HELSINKI UNIVERSITY OF TECHNOLOGY
Faculty of Electronics, Communications and Automation
Department of Communications and Networking

Tapio Levä

SCENARIO ANALYSIS ON FUTURE INTERNET

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Engineering

Espoo, May 15th, 2009

Supervisor: Professor Heikki Hämmäinen
Instructor: Docent Kalevi Kilkki

HELSINKI UNIVERSITY OF TECHNOLOGY ABSTRACT OF MASTER'S THESIS
Faculty of Electronics, Communications and Automation
Department of Communications and Networking

Author:	Tapio Levä		
Title:	Scenario Analysis on Future Internet		
Date:	May 15th, 2009	**Number of pages:**	6 + 94
Faculty:	Faculty of Electronics, Communications and Automation		
Professorship:	S-38 Networking Technology		
Supervisor:	Professor Heikki Hämmäinen		
Instructor:	Docent Kalevi Kilkki		

The Internet has grown out of its original scope and scale while its importance for the society has increased. Improved awareness of the challenges the Internet is confronting has activated decision-makers around the world, and various initiatives have been established to study the Future Internet. All these research efforts share, however, the same challenge, how to direct the research to the most relevant topics. This thesis eases the problem through scenarios which disclose the most significant trends and uncertainties having impact on Internet evolution for 10 years from now.

Before looking to the future, the historical milestones and current situation of the Internet ecosystem are studied based on various written sources. With the help of ideas and information gathered from brainstorming sessions and expert interviews, four alternative evolution scenarios for the Internet are developed by using Schoemaker's scenario planning method. Use of PEST framework in identifying key trends and key uncertainties ensures that all the important macro-environmental factors affecting the Future Internet are taken into account. Finally, the scenarios are used in analyzing the research strategy of the Finnish Future Internet program.

The scenarios show that the challenges the Internet is facing can be solved in various ways which lead to different network and business architectures. Differences between the scenarios concerning the power relationships and value distribution between stakeholders reveal the underlying tensions and differing interests of stakeholders. Strategic analysis suggests that deployment of new solutions needs to be planned carefully already from the beginning. Overall, the results are valuable in guiding the discussion about the Future Internet.

Keywords: Internet; scenario analysis; network architecture; value distribution

TEKNILLINEN KORKEAKOULU DIPLOMITYÖN TIIVISTELMÄ
Elektroniikan, tietoliikenteen ja automaation tiedekunta
Tietoliikenne- ja tietoverkkotekniikan laitos

Tekijä:	Tapio Levä		
Otsikko:	Skenaarioanalyysi tulevaisuuden Internetistä		
Päiväys:	15.5.2009	**Sivumäärä:**	6 + 94
Tiedekunta:	Elektroniikan, tietoliikenteen ja automaation tiedekunta		
Professuuri:	S-38 Tietoverkkotekniikka		
Valvoja:	Professori Heikki Hämmäinen		
Ohjaaja:	Dosentti Kalevi Kilkki		

Internet on kasvanut ulos alkuperäisistä raameistaan, samalla kun sen yhteiskunnallinen merkitys on kasvanut. Parantunut tietoisuus Internetin kohtaamista haasteista on aktivoinut päätöksentekijät ympäri maailmaa, ja lukuisia hankkeita on perustettu tutkimaan tulevaisuuden Internetiä. Kaikilla tutkimusprojekteilla on kuitenkin haasteena, miten suunnata tutkimus tärkeimpiin asioihin. Tämä diplomityö helpottaa ongelmaa skenaarioiden avulla, jotka tuovat esille Internetin evoluutioon seuraavan kymmenen vuoden aikana vaikuttavat merkittävimmät trendit ja epävarmuudet.

Ennen tulevaisuuden tutkimista perehdytään Internetin historiallisiin virstanpylväisiin ja nykytilanteeseen kirjallisuustutkimuksen keinoin. Aivoriihissä ja asiantuntijahaastatteluissa kerättyjen ajatusten ja tietojen avulla luodaan neljä vaihtoehtoista Internetin evoluutioskenaariota käyttämällä Schoemakerin menetelmää. PEST-mallin käyttö trendien ja epävarmuuksien tunnistamisessa varmistaa, että kaikki tärkeät Internetin makroympäristön tekijät huomioidaan. Lopuksi skenaarioita käytetään analysoitaessa suomalaisen Tulevaisuuden Internet –tutkimusohjelman tutkimusstrategiaa.

Skenaariot esittävät, että Internetin kohtaamat haasteet voidaan ratkaista monella tavalla, jotka johtavat erilaisiin verkko- ja liiketoiminta-arkkitehtuureihin. Skenaarioiden väliset erot sidosryhmien voimasuhteissa ja arvonjakautumisessa kertovat taustalla olevista jännitteistä ja sidosryhmien eriävistä intresseistä. Strateginen analyysi ehdottaa, että uusien ratkaisujen käyttöönotto pitää suunnitella huolellisesti alusta alkaen. Kaiken kaikkiaan tulokset ovat arvokkaita, sillä ne ohjaavat keskustelua tulevaisuuden Internetistä.

Avainsanat: Internet; skenaarioanalyysi; verkkoarkkitehtuuri; arvon jakautuminen

Preface

This Master's Thesis has been written as a partial fulfillment for the Master of Science degree in Helsinki University of Technology. The work has been carried out between June 2008 and May 2009 at the Department of Communications and Networking as a deliverable for the Future Internet program of Tivit (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT), funded by the Finnish Funding Agency for Technology and Innovation (Tekes), and coordinated within the Econ@Tel (COST605) network.

I wish to express my gratitude to the people who have supported me in this work. First of all, I would like to thank Professor Heikki Hämmäinen for the opportunity to write this thesis in his team and for his extensive guidance and insights throughout the research process. I am grateful to Kalevi Kilkki for valuable advices during the writing process. I also thank my other co-workers in the Networking Business team, as well as the Future Internet program partners and fellow researchers. Without the contribution and enthusiasm of the interviewees and the participants of the brainstorming sessions this research would not have been possible. Thus I owe an especially large word of thanks to the experts for their comments and opinions.

Without my family, fellow students and friends it would have been much harder to get here. Special thanks to my dearest, Hanna, for the strength and wisdom you gave me during the course of my work.

Finally, I want to thank my parents, Marja and Jorma, for excellent upbringing and support during my studies.

Espoo, May 15th, 2009

Tapio Levä

Table of contents

List of figures

List of tables

Acronyms and terms

3G	Third Generation
3GPP	the Third Generation Partnership Project
4G	Fourth Generation
Adobe Flash	A multimedia platform used to create animation, advertisements, and various web page components, to integrate video into web pages, and to develop rich Internet applications.
AS	Autonomous System
BGP	Border Gateway Protocol (RFC 4271)
CAIDA	Cooperative Association for Internet Data Analysis
CDN	Content Delivery Network
CERN	Conseil Européen pour la Recherche Nucléaire (European Organization for Nuclear Research)
CIDR	Classless Inter-Domain Routing (RFC 4632)
CSC	IT Center for Science
(D)ARPA	(Defence) Advanced Projects Research Agency
DCCP	Datagram Congestion Control Protocol (RFC 4330)
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DNS	Domain Name System (RFC 1035)
DoS	Denial of Service (attack)
EGP	Exterior Gateway Protocol (RFC 904)
ESP	Encapsulating Security Payload (RFC 4303)
EU	European Union
FDM	Frequency-Division Multiplexing
femtocell	A small cellular base station designed for use in residential or small business environments. It connects to the service provider's network via broadband.
FI	Future Internet
FIA	Future Internet Assembly
FP7	Seventh Framework Programme
FTP	File Transfer Protocol (RFC 959)
GRE	Generic Routing Encapsulation (2784)
GSM	Global System for Mobile communications (originally Groupe Spécial Mobile)
HIIT	Helsinki Institute for Information Technology
HIP	Host Identification Protocol (RFC 4423)
HMTL	Hyper-Text Mark-up Language (RFC 1866)
HTTP	Hyper-Text Transfer Protocol (RFC 2616)

HTTPS	Hyper-Text Transfer Protocol Secure (RFC 2818)
HW	Hardware
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol (TFC 792)
ICT	Information and Communications Technologies
IDN	Internationalized Domain Names
IETF	Internet Engineering Task Force
IGP	Internet Governance Project
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IP	Internet Protocol (RFC 791)
IPR	Intellectual Property Rights
IPsec	Internet Protocol Security (RFC 4301)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	Internet Systems Consortium
ISP	Internet Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
MP3	MPEG-1 Audio Layer 3
NAT	Network Address Translator (RFC 3022)
NIC	Newly Industrialized Country
NSF	National Science Foundation
NCP	Network Control Protocol (RFC 36)
OECD	Organization for Economic Co-operation and Development
P2P	Peer-to-Peer
P2PTV	Peer-to-Peer Television
PEST	Political, Economic, Social, Technological (framework for environmental scanning)
PSTN	Public Switched Telephone Network
QoS	Quality of Service
R&D	Research & Development
RFC	Request For Comments
RSVP	Resource ReSerVation Protocol (RFC 2205)
RTCP	RTP Control Protocol (RFC 3550)
RTP	Real-time Transport Protocol (RFC 3550)
RTSP	Real Time Streaming Protocol (RFC 2326)

SCTP	Stream Control Transmission Protocol (4960)
SIP	Session Initiation Protocol (RFC 3261)
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol (RFC 5321)
SRA	Strategic Research Agenda
SRI	Stanford Research Institute
SSH	Secure Shell (RFC 4251)
SSL	Secure Socket Layer
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats (SWOT Analysis: a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture)
TCP	Transmission Control Protocol (RFC 793)
telco	telephone company
TDM	Time-Division Multiplexing
TLS	Transport Layer Security (RFC 5246)
Ubicomp	Ubiquitous computing
UCLA	University of California
UDP	User Datagram Protocol (RFC 768)
UI	User Interface
UN	United Nations
URI	Universal Resource Identifier (RFC 3986)
URL	Uniform Resource Locator (RFC 1738)
U.S.	United States of America
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WDM	Wavelength-Division Multiplexing
WWW	World Wide Web (also Web and W3)
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

1 Introduction

The importance of the Internet for the society is constantly increasing. In four decades the Internet has grown from a network of computer science researchers to a global backbone of the information society, and currently over one billion people use it to communicate, search and share information, conduct business, and enjoy entertainment. The Internet community lead by IETF (Internet Engineering Task Force) has been remarkably successful in solving scalability bottlenecks caused by novel application requirements and surprising growth in user base. Nevertheless, the Internet and its architectural principles (Carpenter, 1996) were designed in the 1970s mostly for purposes that resemble very little the current and foreseen usage scenarios. Thus the Internet community is questioning the ability of the Internet to cope with the forthcoming challenges.

Increased awareness of the challenges the Internet is confronting and of the possibilities it is offering has activated decision-makers and researchers around the world. Various initiatives for example in Europe, U.S., Japan, and South Korea have been established to study the Future Internet. These research efforts are seen important in the global space but also local interests are high since governments and regions try to maximize their future competitiveness through strategically well-aimed investments to the Future Internet. For example Vivian Reding, European Union Commissioner for information society and media, recently stated that Europe must be a key player in the future of the Internet (Reding, 2009). Consequently the financial investments are high; for instance European Union member states have already committed over €9.1 billion of funding for ICT (Information and Communications Technologies) research (European Commission, 2008).

Investing in the Future Internet contains high level of risks because the researchers are missing the crystal ball that would tell which are the most relevant issues to research. Besides, recognizing the technical shortcomings is not enough since the Internet evolution is affected also by political, economic and social forces that need to be understood so that technical solutions are accepted and adopted successfully.

Additionally, the varying stakeholder interests and incentives as well as the inertia of the Internet caused by its sheer size need to be taken into account when planning the deployment of new technical solutions.

Creating scenarios is one way to deal with the complex uncertainties related to the evolution of the Internet ecosystem. For instance Future Internet Assembly (FIA) has asked its cross-domain working groups to provide scenarios for the Future Internet to direct the discussion and allocate related funding (Silva & Campolargo, 2009). This thesis and its scenario work, for one, are conducted in the frame of the Finnish national Future Internet (FI) program which is aimed to bring together the key research resources to develop Future Internet networking technologies and create new global ICT based business ecosystems. The participants of the project represent broadly the Finnish telecommunications industry landscape including both industrial partners: The Finnish IT center for science (CSC), Ericsson, Nokia, Nokia Siemens Networks, and Sonera; and research partners: Helsinki and Tampere Universities of Technology, Universities of Helsinki and Jyväskylä, Helsinki Institute for Information Technology (HIIT), and VTT Technical Research Centre of Finland. The program is a part of the ICT cluster of the Finnish Strategic Centres for Science, Technology and Innovation (TIVIT / ICT SHOK) funded by the National Technology Agency of Finland (TEKES).

1.1 Research question and objectives

While the Internet is becoming more and more integral part of the society the interest of various stakeholders is increasing. These stakeholders try to get competitive advantage through strategically well-aimed research efforts. However, due to the size and complexity of the Internet ecosystem directing expensive research to the “right” targets is difficult. Thus desire for understanding and bounding the uncertainties relating to the future development of Internet increases. This thesis tries to ease the problem through scenarios which disclose the most significant trends and uncertainties. The main research questions are expressed as follows:

Which are the alternative (technological) scenarios for Internet over 10 years?

What are the key trends and uncertainties that produce these scenarios?

The key stakeholder in this study is the Finnish Future Internet program. The answer to the main research question is used in analyzing the strategic research agenda of the program. This is formulated in a supporting strategic question:

> *What should be the IETF research strategy of TIVIT/FI program to cope with each scenario?*

To make the problem more convenient to handle, a handful of objectives is recognized and achieved during the research:

- Identify historical milestone technologies and link them to IETF RFCs (Request for Comments).
- Identify key trends and uncertainties of the Future Internet evolution by organizing brainstorming sessions and expert interviews.
- Create four scenarios presenting alternative futures.
- Analyze and compare scenarios from the perspective of technical and business architecture, and value distribution.
- Analyze the applicability of the strategic research agenda of Finnish Future Internet program in the scenarios.

1.2 Scope

The research question is quite broad, and some focusing is needed to make the problem more convenient to handle. The most important question is explaining the meaning of the word Internet that is typically defined very vaguely. U.S. Federal Networking Council definition from the year 1995 is used as the basis for our own definition:

> *"Internet refers to the global information system that -- (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP compatible protocols; and (iii) provides or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."* (FNC, 1995)

The two first criteria – IP address space and TCP/IP suite – are purely architectural. The third point considering services presents the usage perspective. In this thesis these both aspects are taken into account. From technical perspective, the scope is only on the IP layer and the layers above that, which means that data link and physical layers are mostly neglected. Likewise, different access methods are not studied in this thesis since the concentration is more on the core network. In addition to a technical point of view, the Internet is also understood as a phenomenon having economic, regulatory and social implications.

The time frame is a ten years period from 2009 to 2018. Although the scenarios are studied in the global space, the strategic implications of resulting scenarios are discussed only from the perspective of the Finnish Future Internet program. The focus of strategic analysis is further limited to research strategy, and especially to IETF work.

1.3 Research methods

The research methods applied in this thesis are

- literature survey,
- brainstorming,
- interviews, and
- analysis based on theoretical frameworks.

Literature survey is used in analyzing the most important historical milestones in the Internet evolution and in getting good understanding of the current state of the Internet ecosystem. The chosen approach is qualitative and written sources include academic publications, IETF RFCs, technical and management books, relevant future forecasts, news articles, and white papers.

After attaining sufficient grounding, brainstorming sessions and interviews are organized to broaden the view. The participants of brainstorming sessions and interviews come from Finnish academia and telecommunications industry, and most of them are closely related to the Finnish Future Internet program. The results from brainstorming and interviews act as the basis during scenario construction and thus have great influence on this thesis. Eventually, few theoretical frameworks are combined with these results and they include

- scenario planning, and
- PEST framework.

1.4 Structure of the thesis

The structure of the thesis is presented in Figure 1.

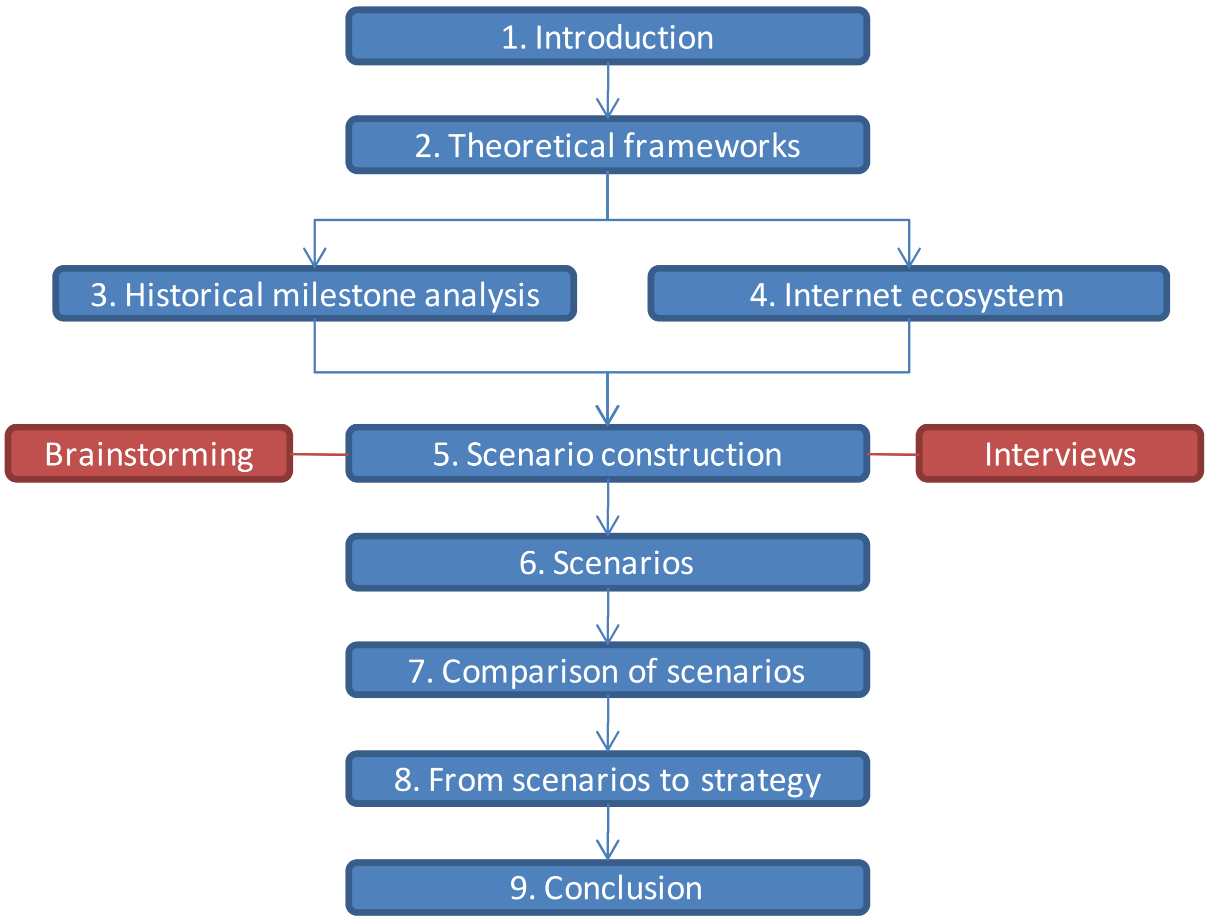

Figure 1: Structure of the thesis

This first chapter introduces the thesis to the reader. Then Chapter 2 explains theoretical frameworks, including the scenario planning method and PEST analysis. Additionally, theory behind brainstorming and interviews as data collection methods is described.

The IETF and RFC-centric view on historical milestones of the Internet is presented in the third chapter and the nature and challenges of the current Internet ecosystem in the fourth chapter.

The process of creating scenarios is presented in Chapter 5. This includes application of research methods (brainstorming and expert interviews) as well as descriptions of the key trends and uncertainties.

Chapters 6 and 7 describe the derived scenarios first one by one and then compared with each other. After that in the eighth chapter, the scenarios are used in analyzing the research strategy of the Finnish Future Internet program.

Finally, Chapter 9 concludes the findings and suggests some topics for further research.

2 Theoretical frameworks

This chapter introduces the theoretical frameworks and research methods that are used in this thesis, and explains how they relate to each other.

2.1 Scenario planning

Scenario planning is an established tool for exploring complex situations with high uncertainty. Modern scenario techniques stem from war game simulations at the Rand Corporation in the 1950s (Schoemaker, 1993). In the 1970s they were used successfully in the petrochemical industry (Wack, 1985) to cope with the oil crisis.

More recently, scenario planning has been used in dealing with high uncertainty of emerging technologies in the ICT field. Karlson et al. (2003) took a holistic view and created four possible scenarios for the evolution of wireless industry from 2003 to 2015. Nordlund et al. (2007) used Karlson et al.'s method to create scenarios for digital home management. Heikkinen (2008ab) has used scenarios to understand the usage of mobile peer-to-peer services. Additionally, Smura and Sorri (2009) have studied the wireless local area access market concentrating on indoor access and especially on rivalry between WLANs (wireless local area networks) and femtocells.

Although practitioners have developed scenario planning to several directions during the past decades (see comparison in Bradfield et al., 2005), they all build on identifying driving forces consisting of both predetermined and uncertain elements. Predetermined elements, often called as trends, describe the collective knowledge of the industry. They do not depend on any particular chain of events nor scenario come to pass, and thus apply in all the scenarios (Schwartz, 1998). Uncertain elements, or simply uncertainties, are forces deemed important but whose outcomes are not very predictable (Schoemaker & Mavaddat, 2000). Thus they can be described as variables or as things "we know we don't know". When uncertainties are studied, the interdependencies and relationships between them are of high importance, since not all combinations may occur. Especially important is finding of the root causes or independent uncertainties that can then be used as basis for separating the scenarios.

Van der Heijden (1996) lists following principles that can be taken as guidelines in scenario planning.

- There has to be at least two scenarios. More than four is often too complex.
- Each scenario must be plausible.
- The scenarios must be internally consistent.
- The scenarios must be relevant to the issues that are being researched.
- The scenarios must provide new ideas and insights usable in strategic planning.

If the scenario planner conforms to these rules, he can freely choose the scenario construction method and presentation format.

From many alternatives, Schoemaker's method was seen as the most suitable one for this study (Schoemaker, 1991, 1993, 1995; Schoemaker & Mavaddat, 2000). Schoemaker (1993) defines scenarios as *"focused descriptions of fundamentally different futures presented in coherent script-like or narrative fashion".* They simplify the avalanche of data into a limited number of possible states (Schoemaker, 1995). Nevertheless, scenarios should not be treated as forecasts but rather as means for bounding and understanding future uncertainties. If successfully used scenario planning can prevent tunnel vision by revealing hidden or weak signals and by stimulating decision makers to consider changes they would otherwise ignore (Schoemaker, 1995).

The ten-step framework presented in (Schoemaker & Mavaddat, 2000) was used although the last two steps requiring quantitative modeling were not carried out. The method is summarized in Figure 2. First, the scene and scope is set by defining time frame, scope and decision variables. Also major stakeholders need to be identified. Second, key trends and uncertainties are identified. Third, four internally consistent and plausible scenarios are constructed based on the most important uncertain elements. Finally, the stakeholder behavior in the resulting scenarios is assessed. After the scenario process is completed the scenarios are typically used in planning strategic actions of a given market player.

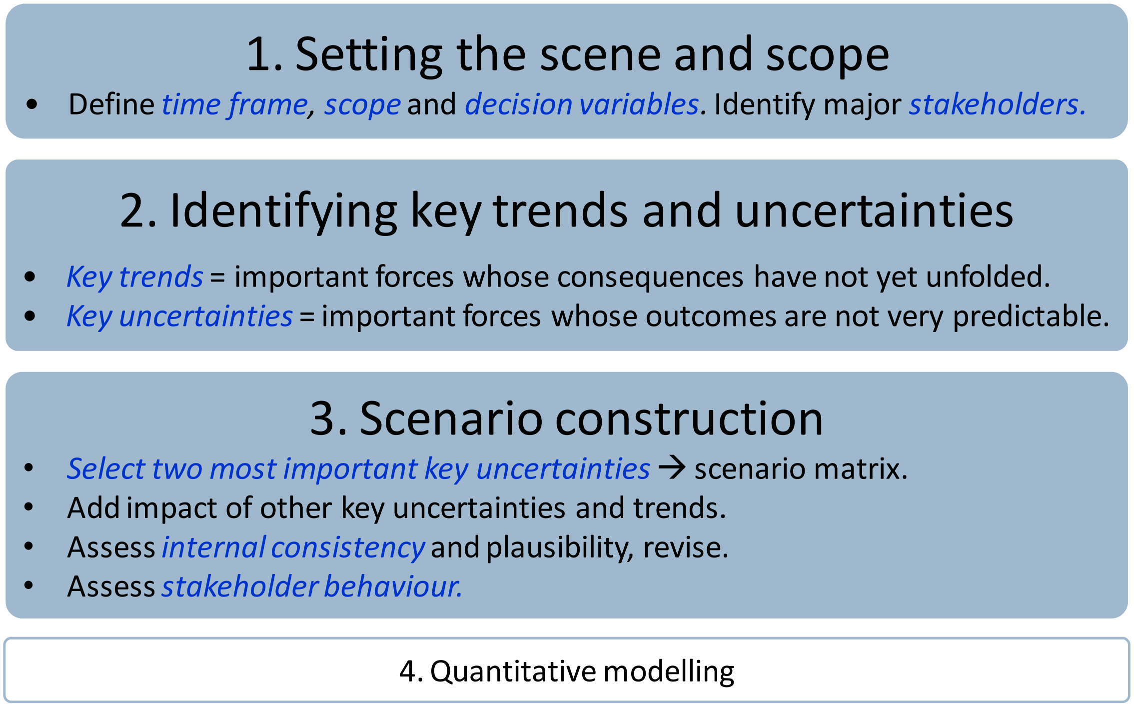

Figure 2: Scenario planning process (Schoemaker, 1993; Schoemaker & Mavaddat, 2000)

2.2 PEST analysis

Acronym PEST stands for Political, Economic, Social and Technological, and describes a framework of macro-environmental factors used in the environmental scanning component of strategic management. The components of the acronym are sometimes reordered to STEP, and also new components like Legal and Environmental are added to form PESTLE.

Tools and techniques for environmental scanning were firstly discussed by Aguilar (1967) who defined it as a process that seeks "*information about events and relationships in a company's outside environment, the knowledge of which would assist top management in its task of charting the company's future course of action*" (Fahey & King, 1977). This external environment can be divided into the operating environment – the suppliers and other interest groups, with which the firm deals, and the general environment – the national and global context of social, political, regulatory, economic and technological conditions (Thomas, 1974). As can be understood, PEST analysis concentrates on the general environment.

In the academic literature environmental scanning and PEST analysis are not widely covered. PEST is mainly taken as a practical tool for the companies' top management to be used for example in conjunction with SWOT analysis to help defining opportunities and threats. Thomas (1974) describes the situation by saying that the idea of taking PEST factors into account is *"somewhat in the nature of conventional wisdom"*, and that PEST conditions are *"almost ritually invoked in planning literature"*. Thus PEST analysis can be used to perceive the surrounding world also in other situations than in planning corporate strategy.

The Internet is not anymore a piece of technology in vacuum but it is also affected by the political, social and economic interests. Usage of PEST analysis offers broad view to these forces that may affect Internet evolution in the future. Thus it is used in identifying the key trends and uncertainties during the brainstorming sessions and expert interviews.

2.3 Brainstorming

Rickards (1999) defines the brainstorming as *"an individual or group process of idea generation following structural guidelines for weakening intrapersonal and interpersonal barriers to the generation of new and useful ideas".* Brainstorming is exploited to enhance creativity and generate a large number of ideas. Practical evidence shows that brainstorming leads to behavioral and ideational gains over outputs of conventional individual and group work (Rickards, 1999).

The modern applications of brainstorming are associated with Alex Osborn who popularized the method in the late 1930s (Rickards, 1999). Osborn (1963) had two key concepts, the principle of deferment of judgment and the principle of extended search, based on which he defined the four ground rules for the brainstorming:

1. *Focus on quantity.*
2. *Withhold criticism.*
3. *Welcome unusual ideas.*
4. *Combine and improve ideas.*

These rules are used in a brainstorming session lasting from couple of minutes to several hours. The structure for the session is given by the facilitator who motivates and steers the brainstorming group to the right direction.

The variety of brainstorming techniques can be divided into two broad groups – interactive and nominal. In interactive brainstorming participants interact during the brainstorming while in nominal brainstorming the interaction is inhibited and participants create ideas in isolation. Interactive brainstorming has various defects including distraction, social loafing, evaluation apprehension, and production blocking, which lead to productivity losses (Diehl & Stroebe, 1991). Thus nominal groups are more effective in terms of productivity, and the productivity can be further enhanced by using electronic support systems (Rickards, 1999). However, productivity and efficiency are not the only aspects (Rietzschel et al., 2006). Participants may favor social and interactive, but less efficient methods which enable sharing of ideas. From the practical point of view, the potential difficulty of choosing between interactive and nominal methods can be sidestepped by using a cocktail of techniques (Rickards, 1999).

2.4 Interviews

Interview is a very widely used research method which involves a researcher (interviewer) asking questions and receiving answers from the people she is interviewing (interviewee). Interviews are conducted normally face-to-face and one-to-one, but also telephone interviews as well as group interviews are possible. Interviews are typically divided into three classes based on the degree of structure and standardization (Robson, 2002). 1) Fully structured interview has predetermined questions with fixed wording, usually in pre-set order. 2) Semi-structured interview also has predetermined questions but the order and wording of them can be changed, some questions can be omitted and new ones added, and the interviewer can give explanations. 3) Unstructured interviews are most informal, they have a theme, a general area of interest, and the conversation is free and can develop to any direction.

Here the concentration is on the latter two (semi-structured and unstructured) which King (2004) refers as qualitative research interviews. Kvale (1983) gives a formal definition for qualitative research interview as *"an interview, whose purpose is to gather descriptions of the life-world of the interviewee with respect to interpretation of the meaning of the described phenomena"*. Qualitative research interviews are characterized by the low degree of structure, preponderance of open questions, and focus on specific situations in the world of interviewee (King, 2004). Thus they concentrate more on interviewee's opinions than abstractions or general opinions.

The interviewer-interviewee relationship plays a key role in success of an interview (King, 2004). When structured interview tries to minimize the impact of interpersonal factors, in qualitative interviews they are taken as an inseparable part of the research process. Hence the interviewee is seen rather as a participant, not as a research subject, and she participates actively in shaping the course of the interview. Recruiting interviewees is an essential step which affects the quality and variety of results. In order to cover the studied subject as wide as possible, the amount of interviewees and diversity in their backgrounds is desirable. Practical reasons, mainly amount of time and resources, however, restrict the scope of the interview study.

Robson (2002) lists some advantages and disadvantages of interview study. On the pros side is that interviews are flexible and adaptable to many problems, and they have potential of providing rich and highly illuminating material. It is possible to modify the question, ask follow-up questions, and investigate motives. Face-to-face contact also gives an experienced interviewer a possibility to follow non-verbal cues. On the other hand, the low level of structure and standardization raise questions about the reliability and repeatability of the interviews. Interpersonal factors mean that biases cannot be ruled out and that the skills and personality of the interviewer impact on the quality of results. Furthermore, interviewing, including also preparation and transcribing of notes, is very time-consuming and thus limits the sample size.

3 Historical milestones of the Internet evolution

The Internet was born in the October 29th, 1969 when first packets were sent by Charley Kline at University of California (UCLA) as he tried to log into Stanford Research Institute (SRI) (Zakon, 2006). In the following four decades the Internet has evolved from a research project to a worldwide communications network having huge economic value. The conducted milestone study tries not to depict the complete history of the Internet[1] but it highlights the most important evolution steps.

3.1 Division into research and commercial eras

Internet evolution can be divided into the research era and the commercial era. The foundations of the Internet were designed in the research era lasting from the 60s to the beginning of the 90s. The invention of packet switching theory (Kleinrock, 1961; Baran, 1964) and global networking concept (Licklider & Clark, 1962) were major steps towards computer networking and the Internet. In the next years the plan for the first version of the Internet called ARPANET (Roberts, 1967) was developed within the computer research program at ARPA[2]. After the initial network launch consisting of four nodes, the development of the Internet continued. For 20 years the Internet was mainly a tool for computer science researchers, and it was mostly used in distributed computing by logging remotely to the hosts and running commands on them (Leiner et al., 2003).

Privatization of the Internet backbone enabled commercialization of the Internet. At the same time Tim Berners-Lee invented Web which brought the Internet available to everyman. These two parallel milestones work as a divide between research and commercial eras. In the commercial era the Internet has experienced exponential growth in the amount of hosts, users, networks, traffic and services. The foundations have not changed but the research concentration has shifted to solving scalability bottlenecks and innovating new services and usages. The most new users have been non-professional, and the Internet has evolved way beyond its original intention.

[1] For example Hobbes' Internet Timeline (Zakon, 2006) and ISOC's link collection (ISOC, 2009) offer extensive amount of information about the history of the Internet.
[2] The Advanced Research Project Agency of U.S. Department of Defense (DoD), renamed to DARPA (for Defense) in 1972.

3.2 Structure of the milestone study

Studying milestones is motivated by the need to understand the historical development of the Internet. The term milestone covers important principles, seminal technologies and protocols, and revolutionary services. Due to the strategic question concerning IETF, the study maps the milestones to IETF standards called Requests for Comments (RFCs). Identified milestones can be divided into two broad categories, infrastructure and service milestones. Infrastructure milestones (Chapter 3.3) are either fundaments of the Internet or protocols that removed scalability bottlenecks, while service milestones (Chapter 3.4) are important applications that created demand, tempted new users, and increased traffic.

The selection of milestones was done based on few evaluation criteria presented in Table 1 below. All the applicable criteria were graded in the three-level scale large-medium-small, depending on how much a milestone affected on each evaluation criteria. Some of the effects happened before the others, for example DNS primarily enabled larger number of hosts but later domain names had significant effect on commercialization of the Internet. Thus the primary effect is underlined to emphasize its importance.

Table 1: Evaluation criteria of the milestones

Evaluation criterion	Explanation
Number of users	Increased the amount of users = created demand.
Number of hosts	Enabled increasing of the number of hosts = scalability.
Amount of traffic	Increased the amount of traffic.
Number of services	Increased the number of services and innovations.
Economic impact	Had large economic impact for society.
Time consumption	Increased users' Internet usage.
Change in usage patterns	Changed people's Internet usage patterns.

The milestones are gathered in Table 2 and Table 3. A short description, year of the introduction, most important original RFC, and the grading based on evaluation criteria are presented for every milestone.

3.3 Infrastructure milestones

When looked from the infrastructural (or supply) side the Internet has been a very successful scalability story. Generally speaking, infra milestones can be divided into the foundations of the Internet dating back to the research era (the first four) and the protocols that enabled increasing user base (the last five). All the infrastructure milestones are listed in Table 2 below and described more deeply in the next sections.

Table 2: Infrastructure milestones.

	Milestones		The most influential RFC		Evaluation criteria						
	Description	**Year**	**First RFC Nr. (year)**	**Name**	**Nr. of users**	**Nr. of hosts**	**Amount of traffic**	**Econ. impact**	**Nr. of services**	**Time con-sumption**	**Change in usage patterns**
Research era	**RFC Process - Rough consensus and running code**	1969	1310 (-92)	The Internet Standards Process	-	-	-	-	**Large**	-	-
Research era	**TCP/IP**	1974	675 (-74), 791 (-81)	TCP, IP	-	-	-	Large	**Large**	-	-
Research era	**End-to-end argument**	1981	1958 (-96)	Architectural Principles of the Internet	-	-	-	Large	**Large**	-	-
Research era	**Transition from HOSTS.txt to DNS**	1984	883 (-83), 884 (-83)	DNS	Medium	**Large**	Medium	Large	-	-	-
Commercial era	**Privatization of the Internet backbone**	1995	1105 (-89)	BGP	-	Large	-	**Large**	-	-	-
Commercial era	**CIDR enables routing table scalability**	1993	1519 (-93)	CIDR	-	**Large**	-	Medium	-	-	-
Commercial era	**DHCP enables dynamic IP address allocation**	1993	1531 (-93)	DHCP	-	**Large**	-	Medium	-	Small	-
Commercial era	**NAT alleviates IP address shortage & improves security**	1994	1597 (-94)	Address Allocation for Private Internets	Medium	**Large**	Medium	-		-	-

3.3.1 RFC process – rough consensus and running code

The Internet standardization process based on informal documents called RFCs is as old as the Internet. The first RFC titled Host Software was published on 7 April 1969 by Steve Crocker. Its contents were modest and forgettable but it was the initiative that was significant (RFC Editor et al., 1999). From that day on the idea of the RFC process has been to be a fast distribution way for sharing ideas within the Internet community. Hence all the RFCs are not official protocol specifications (although over time they are more focused on them) but some of them are informational, and describe alternate approaches or provide background information.

One of the keys to the rapid growth of the Internet has been the free and open access to RFCs, which promotes the innovation because it allows the actual specifications to be used by anyone, for example by university students and entrepreneurs developing new systems (Leiner et al., 2003). Anyone can also submit a document to be an RFC but typically they are generated by IETF. Open nature of the RFC process is also present in IETF which is an open organization of individuals. Anyone can participate in the meetings and contribute to the work. The standardization is based on *"rough consensus and running code"* meaning that a protocol needs to be widely accepted by the community and its functioning needs to be proved by working applications before the final version of an RFC is published (Alvestrand, 2004).

3.3.2 End-to-end argument

The basic design principle of the Internet is known as the end-to-end argument and was phrased by Saltzer, Reed and Clark (1984) as followed:

> *"The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible."*

The key idea is that a network should do as little as possible, just transmit packets as efficiently and flexibly as possible, and everything else, including error detection and correction, reordering of packets, and encryption, should be left at the fringes (Carpenter, 1996). This approach of a dumb network and smart end points was revolutionary when introduced because of prevailing architecture in which it was the network's sacrosanct responsibility to do everything possible to ensure that it does not drop data (Huston, 2008a). The end-to-end argument leads to the best effort traffic pattern and the network neutrality principle of equality of any kind of traffic. It also has hidden assumption of mutual trust between end points (Clark & Blumenthal, 2001).

The end-to-end argument has important impact on network architecture. It decreases the complexity of networks, which reduces costs and facilitates future upgrades. From the application perspective a dumb network allows new applications to be added without changing the core, and these applications stay independent of implementation and successful operation of application-specific services in the network (Clark &

Blumenthal, 2001). Thereby anyone can write a communications application, share it with people and start using it. On the contrary, smart networks like telephone network inhibit this kind of behavior. Thus the most important impact of the end-to-end argument is its ability to foster innovation (Isenberg, 1998).

Although the end-to-end argument is without a doubt one of the keys to the Internet's success, it has also been criticized. For instance Moors (2002) as well as Clark and Blumenthal (2001) state that the end-to-end argument is not appropriate in every place and it should not be taken as the only choice. Some functions can only be implemented in the core of the network, and also performance-related issues can drive for core-located features. Additionally, some of today's problems in the Internet stem from the original design decisions and the end-to-end argument which were made mutually trusting research community in mind.

3.3.3 TCP/IP

The Internet protocol suite, TCP/IP, forms the core of the Internet. The definition of the Internet presented in Section 1.2 actually relies solely on these protocols. Nevertheless, they have not been present from the beginning. The initial host-to-host protocol called Network Control Protocol (NCP) (Crocker, 1970) was used until the transition to TCP/IP was executed on January 1, 1983 (Zakon, 2006). The development of TCP/IP started already in the early 70s and the original paper presenting TCP was published in 1974 (Cerf & Kahn, 1974). At that time TCP and IP were bundled to one protocol which allowed only virtual circuit style of communication in the Internet. Some applications, for example early work on packet switched voice communication, revealed that in some cases more unreliable datagram service would be needed. Thus in 1978 TCP was reorganized into two protocols, TCP and IP, and User Datagram Protocol (UDP) was introduced in order to provide direct access to the basic service of IP.

Since TCP and IP are fundamental pieces of the Internet, their design principles have fundamental effect on the nature of the Internet. When they were designed, the top level goal was to develop effective technique to utilize existing interconnected networks

(Clark, 1988). Clark also lists seven second level goals presented in the order of importance:

1. *Internet communication must continue despite loss of networks or gateways.*
2. *The Internet must support multiple types of communications service.*
3. *The Internet architecture must accommodate a variety of networks.*
4. *The Internet architecture must permit distributed management of its resources.*
5. *The Internet architecture must be cost effective.*
6. *The Internet architecture must permit host attachment with a low level of effort.*
7. *The resources used in the Internet architecture must be accountable.*

The hourglass structure of the Internet protocol suite (Figure 3) summarizes the points 2 and 3 nicely. TCP/IP does not restrict the network technology or the applications that can be used in the Internet. This flexibility has allowed the innovation and enabled cost savings because no dedicated network was needed to build since various existing networks, most notably PSTN (Public Switched Telephone Network), could be used. Later, when Internet usage has increased, also the economies of scale have had an important effect in lowering the costs.

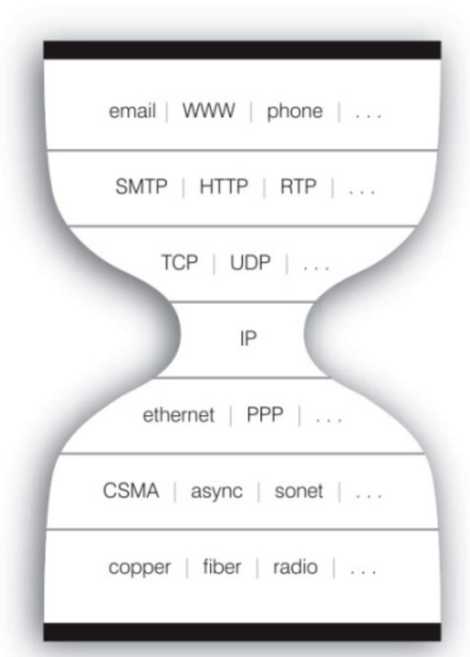

Figure 3: Hourglass architecture of the Internet (adapted from Zittrain, 2008).

3.3.4 Transition from HOSTS.TXT to DNS

Domain name system (DNS) introduced in 1983 and taken into use in 1987 solved the scalability problems of HOSTS.TXT system (Levien, 2005). HOSTS.TXT was a single file containing all host name to address mappings which was FTPed by all the hosts (Mockapetris, 1987). Thus every change in the network, for example adding a new host, required updating of the file and sending the entire table to all the hosts. With time when increasing number of computers joined the Internet, the updating task became more burdensome and suspect to failure, the process was too slow and name conflicts started to occur due to the flat name space (Levien, 2005). Most importantly, the HOSTS.TXT system formed a scalability bottleneck since more hosts on the network meant more updates, more hosts trying to download and more data to download. Distributed and hierarchical structure of the DNS was and still is the key that enables the scalability of host name to address mappings.

The importance of DNS is not restricted to enabling scalability. Hierarchical structure allows local administration of names and addressing as well as local structure on the name space. Domain names are mnemonic compared to IP addresses and so, after the rapid growth of Web, they began to refer to products or services, rather than just network resources (Levien, 2005). Additionally, many Internet companies, e.g., Amazon.com, use domain names as their corporate names.

3.3.5 Privatization of the Internet backbone

In the early years of the Internet many networks existed, but not all of them were compatible with and connected to each others. In the middle of the 80s National Science Foundation (NSF) funded by the U.S. government built NSFNET that formed the initial Internet backbone by connecting universities and research organizations in the U.S. The NSFNET backbone was restricted to research and educational purposes. The growing number of users, however, was interested in using the Internet for commerce, which encouraged commercial companies to offer Internet connectivity by building their own backbone networks (Kesan & Shah, 2001).

The technical piece of the puzzle, Border Gateway Protocol (BGP), was created in the beginning of 90s to replace the EGP (Exterior Gateway Protocol) used in NSFNET. Although EGP had not faced serious scalability problems, decentralization of inter-domain routing allowed the increasing scale of the Internet. Foremost, BGP enabled multiple backbones through fully decentralized routing and thus made it possible to put NSFNET backbone out to pasture. Privatization and BGP together combined the separate networks and paved the way for the explosive growth.

3.3.6 Enabling growth

In the early 90s it became obvious that the Internet had grown beyond anyone's expectations and that the growth would continue and bring along serious scaling problems related to routing and addressing (Clark et al., 1991). The original 32-bit address space was seen inadequate in the long time span, and there also were plenty of short-term problems that were seen urgent to solve. Additionally, the BGP table growth rate exceeded the growth in router hardware and software capabilities. Thus three different solutions – Classless Inter-Domain Routing (CIDR), Network Address Translators (NATs) and Dynamic Host Configuration Protocol (DHCP) – were introduced to ease the situation.

As RFC 1517 (Hinden, 1993) notes, IP address allocation based on classes (A, B, and C with ~16 million, 65 536 and 256 addresses respectively) was not flexible enough. The C class was too small and the B class way too large for midsized organizations. CIDR solved this issue through more flexible (classless) address allocation, and at the same time changed the BGP table growth rate from exponential to linear by introducing provider address aggregation (Huston, 2001).

Network address translators were introduced to alleviate IPv4 address exhaustion by enabling the sharing of one global IP address with multiple hosts using private address space (Egevang & Francis, 1994). Additional benefits of NATs include improved security, since all the inbounding connections are blocked to all the ports until the mapping is completed (Hain, 2000). The use of NATs distorts the one-to-one mapping between Internet hosts and IP addresses and thus breaks the end-to-end connectivity. Besides, NATs were thought to be a short-term solution but their extensive usage has disrupted implementation of longer-term solutions, for instance the adoption of IPv6.

DHCP, for one, was mainly developed to allow automatic and dynamic IP address allocation and thus support system and local area network (LAN) management and auto-configuration. Nevertheless, the timing was fortuitous because DHCP was also able to help with the conservation of IP addresses (Levien, 2005).

3.4 Service milestones

When looked from the service (or demand) side, the Internet has not limited services and applications that can use the network. There is clearly one milestone above all other – Web. Its impact is evaluated large in all the categories and added to this, three of the following four milestone services (search engines, TLS (Transport Layer Security) and video streaming) are used mostly on top of the Web. The most influential service milestones are listed in Table 3 below and described more deeply in the next sections.

Table 3: Service milestones

	Milestones		The most influential RFC		Evaluation criteria						
	Description	Year	First RFC Nr. (year)	Name	Nr. of users	Nr. of hosts	Amount of traffic	Econ. impact	Nr. of services	Time con-sumption	Change in usage patterns
Research era	File Transfer Protocol	1971	765 (-82)	FTP	-	-	**Large**	-	-	-	-
Research era	Original Killer App - Email	1973	822 (-82)	SMTP	Medium	Medium	Medium	Large	Small	-	**Large**
Commercial era	Web takes the Internet by storm	1993	1866 (-95), 1738 (-94), 2068 (-97)	URL, HTML, HTTP	**Large**	Large	Large	Large	Large	Large	Large
Commercial era	Search engines change the way people browse the Web	1995	2068 (-97)	HTTP (Altavista, later Google)	Large	-	Medium	Large	Medium	Small	**Large**
Commercial era	TLS provides privacy and enables e-commerce	1996	2246 (-99)	TLS (SSL)	-	-	-	**Large**	Large	-	Medium
Commercial era	P2P Traffic Boom	2000	1958 (-96)	Architectural Principles of the Internet (Napster)	Medium	Small	**Large**	Small	Small	Small	Medium
Commercial era	Video streaming proliferates	2005	2616, 3550	HTTP, RTP (Youtube)	Small	Small	**Large**	Medium	Small	Medium	Medium

3.4.1 File transfer protocol

Transferring files over the Internet was one of the earliest applications in the Internet. The first proposed mechanism was specified in RFC 114 (A File Transfer Protocol) in 1971. After the many development steps, RFC 765 specified FTP for use on TCP (Postel & Reynolds, 1985). Before the Web traffic surpassed FTP traffic in 1995, FTP produced by far the largest amount of traffic in the NSFNET backbone (Merit, 1995).

FTP was and is used for many purposes. In the early days of the Internet FTP was utilized in distributing the HOSTS.TXT file, predecessor of DNS. Nowadays FTP has much smaller role but still many users connect to their web servers by using FTP, although more secure options like SSH (Secure Shell) are available.

3.4.2 Email – the original killer app

Already in the beginning, in the era of timesharing computers, it was found out that extending human communication was a natural use of the new technology. In the 1971 Ray Tomlinson invented an email program to send messages across a distributed network (Zakon, 2006). RFC 733 defined format of the email messages in 1977, and the current email protocol called Simple Mail Transfer Protocol was described in RFC 822 in 1982.

Most importantly, email provided a new way for people to communicate and changed the nature of collaboration. First the email connected separate groups of computer science researcher in building the Internet (Leiner, 2003), later it made corporate communication more effective and drove (together with Web) consumers to buy Internet access. And yet still it is the most popular purpose of use in the Internet (Statistics Finland, 2008).

3.4.3 Web takes the Internet by storm

World Wide Web (Web, WWW, W3), developed at CERN by Tim Berners-Lee, was released in the end of year 1990. Two basic design principles were principle of minimal constraint (meaning as few specifications as possible) and principle of modularity and information hiding (meaning that necessary specifications should be made independently) (Berners-Lee, 1996). These principles resulted in three protocols: 1)

HTTP (Hyper-Text Transport Protocol), the network protocol used between Web servers and clients; 2) HMTL (Hyper-Text Mark-up Language), the markup language to describe the structure of web pages; and 3) URI (Universal Resource Identifier), the address system to identify resources in the Web (Berners-Lee, 1994).

The Web enabled information dissemination over the Internet in easy and flexible manner. The universality and accessibility of Web meant that people were able to surf the Web independent of operating system or computer model. Especially after Mozaic, an early web browser, was released 22 April 1993, the Web proliferated at a 341,634% annual growth rate (Zakon, 2006). Already in 1995 the Web surpassed ftp-data as the service with greatest traffic in the Internet. Thus it can be said that the Web played a key role in popularizing the Internet. During the last 15 years the Web has grown to be a platform of tremendous (commercial) potential. It has changed the way we search information and conduct business. Hence the terms Internet and Web are often conflated in popular use.

3.4.4 Search engines change the way people browse the Web

Finding the desired Web pages and information is the starting point for using the Web. In the early days of the Web, navigating was based either on guessing the URL (Uniform Resource Locator) or using directory services (e.g., Yahoo) (Levien, 2005). Search engines, at the beginning for instance Excite, Lycos, and AltaVista, little later Google, revolutionized the way people navigate in the Web. Finding a related RFC is, however, not too easy, since the key components of search engines – proprietary search algorithms and databases – are not standardized in RFCs. Thus the search engines are linked to the Web through HTTP.

A study of Pew Internet Project reports that 84% of the U.S. Internet users have used search engines, and on any given day, 56% of those online use them (Fallows, 2005). According to Alexa.com (2009), the top two web pages in the Internet in April 2009 were google.com and yahoo.com, both search engines. The success of Google has created an expression *"to google"* which by Webster's New Millennium Dictionary has the meaning *"to search for information on the Internet, especially using the Google search engine"*.

Although the initial impact of search engines was how they changed the way people browse the Internet, economic effects should not be forgotten. Search engine companies, most prominently Google, have been able to convert their search engines into advertising business. This is done both by offering paid ads related to web searches and selling ad space to a large base of Web pages and using search algorithms to show relevant ads in each page. The importance of search engines in finding new information has also created market for search engine optimization that tries to help Web sites to raise their position in search results (Levien, 2005).

3.4.5 TLS provides privacy and enables e-commerce

Need for securing privacy, authentication and data integrity in client-server communication was identified soon after the invention of the Web. The SSL (Secure Socket Layer) protocol was originally developed by Netscape and after a couple of draft versions, the stable 3.0 version was released in 1996 (Rescorla, 2001). Shortly after that SSL development became responsibility of IETF which renamed the protocol to TLS (Transport Layer Security) (Thomas, 2000). Most commonly TLS is used together with HTTP to form HTTPS used in securing Web pages. As a flexible protocol located between application and transport layers it also supports other application layer protocols.

TLS enabled reliable e-commerce and allowed the Web to be used as a commercial service platform (Thomas, 2000). E-banking, credit card payments, and using different kind of online services requiring authentication are some examples of applications which use TLS.

3.4.6 P2P Traffic boom

Peer-to-Peer (P2P) systems came to notice of the wide public in 1999 through MP3 (MPEG-1 Audio Layer 3) file sharing application called Napster. It made sharing of MP3 files easy and paved the way for later peer-to-peer file sharing applications. Nowadays peer-to-peer file sharing is the best known application of P2P but it is not the only one. Other possibilities cover VoIP (e.g., Skype[3]), instant messaging (e.g., ICQ[4]), remote

[3] http://www.skype.com
[4] http://www.icq.com/

collaboration (e.g., shared file editing), distributed computing (e.g., SETI@home[5]) and streaming media (P2PTV) (Beijar, 2008). Most of these P2P systems use proprietary protocols and dedicated client applications. Thus linking to RFCs is possible only through basic design principles of the Internet since the rise of P2P applications means actually reverting from the client-server architecture dominating in the Web to the original Internet architecture consisting of equal peers (Oram, 2001).

Peer-to-peer (file sharing) systems increased the Internet traffic substantially. Ipoque (2007) found out that P2P is producing more traffic in the Internet than all the other applications combined. In Eastern Europe the proportion of P2P traffic was as much as 83%. The other implications relate to the economic aspects. Easiness to find and download music, movies, TV series, and other content free of charge has affected the purchase behavior of some users by changing the willingness to pay for content and by allowing experimentation. Although the content industry anxiously claims that P2P declines the sales, for example the study of Oberholzer-Gee and Strumpf (2006) regarding music sales suggests that P2P file sharing has no statistically significant effect on sales. The increasing traffic amount and symmetric traffic pattern have also effect on Internet service providers' (ISPs') (transit) costs, which has made some companies to restrict or optimize peer-to-peer traffic.

3.4.7 Video streaming proliferates

Streaming media, especially streaming video, is responsible for large amount of Internet traffic. Ellacoya Research (2007) and Cisco (2008a) report that Internet video accounts for about 20% of the Internet traffic. Despite historical importance of video, the impact and proportion of video traffic will most likely just increase. Cisco (2008a) namely forecasts that already in 2012 Internet video will account for 50 % of total Internet traffic. The requirements of Internet video streaming have been one of the factors that have created market for content delivery networks (CDNs).

[5] http://setiathome.ssl.berkeley.edu/

The world's third most popular web site (Alexa, 2009), YouTube[6], creates about half of the Internet video traffic, at least in North America (Ellacoya Research, 2007). YouTube, as most of the other video streaming services, uses Adobe Flash to display the video (Ipoque, 2009). In Flash the video is delivered using HTTP/TCP, and the delivery technique is called progressive downloading or pseudo-streaming, since the file is actually downloaded to the user but the playback can be started before the whole file is delivered (Gill et al., 2007). There are also many protocols for non-HTTP video streaming. IETF has standardized the RTP family (RTP, Real-time Transport Protocol; RTCP, RTP Control Protocol; RTSP, Real Time Streaming Protocol) for this purpose. Although non-HTTP streaming is used in live streaming, its amount of total Internet traffic is petty (only 3% compared to 17% of HTTP video in North America (Ellacoya research, 2007)).

[6] http://www.youtube.com

4 Internet ecosystem

This chapter presents the current status of the Internet ecosystem. The purpose is to first describe the industry structure, size and traffic characteristics, and then list some identified problems as well as efforts that try to tackle them.

4.1 Internet interconnectivity

To understand the Internet ecosystem, the different players and their interrelations need to be explained. This can be handled both from technical, network-centric perspective and from economic point of view. This section takes the network level view while Section 4.2 explains the most important stakeholders.

The Internet consists of heterogeneous networks called autonomous systems (ASes). They are operated mostly by commercial Internet Service Providers (ISPs), but also by corporations and other enterprise providers, universities, government agencies, and content providers and other specialized service providers (Clark et. al, 2008). ISPs connect end users and businesses to the public Internet by selling Internet access. They compete over customers on price, performance, reliability etc. but they must also co-operate to offer universal end-to-end connectivity (Norton, 2001).

The interconnectivity between ASes is arranged by two basic types of agreements – paid transit and settlement-free peering.

Definition: A Transit Relationship is a business arrangement whereby an ISP provides (typically sells) access to the global Internet (Norton, 2002).

Definition: Peering is the business relationship whereby ISPs reciprocally provide access to each others' customers (Norton, 2002).

The recursive combination of these standardized contracts resulting from complex and dynamic bargaining game between pairs of ASes creates the web of interconnections (Clark et. al, 2008).

The simplified structure of the Internet consists of ISPs, content and enterprise companies, and end users. ISPs can be divided into two groups – Tier 1 ISPs and Tier 2 ISPs. Generalized Internet ecosystem is presented in Figure 4.

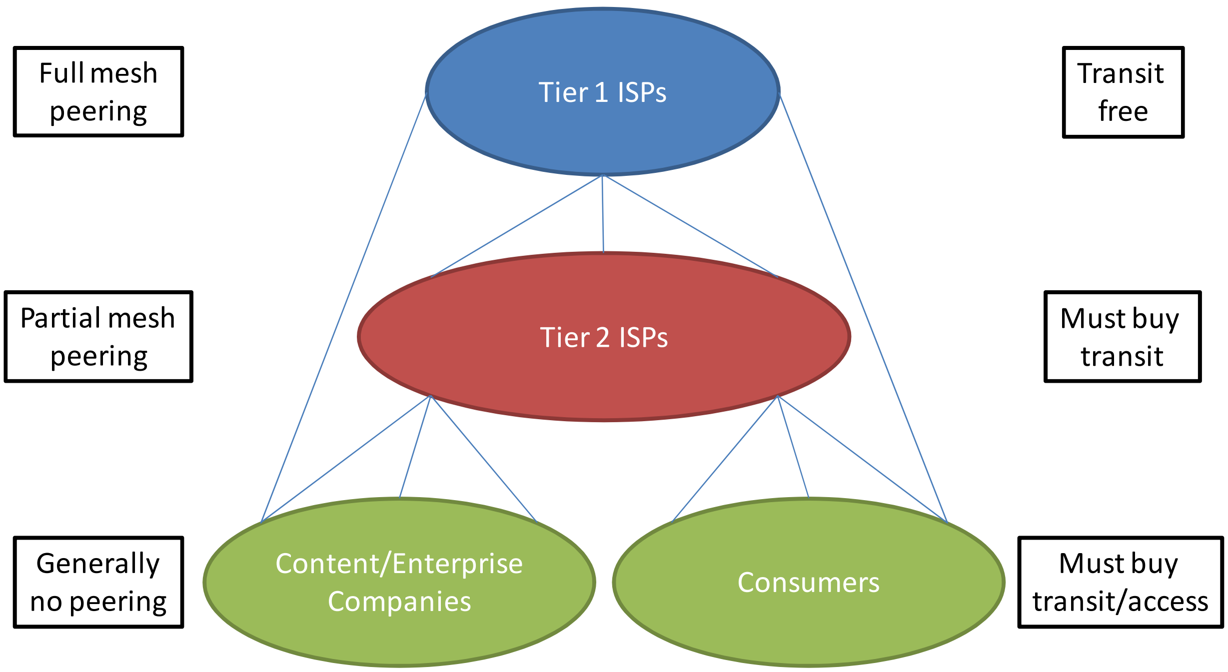

Figure 4: Generalized Internet ecosystem (adapted from Norton, 2003, modified).

Definition: A Tier 1 ISP is an ISP that has access to the global Internet routing table but does not purchase transit from anyone (Norton, 2001).[7]

Since Tier 1 ISPs do not buy transit, they have to get access to the entire Internet solely through peering relationships. This means that every Tier 1 ISP must peer with all the other Tier 1 ISPs, and thus the amount of Tier 1 ISPs has stayed quite limited. According to Renesys Corporation (2009), there were 13 Tier 1 ISPs in January 2009.

Tier 2 ISPs are a heterogeneous group of ISPs that differ in geographical coverage, amount of customers and proportion of transit and peering traffic. Some small ISPs buy only transit and some large ISPs have vast amount of peering agreements. The common factor is that they still have to buy transit.

[7] Strict definition of Tier 1 ISP requires that ISP is not only transit-free but also all of its peering relationships need to be settlement-free. Technically there is no difference in settlement-free and paid peering, so the looser Tier 1 definition is used here.

Content and enterprise companies are typically customers of ISPs. Their connectivity to the Internet is mostly based on transit agreements, and peering is rare. ISPs also connect end users (consumers) to the Internet by selling Internet access.

4.2 Stakeholders

While the Internet has extended its tentacles to the entire society, the amount of stakeholders has increased and their incentives to influence on Internet evolution have become stronger and more diverse. Clark et al. (2002) call this process of adverse interests between stakeholders *"the tussle".* They have identified various stakeholders of the Internet landscape and some examples of tussles. Identified stakeholders include users, commercial ISPs, private sector network providers, governments, intellectual property rights holders, and providers of content and higher level services. Some key players are, however, missing from this list. Therefore our own view of the key players and their interrelations is explained briefly below and drawn in Figure 5.

- **Network infra vendors** deliver network HW and SW (e.g., routers, fiber, radio access components, network management tools) to both access and backbone operators.
- **Backbone operators** (ISPs) sell global Internet interconnectivity to access operators. An ISP can be at the same time both backbone and access operator.
- **Access operators** (ISPs) sell Internet access to the end-users and buy interconnectivity from backbone operators.
- **Device & Software vendors** manufacture devices like computers, mobile phones, and PDAs as well as software like operating systems, browsers, and email clients to end users and content & application providers.
- **Advertisers** enable many Internet services by paying for advertising space.
- **Content & Application providers** produce Internet services that attract end-users to use the Internet.
- **End-users**, covering both consumers and enterprise customers, access Internet content, services and applications with their devices that run software. The connectivity is offered by the access operators and legitimate actions are defined by the regulators.

- **Governments & Regulators** enact laws on the grounds of the society's demand. Governments have also national motives for influencing actively the Internet evolution.
- **Research institutes**, for instance universities, develop Internet protocols and technologies.
- **Standardization bodies**, also including Internet governance bodies like ICANN, standardize technologies and allocate resources.

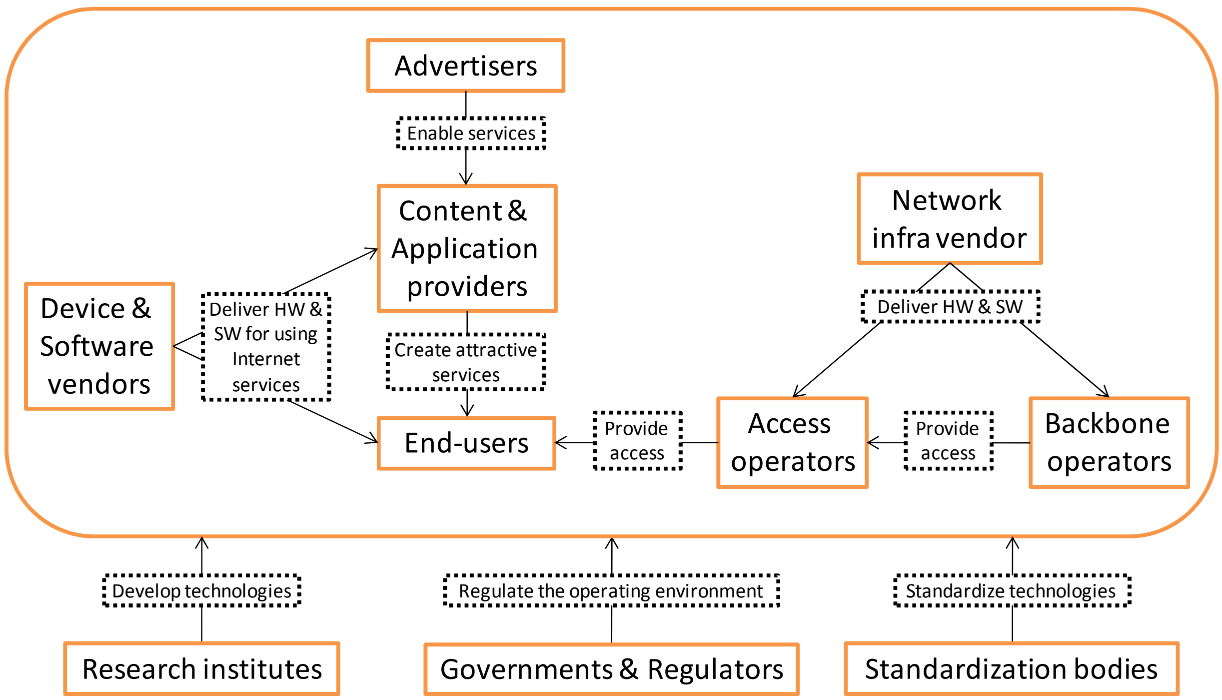

Figure 5: Stakeholders of the Internet ecosystem.

4.3 Size of the Internet

How big the Internet is? The answer is we really do not know because it is unorganized, uncatalogued and continues to grow at a phenomenal rate. However, some sources are offering guestimates from different perspectives ranging from the parts of the technical infrastructure to the actual usage. Next sections give a brief overview to the question from both technical and usage viewpoints.

4.3.1 Technical viewpoint

The first measure of scale is the amount of autonomous networks (ASes) in the Internet. The amount of them on 14 April 2009 was 30872 (ASN, 2009). This figure does not give a very good estimate of the Internet size since some of the ASes (typically ISP networks) are huge networks consisting of millions of hosts and users while others (for example corporate networks) are much smaller.

The host count is another thing that can be used as a measure of scale. Internet Systems Consortium (ISC) has collected the number of hosts advertised in the DNS twice a year since 1987. The latest survey conducted in January 2009 found 625,226,456 hosts connected to the Internet (ISC, 2009). Figure 6 presents the survey results since 1994 and gives a nice overview of the growth of the Internet.

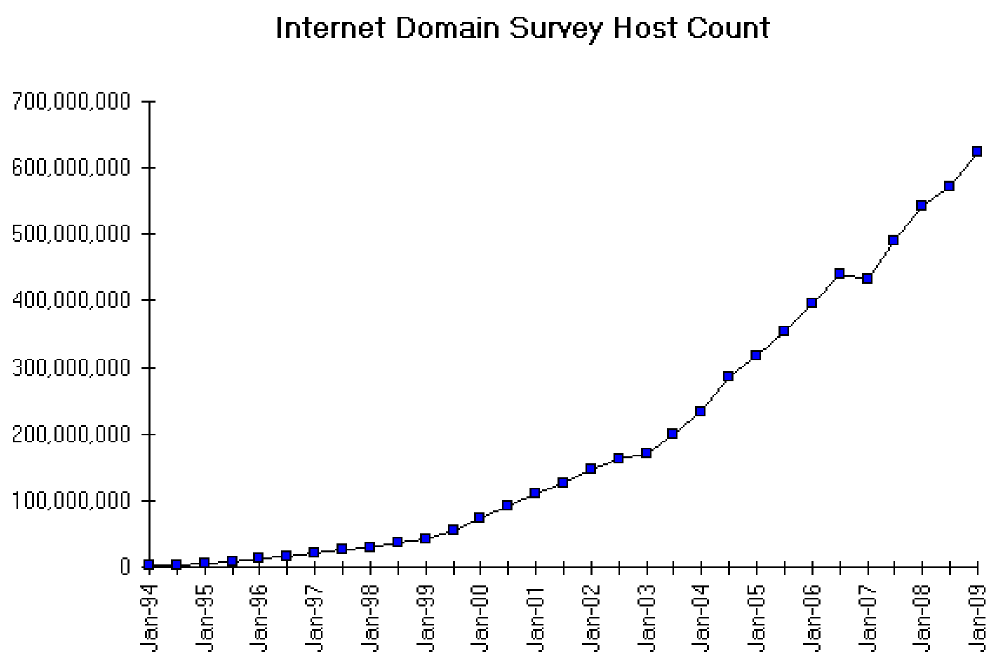

Figure 6: Internet domain survey host count (adapted from ISC, 2009).

4.3.2 Usage viewpoint

The Internet's impact on society can be evaluated by dissecting the number of users and penetration rates around the world. Internet World Stats (2009) collects this information from market research companies, international telecommunication agents, and local regulators. Their report shows that there are almost 1.6 billion Internet users among population of 6.7 billion, which means average penetration rate of 23.8%. Although it can be questioned if the numbers are a little high, they give at least a rough conception of the dimensions.

Statistics about number of users and penetration rates (Figure 7) reveal large regional differences. The Internet plays the most significant role in North America, Oceania and (Western) Europe where the penetration rates are over 50%. However, the largest growth potential is in developing countries in Asia, Africa and Latin America, which have large population but modest penetration rates. Asia for instance has already now the most Internet users (and China is the largest country, 298 million users), but this is not due to high penetration rate but large population (56.3% of the world's population).

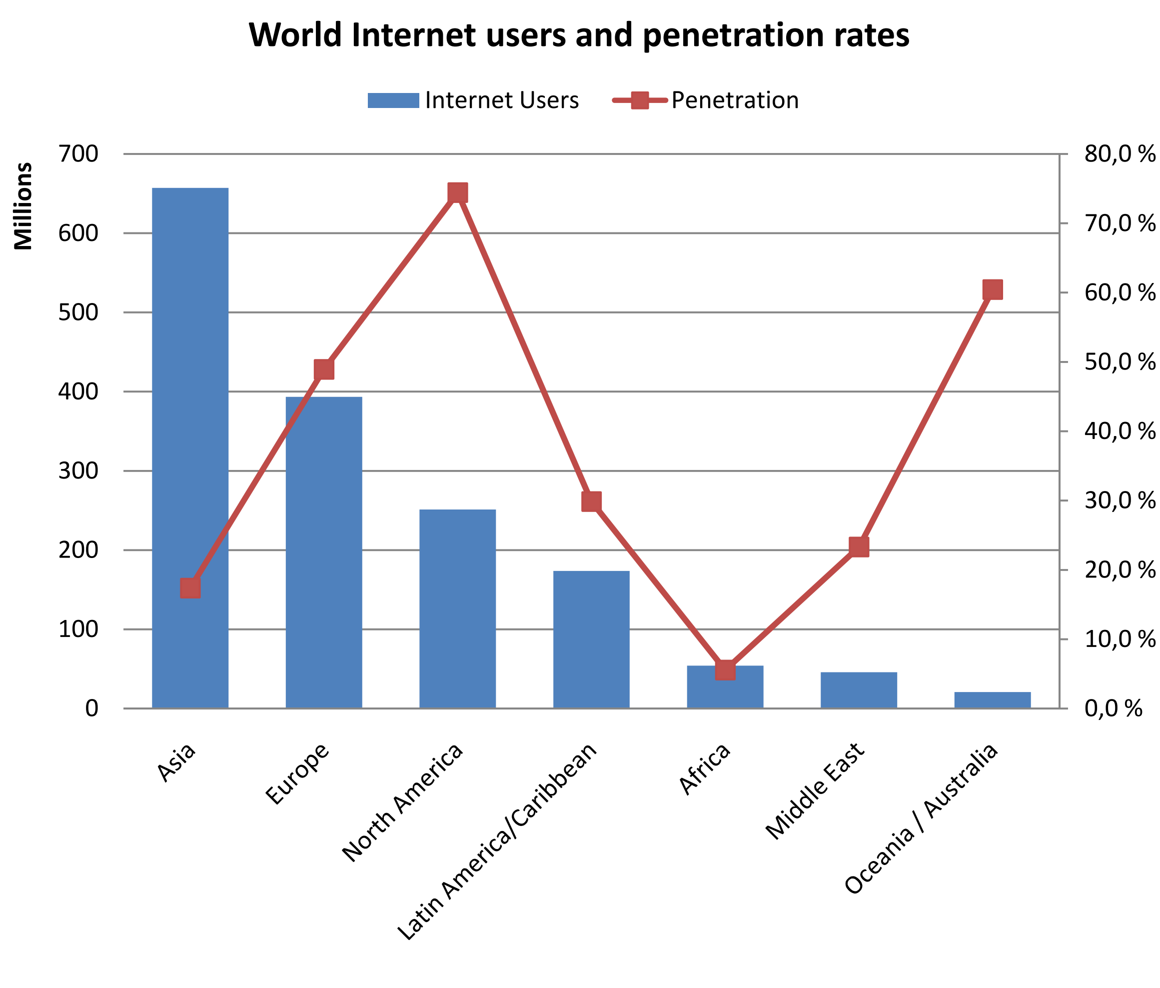

Figure 7: Internet users and penetration rates in the world by geographic regions on 31 March 2009 (Internet World Stats, 2009).

The usage can also be studied by looking the amount of transferred data in the Internet. Cisco's (2008a) estimate based on the analyst projections suggests that the amount of monthly Internet traffic in 2009 is 10666 PB. When this is divided among 1.6 billion users it means approximately 6.7 GB traffic per user per month which is 233 MB per day. That is quite a high number if an average consumer is considered but there are also heavy users both in the private and in the commercial sector that certainly exceed the number.

4.4 Traffic characteristics

What kind of traffic is carried by the Internet? This is an interesting question in order to understand how people truly use the Internet. Furthermore, traffic characteristics are of high interest from technical perspective since they reveal how dependent the Internet is on a handful of protocols. Thus the traffic distribution in the network, transport and application layers is presented in the following three sections. Due to the decentralized structure of the Internet, it is difficult to measure the traffic characteristics globally. Thus the numbers in this section are based on small subsets of Internet traffic which are believed to present the global situation at least coarsely.

4.4.1 Network layer

Network layer is the thin waist of the Internet protocol suite which offers transparent connectivity for various applications between diverse underlying network technologies. Hence IP is the only major protocol in this layer[8]. The original version of the protocol, IPv4, dominates the Internet. The newer version, IPv6, which offers larger address space, has been available for over 10 years now but its adoption has been really slow. Mike Leber's global IPv6 deployment report tells that currently only 4.4% of all the networks (ASes) and one of the 500 most popular websites (identified by Alexa.com) run IPv6 (Leber, 2009). On the traffic level the situation is even poorer. CAIDA's (2009) measurements show that the proportion of IPv6 is as petty as 0.005% of the traffic in a backbone link between Seattle and Chicago (Table 4).

[8] Internet Control Message Protocol (ICMP) is important but its messages are encapsulated within IP datagrams, and secure version of IP (IPsec) has bunch of protocols (ESP, GRE, etc.) that create little traffic.

4.4.2 Transport layer

On the transport layer the market is shared among TCP and UDP, two protocols that have been available from the early days of the Internet. Together they account for over 99 % of the traffic in a backbone link from Seattle to Chicago (CAIDA, 2009). Furthermore, reliable TCP dominates the transport layer with its 92% share of the bits compared to 7% of unreliable UDP (Table 4). Similar proportion of TCP (94%) was identified in a study concerning Finnish mobile packet network data traffic in 2007 (Kivi, 2008). On the packet level, the proportion of TCP is slightly smaller and proportion of UDP is higher, which indicates that UDP packets are much smaller than TCP packets. Newer and more effective transport protocols for certain use cases (e.g., DCCP and SCTP) have been developed to overcome some of TCP's shortcomings. However, these new transport protocols are not typically recognized by transport-aware middleware (e.g., NATs and firewalls), which restricts their wide scale deployment (Huston, 2008b).

Table 4: Protocol traffic distribution in OC192 backbone link from Seattle to Chicago (CAIDA, 2009).

	1 day *		1 week **		4 weeks ***		2 years ****	
Protocol	**bits/s**	**packets/s**	**bits/s**	**packets/s**	**bits/s**	**packets/s**	**bits/s**	**packets/s**
TCP	91,86 %	81,01 %	92,39 %	81,71 %	92,87 %	82,59 %	92,49 %	83,69 %
UDP	7,61 %	17,84 %	6,99 %	17,08 %	6,42 %	16,19 %	7,79 %	16,35 %
ESP	0,31 %	0,62 %	0,38 %	0,64 %	0,49 %	0,67 %	0,35 %	0,48 %
GRE	0,17 %	0,14 %	0,19 %	0,16 %	0,21 %	0,17 %	0,33 %	0,23 %
ICMP	0,0490 %	0,3700 %	0,0560 %	0,4000 %	0,0580 %	0,4200 %	0,1200 %	0,4500 %
IPv6	0,0054 %	0,0072 %	0,0047 %	0,0054 %	0,0047 %	0,0055 %	0,0024 %	0,0026 %
RSVP	0,0020 %	0,0073 %	0,0022 %	0,0078 %	0,0025 %	0,0086 %	0,0029 %	0,0053 %
other	0,00 %	0,00 %	0,00 %	0,00 %	0,00 %	0,00 %	0,00 %	0,00 %

*	1 day	April 16 2009 - April 17 2009
**	1 week	April 10 2009 - April 17 2009
***	4 weeks	March 20 2009 - April 17 2009
****	2 years	April 18 2007 - April 17 2009

4.4.3 Application layer

Various companies (CacheLogic, 2005 and 2006; Ellacoya Networks, 2007; Cisco, 2008b; Ipoque, 2007 & 2009; TeleGeography, 2009) have reported application traffic distributions during the last years. The results show some variance so just the rough estimates are presented here. About 85% of the traffic is HTTP or P2P (e.g., BitTorrent, eDonkey, Gnutella) traffic. Some sources suggest that over 60% of the traffic is P2P (CacheLogic, 2006; Ipoque, 2009) while others (Ellacoya Networks, 2007; TeleGeography, 2009) report that HTTP has recently eclipsed P2P because of YouTube style video streaming. About half of the remaining 15% of the traffic comes from non-HTTP streaming. VoIP (e.g., SIP), email (SMTP), and other application level protocols cover the rest. The most significant discovery in application layer is the importance of HTTP. It was developed for Web to support retrieval of Web pages but nowadays it is used by multitude of applications.

4.5 Present problems

As the Internet has evolved beyond its original scale and scope the drawbacks and deficiencies of the original design principles following from the end-to-end argument have been exposed. David Clark, the most famous advocate of the end-to-end argument, and Blumenthal list multiple trends and problems that may erode the applicability of the end-to-end argument and lead to architectural change of the Internet (Clark & Blumenthal, 2001).

The strategic research agenda (SRA) of FI program (Nikander & Mäntylä, 2007) identifies six present problems:

- unwanted traffic,
- choking of the routing system,
- mobility and multi-homing,
- consumption and compensation,
- privacy and compensation, and
- trust and reputation.

These problems are used here as the basis for describing some of the motives for Future Internet research. Next sections (4.5.1-4.5.6) explain them in more detail.

4.5.1 Unwanted traffic

Unwanted traffic, including application-level flooding (e.g., email and instant messaging (IM) spam), security attacks (e.g., worms, Trojan horses, or direct), and distributed denial of service attacks, is a consequence of naïve assumption that users act benevolently. The Internet was built homogenous, mutually trusting research community in mind, and it was assumed, that the sender does not send packets if the receiver is not willing to receive them. Due to the economic reasons some parties are, however, interested in forcing interaction on another (Clark & Blumenthal, 2001). The unintentional consequence of the Internet's network architecture is that the main cost of communication is paid by the recipient. And when the marginal cost of sending packets is very close to zero, there are few incentives not to send unwanted traffic. The typical counterattack against unwanted traffic is use of firewall-like middle boxes although they have their own problems relating to reachability limitations. From wider perspective unwanted traffic has to do with fairness since the cost of unwanted traffic is mostly paid by the party that does not even want to interact at all.

4.5.2 Choking of the routing system

RFC 4984 – Report from the IAB workshop on routing and addressing (Meyer et al, 2007) names the routing scalability as the most important problem facing the Internet today. The problem includes the size of the BGP table and the implications of growth to the routing convergence times. Consequently the core router hardware needs to be more effective (faster memory and processing). Additionally, traffic engineering complicates the routing system since BGP does not offer any good tools for it. The routing problems relate inherently to addressing. The non-allocated IPv4 address space is projected to exhaust in 2011-2012 (IPv4, 2009), which brings urgency to solve the problem somehow. All the proposed solutions (transition to IPv6, re-allocation of IPv4 addresses through transfer markets (Mueller, 2008), and more extensive usage of NATs (Nishitani et al., 2008)) increase stress on the routing system. Although the problems in routing system are not acute (Huston, 2009), their difficulty calls for immediate attention (Meyer et al., 2007).

4.5.3 Mobility and multi-homing

Mobility is another dilemma which was not addressed when the Internet was designed. Today, however, there is a clear need for mobility and multi-homing. Semantic overload of IP addresses is one of the reasons behind the mobility problem (Huston, 2006). IP addresses are used both as locators (answer to question WHERE) and identifiers (WHO). They work also as lookup keys in making local switching decisions (HOW). Mobile devices change their location constantly while they still wish to keep their identity. Thus either a new namespace offered for example by Host Identification Protocol (Moskowitz and Nikander, 2006) or level of indirection is needed to provide effective solution for mobility and multi-homing. Mobility is a problematic requirement not only from the perspective of terminal mobility but also from the perspective of user, session and process mobility.

4.5.4 Consumption and compensation

Deep in the Internet architecture lies an assumption of benevolent and co-operative agents that together work for maximizing throughput in the network. But if agents behave selfishly, as they do more and more today, some mechanisms for compensating the resources they (over)use are inevitable. The Internet, however, is missing mechanisms and incentives for compensation. This can be seen as exiguity of resource and congestion control mechanisms (Nikander & Mäntylä, 2007). Resource control tries to guarantee sufficient resources at all times while congestion control attempts to allocate resources "fairly" in those situations where there is scarcity of them. One aspect of this problem is how to satisfy diverse performance requirements of different types of applications, and at the same time implement feasible and fair congestion control. Another question is: Does the revenues in the Internet flow to them who need to do the investments? The Internet lacks means of routing money, which is one of the reasons for the success of ad-based business models. From customer perspective the key question is usability of paying meaning that the inconvenience of paying needs to be minimized[9].

[9] Only easy enough solutions (usable, the amount of payments is minimized) may succeed, e.g., paying only once a month (operators), paying not at all = ad-based (Google), paying is bundled with device (Nokia).

4.5.5 Privacy and attribution

The relationship between users' rights and responsibilities is not clear in the Internet. The most critical tension is the one between anonymity and accountability (Clark & Blumenthal, 2001). Privacy, if not absolute anonymity, is seen important in many societies. To prevent bad things happening, the desire for privacy needs to be balanced against the need for accountability. Unfortunately there are very little tools for fostering accountability in the Internet architecture. This is related to the more common characteristics of information technology recognized by Lawrence Lessig. His famous quote *"Code is Law"* proposes that Internet design realized in TCP/IP has such characteristics that make regulating behavior difficult (Lessig, 2000). Due to this Lessig sees that the technical foundation needs to be built in a way that provides balanced level of privacy and attribution.

4.5.6 Trust and reputation

A simple model of the early Internet – a mutually trusting community – is gone forever. However, users who do not trust each other still desire to communicate (Clark & Blumenthal, 2001). In their more recent paper Clark and Blumenthal (2007) reassess the original end-to-end principle and re-formulate it as a trust-to-trust principle:

> *The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at a point where it can be trusted to do its job in a reliable and trustworthy fashion."*

This moves the focus from end points to trustworthy points of execution. Although Särelä and Nikander (2008) see that the technical architecture needs to foster trust, the problems of trust and reputation are largely non-technical and relate for instance to human factors like the ability to make decisions involving risks using existing and possibly inadequate information.

4.6 Future Internet research

Although the Internet technologies have been studied extensively from the beginning, a new wave of research activities has emerged in recent years due to the increased public awareness of the shortcomings in the Internet architecture. Future Internet is a summarizing term for all these research activities that strive for developing the original Internet. The diversity of Internet technologies means that the related research topics are wide spread. Some efforts concentrate solely on incremental evolution while others aim for complete architectural re-design (also called as a clean slate approach). In many research efforts these approaches live side-by-side so that incremental developments are used to tackle short-term problems while clean slate is seen as a long-term solution. Despite of the many clean slate research efforts, not all the academics are convinced of their rationality or value. Milton Mueller, scientific committee member of Internet Governance Project (IGP), claims that promising new Internet may be a great strategy for government funding but it is not honest since the inertia of the Internet affects so that there is no replacement of the old Internet with a new one (Mueller, 2009).

Table 5 lists several Future Internet research efforts in Europe and elsewhere. Future Internet Assembly (FIA) is a European Union initiative that acts like an umbrella over diverse research projects funded by Seventh Framework Programme (FP7). National research efforts, like Finnish Future Internet program, supplement European-level projects. Outside of Europe, U.S. National Science Foundation has launched two projects (GENI and FIND), and Japanese and South Koreans have their own efforts too. Although all these national or regional projects aim for rising to the challenges the Internet is facing, and they speak for and understand the need of international cooperation, a significant motivation for them is the (foreseen) strategic importance of the Internet. Thus every nation tries to shore up their future position in the networked world through being a key player in the development of the next generation Internet.

Table 5: Future Internet research efforts

Europe	**Country**	**Link**
FIA: Future Internet Assembly	EU	www.future-internet.eu
Future Internet programme	Finland	www.futureinternet.fi
Internet del Futuro	Spain	www.internetdelfuturo.es
G-Lab	Germany	www.german-lab.de
GRIF: Groupe de Reflexion Internet du Futur	France	
Ambient Sweden	Sweden	www.vinnova.se/upload/EPiStorePDF/AmbientSweden.pdf
IBBT: Interdisciplinary Institute for Broadband Technology	Belgium	www.ibbt.be
Luxembourg IPv6 Council	Luxembourg	www.ipv6council.lu
	Italy	http://cit.fbk.eu/future_internet
	The Netherlands	www.futureinternet.ez.nl
	Ireland	www.futureinternet.ie
	UK	www.internetcentre.imperial.ac.uk
Other	**Country**	**Link**
GENI: Global Environment for Network Innovations.	USA	www.geni.net
FIND: Future Internet Design	USA	www.nets-find.net
AKARI: Architecture Design Project for New Generation Network	Japan	http://akari-project.nict.go.jp/eng/index2.htm
FIF: Future Internet Forum	South Korea	www.fif.kr/

5 Scenario construction process

In this chapter the process used in constructing scenarios is presented. The findings are expressed in form of key trends and uncertainties which summarize the acquired understanding of the Future Internet.

5.1 Brainstorming

Key trends and uncertainties were identified in three brainstorming sessions organized in the autumn of 2008. Each session had 6-8 academics/industry experts representing different stakeholders. PEST framework was used to cover broadly all the important macro-environmental factors affecting the Future Internet. Different domains of the framework were brainstormed separately in two phases (1. nominal, 2. interactive). First, every participant had 10 minutes to write statements to Post-its about forces having effect on the Future Internet. Discussing was forbidden but couple of key words were shown to guide and help the thinking (Figure 8). Second, the participants were asked to present their thoughts in the order of importance. In this phase (30 min) discussion was open and similar Post-its were grouped. After rapid exchange of thoughts a grouped idea was placed on one of the four boxes of flip chart matrix (Figure 9) based on its importance and uncertainty. All the identified forces from three sessions are listed in Appendix A.

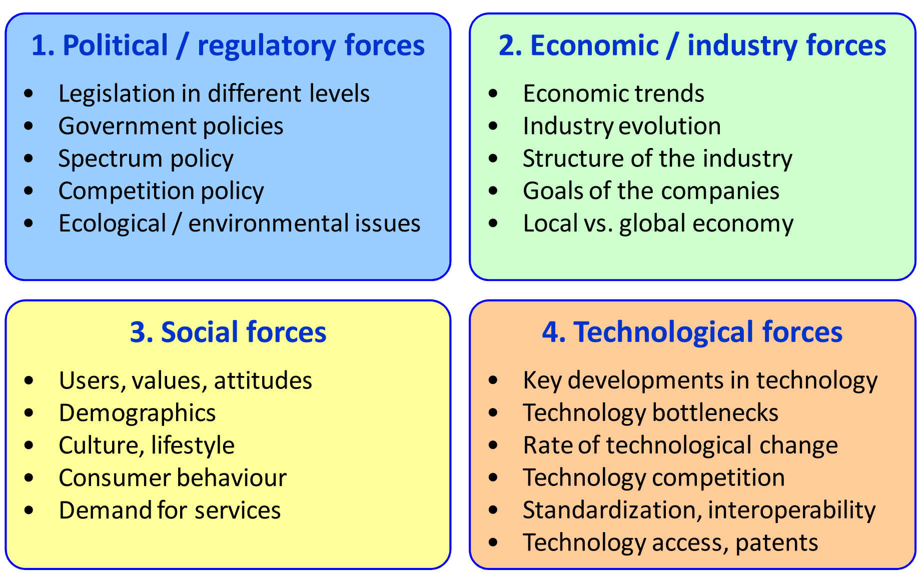

Figure 8: List of key words used to feed the brainstorming

5.2 Key trends

Key trends are important factors that are certain or very likely to realize and have significant impact on the Future Internet. They are underlying all four scenarios and are assumed to be valid with a reasonable probability for the chosen ten-year period. Final key trends presented in Table 6 are combined from several trends identified in the brainstorming sessions. The presentation is divided into four categories based on the PEST framework.

Table 6: Key trends

Political/Regulatory trends
PT1: The society will be increasingly dependent on the Internet.
PT2: The world (and the Internet) is moving from unipolar to multipolar.
PT3: The usage and allocation of spectrum will be more market-based.
PT4: Environment and energy will be more important.
Economic/Business trends
ET1: The world is moving from products to services.
ET2: Using ICT becomes low-cost compared to manual alternatives.
ET3: Power consumption becomes a cost driver in ICT.
ET4: Globalization continues.
Social Trends
ST1: The Internet is integrating deeper into everyday life.
ST2: Desire for all around availability increases.
ST3: Social networking will be faster and stronger.
ST4: Content creation will be more user-driven.
ST5: Internet generation continues to drive Internet usage.
Technological trends
TT1: Mobile always-on Internet connectivity increases.
TT2: Performance continues to improve.
TT3: Complexity of software, services and architectures increases.
TT4: Diversity of networks and devices increases.
TT5: Remote management of network and home devices increases.

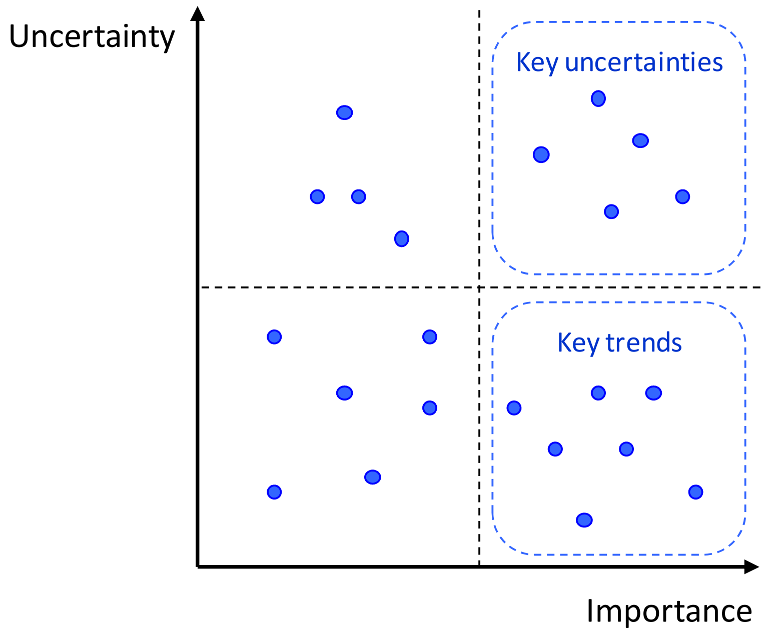

Figure 9: Flip chart matrix used in evaluating the importance and uncertainty of identified forces.

5.2.1 Politic/Regulatory trends

- **PT1: The society will be increasingly dependent on the Internet.** Economy, industry, administration, and education move their operations increasingly to the Internet and manual fall-backs in problem situations are disappearing. This raises governmental interest in regulative control through re-regulation.

- **PT2: The world (and the Internet) is moving from unipolar to multipolar.** The U.S.-centered western world loses its dominant role since the rise of China, India, and other developing nations scatters the power around the globe. Additionally, the next 2 billion Internet users come mostly from the 3rd world and developing nations.

- **PT3: The usage and allocation of spectrum will be more market-based.** Increasing mobile Internet usage channels more spectrum for Internet access. Spectrum usage will be more effective and spectrum auctions are used in most countries.

- **PT4: Environment and energy will be more important.** Environmental awareness increases and energy consumption is controlled and regulated stricter.

5.2.2 Economic/Business trends

- **ET1: The world is moving from products to services.** The money is on the services, because producing goods is highly competed on the global space. The Internet speeds up this development.

- **ET2: Using ICT becomes low-cost compared to manual alternatives.** Cost reductions and possibility for rationalization of business processes drive adoption of ICT in every field of economy.

- **ET3: Power consumption becomes a cost driver in ICT.** Awareness of ICT's power consumption and environmental effects increases at the same pace with improving performance of devices. Therefore, energy efficiency becomes an important design criterion. "Green ICT" is also seen as having marketing value.

- **ET4: Globalization continues.** This old trend continues to hold true since countries depend more and more on each other and borders disappear. However, in the future globalization will be stronger in service and knowledge industries than in manufacturing industries.

5.2.3 Social trends

- **ST1: The Internet is integrating deeper into everyday life.** Mapping between the real and virtual worlds tightens and people are increasingly able and willing to use Internet services. Tighter integration creates need for improvements in security, trust, and privacy.

- **ST2: Desire for all around availability increases.** People are used to being reachable all the time with their mobile phones and now the same level of accessibility to email, social networking sites, and instant messaging is generating a demand for mobile data services. This is supported by the increasing use of location and context information.

- **ST3: Social networking will be faster and stronger.** Social networking services gain importance and affect how people communicate and consume. For example, the increasing usage of ratings and suggestions from other consumers changes buying behavior.

- **ST4: Content creation will be more user-driven.** The easiness of creating and sharing content in the Internet drives to YouTube and Wikipedia[10] style of services where users are active participants and not just passive consumers.

- **ST5: Internet generation continues to drive Internet usage.** Young people are eager to adopt new services while old people are not able to do that. This preserves the generation gap between the Internet generation and older people.

5.2.4 Technological trends

- **TT1: Mobile always-on Internet connectivity increases.** The Internet will be used more and more with small, portable devices like mobile phones, PDAs, and ultra-portable PCs. Additionally, for many new users mobile connectivity will be the first and only access method.

- **TT2: Performance continues to improve.** Processing power improves, optical transmission boosts transfer rates and storage capacity increases. These improvements can also be seen in better price-performance ratios.

- **TT3: Complexity of software, services and architectures increases.** Patch-on-patch tradition and new requirements increase the complexity of networks. At the same time usage of new applications is still too complex for most users. This raises usability and reliability questions to a new level.

- **TT4: Diversity of networks and devices increases.** The Internet of things spreads ubiquitous computing quietly and increases the amount of hosts significantly. The diverse device base is connected to the Internet with a variety of access technologies. Also machine-to-machine communication brings new requirements for networking.

[10] http://www.wikipedia.com

- **TT5: Remote management of network and home devices increases.** Managing prolific and more complex device base will be carried out more and more remotely. This will happen both in households and in the core network.

5.3 Initial key uncertainties

Key uncertainties are important factors with uncertain direction and impact on the Future Internet. While key trends form a stable ground for scenarios, key uncertainties make them distinct from each other. Identifying and formulating the key uncertainties was not as straightforward as finding key trends. The process was iterative and consisted of three steps. First, the initial key uncertainties presented in this chapter were formed based on the brainstorming sessions. Second, some experts were interviewed. During this step many important things were discovered. Third, the gathered feedback was used to form the final key uncertainties. Each step used in the build-up of the final key uncertainties is presented one-by-one.

The main concern in the brainstorming sessions related to the scalability of the Internet. Depleting address space combined to painful IPv6 migration, choking routing system, increasing energy consumption and problematic purposes of use like multicasting raised a concern, will the Internet scale up. Collision between Internet's built-in freedom and increasing pressure to control the usage formed to the uncertainty whether control will increase in the Internet. Increasing complexity of the Internet combined to its criticality brought up concern, what would happen if the Internet were to face a larger collapse. To summarize, the initial most important key uncertainties are listed below.

Initial key uncertainties

1) Will the Internet scale up?
2) Will control clearly increase in the Internet?
3) Will the Internet face a larger collapse?

First two of these were chosen to form the initial scenario matrix (Figure 10), while a larger collapse was seen rather as a catalyst that could speed up the changes and thus is of high interest.

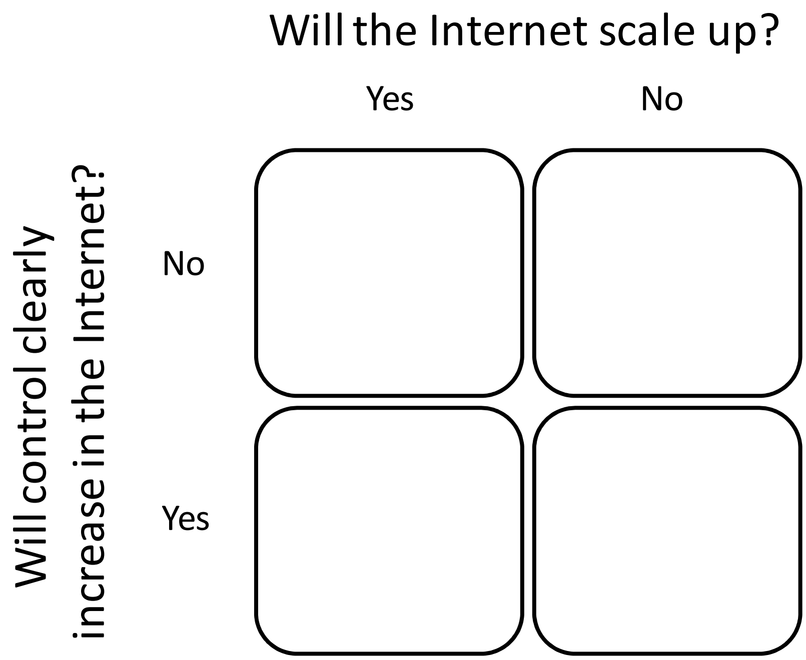

Figure 10: Initial scenario axes

5.4 Expert interviews

Due to the rapid nature of brainstorming it was not possible to get complete understanding of forces, especially of uncertainties, during the sessions. Thus altogether 11 experts from different fields were interviewed to deepen the knowledge. The interviews were conducted between December 5, 2008 and January 21, 2009 in Helsinki and Espoo. Table 7 lists the interviewed persons.

In the beginning of each interview the topic was introduced by explaining the key trends. The main focus was to confirm the selected most important key uncertainties. The interviews were unstructured and the emphasis varied depending on interviewee's area of expertise. For example with regulative authority representatives concentration was on the control uncertainty. Although the interviews succeeded in improving understanding, the initial purpose of confirming chosen scenario axes was not accomplished. Topics behind the initial most important key uncertainties were seen important and had great deal of uncertain elements but the formulation of them was problematic. Following sections explain why the initial most important key uncertainties needed to be refined.

Table 7: List of interviewees

Name	Working title	Organization
Pekka Nikander	Chief scientist	Ericsson Research Nomadic Lab
Jukka Manner	Professor, Networking technology	TKK / Dep. of Communications & Networking
Klaus Nieminen	Senior Advisor	FICORA
Kari Ojala	Communications Counselor	Ministry of Transport and Communications
Ossi Pöllänen	Senior Expert	Nokia Siemens Networks
Hannu Flinck	Manager, Future Internet	Nokia Siemens Networks
Timo Ali-Vehmas	VP CIC	Nokia
Reijo Juvonen	Head of Operations, Research and Technology	Nokia Siemens Networks
Martti Mäntylä	Professor, Principal Scientist	TKK / HIIT
Matti Peltola	PhD Student	TKK / Dep. of Communications & Networking
Heikki Hämmäinen	Professor, Network economics	TKK / Dep. of Communications & Networking

5.4.1 Scalability

Discussions about scalability lead to the dilemma that although many scalability-related issues were seen uncertain in brainstorming, the possibility that the Internet would not scale, at least due to technical reasons, was seen not uncertain but impossible by most interviewees. When thought again, also the identified key trend about the society's increasing dependency on the Internet (PT1, see Section 5.2.1) creates economic pressure that ensures necessary efforts and investments to solve scalability bottlenecks. The key discovery was that scalability may be realized in many ways, not only implementing improvements to the entire Internet. Parallelism could be one solution, which, however, threatens the integrity of the Internet. Altogether the most severe scalability problems relate to new uses where the best effort Internet is not adequate.

5.4.2 Control

Word control caused different interpretations among the interviewees. Some of them associated it to regulative control, others rather to operator control. Thus a more generic definition of restricted versus free Internet was brought up, which matched quite well to the spirit of the brainstorming. Couple of interviewees proposed a separate examination from the viewpoint of all the possible control authorities including regulator, ISP, application service provider and consumer. This thought was processed and discarded since the resulting worlds would have been highly diverse depending on the chosen authority.

In discussions with regulative authority representatives it became clear that control does not automatically mean restrictions but may as well protect freedom. This applies especially to regulative control which may be seen as an adjustment lever ranging from anarchy to full control. The Internet has been self-regulated, which has enabled anarchistic behavior. Exponential growth and increasing role in today's society has brought side-effects that need to be controlled. In the best case regulation enables freedom through reasonable set of laws, not anarchistic freedom, and thus some level of control is favorable.

Based on the interviews evolution of the control in the Internet is comparable to the evolution of automotive legislation. Driving a car was nearly completely unregulated in the beginning but in the course of time when car penetration has increased also the control has increased. This analogy is supported by the interviewees' opinion that control will increase in the Internet during the next 10 years. Hence it is justified to say that increasing control is a trend, and it is actually the result of this development which remains nebulous.

5.4.3 Collapse

A larger collapse was defined as an event that would black-out parts of the Internet for a short period of time. It has significant analogies with the current financial crisis. If a larger collapse would happen, it would probably cause severe economical losses and reduce people's trust on the Internet. Regardless of possible consequences many interviewees were skeptical if a larger collapse really would have a permanent and significant impact on the Internet's evolution. The experts argued that decision-makers do not have enough knowledge on the possible solutions and that people do not easily change their behavior. Thus the effects would be limited to faster implementation of new technical or regulatory means, increase in regulative control, and higher level of back-ups. The most important notion from this uncertainty is that the fear for collapse drives for pre-emptive actions like improving resiliency of the networks and services.

5.4.4 Other thoughts

After fruitful discussion about initial key uncertainties the experts were asked to give some thoughts about possible scenarios sketched in Figure 10. The most problematic scenario was the one with no scalability and no increasing control. Firstly, the interviewees were seeing scalability and control increase as trends, and secondly, if the Internet did not scale up, the control would certainly increase. This opinion signaled that chosen scenario variables were not independent enough.

Although the interviews did not give too much direct support to chosen scenario variables, they succeeded in refining them. Understanding the real issues behind the control uncertainty was one important thing but especially significant was the repeatedly mentioned concern about fragmentation of the Internet. Most often fragmentation was seen as a result of, and solution to, scalability problems but experts also saw it as a possible outcome of increasing control and a larger collapse. Based on these two key findings it was possible to formulate the final key uncertainties.

5.5 Final key uncertainties

The final key uncertainties are divided into two groups: the most important span the scenario matrix while the less important add flavor to the scenarios. Additionally, uncertainty related to the possible collapse of the Internet is discussed separately from the scenarios. All the key uncertainties are listed in Table 8 and introduced in-depth in the next sections.

Table 8: Final key uncertainties

The most important key uncertainties
U1: What will be the network structure?
U2: What is the level of openness of content, applications, and hosts?

Other key uncertainties

U3: Where will the intelligence be located?

U4: What will be the dominating business model in the Internet economy?

U5: How will solutions for trust, security and authentication be implemented?

U6: Will the traffic be treated neutral?

U7: The amount of standardization: standards vs. proprietary solutions?

U8: Where will the standardization happen?

Separate key uncertainty

U9: Will Internet face a larger collapse?

5.5.1 The most important key uncertainties

The most important key uncertainties were derived in an iterative process in which interviews played a key role. The initial key uncertainty of scalability of the Internet formed to the question of the network structure, to the level of fragmentation of the Internet, to be exact. The control uncertainty, for one, transformed to deal with the openness of content, applications and hosts.

U1: Network structure

The Future Internet may either remain a whole network or it may fragment into many networks. The characteristics of these two extremes – one network vs. fragmented network – are presented by relating questions listed below.

Relating questions

Will there be free connectivity in the Internet?

Will the Internet be able to scale up?

Will the Internet be suited to all purposes of use?

Although the Internet consists of many different networks they still form one Internet where, at least theoretically, every host is able to connect to every other host only by knowing their IP addresses. The flexibility of the Internet protocol suite has allowed the all-IP trend meaning that the IP technology is used for various networking needs including telephony and video services. This development underlines the possible cost savings that the economies of scale enable when only one network infrastructure is used.

Regardless of the same network technology, telephone traffic is still separated from data traffic to its own network. In a truly single network there is not that kind of separation. All the traffic flows in the same wires and diverse requirements of different traffic types can be taken into account at the network level. Fundamental prerequisite of one network to be possible can be expressed as a slogan *"one size fits all"*.

Fragmentation would mean that free end-to-end connectivity would be questioned. Extensive usage of NATs, firewalls and other middle-boxes alike disturb already nowadays end-to-end connectivity. Due to the importance of the connectivity complete separation of the networks does not seem feasible but the connectivity may be heavily restricted so that all traffic between networks travels through gateways. The fragmentation does not need to happen in the physical level but it can as well – or even more probably – happen in the service level through overlay networks. These overlays borrow only the connectivity from the Internet and use their own, possibly proprietary protocols to fulfill requirements that the core Internet architecture is not capable to satisfy. These solutions, however, break the Internet architecture intentionally and thus increase complexity of the Internet ecosystem.

Scalability (from a technical viewpoint meaning a large enough address space, fast enough routing protocols and algorithms, and small enough energy consumption) is one issue that can be solved either in the level of the Internet architecture or by building separate networks. The applicability of the Internet to every imaginable and non-imaginable purpose of use is another type of scalability issue that affects substantially the level of fragmentation. For instance, end-to-end multicasting and end-to-end quality of service (QoS) are not well supported by the best effort type of service. Increasing real-time (video) traffic is one of those applications that have created demand for specialized network fragments called content delivery networks (CDNs). They are able to offer guaranteed quality of service for those who are willing to pay. Privacy requirements of companies create business case for virtual private networks (VPNs) and national security concerns may make some countries to build separate secure networks with strong authentication, or even to close their networks from the world outside.

U2: Openness of applications, services and hosts

While the other scenario axis has basis in the network layer this one relates to the upper layers of the protocol stack. Applications, services and hosts may either be open like PC's and their open source software or closed like Apple's iPhone with proprietary software. After recognizing the importance of this uncertainty, the same thought was found from Jonathan Zittrain's book (2008). Zittrain uses the word generativity to describe the level of openness. The both possible worlds – open and closed – are explained by relating questions listed below.

Relating questions
Are the hosts freely programmable?
Are users willing to be dependent on a single actor?
Do users prefer bundling or buying separately?

The world of open applications, services and hosts is the world of PC-like multipurpose devices. A single device is used to access various kinds of applications and services, and is able to suffice most purposes of use. Successful and open standardization, particularly in the application level, and high availability of open source software mean that everyone has in principle the possibility to program own applications. Closed applications, services and hosts, for one, are optimized for some usages (or even for a single use). Specialization may enable better usability and fewer bugs since all the use cases are predictable, but it restricts versatility. Security is another issue that is much easier to take into account in closed systems. Actually, Zittrain (2008) sees security nuisances of open systems one of the most important drivers for closed world.

All the causal factors relate to the question: who has the control over users' actions? In the open world user is the king of the hill. The Internet offers wide selection of services and user has the freedom of choice. He can install whichever applications he wants and is not locked in to one service for a long period of time. Thus open world is naturally competitive and business model -wise mostly advertisement-based. Anonymity is still possible in the Internet, which makes it more difficult to enforce copyright and IPR (Intellectual Property Rights) regulation than in closed systems. Respectively, in the closed world, user has handed the control to another actor. Companies can most easily acquire this kind of control position through end user devices that cannot be changed to new ones as often as applications and services. There are already plenty of examples of this kind of closed devices. For instance, Microsoft's xBox[11], like all the other game consoles, is actually a PC performance-wise but Microsoft decides, which games are allowed to be run in them. The strong control over users creates opportunity for other business models than ad-based, e.g., subscription-based, to succeed.

User's strong position in the open world has, however, a flip side – responsibility. Openness requires more purchase decisions, and user's knowledge on purchase situations needs to be higher. Also finding and installing services rely on user's competence and activity, and the same applies to security. Bundling devices, applications, services and even networks together is one method by which a stakeholder may try to get customer locked in and dependent on single actor. From user perspective bundling reduces the amount of purchase decisions and may thereby be an easier choice, especially for technology non-enthusiasts. Another advantage from customer perspective is that the providers of closed systems can more easily be held accountable and responsible in front of malfunctioning.

5.5.2 Other key uncertainties

The other key uncertainties with their extreme outcomes are presented here briefly. They are scaled in a five-point scale between the two extremes (Figure 11 - Figure 16). Later, when scenarios are presented in Chapter 6, the values for each scenario are showed.

U3: Where will the intelligence be located?

Originally the Internet was a dumb network connecting smart hosts. The hosts were equal in their capabilities and roles. Client-server model used widely in the Web differentiated the roles of the hosts. High level of intelligence in clients indicates more important role of peer-to-peer model, whereas significant amount of intelligence in servers speaks for client-server model. It is also constantly questioned if any intelligence

[11] http://www.xbox.com/

should be inserted to the network. Thus the question here is divided into two questions: 1) client vs. server and 2) end points vs. network.

	Where will the intelligence be located?	
	Client vs. Server	
In clients	○ ○ ○ ○ ○	In servers
	End points vs. Network	
In end points / edges	○ ○ ○ ○ ○	In the network

Figure 11: U3 - Where will the intelligence be located?

U4: What will be the dominating business model in the Internet economy?

Simple and "free" ad-based business model has been by far the most successful revenue model when Internet services are considered. Transaction-based business model, like paying with PayPal or credit cards, has been mostly used when physical goods are sold through the Internet. Additionally, subscription-based model would be highly interesting to companies and simple enough for users. Thus the big question here is, will the Internet business be mostly ad-based or do other models break through?

	What will be the dominating business model in the Internet economy?	
Ad-based model	○ ○ ○ ○ ○	Other models

Figure 12: U4 - What will be the dominating business model in the Internet economy?

U5: How will solutions for trust, security and authentication be implemented?

Lack of trust, security and authentication is a recognized challenge that needs to be tackled somehow, at least in the case of mission-critical applications. Universal, open solutions built in the architecture are a reasonable option, but closed solutions relating for example to separate network or to provider-controlled solutions in closed architecture are other choices.

How will solutions for trust, security and authentication be implemented?		
Openly in the architecture	○ ○ ○ ○ ○	Somewhere else in closed form

Figure 13: U5 - How will solutions for trust, security and authentication be implemented?

U6: Will the traffic be treated neutral?

The principle of net neutrality requires that all content, sites, and platforms are treated equally (Wu, 2009). In a neutral network traffic flows related to for instance e-banking, video streaming, peer-to-peer file sharing or emailing are not treated differently but they all have same priority level from the network perspective. Blocking content and communication is one of the things that violate net neutrality.

Will the traffic be treated neutral?		
Yes	○ ○ ○ ○ ○	No

Figure 14: U6 - Will the traffic be treated neutral?

U7: Amount of standardization: standards vs. proprietary solutions?

The Internet architecture relies heavily on open standards (RFCs). On the application and service level, proprietary solutions have, however, an important role. For example some important network overlays, VoIP network Skype and peer-to-peer file sharing network BitTorrent[12], are based on proprietary solutions. Standards allow competition, while proprietary solutions enable emergence of monopolistic pockets. The question here is: will the Internet be based mostly on standards or on proprietary solutions?

Amount of standardization: standards vs. proprietary solutions?		
Standards	○ ○ ○ ○ ○	Proprietary solutions

Figure 15: U7 - Amount of standardization: standards vs. proprietary solutions?

[12] http://www.bittorrent.org/

U8: Where will the standardization happen?

Internet-related issues have been traditionally standardized in the IETF. After the commercialization, other forums have emerged including W3C (The World Wide Web Consortium) concentrating on Web standards and 3GPP (The Third Generation Partnership Project) working for the third generation mobile phone system. Standardization could also be done in industry-driven forums that would be open only for part of the Internet industry.

	Where will the standardization happen?	
IETF	○ ○ ○ ○ ○	Industry-driven forum

Figure 16: U8 - Where will the standardization happen?

5.5.3 Separate key uncertainty – U9: Collapse

Collapse uncertainty was firstly introduced in Section 5.3 as an initial uncertainty after which its role in the scenarios was evaluated again. A larger collapse blacking out parts of the Internet for some period of time could wake-up the Internet community, especially decision-makers, and thus disrupt Internet's evolutional development and speed up some changes. Depending on its nature, a larger collapse could create pressure to whichever direction following both scenario axes (although pressure towards network fragmentation and closed applications, services and hosts seems stronger) meaning that a larger collapse will rather lead to a scenario, not vice versa. Hence the collapse uncertainty is studied separately from the scenarios by identifying several possible causes and their consequences (Table 9).

Table 9: U9 – Possible causes for collapse

Cause	Explanation	Consequences
Terrorism or cyber war	A very significant nation in the Internet (e.g. U.S.) closes its network in front of terrorism or cyber war.	Functional halt for some period of time. Driver for multipolarity.
"Cisco worm"	A worm using severe security hole in routers causes a Morris worm (Reynolds, 1989) like phenomenon.	Internet connectivity breaks all around the world.
Information breach or seepage	Breach or seepage (and misuse) of massive amount of sensitive personal information stored by e.g. Google, Facebook or credit card companies.	Trust in the Internet decreases and it is hard to get back. Openness vanishes. Handling money in the Internet decreases.
Signaling fault	Internet routing and signaling system is more and more complex, which may lead to misconfigurations causing signaling fault.	Level of protection increases. Operator control increases. May speed up take-up of IPv6.
New type of unwanted traffic	Huge amounts of some new type of unwanted traffic.	Consequences vary depending on the type of unwanted traffic.
Public key cryptography becomes unusable	Some fundamental deficiency in public key cryptography is found and it cannot be easily fixed.	Systems using public key cryptography need to be shut down and a new security solution needs to be adopted.
Sudden extinction of IPv4 addresses	Free pool of IPv4 addresses is about to be exhausted in couple of years. Hoarding of addresses may lead a sudden extinction of them.	Growth of the Internet is questioned. New ways to allocate IPv4 addresses or adoption of IPv6 needed.
Denial of Service attack	A DoS attack on a fragile and critical component of the Internet may black out parts of the Internet.	Openness of Internet decreases. Pressure for legal harmonization and for catching criminals increases.
Virus deleting lots of data	Rapidly spreading virus deletes lots of important data.	Trust in the Internet decreases. People wake up to demand means to provide better security.
Spam	Increasing amount of spam makes email unusable. It is impossible to separate useful mails from spam. Emails may be sent to false addresses or they may not be delivered at all.	Better way to avoid spam needed (e.g., authentication, email stamp). Other ways to communicate (e.g., IM, SMS, social networking sites) catch on.

6 Scenarios

The final scenarios were formed iteratively based on the interviews. The two most important key uncertainties were chosen to form a scenario matrix. Finally the scenarios were named descriptively to illustrate their idea immediately. The scenario matrix including some descriptive characteristics of each scenario is presented below in Figure 17.

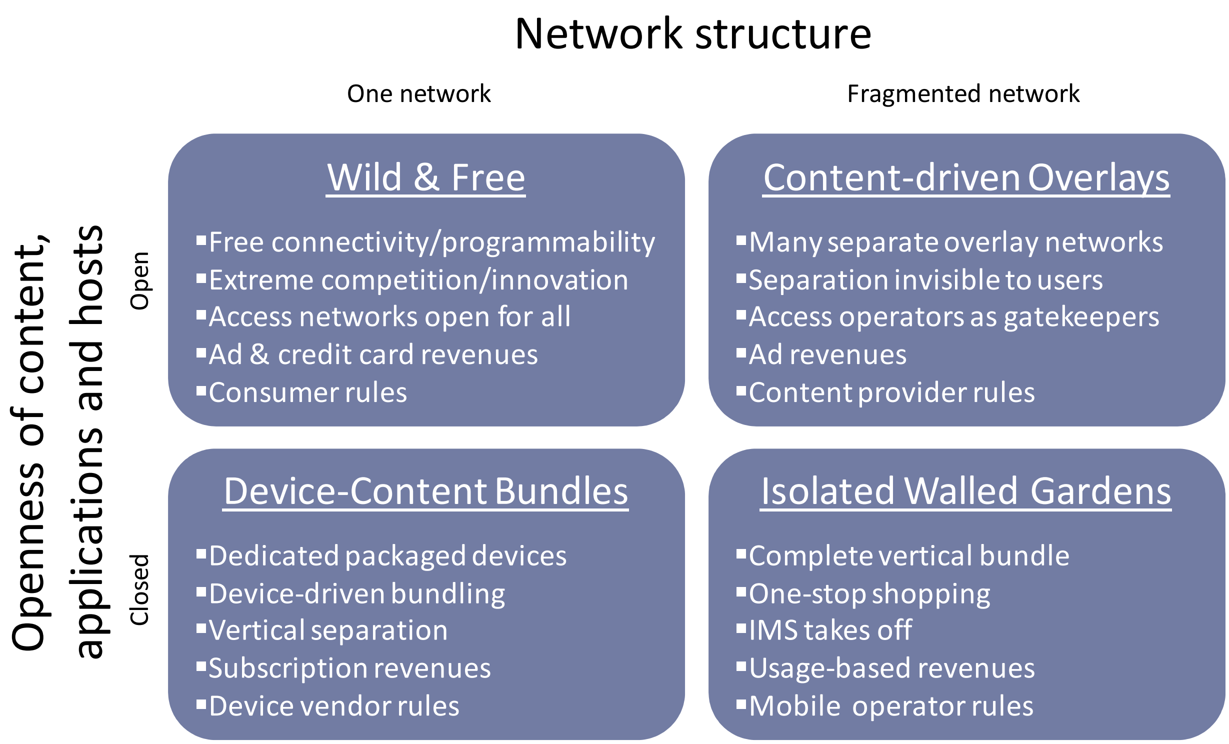

Figure 17: Scenario matrix

As for the Internet evolution, it cannot be described only by two variables. Other key uncertainties and their impact on the scenarios are presented in Figure 18. The uncertainties are valued in the five point scale between the two extremes, and together with trends they add more flavor to the scenarios. Although values of the uncertainties give some idea about the scenarios, they are defined in more detail in the next sections. First, the descriptive narratives about the Internet in 2018 are presented for each scenario. This is followed by explaining the differences between the scenarios in architectural structure and in value distribution in the next chapter.

1 = Wild & Free
2 = Content-driven Overlays
3 = Device-Content Bundles
4 = Isolated Walled Gardens

U3: Where will the intelligence be located?						
			Client vs. Server			
In clients	●	●	○	●	●	In servers
	1	2		3	4	
			End points vs. Network			
In end points / edges	●	●	○	●	●	In the network
	1	3		2	4	
U4: What will be the dominating business model in the Internet economy?						
Ad-based model	●	●	●	○	●	Other models
	1	2	3		4	
U5: How will solutions for trust, security, and authentication be implemented?						
Openly in the architecture	●	○	●	●	●	Somewhere else in closed form
	1		2	3	4	
U6: Will the traffic be treated neutral?						
Yes	●	○	●	○	●	No
	1		2,3		4	
U7: Amount of standardization: standards vs. proprietary solutions?						
Standards	●	●	●	○	●	Proprietary solutions
	1	2	3		4	
U8: Where will the standardization happen?						
IETF	●	○	●	○	●	Industry-driven forum
	1,2		3		4	

Figure 18: Uncertainties valued in five-point scale

6.1 Wild & Free

In the wild and free Internet a multitude of services and applications are offered in a single network. The Internet architecture is hourglass-shaped like the original Internet architecture and in some sense Wild & Free means returning to the roots of the Internet, where peer-to-peer communications is really important. Users have versatile, freely programmable devices that can connect freely to each other and to any available content, service and application. Free connectivity has reached its ultimate level since access networks have been opened and all users can connect to the Internet through whichever network they want.[13] Consumers are kings who enjoy the ever-increasing supply of new services and are not willing to constrain on the service offering of a single company. Due to absence of lock-ins consumers can easily switch from a service to another, if a better service becomes available. Thus it is difficult for other business models to compete with advertisement-based model offering the service "for free" to the customers. In some cases, however, credit-card based payments are used.

The current and forthcoming scalability problems have been solved so that Internet can handle both increasing amount of users, hosts and traffic as well as old and novel usage scenarios with diverse service level requirements. Some examples of success stories are eventual adoption of IPv6 and implementation of end-to-end multicast and end-to-end QoS in the protocol level. Success in solving the core problems in technological domain has allowed regulator to concentrate on enabling competition and innovation in the free markets. The last monopolistic pocket in the Internet, access networks, is brought down, and thus the industry is completely horizontal and extremely competitive.

The IETF has come to its own and standardization and open source software are seen important. Trust, security and authentication are implemented openly in the architecture but only concerning those applications that require them. Due to free programmability and imbalance between regional regulations, unwanted traffic remains as a serious problem and the race between malware makers and security companies continues. Additionally, anonymity in the Internet is still possible, although tracking of (hostile) users is easier than nowadays.

6.2 Isolated Walled Gardens

Isolated walled gardens are access operator centric network fragments[14] which bundle all the components of the value chain – devices, network and content – together. The complete vertical bundle means that access operators have control over end users and content. Devices, software and Internet connection are sold at the same time by access operators who also take the responsibility for managing the complete package remotely.

[13] This could be realized for example by socializing the access networks, introducing global authentication or extending ad-based business model to access networks.
[14] Also some countries may build isolated walled gardens which cover the whole country.

This decreases the amount of (purchase) decisions needed and makes life easy for consumers. Customer experience and security are optimized by letting consumers to install only those applications and use only those services that access operators have allowed to be offered in their networks. Restrictions in installing applications leads to the situation in which most of the services are running on the servers of the providers who need cloud computing style-of-solutions to scale to the increasing usage.

Technology-wise Isolated Walled Gardens is the IMS (IP Multimedia Subsystem) world. Refined usage-based monthly billing is possible and is used extensively like in the telco world. The dominant role of access operators means that the largest amount of profits is flowing in their pockets. Japanese mobile telephony market (e.g. NTT DOCOMO[15]) is an existing example of strong operator controlled value chain which resembles the Isolated Walled Garden scenario.

Some of the network fragments are interoperable, while others are isolated by design. However, interworking between competing access operators is always separately negotiated, which means more proprietary solutions and standardizing interfaces only. A strong industry forum driven by access operators has replaced IETF-style of standardization. This change combined with restricted programmability results in the situation where open innovation and entering the Internet business becomes much more difficult leading to oligopolistic markets and higher prices. Internet pioneers and academics are longing for *"the good old Internet",* while many users are satisfied with better security, quality of service and trust between the users.

6.3 Content-driven Overlays

Because the common Internet architecture has not been able to support all the varying service requirements of different applications, the network is fragmented into overlay networks based on content type and application. Companies, mostly content providers, offer better quality of service in dedicated service networks like video streaming CDNs. At the same time governments and companies have built secure networks for critical functions of the society. Although all these overlays are built on the top of IP, they are

[15] http://www.nttdocomo.com/

optimized for certain use and have much tighter control over the traffic generated by end users. To achieve better performance and conformance to standards, the common Internet architecture is intentionally broken when needed, which increases the complexity of the networks.

Building of dedicated networks is paid by competing content providers which try to attract as many customers as possible to maximize advertiser value. This puts companies in unequal position since those providers which are able to pay for better quality, get it, and those which cannot afford, must content themselves on poorer quality. This favors large players which can attract more customers and thus more advertisers by offering better services. From consumer point of view the situation is good since fragmentation of the networks is invisible to them, and they just enjoy broad variety of free, good quality services. Furthermore, regulators fight for open competition in the markets, which keeps prices low, decreases companies' possibilities to get customer lock-in, and favors ad-based business model. Although content providers skim the cream off the cake, access operators have important role in forwarding the traffic to the right overlay network.

If optimized network fragments fully take over, the development of the basic, best effort Internet may stop since the concentration is on content-driven overlays. Nevertheless, the network can also defragment, if an overlay (e.g., information networking or social networking) solves the largest problems that lead to the fragmentation.

6.4 Device-Content Bundles

While Internet usage moves increasingly from PCs to mobile phones and other portable devices, users' interest in installing applications and updating their devices themselves decreases. At the same time device vendors offer tempting device-content bundles which combine devices and services in a seamless manner. Due to their unbeatable user experience, including enhanced reliability and security, and hyper-usability, consumers are willing to accept lock-in. The Internet is still whole but consumers choose which part of the service offering is available to them when they purchase their devices.

Updating and installing new services is possible only through device vendor controlled service portals (like Apple's AppStore[16] and Nokia's Ovi[17]) meaning that device vendors take their share of all the purchases. Restricted ability to install applications raises the role of web applications and client-server model, which changes user devices from active participants to merely passive terminals and increases the importance of service clouds. This development leads to closed and more dedicated devices, resembling today's Xboxes and iPhones[18]. Device manufacturers' control enables subscription-based revenue models in which device price includes access to content and services for some period of time. Nokia's Comes with Music handsets[19] are an early example of this kind of innovative bundle.

[16] http://www.apple.com/iphone/appstore/
[17] http://ovi.nokia.com/
[18] http://www.apple.com/iphone/
[19] http://comeswithmusic.com/

7 Comparison of scenarios

In the previous chapter the scenarios were described one by one. In the following sections they are compared in terms of technical and business architecture and value distribution between different stakeholders.

7.1 Architecture

The architectural differences of the scenarios are illustrated in Figure 19. The presentation is simplified and takes into account only content, network, and end user devices. Content covers not only textual, audio and video data but also services and applications. The architecture can be understood both as business and as technical architecture which are uniform in the scenarios.

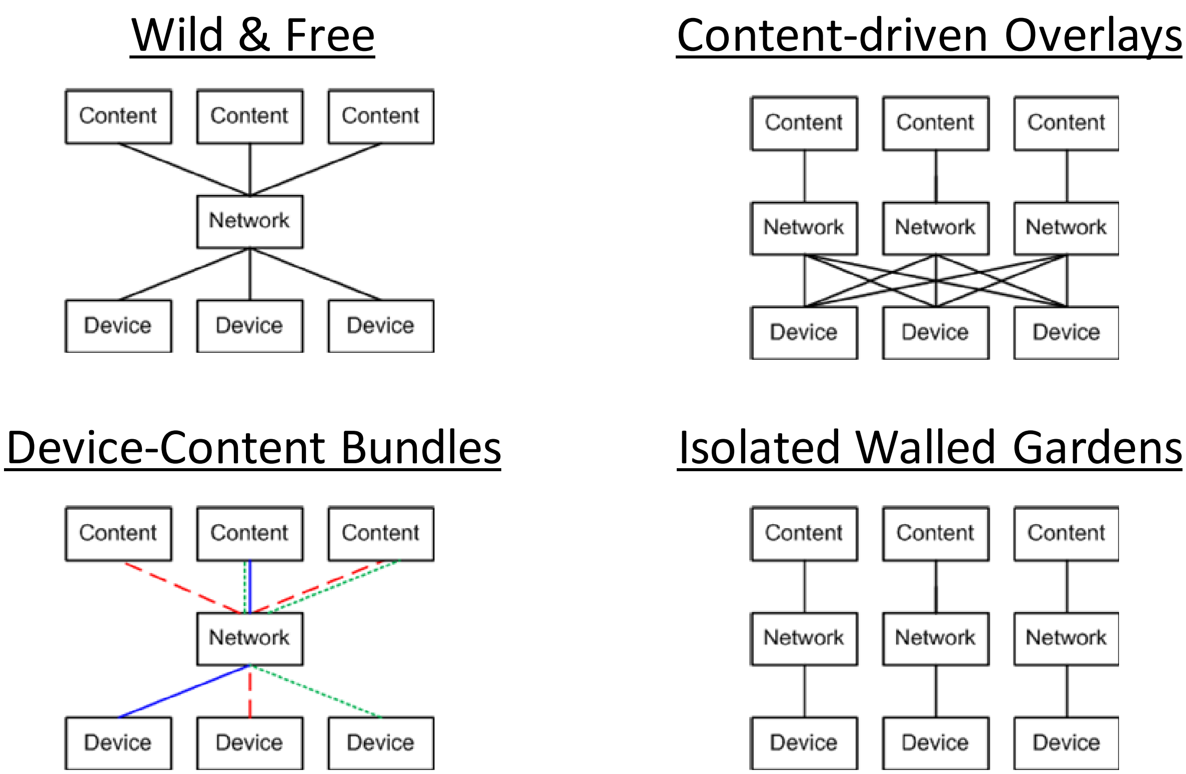

Figure 19: Simplified business and technical architectures in scenarios

Difference in network structure separates the left-hand side scenarios from the right-hand side scenarios. Openness of applications, services and hosts determines how devices can access the content. For example the Wild & Free and Device-Content Bundles scenarios share the same architecture with the exception that in Device-Content Bundles the device in use (and ultimately the device vendor) defines which part of the content is accessible.

In the Content-driven Overlays the content and network are bundled together, but devices can connect to every network, whereas in the Isolated Walled Gardens all the elements – device, network and content – are bundled together. Although the walled gardens are isolated, communication between users belonging to different networks is restrictedly possible through access operator controlled gateways.

7.2 Value distribution

The power positions of the most important stakeholders are illustrated by presenting value distribution in the scenarios. Figure 20, inspired by Christensen et al. (2001), depicts in a simplified manner to whose pockets the profits are flowing in. Device vendors include end-user device manufacturers like Nokia, Apple and Dell. Content providers cover software companies (Microsoft, SAP), Internet service giants (Google, Yahoo), media houses (NBC, BBC) and entertainment companies (Disney, Universal). Access operators include traditional ISPs like Comcast and Verizon as well as mobile operators like Vodafone and Orange. Backbone providers and network infra vendors are neglected in the figure since their profits are not analyzed deeper, although they may vary between scenarios.

The presentation is qualitative, although the money is presented as amount of coins. Thus only the ratio of coins inside a scenario and between the scenarios should be examined. For example, the Device-Content Bundles scenario is more profitable for device manufacturers than for access operators while the Content-driven Overlays offers best prospects for content providers. One important issue to clarify is the difference in the amount of coins between the Wild & Free and other scenarios. Due to the extreme competition covering every business sector the profits are smaller than in other scenarios since a larger part of the money remains in consumers' pockets.

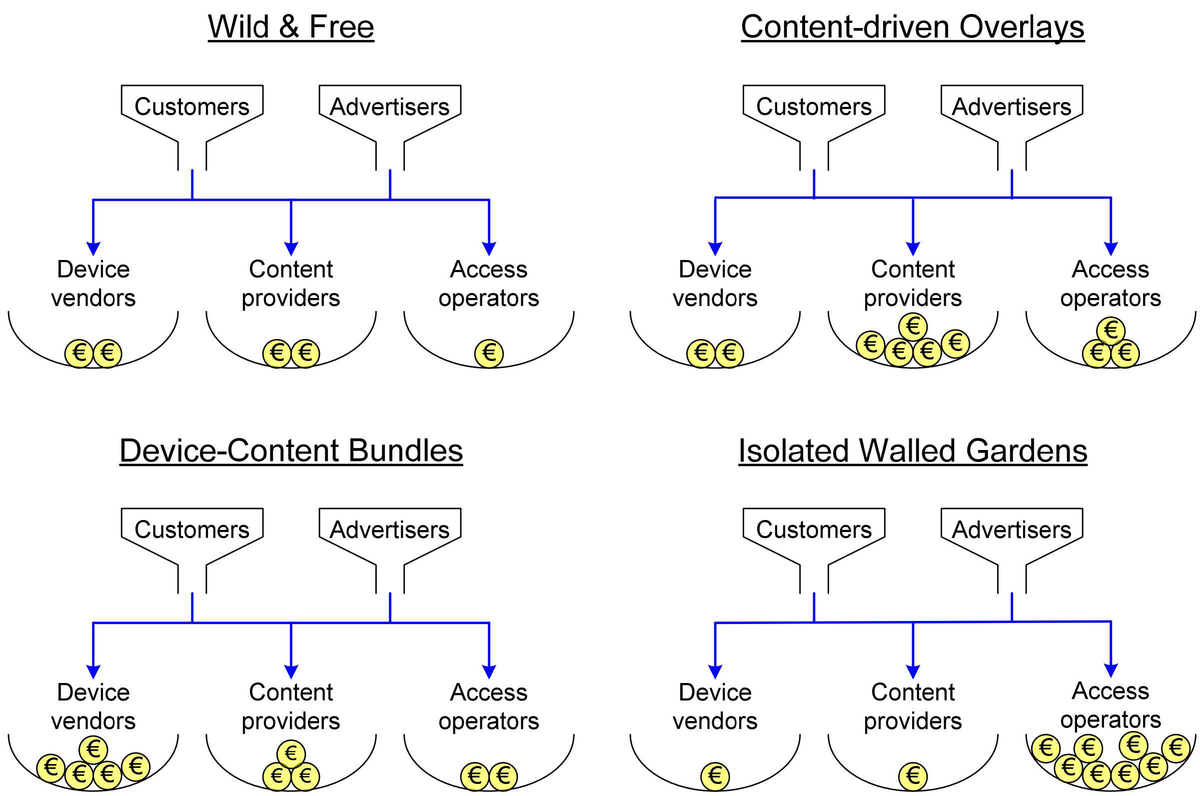

Figure 20: Simplified value distribution in scenarios

Which scenario is best for the society? Regulator's goal is to maximize social welfare which is compounded of customer surplus and producer surplus (Courcoubetis & Weber, 2003). Although it is difficult to say, which of the scenarios would be optimal from regulator's perspective, some speculation is still possible to carry out. The short-term societal optimum is close to users' momentary optimum which may be against of industry players' success. However, regulators typically try to see far instead of striving for short-term user value maximization. Thus the functioning of the whole Internet industry is of key importance and regulators need to take into account the welfare of all the stakeholders.

At least from short-term economic perspective Wild & Free seems to be favorable scenario because, due to extreme competition, customers' costs are smallest. Anyway, Wild & Free could be the best scenario also in the long term, since at least in the past the open and horizontal market (and network) structure has been highly successful in the Internet. Furthermore, characteristics of Wild & Free are typically linked to the fierce pace of innovation which is seen as a key ingredient in chasing the societal optimum. Innovation is naturally possible also in the other scenarios but higher market entry barriers and dominant player's control over innovators hinder perfect competition and full use of innovation possibilities. Completely vertical industry structure of Isolated Walled Gardens seems to be especially undesirable from this perspective.

On the other hand, the other scenarios than Wild & Free may be able to offer more value to users through better customer experience. Thus the societal welfare can also be reached in these scenarios but the regulator's task is more difficult since more restrictions to prevent emergence of monopolistic pockets in the market are needed. If the two scenario axes are compared to each other, the uncertainty concerning openness of applications, services and hosts has higher impact on social welfare than level of fragmentation has. Because of this, Content-driven Overlays can be seen as a slightly better scenario from regulator's perspective than Device-Content Bundles.

8 From scenarios to research strategy

Converting scenarios into strategy is a natural step after the scenario construction. Normally one stakeholder, either a company or an industry branch, is chosen and strategic suggestions to cope with each scenario are given. Based on the strategic analysis the stakeholder can either prepare for each scenario or try to use its (market) power to push through the most favorable scenario.

The key stakeholder in this exercise is the Finnish Future Internet (FI) program. It consists of multiple stakeholders that probably do not have a common opinion on each topic. Due to this the task is somewhat different compared to planning strategy for a single industry player. Hence the strategic suggestions are limited to research strategy. The goal is to describe the key research topics in each scenario. The idea is to jump to the year 2018, imagine one scenario at a time, and describe which development steps have been paramount. By analyzing which challenges have needed to be addressed in order to a scenario to come true, it is possible to suggest the key research topics for each scenario.

Next two sections first describe the current research plan of the FI program, and then present the key research topics for each scenario and their appearance in this plan. Furthermore, some suggestions, how FI program should provide for each scenario, are given. Experts were not interviewed in this part of the work and so the following analysis is based only on the self-obtained understanding of the scenarios.

8.1 Research plan of the Future Internet program

The research themes are structured into six work packages (WP0 – WP5) and to six cross issues like illustrated in Figure 21 (Juvonen, 2008). The focus is on three main themes studied in the work packages 1-3, namely the health of the Internet routing system (WP1), exploration of ways to improve the quality of end-to-end connectivity (WP2), and investigation of new ways of information storage and delivery (WP3). Additionally, several other important research topics with broader scope are covered by the cross issues.

The program looks at solutions with different time scales (Nikander & Mäntylä, 2008). Short term research topics (1-2 years) have a foreseeable deployment plan in next few years, whereas the main focus of FI program is in medium term research giving applicable results in 3-5 years. Long term research, for one, provides the overall vision, and answers to the question "where do we want to be in 10 years" by also suggesting more fundamental changes to the Internet architecture.

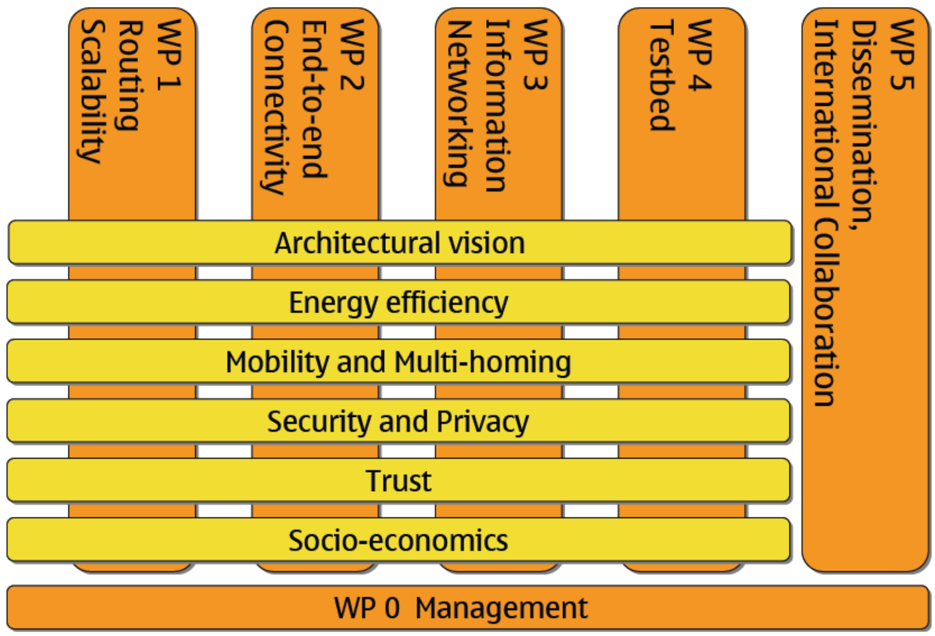

Figure 21: Work packages and cross-issues of FI Program (Juvonen, 2008).

8.2 Identified research topics

Table 10 lists some research topics which were identified to be important at least in one depicted scenario. The concise list highlights some topics brought up during the research. The importance of each research topic in every scenario is evaluated in three-level scale high-medium-low and the possible place in structure of the FI program is defined in the level of work package (WP) or cross issue (Cr. I.).

As can be seen, some of the research topics are equally important in every scenario. These topics stem from trends, like the first two topics in the list that tie up with the trends PT4 and TT1 (see Section 5.2). Trend-based research is secure and easily arguable although achieving unique breakthrough results may be more difficult since the whole research community is wrestling with the same problems. The importance of other research topics varies more between the scenarios. Some of them have background in trends but most of them relate rather to uncertainties. For example some research topics are more important in fragmented networks and some in one network. It is also clearly noticeable that majority of the research topics is important in the Wild and Free scenario, whereas far fewer topics have high importance in the Isolated Walled Gardens scenario. This can be interpreted so that many research topics require more attention in the wild and free world, where the solutions need to be implemented mainly in the core architecture, than in the world of isolated walled gardens, where the solutions can also be implemented either in individual network fragments or by closing the applications, services and hosts.

Table 10: Importance of the chosen research topics in the scenarios

		Importance in scenarios			
Research topic	**Place in FI program**	**Wild & Free**	**Content-driven Overlays**	**Device-Content Bundles**	**Isolated Walled Gardens**
Energy consumption	WP2, Cr. I.	High	High	High	High
Mobility and multihoming	WP2, Cr. I.	High	High	High	High
Privacy vs. Accountability	Cr. I.	High	High	High	Medium
Cognitive radio	-	High	High	High	Low
Universal (3rd party) authentication	Cr. I.	High	High	Medium	Low
Traffic & congestion control, load balancing	WP2	High	Medium	High	Medium
Lawful and fair use of resources	WP2	High	Medium	Medium	Low
Configuration agility	-	High	Medium	Medium	Low
Information networking	WP3	High	Medium	Medium	Low
Clean slate Internet	WP3	High	Medium	High	Low
Routing scalability	WP1	High	Medium	High	Low
Security and trust openly in architecture	Cr. I.	High	Medium	Medium	Low
Peer-to-Peer	-	High	Medium	Low	Low
DHCP-style network selection	-	Low	High	Low	Medium
Interconnectivity between networks	-	Low	High	Low	Medium
Building separate secure Internet	-	Low	High	Low	Medium
Cloud computing	-	Low	High	High	Medium
IP Multimedia Subsystem (IMS)	-	Low	Medium	Low	High

8.3 Future Internet program and scenarios

This section suggests how FI program could prepare to each scenario. Scenarios are gone through one-by-one and the analysis rests on the identified research topics (Table 10).

8.3.1 Wild & Free

The Wild & Free scenario is close to the traditional IETF ideology. All the critical shortcomings are solved in the core Internet architecture which is uniform and robust. Since FI program has heavy emphasis on IETF, this scenario is closest to the program. Table 10 suggests a long list of research topics important in this scenario and most of them are already addressed by the program. The problematic transition to IPv6 in mind it is arguable that making changes to the core architecture is difficult, even though the technical solutions would be ready and offer undisputable benefits. Thus the deployment of the derived results needs to be planned already from the start, if the intent of the program is to be something more than just an academic exercise. Backwards compatibility plays a key role since the overnight transition to a new architecture is not possible. Clean slate approach of information networking may be inevitable for Wild & Free to come true but its deployment needs to be even more carefully planned than the deployment of incremental changes.

8.3.2 Isolated Walled Gardens

The FI program has not prepared particularly well to this scenario. Finnish access operators are small compared to the giants like Vodafone and they do not have power to push for this scenario even though they certainly would be interested. However, network device vendors, especially those who have strong position in mobile access networks, may welcome this kind of world which favors players with telco background.

In Isolated Walled Gardens majority of the problems is solved by creating closed and more controlled networks. In this kind of environment most of the current and foreseeable problems relating for example to scalability, security and trust are easier to solve and this can be partially done by existing means. Hence the amount of research needed is smaller and large part of it is carried out by access operators. The research topics relate mostly to interconnectivity and interfaces between diverse network entities. The complexity of an isolated walled garden may be smaller than the complexity of a single network but the overall complexity increases with the amount of isolated walled gardens.

8.3.3 Content-driven Overlays

FI program is not best positioned to deploy content-driven overlays because the list of program participants (and Finnish industry in general) is missing large content providers which would benefit from research results that enable overlays. FI program could either start cooperation with large content houses or position itself as a developer of an IETF-centric and provider-independent platform which allows building of variable specified overlays through flexible tuning. WP3's work for information (or content-centric) networking suits well to this scenario which actually offers a clear deployment path for such clean slate approach. Another interesting research problem is how the hosts can choose a right overlay for right purpose. For instance a DHCP-like mechanism for network selection could solve the problem.

8.3.4 Device-Content Bundles

This scenario is close to the heart of Nokia, a key stakeholder of the FI program. Interestingly, however, no special attention is paid for this scenario. Fortunately this is not a large problem since due to the architectural similarity the research topics resemble those of the Wild & Free scenario. Altogether scenario axis based on network structure separates the (mostly architecture-centric) research needs more than the more application-oriented axis of openness. However, to make out in this scenario the FI program should concentrate more on developing lucrative business models and unbeatable user experience in the world of closed and more limited hosts. Because of the high importance of server-side operation or *"cloud computing"* cooperation with recently announced Supermatrix project is an important and natural possibility since many stakeholders participate on both projects (Finnet, 2009). The Supermatrix project aims at bringing 100-megabits connections to homes and providing the whole desktop as a service by moving execution of applications and storage of data to local supercomputers.

9 Conclusion

This chapter concludes the key findings, discusses the limitations of the study and exploitation of the results, and finally suggests some topics for future research.

9.1 Key findings

One of the key findings, even though an obvious one, is that in the future the Internet will be a critical infrastructural part of the society. The increasing importance diversifies the stakeholder corps and changes the co-operative playfield into a tussle in which political, economic and social motives are at least as important as technical enablers. The conducted study on historical milestones proposes that the success story of the Internet is based on the flexibility of Internet architecture and the capability of Internet community to introduce technical, bottleneck-removing solutions as an answer to the increasing demand and diversified application requirements. For the Internet-dependent society of tomorrow solving of emerging challenges is even more crucial but the work is more difficult and the possible solutions more unsure and diverse than before.

Scenario planning process bounds the uncertainty through identifying the key trends and, foremost, the key uncertainties. The uncertainty revolving around the Future Internet is defined by two independent key uncertainties: *network structure* referring to the level of network fragmentation, and *openness of applications, services, and hosts* relating to who has the control over usage possibilities. The different outcome combinations from these uncertainties create four scenarios that present and summarize the alternative futures.

The first scenario, *Wild & Free*, means transition back to the original Internet in which free connectivity and free programmability prevail and the Internet industry is entirely horizontal and highly competitive. The *Isolated Walled Gardens* scenario describes a fully opposite world. The Internet is fragmented into access operator controlled islands and all the components – devices, network, and content – are bundled together through the vertical industry structure. The two latter scenarios present different shades of gray between these black and white worlds. *In Content-driven Overlays* network is fragmented into multiple overlay networks based on the characteristics of content types. Contrary to

Isolated Walled Gardens the separation is invisible to users that can access any network-content bundle available. In *Device-Content Bundles*, for one, network is technically similar to the network in Wild & Free but the strong device vendor control drives for simple, closed devices that restrict the choice of applications and services.

The most important finding derived during the scenario process is that the challenges the Internet is encountering can be solved at many levels. As the scenarios propose, there are three possible ways to satisfy emerging requirements and solve forthcoming bottlenecks. First, IETF strives for openness and network integrity preserving solutions implemented in the core Internet architecture. Second, business interests of various stakeholders and failures in implementing some features in the core architecture pave the way for solutions that rely on building separate network fragments or closing the applications, services, and hosts. Third, a completely new clean slate approach might be able to solve a bunch of problems, although the deployment conditions of a complete redesign are not studied closer in this thesis.

The strength and relevance of uncertainty-based scenarios depend on the match of technical and business architectures in each distinctive scenario. Each produced scenario corresponds to a characteristic technical and business architecture, which may trigger valuable forward-looking debates among experts. Differences between the constructed scenarios concerning the power relationships and value distribution between stakeholders reveal the underlying tensions and differing interests of stakeholders. This suggests that the actual outcome ten years from now will likely be a hybrid of several scenarios.

Scenario planning should stimulate decision makers to consider changes they would otherwise ignore. A short analysis concerning the research strategy of the Finnish Future Internet program reveals that the research focus is clearly in the core architecture and in the Wild & Free scenario. The other scenarios are seen resulting from failures of the IETF-centric research. The key finding from the strategic analysis is that deployment of new solutions needs to be planned carefully already from the beginning.

9.2 Discussion

The main purpose of the conducted scenario analysis is to clarify possible future advances in the Internet evolution. It limits the amount of uncertainties, generates consistent pictures, and identifies issues that might otherwise remain ignored. The constructed scenarios depict four distinct futures and often when presenting the results to audience, I was asked to evaluate odds for their realization. This thesis, however, deliberately refrains from assigning probabilities. The only answer that can be given is that if the analysis has succeeded, the Internet in 2018 can be defined by the constructed scenario space – either as one of the scenarios but more probably containing elements from multiple scenarios.

Due to the chosen scope, the scenarios mainly present the final states leaving the description of paths and turning points leading to the scenarios to smaller attention. Because of very holistic framing of the research questions the scenarios take top-down approach which limits their technical precision. Across the board, no specified technical solutions are presented and finding of them remains a task of later research. Furthermore, although the scope of the research was global, the resulting perspective is inevitably Finland-centric and may be biased towards issues important for participated experts.

An important contribution of this thesis is that it guides the discussion about Future Internet. During the construction process the scenarios were not looked from a perspective of a given stakeholder, which made the process more difficult. Nevertheless, the neutrality of the scenarios means that the results can be exploited in planning the strategic actions of any stakeholder. Presented analysis of the research strategy of FI program (see Chapter 8) is just an example of the possibilities the constructed scenario analysis offers of help for managerial decisions.

9.3 Future research

This thesis has increased understanding of the big picture of historical and forthcoming evolution of the Internet. The next task is to dive deeper and concentrate on topics with narrower scope. As presented in the discussion part, analysis of the turning points that change the evolution path towards a certain scenario could be enhanced by analyzing the scenarios from multi-stakeholder perspective. One interesting topic could be further analysis on the conflicting interests and motives between the stakeholders from economic perspective. On the whole, the future research could keep technical view at arm's length and concentrate more on economic, social and political viewpoints. Analysis on political and regulatory prerequisites for the scenarios – originally a part of this thesis but omitted in order to narrow the scope – could reveal the required change in the political climate to enable the scenarios to come true.

Quantitative research is an essential and natural follow-up that can increase concreteness of the scenario analysis. Because it is impossible to get quantitative data from the future, other methods need to be used. Modeling of historical development and extrapolating derived results to the future is one possible option. From techno-economic perspective, price ratio changes between different technologies can have fundamental impact on architecture evolution and allocation of roles in the value networks. Analyzing for example the price ratio evolution between transport and storage could give a cue, if the future of the Internet is based more on transport or storage of data. System dynamic modeling is another step that can be taken based on the created scenarios.

All in all, the Internet has changed the society more and faster than any other development during the last century but its potential is not yet completely unleashed or even understood. Produced scenarios shed light on the multifaceted future research topics by illustrating interesting visions of the future. Scenarios, however well constructed, can embody only a finite set of phenomena. Thereby the actual evolution of the Internet can be studied only by following real life events.

References

Aguilar, F. (1967), *Scanning the business environment*. New York: Macmillan.

Alexa.com (2009), *The top 500 sites on the Web on April 2nd, 2009*. http://alexa.com/topsites (accessed 2 April 2009).

Alvestrand, H. (2004), *The Role of the Standards Process in Shaping the Internet*, Proceedings of the IEEE, vol. 92, pp. 1371-1374.

ASN (2009), *The 32-bit AS Number Report*. http://www.potaroo.net/tools/asn32/ (accessed 14 April 2009).

Baran, P. (1964), *On Distributed Communication Networks*, IEEE Transactions on Communications Systems, vol. 12, pp. 1-9.

Beijar, N. (2008), *Peer-to-Peer Architecture and Signaling*, Lecture slides of the Signaling Protocols course on April 4, 2008. http://www.netlab.tkk.fi/opetus/s383115/2008/kalvot/P2P_lecture.pdf (accessed 8 December 2008).

Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H. F., Secret, A. (1994), *The World-Wide Web*, Communications of the ACM, vol. 37, pp. 76-82.

Berners-Lee, T. (1996), *WWW: Past, Present, and Future*, Computer, vol. 29, pp. 69-77.

Bradfield, R., Wright, G., Burt, G., Cairns, G., Van Der Heijden, K. (2005), *The origins and evolution of scenario techniques in long range business planning*, Futures, vol. 37, pp. 795-812.

CacheLogic (2005), *Internet protocol trends 1993-2004*, in P2P in 2005. http://www.readwriteweb.com/archives/p2p_growth_trend_watch.php (accessed 19 April 2009).

CacheLogic (2006), *Internet protocol trends 1993-2006*, in P2P File Sharing – The Evolving Distribution Chain presentation of David Ferguson. http://www.dcia.info/activities/p2pmswdc2006/ferguson.pdf (accessed 19 April 2009).

CAIDA (2009), *Chicago passive network monitor A*. http://www.caida.org/data/realtime/passive/?monitor=equinix-chicago-dirA (accessed 18 April 2009)

Carpenter, B. (1996), *RFC 1958 – Architectural Principles of the Internet*. http://www.ietf.org/rfc/rfc1958.txt (accessed 20 March 2009).

Cerf , V., Kahn, R. (1974), *A Protocol for Packet Network Intercommunication*, IEEE Transactions on Communications, vol. 22, pp. 637-648.

Christensen, C.M., Raynor, M., Verlinden, M. (2001), *Skate to where the money will be*, Harvard Business Review, vol. 79, pp. 72-81.

Cisco (2008a), *Visual Networking Index – Forecasts and Methodology, 2007-2012*. http://newsroom.cisco.com/dlls/2008/ekits/Cisco_Visual_Networking_Index_061608.pdf (accessed 5 April 2009).

Cisco (2008b), *Visual Networking Index – Approaching the Zettabyte Era*. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481374.pdf (accessed 19 April 2009).

Clark, D. (1988), *The design philosophy of the DARPA Internet protocols*, ACM SIGCOMM Computer communication review, vol. 18, pp. 106-114.

Clark, D., Chapin, L., Cerf, V., Braden, R., Hobby, R. (1991), *RFC 1287 - Towards the Future Internet Architecture*. http://www.ietf.org/rfc/rfc1287.txt (accessed 1 April 2009).

Clark, D., Blumenthal, M. (2001), *Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world*, ACM Transactions on Internet Technology (TOIT), vol 1, pp. 70-109.

Clark, D., Sollins, K., Wroclawski, J., Braden, R. (2002*), Tussle in Cyberspace: Defining Tomorrow's Internet*, Proceedings of ACM SIGCOMM 2002, pp. 347-356.

Clark D., Blumenthal, M. (2007), *The end-to-end argument and application design: the role of trust*, Proceedings of the Conference on Communication, Information and Internet Policy (TPRC), Sept. 2007

Clark, D., Faratin, P., Gilmore, P., Bauer, S., Berger A., and Lehr W. (2008), *The Growing Complexity of Internet Interconnection*, Communications & Strategies, No. 72, 4th quarter 2008, pp. 51-71.

Courcoubetis, C., Weber, R. (2003), *Pricing Communication Networks*, John Wiley & Sons.

Crocker, S. (1970), *RFC 36 - Protocol Notes*. http://www.ietf.org/rfc/rfc36.txt (accessed 20 March 2009).

Diehl, M., Stroebe, W. (1991), *Productivity loss in idea-generating groups: Tracking down the blocking effect,* Journal of Personality and Social Psychology, vol. 61, pp. 392-403.

Egevang, K., Francis, P. (1994), *RFC 1631 - The IP Network Address Translator (NAT)*. http://www.ietf.org/rfc/rfc1631.txt (accessed 1 April 2009).

Ellacoya Networks (2007), *The YouTube effect: HTTP traffic now eclipses P2P*. http://arstechnica.com/news.ars/post/20070619-the-youtube-effect-http-traffic-now-eclipses-p2p.html (accessed 5 April 2009).

European Commission (2008), *Bled Declaration*. http://www.future-internet.eu/publications/bled-declaration.html (accessed 27 March 2009).

Fahey, L., King, W. (1977), *Environmental Scanning for Corporate Planning*, Business Horizons, vol. 20(4), pp. 61-71.

Fallows, D. (2005), *Search Engine Users, report of Pew Internet & American Life project*. http://www.pewinternet.org/~/media//Files/Reports/2005/PIP_Searchengine_users.pdf.pdf (accessed 2 April 2009).

Finnet (2009), *Finnet starts a major paradigm shift in computing – involving largest local and global system suppliers*, bulletin on 17 April 2009. http://www.finnet.fi/index.asp?id=116&menupath=116&language=1&klik=1 (accessed 28 April 2009).

FNC (1995), *Definition of "Internet", U.S. Federal Networking Council*. http://www.nitrd.gov/fnc/Internet_res.html (accessed 19 March 2009).

Gill, P., Arlitt, M., Li, Z., Mahanti, A. (2007), *Youtube traffic characterization: a view from the edge*, Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, pp. 15-28.

Hain, T. (2000), *RFC 2993 - Architectural Implications of NAT*. http://www.ietf.org/rfc/rfc2993.txt (accessed 11 May 2009).

Heikkinen M., Hämmäinen, H. (2008a), *Scenario Planning of Mobile Peer-to-Peer Service Usage*, Proceedings of 7th International Conference on Mobile Business (ICMB 2008), pp. 145-152.

Heikkinen, M., Matuszewski, M., Hämmäinen, H. (2008b), *Scenario planning for emerging mobile services decision making: mobile Peer-to-Peer Session Initiation Protocol case study*, Int. J. Information and Decision Sciences, vol. 1, pp. 26-43.

Hinden, R. (1993), *RFC 1517 - Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR)*. http://www.ietf.org/rfc/rfc1517.txt (accessed 1 April 2009).

Huston, G.(2001), *Analyzing the Internet's BGP routing table*, The Internet Protocol Journal, vol. 4, nr. 1.

Huston, G. (2006), *Identity and Location in IP*, presentation in CAIA Seminar, Swinburne University of Technology. http://www.potaroo.net/presentations/2006-11-30-whoareyou.pdf (accessed 16 April 2009).

Huston, G. (2008a), *The End of End to End?* http://www.potaroo.net/ispcol/2008-05/eoe2e.html (accessed 20 March 2009).

Huston, G. (2008b), *10 Years Later*. http://www.potaroo.net/ispcol/2008-06/10years.html (accessed 19 April 2009).

Huston, G. (2009), *BGP in 2008*. http://www.potaroo.net/ispcol/2009-03/bgp2008.html (accessed 16 April 2009).

Internet World Stats (2009), *World Internet Usage and Population Statistics*, Miniwatts Marketing Group. http://internetworldstats.com/stats.htm (accessed 9 April 2009).

Ipoque (2007), *Internet Study 2007*. http://www.ipoque.com/resources/internet-studies/internet-study-2007 (accessed December 8, 2008).

Ipoque (2009), *Internet Study 2008/2009*. http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009 (accessed 3 March 2009).

IPv4 (2009), *IPv4 Address Report*. http://www.potaroo.net/tools/ipv4/ (accessed 16 April 2009).

Isenberg, D. (1998), *The dawn of the "stupid network"*, netWorker, vol. 2, pp. 24-31.

ISC (2009), *The ISC Domain Survey*. https://www.isc.org/solutions/survey (accessed 20 April 2009).

ISOC (2009), *Internet Society – Histories of the Internet*. http://www.isoc.org/internet/history/ (accessed 18 March 2009).

Juvonen, R. (2008), *ICT SHOK Future Internet Programme*, presentation on Tivit Foresight Seminar on December 4th, 2008.

http://www.tieke.fi/mp/db/file_library/x/IMG/36751/file/TIVITForesightSeminar2008Juvonen.pdf (accessed 28 April 2009).

Karlson, B., Bria, A., Lönnqvist, P., Norlin, C., Lind, J. (2003), *Wireless Foresight: Scenarios of the mobile world in 2015*, Chichester, UK: Wiley.

Kesan, J., Shah, R. (2001), *Fool Us Once Shame On You—Fool Us Twice Shame On Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, Washington University Law Quarterly, vol. 79, pp. 89-220.

King, N. (2004), *Using interviews in qualitative research*, in Cassel, C., Symon, G. (eds.), Essential guide to qualitative methods in organizational research, London, UK: Sage, pp. 11-22.

Kivi, A. (2008), *Mobile data service usage measurements – results 2005-2007*. http://www.netlab.tkk.fi/~jakivi/publications/Kivi_Mobile_Data_Service_Usage_2005_2007.pdf (accessed 19 April 2009).

Kleinrock, L. (1961), *Information Flow in Large Communication Nets*, RLE Quarterly Progress Report, July 1961.

Kvale, S. (1983), *The Qualitative Research Interview: A Phenomenological and a Hermeneutical Mode of Understanding*, Journal of Phenomenological Psychology, vol. 14, pp. 171-196.

Licklider, J., Clark W. (1962), *On-Line Man Computer Communication*, AFIPS Joint Computer Conferences, Proceedings of the May 1-3, 1962, pp. 113-128.

Leber, M. (2009), *Global IPv6 Deployment Progress Report*. http://bgp.he.net/ipv6-progress-report.cgi (accessed 18 April 2009).

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., Wolff, S. (2003), *A Brief History of the Internet, version 3.32*. http://www.isoc.org/internet/history/brief.shtml (accessed 19 March 2009).

Lessig, L. (2000), *Code is Law – On Liberty in Cyberspace*, Harvard Magazine, vol. 103(2). http://harvardmagazine.com/2000/01/code-is-law.html (accessed 16 April 2009).

Levien, R., Austein, R., Borgman, C., Casey, T., Dubberly, H., Falstrom, P., Halvorsen, P., Jenkins M., Klensin, J., Mueller, M., Nelson, S., Partridge, C., Raduchel, W., Varian, H. (2005), *Signposts in Cyberspace: The Domain Name System and Internet Navigation*, Washington, D.C.: National Academies Press.

Merit (1995), *Relation between percentage of bytes & packets transferred per month by service*. http://www.cc.gatech.edu/gvu/stats/NSF/BothP.GIF (accessed 6 April 2009).

Meyer, D., Zhang, L, Fall, K. (2007), *RFC 4984 – Report from the IAB Workshop on Routing and Addressing*. http://www.ietf.org/rfc/rfc4984.txt (accessed 16 April 2009).

Mockapetris, P. (1987) *RFC 1034 – Domain Names – Concept and Facilities*. http://www.ietf.org/rfc/rfc1034.txt (accessed 23 March 2009).

Moors, T. (2002), *A critical review of "End-to-end arguments in system design"*, IEEE International Conference on Communications, vol. 2, pp. 1214-1219.

Moskowitz, R., Nikander, P. (2006), *RFC 4423 – Host Identity Protocol (HIP) Architecture*. http://tools.ietf.org/html/rfc4423 (accessed 16 April 2009).

Mueller, M. (2008), *Scarcity in IP addresses: IPv4 Address Transfer Markets and the Regional Internet Address Registries*. http://www.internetgovernance.org/pdf/IPAddress_TransferMarkets.pdf (accessed 16 April 2009).

Mueller, M. (2009), *Memo to John Markoff: There are no "do overs" in history*, Blog post in Internet Governance Project web page. http://blog.internetgovernance.org/blog/_archives/2009/2/28/4107895.html (accessed 14 April 2009).

Nikander, P., Mäntylä, M. (eds.)(2007*), ICT SHOK Future Internet – Research Agenda*. http://www.futureinternet.fi/publications/ICT_SHOK_FI_SRA_Research_Agenda.pdf (accessed 15 April 2009).

Nishitani, T, Miyakawa, S., Nakagawa, A., Ashida, H. (2008), *Common Functions of Large Scale NAT (LSN), IETF Internet-Draft*. http://tools.ietf.org/html/draft-nishitani-cgn-01 (accessed 16 April 2009).

Nordlund, T., Tallberg, M., Hämmäinen, H. (2007), *Scenarios for management of digital homes*, Proceedings of 6th Conference on Telecommunication Techno-Economics (CTTE 2007), pp. 1-8.

Norton, W. B. (2001), *Internet Service Providers and Peering*. http://www.cs.cmu.edu/~srini/15-744/readings/Nor01.pdf (accessed 25 February 2009).

Norton, W. B. (2002), *A Business Case for ISP Peering*. http://pages.cs.wisc.edu/~akella/CS640/F06/readings/norton.pdf (accessed 25 February 2009).

Oberholzer-Gee, F., Strumpf, K. (2007), *The Effect of File Sharing on Record Sales: An Empirical Analysis,* Journal of Political Economy, vol. 115, pp. 1-42.

Oram, A., (2001), *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. Sebastopol, CA: O'Reilly, pp. 8-18.

Osborn, A. (1963), *Applied imagination: Principles and procedures of creative problem solving, Third Revised Edition*, New York, NY: Charles Scribner's Sons.

Postel, J., Reynolds, J. (1985), *RFC 959 – File Transfer Protocol (FTP)*. http://www.ietf.org/rfc/rfc959.txt (accessed 6 April 2009).

Reding, V. (2009), *Internet of the future: Europe must be a key player*, speech to the Lisbon Council on 2 February 2009. http://ec.europa.eu/commission_barroso/reding/docs/speeches/2009/brussels-20090202.pdf (accessed 27 March 2009).

Renesys Corp. (2009), *Internet Captivity and the De-peering Menace*, presentation at NANOG45 conference. http://www.renesys.com/tech/presentations/pdf/nanog-45-Internet-Peering.pdf (accessed 25 February 2009).

Rescorla, E. (2001), *SSL and TLS: Designing and Building Secure Systems*, United States: Addison-Wesley.

Reynolds, J. (1989), *RFC 1135 - The Helminthiasis of the Internet*. http://www.ietf.org/rfc/rfc1135.txt (accessed 5 May 2009).

RFC Editor et. al (1999), *RFC 2555 - 30 Years of RFCs*. http://www.ietf.org/rfc/rfc2555.txt (accessed 20 March 2009).

Rickards, T. (1999), *Brainstorming*, in M. Runco, and S. Pritzker (eds.): Encyclopedia of Creativity, San Diego, CA: Academic Press, vol. 1, pp. 219-227.

Rietzschel E., Nijstada, B. Stroebe, W. (2006), *Productivity is not enough: A comparison of interactive and nominal brainstorming groups on idea generation and selection*, Journal of Experimental Social Psychology, vol. 42, pp. 244-251.

Roberts, L. (1967), *Multiple Computer Networks and Intercomputer Communication*, Proceedings of the first ACM symposium on Operating System Principles, pp. 3.1-3.6.

Robson, C. (2002), *Real World Research, 2nd Ed.*, Cornwall, UK: Blackwell, pp. 269-291.

Saltzer, J., Reed, D., Clark D. (1984), *End-to-end arguments in system design*, ACM Transactions on Computer Systems (TOCS), vol.2, pp. 277-288.

Schoemaker, P. (1991), *When and how to use scenario planning: A heuristic approach*, Journal of Forecasting, vol. 10, pp. 549-564.

Schoemaker, P. (1993), *Multiple scenario development: Its conceptual and behavioral foundation*, Strategic Management Journal, vol. 14, pp. 193-213.

Schoemaker, P. (1995), *Scenario planning: A tool for strategic thinking*, Sloan Management Review, vol. 36, pp. 25-40.

Schoemaker, P., Mavaddat V. (2000), *Scenario Planning for Disruptive Technologies*, in G.S. Day and P.J.H. Schoemaker (eds.): Wharton on Managing Emerging Technologies, New York: John Wiley & Sons, pp. 206-241.

Schwartz, P. (1998), *The Art of the Long View – Planning for the future in an Uncertain World*, Chichester, UK: John Wiley & Sons.

Silva, J., Campolargo, M. (2009), *Message by Joao da Silva and Mario Campolargo in the FIA web page*. http://www.future-internet.eu/home/future-internet-assembly/prague-may-2009.html#c135 (accessed 24 April 2009).

Smura, T., Sorri, A. (2009), *Future Scenarios for Local Area Access: Industry Structure and Access Fragmentation*, in Proceedings of the Eighth International Conference on Mobile Business (ICMB 2009), Dalian, China, June 27-28, 2009.

Statistics Finland (2008), *Purposes of the use of the Internet in spring 2008, per cent of Internet users by age group*. http://stat.fi/til/sutivi/2008/sutivi_2008_2008-08-25_tau_001_en.html (accessed 1 April 2009).

Särelä, M., Nikander, P. (2008), *Social Aspects of Trust in the Internet: Issues and Incentives*. https://www.tml.tkk.fi/~pnr/publications/CTTE_sarela_2008.pdf (accessed 16 April 2009).

TeleGeography (2009), *TeleGeography International Telecom Trends Seminar, PTC 2009*. http://www.ptc.org/ptc09/images/papers/PTC%2709_TeleGeography_Slides.pdf (accessed 25 February 2009).

Thomas, P. (1974*), Environmental Analysis for Corporate Planning*, Business Horizons, vol. 17(5), pp. 27-38.

Thomas, S. (2000), *SSL and TLS essentials securing the Web*, New York, U.S.: Wiley.

Zakon, R. (2006), *Hobbes' Internet Timeline*. http://www.zakon.org/robert/internet/timeline/ (accessed 18 March 2009).

Zittrain, J. (2008), *The Future of the Internet - And How to Stop It*, New Haven & London: Yale University Press.

Van der Heijden, K. (1996), *Scenarios – The Art of Strategic Conversation*, Chichester, UK: John Wiley & Sons, pp. 305.

Wack, P. (1985), *Scenarios: Uncharted Waters Ahead*, Harvard Business Review, vol. 63, pp. 73-89.

Wu, T. (2009), *Network Neutrality FAQ*. http://timwu.org/network_neutrality.html (accessed 27 March 2009).

Appendices

A) Summary of brainstorming results

The forces identified in the three brainstorming sessions are grouped into four groups based on the evaluation of importance and uncertainty. The groups are explained in Figure 22 below. The most important groups – key uncertainties (4) and key trends (3) – are also colored. Additionally, the number of Post-its grouped together is given. Some forces remained ungrouped due to time constraints, and they are marked with "-".

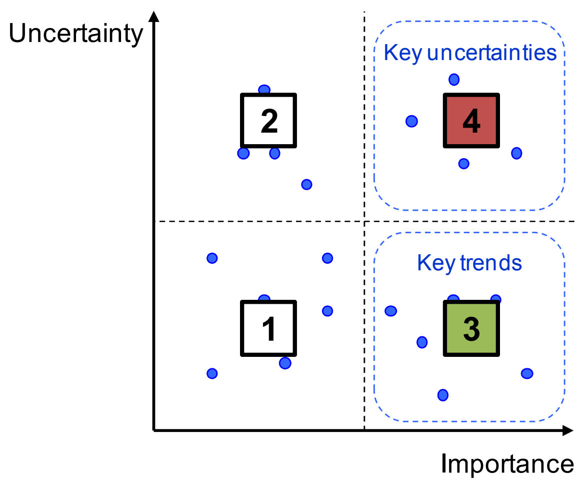

Figure 22: Explanation of the groups of identified forces

29.8.2008 – First brainstorming session

Political/Regulatory Forces	Group	Post-Its
Where standardization happens and by which authority?	4	4
Operator Control increases (net neutrality, regulator has something to say).	4	3
Governmental Control (censorship, regulatory) increases.	3	2
Energy consumption increases and green values become more important.	3	2

Economic/Business Forces	Group	Post-Its
The Internet will be split to many Internets (safe & restricted vs. anarchy; geographically).	4	2
The business model of the Internet economy will change (ads vs. micropayments vs. ...).	4	1
Industry consolidation increases (fewer players).	3	1
Technological leadership: Western vs. Asian.	2	1

Social Forces	Group	Post-Its
Security and privacy will become more important.	3	6
Need for mobility and all around availability increases.	3	3
Content creating will be easier and more user driven.	3	1
Social networking increases and people spend more time online.	3	1
Need for simplicity increases.	3	1
Service development will be more user-driven.	2	4
Remote work will increase.	1	1

Technological Forces	Group	Post-Its
Intelligence moves from edges to the network (cloud computing, data storage).	4	3
Routing system is choking under the increasing traffic.	4	1
P2P replaces client-server model as the main architecture.	4	1
Unwanted traffic will stay as a problem.	4	1
The amount of users and hosts will be increasing (IoT, 3rd world).	3	4
Open source gains more popularity.	3	1
Complexity (of programs, services, architectures) increases.	3	1
Shortage of the IPv4 addresses limits the amount of hosts that can be connected to the Internet.	3	1
More and more middle-boxes in the Internet.	3	1
Traffic optimization increases (P2P overlay optimization, YouTube servers inside the ISPs).	3	1
Devices with limited processing etc. capabilities will become more common in the Internet (Internet of Things).	2	1
IMS Future: Yes/No.	2	1
Closed appliances will become more common.	2	1
Video increases Internet traffic remarkably.	1	1
Mobile device battery life stays as a bottleneck.	1	1
Data storage capacity is not a bottleneck.	1	1

23.9.2009 – Second brainstorming session

Political/Regulatory Forces	Group	Post-Its
World changes from U.S.-driven unipolar to multipolar, same happens to the Internet? (Openness? China out of the Internet?)	4	3
IPR regulation changes, but to which direction? Increasingly strict and broad? Alternative (open source, creative commons, file sharing)? No IPR at all?	4	3
EU cannot agree about the Future Internet -> failure in its Future Internet objectives (no supporting industry for research, should be co-located)	4	2
Horizontalization of ecosystems develops gradually (Politicians drive to this direction, companies oppose).	4	1
Law maker sets high penalties for misuse (spam, DoS attacks).	4	1
Amount of spectrum given for the Internet?	4	1
Spectrum will be auctioned in most countries and liberalization of spectrum continues.	3	4
Privacy and trust issues become more important and require new kind of legislation.	3	2
Government role is increasing and policies boost Internet use & traffic -> re-regulation.	3	2
Legislation won't change dramatically (disruptively) in 10 years (all the changes are already at least under discussion).	3	1
Strict energy limits for ICT.	3	1
Power and energy consumption speed up horizontalization (ownership of things).	3	1
Global regulator?	2	1
EU defines minimum Internet access (free of charge?).	2	1
Environmental crises will cause more restrictive legislation / Environmental regulation increases the use of ICT and env. information in services --> driver for new services / environmental concerns boost broadband build-up.	1	3
Flat rate, flat architecture will dominate in the Internet.	1	1
EU will steadily increase its role and harmonization.	1	1
Monopoly position of huge Internet players recognized (Google etc.).	1	1
Fixed/mobile differentiation will disappear and flux will change.	1	1
China and India will confuse the development of the Future Internet.	-	1
Competition will be oligopolic.	-	1
Global hub model (Google) wins over local.	-	1

Economic/Business Forces	Group	Post-Its
Industry divergence or convergence; Content creation by industry or by end users; Porter thinking in industry, altruism supported by the people.	4	3
Business --> global, Individual --> local; Content & Apps --> local, Network & Access --> global.	4	2
Most companies focus to single layer player in ecosystem.	4	1
Internet micropayment happens?	4	1
A new player (like Google) disturbs the current ecosystem.	4	1
Emerging markets (China, India) take the lead, manufacturing goes to China & India --> Services increasingly important.	3	5
Environmental crises change economical rules and bring business opportunities.	3	2
Economic value of the Internet drives the future; Techno-economical criteria will dominate the investments for Future Internet.	3	2
Increase of ad-based business models.	3	1
Internet matures (impact on technology life cycle).	3	1
ICT becomes cheap compared to non-ICT --> bottlenecks elsewhere.	3	1
Bigger operators --> Consolidation.	3	1
Mobile network vendors (NSN, Ericsson, etc.) do not know what to do.	2	1
Globalization increases (information exchange increases) but transporting goods decreases.	1	2
Router companies (Cisco, etc.) will lose leadership.	1	1
Wireless Internet helps local economics.	-	1
2 billion new users will be mostly wireless.	-	1
China has two angles of incidence, Europe and USA just one.	-	1
Services are not equal, some of them more prominent --> service sector divided.	-	1
The whole economic cycle in 10 years --> first depression, then high season.	-	1
Horizontal markets rule.	-	1
Flat rate rules in networks and content.	-	1
New global hubs will emerge.	-	1
Some key players try to build vertical bundles.	-	1

Social Forces	Group	Post-Its
Consumer preference: bundles vs. buying separately? (especially relationship between possibilities)	4	1
Privacy concerns will slow down take-up of new services.	4	1
Threats between virtual world and real world (e.g. Chinese want outside).	4	1
Mapping between real and virtual worlds improves --> acceptable to people, brings new services.	3	3
Flash crowds rules --> grass-root activism --> large impacts.	3	3
User-driven service design & engineering increases.	3	1
Social networking gains importance.	3	1
Segmentation in all Internet services will develop.	3	1
Next 2 billion users will come from 3rd world and NICs (will use mostly wireless access).	3	1
Aging population --> more free time and service consumption.	3	1
Language barriers less important, but also lot of local language content (IDN).	3	1
Business use will continue to grow fast.	3	1
Fragmentation of content markets will increase.	3	1
Generation Y (born in the 80s) becomes economically important.	3	1
Communality overcomes individuality.	3	1
People are increasingly able and willing to use Internet services.	3	1
Consumer as the king will dominate new services --> personalization, mass customization.	3	1
Outsourcing of ethical and moral behavior (Microsoft vs. Linux, Google vs. ??); Ecological behavior becomes socially imperative.	1	2
Consumers will be ready to pay for evident added value.	-	1
Green values will drive for green services.	-	1
Communities are tribes for like-minded.	-	1
Value leadership important trend-setter.	-	1
Neutral good do not need to care so much about values. No harm = important.	-	1

Technological Forces	**Group**	**Post-Its**
Internet without IP will emerge; Ethernet rules; 1 T links --> new protocol stack; scaling 100x --> packet transmission.	4	4
New solution to privacy problems will be invented; Several ways to support secure identity; Universal citizen authentication happens.	4	3
Open source software becomes totally dominant; Open source, open interfaces: how much and where?	4	2
Silicon technology develops still 10 years (Moore's law).	4	2
Web services/XML wins (possible stopper: inefficiency --> energy consumption).	4	1
Which access? Optical, copper, cable or wireless?	4	1
Self-organizing networks simplify complications of management and configuration.	4	1
Cognitive radio will change spectrum use.	4	1
Internet of things --> Ubicomp spreads quietly; Strong local connectivity; Need for new technology competences.	3	4
Power consumption becomes the main bottleneck --> bigger driver.	3	2
Software technologies become bottleneck; Application development still too complex for most users.	3	2
Fragmentation of radio technologies limits mobility.	3	1
Server vs. client: both get fat.	3	1
Cellular technology development ceases (FDM, TDM, WDM - all used).	3	1
Cost of intensive use of wireless technology goes down.	3	1
Technology optimization = fiber as far as possible, only last 100 m wireless (optimizing power consumption).	3	1
IP/Internet takes it all (broadcast etc.).	3	1
Broadband as common as GSM today (both fixed and wireless).	3	1
High-resolution displays in mobile devices enable better services/UIs.	-	1
Location-aware technologies spread.	-	1
Internet structure will remain. Access, core, services and content horizontalize.	-	1

7.10.2009 – Third brainstorming session

Politic/Regulatory Forces	**Group**	**Post-its**
Legal interception will become mandatory; Content filtering will increase.	4	2
UN + ITU will take stronger role in fair sharing of Internet resources (e.g. IP addresses / names) <--> Commercial approach.	4	1
Developments in "green ICT"? Will this affect the common citizen?	4	1
Anonymity in the Internet disappears (User registration --> will Internet users be forced to register/acquire a license to use the net?).	4	1
Global and regional harmonization at high level - selected topics (still plenty of local differences, the development still slow).	4	1
Need for net neutrality discussion? Actions required?	4	1
Political & regulatory interest has risen --> no more a free industry.	3	1
Moral entrepreneurs become more important in shaping technology regardless of what's actually happening.	3	1
Regulation is a political issue across in political spectrum --> gets out of hands of experts.	-	1

Economic/Business Forces	**Group**	**Post-its**
Communication will not be a fast growing industry --> back to normal economy (ICT is still growing though); Increase in cost control --> investments need to have clear cost/revenue impact.	4	2
Productivity vs. innovation in operator strategies is crucial (how much R&D?)	4	1
L2+L3 split/combination disrupts the Internet infra vendor market (network device manufacturers).	4	1
Proprietary solutions vs. industry standards --> what will prevail?	4	1
Movement from bit-pipe providers to services (or just packetizing services).	4	1
The role of the services increases.	3	1
Service market is global, access market and content local.	3	1
Content will be increasingly localized and dependent on location information.	3	1
Too much/heavy emphasis on the Internet only --> what happens when links break, cyber attacks etc.?	3	1
Remote maintenance of devices increases.	3	1
New business opportunities: identity/trust provider (banks), remote network management provider.	3	1
ISP/Telco convergence continues.	1	1
Providers increasingly subcontract service development.	-	1

Social Forces	**Group**	**Post-its**
Lack of trust increases, because the Internet is increasingly hostile.	4	2
Digital divide changes its nature. Net integrates to everyday life in OECD but not so much in the 3rd world. Mobile phones function like an equalizing force.	4	1
Net is more natural for young users (courage/interest to try new things); Net is more essential/integrated part of everyday life; Ordinary life increasingly dependent on not just communications but also services.	3	3
People too Internet-centric = information flows, communication flows --> people stop physical activities.	3	1
Openness vs. privacy: privacy needed in specific applications only --> high commercial value, openness enough/needed in most applications.	3	1
Nature of net and ease of use make people careless (give too much information to the Internet).	3	1
Communications, sharing and user created content drive new applications.	3	1
More late adopters to use ICT --> better usability needed	3	1
Consumer market becomes increasingly a vote --> recommendations, price comparisons more popular --> affects on buying behavior.	3	1
Consumers accept complex (& judged) information in virtual world.	3	1
Generation gap: youth is eager to adopt new services, elders can't stay with.	-	1

Technological Forces	**Group**	**Post-its**
Increased use of IPv6 together with IPv4 --> can routers handle?	4	1
Number of technologies in 4G wireless? Single or many more than in 3G?	4	1
Secure Internet emerges, providing trust (but also anonymity). May lead to isolated islands.	4	1
IETF loses its role as a primary Internet standardization body --> new industry driven forum.	4	1
P2P-model will be developed in large scale (better reputation); P2P technologies deployed as main info delivery technology.	3	2
Shortage of IPv4 addresses.	3	1
Technology changes too fast --> ordinary people need too much techno-awareness.	3	1
The role of mobility will increase.	3	1
Increased processing power and bandwidths lead to higher power consumption --> high costs, global warming (can this be solved somehow?).	3	1
Existing equipment and technologies will prevent any major changes in medium term --> slow changes (legacy burden).	3	1
Battery capacity remains as bottleneck (Increased wireless bandwidth requires huge battery capacities).	3	1