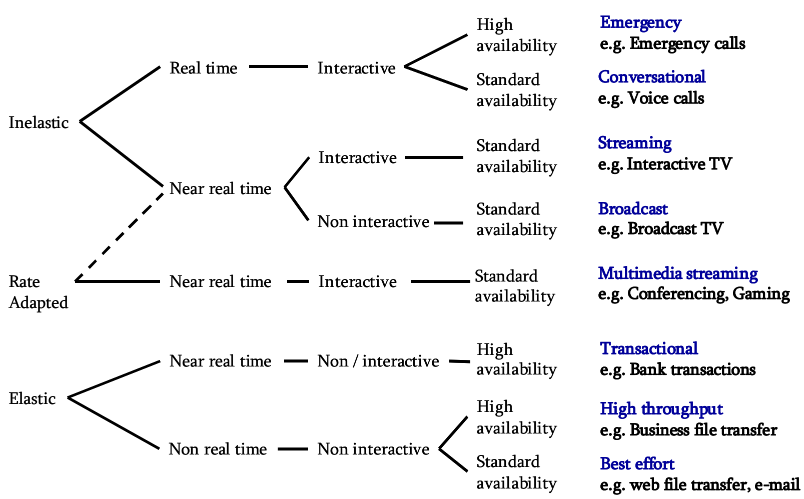


Fig.3. Future Internet Traffic Properties

While the focus of today's Internet is mainly on elastic traffic (e.g. HTTP applications), bulk data transfers (e.g. peer-to-peer applications) and multimedia streaming (e.g. Internet TV, gaming), it is also expected that new applications will demand for new capabilities from the networks - see Fig.3. For instance, strict real-time communication, and reliable connectivity with no information loss during failure scenarios are examples of high interest especially for industrial applications. These place new demands on the network and transport layers requiring new approaches and designs.

In addition, an increase in the traffic volume from direct so-called machine-to-machine communication is expected to further fuel the need for connectivity and bandwidth as well as to change the pattern of traffic in the Internet. Technologies such as RFID will push this limit (for example, because of the need for mobile readers) even further. Using IPv6 addresses for RFID numbering could accelerate could accelerate the transition away from IPv4. Moreover, the Internet user should have the possibility, at the same time, as information consumer and information producer in order to make the Internet a real opportunity to increase business and commerce. It is therefore fundamental that the Internet is being designed able to support a range of different business models so as to cope with conflicting interests such as conflicting policies, traffic patterns and compensation modes.

2.3.6 Evolutionary vs Clean-Slate Approach

A significant effort in R&D will be required to address the different challenges detailed in the Technological Challenges – Working Document. The research approach will encompass both evolutionary and revolutionary paths. Evolutionary approach builds on the evolution of the current existing Internet to conceive pragmatic and viable solutions for commercial rollout. Revolutionary approach starts from a clean slate to eliminate legacy Internet design constraints (these pre-assumes these can be identified). Both approaches target the same usage vision and will have to be synchronized on phased agendas.

There is a need to separate clean slate research from clean slate deployment. Clean slate research is important in order to pursue research that is unbiased, not taking into account preconditions of the current Internet - a way of thinking out of the box! The research results will however, have to be applied to the current Internet, if commercially viable, and a migration approach will have to be devised. Clean slate research is not the same as clean slate deployment. We should expect a number of results that should be possible to apply to the current Internet, and we need to ensure that this is coordinated and compliment the continued evolution of the Internet.

It is assumed that since the current Internet has grown to become so large (about 1.5 billions users currently and still rapidly growing), it will be commercially and operationally very difficult to replace the entire Internet in “a clean slate deployment”. Instead, clean-state research results is expected to feed the evolution of the Internet but even then there are several possible trajectories for the development of Internet, among which:

i) *By incremental evolution*: evolve the current Internet architecture by incremental evolution by adding (or removing) functionality without changing the prevailing design principles and model. This is the approach that has been followed so far to evolve the Internet and mostly reactively.

ii) *By applying virtualization*: either by enabling logically independent networks built on a common physical infrastructure for deploying new network functionalities and protocols but also providing specialized networks or by building overlays (or underlay techniques) running new protocols on top of (or below) TCP/IP. Nevertheless, there is no proof so far that virtualization (relying on the indirection principle) is resolving any of the FI technological challenges. Indeed, as enounced by D.Wheeler, "*Any problem in computer* *science can be solved with another layer of indirection. But that usually will create another problem.*". In the present cases, there is no definitive answer concerning negative impact that would result from the introduction of this new level of indirection.

While it is clear that clean-slate concepts need to be pursued, it is likewise clear that evolution of the technology need to be addressed with increased rigor. It thus remains to be seen how far following these trajectories would address the FI challenges.

2.4 Key Technological Challenges

The fundamental technological challenge for the Future Internet is to be able to tackle the question on ***where to place the additional capabilities including intelligence and processing capacity and at which level to realize them*** – as driven by cost/performance and cost/gain ratio and taking into account end-user utility function –. This is the most fundamental effect of the diversity and heterogeneity of needs and interests. Indeed, the Future Internet should lead to a tangible win-win situation for stakeholders ranging from software/ equipment vendors to service providers.

From the technological perspective, most recent innovations in the networking domain i) are not intrinsic to the networking space but comes from computer science and associated disciplines (examples are numerous: autonomic computing transposed into autonomic networking, abstraction transposed into virtualization, etc.) but also solid state physics/electronic and electricity/radio, and ii) are developed and deployed at the edge of the Internet infrastructure even if recent advances in the host network stack such as Host Identity (e.g. HIP) and multi-homing (e,g, SHIM6) to name a few are also subject to the same deployability constraints as other core networking advances. Also investing in core technologies of the Internet is and shall remain a strategic objective to sustain fundamental advances in the space of core Internet technologies.

Key technological challenges (associated to the Future Internet) have been identified and are listed here below with the objective to drive/orient stakeholders R&D so that their investment can position them as actors for their resolution. We recognize that addressing these challenges must involve a larger and broader set of the multi-disciplinary scientific and technical community due to their inherent complexity and exigent nature. The challenges identified so far cover i) cross-pillar challenges (referred to as cross-cutting challenges), ii) network foundation challenges, and iii) generic challenges for the Future Internet. Note that no claim is made here that this list is exhaustive. For each of these challenges, pointers to the "Technological Challenges" Working document (TC-WD) are provided. We also identified per pillar, a key specific challenge.

1. Routing and addressing scalability and dynamics

- Network foundation specific challenge.
- This challenge is detailed in TC-WD Section 1.5.

2. Resource (forwarding, processing, and storage) and data/traffic manageability and diagnosability

- Network foundation specific challenge.
- This challenge is detailed in TC-WD Section 1.3.

3. Security, privacy, trust, and accountability

- Generic challenge (security built-in at design time).
- This challenge is detailed in TC-WD Section 1.1, and 1.2.

4. Availability, ubiquity, and simplicity

- Cross-cutting challenge covering Network foundation as well as Internet by and for People, Internet of Services, and Internet of Contents and Knowledge.

- This challenge is detailed in TC-WD Section 1.4, 2.1, 2.2, and 2.4.

5. Adaptability and evolvability to heterogeneous environments, content, context/situation, and application needs (vehicular, ambient/domestic, industrial, etc.)
- Cross-cutting challenge covering Network foundation as well as Internet by and for People, Internet of Services, Internet of Contents and Knowledge, and Internet of Things.
- This challenge is detailed in TC-WD Section 1.4, 1.7, 2.1, 2.2, 2.3, and 2.4.

6. Operating system, application and host mobility / nomadicity
- Cross-cutting challenge covering Network foundation as well as Internet by and for People, Internet of Contents and Knowledge, and Internet of Services,.
- This challenge is detailed in TC-WD Section 1.6, 2.1, 2.2, and 2.4.

7. Energetic and economic sustainability
- Generic challenge with societal and economical impact.

8. Conflicting interests and dissimilar utility
- Generic challenge (intelligence at execution time) involving policing aspects.

9. Searchability/localisation, selection, composition, and adaptation
- Cross-cutting challenge covering Internet of Contents and Knowledge, and Internet of Services.
- This challenge is detailed in TC-WD Section 2.2, and 2.4.

10. Beyond digital communication: semantic (intelligibility of things and content, language, etc.), haptic, emotion, etc.
- Cross-cutting challenge covering Internet by and for People, Internet of Contents and Knowledge, Internet of Things, and Internet of Services.
- This challenge is detailed in TC-WD Section 2.1, 2.2, 2.3, and 2.4.

Pillar specific challenges:

The following challenges are specific to the pillars detailed in Section 2.3:

- **Internet by and for People:** accommodate anticipated and unanticipated people and community expectations together with their continuous empowerment, cultural acumen, and self-arbitration (by recognizing that access and use of information as well as associated processing means are common non-discriminatory universal rights).
- **Internet of Contents and Knowledge:** access by advanced search means and interact with multimedia content (e.g. 3D and virtual reality) that can be created, and manipulated by professionals and non-professionals and be distributed and shared everywhere on any terminal per needs.
- **Internet of Things:** context-aware autonomic objects able to generate automatic code and human-controlled behaviors, exploiting peer-to-peer bio-inspired communication models.
- **Internet of Services:** service "consumers" look for the ***perfect interactivity*** in context. With “perfect” we mean here ***permanent*** (i.e. interactivity that has no time limits), ***direct*** (i.e. the service consumer is only concentrated on the benefits of the service he/she is using), ***seamless*** (i.e. the interaction is performed using the “typical” devices of the context), and ***confident***.

3. Stakes and Opportunities

This section introduces the additional (non-technological) dimensions and objectives that the Future Internet shall take into account to develop the overall opportunities and reduce the specific risks.

3.1 Ethical and Societal

There is an increasing dependence of society on the Internet. On the other hand, the current Internet model is still privileging a fraction of the population (for many reasons). The Internet needs to expand to address the digital divide in developing countries. The Future Internet has also to address from the very beginning of its development the Societal and Ethical perspective to grant the basic human rights and the respect to different cultures and communities.

From a ***Societal perspective***, the future networks have to deal with equal and fair access to the Internet, facilitate social activities and assist society in emergency situations.

The coverage to access Internet shall grant equality of rights to access the network to all citizens in every country all around the world. Infrastructure and service providers shall have to commit themselves in cooperation with the countries authorities, to deploy an open worldwide access network with low cost and that provides access in regional decentralized areas. For instance, the Future Internet shall build capacities among ICT practitioners towards bridging the digital divide caused by economical factors within and between Africa, and South America, and Europe, and North America, while advocating and sustaining for paradigm shift in global development. A short-term approach may be to expand infrastructure by combining various communication means: terrestrial (wireline, wireless), satellite, etc. The Internet should be at the same time global and local. On the one hand, Internet should be global in order to improve the cultural and scientific exchanges between users belonging to different geographical areas and to reach users with the required services wherever they are in the world. On the other hand, the Internet should be local in order to address the requirements of local communities. It is clear that the Future Internet shall not discriminate users depending on their geographies. The unbalance of Internet accesses, and consequently, behavior of citizens towards Internet varies significantly depending on the service qualities. It is also crucial that new developments for Internet take into account the needs to serve devices connected to a multiplicity of access platforms (cable, over the air, satellite, etc.)

The applications running on top of the Future Internet infrastructure will support the users' and communities needs in their daily social activities. The Internet and new technologies facilitate communication between humans, but even with the explosion of new social networking tools, there remain many opportunities to improve the users' sense of belonging and community in their daily life. More generally there is a need to ease the social activities of end-users. Therefore, the Future Internet shall provide a framework that allows applications to rely on social interactions data. This leads to the requirement to be able to build dynamic networks of people around the users, in order to develop applications that help end-users to interact with each other. This encompasses developing technological supports for modeling more complicated relationships between people and developing innovative and added-value communication applications.

The Future Internet shall also be able to support emergency management and to assist society to restore situations on emergencies, crises or natural disasters. In this regard, to further guarantee ubiquitous usability to everyone and quick-to-get service, Future Internet must be easy to access and independent of specific limitations, such as the language used. This feature is particularly critical and crucial in emergency scenarios. The integration of a range of communications technologies (terrestrial and satellite) as well as sophisticated location based services allowing users to obtain critical information and request assistance based on their location appear as a superior overall solution to tackle the issue in Future Internet of global coverage and emergency management, particularly in less developed regions and rural areas. Furthermore, Future Internet shall put more emphasis to social needs and in particular to collective social needs such as service in times of crisis. For most users, on the one hand, their access to the Internet is not even designed to stay up when the power goes down, so a disaster renders the Internet useless today. On the other hand, the Internet has tremendous potential as a tool for citizen access to information, emergency notification and to provide access to emergency services. In such critical cases like disasters, emergencies or crises, the Future Internet must be a real "salvation anchor" for disrupted populations and therefore, it needs to support emergency services such as personal/human-to-human communications, emergency communications among rescue units, tracking and location information, data dissemination, etc. Taking into account the "Total Conversation" technology (voice, text and video communication at the same time and in real time), the Future Internet shall be a multimedia network able to inform citizens of a natural disaster based on their location, and able to provide reliable and trustworthy information during an emergency crisis, such as a terrorist attack. The technical framework of "emergency Internet" needs to stimulate technology development targeted to immediate restoration of a "minimum degree" of connectivity which must be rapidly deployed, robust, and resilient, demanding an alternative to the existing communication infrastructures. Supporting this sort of public-sector social requirement should be a primary goal of Future Internet.

From an ***Ethical perspective***, the Future Internet has to meet the challenge of being the true cornerstone where undeveloped countries shall set their basic pillars for the growth and development of their communities moving and transforming the society of the 21st Century towards the turning point of technological development when at last the real development of the 3rd World becomes a reality. This can only be realized with the commitment of the authorities of the major developed states, unions and federations building a true collaboration link with United Nations. The rights to freedom of speech need to be preserved, both by non-interference from Governments, and by technological means that help producers and consumers circumvent potential controls on information from third parties, insofar as the information does not represent a violation of applicable laws.

The Future Internet shall also recognize that access to that information and means to process that information are common non-discriminatory universal rights. As the universal right introduced the notion of citizenship, the information access and processing rights shall trigger the inception of Internet citizenship. This by keeping into account that means to process information has cultural / educational dependency without removing the end-user empowerment in deciding and controlling their activities. This fundamental issue of the Future Internet Society's refers to the degree to which today's Internet user will have the same "choice and control over their online activities" in the future. Vint Cerf, Chief Internet Evangelist, captured this problematic very well: *The Internet's open, neutral architecture has proven to be an enormous engine for market innovation, economic growth, social discourse, and the free flow of ideas. The remarkable success of the Internet can be traced to a few simple network principles -end-to-end design, layered architecture, and open standards -- which together give consumers choice and control over their online activities.*

3.2 Legal, Regulation, and Standardization

Internet is today and will increasingly be a critical infrastructure and is playing a dominant role for the society and the economy. New and far closer relationships are being created between the businesses, the public sector, the citizens, and the consumers, and it has a huge social and economic impact in all countries. The Future Internet will be the basis for more efficient private and public services and will improve the relationship between all stakeholders. Solutions, which empower citizens, e.g. to participate in healthcare processes remotely and facilitate remote monitoring and care allow social interaction without travel. It will also have an important role in democracy by the more direct involvement of citizens in decision making and public administration. In addition, more and more communication and information technology will be used for surveillance.

These developments show the importance of the Future Internet that public authorities want to understand and influence its operation. Therefore, the exchange and handling of information and in particular of personal and financial data has to follow national and European law and regulation in order to secure the interests of citizens. Interaction between different communities is needed to make these rules reasonable. The access to the Future Internet should be open without restrictions, e.g. by government. However, appropriate copyright techniques have to be developed. From the user perspective there should be sovereignty on their own data. This also leads to issues of preserving trust e.g. by offering trusted identification and authentication as well as to issues of privacy protection for the individual user. Again, the Internet development is too dynamic to find static solutions for these issues. It will be a major challenge from the legal perspective to ensure privacy and security of data and on the other side to keep the Future Internet an open platform for business and administrative applications, entertainment information exchange, etc.

The Future Internet calls for an "open and transparent" Governance model based on international agreements and regulations relying on a stable channel of communication and discussion between all stakeholders such as governments, the private sector (ICT industry), academics and civil society each in their respective roles. These stakeholders in the governance model will develop and grant a common set of shared principles, norms, regulations, decision-making procedures, and programs that will shape the development and use of the Future Internet. Governance of Future Internet will be beyond Internet names and addresses, issues dealt with today by the Internet Corporation for Assigned Names and Numbers (ICANN). It will include other significant public policy issues, such as critical Internet resources, security and safety, and developmental aspects and issues pertaining to the use of the Internet.

The Future Internet is also increasingly determined by critical resources and core services related to the DNS but also more complex services – e.g. to provide digital identities or to access cloud-style remote computing power, storage or long-term data preservation. Guaranteeing open access and stability of these critical resources and core services will also be high on the agenda of governing bodies and regulators. An equally important aspect, the Future Internet is determined by participation. It offers new ways of social interaction and can lead to new forms of virtual public spaces – e.g. in the form of 3D worlds. Increasingly, mass collaboration and social interaction become a defining element of the Future Internet. In the same way as physical public spaces are open and freely accessible – the Internet will therefore increasingly see virtual spaces where non-discriminatory access and possibility for participation need to be guaranteed. Discussions on these issues should be opened by the Governments and must include the contribution and support of the private sector, ICT industry, Academics and Civil Society each in their respective roles to develop and grant a common set of shared principles, norms, regulations, decision-making procedures, and programs that can shape the development and use of the Future Internet.

Coordinated international standards in the emerging areas of the Future Internet will be essential to guarantee its interoperability and its openness as an innovation space. These standards are crucial for the success of the Future Internet in terms of its development, maintenance and implementation by third parties (to quote the definition of the European Commission's European Interoperability Framework). It would be desirable to organize the standardization of Future Internet in a less fragmented manner compared to the today's standardization landscape (global e.g. IETF, ITU, and regional e.g. ETSI, ANSI) to address the technical challenges more efficiently and to ensure interoperability. Efficiency and interoperability of each segment are main challenges, which requires coordinated international standard. These standards are mainly related to the foundation of the network infrastructure. However, it needs to be recognized that many new Internet relevant technologies – e.g. relating to new content formats, device- or services interoperation – are created outside of standardization organizations – even outside of industrial organizations like W3C. Also the innovation mechanisms of the Internet demand the parallel emergence of competing technologies in early stages. Some of these developments may lead to "de facto" standards (like in RFID / EPC technology), which needs to be coordinated with International standards to ensure interoperability. In this context, mechanisms towards incorporating innovation into the Internet space and Open Source will be found as well. Open source may be a powerful tool (in addition to other innovations) to support Future Internet standards. It can also well co-exist with proprietary software and services. In addition to the standard technologies that shape the Internet, the Future Internet will further boost the possibilities for deploying new applications and services. Many of them will be using sensitive and personal information, but in-turn may offer diverse possibilities for misuse.

3.3 Operational

The concept of the operational community (providers of all kinds) is changing. The current Internet architecture was developed on the assumption that there is a single provider of communication services and infrastructure. Over time the Internet technology has developed to allow for multiple organizations to provide the parts of the infrastructure in collaboration, and recently there has been the emergence of service providers that utilize the physical infrastructure without owning any of it. However, the current business models assume that the service provider is monolithic and that information is free. With the advent of the Internet of Services and the Internet of Things it will no longer be possible to think of a single provider of a service. Services in the Future Internet will be delivered by the orchestrated actions of a number of service and data providers at the point of delivery. As a result the need for the Future Internet to address new operational models "incontournable". The operational model required to address i) increasing demand for performance, availability, and reliability, ii) new classes of applications, iii) new models for delivering services from multiple actors and the resulting business models, iv) management requirements themselves resulting from required security mechanisms and scalability enablers give rise currently to point solutions that extend the architecture without regard to the original key design principles. This results in complexity that is currently impacting the evolution of the Internet itself. For instance, operators are spending ever more effort to mitigate effects of IPv4 address space depletion, bandwidth increase and its increasing unfair share and the limitations of current inter-domain routing protocols (note: we argue here that some of these constricting operational limitations are imposed by the current Internet architecture itself).

The Future Internet will ensure that the operational complexity and cost do not increase linearly with the number of nodes composing the network, the number of hosts/devices attached to the network, the number of service provides using the network, or the amount of data being transferred by it. Distributed architectures can control and mitigate the increase of complexity as they allow expanding the network capabilities without replacing or upgrading existing nodes (thus not increasing costs) and providing intelligence and direct access to user terminals. Furthermore, mesh connectivity patterns may help control and mitigate the increase of complexity and cost.

Many operational aspects will be addressed on the Future Internet research initiatives to provide a real openly accessible, dynamic and secure network that provides anywhere and anytime multi-device access. The relationship between requirements and operational and architectural models is not a simple issue to solve. Although the main requirements of the network arise from non-technical topics from the real world – e.g., business models, regulatory models, and politics – other requirements are themselves the result of previous technical decisions, i.e., depend upon the architecture itself. As a consequence, a design of a new operational model cannot be completely performed top-down. There is not likely to be a unique answer for every requirement, and every requirement has some cost. The cost of a certain requirement may become clear only after examination of the operational consequences of meeting that objective, in conjunction with the other objectives. It therefore involves an interactive process, in which requirements can be re-examined and perhaps promoted or demoted during the early steps of research.

Finally, since Future Internet needs to be seen as a "global interconnection network", it needs to remain operational in the cases of disasters, emergencies or crises, as well. In such critical cases, Future Internet must be a real "salvation anchor" for disrupted populations and therefore, it needs to support emergency services such as personal/human-to-human communications, emergency communications among rescue units, tracking and location information, data dissemination, etc. The technical framework of "emergency Internet" needs to stimulate technology development targeted to immediate restoration of a "minimum degree" of connectivity which must be rapidly deployed, robust, and resilient, demanding an alternative to the existing communication infrastructures.

3.4 Economics

The Internet, being a crucial piece of the communication infrastructure, it will be an integral part of future industry and economy as a whole, similar to any other utility (e.g., electricity and water). However, the current Internet was not designed so as to be or become a critical part of an economy's infrastructure. Information plays in this context the same utility role as electricity and water in other industrial domains. Digitalization of the information implies infinite reproduction available and quasi-infinite number of location at almost no cost beyond those of operating the information repository at the location. In addition, the Internet user should be allowed to be, at the same time, information consumer and information producer in order to make the Internet a real opportunity to increase business and commerce.

Hence, the laws of economy that are based on a product market (typically driven by scarcity and limited availability/accessibility) must be reviewed and revisited so as to lead to new economical models that are applicable to services and profitable to all actors. From this perspective, **the Future Internet shall investigate new retribution, economical, and business models that are not restricted to pure financial transactions in a world where everything is available to anyone, anywhere**. Also accumulation of information and content is not going to determine anymore a sense of value (as the "so-called" developed countries tend to impose) but the capacity to consciously and intelligently process that information.

As we are moving towards an information-driven society where networking capability becomes pervasive, it is also important that all socio-economical aspects are considered holistically such that all actors (prosumers, providers/enablers, etc.) become involved in a dynamic value constellation relying on federated network and systems. From this perspective, **the Future Internet will provide improved capabilities without imposing single economical/business model and by avoiding prejudging commercial and social outcomes for the different involved players/actors** but rather taking into account support of application and service evolution (prevent contention between different ISPs and users interest) as well as the configuration and operational changes.

The Future Internet will have by nature to constitute one ecosystem where the different actors and roles will be sustainable. There is one crucial need for research, in order to define the unambiguous and comprehensive ontology of business roles and relationships, assess the overall question of costs and values for the different stakeholders of the ecosystem (identification and quantification) and clarify the issues of control, liability and responsibility supported by the entities involved in the model. Such business studies are essential and they are intimately linked to societal, legal and ethical issues.

Today the Telecom and the Internet industry are structured completely differently with regards to applications: on one hand in the Telecom industry, applications are network infrastructure-centric including lots of standards. Applications could look similar but are expected to be fully interoperable. On the other hand, in the Internet Industry, service providers are completely answering a customer need without paying attention to the interoperability and relying on very lightweight infrastructure. ***It is hopeless for Telecom players to compete with Internet players keeping Telecom model development for applications***. The Future Internet shall provide a twofold path: enabling to focus on a specific user need and to develop a solution without paying attention to the network infrastructure. Once a leader on a specific application emerges, the Future Internet should also enable the growth of an eco system of players being able to build their own applications on top of its system.

3.5 Industrial and Governmental

Many sectors e.g. industrial, government, will undergo transformations in the coming years due to new business and technological opportunities and trends related to the Future Internet as highlighted in the following paragraphs addressing substantial changes expected in these and other sectors:

eEnergy: A new Internet-based infrastructure tightly coupled to the energy domain, will come to place to control the future decentralized power generation and storage networks and to support innovative trading models and mechanisms for trade based on supply and demand in the electricity market. The Internet of Things and Services will provide there services such as electronic marketplaces, facilitating the commercial activity associated with the buying and selling of electricity and its derivatives, not only for utility companies but also for decentralized consumers and producers. The Future Internet will combine ICT technologies such as intelligent sensors, agile middleware and business back end systems and this way provide new forms of more intelligently managed energy production, distribution and consumption on a point-to-point basis. This will in the end create a wide spectrum of market-based and regulatory options which quickly react to the changing supply and demand side of ecosystems.

Retail: The Internet of Things and Services will enable retailers (through an intelligent ICT-based management of the entire retail chain) to attract and retain consumers, while simultaneously allowing increased operational efficiencies in terms of product range, inventory levels and stock replenishment. This will be most visible on the shelves by increased availability of fresh products, more information on goods and their origins, guaranteed authenticity, etc. Furthermore, RFID technologies combined with web-based services will enable retailers and consumers to tackle plagiarism and thus facilitate the fight against piracy. In the same way, RFID in the health sector will avoid false medical treatment and prevent health damage caused by counterfeited drugs.

Logistics: With the Internet of Things many services can be offered to increase transport, storage and handling efficiency as well as traceability achieving Intelligent logistic management that integrates with traffic control and management systems considerable reduction in natural resource consumption. RFID applications are now being introduced at airports to significantly improve baggage handlings. Increasing capabilities of RFID technology and embedded systems allow for more information being stored and processed on physical objects which move new application domains closer to commercialization. The most promising ones are in the area of production, e.g. for more robust or decentralized production, as well as maintenance and repair.

Manufacturing: The Future Internet will support distributed "Green" manufacturing while providing the required integration of techniques and mechanisms to exchange all relevant information in a collaborative manufacturing environment. The Internet of Things and Services have indeed the potential to provide the right means for better traceability and real-time decision-making. It can also improve collaboration along the manufacturing process, this way opening up new opportunities for flexible business processes and introducing a swifter implementation of disruptive business models and products.

Financial: The trend towards the Internet of Services is visible through the emergence of Internet banks and loan providers as well as of new platforms for loan and insurance brokering. The successful integration of the financial supply chain services will enable financial service providers to offer the management of the entire working capital including inventory management. Finally, the recent banking crisis has shown that ICT should also be much better utilized in the context of risk assessment, mitigation, and compliance. The Future Internet can help here to quickly access and neatly pull together all information that is instrumental in this regard. For the insurance sector, the Internet of Things and Services will provide huge opportunities to differentiate products; for instance, insurers can monitor the status of a client's car by connecting to car devices, allowing for policy premiums based on the actual car usage. In addition, it will help to provide instant information to a car owner's insurance company in case of an accident to assist the policyholder with emergency services, towing or vehicle repair services.

eGovernment: The Future Internet can lead to efficiency gains and innovative services in the Public Sector. Semantic technologies as part of the Internet of Services would allow for aligning the information and for providing value-added services for entrepreneurs. Public Security is another important area where these new technologies can help to improve trans-national incident and crisis management, which is driven by the need to instantaneously coordinate relief operations between different public authorities. As a result, a coherent and holistic cooperation of different public and private stakeholders is essential to manage large events or complex transnational crises. A unified, pan-European web-based service platform would foster faster integration of and cooperation between public security agencies and should be a main objective of EU security policy.

eHealth: where conception is turning to a patient-centered universe. Firstly, the access by the patient to information services of global medical knowledge - comprising for first time genomics, proteomics and metabolomics at large scale -, each knowledge item being attached to a specific quality endorsement, as well as the accessibility of medical professionals to professional knowledge in order to let them perform better their duties. Also, interoperability among medical institutions (emergency services, hospitals, pharmacies, authorities, research labs) as well as among devices (data acquisition devices, medical actuators) will lead to an environment in which the "healthcare service" as a non-IT concept will get enhanced. New advanced approaches as Virtual Physiological Human, which requires a large set of computers with the capability to provide a personalization of a human body down to molecular level, as well as support in the diagnosis out of comparative effectiveness, understanding it as a new trend which combines personalized health and evidence-based medicine, will be leveraged by the new Internet of Services developments and new communication means e.g. sensors, medical picture archives. The consequent transformation of medical services industries which will take place out of this technological leapfrog will drive both to a better quality of healthcare and to a new growth in terms of high-quality jobs.

3.6 Environmental

The Future Internet must be ***environmental-friendly*** and so, appropriate network / system architectures that can offer such ecologically sensitive connectivity around the globe are needed. For this purpose, environmental issues should be taken into account in all studies related to Future Internet. As operators and manufacturers start to roll out revised products to reduce energy consumption and energy costs, the Future Internet offers an opportunity for redesign at a systems level on the basis of low energy, carbon neutral products and services. The overall usage of ICT today is using about 2 % of total energy consumption and thereby about 2 % of overall CO^2 emissions. However, the requirements for more advanced applications are increasing, which might increase again the power consumption (e.g. always-on, higher throughput). Therefore, more efficient technologies are needed to mitigate the potentially increasing power consumption.

Additionally, the increased use of ICT in a plethora of large-scale applications (e.g. eHealth, Transport) offers the opportunity to reduce the carbon footprint of user sectors through the support of their business processes by the Future Internet. The Future Internet shall support a rapidly increasing use of communications by applications sectors, on a global scale, in an energy efficient manner. For example communication between cars is able to optimize traffic flow and will reduce CO_2 emissions and the risk for traffic accidents. Such concepts of Green IT/computing are just starting.

The economic impact of the power efficient Future Internet technologies is hard to over-estimate. New technical innovations are needed to enable European vendors of telecommunications hardware and services to offer lower energy consumption communications solutions than their competitors do. The strategic relevance of this is that existing and new customers will be offered lower Capital Expenditure solutions with lower Operating costs. Smarter technology use could reduce global emissions by 15 percent and save the global industry EUR 500 billion in annual energy costs by 2020, according to a new industry study by the independent non-profit The Climate Group and the Global e – Sustainability Initiative (GeSI). (ref. http://www.smart2020.org)

4. Recommendations

Future Internet should be seen as a clear opportunity and means to meet the societal needs ahead in terms of economic growth, sustainable environment and quality of life.

As cross-ETPs Future Internet Group, we strongly recommend to the EU Commission, Members States and European Parliament to actively support our efforts to make the Future Internet a reality driven by European interests.

We will act to:

- Identify achievable business models based on the current ecosystem and based on disruptions brought by the Future Internet developments,
- Develop a dynamic roadmap for the key research challenges to be tackled, and establish a road map ensuring the take-up of the research results,
- Explore different R&D evolutionary and disruptive approaches, covering classical, clean-slate, and experimentally-driven,
- Further develop the cross-domain research fertilization covered by the set of projects working together in the Future Internet Assembly.

We however call on the European Union to:

- Provide the financial resources allowing for the strengthening of the industrial/public partnerships in R&D,
- Develop appropriate multi-disciplinary teaching and life-long training programs to ensure sustainable knowledge and skills acquisition facilitating innovation,
- Develop the an integrated and structured approach between National and European R&D programs so as to overcome the current fragmentation of efforts,
- Develop and implement the so-called push-pull model: large investment in R&D accompanied by a solid and homogenous policy of leading edge markets development and public procurements,
- Stimulate a pan-European coordinated approach on matters relating to standardization and the single market,
- Provide the means to ensure global coordination of concepts and plans for the Future Internet to address industrial perspective,
- Raise awareness of all European citizens about the clear and visible benefit of the outcome of the investment in Future Internet development.

Developing a successful European leadership requires to embrace the complete system perspective, to guarantee that the benefit will be much higher that just the sum of each individual component. Stakeholders in Europe developed the early understanding about the potential of this evolution and engaged in the current Cross-ETPs Future Internet Group. This is now a turning point to make this vision become a reality. Referencing Joel Arthur Baker (in the Power of Vision) "*Vision without action is merely a dream, action without vision just passes time, vision with action can change the world*", Europe shall now move on different specific actions in order to move beyond the vision.

Working document: Technological Challenges

This working document provides for a first description of our thoughts on the technological challenges compared to the current Internet.

1. Challenges associated to Network Foundation

The term Internet includes both the "core Internet" (Internet Service Provider networks) and "edge Internet" (corporate, private, and community networks). The Internet architecture relies on design principles such as modularization by layering, connectionless packet forwarding (no virtual circuit), network inter-networking principle (gateways), and the end-to-end principle. The latter is the fundamental architectural principle, around which the Internet has been built. The application of the end-to-end principle results in a network that is transparent, that ensures for applications to survive partial network failures, and provides for a general connectivity service capable of supporting many different applications. The Internet is not designed or optimized for any single application, but designed for genericity and evolvability (i.e., for any applications that can be supported by a best effort communication path). The network forwards packets while knowledge of the application is localized to the edges, where the attached hosts sit. This functional decomposition should, in principle, facilitate innovation and the deployment of new applications.

As a result of the Internet growth and the increasing communication requirements, many patch solutions have been progressively developed and deployed to enable the Internet to cope with the increasing demand in terms of user connectivity and capacity. There is, however, a growing consensus among the scientific and technical community that the current methodology of “patching” the Internet technology will not be able to sustain its continuing growth and cope with it at an acceptable cost and speed. - Note however that this does not mean imply that a clean-slate approach is the way forward and in particular the only way forward -Indeed, with the erosion of the five base design principles (modularization by layering, connectionless packet forwarding, end-to-end principle, uniform inter-networking principle and simplicity principle), the Internet has progressively become an infrastructure more complex to operate. This complexity results from various layer violations (e.g., complex cross-layer design) to supposedly optimize network and system resource consumption, the proliferation of various sub-layers, e.g., Multi-Protocol Label Switching (MPLS), and Transport Layer Security (TLS) to expectedly compensate for intrinsic shortcoming in terms of forwarding performance and security functionality, IP addressing space overload (including network graph locator, node identity, connection termination), and routing system scalability and quality limitations (e.g., Border Gateway Protocol (BGP) path exploration and oscillations) to name a few. This complexity progressively impacts the Internet robustness and reliability and in turn impacts its scalability (resulting from the violation of the Occam's razor simplicity principle also known as the "Robustness through simplicity" principle).

Hence, although the design principles of the Internet are still suitable and applicable -- there is no evidence that the existing principles shall be demoted but instead that some may benefit from adaptation to cope with the Internet evolution and new principles shall complement them --, there is growing evidence that the resulting design components, as defined today, face certain technical limits (in particular, in terms of scalability). On the other hand, certain objectives of the Internet are no longer adapted to users’new expectations and behaviors when using the Internet (in particular, in terms of reliability). In other terms, the current Internet architecture is progressively reaching a saturation point in meeting increasing user's expectations and behaviors as well as progressively showing inability to efficiently respond to new technological challenges (in terms of security, mobility, availability, and manageability), in inability to support the business models necessary to allow value flow in an increasingly complex service delivery ecosystem that can involve multiple actors, and socio-economical challenges. Even worse, misguided attempts to sustain the Internet growth resulted into progressive violation and erosion of the end-to-end principle. Sacrificing the end-to-end principle has in turn resulted in decreasing the Internet availability, negatively impacting its robustness and scalability as well as making its manageability more complex. Over time, the erosion of the end-to-end principle has also resulted in the proliferation of peer-to-peer and application-specific overlay networks that are progressively substituting the end-to-end IP networking layer by an end-to-end applicative communication layer. Indeed, many new applications provide their own path selection to ensure proper connectivity and quality, resulting in an ineffective network level resources use.

To cope with the increasing expectations on the Internet infrastructure, the IPv6 technology has been designed by the IETF to replace the current version of the Internet Protocol, IPv4. This replacement would concurrently re-establish the global end-to-end communication paradigm restoring the valuable properties of the end-to-end IP architecture. Indeed, these properties have been lost in the IPv4 Internet due to the increasing number of Application Layer Gateways (ALGs), Network Address Translators (NATs) and firewalls as well as caches and proxies deployed at various network places and for various applications. Over the past decade, heated debates have raged on whether or not IPv6 can offer clearly superior value propositions to the industry. Indeed, also simpler and cheaper network models would also address the problem of revenue erosion. This reasoning has resulted into a common industry belief that the conditions for IPv6 deployment will be met "in the future" (but without clear target). Delaying the decision for wide-scale IPv6 deployment has created the conditions for the development of a parallel industry supplying "solutions" that rely on network complexity, address scarcity, and insecurity. Following this view, applications and services are engineered for environments where ALGs, NATs, and firewalls are assumed to be part of the current IP plumbing with NAT deployed for compensating the lack of address prefixes and firewalls proliferating to ensure security of the end-user.

However, this complexity just results in more fragile application communication (resulting in turn in decreased user satisfaction) and lower operational margins (resulting in turn in decreased ISP satisfaction). At the time of writing of this document, available studies show that the Regional Internet Registry (RIR) IPv4 unallocated address pool will be exhausted by end of 2011, and that the IANA IPv4 unallocated address pool will be exhausted by end of 2010. Therefore, even if IPv6 deployment is required to compensate IPv4 address space exhaustion, contrary to the initial expectations it will at best provide a partial answer to some of the Future Internet challenges. Indeed, the IPv6 technology does not per-se improve manageability (e.g., intrusion and attack/anomaly detection, and problem/root cause analysis), and resiliency. Moreover, resolving the IPv4 address exhaustion implicitly increases the concerns related to routing scalability and quality whereas IPv6 does not improve these required properties of the routing system.

All actors involved in the Internet (including, academic, vendor and network operator communities, etc.) are now actively discussing the limitations of the current Internet architecture as well as its potential evolution. Indeed, despite ongoing efforts, no satisfactory solution is currently available or even exists to address altogether the challenges experienced by the Internet and its evolution (there is no order of precedence in the below numbering):

1.1 Security, Privacy and Trust

1.1.1 Security

Security is only supported weakly by the current Internet infrastructure. From its inception, the Internet was conceived with the principle that computing systems are by definition trustable entities, enumerable (their number was limited to tens of hundred or thousands), and cooperating/

acting toward commonly shared universal goals. The situation as of today is the complete opposite: trustable computing systems and end-users are the exception, their number makes anonymity a powerful weapon for security breaks of any sort, and finally the end-user basis is heterogeneous than ever in its objectives, usage, and utility. However, viruses, phishing, spyware, and identity frauds risk induce reduction of users' confidence in the network and therefore its usefulness. From the latter perspective, the usage of the Internet has partially become the mirror of our "modern" society. As such security is one of the biggest imminent problem facing the Internet.

These considerations reveal a range of security issues and needs to be addressed when re-examining the network architecture. These include requirements for acceptable security for users, protection of the network (e.g. against Denial of Service, DoS), guarantees of acceptable availability (in some cases supporting multiple levels of priority and preemption), and specific networking issues such as multicast key distribution. The security implications of middleboxes must specifically be considered as the Internet evolves to determine the potential for performance acceleration, policy and security implications. The wide-coverage of many satellite networks, also requires the security framework to encompass the legal mechanisms requited to deter and trace attackers, coupled with the implications of providing lawful interception. It is important that security is considered early in the design. Security in a complex network is exploited through several services and can be provided/ensured at different layers. According to network architecture and complexity, security provision must be optimized taking into account the characteristics of the different components. In presence of wireless segments, specific challenges must be addressed in terms of protection from undesired users at physical level (jamming) or network level (access, data integrity, unauthorized data acquisition, etc.).

The main security challenges include:

- Securing the architecture of Future Internet: we need to rethink security at Future Internet design to have it built-in (security at design time) in addition to the execution (security at running time). This calls for new and innovative approaches such as for example collaborative security (leveraging existing ones and research on that field) but also for proper tools to ensure monitoring.
- Protection against existing and most importantly emerging threats:
  - *Means for proactive identification and protection from arbitrary attacks* such as Denial of service (DoS) and intrusion detection: as the Internet is becoming the universal communication network, conveying all kinds of information, ranging from the simple transfer of binary computer data to the real-time transmission of voice, video, or interactive information, it is also deeply impacted by unwanted traffic of all sort (ranging from spam to worms). A major consequence being that it becomes highly exposed to attacks, especially to denial of services (DoS) and distributed DoS (DDoS) attacks. DoS attacks are responsible for large changes in traffic characteristics, which may, in turn, significantly reduce the quality of service (QoS) level perceived by all users of the network. This may result in breaking of the service level agreement, with the Internet Service Provider (ISP) being accountable, potentially causing major financial losses for them.
  - *Means for proactive identification and protection from malicious software (malware)* such as viruses, spyware, and fraudulent adware.

1.1.2 Privacy

Privacy is often defined as the right to informational self-determination, i.e. individuals must be able to determine for themselves when, how, to what extent and for what purpose information about them is communicated to others.

Privacy issues fall into two broad categories: users' data privacy and location privacy.

- *Data privacy* involves control over personal information contained on the devices and the services providers and in associated database(s). True policy concerning the protection and the use of the personal's data is absolutely requested (current declarations of intent are not enough) in order to generate trust and confidence in services offered through
- *Location privacy* involves control over the information regarding the individual's physical location and movement. Major threats caused by location based services to the user's right of informational self-determination are unsolicited profiling, location tracking and the disclosure of the user's social network. Another problem is that exposed information about social contacts can be revealed that is often of a private nature. In a misuse scenario, an unauthorized party can gather a list of the close friends and private locations of a user. In the same way, for today's commercial multi-user location based service (LBS) applications, such as friend Finder, the user lacks efficient control over his "reachability".

Future Internet. It is thus important to define proper global (EU first and second International) privacy standards on the basis of what to develop the right technology to let people make informed decisions about the services they access. A challenge will also be to preserve anonymity and privacy at large of users of mobile-capable Internet devices. Domain is far-reaching and problems very different, relating to privacy risks and traceability, for mobile internet, mobile phone, electronic toll payment tags, ePassports, loyalty card programs, mobile RFID (Radio Frequency Identification) service, Mobile P2P Systems, vehicular ad hoc networks (VANET), Mobile Ad-hoc Networks (MANET). The mobile Internet and location based service (LBS) applications poses new social risks and challenges that have to be addressed by law and technology if we want Future Internet to come to Life and be widely adopted. For that we could leverage research on PETs (Privacy enhancing technologies) and move towards privacy enabling technologies to manage PII on the Internet throughout the whole information life cycle (collection, processing, use, disclosure, retention, and destruction). This would call for example to seamlessly embedding PETs into FI design so as to achieve comprehensive risk management. How to take care of its privacy is also an issue that needs to be addressed. Indeed, individual actions are limited because of ill-defined rights. As such individuals can not be aware of privacy violations. This calls once again for global privacy standard(s) in order for a platform/framework to comprehensively manage risk and warn people in case of any security breach and/or privacy violation. In the meantime more attention should be paid to the proportionality requirement and what it offers in terms of solutions (e.g. not condemn data mining but compensate generously innocent people by means of post factor redress both legal and financial).

Internet users have several identities when performing different online transactions. For example, users could have an "anonymous identity" to surf general web sites, a "domestic identity" for accessing retail web sites, and an "office identity" for accessing corporate intranets. Decoupling identities from individuals can reduce the information collected about a single individual. However, identity management technologies are rather complex. So far, allowing easy definition of policies and simple awareness active personas has proven to be a difficult task. In addition, identity federation can be defined as the set of agreements, standards and technologies that enable a group of service providers to recognize user identifiers and entitlements from other service providers within a federated domain. In a federated identity domain, agreements are established between Service Providers so that identities from different Service Providers specific identity domains are recognized across all domains. These agreements include policy and technology standards. A mapping is established between the different identifiers owned by the same client in different domains that links the associated identities. The federation of isolated identifier domains gives the client the illusion that there is a single identifier domain. The user can still hold separate identifiers for each service provider. However, he does not necessarily need to know or possess them all. A single identifier and credential is sufficient for him to access all services in the federated domain.

However, a potential problem is that users will still have to manage multiple identities and credentials, even if they are not actively using all of them. In centralized user identity models, there exists a single identifier and credentials provider that are used by all service providers, either exclusively, or in addition to other identifier and credentials providers. From a user perspective, an increasing number of identifiers and credentials rapidly become totally unmanageable. In the context of FI design this would call for a user-centric approach to identity management to improve the user experience, and thereby the security of online service provision as a whole.

To address these challenges, research in the following space is thus required:

- Design of user interaction for identity management, expressing trustworthiness of identity management to users and privacy-enhancing identity management,
- Accounting/logging tools required for forensic purposes (but not limited to),
- Methodologies and interfaces for managing multiple identities and credentials including delegation,
- Distributed identity management at each providers of services, synchronization with repositories of record, access right framework based on semantic, in particular with respect to user centric identity and high-level identity assurance.

1.1.3. Trust

Mature service-based society can only be successful if citizens and service consumers can really trust underlying technologies. The key point here is that the Future Internet will need to provide means for easy and natural exchange of critical, protected and sensitive data between countries, public and private organizations, and individuals. In that context one of the key challenges would be to make trust part of the FI design and "built-in" by construction in order to achieve end-to-end trust to subsume end-to-end security.

End-to-end trust is an inclusive approach where trust is intimately integrated in all the capabilities of Future Internet in a pervasive way to cope with the software for all of the applications surrounding us. In Future Internet, trust will appear natural and intuitive to human beings, around everyday life. Some services "you can trust" (together with economic models) behind them have already been defined but are still limited to some specific domain (such as eBanking domain and other ePayment service). This type of Service you can Trust has to be generalized and made part of FI design in order for trust to become implicit and granted thus enabling users to be confident in Services they access and use (Internet of Services) and the fact Smart things (Internet of Things) will communicate on behalf of users. This obviously would also call for trust defined and guaranteed by contract together with services and techniques (e.g. trust negotiation techniques) enabling this to happen. One important challenge also to consider here would be address trust also at the level of the device used to access the Internet through a potentially virtual desktop. Indeed in the context of virtualized environment the problem is not so much to secure the device by itself but to secure user and/or corporate resources which are virtualized due to upcoming trends (e.g. resources virtualization, cloud computing).

To address these challenges, research in the following space is required:

- Semantics for trust,
- Trust target certification,
- Trust lifecycle management in highly dynamic environment (modeling, monitoring, audit, recovery),
- Automated or semi-automated (collaborative) decision-making on trust (including trust negotiation techniques).

1.1.4. Enablers

Enabling users to understand security, privacy and trust in the FI: this challenge was partially described above: it relates to the fact end users have to be educated in order to make informed decisions as a real FI user (so security-, privacy- and trust- aware when making decision using FI). Users often do not understand the privacy implications of their online behavior. They may not realize that certain combinations of seemingly non-personal information (for example: birth date and zip code) might be used to identify them or to infer private information (this is known as an "inference attack"). They also may be unaware of the potential for their computer to be tracked as a result of the IP address that it transmits to web sites. In addition, they may not be able to anticipate in advance when they might want information about their online behavior to remain private. Many protocols reveal user and machine identity and affiliation leading to potential exposure to unwanted attention and targeted attacks. Currently, using wireless computing is like wearing a name tag (e.g. Apple iTunes discovers other users nearby to enable sharing – Bonjour protocol broadcasts user and computer name to establish the link). New approaches could be based here on network location awareness (NLA) so as to enable adaptive privacy policy. Another challenge would be to find the best mechanisms to present the information "intelligibly" to the users so as to reduce the user interaction to a minimum (i.e. perform as many decisions as possible in an autonomous way).

Development of information security (e.g. security for information exchanged) and service security (e.g. security for exposed services) is also needed. This will ensure and balance the confidentiality, integrity and availability of information and knowledge in the context of Future Internet in order to become a value-creating net directly from services and their composition. This is key to create greater certainty for business, to stimulate economic activity and/or innovation.

Finally, addressing all these security, privacy and trust challenges calls for a multi-disciplinary and integrated approach with all relevant stakeholder's perspectives including the technologists, government, policy, business and user/societal[5] .

1.2 Accountability

The current Internet design positions (resource) accountability as a secondary goal – the primary being the effective multiplexed utilization of existing interconnected networks which are owned by and operated in a federation – underlying the DARPA Internet protocol. At the same time, he acknowledged that accountability has received little attention during the initial phases of the Internet and its deployment. The shift of the Internet role toward an infrastructure with increasing commercial and business usage resulted in an increasing need to address this initial Internet design goal. Hence, over time, a number of techniques have been proposed to provide for accountability support by the Internet Infrastructure such as congestion control and IP traceback. In other words, accountability (part of the initial Internet design objectives) has never been really met by the current Internet infrastructure, e.g., traceback and other congestion control techniques are not widely deployed to identify misbehaving users and traffic sources.

In the future this problem will be exacerbated as the concept of a single owner of the service being delivered no longer holds true. The Internet of Services is a step towards an ecosystem where there will also be a need for service elements to be accountable to each other. Equally we are envisaging that services and things as well as devices will use the infrastructure.

[5] http://www.think-trust.eu/

The Future Internet needs to address multiple accountability challenges including:

- Service to infrastructure accountability (service provider accountable for resource usage)
- Infrastructure to Service accountability (Internet delivering what service provider expects)
- User to network infrastructure accountability (user accountable for resource usage)
- Network infrastructure to user accountability (Internet delivering what user expects)
- Service to Service accountability (service delivering functionality another service expects)
- Service to user accountability (service delivering what user expects)

1.3 Manageability and Diagnosability

It is commonly acknowledged that the Future Internet should have a considerably enhanced network manageability capability, and be an inseparable part of the network itself. Manageability of the current network typically resides in client stations and servers, which interact with network elements via protocols such as SNMP. The limitations of this approach are reduced scaling properties to large networks, and the need for extensive human supervision and intervention. A new network manageability paradigm is thus needed that allows network elements to be autonomously interrelated and controlled, that adapts dynamically to changing environments, and that learns the desired behavior over time.

The effective design of monitoring protocols so as to support detection mechanisms critical for the elaboration of self-organizing networks has to be based on a clear understanding of engineering trade-offs with respect to local vs. non-local and aggregated information, for instance. Possible techniques for realizing these protocols include distributed tree algorithms, gossip algorithms and stochastic models. One important aspect for making network manageability effective and efficient is situation awareness (local reaction wrt contextual changes). Due to the resource limitations, this functionality is almost impossible today. It is therefore important to understand and control the relationship between decision quality and the cost of achieving a specific level of situation awareness.

The Future Internet will comprise heterogeneous networks and underlying data link technologies having high-level distribution. However, service and applications running on top of it will execute independently of the underlying networking technologies so as to prevent complex / statefull and thus harmful cross-layer dependencies. In the FI context, manageability needs to deal with this heterogeneity and to successfully manage the network operations incorporate autonomous decision-making so as to allow network to adapt accordingly. It should also involve the operations of facilities and services, and business relationships with customers, partners and suppliers, in order to capture the behind-the-scenes operations that are required to enable services to be delivered reliably and to ensure that the operations of the FI is profitable.

Importance of manageability and diagnosability are caused by a performance drop due to an increasingly growing Internet infrastructure, for which existing solutions are no longer adequate to allow for correlation of a priori unrelated events that may impact (some part of) the infrastructure e.g. routing system. The fundamental challenges to be addressed are:

- Configuration and upgrade management (and their resulting cost) knowing that in practice continuous patching results in relative decreasing gain but increasing complexity
- Address and routing information management
- Stateless resource control (so as to prevent negative impacting on scalability)
- Problem (e.g. anomaly, inconsistency) detection and root cause analysis (as the current paradigms, techniques and toolset for debugging the Internet are limited).

1.4 Availability (maintainability and reliability)

Successful communication means and architectures, which have been offering reliable and dependable services and have been extensively and effectively used as a fallback for major communication links to assure resilience to infrastructure failure, shall be maintained and possibly reinforced in the FI. From this perspective, ISPs face the task of providing an increasing set of services, which meets user expectations in terms of availability and reliability. Availability problems result mainly from the decreasing routing system quality (in part., its stability, its robustness, and its convergence properties) but also from the increasing operational complexity. These problems are exacerbated because there is no capability in the current architecture for the value of the services being delivered to flow through to the capability provider who needs a return on any investment that could address such concerns in part.

An important aspect that characterizes services offered by the Internet is the availability of the IP connectivity service. For Internet users the important aspect is the resulting service availability, measured in terms of average service availability over a given period of time (e.g. one week or one month) and of maximum service interruption (max recovery time) before real outage time starts being counted. Availability is defined as the probability that the system is operating properly when it is requested for use, i.e., the probability that a system is not in a failure state or undergoing a repair action when it needs to be used. It is expressed as a function of reliability and maintainability. Improving availability implies thus improving the maintainability capabilities of the Internet infrastructure using resiliency techniques. Resiliency is the ability of a system to reach (rapidly) and maintain an acceptable level of functioning and structure with one or more of its components malfunctioning. In particular, a resilient network aims at minimizing impact on resource (soft or hard reservation) and access downtime to controlled resources. Note that resiliency does not refer to a "full" but an "acceptable" level of functioning and does not refer to the correction of these malfunctioning components. Availability is also a function of security measures to avoid unwanted traffic and is a second-level function of the robustness of the component protocols. Hence, architectural and design techniques can significantly impact the survivability under stress conditions.

However, until recently, the Internet and most the routing protocols were not designed with much attention to accommodate fast recovery mechanisms (time performance were designed to support failure recovery of the order of the second). Indeed, traffic disruptions resulting from network failure have lasted for periods of at least several seconds, and most applications have been constructed to tolerate such a quality of service. Recent advances in routers have reduced this interval to below a second for link state routing protocols (such as OSPF and IS-IS). Such techniques allow the failure to be repaired locally by the router(s) detecting the failure without the immediate need to inform other routers of the failure. In this case, the disruption time can be limited to the time taken to detect the adjacent failure and invoke the alternate routes. However, new Internet services are emerging which may be sensitive to periods of traffic loss, which are orders of magnitude shorter than this. Nowadays, network resiliency techniques need to ensure time performance for sub-second recoverability.

In the future Internet, there will be a large number of ways to access to internet and customer premises equipment may be attached to several networks i.e. multi-homed. These devices and applications will thus offer the possibility to choose which network/access technology to use. In the current Internet, there is a need for a “gap filler” regarding the provision and availability of Internet connectivity services to specific areas, such as rural and remote areas, on trains, airplanes, ships, etc. Future Internet shall allow the design and deployment of hybrid terrestrial/satellite communication networks to increase availability in these critical areas, as well, to reduce deployment costs, to increase efficiency and flexibility and to provide dependability. Furthermore, in the context of “Broadband for all”, the space segment can play a key role generally available in short and medium range (in IEEE 802.11 pico-cells, in IEEE 802.16 micro-cells, in xDSL of the order of a few kilometers). Therefore, the integration of terrestrial networks with satellite networks can be key factor for the realization of global connectivity coverage. This integration can be regarded as a valuable mean to reduce the effect of the “digital divide” with low deployment costs, allowing Future Internet to reach a lot of users in many areas of the world (particularly in Africa and Latin America) where the lack of connectivity is a serious impairment for social and economical development.

The Future Internet should be able to support a delay tolerant and disruption tolerant network service based on a communication with disruption and disconnections with high delay of heterogeneous peers[6]. An architecture including scheduled intermittent connectivity, wireless links that cannot maintain end-to-end connectivity, satellite networks with moderate delays and periodic connectivity and moderate delays links with frequent interruptions due to environmental factors.

Furthermore, the Future Internet needs to support emergency situation and to assist society to restore situations on emergencies, crises or natural disasters. Since Future Internet is expected to play a key role in information access, this feature must be maintained also under critical events. To this end, both backbone and access segments of the network must be capable of providing self-healing capability. This structure is certainly beneficial to emergency operations coupled with access priority mechanisms and shall be addressed, as well.

The specific challenges to be addressed with this respect are:

- Monitoring and measurement
- Resiliency against normal accidents and failures
- Fast convergence/recovery of routing system
- Global connectivity coverage availability
- Availability and reliability even in critical emergency situations

1.5 Scalability

With the expanding number of hosts/devices the FI must be able to accommodate very large network topologies without demanding exponential increase in operations for the communication network. Under these circumstances, the FI should be highly scalable and should include network architectures able to meet these specific requirements. Flexible networking possibilities should expand communication network infrastructures to allow easy connections among geographically dispersed locations without relying on public infrastructures or tunnels thus enhancing scalability to support from one to an unlimited number of locations.

Also as the Internet grows, the routing system scalability progressively results into major cost concerns for both vendors and Internet Service Providers (ISP). The most fundamental issue about scalability of the current Internet architecture is related to its routing system. Indeed, the current Internet routing system is facing

- Due its expansion to its expansion, an increasing number of autonomous systems (mainly at the edge/periphery of the Internet) and thus increasing number of routes that in turns result in routing scalability burdens (cost per BGP state).
- Growth of routing table entries resulting from site multi-homing and prefix de-aggregation for traffic-engineering purposes (the Internet routing system shall thus not only scale with increasing number AS/address prefixes)

[6] This work has been pioneered by the DTN research group of the IRTF.

- o User/site addressing (Provider Independent) vs network addressing (Provider Allocated) that impedes prefix aggregation and in turn contributes to degrade the Internet routing system stability (since BGP has to cope with an increasing BGP update rate)

Also due to this increase, the routing system dynamics (robustness/stability and convergence) resulting from BGP deficiencies (security and convergence properties - path vector protocols are impacted by path exploration/hunting), inconsistencies (software and configuration bugs, routing policies, etc.), BGP instabilities, and failures are also becoming a key concern in the operational community since exacerbating the observed trends. A fundamental dimension in this context is the dynamics of the routing information exchange between routers, in particular, the routing topology updates that dynamically react to topological structure changes. Indeed, inter-domain routing quality (convergence, stability) and scalability do not only depend on the algorithm used to select the paths, but also on the number of inter-domain routing messages that are exchanged among routers. Solving the routing scalability and quality problems together is challenging. On one hand, routing convergence, i.e. the delay between an event and the instant when all routers have correctly reacted to this event, should be minimized. On the other hand, scalability implies that the number of message exchanged should be minimized to avoid overloading the inter-domain routers.

The specific challenges to be addressed with this respect are:

- o User vs network addressing space to cope with the overload/mis-use of IP addressing space usage
- o Sub-linear scalability of routing system wrt to number nodes ~log (n), ideally (today scaling of routing system based on stretch-1 shortest path routing algorithms is uncompressible beyond n log (n))
- o Robustness/stability and convergence properties of the routing system
- o Ensure the Internet infrastructure can cope with an increasing number of autonomous systems in particular at its periphery

1.6 Mobility

The requirement for mobility and global wireless broadband coverage has been a key research issue in the last ten years (e.g. for the EC FP6 and FP7 programs). The number of systems accessing services using a wireless communication path has increased significantly (for example the number of mobile subscribers is about 3 billion today) and it is predicted increase significantly in the future with the advent of new wireless technologies. From this perspective, the critical challenge is to enable such communication to be possible using the Internet.

Furthermore, wireless communicating devices will increasingly exchange elastic and streaming traffic resulting in increased expectations in terms of higher throughput values per device with lower latency than in today's systems. Significantly improved transmission capabilities are increasingly required to support increased traffic originating from data applications. For this reason, new and more efficient radio access technologies compared to existing systems will be needed supporting ubiquitous communication at an affordable cost-benefit-ratio.

The space segment will also play a key role in combination with terrestrial networks that are able to serve certain areas, extended at most in metropolitan environments. Nowadays, the use of term “broadband mobility” mainly refers to “nomadic broadband users” that are free of wires, but slowly moving inside a small geographical, mostly indoor, area. Extended mobility can be guaranteed with terrestrial cellular networks, but this kind of mobility is still “narrowband”. Aeronautical and naval transportation services for instance cannot be satisfied by terrestrial connectivity. In contrast, the demand for low-cost Internet services on trains, airplanes and ships is continuously increasing.

Therefore, the FI should “reach” the user also during his/her job or vacancy trips. Up to now, the cost of Internet services offered “on board” is quite high and the quality of the provided service is not particularly exciting. Significant work is thus still to needed to increase the “broadband mobility” for “really mobile” users. The achievement of such ambitious objective can be realized by means of integration between terrestrial and satellite networks in an enhanced “vision of convergence” already mentioned in “4G and beyond” future issues.

The specific challenges to be addressed with this respect are:

- Wireless access: the Internet’s main transport protocol (Transmission Control Protocol, TCP) end-to-end flow control and congestion control needs to cope with corruption and transmission loss and react appropriately (instead of interpreting losses as a sign of congestion). So the key challenge is how to project the needs derived from the existence of heterogeneous links, both wired and wireless yielding a different trade-off between performance, efficiency and cost.
- TCP connection continuity: using IP address as both network identifier and host identifier but also TCP connection identifier results in TCP connection continuity problem. Resolving the latter requires a certain level of decoupling between the identifier of the position of the mobile host in the network graph (network address) from the identifier used for the TCP connection identification purposes.
- Moving mobile devices such as cellular phones on the Internet is challenging due to limited scalability of Mobile IP (relying on home agent and tunneling). Note that contrary to a persistent belief, the problem is not entirely resolved in IPv6 that still make use of home agents.
- Together with host mobility/nomadicity, suitable localization techniques
- Take benefit of the radio interface/technologies have inherent broad-/multicast capabilities (air-interface resource consumption)
- Extended broadband coverage to specific critical mobile platforms, such as airplanes, ships and trains.

The challenge/technical impact of administrative borders shall also be considered when dealing with mobility/nomadicity. Today, mobile networks extensively use roaming agreements to regulate relationships between operators and having subsequent effect on user billing. Now in ISP world is the operator relationship much simple with peering or customer (transit) agreements. However the pressure in ISP side is to have more complex relationships. Future automation of peering/roaming to support a more dynamic infrastructure for both end users and operators shall be further investigated. Aspects like heterogeneous access and even sensor networks accentuate the need.

1.7 Heterogeneity

1.7.1 Heterogeneous Applications

Applications are not only programs running on computers or mobiles. An application in the Future Internet would be defined has a set of components that answer completely and entirely to a customer need. Let’s take as example Apple providing a device, the iPod, a computer program, iTunes to manage MP3 library on the user computer, and an online service with MusicStore. This set of components is one single application that fulfills the end user need: “I want to buy easily music and listen to it in mobility”.

The software industry landscape is drastically changing due to double phenomena. First everybody expects a share of the perceived value. On one hand, the classical software vendors are becoming service providers (e.g. Microsoft with Windows live) and on the other hand service providers are more and more involved in the initial phase of application building (e.g. Google with the Android development platform for mobile device). The role of each player is completely redefined and everybody is trying to get closer to the end user. Second, the end user is himself implied in several steps of application creation. The development of Web2.0, 3.0, etc is important for communication service providers for three main reasons, first because internet users are organized in social networks, secondly because they became the major contributors to the web content and third because the content is not only documents but also multimedia content.

The applications built on top of the Future Internet will require a variety of different communication services (one-to-one, one-to-(m)any, many-to-one, and many-to-many): a non-exhaustive list of examples is the following (compared to the so-called best effort service, most needs can be expressed as a combination of delay and rate):

- real-time service
- guaranteed minimum available bandwidth
- reliable data delivery with relaxed constraints concerning delay and jitter
- data flow resilient against infrastructure failures
- best effort

These different communication services need to be established throughout heterogeneous networks (e.g., wireless, wireline, and hybrid environment) and shall allow an easy integration of future technologies.

1.7.2 Heterogeneous Environments

Control systems for manufacturing lines, drive systems and motors for application to automotive and transportation, control of energy flow in complex power generation systems, building technology, process automation and control and also environmental protection and monitoring systems, just to name a few pose a different set of requirements than "usual" web and streaming applications. Some of the corresponding requirement categories do map quite well to the Future Internet challenges in terms of availability, scalability, security, etc. but in many cases the corresponding requirements are more stringent in industrial environment. For instance, in terms of availability, seamless failover mechanisms are required in the area of automation which does not allow for any lost information during a communication network recovery process. In terms of security, a security violation is critical for protection of life when distributed energy networks are controlled via communication networks which require extremely high protection against any kind of security attacks. Embedded and IP enabled devices are found almost everywhere in the future due to miniaturization and the fact that computing gets more and more pervasive especially in the world of industrial applications, e.g. for robotics, energy control or building automation. Since these embedded devices show special constraints concerning their capabilities such as e.g. performance or energy consumption, the Future Internet protocols and services must be able to cope with for needs of embedded systems. For instance, embedded services are required for small microcontrollers to also fulfill the real-time and robustness requirements of some field applications (e.g. in manufacturing, building management, metering infrastructures). At present, those networks are more or less separated from the enterprise or public networks by means of gateways and firewalls. A tighter integration promises cost savings due to a consistent management and eases the development of new applications which then can run more easily end-to-end, from Web server to the sensor. However, this creates new challenges when running e.g. hard real-time applications over the same physical media as voice, video or data traffic.

Typical enterprise applications (i.e. communication suites) are already IPv6 enabled. This is not so obvious for the currently closed and much more separated networks in industry or building automation or energy control. Dominant protocols find their roots in the 80's of the last century (i.e. BacNet, Profinet). However, one observation is the trend not only to use standard IP and Ethernet technology but also to couple those networks tighter with the enterprise. Not only will this create a pressure here for IPv6 migration, the protocols and middleware stacks used in these areas may take advantage from the enhanced IPv6 features such as anycast, mobility, and security. We expect that using these native IP techniques to be more efficient than respective functionality on higher layers when it comes to real-time discovery or security (as IPv6 mandates support of IPSec). Also a seamless integration will simplify network management and monitoring and thus will reduce costs. As industrial communication is crucial for the European secondary sector - both for large companies and small/medium enterprise - we consider research in the area of automation and control with respect to IPv6 and new layer-2 techniques as a crucial issue.

1.7.3 Heterogeneous Devices

The Future Internet has to be an enabler for applications connecting any kind of devices including also embedded devices, which will be found almost everywhere in future due to the fact that computing gets more and more pervasive. Since these embedded devices show special constraints concerning their capabilities, their performance, their energy consumption, …, the Future Internet concepts, protocols and services must be built in a way that they are applicable for these ultra-small embedded systems. E.g., embedded services are required for small microcontrollers to also fulfill the real-time and robustness requirements of some field applications (e.g. in manufacturing, building management, metering infrastructures).

Note on evolving physical layer and capacity:

1. Higher bit rate optical solutions shall be investigated so as to satisfy the bandwidth demand generated by the deployment of ultra-broadband access. Solutions have to be high bit rate but also economically viable. Research is needed on cost effective optical components. Concerning optical access, key drivers will be:

- Capacity (how to increase spectral efficiency of optical systems, even in existing fiber infrastructures impaired by polarization mode dispersion),
- Transparency (how to reduce the number of optical-electrical-optical conversions in the network),
- Agility (how to use the wavelength domain so as to optimize in real time optical resource usage)

2. High speed radio technologies and their integration in the heterogeneous systems. Research work is needed on radio systems with specific emphasis on the physical layer itself. Studies should also concentrate on an appropriate architecture, granting full distribution and simpler access, allowing decentralized resource management, command and control. Seamless mobility and service continuity have to be ensured in this particular context.

2. Challenges associated to Pillars

The challenges will apply to the different pillars. As a summary of some of the most urgent challenges, the following can be highlighted:

2.1 Internet by and for People

Among the activities related to increase the knowledge of the user, learning their habits and needs to better design future applications, interfaces and services while keeping people self-arbitration and mindful is a major area of investigation. This includes research challenges in the following areas:

- ***Knowledge of users***: services and the web should be adaptable by and accustomed for the user. This implies some effort in customer characterization and personalization that is considered a key element. This possibly shall require new applications that extract information from the user data and usage (subject to legal and personal limitations).

- *Content and user awareness*. This area is focused on recommendation systems, particularly for mobile web and localized services. Particular attention will be given to personalized and contextualized advertisements without prevailing over user self-arbitration. This implies providing at the same time the means for the end-user to control this contextual and customized information.

- *Active users*. There are evidences that the tendency towards more and better "free services" will be growing over time. Also, the evolution of users towards "prosumers" (consumers and producers of new content and applications) is seen as a major trend that will result in fundamental re-definition of content creation. This trend is to be encouraged and new tools shall be developed to further empower user and communities of users.

- *User experience*. There is a need to develop new ergonomic interfaces and advanced interaction mechanisms including multimodality, based on evolution from existing solutions to improve the user experience. Also semantic combination and adaptation of information from different sources (resulting from conscious user preferences and selection) into useful piece of information for the user as well as combining user interfaces constitute relevant research areas.

2.2 Internet of Contents and Knowledge

This broad area relates to the generation and processing of content and the transformation to that content into useful information. It also includes the aspects regarding the user and its characterization and relationships between user and content. In this area, the main challenges are:

- *Digital Content* – 'Content' refers to the 'understandable information made available to a user at any stage of the value chain', including both the 'essence' – the data representing text, audiovisual services, games programs etc. that is the object of the value chain – as well as the metadata that describes the essence and allows it to be searched, routed, processed, selected, and consumed. 'Content' thus goes well beyond the products of the traditional media industries such as broadcasting and computer games. Until recently, content creation was the preserve of professionals, and was very much a craft process. In future, content will be much more widely produced, and the production industry will have to evolve to reflect this change.

  The ***main challenges*** are the design of media content by professionals and non-professionals supported by open tools for content creation, storage, representation, and indexing ensuring interoperability of various content formats, including efficient search and selection engines, and creation of new innovative media applications.

- *Distributed Media Applications* – Prosumers will play a leading role allow for an automated selection without need to care anymore how recipients are going to access the produced content. Although professional content production is expected to keep its attractiveness, the traditional distinction between the creator or producer and the end-user or consumer will change radically: content will come from any user. To take some examples from today's applications, a 'user' might be a private individual sharing photos, a recreational music producer, an originator of a semi-professional video, or a specialized branch news agency. New techniques are required to will also allow new groups to form, defined by their media interests. They will be able to create their own scheduled events – created by an individual member of the group, or collaboratively – and to interact as a group to participate in them and to discuss them, wherever the members are. In such groups, interaction and communication generally will melt together as an integral part of media.

The *main challenges* are the realization of integrated multi-content communications, integration of classical and new media applications, and creation or adaptation of content dedicated to specific user groups, supported by novel open software and tools for integration of multimedia communications applications.

- *New User Devices and Terminals* - Users should be able to access services wherever they are, whatever terminal they are using, with seamless handover as they change from one terminal to another. Users cannot expect the same experience, for example, from viewing a football match on a handheld screen as on a fixed HD display, but they should be able to access the service. This will require appropriate coding of content, perhaps hierarchically, so that it can be reproduced appropriately on a wide range of devices, allowing the content creator to offer the same content to a wide range of terminal equipment without further adaptation. Terminals will need middleware – the software that turns a terminal into a platform that can support multiple applications – that can extract the appropriate elements of the signal. In this vision, ad hoc federations of devices self-assemble on demand on the basis of essential components distributed in the near environment, for instance interface devices available in a home or office environment, or worn by the user as accessories and clothing. The corresponding device assemblies might be called "virtual distributed interface devices". Nothing comparable exists today. Some early work is going on in labs, for instance with intelligent devices woven into clothes, or mobile augmented reality with a regular camera phone. Further research should address architectures and interfaces for such classes of devices

  The *main challenges* are associated to advances in integrated, scalable, and modular multi-media devices with auto-configuration and auto-maintenance features and application programming interfaces for new media applications.

2.3 Internet of Things

It consists of the management of information about real world objects and their surroundings provided by a number of sensors and wireless communications devices mounted in different environments, embedded in systems, worn by users or even swallowed. The ambient intelligence paradigm builds upon ubiquitous computing and human-centric computer interaction design and is characterized by systems and technologies that are: embedded, context-aware, personalized, adaptive and anticipatory.

From the technological point of view, the challenge is to handle the large amount of information coming from the things and to combine it to give useful services. As the current network structure is not suited for this exponential traffic growth, there is a need by all the actors to re-think current networking and storage architectures. It will be imperative to find novel ways and mechanisms to find, fetch, and transmit data. Distributed, loosely coupled, ad-hoc peer-to-peer architectures connecting smart devices might represent the network of the future. In this context the following elements require specific attention:

- Discovery of sensor data — in time and space
- Communication of sensor data: Complex Queries (synchronous), Publish/Subscribe (asynchronous)
- Processing of great variety of sensor data streams
- In-network processing of sensor data: correlation, aggregation, filtering

Another major technological (in relation with the ethical and societal dimension) is striking the right balance between **privacy and security**. While in many cases the security has been done as an add-on feature, it is the feeling that the public acceptance for the Internet of things will happen only when the strong security and privacy solutions are in place. The simple observation of what already happened in the pioneer applications of the retail industry, where consumers' group blocked the adoption of electronic tags, clearly shows that there is a need of huge progress in both technology and instruction.

Non-technological challenges shall also be recognized in the context of the Internet of Things:

- "**Digital divide between things**" with the risk of separating even more the rich areas and people of our planet to the poorest ones. While some humans will still be in condition of hunger and live in famine and illness, some other might enjoy unprecedented "computer-assisted pamper", concentrating only on the activities they enjoy, and leaving behind all the small, tedious matters that compose our daily life. Even in rich areas, efficiency may (and probably will) create redundancy; new business models may overthrow traditionally strong enterprises. Monolithic corporations may crumble into networks of peers, and trusts and monopolies can emerge from the most successful actors in a sector. The legal framework regarding privacy and security must adapt to a new reality. New social networks and organized sub-groups may renew the democracies and challenge existing power structures.

- **Governance:** One major challenge for the widespread adoption of the Internet of Things is the absence of governance. Without an authority, similar to the one that is governing Internet, there are high chances that it will be impossible to have a truly global "internet of things". What could be the governance of the Internet of things, and how different should it be from the governance of today's Internet? It remains an open question if it should be a state-led agency, or a group under the supervision of the United Nations, or an industrial consortium. The guidance of the EU can be crucial to stimulate the emergence of open, global governance.

2.4 Internet of Services

The Future Internet will not only allow access to services based on technical characteristics such as IP-location or web service identifiers but also based on contextual information (e.g. using geographical context or business context). Services can be searched, identified and composed into business process components. This will allow business processes to be flexibly adapted ("**Internet of Services**"). Service consumers look for the "Perfect interactivity". With "perfect" we mean here ***permanent*** (i.e. an interactivity that has no time limits), ***transparent*** (i.e. the service consumer is only concentrated on the benefits of the service he/she is using), ***seamless*** (i.e., supporting mobility of users across different devices without interruption), ***context-aware*** (i.e. the interaction gets adapted to context in its widest sense, including characteristics of devices, location, user preferences or social networks the user belong to), ***empowering*** (i.e., users are enable to self-configure the way they want to get access to services) and ***trustworthy*** (i.e., users feel confident that their interaction with services is safe).

The term services would include a broad variety of applications that will run over a service-aware made up of elements for which further research is needed:

- *Cloud computing* deals with the virtualization of services through more flexible and granular optimization of processing and storage resources, providing applications the necessary runtime support to be provided "as a service" without no limitations of scale in number of users accessing or the amount of resources consumed, all this while complying with the terms of subscribed Service Level Agreements (SLA). This "on the cloud" support will be used by enterprises in a cost-effective manner, using on-demand provisioning and offering flexible and innovative billing and service revenue models which rely on dynamic and intelligent accounting.

- *Open Service Platforms* aim at overcoming incoherent standards, architectures and deployed service platforms exist in the Internet. In order to progress towards a coherent "Internet of Services", significant advances need to be made on the interoperability of platforms, their components, core services, APIs and related open standards. In addition, most of today's Internet service platforms are *closed* in the sense that they only offer a minimal service interface to the outer world. *Open* service platforms of the Future Internet will however allow user-designed components and services to be deployed within the platform and therefore lead to intense co-creation involving end users, since they will be able to develop powerful and highly individual services with minimal configuration or programming effort.

- *Autonomic computing*: aims at creating computer systems capable of self-management, to overcome the rapidly growing complexity of computing systems management, and to reduce the barrier that that complexity poses to further growth. A general problem of modern distributed computing systems, which has to be considered, is that their complexity, and in particular, the complexity of their management, is becoming a significant limiting factor in their further development. Autonomic computing has to solve the problem of large companies and institutions employing large-scale computer networks for communication and computation. The distributed applications running on these computer networks are diverse and deal with many different tasks, ranging from internal control processes to presenting web content and to customer support.

- *Green IT:* the need for optimized consumption and efficiency of future platforms is also a significant challenge in the development of new platforms. Indeed, service facilities or data centers concentrate 23% of the overall ICT CO2 emissions[7] and are estimated to consume, just to mention some examples, between 2.2 - 3.3% of the UK's total electricity, 2% of the electricity in the Netherlands, and around 1.6% of Germany's electricity[8].

[7] Gartner Inc., "Gartner Says Data Centres Account for 23 Per Cent of Global ICT CO2 Emissions" (Press release), http://www.gartner.com/it/page.jsp?id=530912, Oct. 2007.

[8] European Information & Communications Technology Industry Association (EICTA), "High Tech: Low Carbon: The role of the European digital technology industry in tackling climate change", http://www.eicta.org/web/news/telecharger.php?iddoc=762, Apr. 2008.

Working Document: Future Internet - Architectural Vision

This working document details our initial thoughts on the functional and the architectural properties that should be met by the Future Internet.

1. Future Internet Properties

A number of basic properties can already be found in today's Internet and are to be carried forward as they have proven their effective support of the basic requirements found in common usage. These properties include forwarding, routing, encapsulation, tunneling and so forth. In the following, mainly additional properties are addressed, although some overlap with today's function can also be observed.

1.1 Functional

Considering the multifaceted requirements facing the Future Internet, individual demands should be fulfilled enjoying the scale and scope effects following from a common network. These go across all the areas described in Section 4.1. Although without implying prioritization, the functional properties of the FI shall include:

- Accountability
- Security
- Privacy
- Availability (maintainability and reliability)
- Manageability, and diagnosability (root cause detection and analysis)
- Mobility, and nomadicity
- Accessibility
- Openness
- Transparency (the end-user/application is only concerned with the end-to-end service, in the current Internet this service is the connectivity)
- Neutrality

Note: seamless persvasivity and interactivity shall be further detailed (they seem to be not atomic properties)

1.2 Architecture

The architectural properties of the FI shall include:

- Distributed, automated, and autonomy (organic deployment)
- Scalability (e.g. routing scalability -> log(n) where n is the number of nodes and computational scalability i.e. to allow support of any business size)
- Resiliency and survivability
- Robustness/stability
- Genericity (e.g. support multiple traffic (streams, messages, etc.), independent of infrastructure partitioning/divisions, device/system independent)
- Flexibility (e.g. support multiple socio-economic models, and operational models)
- Simplicity
- Evolvability: evolutionability and extendability
- Heterogeneity (e.g. wireline and wireless access technologies,)
- Carbon neutrality

Besides the functional and architectural aspects by themselves, there are also several requirements that the Future Internet should comply with:

- Support for dynamic federation and collaboration for service offerings; this raises the need for publishing and identifying partners to come up with the service offering. This also places requirements related to monitoring and accounting for such dynamic role configurations to effectively work and be profitable.
- Encapsulating off-line and on-line operations; as a result of the vast types of devices as well as user categories, one must support that some devices/services/etc. can be temporarily off-line, e.g. to save power or that links are down.
- Managing risk aspects and evolution incentives; to ensure future evolution, a stepwise approach should be allowed (note: this may come from introducing the virtualization as different “slices” could evolve partly independently).

2. Design Principles

2.1 Current Internet Design Principles

To achieve the Internet design objectives, the following design principles have been used in the current Internet:

- ***Modularization by layering***: the distributed implementation of the Internet across routers and hosts is based upon: i) layers of packet headers, referred to as “encapsulation”, ii) layers of services: a service provided by one layer is based solely on the service provided by the underlying layer. The data passes the network stack at the sender from the top to the bottom and at the receiver from the bottom to the top. The Internet has the following five layers (top to bottom): application, transport, network, link, and physical. The use of layers enables: i) the simple interconnection of existing networks and ii) the accommodation of a variety of networks and services.
- ***Connectionless packet forwarding***: implies that before being exchanged between hosts the data is segmented into packets. Each packet carries the address of its destination and traverses the network independently of the other packets. The forwarding decision is taken per-packet, independently at each hop. Any packet can use the full link bandwidth on any link but may have to wait in a queue if other packets are already using the link. Should a packet traverse a hop with a full queue it is simply dropped, which corresponds to the best effort service principle. This implies also that it is possible to use a stateless forwarding system at the network layer, which does not require per connection state. This ensures scalability and contributes to cost effectiveness[9].
- ***Network of collaborating networks*** (Interconnection via gateways): routers provide for the inter-connection of network devices of the Internet infrastructure that is sub-divided into a collection of autonomous systems (ASs) managed by an ISP. Within an AS, routing is determined by interior gateway protocols such as OSPF and IS-IS. Inter-domain routing between ASs is controlled by the Border Gateway Protocol (BGP). BGP is a policy-routing protocol, which distributes routing information between routers belonging to different AS. This design of the routing system ensures survivability and allows for distributed management as long as the ISPs collaborate.
- ***End-to-end principle/fate sharing*** combined with intelligent end-systems (user-stateless network): The end-to-end principle is the fundamental principle around which the Internet

[9] Note however that over time this principle has been relaxed to allow e.g. Active Queue Management instead of drop-tail/FIFO queuing. One of the main research challenges is thus into how network layer equipment, in particular routers, can improve performance in the complete range of communication scenarios that exists in the current Internet and that are foreseen in the future Internet without damaging or impacting the stateless forwarding principle?

architecture has been built, that ensures applications to survive partial network failures (design goal 1). The end-to-end principle states "that a mechanism should not be placed in the network if it can be placed at the end node, and that the core of the network should provide a general connectivity service, not one that is tailored to a specific application." The application of the end-to-end arguments results in a network that is transparent and provides for a general transport service capable of supporting many different applications. So, contrary to the telephony networks (PSTN), the Internet is not tailored for any single application, but is designed for generality and evolvability. The end-to-end principle is also guiding placement of functionality inside the network rather than at host/end-systems: if all applications need it, or if a large number of applications benefit from an increase in performance while keeping cost/performance ratio acceptable.

- *Simplicity principle* (Occam's razor principle) also known as the Keep It Simple Stupid (KISS) principle. When applied to packet network architectures, fundamental motivation of this design principle has been enounced by J.Doyle "*The evolution of protocols can lead to a robustness/complexity/fragility spiral where complexity added for robustness also adds new fragilities, which in turn leads to new and thus spiraling complexities*".
- *Loose coupling principle*
- *Locality principle* (local cause(s) shall result in local effects). This principle is the transposition in the communication space of the principle stated by Albert Einstein in his article "Quantum Mechanics and Reality" ("Quanten-Mechanik und Wirklichkeit", Dialectica 2:320-324, 1948). The locality principle also guides design of thrashing-proof, self-regulating and robust virtual systems. The locality principle will be useful wherever there is an advantage in reducing the apparent distance from a process to the information/ data it accesses but also context-aware software. In the latter case, the locality principle will be exploited to infer context and intent by watching sequences of references data objects.

The key issue when designing the FI architecture is to determine which principles shall be revisited and/or deprecated keeping in mind that replacing an existing principle impacts the whole architecture. Hence such effort can never be conducted if not accompanied by a thorough motivation, rationalization and argumentation compared to the existing principles.

2.2 Additional/New Design Principles

Internet design principles are so robust and the invention of new design principles for the Future Internet architecture is not as straightforward as some communities may think.

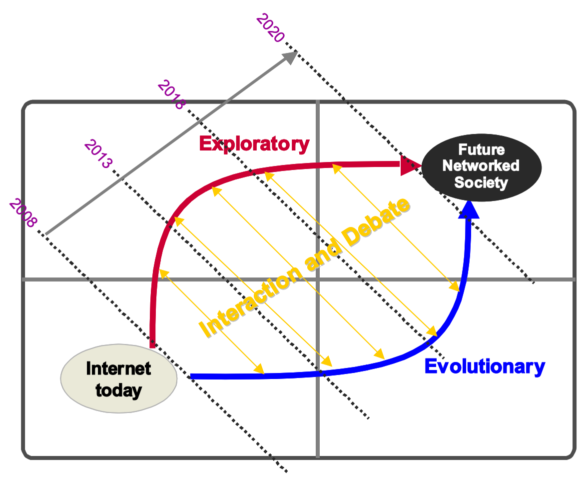
- *Situated and Autonomic*: design principle with which a novel network architecture can be built that enables flexible, dynamic, and autonomic formation of network nodes as well as whole networks. This principle will allow for dynamic adaptation (a.k.a. self-adaptive), re-organization, and re-configuration of the network and underlying systems, according to the network running conditions and state as well as the economical and societal needs of the users.

- *Host-network cooperation*: in order to support application(s)/user needs we can't predict yet (without negatively impacting others), cooperation between the end-user applicative space and the network becomes a key design principle. The end-user applicative space (located at the end-host) receiving feedback information from the network would have the capability to make use of that information so as to better serve its applicative needs - as this feedback information would allow for better decision by the end-user, while improving its empowerment. For this purpose, generic and loosely coupled mediation (between the network and the applicative / end-user space) is required to enable this cooperation in a scalable, distributed and dynamic, reliable, and robust way so as to sustain existing and future application and end-user expectations.

o *Abstraction*: can be considered for increasing scalability by factoring out details of the constituting entities of the system itself. Similarly to object-oriented programming, and instead of system and/or network virtualization, abstracting actions (associated to the control/ processing) and data structures (associated to the informational and message exchanges) would allow offering desired processing and messaging capability without incurring complexity to entities external to the system.

2.3 Analysis

Having identified the Internet functional and architectural properties as well as its design principles the question becomes whether the Future of the Internet shall be built between the “evolutionary approach” and the “clean slate approach” or "revolutionary approach" or "exploratory approach". Both approaches address the same problematic and themes. In the Evolutionary approach, the system is moved from one state to another with incremental updates. This approach builds on the evolution of the current existing Internet to conceive pragmatic & viable solutions for commercial roll-out. The clean-slate approach the system is redesigned from scratch to offer improved abstractions and/or performance, while providing similar functionality based on new core principles. This approach works from clean-slate to eliminate legacy Internet design constraints. Both approaches will target the same usage vision and will have to be synchronized on phased agendas.



Note: dates are indicative of timeframe

Fig.1: Exploratory and Evolutionary approach.

Evolutionary approach (Figure 1): no architectural breakthrough (innovation in context of current Internet architecture)

- Non-disruptive evolution of current architecture & technologies (maintaining the present network design and principles while resolving the specific gaps like trust, security, mobility, etc.)
- Future Internet challenges may be addressed modularly.
- Certain level of backward compatibility (at design phase) while improving the linking technology with new traffic and routing algorithms and protocols advancement to avoid traffic congestions.
- Deployability taking into account the current Internet conditions and constraints (at least partially) so enabling a migration path. Example: critical migration to IPv6 to solve the addressing space problem and / or massively deployment of NAT boxes for IP sharing.

Clean-slate approach (Figure 1): architectural breakthrough (referred to as clean-slate)

- Define a new Internet architecture from scratch that would provide for a better global solution (addressing Future Internet challenges as a bundle)
- Disruptive innovation not impacted by existing install base/technologies
- Feasability in the context of large-scale experimental facilities
- Development of new networking concepts that will arise from the perspectives of new business models, service architectures, application procedures and new technology implementations.

The EIFFEL think tank concluded that both approaches are needed from an investigation perspective. Still, the need for cooperative debates between the various approaches and activities was also identified as fundamental in the process of bringing the current Internet towards to Future Networked Society. The intention is thus to open work in this field along several technological paths and (r)evolution strategies, but in a coordinated manner with “disruption” not being measured in technological terms, but rather from the point of view of business models, applications, and new industrial structures that may eventually emerge.

Also, there is the need to separate clean slate research from clean slate deployment. Clean slate research is important in order to pursue research that is unbiased, not taking into of account preconditions of current Internet - a way of thinking out of the box! The research results will however, have to be applied to the current Internet, if commercially viable, and a migration approach will have to be devised. We should expect a number of results that should be possible to apply to the current Internet and the figure illustrates this. Indeed, since the current Internet has grown to become so big (about 1.5 billions users currently and still quickly growing) it will be commercially very difficult to replace the Internet by “a clean slate deployment”.

There are several possible trajectories for the development of Internet, among which:

i) *By incremental evolution*: evolve the current Internet by incremental evolution by adding (or removing) functionality without changing the prevailing design principles and model. This is the approach that has been followed so far to evolve the Internet and mostly reactively.
ii) *By applying virtualization*: either by enabling logically independent networks built on a common physical infrastructure for deploying new network functionalities and protocols but also providing specialized networks or by building overlays (or underlay techniques) running new protocols on top of (or below) TCP/IP. Nevertheless, there is no proof so far that virtualization (that relies on the indirection principle) is resolving any of the FI technological challenges. Indeed, as enounced by D.Wheeler, "*Any problem in computer science can be solved with another layer of indirection. But that usually will create another problem*." In the present cases, there is no definitive answer concerning negative impact that would result from the introduction of this new level of indirection.

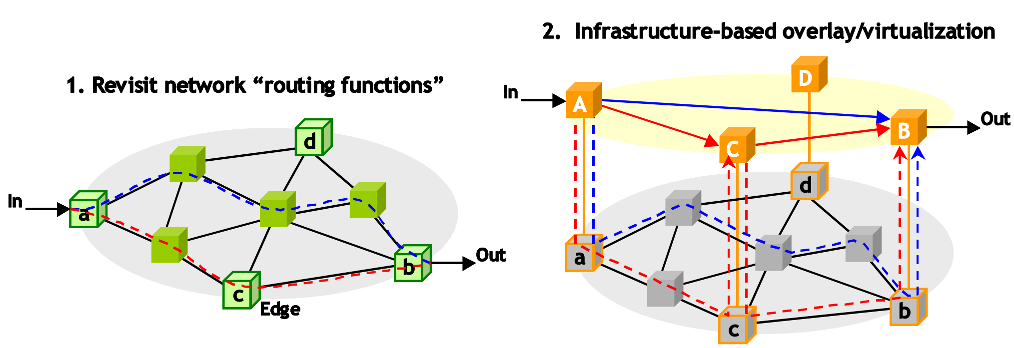


Fig.2. Native vs overlay routing

There is no definitive answer concerning negative impact that would result from the introduction of this new level of indirection. Indeed, additional level of indirection based on overlay and/or network virtualization benefits from customization and independence but also results in side effects such as

- Change properties in one or more areas of underlying network (in part. edges)
- Horizontal and vertical cross-layer conflicting interactions impacting overall network performance (amplified by selfish routing)
- Scalability, stability/convergence, security, etc.

As such performing dynamic routing at both layers (overlay and native IP layers, see Figure 2) leads to conflicting cross-layer interactions due to

- Functional overlap (unintended interactions/interferences)
- Vertical: mismatch/conflict in (re-)routing objectives
- Horizontal: contention for limited physical resources (race conditions & load oscillations)

Complex cross-layer interactions are amplified by

- Selfish routing where individual user/overlay controls routing of infinitesimal amount of traffic to optimize its own performance without considering system-wide criteria
- Lack of information about other layer(s) leading to uninformed optimizations leading to loose-loose situation

Hence, the need to overcome degradation of overall network performance.

3. Architectural Framework

In designing the future Internet, one key issue is how to enable appropriate inter-networking among today's communication networks including wireless/wireline access, and core networks. This leads to an architectural challenge encompassing the logical network architecture, the node/system architecture, as well as the protocols architecture.

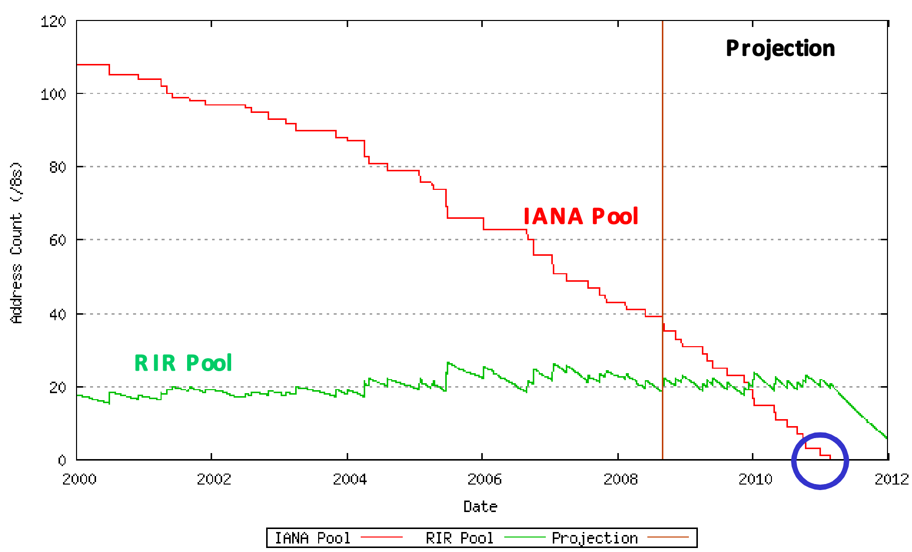


Fig.3. Projected RIR and IANA Consumption (/8s).
Source: http://www.potaroo.net/tools/ipv4/

3.1 Models

The Internet was originally conceived using an ***hour-glass model*** that depicts the protocol stack as a narrow-necked hourglass, with all upper layers riding over a single IP protocol, which itself rides over a variety of hardware layers. This model is currently questioned / challenged - for good and bad reasons / motivations. Analysis has demonstrated how additions such as NAT, firewalls, multi-homing, non-compatibility of IPv6 and IPv4, etc. have transformed the narrow-waist hour-glass model. Nevertheless, NO alternative or new model is currently known that would overcome current Internet design model limitations and provide for a sustainable network infrastructure whose cost/gain and cost/performance ratios significantly (at least one order of magnitude) higher than the current model.

It is representative here to draw a parallel with IPv6 evolution. Presented initially as new architectural model of the Internet more than a decade ago, IPv6 turned over time to become as of today just a mean to overcome the IPv4 address space exhaustion (as depicted in Fig.3). The Internet Assigned Numbers Authority (IANA) unallocated address pool exhaustion is expected by end-2010. As a consequence, no further addresses will be available in the IANA unallocated pool to replenish the Regional Internet Registries (RIRs). So, ISPs that receive addresses from the RIRs pool will not have enough IPv4 space to give one IPv4 address to each consumer CPE for IPv4 connectivity.

3.2 Components

This section addresses the evolution of i) the network entities and system components of the common infrastructure, ii) the applicative components, their distribution, etc. iii) the user space/consumer components (today mainly computers and handsets).

3.2.1 Network entities and system components

This section outlines the ***additional*** network architectural and system components of the Future Internet.

The (current) Internet infrastructure is an interconnected set of (heterogeneous) networks architected around a distributed routing system partitioned into autonomous systems (AS) that are independently administrated. The Internet includes two classes of devices: user devices/hosts, and routers that compose the Internet infrastructure (access/edge and core). Routers are structured around a routing and a forwarding engine (and a management agent). The function of the routing engine is to process routing information (exchanged between routers using a routing protocols such as BGP) so as to compute and select routes that are stored in routing information bases (RIB)[10] and that are composed by a destination, a next-hop interface, and a metric. Routing entries are subsequently populating the forwarding information base (FIB) whose entries are used by the forwarding engine. The function of the forwarding engine is to transfer incoming traffic to an outgoing interface directed towards a router closer to the traffic destination by performing a longest match prefix lookup using the incoming traffic destination address. The forwarding process is connectionless implying that at each hop the forwarding decision is taken independently for each datagram. Basically, forwarding and routing components will remain in the Future Internet context even if new routing paradigms could replace existing shortest path routing (e.g. compact routing).

Cognitive component: Augmenting the existing Internet system and network lower-level data collection and decision making, with a cognitive component enables the Internet infrastructure to learn about its own behavior and environment over time in order to better analyze problems, to tune its operation, and to enforce its decisions on manageability, security, availability, and accountability, to better satisfy end-users. Thus, the introduction of a cognitive component

[10] RIB are also often referred to as routing table (RT)

provides the lower level mechanisms and means by which the Internet would resolve any new challenges that result from its evolution: a growing end-user basis with higher heterogeneity in their needs, and a wider utilization for which the Internet was not initially designed.

Situation awareness components provide for the perception of conditions within and surrounding an actor, the inference of information relevant for the actors' goal and the prediction of potential future events. In communication networks, situation awareness is a pre-requisite to make sound decisions for achieving self-organization. Within a network situation awareness is established on one hand by observing and analyzing network node behavior and information flows in the direct neighborhood of an entity. On the other hand, cooperation is necessary to provide information on remote events. The situational view provides the basis to decide, based on the current state of the network. The analysis of information improves the situational view step by step. If perfect situation awareness is achieved i.e. all the important factors for autonomic decisions are known and processed with respect to the decision-makers goal, then, the decision is evident. Nevertheless, this ideal case is usually not achievable due to missing information, resource or time constraints.

Usually it is necessary to make decisions without perfect situation awareness, i.e. with some degree of uncertainty about the situation, in order to invoke actions in time. Future networks need to include methods to achieve situation awareness and to deal with decision-making in uncertainty. A general framework for situation awareness in Future Internet has to include methods for

- Achieving resource efficiency which result in trade-off between performance and flexibility / re-configurability. As data selection and statistical estimation techniques substitutes exact observations by an estimate requires in turn accuracy statements in order to assess the estimation error. This is no trivial task as the accuracy often depends on the network traffic dynamicity and variability.
- Providing flexibility with regard to viewpoints is extremely valuable for establishing situation awareness. In order to generate a good representation of the current situation, it is useful to have the option of zooming in or out. Obtaining such representation can be achieved by providing adaptive observation techniques that are controlled by the decision process.
- Respecting privacy concerns often contradicts required actions to achieve situation awareness. Therefore, decision algorithms that can work with anonymous, aggregated or sampled data provide a clear advantage.
- Cooperating with other nodes and services: since sharing information is the prerequisite for learning from others, the future Internet should include techniques that help network nodes and services to cooperate. There exist a variety of cooperation strategies that could be applied and extended for the need of decision making within future networks.

Specialized hardware and the optimization of algorithms is useful for coping with resource constraints, but it has limitations. Algorithms implemented in hardware often lack the flexibility and re-configurability that software-based solutions can offer.

Autonomic components provide for fully distributed self-configuration & organization, self-healing, self-protection, and self-optimization functionality. The objective of self-organizing communication network (concept and technology) is to be situated in multiple and dynamic contexts, that is task- and knowledge-driven, and fully scalable. Four functional components are defined:

- Self-Configuration: Automatic configuration of components
- Self-Healing: Automatic discovery, and correction of faults
- Self-Optimization: Automatic monitoring and control of resources to ensure the optimal functioning with respect to the defined requirements
- Self-Protection: Proactive identification and protection from arbitrary attacks

A pre-requisite for integrating autonomic components as part of the Future Internet infrastructure implies analyzing traffic in combination with network events / status and to achieve situation awareness. It is crucial to know about the network status in order to detect that something unusual happens in the network (e.g. overload, unavailability of services, etc.). Based on detailed information counteractions can be planned and executed. Without knowledge about the situation no sound decisions about future actions can be made. But establishing situation awareness itself is not a trivial task and has many challenges that need to be considered during its design. The problems that have to be addressed are:

- High dynamic and unpredictability of network events
- Resource limitations
- Synchronization of observations
- Privacy protection

Network events are extremely dynamic and difficult to be perceived, interfered or predicted. Hence the view of the situation needs to be constantly updated. The goal of gaining a complete picture of the network, and be able to process it, is simply utopic: observe every packet, at every network node, and fully analyze it. Subsequently, it would be possible to, e.g. redirect the traffic to avoid congestion or detect even sophisticated application-level attacks. However, this requires at the very minimum equal processing powers as for the normal network operation. Therefore, one shall assume that it is not possible (nor desirable) to observe everything everywhere in (future) networks. On the other hand, privacy concerns also contract a concept based on in depth observations: users do not want to reveal too much information about themselves. Providers are reluctant and often prohibited by law to share captured data.

The role of the ***packet-switching component*** resulting from the emergence of packet technologies in transport networks (the so-called packetisation of transport networks) and their possible influence on the Future Internet architecture, i.e. the general function split and interworking between the lower layers (physical and data link) and the networking layer (IP, IP/MPLS). By virtue of forthcoming control plane technologies as well as multi-domain and multi-layer capabilities, the transport network is progressively evolving into a more flexible and fully featured packet-switching layer beneath the Internet IP networking layer. Cost-efficiency requirements, however, render the co-existence of two fully-fledged packet layers, which are operated concurrently, a critical issue. Therefore, the possible functional split between the IP/networking layer and the underlying packet transport layer(s) becomes a crucial topic.

3.2.2 Applicative and Service Components

The applicative and service components are numerous and of diverse natures, in particular:

Service Delivery Platforms: The present concept of global Service Delivery Platform (SDP) should go beyond the client service model to support mechanisms of global service supply where third parties will have the capability to aggregate services, act as intermediaries for service delivery and provide new channels. In fact, SDP should evolve to become Service Delivery Frameworks (SDF) and services should evolve to provide not only functional but also management interfaces, which allow their management across domains. SDFs provide the framework to manage end to end the service lifecycle across domains. SDFs extend management processes across SDPs of different Service Providers. SDFs enable the birth of open markets of services in Internet (where a Service Provider can syndicate its services to other SDFs of other Service Providers to be reused, traded without loss of control of the customer experience).

Extending Service Oriented Architecture: The open platform will be extended to include SOA (Service Oriented Architecture) for value added services. Semantics is a very good tool to enhance service descriptions allowing automatic composition.

Even Driven Architecture will complement SOA in customized complex services, creating added value complex services for sensing and reacting to situations typical of compliance, logistics and finance services. This tendency of incorporating new functionalities as required by the applications will lead to the new SOA/Web 3.0 that will include new features that have to be fully developed and used:

- SOA for things
- Indexing of internal applications
- Semantic services
- Automatic behavior

The above mentioned vast amount of information, coupled with the incorporation of data coming from the huge amount of sensors being deployed (the "sensor web") will preclude human processing; therefore at the application space, it is increasingly becoming a game of machine-to-machine communication. A great share of the future Web will consist of systems talking to systems, not to humans.

3.2.3 User/Community/Prosumer Space Components

Future Internet systems will allow people to seamless request and provide services in a much more symmetrical and de-centralized way that today's systems. People, and even autonomous systems, will progressively become active service creators and knowledge providers for other people or for the network itself. Service front-ends and interaction systems are key components not only for the wider acceptance, adoption and experience of services, but as a driver to help people to move into the core of e-service provision. Recent trends show the major impact of user-generated information and media in society. The global trend is to empower people with the tools to create and personalize media, devices and functionality. New full lifecycle service front-ends and components are then required to drive open and inexpensive e-services. These new components should be capable to empower users, even non-technically skilled, to use, customize, contribute, enhance and compose services.

With this vision, traditional end-terminals, i.e., those communication devices carried (or used) by people, will become fully multimedia assistants that can operate either at the end of the communication chain or just in the middle, as both network and knowledge service resources. Service front-end components will have the property of being independent of any specific device or operation mode. At the device side, these components detect and manipulate contextual information and exploit people's knowledge and collective intelligence.

3.2.4 Internet of Things Components

The enablers for what concerns the Internet of Things are numerous and of diverse natures, in particular:

Energy: Energy issues such as energy harvesting and low-power chipsets are central to the development of the IoT. On-going research regarding high efficiency energy storage devices such as nano-batteries, fuel cells, and printed/polymer batteries, as well as new energy generation devices coupling energy transmission methods or energy harvesting using energy conversion will be the key factors for implementing autonomous wireless smart systems.

Intelligence: Capabilities such as context awareness and inter-machine communication are considered a high priority for the IoT. Additional priorities are the integration of memory and processing power, the capacity of resisting harsh environments, and an affordable security. Furthermore, the development of ultra low power processors/microcontrollers cores designed specifically for mobile IoT devices and a new class of simple and affordable IoT-centric smart systems will be an enabling factor.

Communication: New, smart multi frequency band antennas, integrated on-chip and made of new materials are the communication means that will enable the devices to communicate. On-chip antennas, optimized for size, cost and efficiency, will come in various forms like coil on chip, printed antennas, embedded antennas, and multiple antenna using different substrates and 3D structures. Modulation schemes and transmission speed are also important issues to be tackled allowing multi-frequency energy efficient communication protocols and transmission rates. The communication protocols will be designed for Service-Oriented Architectures of the Internet of Things platform

Integration: Integration of smart devices into packaging, or better, into the products themselves will allow a significant cost saving and increase the eco-friendliness of products. The use of integration of chips and antennas into non-standard substrates like textiles and paper, and the development of new substrates, conducting paths and bonding materials adequate for harsh environments and for ecologically sound disposal will continue. System-in-Package (SiP) technology allows flexible and 3D integration of different elements such as antennas, sensors, active and passive components into the packaging, improving performance and reducing the tag cost. RFID inlays with a strap coupling structure are used to connect the integrated circuit chip and antenna in order to produce a variety of shapes and sizes of labels, instead of direct mounting.

4. Operational Impact

The operational impact in terms of migration and operational cost (knowing that manageability, diagnosability, and maintainability are key challenges for service providers) is a research topic/challenge on its own.

5. Learning from Experience

5.1 Assessment of Future Internet Solutions

Even if a new clean slate design will provide the basis of the future Internet, the Internet will continue evolving. Therefore adaptation and learning techniques will play a central role in future Internet design and in the provisioning of self-x capabilities. This provides a challenging task when trying to assess and compare different solutions.

In contrast to classical conformance or performance tests that consider specification, implementation and current environment of the system under test, the assessment of systems with learning components have to take the knowledge into account that was gained by the system. This increases the complexity of evaluation and comparison of such systems.

The new assessment group within the AC Forum wants to address these problems and wants to work on an AC Assessment framework that helps to evaluate new concepts. They distinguish traditional, autonomic and cognitive systems. Traditional systems can be assessed by state of the art testing methods.

- Autonomic systems include adaptive components, which react with the application of pre-defined algorithms to pre-defined policies. The correct operation of the adaptation can be checked by considering the state of the adaptation process during testing. Metrics for evaluation of such systems include the time to adapt, adaptation errors, etc.

- Cognitive systems include learning behavior. Learning means that new algorithms can be detected and applied and the policies for adaptation itself are altered during operation. Assessment metrics for such systems have to include time to learn, cost of learning, etc. In order to assess these key parameters, the systems needs to run through a well-defined process, where knowledge is stepwise increased by providing information and by the learning process.

5.2 Experimentation

Cross-disciplinary research resulting from this architectural vision shall also lead to practical and palatable realizations (experimental, industrial, and not just paperwork.).

Cross-disciplinary research resulting from this architectural vision shall also lead to practical and palatable realizations (experimental, industrial, etc.) and not limited to theoretical research without any actual feasibility consideration. The FIRE (Future Internet Research and Experimentation) European initiative should be pursued and extended to address those needs, gearing itself towards creating a multi-disciplinary research environment for investigating and experimentally validating highly innovative and revolutionary ideas for new networking and service paradigms. It should also federate national and regional initiatives which are also needed as they are closer to the end users, by inter-connecting the existing (or being implemented experimentation platforms). The Living Labs label put in place at European level is a well supportive initiative to identifying relevant experimentation platforms.

Role of Experimentation: experimentally driven research is needed to join the two ends between multi-disciplinary, exploratory, and long-term research with technology engineering, large-scale validation, and testing. This has to be built by gradually connecting and federating existing and new testbeds for emerging or future Internet technologies. It should be also an easily accessible and usable mean for SMEs to test their innovation (technology, services) and new usages.