NTVA - report: 2 - 2009

Future Internet: Global market – National opportunities

Unleashing Internet Opportunities

Dr. Terje Jensen,

The Centre for Quantifiable Quality of Service in Communication Systems, The Norwegian University of Science and Technology

> Section 10.3 authored by Willy Jensen, Director General, Norwegian Post and Telecommunication Authority

Program Committee:

Terje Jensen, Senior Researcher, Q2S/NTNU (Chairman) Bjarne E. Helvik, Professor, Q2S/NTNU Kjell Arne Ingebrigtsen, Professor, IET/NTNU Willy Jensen, Director, NPT Svein Knapskog, Professor, Q2S/NTNU Petter Kongshaug, CEO, UNINETT Øivind Kure, Professor, Q2S/NTNU Hein Johnson, Secretary General, NTVA

Abstract

The Internet has found its way into every Norwegian home, enterprise and public institution. It has moved from nice-to-have till need-to-have in everyday life and business. About *every fourth person in the world is a user of Internet* although this number has passed 85 % in Norway. Internet is widely used as an arena for various types of trade, payments, reporting, education, entertainment, games and social interaction.

The Information and Communication Technology (ICT) area, which includes the Internet area, is a key element in a society's prosperous situation. In fact, for the European region the ICT area has contributed to more than 40 % of our society's productivity growth during the last decade. In that respect Internet is an essential component for multiple purposes. These include *conducting business, solving governmental tasks and enjoying leisure activities*.

So, can we just lean back and continue in the same manner? Or, are we taking too high risks by simply adding more of our personal and society welfare on the stability of a running Internet? Will it break as we continue to add more applications, connect more devices, publish more information on the Internet? Steadily more persons raise the "*be aware sign*" when faced with these questions. This is due to *severe limitations in today's Internet* considering aspects like scalability, security, information search, adaptability and other key areas.

This report addresses various aspects of the Internet; History, status and future options are discussed. One motivation is to relate the technology challenges and objectives to societal needs and trends. In that respect, critical issues with today's Internet are presented. There are also descriptions of several technical areas that have to be improved. Again, these are motivated by requirements following from current demands and trends.

Several national and regional initiatives have been launched. Some of the more relevant ones, in view of Norway's environment are presented in this report. The research on Future Internet has started by several research groups. There are several national and international initiatives on-going in different parts of the world.

Main objective of the report is to provide background and some arguments related to current challenges and future options in the Internet space. It is believed that a broader discussion should be undertaken also in *Norway to seize the opportunities revealed*. Several persons state that a balanced portfolio of *governmental and private activities must be started*. In particular the national initiatives will is most cases work as major drivers for other activities.

A key point is to maintain the *innovation force* related to Internet at the same time as sustainable *commercial operations* are fuelled. Today's dependency of Internet regarding key society and business functions will become even stronger in the future. For example, related to work steadily more persons utilise Internet for flexible work situations, information sharing and electronic collaboration. Similar benefits are also seen for personal use (e.g. banking/payment, information gathering, and social interactions) and governmental duties.

To further allow for increased societal welfare, therefore, it is essential to ensure that the Internet evolves correspondingly. Selected areas are described in this report, together with illustrations of how these could be realized.

Preface

This report is prepared for the NTVA Technology Forum taking place in Trondheim, September 9th, 2009.

The Technology Forum is set out to identify opportunities for different players, including government, industry and, academic players. The presentations include perspectives from industry, government and academy. The blending viewpoints create an arena for discovering emerging opportunities and activities to be undertaken on different levels.

Main questions to be addressed at the event include:

- Which factors are driving the Internet evolution?
- What technologies are basis for the Future Internet?
- How to govern the Future Internet balancing local and global concerns?
- What will future naming and addressing regimes allow?
- How to do business in the Future Internet area?
- What is the value of Internet service quality?
- Which actions should be undertaken to be successful in this area?

The event programme is:

Welcome address. Kjell Arne Ingebrigtsen, President, NTVA

European ICT challenges and initiatives. Rudolf Strohmeier, Head of Viviane Reding's cabinet (EU)

GENI activities - background, motivation and results. Chip Elliott, GENI Project Director (USA)

Internet-related initiatives - background and results in Japan. Professor Hideyuki Tanaka, University of Tokyo

Future Internet - Selected key trends and opportunities. Petter Kongshaug, CEO Uninett

From Telco to Webco. Hans Christian Haugli, CEO Telenor Research and Innovation

Internet technologies entering new areas. Professor Øivind Kure, The Norwegian University of Science and Technology

Internet Governance issues; has the multi-stakeholder model already failed? Willy Jensen, Director General Norwegian Post and Telecommunications Authority

How should we manage "Names and numbers"? Professor Jon Bing, University of Oslo

Differentiated dependability in one network? Professor Bjarne E. Helvik, The Norwegian University of Science and Technology

Panel discussion – National opportunities and actions. Panel facilitator: Professor Kjersti Moldeklev, The Norwegian University of Science and Technology

Table of Contents

1. In	ntroduction	1
2. In	nternet basics	6
3. A	brief on Internet's history	9
3.1.	Steps towards the technical realisation	9
3.2.	Administrative units	11
3.3.	Sample of Internet growth	12
4. In	nternet's importance for the society	14
4.1.	General effects	14
4.2.	Pivotal position in global society	14
4.3.	Impacts on Norway's positions and options	16
5. In	nitiatives from European Union	19
6. T	echnology-based challenges of today's Internet	24
6.1.	Originally identified shortcomings	24
6.2.	Sample list of shortcomings	25
6.3.	Example from security area	27
6.4.	Example from area of addressing	
6.5.	Example from area of service quality	29
7. B	asic technical trends	
7.1.	Fundamental technical trends	
7.2.	Who communicates with whom	
7.3.	Convergence – multiple applications on a common infrastructure	
7.4.	Future expectations	
8. E	volution opportunities	
8.1.	General approaches	
8.2.	Identities	
8.3.	Virtualisation	
8.4.	Internet Protocol version 6	40
8.5.	Routing	
8.6.	Transport protocol	
8.7.	Machines that communicate	
8.8.	Security and trust	46
8.9.	Personal cyber-experience	
8.10	Privacy in view of Internet evolution	49
9. S	elected market perspectives	

9.1.	General market trends	58
9.2.	General societal trends	59
9.3.	Example: Internet and the climate debate	61
9.4.	Some network-related trends	61
9.5.	Change of communication patterns	
9.6.	Example: Peer-to-peer	64
10.	Governance of Internet aspects	67
10.1	. Controlling technical evolution	67
10.2	Global initiatives	67
10.3	. Internet Governance – How to improve the present structure?	
10.4	. Internet – part of Universal Service Obligation package?	73
10.5	End-point responsibilities	73
10.6	. Network neutrality	74
10.7	'. Norway	75
11.	Selected national initiatives	79
11.1	. Australia	79
11.2	Finland	79
11.3	. Italy	79
11.4	Japan	79
11.5	New Zealand	
11.6	Sweden	
11.7	. UK	
11.8	The USA	
12.	Summarising selected prospectives	86
12.1	. Broadband versus Internet	86
12.2	Future Internet issues	
12.3	Example applications and functionality	90
12.4	Example: contributions to poorer regions	91
13.	Concluding remarks	

1. Introduction

So, imagine -

How would life be without the Internet?

Would we be as efficient as today, or would there be no talk about the time squeeze? Would the number of faxes sent be at the same volume as the number of e-mails today? What about the access to information, would the number of paper/hard copies flourish similar to number of today's downloads?

The questions are manifold and similarly are the reflections on options to the "*Internet way*". The simple fact is that Internet has become a key component in any modern society. Access to and usage of Internet is in several statistics seen as one *measure of welfare*. In particular Internet has taken a dominating place for exchanging information between users. This goes both on private and work-related purposes. In fact, Internet is essential in almost any application of Information and Communications Technologies (ICT).

During the last years we have experienced how the growth of the information society has changed the way people communicate and interact. For information, entertainment and business, Internet is no longer a "nice to have" feature, but has changed into a "*need to have*" role.

Some estimates were done as part of the background for adopting the i2010 initiative by the European Commission (European Information Society 2010)¹: "Information and Communication Technologies are a powerful driver of growth and employment. A *quarter of* $EU GDP^2$ growth and 20 % of productivity growth are due to ICT. Differences in economic performance between industrialised countries are largely explained by their levels of ICT investment, research, and use, and by the competitiveness of their Information Societies".

There are major differences between different regions in the world, see Figure 1. An immediate observation is how the *European region lags compared with USA and Japan*. This goes both on the overall investment levels and what share of ICT R&D³ compose out of the total R&D investments. These numbers have changed during the last years, where Europe has increased its spending on ICT.

The spending is, however, partly in contrast to the contribution to the productivity gain as shown in Figure 2. Zooming into individual countries, a clear correlation is observed between *labour productivity growth and ICT investments* (see [CELT09]). The European Commission estimated that Internet and broadband access could potentially create 1 million jobs and boost the EU's economy by \in 850 billion by 2015.

¹ Information on i2010 available on http://ec.europa.eu/information_society/eeurope/i2010/invest_innov/index_en.htm

² Gross Domestic Product

³ Research and Development



Figure 1 Investments in ICT from private and public sources, and percentage of ICT investments as share of total R&D investments (from [ECi2010-05]).



Figure 2 Contribution to productivity for the European region (from [EIU02])

[NIDwg08] points to the effects Internet has had on our society over the last decades:

- "Internet has grown from an experimental research network to an infrastructure supporting the economy as well as the provision of societal services.
- Internet is becoming pervasive and ubiquitous, with already 25 % of the world population having access to it whilst mobile broadband is expected to rapidly provide access to another 2 billion users globally.
- It has enabled user and consumer empowerment, through the emergence of eCommerce and social networks.⁴
- It has helped the modernisation of public administration through emergence of eGovernment, eHealth, eEducation.
- Internet use is also expected to contribute significantly to solve emerging challenges such as climate change and energy efficiency.

⁴ According to [Pear09] about two-thirds of the worldwide Internet users are regularly visiting social networks.

- Internet has catalysed innovation and favoured the emergence of new disruptive business models; in 2008, about 300 million persons use free VoIP Skype Software; novel video consumption models such as YouTube have emerged, with global users uploading some 10 hours of video per minute from that site.
- It has supported the creativity of entrepreneurs through openness, which has made it possible for thousands of innovators would wide, to develop application acquiring almost instantly value through the networking multiplier effect."

In retrospective, looking at the evolution within the Internet area, the *speed of evolution* is breathtaking. Particularly when comparing it to speed of developing earlier telecom systems.

For certain areas new applications emerge in the matter of months rather than years.

However, one should not simply just extrapolate the past in order to predict the future. There are many aspects of the basic Internet design that are still in use today. These were made during the 1970's. Some of theses provide *kev hindrance for further sustainable* evolution; key topics being security, availability, flexibility and manageability. These limitations can not be simply removed by patching on today's systems, but require a re-design. As argued by [GENI07] there is growing consensus that we have reached the stage where patching is

The technical Internet:

Internet can be regarded as a set of computers connected by a set of links and routers. The computers exchange information by using a stack of protocols. Computers are referred to as hosts and contain different content and functions. Information is transported in the form of packets. Hence, the Internet is packet-switched. Every packet has a header that tells who the sender and the receiver are as well as other characteristics regarding how the packet is to be treated.

However, the term Internet is commonly used in a looser meaning, including aspects such as web, e-mail, chatting and so forth. As such it simply includes a set of services available to users through any Internet access.

no longer sufficient. Hence, a *fundamental rethinking of the Internet is required*. Not resolving these hindrances will not allow the society to fully utilize and exploit options of a future Internet.

Some of the *intrinsic characteristics accompanying the basic Internet* are (partly based on [Afua01]):

- Mediator \rightarrow Internet connects a waste number of users and devices
- Universality → Internet grows it presence to more "corners of the world" providing similar possibilities for all users
- Network externalities → the value of Internet grows by its number of users (the more users → the greater value → the more users → ...)
- Distribution channel → more and more content can be distributed. Several commercial content distributors apply the Internet for getting their content brought to the users
- Time moderator \rightarrow information and services are available through a "click". The asynchronous nature allows parties to engage according to their own best schedule

- Information asymmetry shrinker → any user may have access to the same information reducing the gap between different geographical regions. Any user may also contribute to the available information
- Infinite virtual capacity → a user may access information and services on different sites and by different means. Users also contribute to the available capacity by storing information on their equipment. Similarly the innovation capacity is high as users may engage in deploying new services
- Low cost standard → the volume of devices allows for economy of scale. Making use of Internet services or starting up a business based on Internet would not require major investments (according to Western scale). Then, marginal cost of transferring content or making use of a service is considered as small.
- Creativity challenger → as more information is a "a click" away, it could be tempting to copy someone else's then making your own. However, this can also be turned around, due to the easy access to several source, one should be better prepared for adding on to bring new material.

In order to connect all the Internet users⁵ several commercial roles are revealed. One of the key roles is the Internet Service Provider (ISP). An ISP provides Internet access for a user. This typically includes managing user identities, log in credentials, e-mail addresses, web home pages and security packages. The ISPs become the mediators between different user types.

There may be a range of mediators between two users. The ISPs possess different capabilities as some may manage a network of nodes and links, while others do not. ISPs commonly list the following challenges following from the current Internet model:

- Fixed pricing, rather than per-service or per-usage pricing
- Lack of commercial models for inter-provider collaboration beyond support of single class, best-effort services
- "Lowest common denominator" investments make premium services hard to justify
- Poor trust models overly permissive environment

These may also result in lack of incentives to further develop basic Internet features. An ISP may not see the benefits from spending money on introducing innovative services unless there is additional revenue or other returns. In fact, this may *hinder innovation* in these areas as argued by several players in the markets. The result might become that most of the innovations related to Internet are done by "*over the top players*" based on the basic infrastructure. Examples of this are FaceBook, Skype and Wiki. As the different applications grow in numbers and characteristics, the basic infrastructure faces steadily more challenges to keep up to speed.

The innovation related to Internet has enabled it to take *several critical positions in the modern society* as elaborated by several politics and public statements. Mid 2008 an OECD declaration was issued for the Future of the Internet Economy signed by 40 governments. It started out by stating the "common desire to *promote the Internet Economy and stimulate sustainable economic growth and prosperity* by means of policy and regulatory environments

⁵ Note: Here, no distinction is made between users of different kinds (such as human users, information producers, content producers, etc.)

that *support innovation, investment, and competition* in of the information and communications technology (ICT) sector". They further see that expansion of Internet will strengthen the *free flow of information, freedom of expression, and protection of individual liberties*. These are all seen as critical components of a democratic society and cultural diversity.

In fact, the OECD declaration state that *quality of life can be improved* by:

- "Providing new opportunities for employment, productivity, education, health and public services as well as addressing environmental and demographic concerns.
- Acting as a key deriver for the creation of enterprises and communities and stimulating closer global co-operation.
- Enabling new forms of civic engagement and participation that promote diversity of opinions and enhance transparency, accountability, privacy and trust.
- Empower consumers and users in on-line transaction and exchanges.
- Reinforcing a culture of security which applies to information systems and networks, and their users.
- Developing an increasingly important platform for research international science cooperation, creativity and innovation in many different sectors.
- Creating opportunities for new economic and social activities, application and services through ubiquitous and seamless access to communication and information networks.
- Promoting a global information society based on fast, secure and ubiquitous networks which connect billions of people, machines an objects."

Some technical areas brought forward are:

- Open standards for promoting competition, innovation and users' choice
- Protection of personal information and intellectual property rights
- Securing information infrastructure from relevant threats
- Efficient use of radio frequency spectrum
- IP version 6
- Clear and accurate information to users regarding service quality and costs.

They also emphasis the need for stimulating further research, investment and competition on infrastructure and services. In particular *collaborative innovation networks* are mentioned jointly driven by universities, governments, public research, users and business.

- Internet is a key component for modern social welfare
- Significant increase of Internet usage
- Evolution of the Internet is frequently on political agendas
- Technical challenges ahead regarding basic Internet design

2. Internet basics

Several considers Internet (or "the net") as a means for communicating, searching for information, downloading interesting objects, carry out trades, and completing governmental forms/reporting. In a technical manner, however, the Internet consists of an underlying number of machines and links providing every user access to the relevant services. Figure 3 depicts a simplified illustration.



Figure 3 Principle illustration of the Internet

Zooming into the "Internet cloud" one finds that it actually is combined by a number of networks, managed by different Internet Service Providers (ISPs) – or network operators. A distinction may be made between a provider connecting individual end-users and an operator providing transport services to other providers. Every ISP has to provide access to its users and to connect to other ISPs, see Figure 4.

Interconnections between networks could be done directly between pairs of networks or through an Internet Exchange point (in Norway referred to as Norwegian Internet Exchange, NIX). In result there are typically *several paths between the parties that want to communicate* of the user and a server that provides the requested service.



Figure 4 Internet involves connecting a number of networks

The *Internet Protocol* (IP) is applied as the *common "glue" carrying different applications across different underlying infrastructures*. For example, the IP traffic is initiated in a terminal that is running a browser application. This is started by a user clicking on a corresponding link or icon on the desktop. A request will then be sent from the terminal to the relevant host (servers, gateways) to fetch the relevant content.

Before this is allowed to happen, the terminal has to be allocated an IP address and the relevant access has to be "opened" as seen from the network side. In order to do this a log-in procedure has to be completed. An authentication and authorization procedure is done. This could be done by providing a user identity and corresponding password. Commonly this is automated by installing the proper credentials in the terminal. These are verified by the first ISP there the user has an account (depicted as IP access termination in Figure 5).

Servers could be storing e-mails, web pages, or other services and content. Services and content are commonly identified by a name string, e.g. <u>www.q2s.ntnu.no</u>. In order to make such names useful for the routers in the network, a name has to be converted to an IP address. For this purpose a Domain Name Service (DNS) is invoked.



Figure 5 Example of configuration for Internet-based services to residential market

Features in the intermediate networks are "hidden" for the users; a user merely experiences the response from his or hers actions. So, even if some information is fetched from a server at the other side of the globe, a user might not be aware of this fact, besides that it might take some additional time.

On top of IP a transport protocol is applied; The Transport Control Protocol (TCP) provides effort correction and congestion control. The latter implies that the transmission rate is reduced in case indication of congestion is received. This is typically used when transferring files or downloading objects from a web page. In result the user has to wait for a longer time until the task is completed and the screen is displayed in a correct manner.

When applications can not adapt to the effective bit rate the User Datagram Protocol (UDP) can be applied. Examples of such applications are voice and video with constant bit rates.

There are also a range of other protocols utilized in order to ensure operational Internet services. One class of protocols deals with routing. This is to inform every router along the way from a user/server what to do with a packet containing a certain IP address.

- Internet is based on the Internet Protocol (IP)
- Internet consist of a set of interconnected networks and systems
- Most technical mechanisms are hidden for the user

3. A brief on Internet's history

3.1. Steps towards the technical realisation

For many persons Internet is considered to be the same as the Word Wide Web. That is, the experience on clicking on links to open new objects and looking at information posted anywhere in the world. Information is commonly posted on so-called home pages either by private persons or by enterprises. Also other players have utilised similar mechanisms allowing person to interact in the form of social networks, e.g. Facebook, MySpace and LinkedIn. The information is coded in a standardised manner and stored on computers connected to the Internet.

The World Wide Web, however, is not describing every aspect of the Internet. It is considered as only one out of several possibilities and application areas. Others include e-mail, file transfers, home office, and so forth. The Web technique, in the form we recognize it today, was elaborated in a large international research establishment in Switzerland (CERN) in 1990 – 1991. However, the basic idea of opening windows for collecting information and to navigate by clicking on links were demonstrated already in 1968 [Lund01].

The name Internet comes from the *net of interconnected networks*. This implies that a number of different networks are linked together. In the early days examples of such networks were found at university campuses. Today commercial networks have been installed in every country. The transport between different networks is handled by mechanisms called protocols. The concept of protocol can be considered as an envelope that contains some piece of information to be carried from a sender to a receiver (see Figure 6).



Figure 6 Comparing basic Internet functions with postal service

Basic principles of the Internet, namely the common Internet Protocol and Transport Control Protocol, were developed in the *late 1960's*. In the late 1970s the Internet architecture was developed and tested by a small group of network researchers, [RFC1287].

The fist recorded description of the social interaction that could be enabled through a network was done in a series of memos written by J. C. R Licklider of MIT in August 1962, [Lein07]. This was referred to as the "*Galactic Network*" concept, represented by a set of interconnected

set of computers. Objective was that everyone could get access to data and programs from any site. Licklider was the fist head of the computer research program at DARPA. This started in October 1962.

In the same period, a paper on packet switching theory was published in July 1961 by Leonard Kleinrock at MIT. This was followed up by a book on the subject in 1964. It also paved the way for the theoretic fundament for the feasibility of packet switching.

This all lead up to a Request for Quotation (RfQ) issued by DARAPA. This was done to motivate development of packet switches (referred to as Interface Message Processors, IMPs). The delivery of this equipment was awarded to the Bolt Beranek and Newman (BBN) company in December 1968. By the end of 1969, four computers were connected together to make up the initial ARPANET. As more computers were added, an imminent need for a common protocol suite arose. The network Control Protocol (NCP) as completed in December 1970. As this was introduced on the host computers, applications could be developed. Then, in *1972 the e-mail* as a simple application was introduced. This was motivated by the need for developers to coordinate further activities.

The idea of *an open architecture network* was launched in *1972*. As the NCP was not able to address a destination beyond the IMP⁶, there was a need to enhance it. The protocols emerging would eventually be referred to as the *Internet Protocol (IP)* and the Transmission Control Protocol (TCP). This was driven by Robert E. Kahn according to the following basic rules:

- Each distinct network would have to stand on its own and no internal changes could be required to any such network to connect it to the Internet.
- Communications would be on a best effort basis. If a packet did not make it to the final destination, it would shortly be retransmitted from the source.
- Black boxes would be used to connect the networks; these would later be called gateways and routes. There would be no information retained by the gateways about the individual flows of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recover from various failure modes.
- There would be no global control at the operations level.

These principles are still accompanying most of the development related to Internet.

The original structure was a fairly small number of national level networks. The first address format was a 32 bit IP address. Out of those bits the 8 first bits identified the network and the remaining 24 bit gave the host in that network. Hence, in total 256 networks were supported. This soon came up for review as Local Area Networks (LANs) started to appear in the late 1970s.

As the number of hosts grew it became more challenging to remember their numeric addresses. The *Domain Name System* (DNS) was then invented by Paul Mockapetris of USC/ISI. This was to allow resolving hierarchical host names into Internet addresses.

The size of the Internet grew further. To manage this, *routing protocols* were needed. A main objective of such a protocol was to automatically identify how to handle packets to given destinations. Two protocols were defined; i) Interior Gateway Protocol (IGP), and, ii) Exterior Gateway Protocol (EGP). The former was used within a region/network, while the latter was applied to connect the regions together.

⁶ An IMP corresponds to today's routers, which handles IP packets

The final transition from the NCP to the *TCP/IP* was not done until *1st of January 1983*. This implied at every host hat to convert simultaneously to still be connected. The TCP/IP had already been adopted as a defence standard in 1980. This transition also allowed a separation between the defence/operational and the research network.

At that period, most networks were purpose-built. That is, they were intended for and designed to serve a closed community of persons. In 1984 (British JANET) and 1985 (US NSFNET) announced that the networks should *serve all education communities*, regardless of discipline. In fact, in order to receive funding from NSFNET "... the connection must be made available to all qualified users on campus". The *TCP/IP suite became mandatory* for the NSFNET program providing it formidable backing to gain its dominating position.

From around 1980 there was equipment available from different commercial vendors allowing the networks and nodes to be interconnected. The equipment was used to make a network for research and development traffic with main points located in the USA.

3.2. Administrative units

The *Advanced Research Projects Agency* (ARPA) was initiated in the late 1960s. This was mainly sponsored by the US Department of Defence. A resource sharing network named Arpanet was then established. Initially it connected four computers in the Western US. By 1974 the Arpanet had extended to Hawaii and east to England and Norway.

The *Norwegian Defence Research Establishment* (NDRE) was invited by ARPA in 1972 to a co-operative effort with resource sharing networking. The work by NDRE was mainly related to packet-switched satellite channels, [Lund01]. Measurements were made on a 64000 bit per second channel in Intelsat IV. This resulted in a satellite channel access protocol called Contention Priority Oriented Demand Access (CPODA).

In 1969, S. Crocker (UCLA) established the *Request for Comments* (RFC) style. These were intended as informal fast distribution of ideas to fellow researchers. The set of researches who defined the Internet architecture formed the Internet Activities Boards (IAB). This was set up in 1981 by DARPA and later became the general technical and policy oversight body.

IAB created the *Internet Engineering Task Force* (IETF⁷) who has worked to engineer, define, extent, test and standardize protocols for the Internet. The IETF combined working groups into Areas. Each area is headed by an Area Director. The Internet Engineering Steering Group (IESG) was formed by the Area Directors. The IESG was also formally recognized as a body for reviewing standards. The Internet Research Task Force (IRTF) was also formed.

In 1992, the IAB was re-named as *Intern Architecture Board*. The relations between the IAB and the IESG also became more of a "peer" model.

Only as late as *1991* was the *ban on commercial traffic on Internet lifted*. One of the drivers behind this was the computer evolution. Computers had made their practical applications from the last part of the 1950s. From the academic side it was a request to allow wide access to the computing resources available. Computing resources were quite expensive an only few installations could be afforded.

Most academic groups in Norway (and elsewhere) did not start to show interest in the ARPA collaboration until the 1980s. The network then gradually grew to become global. However, as commercial traffic was prohibited till 1991, there were also little interests from other

⁷ Ref. IETF's home page www.ietf.org

parties. From then on the number of connected computers and the traffic began a phenomenal growth. In the early 1990s these numbers doubled about every 7 months.

In 1994 a few articles in the general press began to point to the Internet as an interesting phenomenon.

On 24th of October 1995 the Federal Networking Council passed as resolution that the term "Internet" should be used. This is to mean a global system that,

- is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons,
- 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
- provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

3.3. Sample of Internet growth

According to [ITU_IDX09], ITU estimates that on a global scale 23 out of 100 persons were users of the Internet by end of 2008, see Figure 7. The same source also illustrates the dominance of mobile as access, although mostly used for voice and short message services in quite a few countries.

Global ICT Developments



Note: * Estimates.

Source: ITU World Telecommunication/ICT Indicators database.

Figure 7 Statistics of ICT-related development on global scale (from [ITU-IDX09])

Although starting as a pure academic network, Internet is today dominated by commercial interests of different types. Regarding banking and trading there is a considerable amount of money exchanged per hour.

Advertisement is another example; According to [AbSw08] the global value of advertisements on Internet is almost the same as all advertisements on TV channels. Internet advertisement has increased by 230 % from 2005 till 2007 to reach about 4 bill. NOK.

- Ideas behind Internet shaped in the 1960s.
- Original principles are still used for today's basic Internet design.
- *Phenomenal traffic growth and increased value only during the last two decades.*

4. Internet's importance for the society

4.1. General effects

There are different effects on the society by the Internet development. These would naturally differ depending on a region's situation.

A first effect is the *improved quality of life* through easy accessible services and content. This would, for example, simplify tasks, avoiding that effort need to be spent on challenges where counter measures have been published by others. Internet does also provide a wider selection of choice among services and content. For person-to-person communication it is a means for easier keeping in contact with persons without having to meet physically. Quite wide spread tools are e-mails, chatting and blogs. These tools are used differently depending on the receiver (or audience) of the messages. A potential drawback is the balance of freedom of speech versus privacy matters, see Section 8.10.

Another effect is the *increasing efficiency of enterprises and governments*. For example, the health sector can gain from simpler communication and surveillance. Another area is better logistics management for ordering and tracking goods. Use of the Internet for intelligent machine-to-machine communication may lead to significant improved productivity. Self-serving, for example network banking also allow for efficiency increase and further cost savings.

One effect of the increased efficiency is improving the nation's *level of international competition*. This is again enforcing a society's wealth. More flexible location of work places could for example attract highly educated persons. The persons working in the field would then contribute with attracting further investments. This may again be utilized to improve a region's attractively.

Promoting electronic collaboration on Internet physical travels and transfer of physical goods could be reduced. In effect, a sustainable society is assisted by applying *climate-friendly* solutions. Reducing work-related travels by remote working and substituting travels by video conference sessions. Lower energy levels could further be achieved by technical development, e.g. using machine-to-machine solutions.

4.2. Pivotal position in global society

Lengthy discussions have taken place regarding different aspects of the impact on the society in general by Internet. In particular two aspects have been mentioned: i) Internet's ability to convey information to anyone, and, ii) potential mis-use by individuals or groups.

A general challenge is to balance the different concerns. A high-level summary of this was endorsed by the UN Assembly of 27 March 2006:

- Principles of non-discrimination regarding access
- Promotion of ICTs as a *tool for peace*
- Instruments to enhance *democracy cohesion and good governance*
- Prevention of abuse, with due regard for human rights

Cost of services is also a critical element as this has to consider the cost of living. Price of ICT in general according to the basket applied for ITU's ICT development index shows that *Norway is among the 10 countries with lowest prices*, see Figure 14. Prices are related to

Gross National Income per capita⁸. For the countries covered in [ITU-IDX09], on average, ICT prices correspond to 15 % of the countries' average GNI per capita. There are significant variations though, from 1.6 % in developed countries to 20 % in developing countries. It is stated that this is often due to very high tariffs for fixed Internet broadband in some developing countries.

1.0 CT Price Basket value 0.5 0.0 Finland Iceland Canada Cyprus Bahrain Hong Kong, China Macao, China Netherlands 3 erman y Singapore **United States** .uxembourg Denmark Inted Arab Emirates Taiwan, China Sweden Norway Switzerland Inited Kingdom Source: ITU

Economies with lowest ICT prices (2008)

Figure 8 Selected service basket prices in different countries (from [ITU-IDX09])

In the same report the ICT Development Index has been tracked over a period from year 2002 till year 2007. This index combines 11 indicators into a single measure in order to benchmark different countries and regions. The indicators are related to ICT access, use and skills. These indicators cover aspects such as number of households with a computer, the number of Internet users and literacy levels. A few of the countries are depicted in Figure 9. According to this the most advanced countries are found in Northern Europe in addition to South Korea. In general a close correlation between GDP and ICT level can be observed. However, South Korea stands out with higher then expected ICT levels in that respect.

Based on estimates from ITU, on a global scale, 23 out of 100 persons used the Internet at the end of 2008. This goes from 5 % in certain countries in Africa to 90 % in other countries in the world.

⁸ Gross National Income (GNI) comprises the total value produced within a country (i.e. its Gross Domestic Product), together with its income received from other countries (notably interest and dividends), less similar payments made to other countries.

The GNI consists of: the personal consumption expenditures, the gross private investment, the government consumption expenditures, the net income from assets abroad (net income receipts), and the gross exports of goods and services, after deducting two components: the gross imports of goods and services, and the indirect business taxes. The GNI is similar to the Gross National Product (GNP), except that in measuring the GNP one does not deduct the indirect business taxes.

For example, the profits of a US-owned company operating in the UK will count towards US GNI and UK GDP, but will not count towards UK GNI or US GDP. [ref. Wikipedia]

The report states that almost all countries have improved their ICT levels during that 5 years period. Eastern Europe is the region where the IDI value has highest relative gains. Other countries with significantly improved ICT levels are Luxembourg, the United Arab Emirates, Ireland, Macao (China), Japan, Italy and France.

The ICT Development Index may also be used to measure the difference and evolution between different countries. This is also referred to as the *digital divide*. The ITU report shows that this has broadly *remained unchanged between 2002 and 2008*, despite significant improvements in the developing world.

On the digital divide topic, [ITU-IDX09] continues with a model on dividing the countries into four groups based on different ICT levels; high, upper, medium and lower. Through the period 2002 - 2007, the distance between high and the others have decreased, while the distance between upper and medium/lower has increased. The report then suggests that as information societies become more mature, ICT levels flatten out. Less mature, but reasonably advanced information societies grow strongly, thereby leaving behind those at the lower end of the scale.

The ICT indicator with the *highest progress is the ICT access*. This indicator includes fixed and mobile telephony, Internet bandwidth and number of households with computers and Internet access. The ICT usage indicator shows a much slower increase. This indicator includes number of Internet users and number of fixed and mobile broadband subscriptions.

Some so-called developing countries have moved considerably higher on the ICT level ranging, including Pakistan, Saudi Arabia, China and Vietnam. This is partly due to high mobile cellular growth, coupled with an increase in Internet users.



Top ten IDI countries

Figure 9 International Telecommunications Union's ICT Development Index (from [ITU-IDX09])

4.3. Impacts on Norway's positions and options

Electronic communications and related services are the largest segment in the entire telecommunications sector. In 2004 it was reported [EC97/21] that about 90 % of European

businesses actively used the Internet, with 65 % of them creating their own web site, while an estimated 50 % of European people regularly used the Internet and 25 % of households used broadband access on an on-gong basis. In view of these numbers, *Norway is among the top nations* in Europe.

EC says that 93 % of the adult population on average have high-speed Internet access in Europe. However, this number is about 70 % on average in rural areas. In some countries such as Greece, Poland, Slovakia, Bulgaria and Romania, broadband Internet covers less than 50 or less of the rural population.

For Norway, reports show that 84 % of households have Internet access by 2nd quarter of 2008, while 73 % of the households have broadband access (up by 6 percent points year-byyear). At the same time 5 % of the population has mobile broadband. About 1 % of the population used mobile broadband as the only Internet access type.

Further samples of statistics from Norway include:

- 90 % of the population has used PC some time during the last three months.
- 75 % uses PC on a daily basis.
- Out of the Internet users, 92 % sends and receives e-mail,
- 47 % downloads software,
- 81 % has contact with public authorities.
- About half has used Internet to watch TV or listen to radio, quite corresponding to the OECD statistics (see Figure 10).
- Looking at the age group 16 24 years;
 - o 91 % has used MSN, 59 % has used chat,
 - o 51 % has read others' blogs.
- About 63 % of the Norwegian population has used Internet for trade/shopping. Among the most popular ones are shopping for travels and hotel bookings.

Statistics, e.g. from the gallup⁹ show that there are clear favourites regarding popularity of public web pages. Typically news sites come out as leaders, while there are also search pages among the top ones.

⁹ Web page: http://rapp.tns-gallup.no



Figure 10 Internet users listening to web radios/watching TV – selected OECD countries (from [OECD07])

When looking at the traffic carried by the Internet, one observes that video content, including TV programmes, short video clips and films gain popularity. Such material is quite bandwidth consuming. For example one minute of medium quality video makes up around 7 - 10 Mbyte of data. Compared with telephony, one minute could result in about 0.5 Mbyte of data. Hence, there will be at least one order of magnitude difference between video and voice. Then, as video evolve to High Definition, this difference grows even further.

To reduce the network load of distributing live TV, multicasting is commonly used. By utilising multicasting the same data is send to many users at the same time instead of sending dedicated stream to each user.

For content distribution, caching is also commonly used. Caching involves storing data closer to the user to that it does not have to be sent over the whole network each time it is requested.

The so-called peer-to-peer mechanisms are also popular when distributing content and information of different types, see Section 9.6.

- Internet holds a key position in any modern society.
- Steadily growing number of applications, services and content.
- Further innovation needed to maintain an efficient Internet.

5. Initiatives from European Union

Various initiatives addressing status and future options for Internet has been high on the political agenda for several regions. For example, as presented by Viviane Reding in February 2009 [Redi09], many European states have taken initiatives towards the future of the Internet. Examples include:

- "plan numérique" in France;
- "IKT 2020" in Germany:
- "Digital Britain" in UK, and
- "ambient Sweden".

The latter states the ambition of Sweden becoming a "leading Internet nation" by 2015 (see Section 11.6). A common element of these initiatives is that they *capitalise on the future developments of the Internet*. However, to be successful, it is stated that governments behind each of these should cooperate within Europe and at the global level.

[Redi09] starts out by setting the scene pointing to how today's Internet is challenging traditional regulatory theories and governance practices. The main reason for this is related to the blurring of concepts of territory and sectors. That is, the virtual worlds of Internet do not know any national borders. There are also several industry sectors that have rough encounters when addressing similar services and markets.

Looking forward, it is more questions are expected in the areas of *security, privacy and governance*. To address these as well as the aspects of effectiveness and inclusiveness, the European commission, from 2009, will increase its efforts regarding:

- increase in the R&D elements,
- active participation in discussions on the regulatory approach to applications and services,
- proposals on governance issues, and
- active promotion of roll-out of IP version 6.

As further stated, ICT contributed to 40 % of the overall productivity growth in the economy for the ten years up to 2004. One factor related to this is the so-called network effect, which has enabled an *accelerated and global diffusion of innovation*. Reding's speech goes further on by stating that "to get out of the economic downturn we need to stimulate a solid and sustainable business growth in the high value goods and services that respond to real market needs".

[Redi09] mentions three main drivers for Internet evolution:

• *Social networks*: examples are Facebook, LinkedIn and others. Some also refers to this as Web 2.0. It is argued for a shift from "Web 2.0 for fun" to "Web 2.0 for productivity and services". Web 2.0 is commonly seen as one of the fastest developments of the Internet today and keeps the potential to connect users of similar interests.

The networking effect of this may open for new opportunities. It can also reach new levels of collective behaviour and meet needs of significant user groups. Some refers to Web 3.0 as a "place" where *collaborative working* and productivity takes place. This means that contributions are offered by different persons to solve a common

challenge. This, however, has already happened for certain areas such as Open Source software development. Web 2.0, or Web 2.0 networking in the business world, holds the prospect of interoperability across different business segments. This lowersthe threshold, in particular for SMEs to enter markets through collaboration.

"*Gov. 2.0*" is mentioned as a facet of the social networks. This could be used to engage more people in political life and democratic processes. A recent example of this was the use of Internet during the Obama campaign autumn 2008 driving at making users feel part of the campaign. In general, a user would also feel part of the government in support of the policy makers.

Consumer force of the social networks should not be neglected either. One example is the protest against Facebook's change of contract during February 2009 rising more than 80 000 protests during the first day of initiation.

• *Internet of things*: Due partly to the miniaturization, the number of objects and devices containing communication capabilities grows intensely. The effect on everyday life from this is not fully understood, although there are several business ideas around.

Related to this is the concept of *virtual and physical worlds*. A device could be accessed and perceived as a certain physical object, although its actual implementation is hidden for the users.

Another aspect is the separation of service from the infrastructure. This implies both the option to offer services without managing a physical network as well as the abstraction of "resources". Several systems have been promoted in this area, for example the "Cloud computing". One idea behind the "Cloud computing" is to gain from the scaling effect of sharing common servers, while the users should not bother themselves as to where "their" resources are located. Again, the thresholds for smaller enterprises are lowered as they do not have to invest in full-blown server capabilities to start their business.

Mobile Internet: This is partly driven by the availability of so-called Smartphones and partly by the general usage of the Internet for which mobile handsets are just another terminal. Capabilities of handsets highly influence the usage. Some measurements show that Internet usage is more than ten times higher for Smart phones compared with less sophisticated handsets. As the bit rates on mobile networks increases, e.g. by HSPA¹⁰ and LTE¹¹, response times improve drastically. This improves the user experience. However, to keep up with the increasing demand, additional frequency spectrum could be released for mobile networks.

In view of the three drivers above, [Redi09] addresses key issues related to the future Internet:

• Openness of the Internet: It is commonly claimed that the openness is a main factor for the innovation volume related to Internet. Two topics within this area are the i) Net neutrality, and, ii) Open standards. As issued by the Norwegian Post and Telecom Regulatory Agency, it is *not allowed to negatively discriminate any application* for a user. This is argued by avoiding anti-competitive practises.

A main advantage of the open standards and interfaces is the number of developers and providers contributing to developments. Typically competition authorities play a

¹⁰ High Speed Packet Access, evolution of Universal Mobile Telecommunications System (UMTS)

¹¹ Long Term Evolution, further upgrade of the mobile system (beyond UMTS)

significant role to avoid that any dominant player introduces any un-fair solutions. In particular, this would be relevant for the Internet of things area. ETSI standardisation has been initiated to provide standards in the machine-to-machine area, promoting open solutions and lowering market-entry barriers.

• Globalisation: As steadily more persons on the globe get access to the Internet, there will also likely be a shift in "power" from traditionally dominating regions to other regions. For example, China is already the largest country in terms of number of Internet users.

The globalisation also raises several other questions like how to cope with cultural preservation, maintaining the economic incentives, open for additional security aspects, and so forth.

Regarding openness, Meglena Kuneva, the EU's Commissioner of Consumer Affairs and Protection in is in the vanguard. This is to prevent the spread of deep packet inspection mechanisms. Such mechanisms can be used to adapt content of information flow or content of web pages. These mechanisms can be applied for different purposes as well. However, they are particularly opposed when used for *intervening with users' behaviour and experience*.

In her speech Ms. Kuneva said "Consumers are in fact paying for services with their personal data and their exposure to advertising¹². This amounts to a new kind of commercial exchange. We need to investigate this quickly, we cannot afford foot-dragging. If we fail to see an adequate response to consumers' concerns on the issues of data collecting and profiling, we will not shy away from our duties."

The European commission has for instance sent a letter to the British government demanding to know the details of an legal justification for the secret trials of the Phorm system that were carried out by BT. The idea behind Phorm is that by tracking a web user's browsing activities, advertisers can send closely targeted ads to individuals based on their particular Internet histories and preferences. BT was running trials without informing users that their web browsing habits were examined. The trails were later closed.

Ms. Kuneva said that the vast majority of Europeans have *no idea what personal data is being collected, how it is being collected, how safely it is being stored, who has access to it and how it is used for commercial purposes* (ref. Section 8.10).

The EU directive on privacy and electronic communications basically says that member states must ensure the confidentiality of data on communications and related data traffic. Unlawful interception and surveillance must be prohibiting unless the users concerned have consented to such activity.

Commissioner Reding reinforces the sentiments in a recent statement, noting: "Europeans must have the right to control how their personal information is used. European privacy rules are crystal clear – *your information can only be used with your prior consent*". She also pointed to other areas where close observation is warranted. This includes significant amounts of data that social networking sites hold on their users, and the increasing use of RFID chips¹³ in a wide range of devices.

¹² On a global scale the value of advertising on Internet is about the same as advertising on TV.

¹³ RFID chips can be implemented on different types of objects and are typically used for tracking the whereabouts of those objects

The European Commission has initiated several actions to encourage innovation related to Internet. One is the Public-Private-Partnership. Research initiatives within the EU system include:

- ICT Framework Programme 7 projects; e.g. 4WARD, TRILOGY, Euro-NF, EIFFEL
- Cross-project initiatives, e.g. Future Internet Research and Experimentation (FIRE)¹⁴
- European Technology Platforms: eMobility, NESSY, ISI, NEMS

The Future Internet Assembly (FIA) was established on 31 March 2008, as a conference organized by the European Commission and the Slovenian European Union Presidency. FIA has an objective to enable fundamental and systematic innovation in Europe in networking and services. This is to realize the future Internet within year 2020. FIA includes most of the research projects within the 7th research programme of EU that are associated with the future Internet. FIA grouped the activities in to a number of areas depicted in Figure 11, and has defined the following strategic goals:

- A joint strategic research agenda for the Future Internet encompassing common actions and requirements
- Fostering common research deliverables and results creating value for the EU research projects concerned.
- Developing a consolidated calendar or events aiming at avoiding fragmentation of research efforts in Europe.



Figure 11 Research areas defined by Future Internet Assembly

The EC has proposed \in 1 billion of additional spending for broadband investments over the next two years. This comes in addition to the \in 15 billion spending on public services and Internet infrastructure under the EU's Cohesion Policy for 2007 – 2013. The additional spending is to achieve *100 % high speed broadband Internet coverage in Europe by 2010*. There is no mentioning of which technologies to prefer.

¹⁴ Future Internet Research and Experiment (FIRE) is to provide an open playground for research that cannot be conducted on a critical infrastructure. Facilities are based on federation of existing testbeds.

- Internet high on EU's political agendas.
- Great attention regarding fair and secure handling of user data and traffic.
- Several initiatives launched to ensure a future efficient operational Internet.

6. Technology-based challenges of today's Internet

6.1. Originally identified shortcomings

Already in the early 1990s several challenges were identified, [RFC1287]. These were summarised as:

- *Routing and addressing*: This is a crucial challenge as it directly goes on ability to further scale. One way forward could be to aggregate addresses into larger units for routing. Some nodes on the way may also contain state information to ensure service levels.
- *Multi-protocol architecture*: Different applications and protocol suites could be requested. Translators and other gateways could be present and should then be recognised by the architecture principles.
- *Security architecture*: Security should be built into the architecture from the beginning. General principles are simplicity, testability, trust, and technology and security perimeter identification.
- *Traffic control and state*: To support real-time applications additional mechanisms might be requested. This is resting on the assumption that some performance guarantees of selected traffic subsets should be supported.
- *Advanced applications*: Innovation and standardisation in building new application types. A common format for describing data items would then be needed for the systems to express and agree upon application characteristics.

To some extent, these have been dealt with during the last two decades. However, several issues still remain. One of the approaches proposed is referred to as *clean slate*. This implies that any limitations from today's Internet are not considered when designing the new architecture. An argument for this is to avoid projecting any unstructured solutions of today into the future architecture, as illustrated in Figure 12.

The Internet allows higher degree of personalisation. This implies that every person can adapt his or hers experience according to individual preferences. This implies that level of quality and security must be predictable to raise the trust level. In order to simulate innovation, services must also be swiftly accessible for users. This is to allow sustainable business to be conducted.



Figure 12 Longer history tend to imply a range of non-optimized components that could be restructured through a new architecture (based on [AKAR08])

6.2. Sample list of shortcomings

As stated in [GENI07] there are serious problem facing the current Internet:

- *Inadequate security* The Internet is not secure: We hear daily about worms, viruses and denial of service attacks¹⁵. We have reason to worry about massive collapse, due either to natural errors or malicious attacks. Problems with "phishing"¹⁶ have prevented institutions such as banks from using e-mail to communicate with their customers. Trust in the Internet could be eroding.
- The current Intent *cannot fully deliver* to society the *potential of emerging technologies* such as wireless communications. Even as all our computers become connected to the Internet, we seen the next wave of computing devices (sensors and controllers) rejecting the Intent if favour of isolated "senor networks".
- *Inadequate reliability* The Internet does not provide adequate levels of availability. The design should be able to deliver a more available service than the telephone systems. Our future network should be robust and reliable enough to meet the needs of society in times of crisis.
- The design of the current Internet actually creates *barriers to economic investment* and enhancement by the private sector. For example, barriers to co-operation among Internet Service Provides have limited the creation and delivery of new services, including transport-level services such as enhanced Quality of Service (QoS), and

¹⁵ Denial of service refers to a planned attack of selected machines by generating a high amount of traffic to these machines such that "normal traffic" is not successfully managed.

¹⁶ Phishing refers to theft of identities.

application such as Internet-based telephone service. A large number of specific problems with the Internet today have their roots in an economic disincentive, rather than a technical shortcoming.

- *Inadequate manageability* The Internet was not designed to make it easy to set up, to identify failures and problems, or to manage. This limitation applies both to large network operators and the consumers at home. Difficulties with installation and debugging of Internet in the home have turned many users away, limiting the future penetration of the Internet into society.
- *Inadequate evolvabilty* The current implementations are often tuned by introducing dependencies. In effect changing a certain aspect of the Internet then would introduce changes of several items. It is a classical problem that the longer a system has been in operation, the more challenging it is to introduce upgrades. This is also related to providing proper incentives for introducing new technologies.

It is summarised that these *shortcomings are rooted in the Internet design*. In the mere two decades since the Internet left the research desk and entered the commercial work, it has changed the way we work, play and learn. In fact, there are few aspects of life that are not touched in some way. We may, however, be at an inflection point in the social utility of the Internet, with *eroding trust, reduced innovation and slowing rates of uptake*.

For some time the approach pursuit by the Internet community is to work around these limitation introducing a series or proposed "patches" (see left part of Figure 12). Implementing these patches would lead to growing complexity and could result in systems that are both less robust and less manageable.

Hence, there are real probabilities that Internet may not be realized because of its technical shortcomings – opportunities and potentials that would be of great importance to the society.

Related to discussions in Future Internet Assembly (see Section 5), the following aspects are considered missing in today's Internet (ref. [Tsel09]):

- Inherent network management functionality, specifically self-management functionality.
- Facilities for the addition of new functionality, including capability for activating a new service on-demand, network functionality, or protocol (i.e. addressing the ossification bottleneck).
- Facilities for the large scale provisioning, management and deployment of service; support for a high-level integration between service and networks.
- Facilities for orchestration of security, reliability, robustness, mobility, context, service support, and management for both the communication resources and the service' resources.
- Mobility of networks, services, and devices.
- Facilities to support Quality of Service (QoS) and Service level Agreements (SLAs).
- Trust Management and Security; Privacy and data-protection mechanisms of distributed data.
- An adequate addressing scheme, where identity and location are not embedded in the same address.

- Facilities to interact with the physical world and seamlessly use the physical context information to enhance and improve existing services and to create the new ones.
- Socio-economic aspects including the need for appropriate incentives, viable business models, legal and regulative issues, and the need for security and privacy.
- Energy awareness.

The Internet Protocol (IP) is the key technical element of the Internet design. The basic protocol has a number of limitations as identified by [AKAR08]. To address these limitations the AKARI project, [AKAR08], has identified the following design guidelines for a future:

- Sufficiently IP long addresses
- Elimination of IP options
- Elimination of fragmentations (packets should be kept between end-points, not broken into several parts)
- Connectionless network layer (removal of the concept of time)
- Removal of PMTUDa¹⁷ in the network layer
- Assignment of hierarchical addresses at the ISP level
- Active support of multiple addresses
- Splitting addresses into identifiers and locators (an identity must not at the same time state where the device is located)
- Recognition of source locator rewriting
- Individual support to diverse data link layers
- Introduction of link broadcasting
- Not requiring standard support of multicasting
- Not requiring standard support of IPsec -
- Each host (including routers) has a non-default route
- Standard support of mobility

One of the main points is the *separation of identifier and location* of node/terminal. As a single IP address is used today both for node identifier and location identifier, there are *challenges to be faced to swiftly support mobility and multi-homing management, network renumbering, security and privacy, scalable routing and traffic engineering.* [AKAR08] mentions that in case today's Internet addressing scheme is continued these challenges will increase due to more diverse services, larger number of users, heterogeneous devices and more dynamic network environment. This leads up to that node identifier should be split from the location.

6.3. Example from security area

As mentioned above, one of the weaker sports of today's Internet is the security area. Commonly users are bothered by different kinds of malware; spam, fraud, spyware, worms,

¹⁷ Path Maximum Transmission Unit Discovery, option for detecting maximum packet sizes and potentially divide a packet into a number of fragments.

etc. There still seems to be lacking guidelines on how to combine different mechanisms to achieve an overall security solution. Many of the security problems that trouble users are not in the Internet itself, but found in the end-nodes and in personal computers that are connected to the Internet. Moreover, many security challenges are not just failures of technology but a combination of human behaviour and technology.

Several of the security issues are related to the distributed applications. This includes authentication access rights, robustness, reliability and security of applications. These could be handled by the application server providers. However, intentional malfunctions and attacks have to be addressed by outside systems.

As one example of increased society's dependence on Internet, considering the following example described in [GENI07]: "In 1989 a bug in the Internet's core routing algorithm inconvenienced a few thousand researchers. In 2003, the SQL slammer attack grounded commercial airline flights, brought down thousands of ATM machines, and in the end, caused an estimated one billion dollars in damage."

There are also several educational topics related to security for example not revealing ones passwords or account information, and to activate virus detectors and preventions.

Some also sort piracy and copyright under the security headline. A basic moral question facing many users is: Why pay when you can download it for free? Illegally distributed content of various types flourishes. Although it is commonly an efficient way of distributing free and open information, is do not attract all the professional users (e.g. within the music and movie business). Hence, Digital Rights Management (DRM) becomes more important for relevant information/content.

As more information and content come in digital format the rights issues grow. This is already observed by piracy, for example for music and movies. When the Norwegian movie "Max Manus" was launched in cinemas late December 2008, it took less than 10 days before it was available on Internet in piracy versions.

6.4. Example from area of addressing

The Internet Protocol version 4 (IPv4) was created in the 1970's. This was in good time before the world wide web, home computers, and in general the Internet as we know it today. Few, or none, could foresee that the protocol's 32 bit address space, as part of the IPv4 headers should become too small. In fact the 32 bit would allow for about 4.3 billion addresses¹⁸.

However, in the beginning of the 1990's there were emerging concerns regarding the exhaustion of addresses. Some of this was related to the way IPv4 addresses had been allocated; Firstly three classes were defined – A, B and C:

- Class A prefixes were 8 bits (supporting 16 777 216 addresses each)
- Class B prefixes were 16 bits (supporting 65 536 addresses each)
- Class C prefixes were 24 bits (supporting 256 addresses each).

One difficulty was the large difference between class B and class C. The latter could only support small networks, while class B often resulted in a waste of addresses. In addition to this, simply the number of devices requesting an IP address outnumbered the total number of addresses available in IPv4 format.

 $^{^{18} 2^{32} = 4 294 967 296}$
So, the initiative for specifying IP version 6 was started.

6.5. Example from area of service quality

For more than a decade, there have been various initiatives for introducing Quality of Service (QoS) into the Internet. There is still no wide-spread implementation of QoS. There seems to be missing coherent understanding of the society demands, business incentives and the technical implementations. As more applications and content are making use of the Intenent, the service requirements may be wider. For example, the expected delay and response time for a packet as part of a voice conversation are not the same as when a link is clicked on. According to ITU's QoS recommendations voice samples delayed more than a few hundred milliseconds would annoy the user. On the other hand, a couple of seconds for a complete web page to download would be acceptable.

As one area within QoS, routing challenges are on trivial in today's IP networks. The AKARI project [AKAR08] lists the following shortcomings:

- Inability to aggregate routes
- Route oscillation
- NP completeness for optimum route calculations
- Advertisement scalability
- Drop in reliability of routing information when a hierarchy of routing information is created
- Loss of routing information for destination locality when a hierarchy of routing information is created
- Optimum selection of inter-domain route
- Combinations of resource constraints with multicasting
 - Technical shortcomings already identified two decades ago and are still valid.
 - Several shortcomings related to basic design of the Internet.
 - Although several proposed solutions, proper incentives and means for implementing new basic functionality are not clear.

7. Basic technical trends

7.1. Fundamental technical trends

There are five fundamental trends within the area of electronics that have impacts on telecom and Internet:

- Increasing *processing capacity*: Morse's law predicts the increase of processing capacity. This has been self-fulfilled for some years and is still expected to continue for a few years.
- Increasing *memory capacity*: Amount of data that can be electronically stored seems to increase even more rapidly than the processing capacity for the last year. It is predicted that, keeping up this trend, one year of video consumption can be stored in a typical mobile phone by year 2012.
- Increasing *bandwidth*: Bit rates transferred on wired and wireless links jump in steps according to new generation equipment. Talking about 64 kbit/s about 15 years ago, bit rates in the range of 1 10 Mbit/s are commonly deployed, and systems of some hundred of Mbit/s (and even higher) are planned.
- *Digitalization of content*: More content is produced and made available in digital format. This invites for distribution on the Internet. Content is made by professionals and any other users. For example, YouTube and other sites have emerged as places where anyone can publish their own content (video clips, pictures, etc.)
- *Miniaturization*: Electronic processing, memory and communication capabilities are implemented in small devices. This includes sensors, readers of different kinds and controllers. The Internet of Things is following as the number of devices is multiple times the number of persons in the world.

These fundamental trends fuel the amount of data to be exchanged, the rate of exchanging data and the number of units that are connected to the Internet. Simply scaling up the current implementations will struggle to keep up with the increasing demands.

7.2. Who communicates with whom

Traditionally, much of the Internet traffic has been US centric. However, this is changing; the rate of Internet traffic crossing US borders has dropped from 75 % to 25 % (see Figure 13). A reason for this is that other sites for information and applications have appeared. It is also, of cause, an effect of that other usage patterns have emerged. A third reason is that some commercial players have installed main sites in other countries outside the USA.

Rerouting the Web

Since the dot-com bust, more and more international Internet pipelines are being created that do not pass through the United States and Canada.

SHARE OF INTERNET BANDWIDTH CONNECTED TO U.S. AND CANADA



Source: Telegeography

Figure 13 Rate of Internet traffic crossing North America borders (from [NYTI08]

One cannot use this observation to claim that the globalisation has been replaced with a more regionalisation trend. As the total amount of traffic is increasing significantly (doubling about every second year), the amount of traffic flowing across continents is not decreasing, but rather increasing in absolute terms. Looking at characteristics of phenomena like peer-to-peer, a requestor also looks for sources in its vicinity, adding to the rate of intra-regional traffic.

7.3. Convergence – multiple applications on a common infrastructure

One of the main trends in our industry is the convergence; *Convergence between telecom, media and information systems*. The term convergence by itself is derived from Latin *con verge*, which means to get together or approach each other.

If we look at the mass media as one example, we find that convergence implies that information and communication flows are approaching each other. For example news paper, books photos, music are now delivered by the same communication channels and networks. A key enabler for this is that *most media types these days are digital*.

There are also voices stating, when only looking within the media arena, this actually implies divergence. That is, in the meaning that regarding different sources for publishing content and the types of content available, the manifold gets bigger.

These days you may record a song in your own living room and publish it at relevant sites on the Internet. The whole process does only require a few clicks on a PC. In effect the song could be available for anyone to download and listen to. This is done without professional tools are required earlier. In effect the threshold for contributing to the amount of content and

information available on the Internet is getting lower through user-friendly applications and interfaces.¹⁹

By itself this is typically considered as an enrichment of available information. It may also involve some doubtful events, such as using these means for expression ones opinions disfavouring other persons. Several events have already been reported, for example harassment among pupils (ref. Section 8.10).

One of the goals from the media companies by utilising such means it to involve the users. One example from 2008 was observed when CNN and Facebook teamed up to stream the inauguration of Barack Obama. The news channel generated 21.3 million live video streams on-line. The social network site generated about 4 000 comments per minute. This could be a step for other players to enter the social network dimension.

Besides the media aspects, convergence is also recognized on the technical side. Earlier, telecom networks were built as vertically integrated solutions. That is, dedicated protocols and mechanisms were defined and installed. Complete systems were then standardised and implemented. This has changed, however. Several of the Internet principles are heavily utilised for emerging telecom systems. For example the *Next Generation Network architecture* as standardised by ITU-T is characterised as a packet-based network able to make use of multiple broadband technologies.

This will enable provision of services to users with independence of service-related functions from transport technologies. In effect, a network arises capable to serve any application, access type and usage situation. A key driver for this is to gain from the *economy of scale/scope*.

7.4. Future expectations

<u>General</u>

On a general level, a future Internet should enable and foster (from [GENI07]):

- A world where *mobility and universal connectivity* is the norm, in which any piece of information is available anytime, anywhere.
- A world where more and more of the world's *information is available online*. A world that meets commercial concerns, provides utility to users, and makes new activities possible. A world where we can all search, store, retrieve, explore, enlighten and entertain ourselves.
- A world that is made smarter *safer, more efficient, healthier, more satisfactory* by the effective user of sensors and controllers.
- A world where we have a balanced realization of important social concerns such as *privacy, accountability, freedom of action* and a predictable shared civil space.
- A world where "computing" and "networking" is no longer something we "do", but a natural part of our everyday world. We no longer use the Internet to go to cyber-space. It has come to us: a world where these *tools are so integrated into our world that they become invisible*.

¹⁹ There is no guarantee that the song will be heard in good quality and become a world hit, though.

Technical implications

From a technical point of view there are several expectations on a future Internet:

- *Multi-service*, supporting convergence of voice, video and data; even though any traffic flow can be carried by the Internet Protocol, there may be additional mechanisms and protocols needed to effectively support the different applications.
- *Quality of Service*; despite numerous activities for introducing QoS support, no single, unique QoS model has been implemented. Some states that a single, best-effort service class may suffice as long as there are sufficient resources available.
- *Plug and play, auto-configuration*; simple processes for installing and removing components, both within the terminals and within the network elements, as well as network elements themselves.
- *Connecting devices*; additional number and types of devices will emerge that want to communicate. Two examples today are electricity power meter and car surveillance. The communication patterns diverge from today's applications dominated by human interactions. The increasing number of devices must also be managed in an efficient manner. Software will also increasingly interact with other software by remotely accessing data, synchronising processes and requesting various resources.
- *Mobility*; for the current Internet the IP address designates both identity and location. Hence, there should be mechanisms allowing the IP address and location as same time to change during sessions. Decoupling the service from the infrastructure, users expect to access services available anytime and anywhere.
- Security and trust; improved privacy and attack prevention mechanisms are asked for. These need to be balanced with lawful requirements and governmental regulations for traffic inspection. Simpler manner for authentications should also be supported e.g. by allowing single-sign-in²⁰ for individuals. Common Internet functions such as DNS should be made more secure (e.g. by introducing secure DNS). Mechanisms to strengthen authentication and tighten spam control and various attacks should also be introduced.
- *Addressing*; one of the security weaknesses is that present addressing schemes allow address-based attacks, such as identity theft. Hence the locator should be separated from the identity. Then, not allocated IP version 4 address space is also almost empty.
- *Routing*; routing protocols (e.g. BGP²¹) do not carry business relationships between ISPs. The recovery times after failures as usually too long, which also may result in instability and routing oscillations.
- *Affordable service offerings*; users' requirements will vary according to multiple dimensions. At the same time as there are simple low-fee services, more advance offerings would also be required. It would be unlikely that a single service will fit every user in all countries.

²⁰ Single-sign-on allows a user to only provide his/her credentials once even though several services are used.

²¹ Border Gateway Protocol, commonly applied between domains of an IP network to exchange information used when routing traffic

- *Data storage provided*; accessing and working on documents and data across different devices requires capabilities for either i) synchronising the different devices, or, ii) storing relevant information in the "network".
- *Simple and intuitive user interfaces*; some claim that the browser-/window-like interface appeals to most users. Hence, this may dominate also for traditional session services like voice and video communication. Usability and user experience aspects are crucial to get foothold in a wider market. Additional features such as voice recognition, eye-tracking, touch displays are improving the user experience, although a certain acceptance period is expected.
- *Management*; current Internet is quite challenging to manage as it lacks uniform specifications of OAM. For some implementations there are too many protocol layers involved implying low overall efficiency, for example due to high protocol overhead. Arguments might be encapsulating non-native Internet protocols and various tunnelling solutions for manageability. The protocol stack should be re-thought for those cases.
- *Climate-aware service implementations*; allowing power saving modes when not fully utilized. This may address features both in the devices and the network/servers.

Any service provider and network operator has dimensioned networks for voice and data traffic for decades. Different traffic characteristics will emerge due to the multi-service applications. Traditionally, Internet traffic has been dominated by best-effort, coming from browsing, e-mail and file transfers.

As the content industry sees Internet as an important distribution channel, some of this may change. Hence, content of any kind of media could be expected including full-length movies, video clips, and interactive pages.

Another emerging traffic type may come from machine-to-machine communication. For some applications the control and management information would dominate the traffic picture and asking for additional dimensioning exercises. Examples include sensor networks, power meter readers, but also more intensive implementations such as for grid computing.

Requirements for a continuous up and running Internet service is also growing from different users. This comes both from the pivotal position Internet has taken for conducting business and the change in attitudes among users in general.

Table 1 summarises a list of expectations for a future Internet regarding aspects that have limitations in today's situation.

Usage trend	Technical limitations	Application enabler			
Mobility	Native support in an infrastructure conceived for fixed usages	upport in an Internet environment open and fully available on the move ages			
End to end very high rate throughput (broadband)	Internet protocols not designed for ultra broadband scenarios	Support of data intensive usage scenarios, such as medical imaging transfer and processing			
Security and trust, privacy	Security and trust mechanism natively supported in service and network infrastructures.Application scenarios invol processing of sensitive pers data or financial transactionPrivacy by designApplication scenarios invol				
Device connectivity coupling of virtual world data with physical world information (RFID, sensors)	Network architecture scalability, non-existing protocols to support device generated traffic, non-existing service architectures enabling also service discovery	Applications coupling physical world information with data, e.g. logistics, transports, environment, energy efficient grids, remote patient monitoring			
User generated services, as a follow up to user generated content	Service architecture enabling dynamic, secure and trusted service compositions and mash ups	Cloud computing type of applications, (global) applications requiring massively distributed computing such as multi-media search, Internet of Services			
3D becoming mainstream	Imposes resource intensive usage of computing and networking platform, standards	3D virtual environment, possibly coupled with physical world information, beyond games			
Negotiated management and control of resources, negotiated SLAs	Dynamic and predictive network management, infrastructure observability and controllability	Variability of business model, from best effort low level of control towards full real time management of quality of service, security level			
User controlled infrastructure	Ad hoc network and service composition	User driven deployment scenario and control of connectivity business model			

Table 1 Expected improved in future Internet compared with today's version (adapted from[NIDwg08])

- Basic trends of electronics increase the pressure on Internet.
- *Relative traffic interests are less dominated by information located in the USA.*
- Lengthy list of expectations regarding the future Internet.
- Many areas of Internet are up for refurbishment.

8. Evolution opportunities

In the following sections, some opportunities are highlighted. Note that this is not considered to be an exhaustive list of opportunities.

8.1. General approaches

Discussion the future Internet there are two main camps (see Figure 12):

- *Migration*: A next generation Internet broadly based on the current version where certain improvements are gradually introduced.
- *Clean slate*: A new version of the Internet not considering the current implementation.

The discussion between these views goes along the arguments on effort needed for migrating from today's Internet and the opportunities revealed in case blank design sheets can be assumed.

The Strategic Research Agenda work as part of the Future Internet X-ETP group has come up with the following illustration of challenges and approaches for the future internet (see Figure 14).



Figure 14 Future Internet challenges and approaches as elaborated by the Future Internet X-ETP group on Strategic Research Agenda

Some common infrastructure is utilized for different areas. The different areas do, however, provide functionality in a coherent manner for the society. The areas identified are:

Internet by and for People: Accommodate anticipated and unanticipated people and community expectations together with their continuous empowerment, cultural

acumen, and self-arbitration (by recognizing that access and use of information as well as associated processing means are common non-discriminatory universal rights).

- *Internet of Contents and Knowledge*: Access by advanced search means and interact with multimedia content (e.g. 3D and virtual reality) that can be created, and manipulated by professionals and non-professionals and be distributed and shared every where on any terminal per needs
- *Internet of Things*: Context-aware autonomic objects able to generate automatic code and human-controlled behaviour, exploiting peer-to-peer bio-inspired communication models
- *Internet of Services*. Service "consumers" look for the perfect interactivity in context. With perfect it is meant
 - \circ Permanent i.e. interactivity that has no time limits.
 - Direct i.e. the service consumer is only concentrated on the benefits of the service he/she is using.
 - Seamless i.e. the interaction is performed using the typical devices of the context.
 - Confident i.e. services can be trusted.

As also shown in Figure 14, a number of aspects have to be elaborated in order to comply with requirements for the future Internet. The following sections address a selection of these aspects. Note that this list is not exhaustive, neither providing a balanced view between the different aspects.

8.2. Identities

A coherent identity management regime is needed. In several ways identities are fundamental for an efficient running Internet. Some of the goals are (from [GENI07]):

- *Authenticity* Users should be able to verify that their data came from the appropriate source.
- *Availability* Data and services should have high reliability and low latency. Commonly availability is increased by providing replication and the network's role is to route user requests to nearby copies.
- *Persistence* Identities of some data or service should remain over time, e.g. avoid "broken links" at web.

In case the system of identifiers is not implemented in a coherent manner, trust can not be established. Considering the huge number of service, devices and users, a single identity scheme would be less likely. Hence, there would be need to translate between different identity formats. This is also done today, such as between domain names and IP addresses (done by Domain Name Service).

Addressing makes a corners stone in the current Intent as it uniquely provides whereabouts of the identified component. The current addressing regime has been designed under several constraints like request for relatively compact address formats and fixed formats to allow for high speed and low cost routing mechanisms. This will also require mechanisms for locating different devices and services, hence also supporting a generalized mobility model.

Different mobility levels can be identified:

- *Terminal mobility*: The mobility of a node, for example a handset or a laptop. This refers to a device changing its point of attachment to the network while the ongoing session is not interrupted.
- *Network mobility*: An IP sub-network changing its point of attachment to an IP backbone. This could, for example, be a mobile router on a bus/train providing further services to devices onto the bus/train. Hence the internal structure of the mobile network is relatively stable.
- *Personal mobility*: The ability of a user to access services regardless of the terminal or network he is using, and focuses on the movement of users rather than devices.
- *Session mobility*: The mobility between two terminals and it is mainly about tracking the communication session between two terminals.

All these should be supported to allow for service flexibility and improved user experience.

8.3. Virtualisation

Virtualisation of network resources is one way of *separating a common network into logically partitions*. Virtualisation has been used for some time, e.g. for Virtual Private Networks (VPNs). The idea is to allow different users to share the same physical infrastructure, while still avoid that their behaviour is seen by other users.

Network virtualization technology implies that a shared physical network can appear as a set of multiple, independent logical networks. This has been proposed as an approach to enable the so-called *clean-slate design* of new Internet models. Network virtualization should then enable different groups to construct, deploy and evaluate different network architectures and service concepts on a shared IP-based network.

All types of resources can be virtualised such as link bandwidths, processing capacities and storage spaces. A major challenge is to define unified control and management mechanisms that automate the sharing of the physical resources. This must consider users' requirements and ensure separation between different user groups.

Some requirements placed on virtualisation are:

- Sliceability; sharing of physical resources
- *Generality*: to make the virtualised resources as flexible as possible. This implies that individual components should be reconfigurable.
- *Fidelity*: the components should resemble a real (physical) resource as closely as possible.
- User access: users need access to set up, manage and observe service levels
- *Controlled isolation*: logical resource groups should be isolated from each other to prevent any form of undesired interaction
- *Diversity and extensibility*: allow the incorporated o a number of networking technologies and protocols.
- *Wide deployment*: accepted solutions principles to gain from economy of scope/scale and points of access.
- *Observability*: support monitoring capabilities to understand traffic characteristics and service levels.

• *Federation and sustainability*: upgradeable to incorporate future enhancements and additional features. Also allow removal of features that are not requested. This enables interworking across domains.

One interpretation of this is to consider virtualisation as a separation between network operator and service provider²². In that case, a provider may lease a set of virtual resource slices. Then a set of services can be realized within these slices applying the relevant protocols and mechanisms. Virtualisation also brings a number of additional challenges, like to how to apply these principles for servers and gateways.

Some see the co-called *Cloud computing* as one component in the virtualization. Basic motivation for the Cloud computing (as for the virtualization) are to:

- Make it easy for users to try and buy services on-line
- Enable simple and automated on-line provisioning
- Make the service catalogue and its architecture, pricing and performance transparent
- Offer standardised configurable services and APIs
- Enable users to self-serve and peer support
- Evolve the service iteratively based on actual user behaviour data
- Engineer for the best practice, lowest operating costs
- Provide seamless scalability and resiliency

Critics, however voice concerns related to aspects like application migration, support of SLAs, data security and privacy, usage metering and billing, integration, software licensing, the lack of standards and the dangers of lock-in to cloud providers.

Overlay network technology can also be seen as a virtualization solution. A main idea is to allow constructing a virtual network on an upper layer to conceal the diversity or limitations of lower layers. An overlay network is formed by a set of applications on top of the network layer. This is typically done by defining a set of end-nodes (hosts) that composes a set of overlay routing nodes.

An overlay network has two main advantages:

- It enables diverse network service to be quickly deployed without restricted by limitations of lower layers. Examples are content duplications, distribution, discover, sharing.
- It allows experimenting on new network and service concepts without changing the underlying physical network. This may imply that lab scale set ups can be scaled across the globe.

The overall complexity, however, has to be considered. For example, a single Internet backbone router configuration file can consist of more than 10 000 command lines. A recent IT study survey claimed that 80 % of the IT budget in enterprises is devoted to maintain just the status quo. In spite of this, configuration errors account for more than 60 % of network down time. So, the more configuration options that are possible, the more likely it is that mistakes are made.

²² This can be related to the discussion of functional separation that has been on-going at different regulatory levels, e.g. in Europe.

8.4. Internet Protocol version 6

Deployment of IP version 6 has a rather slow progress. The main motivation seems to be the *depletion of the IP version 4 address space*. There are estimates that, continuing the latest trends, ICANN may be out of IPv4 addresses around middle of year 2011. Correspondingly, Regional Internet Registries have no IPv4 addresses to allocate from middle of year 2012.

Another challenge with the original addressing regime is that *mobility was not considered*. Today, Internet addresses are used to convey a weak from of identity as well as location. Sine the current IP address captures the notion of identity, it is not possible to change the IP address in a on-going communication. This implies that a terminal cannot change its address as it changes its location. Future Internet must have a dynamic address reassignment support or other similar techniques allowing the modification of the address without session interruption.

IPv6 has a *vast address space*; 128 bits addresses compared with 32 bits for IPv4, see IP packet header formats in Figure 15. Some additional key features of IPv6 are:

- Mandatory support for network layer security; IPsec is mandatory
- Simplified IP header the number of fields is reduced compared with IPv4. This should reduce the processing needed at intermediate routers.
- Presence of flow label can be utilised, for example, to provide certain service levels for selected applications

IP version 4			IP version 6						
Version IHL	Type of Service	Total Length		Version	Version Traffic class Flow label				
Identif	ication	Flags	Fra	igment offsets		Payload Length		Next header	Hop limit
Time To Live	Protocol		Header of	hecksum	Source address				
Source address									
Destination address									
	Options		Padding						
= fields not kept in IPv6					Destinatio	on address			

• Jumbograms – optional support for packets as large as 4 Gbyte.

Figure 15 Packet header formats for IP version 4 (left) and IP version 6 (right)

Managing IP address spaces

Already in the beginning of the 1990s one recognized that the limited address space of IPv4 would become a challenge. Four solutions were then proposed:

- Classless Inter-Domain Routing (CIDR) that allowed allocation of address prefixes as needed (not restricted to Class A, B and C address structures).
- Dynamic Host Configuration Protocol (DHCP) for allocating IP addresses dynamically from a common address pool. This assumes that not all devices are online at the same time.

- Private IP addresses for use when there was no need to communicate outside a private network.
- Network Address Translation (NAT) enabling a set of private addresses to be represented by a smaller set of public addresses.

In addition, the Internet Assigned Numbers Authority (IANA) introduced rules for assigning IPv4 address prefixes (from [Juni09]):

- Networks assigned IPv4 addresses earlier than November 1993 could not receive new allocations until they had used their previously assigned addresses.
- Networks requesting new address allocations had to justify their needs, both in terms of public communication needs and number of devices to be supported.
- Networks would be assigned just enough address space, i.e. in smaller steps.

Although these rules worked well through the 1990s, the demands placed pressure on the IPv4 already by the year 2000. These demands came from:

- The growth in the Internet-based applications, including games, information sources and business systems
- The shift of services from classical networks, such as voice onto the Internet
- Dramatic increase in number of IP devices, including mobile handsets
- Expanding economies in populous countries such as China, India, Russia and Brazil.
- Burgeoning consumer electronics industries that exploit new ways of applying Internet.
- IP-enables sensor and applications for industry, military and medical areas.

All these factors have accelerated the depletion of the remaining IPv4 address space. By October 2008 about 15 % of the IPv4 addresses remained. There are estimates that address pools on global and regional levels will not have any more addresses to allocate in the range end 2010 till end 2012.²³

The huge address space of IPv6 provides a better importunity to support continued growth of devices and services. However, IPv6 has several other advantages over IPv4. These include improved mobility, potentially better multicast capabilities, easier extensibility, more efficient packet processing and cleaner security capabilities.

The speed of IPv6 deployments seems to be rather slow, though. As per November 2008, 3.9 % of the Autonomous Systems(AS)/networks run IPv6. That is, in total there were 20 090 Ases, and 1 160 that run IPv6. Only 47 were running IPv6 only (i.e. no support for IPv4).²⁴

Some IPv6 initiatives

Summer Olympics in 2008 is notable event. All network operations were conduced using IPv6 for the Beijing games. This provided the largest public showcase for IPv6 since its inception. Some applications were lighting control, security cameras and sensors in taxies to ease traffic congestion.

²³ See <u>www.potaroo.net/tools/ipv4/</u> for a running counter on available IPv4 addresses.

²⁴ See <u>http://bgp.he.net/ipv6-progress-report.cgi</u> for updated progress report regarding deployment of IPv6.

In addition to the Summer Olympics, the China Next-Generation Internet (CNGI) project is promoting IPv6. This project is government-led and –funded. A motivation is the population size and growth of Chinese economy. More and more people are getting online. At end of 2008 there are approximately 654 million IPv4 addresses not allocate, while the population of the China is about 1.3 billion.

Japan was among the first countries to initiate an IPv6 (the e-Japan) initiative supported by the government. Some activities are the WIDE project (protocol stacks, system and applications), TAHI (conformance and interoperability) and NTT/Verio (IPv6 deployment). A main driver is the needs from the consumer electronics industries. These produce devices like game systems, cameras and mobile handsets.

South Korea is similar to Japan in its push for IPv6. The government leadership and financial support is evident. This is partly motivated by the huge consumer electronics manufactures.

US government agents are mandated to adopt IPv6. This began with the Department of Defence in 2003. Any shortage of IPv4 addresses is not considered the main driver due to the huge address reserve. Motivation is rather the expected improvements regarding mobile capabilities, multicast features and plug-and-play addressing to improve peer-to-peer and support mobile ad-hoc networks.

For Europe a major deriver seems to be the number of mobile devices. More than 30 research and development projects have been funded. According to the i2010 initiative, EU plans for 25 % of European Internet users to access the Internet utilising IPv6 by year 2010.

European Commission has a strategy similar to the US government, promoting adoption of IPv6 by encouraging member states to state requirements when purchasing equipment and services.

Migration from IPv4 to IPv6

Moving from IPv4 to IPv6 several mechanisms have been defined:

- Dual stacks: a device to support both IPv4 and IPv6on the same interface. Hence, the interface has both an IPv4 and an IPv6 address. The DNS could provide feedback on whether IPv4 or IPv6 should be used towards a server/device. Between routers, the routing protocols need to exchange both IPv4 and IPv6 status.
- Tunnelling: Transporting IP packets of one protocol across part of the network that does only support the other protocol version. This can for example be used to interconnect "islands of IPv6 domains". Tunnels can be manually or automatically set up. Multi-Protocol Label Switching (MPLS) is supported by most service providers' networks and can be utilized when designing tunnels. For automatic tunnel set up an authoritative server (e.g. a tunnel broker) or IPv4 addresses embedded in IPv6 addresses (e.g. 6to4 approach) can be used.
- Translators: Replacing packet headers. The Network Address Translation with Protocol Translation (NAT-PT) is a common implementation. This is also used for security reasons between domains. Packets in both directions usually have to pass through the same NAT-PT node.

Dual stacks are considered the simplest manner, and the translators the most complex one.

8.5. Routing

Routing is used for exchanging information on where to forward traffic. Routing protocols are applied to carry this information. Different routing protocols are used within an administrative

domain and between administrative domains. One argument for this is that less information is exchanged between administrative domains not to reveal internal information.

Several persons raise concerns regarding short-comings in the routing protocols commonly applied. It is, however, not easy to balance the comprehensive list of all requirements such protocols should comply with and the simplicity of implementing these protocols.

The Border Gateway Protocol (BGP) is very popular between administrative domains. Some short-comings of BGP are:

- Sacrifices speed of convergence in the interests of scalability; routing tables expand in part because IP addresses have limited geographical relevance, faster converging protocols like Open Shortest Path First (OSPF) cannot operate on the scale currently required for inter-domain routing.
- The fact that IP addresses have limited geographical relevance leads to routing table expansion. Non-geographic attribution of addresses can lead to anomalies with prefixbased routing like the non-identification of failed sub-networks and creation of routing loops.
- Troubleshooting is hard; while BGP works well most of the time, when failures are experiences the cause of the faults are often very difficult to location.
- Slight modifications to local routing (and unintended mis-configuration) can have unpredictable impacts at remote parts of the Internet.
- The distributed nature of the protocol makes it challenging to have a network-wide view of the control plane.
- Routing is vulnerable to attacks; security enhancements have not been implemented.
- BGP only proposes one "best" route to any destination leading to vulnerability to faults and attacks and lack of availably during convergence.
- Traffic engineering is very difficult to perform using the tools of preferred paths.
- Use of multi-homing amplifies growth in routing table size and load sharing remains difficult.
- Users have limited or no control over path choice for incoming and outgoing traffic; user control would be beneficial for multi-homing load balancing and also for blocking unwanted traffic; users may also wish to use or avoid a particular transit administrative domain.
- Use of overlays as a user-driven solution for traffic engineering can bring instability (as traffic aggregates are switched periodically depending on path performance).

These observations could be used as basis for improving routing in the future Iternet. Some ideas may:

- *Use of virtualisation* with routing protocols specifically designed for each virtual network (e.g. security for banking applications, fast convergence preferred for real-time services, etc.)
- Enabling the network to *offer multiple route choices* and the user to exploit the different paths. This has multiple advantages: i) enhanced protection from attacks since all paths would need to be compromised simultaneously to provoke unavailability, ii) better end-to-end performance by allowing user to choose best path

or use several at once, iii) reduced dependency on fast convergence when network status changes.

- Introducing a *geographically based addressing system* (this was part of the initial Intern design). One proposition is to create "atomic domains" with addresses of the form AD:LID with AD being the atomic domain number and LID being a local identifier relevant only within the AD.
- Creation of a routing control platform allowing *co-ordinated routing decisions*. This would collect additional data beyond reachability. In result informed path choice for enhanced security or QoS would be allowed, for example. This routing control platform would also allow the implementation of standardised inter-domain policy verification and exchange system. It would also help providers to avoid routing policy deployments leading to non-debuggable, inherently instable multi-AS constellations.
- Creation of a *monitoring scheme* allowing ISPs and users to visualise network performance and availability status propositions exist to exploit end user view point in a peer-to-peer structure.

8.6. Transport protocol

The Transport Control Protocol (TCP) was implemented at the same time as the Internet Protocol. It basic behaviour is that the transfer rate is stepwise increased until a packet is lost. Then, the transfer rate is decreased (in a larger step). In effect, the transfer rate behaves like a saw teeth pattern.

The objective is that the *applications back off in case congestion is experienced*. This is to *prevent a major traffic overload*. This behaviour may work for adaptable applications such as transfers of objects/files. On the other hand, other applications may not adapt that easily in case fixed bit rates are applied. Examples today are voice and video conversations.

An option to adapting the transfer rate is to keep all flow sending at maximal rates and then deal with packet losses by error coding. The overall objective is still to *ensure high throughput*. According to [GENI07], the latter may have the following advantages:

- Efficiency: When terminals send packets as fast as possible, all available network resources between source and destination are utilized. Furthermore, because links are typically dimensioned with major margins, any additional capacity is immediately consumed.
- Simplicity: Because packet drops (and re-ordering) are inconsequential, routers can be considerably simplified. For instance, routers no longer need to buffer packets to avoid packet loss, dispensing with the need for expensive and power-hungry line card memory.
- Stability: The approach transforms the sender's main tasks from adjusting its transmission rate to selecting an appropriate encoding. Unlike the former, however, the latter has no impact on other flows. Hence, in this approach, traffic demands may be fundamentally more stable than with traditional congestion control algorithms where the frequent rate variations may influence the behaviour of other flows sharing a bottleneck.
- *Robustness*: Using this approach, terminals are forced to cope with high levels of loss and reordering in steady state. As a result, the network can drop, reorder, or duplicate packets without severely impacting flow throughput. Also, due to the flow isolation

the terminals of one flow need to not consider the congestion due to others when transmitting so greedy parties cannot manipulate the network against each other.

This has not been proven in a large scale network with ranges of traffic mixtures as found in Internet. The aspects listed above, however, are valid for any transport protocol behaviour.

8.7. Machines that communicate

A modern society is quite equipped with devices of different kinds. These are used for various purposes, such as game consoles, TV sets, house warming, power meter readers. The list is steadily getting longer, In fact, *communicating devices* are seen within several application areas:

- E-commerce: devices for carrying out e-commerce transactions, like point-of-sale terminals on busses, in shops.
- Workflow management: registration of work flow tasks, e.g. within health care.
- Process control: monitoring and control of industrial equipment, production lines.
- Asset management: tracking of assets like production equipment, vehicle, containers, etc. Includes following assets during the supply chain.
- Sensoring and monitoring: observing a set of parameters, like temperature, humidity, power consumption, etc.
- Security: intrusion detection and alerts

Only a minor part of the processors manufactured today are found in typical computers. More and more are finding their way into tools and other consumer electronics. Still more are introduced into vehicles and various production units. These are used for logging, analysing, reporting and allowing traceability. Two general arguments are to *increase productivity and to improve safety*.

Some topics of research include *resource management, security of information, network design and identifiers for devices.*

One application area is the in-vehicle communication solutions. The "eCall" initiative launched by the European Union belongs to this area. When a car is equipped with eCall and senses a defined event, it automatically calls the emergency centre and transmits a set of data. The data may for example include the exact geographical location. Knowing the exact location of the crash site, it has been estimated that response time of the emergency services will be reduced by 50 % in rural and 40 % in urban areas. In result, this has been estimated to allow saving up to 2 500 lives each year in the European Union.

The economic losses caused by road accidents within EU are estimated to more than \notin 160 billion per year. Equipping all cars with eCall, savings up to \notin 26 billion could be saved (ca 16 %). The Norwegian government has committed to eCall, and so have several other European governments.

There may also be governmental initiatives for introducing more capabilities into consumer electronics. For example US government is expected to work on a proposal for mandating GPS equipment in mobile phones. This allows locating a phone when an emergency call is made. This has been taken further by US senator Ernest Hollings who has proposed to mandate processing in all consumer electronics that is produced or sold in USA (not approved so far).

Nanotechnology is a key enabler for miniaturizing the devices. Nanotechnology refers to control of small scale objects – typically on the scale of 100 nanometres. This provides opportunities for several areas, such as the integration of ICT, molecular biology and medicine. Other practical solutions are cloths adapting to the environment and body needs, body sensors and "machines" (e.g. automatic medicine dosing).

Radio Frequency Identification (RFID) is also seen as a key enabler. RFID may find a number of application areas. RFID is a method for collecting and storing data by exchanging/reading data on short hold radio. An RFID chip can be identified and tracked wireless. The chips can be integrated into cloths, payment devices, shoes, ID cards, animals and other objects. It has already been implemented in running shoes (Nike) and various payment devices (e.g. for buying bus tickets).

Another effect of the rapidly growing electronic gadgets is the power consumption. The International Energy Agency has estimated that energy consumed by information and communication technologies and consumer electronic products will double by 2022, and triple by 2030. That is, in case no counter-measures are taken.

8.8. Security and trust

Static port number simplifies security attacks

Today, Internet-based services mostly use "*well-known ports*", that is port numbers that are statically assigned to each application. These port numbers are implicitly included in each packet as protocol types. Hence, this allows the identification of the application being used.

Since these numbers are statically assigned, an attacker can easily launch an attack against an application on a given point, just by combining a host address with the port number, and using that destination as the target of an attack.

An alternative may be to design a new mechanism for service rendezvous, and to use random port numbers to identify connections. This change, combined with an increase in the range of port numbers, would essentially eliminate the value of the attack known as port scanning. It would also provide more privacy from anyone observing the network traffic.

Overall security design

In the current Internet there is now way to reason about the properties of terminals and hosts. One is not able to assure that traffic emanating from a given terminal is really valid. Hence, there is no way to reason about the properties of services provided.

There are *fundamental missing items for providing an overall security design*. As identified in [GENI07], such a security design should include:

- Containment the ability to limit the collateral damage caused by security compromises
- Accountability being able to identify a responsible component of the system for any action as well as the ability for that component to demonstrate deniability for any ill action it did not actually commit.
- *Cryptographically verifiable* verify all network addresses and names from their public keys.

As stated in [EC97/21] the security area has poor visibility of return. That is, in case the security means work, no events should be experienced. This may result in risks being underestimated and little focus on developing a security culture.

In case something happens and you are not protected, one should think that a lesson is learnt. This seems to only stay in one's mind for a limited time, though. The European Economic and Social committee supports that a new strategy should be formed to increase network and information security against attacks and intrusion, which have no geographical boundaries. It further states that security in the information society is a fundamental issue in terms of ensuring reliable communication networks and services inspiring confidence. These are key factors in economic and social development.

Can you trust a web page?

Internet users face growing risks in every interaction. This includes browsing, e-mail, ecommerce and entertainment as well as others. *Identity theft* is widespread, and there are more web sites than ever used to distribute *malware*. *Spam* volumes steadily increases. In addition, Internet continues as a prime vehicle for distribution *illegal and harmful content*. These threats erode users' trust and devastate their experience. The threats also imply costs in the range of billions of dollars every year.

Regulators, policy maker, users and the public are all applying increasing pressure to "clean up the Net", while still not violating users' privacy. Five key threats that face Internet users are:

- Identify theft attacks
- Illegal and abusive content
- Malicious content
- Spam
- Denial of service attacks

One way of stealing a user session is to insert *fake records in the DNS*. Nearly all Internet applications rely on DNS. Inserting a fake record may hijack sessions from a domain to a false domain. This could include e-mail, e-commerce, browsing and even social networks. In result, users believing that they are providing information to a legal web site in fact provide the information to a fake web site. Main threats against DNS are depicted in Figure 16. Some of these threats can be prevented by protocols, although most of the left side phenomena cannot be addressed by these means.

Service providers world wide are under pressure by regulators seeking to "clean up" the Internet to protect their users from *illegal and inappropriate content* such as images of child abuse. The scope and seriousness of this problem is forcing action by policy makers and law enforcement bodies.

In essence, the web has become a main method for distributing malicious content. Only by clicking on an inappropriate URL in an e-mail or web page, users can get infected or tricked into disclosing private information (also called *phishing*). Stopping these web-based threats is incredibly difficult as malware is stealthier, originates from more sources and is changing their characteristics faster than ever.

Spam volumes continue to set new records. Anti-spam actors state that there are more than 160 billion spam messages every day, accounting for ca 97 % of all e-mails. In effect, spam is a serious nuisance to users and a costly burden for providers. It is also an important channel for distributing malware and phishing attacks. Almost 90 % of the spam comes from "bots". A "bot" is referring to an infected lap-top or server with malware that is under the remote control of an attacker. Such infection can lead to consumer identity theft or dramatically degrade the user experience by impacting the performance of the laptop of server.



Figure 16 Security threats related to Domain Name Service (adapted from [ENIS08])

A growing number of business initiatives are related to web that include providing purchasing information on-line. Therefore, the crime and fraud related to this is also growing. Hackers may want to copy users' credentials for accessing on-line banking, government gateways, retail and other critical sites. Here they may have the opportunity to purchase items "on behalf" of the actual user, or use the credentials for other purposes.

Several hackers' attacks involve malicious web sites. These could be utilized either as are a vehicle for downloading malware onto the victim's computer when they visit the site, or by posing as a legitimate site. Users are typically enticed to go to these sites by sending a link in e-mail messages, by router poisoning or by corrupting a link in a page of a legitimate site.

Measures for protection include:

- web site certificates these have been around for several years and could be recognized by the icon in the browser window.
- in-browser protection such as highlighting certain suspicious parts in case of diverting to a different site.
- Web site reputation filters.

8.9. Personal cyber-experience

Surveys show that persons connected to Internet on-line devote more time to sophisticated, compelling, networked, and synthetic worlds. On one hand this might foster productivity. On the other hand, it may lead to addiction problems. The addiction phenomenon is seen today related to some games, virtual reality (e.g. Second Life) and gambling.

As an overall trend, communication via Internet will become an even more integral part of social existence compared with today. Hence, the human effect of this should be further understood. This is, however, part of the wider discussion. A richer communication pattern for individuals raises several issues such as:

- Ensuring availability of critical data, sensor inputs and control signals. Examples are personal health care and home automation.
- Tracking individuals and devices, e.g. for geo-fencing, locating lost devices and providing further routing guidance.
- Selective sharing of relevant data according to privacy policies. This could be access to location data, various content, identifiers.
- Forming virtual communities for communication among persons of similar interests.

Critical aspects are privacy, availability, identity handling and sharing of data.

For example, biometrical methods can be used to identify a person. This could be related to photos of the same individual. The most common biometric method is use of finger prints (e.g. when boarding planes and other access control systems).

Biometrical methods can also be applied for recognizing persons in a crowd as well as tracking biological material. Besides faces, other behaviour patterns could be analysed, such as way of walking, and way of moving in a room. For example, software is available for recognizing 500 - 1000 faces per second in a crowd ([NOU09:1]). This can allow automatic surveillance in public and private places and events. It is also stated that several air ports have installed such systems for detecting persons suspected for criminal behaviour.

Software and hardware related to digital video processing are falling rapidly in price. The high definition video capabilities open for similar biological recognition methods to enter the private sphere.

8.10. Privacy in view of Internet evolution

Utilising technical capabilities

The technical development allows a *lower threshold for collecting, storing and processing huge amount of data*. This threshold has become lower both in cost and complexity terms. As the unit storage cost continues to decrease, it becomes less expensive to collect a lot of data per event. This is compared with spending resources on sorting what data elements to delete before storing.

In consequence, we are entering a situation where little data disappears "by itself". Two growing concerns are: i) several data sources can be examined to *collect pieces of information* related to individuals, and, ii) *data that are outdated can be still available* to provide incorrect pictures of individuals.

Applying communication means it is quite easy to track individuals to find answers on:

- *where* are you? (geographical location)
- *when* are you there? (time estimates)
- *how* did you get there? (way of moving)
- *what* are you doing there? (way of behaving)

Regarding the first three toll road systems may collect information of whereabouts of cars carrying identities. There is a proposal to interconnect toll road systems with the European Economic Area (EEA). There are also proposals to install so-called black boxes in vehicles to track location, status of vehicle and behaviour. This could be to direct rescue teams in case of accidents, to follow criminals, to assist assurance settlements, and so forth. A major question is *who should own the logged data* in such a box and who should have access to the data.

Within the telecommunication area, there is a directive to be introduced requesting all service providers to store data regarding all electronic sessions. That is, description of time-of-day, who communicated, etc., not the content of the session itself. This information is to be stored from 6 months to 2 years (according to EC regulation, national authorities may decide upon exact time of storing). Main motivation is to ensure electronic trace that can assist when investigating and preventing criminal acts. Information shall be made available to proper national authorities. For example the police could ask to receive all information regarding a subscription.

Privacy threats

The amount of information exchanged electronically has increased dramatically. This includes mass media, e-commerce, eGovernance, e-mails, various web pages, etc. A main argument is the increased efficiency accompanying these solutions. However, awareness and requirements regarding encryption, security certifications and electronic signatures should be emphasised. These have to be complemented with routines regarding privacy. Several events have been reported such as patient records made available, students social security numbers been placed on open web pages, and so forth.

Particular threats mentioned in [NOU09:1] are:

- Malicious software (malware) on computers and laptops that listen-in (spyware) or compromise (e.g. introducing false evidence) or any other manners of crack privacy.
- Break-in and logging (hacking) include use of technical solutions and manipulation to get access to systems
- Identity theft often by malware of hacking.
- Cookies (that often also have legal motivation), can be used for tracking and information collections.
- Facebook/Google and other common web sites that "exchange" user information and statistics
- Systematic and illegal collection of name and e-mail address for marketing purposes (for directing spam).
- Software and equipment for collecting information and extracting selected data (e.g. about employees).
- Distribution of offending statements and pictures of third party.

In addition come means such as eavesdropping. Eavesdropping has typically been applied by police and military. However, equipment targeted for consumer market has now made its way to the shelves. Related to Internet, more software-oriented solutions are:

- Bugs, or features, introduce in IP routers to duplicate IP packets
- Software installed in laptops to record activity, such as keys pushed, activation of microphones and video cameras.
- Cookies and web buds that identifies specific users and collects tracking data by connecting references in e-mails and web pages.
- Private and public WLAN systems made open and poorly secured.

There are several initiatives regarding the so-called *privacy enhancing technologies*. The term privacy-enhancing technologies (PETs) refers to technical and organizational concepts that aim at protecting personal identity.

An individual's roles provide pieces of information

The reason for focusing on the identity is that privacy may not be that relevant for situations where individuals cannot be identified. *Every individual may play different roles* (see Figure 17). Therefore, it could be tedious to keep track over all characteristics and possible prevent that information about different roles can be collated.

It is also fundamental to make distinctions between what information that should be available related to which roles. For example, employers might have specific requirements, while health care, education systems, tax offices, and so forth, have other needs. In particular this is important as electronic exchange of information between different authorities and enterprises takes place. Then there are different phases of handling information as illustrated in Figure 18.



Figure 17 Relations between individuals, roles and representations in different systems (adapted from [NOU09:1])

There is discussion regarding which technologies to include in privacy-enhancing technologies. Some want to mainly address mechanisms for enabling anonym usage, support of pseudonyms and managing identities in general.

Mechanisms that are typically used are encryption, firewalls, anti virus, anti spyware, spam filters and web browsers that removes traces and cookies. These are mainly covering individual users' equipment and information.

Due to the "always connected" scheme, there is a trend that *private and professional lives of individuals are intermixed*. There is no longer clear separation between work and leisure time as the mobile and e-mail is always with you. This may also strengthen the expectation from employers that persons are continuously available. By electronic means it may also be possible to continue working from home or any other places outside the office. On the other hand, employees may also use employers' equipment for private affairs, such as copying machine, e-mail, mobile phones, etc. This has motivated the initiatives to surveying

employees' activities with respect to which e-mails are sent, which web pages are visited, what is stored on the laptops, etc.



Figure 18 Phases from registration to usage (adapted from [NOU09:1])

Public Key Infrastructure (PKI)

There has been work on encryption related to Internet for some time. Most of the equipment, including mobile phones, memory sticks, hardware drives, can be configured for automatic encrypting everything that is stored.

Common *awareness and knowledge of usage seem to be lagging* though. In particular, this is observed related to exchange of e-mails. There is also lacking an infrastructure for exchange and authentication of public encrypting keys, also referred to as Public Key Infrastructure (PKI).

One of the key identity carriers in Norway is the *social security number* (11 digits). In case information of a person's social security number gets in the wrong hands, several events have taken place regarding challenges which that person has to face. Such episodes include rerouting postal service, application for credit cards, and so forth. Several events on placing social security numbers publicly available on web have been reported.

In order to raise the threshold for misusing this information, some have proposed to introduce a data base for linking identifiable indicators with pseudonyms. This could take place in an automatic manner by a trusted party. This is sometimes referred to as an *identity protector*. Then, of course, this data system would likely be a tempting place for launching security attacks.

Personal information on stray and misused

A result of media and content being digitalised is that individuals may publish and distribute major parts of the private sphere. That is what typically earlier has been referred to as the private sphere. Examples include personal photos, family video recordings, messages to friends. Some parts of the publishing take place through social networks and use of means like blogs and electronic photo albums. A quick evaluation of what is actually publicly

available make one wonder to what extent the persons are aware of the information can be viewed, and possibly misused in the next phase.

One simple example is the social network *patientslikeme.com* where some puts information on illnesses under full name, and even including description of family relations.

This raises the question on to what extent a "medium" or web site must protect individuals against harming themselves? Or any minors under a person's custody? This is not a trivial question. Clearly when others want to publish information of this type, as a rule, permissions from individuals should be obtained in advance.

For social networks, one finds that explicit agreements are accepted by users when signing in. This is often done by ticking a box under a lengthy description of legal conditions (also called click-wrap). Such agreements cannot violate national laws, however. In several cases a person signs off any rights including privacy rights. Hence, some question the legality of such agreements.

On a general level common courtesy and good ethics are regarded as valid for all areas in the society. Based on several events, it may seem that several people regards the Internet as less regulated when it is comes to express ones disrespect of other persons and public organisations. Several examples are found on blogs and home pages. Mobile phones with cameras have also make it quite easy record and transmit harassing messages. Such means may also challenge any clear separation between public and private spheres.

Media classes and levels of responsibilities

As presented in [NOU09:1] there are different classes of media and corresponding roles:

- *Edited media* having a responsible editor. The editor may be prosecuted for the content. In this category we find traditional newspapers, TV news, etc.
- *Post-edited media* having an editorial team reacting on inappropriate statements or contributions after these are posted/published. Reactions may be change or removal of contributions. For a post-edited media, privacy may be violated even though any statements are removed after some while. Digital newspapers (Internet-based news) belong to this category.
- Media collecting user information also referred to as Web 2.0. Some also call this a two-way media in the sense that users are also contributing to the media. Examples include Facebook, MySpace, Nettby, Blink, Underskog, YouTube, Flickr. General features of the Internet site are to facilitate publishing, search and visibility of the media.

It is often seen that the electronic media collect and store tracks of users25. For example Google stores information like IP address, search key *Facebook* is perhaps the most known social network site today. It was established in 2004 and has grown to more 100 million users. A personal profile is stored for every user. This profile contains personal information (some of the information needs special concession to store according to Norwegian regulation). Users may see Facebook as a means for publishing text, photos, videos, etc. In addition Facebook runs routines surveying users' change or status and communication. For example, automatic messages can be generated informing "Facebook friends" about a user's change of status, purchase, etc (after the relevant user accepts that the message is sent).

²⁵ A survey by the company Sophos revealed that more then known or unknown, as their Facebook friend.

words and results. This may be stored in 2 years, although the IP address has to be made anonymous after 9 months. Such information can be used for tailoring commercials, sold as "business intelligence" (usage statistics), and so forth. Information collected from Facebook would also have value for targeting advertisements.

There is a discussion whether enterprises located outside the European Economic Area (EEA) have to comply with Norwegian legislation as long as users and terminals/laptops are located within EEA. For example, in the case of Facebook, individual user's laptop is still located at the same place as each user is. In particular this could be valid when Internet sites use cookies on the user's laptop.

- User-published media allowing a user to publish any material such as use of home page or blog (abbreviation of web log). Privacy concerns could be challenged when material involving other persons is published.
- *Media for private sphere* including means for communicating with addressed persons. Typical examples are e-mails, messages and phone calls. This might not be that straight forward. However, as an e-mail address list can involve several thousands of receivers, is may be a efficient distribution.

When peer-to-peer techniques are applied, content can be shared among a group of users. This may also happen in a great scale, involving many machines and users. Most common use of peer-to-peer to day is sharing of movies and music.

Traditional broadcasters have also started to use the peer-to-peer techniques to distribute content. BBC and NRK are only two examples.

Roles in media/information distribution

Different roles for media distribution are as, see Figure 19:

- Original author/source
- Editor
- Publisher
- Web site owner
- Information host
- Network operator/information carrier
- Receiver/reader/viewer
- Subject with respect to privacy concern, e.g. person described or depicted



Figure 19 Roles related to different media and content (adapted from [NOU09:1])

The discussion regarding anonymity goes back several decennia. In year 1771 hidden identity of the author was accepted. However, it was also implied that a *responsible subject* somehow should be identified. Hence, every printed item must give name of either author or any other person that is responsible for its content.

It is still unclear to what extent an editor is responsible for other media than print and broadcast.

Balancing privacy and freedom of speech

When it comes to limiting other's rights to publish material, some may refer to the Norwegian constitution § 100. This is described by the *freedom of speech*. There is no regulation on the same level regarding privacy.

Privacy is dealt with through the European Convention on Human Rights article 8: *a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society"*²⁶.

In some context public attention and descriptions must be accepted. For example, when a person and the relevant event/subject are considered to be of so-called *public interest*.

Three categories of "mis-behaviour" are:

- privacy and integrity discrediting
- breaking intelligent property rights
- damaging and illegal material

An industry standard exists for marking web pages (Robot Exclusion Protocol) so the pages can be recognized by search and archive engines. Most commercial players, such as Google, respect these principles. In case an owner has tagged the page as non-searchable according to this standard, Google will not present the page as part of the search result.

Google does also provide a service to remove web pages from cache and indexes that have been deleted from public available web sites. Response times are typically 48 hours.

However, The National Library of Norway has decided not to respect such tagging of web pages. According to the Norwegian Privacy Commission, this should be resolved, including how web pages could be removed from the library in case they are considered offending or illegal.

The Norwegian Privacy Commission recommends the following principles regarding media and privacy:

- Every media may have a responsible editor. In case a responsible editor is not appointed, another responsible legal subject has to be defined.
- A responsible editor may not exclude parts of the media from area of the responsibility.
- Anonymity should be protected by legal concerns only when there is a responsible editor.
- A media without a responsible editor must have another responsible subject. Postediting may exempt the responsible subject from legal prosecution when relevant

²⁶ Ref. http://en.wikipedia.org/wiki/European_Convention_on_Human_Rights#Article_8_-_privacy

content is removed as soon as this is brought to the attention of the responsible subject.

• Every media must clearly state whether or not it has a responsible editor.

A survey in Norway reveals that the population is not critical to government and enterprise collecting and using information about individuals. One argument is that most persons have little to hide, and see these means motivated by catching criminals. There seems to be a difference among populations in countries recently been through wars and democracy processes, though. As the population in those countries have an inherent scepticism towards government and enterprises' use of such data.

Recently several incidents of harassments have also been observed. Commonly Internet and mobile phones are involved. Examples are publishing negative statements about a person, placing non-respectable photos on web sites and sending messages. Certain social networks, such as Facebook may allow that groups are formed with special interest to express anger, hate or other negative feelings about others.

One challenge with all these is the *irreversibility*; it could be quite difficult to

As ICT enters the hospital and health care arena, there are various proposals on how to increase the efficiency. An average patient record at Akershus University Hospital is about 120 pages. For each hospital bed there are about 12 patients (and patient records) per year. Then, a hospital with 500 beds generates about 720 000 pages of patient records annually.

A patient may also carry this information by use of memory sticks or other means. The information may then be readily available for health care personnel not having access to a central patient record store, e.g. during travelling.

To improve the handling of these records, in May 2009 there was a suggestion by some politicians to implement a common patient record system that could be available for anyone working in the health care sector. Arguments are to make the information swiftly accessible, updated and post-processed for statistics.

remove all traces of such activity. Another challenge is that anyone excluded from publishing such material could simply set up a new account and continue in the same manner.

The Norwegian law for electronic commerce describes limitations of responsibility for provider of storage in paragraph 18. The general principle seems to be that the information host can not be punished when illegal information is removed as soon as possible after being informed about its status. However, in case the information host acts on behalf of the information provider/editor the case is different.

Similarly paragraph 17 regulates liability regarding interim storing of information. A player providing interim storage (e.g. caching) is not legally responsible unless the illegal information is kept or adapted after being informed about its status. This also implies that the information must be deleted after the player is informed that the original source is deleted.

Proper means are available for keeping logs of who access records of individuals, preventing unauthorized accesses, encrypting sensitive information, and so forth. This is motivated by maintaining privacy concerns Commonly, however, the human factor for such schemes is the weak link as every person involved has to obey rules for printing and distributing information.

When conducting research based on statistics and anonyms records, there are special concerns when the population is quite small. For those cases, individuals might be recognized even though all identities have been removed. This could be done based on other characteristics such as age, family situation, income, etc.

- Several challenges related to today's Internet reveal opportunities of different types.
- Users have embraced several of the applications made available in huge volumes.
- Several areas have not been studied by national initiatives to identify the needs for initiatives and corresponding opportunities.

9. Selected market perspectives

A number of aspects are inter-related regarding the evolution of future Internet. One example is depicted in Figure 20. In this Chapter only certain issues are described in some detail.



Figure **20** Examples for drivers and dependencies related to evolution of future Internet (based on [Haus09])

9.1. General market trends

Several trends have been evident for more than a decade:

- Convergence: on different areas; networks, terminal, market players.
- Changing organisation structures following from alliances, mergers, dynamic relations, etc.
- Consolidation of market actors, although this is a trend that varies on different areas and re-happens at irregular intervals
- Internationalisation and globalisation through entrance of larger multinational corporates.

In particular the convergence trend is strong and provides both opportunities and challenges to market actors. Different areas of convergence can be:

- Network convergence: Same network and infrastructure is used for all service types and distribution of content. More networks can also be utilized for interactive user communication (for example broadcasting networks opens for voice services). Deployment of new infrastructure increases available capacity, in particular on the access sides. This also inspires for continuing lower prices.
- *Service convergence*: Services can integrate several traditional media types (e.g. voice, video, text). The services are increasingly of interactive nature that opens for contribution service concepts (e.g. so-called Web 2.0 solutions). Same services can be offered on more infrastructures and be consumed on different terminal types.

- *Terminal convergence*: Being a result of digitalisation, more terminals can handle different media types at the same time. This opens for real multi-media services. Increasing processing and memory capacity enables more service consumption and storage of content.
- *Market convergence*: Telecom has been associated with large scale gains. This fuels mergers and co-operation between market actors. Several actors are also operating in different countries. New market players are also entering the telecom and Internet arena, utilising these as marketing channels, sales channels, etc.

9.2. General societal trends

The following summarises some of the general societal trends.

Ageing population. In most of Western world, as well as in several non-Western countries, the next decades will experience an aging population. This may imply many consequences in the society, fewer hands to provide for more people being the most fundamental. Also, senior citizens are among the wealthier, so there will be an upward shift in purchasing power. An aging population will also contribute to mobility in population, as there will be more demand for qualified work stock in regions with aging population, such demands can be satisfied by immigration from regions with other demographic balances or regions that are less wealthy.

Environmental changes. Recent investigations from UN bodies illustrate the likelihood that further environmental changes are expected. The full impact may follow during several decades. Implications on economy will be noticeable. Actual effects to be seen depend on the actions agreed in the global community. However, migration pressure seems likely as well as general restrictions on travel and fuel consumption in general.

Multi-cultural societies. There is already a trend in several regions towards multi-cultural societies. Important factors contributing are i) diminishing barriers for work mobility across national boundaries in some regions, ii) refugees due to wars and disasters, and, iii) the general difference in wealth between different regions.

Changes in family patterns. In several regions one may observe changes in the traditional family patterns. There are several causes for this, such as change in economic basis, e.g. industrialisation. But also increased strength and organisation of central governments (e.g. formation of general social services), increased wealth and literacy, and improvement of women's position in the society pull in that direction.

Globalisation. In many sectors in business and industry we observe a diminishing importance of national border and distance. Operations are established where conditions are favourable, e.g. due to labour costs, knowledge, political stability and other factors. A consequence is that dominance and importance of the English language will increase. The general requirement to communicate will increase as well.

Organised crime and terrorism. Both organised crime and terrorism are seeking to utilize opportunities from new technologies and service in order to achieve goals. Then, there will be a race between these forces and the counter-forces of the society. Measures to limit criminal activities may impose important guidelines and restrictions for other activities in the society, including information, communication, travel and finance.

Increased wealth, emerging economies. Many regions in the work experience strong economic growth on the longer run. For certain regions, such as Western Europe and USA,

this development has been on-going for several decades²⁷. In other regions such as Asia Pacific and Eastern Europe, the last development cycle has a more recent history. Such wealth increase has strong impacts on other societal developments such as education demand for goods and service and travel habits. In order to uphold the growth, there is persistent demand to increase efficiency of the processes of commerce, production and administration of in the society.

Main contributing field	Specific contribution				
Energy	Electrical power conservation of new generation network				
	Energy conservation of societal systems				
Environment	Prediction, detection and reporting of environmental pollution				
	Detection of environmental changes				
Disaster	Prediction, detection and reporting of disasters				
	Evacuation and shelter guidance				
	Verification of safety and disaster conditions				
	Data protection				
Medical care	Health care management				
	Medical history management				
	Medical care consultation				
	Telemedicine and telesurgery				
Food	Increase in food self-sufficiency rate				
	Guarantee of food safety				
Security	Secure network				
	Crime prevention				
	Accident prevention				
Rural and urban disparity	Expansion of employment				
	Information ad knowledge sharing				
Low birth rate and aging population	Health maintenance and promotion				
	Support for nursing care				
Globalization	Global migration and communication support				
	Diversity support				

Table 2 Contribution from Internet on certain societal areas (based on [AKAR08])

The so-called *digital natives* (or Net generation), are those born after 1980 and growing up with the Internet. These are commonly in the forefront for adapting technology in social

²⁷ Current finance crises in certain parts of the world is considered a temporary set back, as well as indication of the high growth of wealth these regions have been experienced.

communications. Preferences include staying connected, sharing, creating content, multitasking and assembling information into patterns. They are also referred to as the wisdom-ofcrowds generation that grew up rating peers, physical attributes, products and services.

Some societal areas and contributions from applying Internet are summarised in Table 2.

9.3. Example: Internet and the climate debate

It has been estimated that the ICT sector contributes to around 2 - 2.5 % of the global Greenhouse Gas (GHG) emissions ([Twat08]). This may grow due to increasing ICT usage in developing countries. On the global level the percentage of contribution to GHG is much less than its share of the Gross Domestic Product (GDP).

This is also related to the increasing need for powering Internet activities. An example is that about 4 % of world wide power consumption comes from computers. This is significantly higher for some countries, in particular in certain countries in Asia and Africa. As this fraction grows rapidly, more power efficient solutions must be introduced to prevent this factor becoming a major hurdle.

New models allow energy savings by different means:

- *Reducing the number of main centres*. There is a trend among the network operators to centralize some of the equipment into fewer and larger sites. For example BT states it its current 3 000 locations can be centralized into 100 -120 metropolitan node locations.
- *More tolerant climatic range specifications*. Typical temperature ranges have been between 5 to 40 degrees C. This is commonly widened to -5 to 45 degrees C. In effect this allows for fresh-air cooling rather than special air conditioning in more countries.
- *Specification of several power levels* (e.g. full, low-power and sleep) to reduce power need during low-traffic periods. One example is VDSL2 (ITU-T G.993.2) that has these three modes.
- *Improvement in hardware design* to increase the efficiency. For example, power amplifiers in mobile base stations have been improved, allowing for reduced power need. This also implies that less cooling is needed.

9.4. Some network-related trends

The following summarises some of the trends and corresponding impacts on the Internet.

Trade and commerce. A change is taking place in the relation between the single user and the commercial environment. This relation was previously characterised by companies using the Internet for visibility and advertisements. Even as this will continue, the Internet is developing to a more general market place where all sorts of transactions are taking place. Where such transactions were seen with specialised actors, the development is that also traditional companies and chains move their businesses to the network.

Service can be executed every where. As an intrinsic property of networking, computing can be carried out anywhere in principles. As a part of the globalisation trend, the commercial environment develops in the direction that such distribution is also relevant in practice. In particular, the importance of nation borders diminishes.

New sectors in the society employing the network. Use of Internet-based service diffuses in ever new parts of the society. A trend is that more and more of the relation between the citizen

and the government is handled over the Internet. We can foresee that health and societal services are also realized in a similar manner in the future.

Relations between companies. We should expect that more of the relations between companies, also formal relations, will be handled over the Internet, i.e. more business-to-business communication.

Emerging markets. There are several factor that are characteristics for emerging markets: lack of fixed infrastructure, large low average return per user segment, less knowledge of English language, lack of investment capital in the population even for small and moderate investments. Several markets do get access to Internet either by commercial players, governmental intervention or international aid programmes.

Diffusion of Internet and mobile. The diffusion of both Internet and mobile services in the society will increase in all markets. More factors contribute, two of which are the older and less knowledgeable part of the population is replaced by natural turnover by younger and Internet-competent segments and the increasing penetration in emerging economies.

Formation of communities. The Internet has developed to an arena for forming networked communities. This trend will strengthen as a general consequence of Internet diffusion and societal developments such as multi-cultural societies. According to [Pear09] more than two-thirds of the Internet users are visiting social network sites on a regular basis. In South Korea, more than 90 % of teens and almost half of the entire population are members of Cyworld; a mobile user visits Cyworld on average eleven times per day. In the USA 80 % of the young adults, 60 % of teens and 30 % of adults use social networks. In UK 90 % of teens spend time on social network sites.

Requirements on service levels. As Internet becomes an ever increasing part to the society infrastructure, requirements to performance will increase, at least for certain services. In particular robustness against failures will be important, but there will also be increase expectancy that networked services are available anywhere at any time, and that the infrastructure can provide transport quality in relation to the services employed.

9.5. Change of communication patterns

[Pear09] summarises the communication patterns and control as depicted in Figure 21. The four quadrants refer to different modes. The traditional mode is described by communication between two parties (e.g. telephony) offered by a provider. The upper right quadrant refers to applications such as MySpace, Befo, YouTube, Second Life and Facebook. Steadily more sites of this nature are emergeing. The "Gated communities" quadrant is illustrating portal (or app-stores) offered by players like Apple, Nokia and others.



Figure 21 Shifts in communication control and patterns (from [Pear09])

A general trend is the drift from the traditional services toward the shared social space. It may be that these complement each other as they fill different purposes.

Statistics from YouTube demonstrates the popularity of sharing content and other types of information. During March 2008, for example, 78.3 million videos were uploaded (about 150 000 new ones uploaded every day). On average watching a video clip takes 2 minutes and 46 seconds. This means that it would take ca 412 years to watch all the material at YouTube at that time.

Barriers to Internet could be categorized as shown in Figure 22. Drilling into numbers; the main arguments are affordability (as costs of subscription and terminals/devices), no interesting content/services, and not available service (mainly for rural areas). All these are under pressure from different players such as government (subsidizing), operators (competition and gaining maturity and scale effect), various community (publishing even "long-tail" content and services), as well as others.



Figure **22** Sample barriers and potential response to further use of Internet (adapted from [Davi09])

9.6. Example: Peer-to-peer

Comparing a peer-to-peer (P2P) system with the (traditional) client-server system, the P2P is generally *more scalable, resilient and resource-efficient*. The P2P mechanisms allow opportunities also for established players as suggested by the European Broadcasting Union. On the other hand there are commonly rights issues that are attached with P2P distribution of content. In its original form, there is no operator-control of this distribution. Regulatory considerations such as data retention and security could therefore be challenging.

In a pure P2P system there are no dedicated servers as any terminal can act as a client or a server. Any terminal (peer) shares its resource with other terminals. In that respect the P2P network is an organized collection of virtual resources that can be transparently published, discovered and accessed by any peer/application. After downloading a file, the peer will announce the data shared within the P2P network.

The way peers are organized and data published varies from system to system. Once a peer obtains a file it automatically acts as a relay for that file. Hence, more popular files get replicated faster and can be downloaded in parallel from numerous locations. This is an
argument for P2P being more scalable and resilient than the traditional client – (centralized) server model.

The Norwegian public broadcasting company, NRK, has applied peer-to-peer mechanisms for distributing series such as *Nordkalotten365*. This has been done utilising BitTorrent and Miro. *BitTorrent* has commonly been used for sharing content. It distributes the load amongst the users by taking advantage of individual users' processing and storage capacities. Hence, the source/publisher can reach a wide audience at a low cost.

Miro downloads the files in advance. This allows distributions of full-screen high definition without hiccups or session breaks. As there commonly is a certain response time, Miro might be more adaptable for the TV viewers and not the interactive PC users.

When NRK applied these techniques, users were able to choose which clients to use for downloading the series. Measurements reported in [Jans08] say that 90 000 full downloads were estimated during a two month period. Each episode was 29 minutes long and presented in full HD resolution.

NRK estimated that the two month bill for their bandwidth would come to about USD 300 by using the peer-to-peer approach compared with about USD 8 000 for the direct download (server – client). It was also reported that viewers were getting short download times for the video files as the distribution was spread across thousands of users.

Some of the factors that may push broadcaster to consider Internet are:

- Users can access content from almost unlimited TV and radio stations.
- ISPs have started buying content and offer triple play services (some games in the Summer Olympics 2008 were provided by YouTube to certain parts of the world).
- Easier to enter market as the establishing and maintenance distribution costs are dramatically lower (and decreasing).
- Content owners have begun to broadcast directly to the users/customers. In fact the digital rights issues are orthogonal to the means of distributing the content.
- Young consumers prefer to use the Internet to access media.

Three non-technical aspects may be addressed (from [Liot08]):

• *Copyright*: being the property right that the law gives to authors to protect their creative and artistic works. Typically it allows them to restrain third parties from copying or otherwise exploiting such works. This goes back to the early 18th century when book publishers started lobbying national governments to protect their interests against the activity undertaken by copyists.

Digital technology for transporting data poses additional challenges on the copyright system as no degradation is implied. Under the Copyright Directive, the EU Member States must adopt adequate legal protection against any device primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of an effective technological measurers (watermarking, fingerprinting, encryption etc.). This aims at protecting copyright.

 Consumers' rights – fair use and privacy: including the right to reproduce, copy or otherwise use work for the purposes of teaching, conducting scientific research, expressing criticism or review, publishing by the process for public information. Persons would typically also expect to be able to play a music file in all their digital players and to be able to make and distribute copies for non-commercial purposes.

Most copyright law allows users to make some use of the copyright work without the prior permission of the copyright owner (so-called "fair dealing" or "fair use"). Many of the current solutions used to protect copyrighted material are based on the collection of large amounts of data. The European Data Protection Directive expressly provides that (among other obligations) data controllers have to implement appropriate technical and organizational measures to protect personal data against accidental loss, alteration, unauthorized disclosure in particular where the processing involved transmission of data over a network.

- *Data retention obligations*: impose regulatory obligations on service providers to retain data related to traffic, location and identification of users for a period (between six months and two years). Competent national authorities will have the right to access these data in specific cases, in accordance with national procedural laws. P2P systems case technical obstacles to the ability of operators to continuously track and retain such data as the flows go directly between users.
 - Internet, and its evolution, impacts several societal aspects and way of living.
 - Internet becomes an integrated part in more and more processes.
 - Communication behaviour and expectation is changing as a society gets accustomed to Internet and places additional expectations on service levels.

10. Governance of Internet aspects

10.1. Controlling technical evolution

The Internet Engineering Task Force (IETF) was created in 1986. This was initiated by a number of USA government agencies: DoD, Department of Energy, NASA, NSF. An objective was to supervise design and deployment of Internet protocols. From the beginning IETF was only open to USA government-funded researches.

Already in 1987 a number of industry representatives were invited. Then, within a few months, IETF was open to all interested persons. Now, each of the tri-annual meetings draws about 1000 - 1500 participants.

There are only *individual memberships of IETF*. There are no company or national memberships.

Documents are approved by so-called *rough consensus*. This implies that the opinion is

IETF (<u>www.ietf.org</u>) is an R&D forum to define, describe, review and discuss network protocols and mechanisms. The results are published as Requests For Comments (RFCs). The work is organized into working groups. Each of these groups is in charge of a specific problem and is supervised by two chairs.

Related working groups are put together into an area. An area is supervised by two area directors. Beginning of 2009 there were 8 areas and 120 working groups in IETF.

All area directors form the Internet Engineering Steering Group (IESG). The Internet Architecture Board (IAB) and the IESG ensure the coherence of the outcomes from IETF.

gauged by the chairs of the working group (or by IESG when relevant).

Since 1998 the responsibility for names and numbers has been allocated to the Internet Corporation for Assigned names and Number (ICANN). Responsibility for different parts of the address space is decentralized. Every nation has its own organisation for allocating domain names.

IP addresses are allocated to the Internet Service Providers, who achieves them from a Regional Internet Registry (RIR). This is related to the Internet Assigned Numbers Authority) that handles the operative work on allocating addresses. This is done by agreement with ICANN.

The Internet Society (ISOC) is an organization of enterprises and private persons. ISOC is behind the Internet Engineering Task Force (IETF) that works on various solutions for technical areas.

10.2. Global initiatives

The UN General Assembly decided in 2001 to hold a word summit on the information society. During the first phase it became clear that Internet governance is a controversial issue with polarised views. One of the views came from the private sector and the other from international organisations and civil society.

A Working Group on Internet Governance (WGIG) was founded. A report made by WGIG recognized that several stakeholders have interest in this topic. It defines the *multi-stakeholder governance* as "the development and application of Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".

The report goes on identifying the following public policy issues:

- Issues related to the infrastructure and the management of critical Internet resources administration of the DNS and IP addresses, administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multi-lingual aspects
- Issues related to the aspects concerning the use of the Internet spam, network security, Intellectual Property Rights (IPR) and cyber crime.
- Issues related to the development aspects of Internet governance, the capacity-building in developing countries in particular, since the Internet usage will increase in those countries.

Related to the first issue, WGIG considered that some actions should be necessary concerning the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is responsible for the management of critical Internet resources. This includes the coordination of allocation, assignment and base price setting for domain names and IP addresses, as well as operation and evolution of the domain name system's (DNS) root name server system.

After the initial work of WGIG, the Secretary General of the UN was invited to set up a new forum for multi-stakeholder policy dialogue. Hence, the Internet Governance Forum (IGF) was created.

10.3. Internet Governance – How to improve the present structure?

This section is authored by Willy Jensen²⁸

Increased political awareness for relevant public policy issues

The rapid development of Internet from academic circles, with academic language and technical complexity, has contributed to substantial lack of interest and competent understanding from politicians and to some extent also from bureaucrats. When then now Internet has become the most important infrastructure for economic, industrial and social development at global, regional, national and local level, public authorities were and to some extent still are unprepared.

The WSIS29 initiated by ITU30 in 1998 and carried through under UN auspices from 2002 to 2005 in two summits, in Geneva 2003 and then in Tunis 2005 with Internet Governance as the sole issue, made some politicians aware of the societal dependency of Internet and its applications. However, concern for the extreme complexity of the DNS31 and for the vulnerability of the technical systems for robust and stable operation, has been confused with the very different discussion on DoS32, distribution of unlawful content and IPR33 and piracy. The national jurisdiction is not equipped with competence or capacity and the international jurisdiction is even missing some basic, legal instruments.

²⁸ Willy Jensen, Director General, Norwegian Post and Telecommunication Authority

²⁹ WSIS: World Summit on the Information Society

³⁰ ITU: International Telecommunication Union

³¹ DNS: Domain Name System

³² DoS: Denial of Service

³³ IPR: Intellectual Property Rights

The public policy issues related to Internet and lawful usage could be classified in three categories:

- 1. Issues directly related to Internet stability and dependability.
 - security and reliability of the infrastructure (DNS operation, root server robustness, bankruptcy handling)
 - spam, including DoS attempts and transport of malware
- 2. Issues less directly related to Internet stability
 - content control, including cybercrime, political censorship, ISP³⁴ liability
 - trade, e-commerce, e-government and other essential application categories
 - consumer protection
 - data protection and privacy
 - IPR and piracy
 - competition issues
 - Internet penetration and usage, outreach, enhanced cooperation
- 3. Future development and challenges
 - introduction of new and improved technology like IPv6³⁵, IDN³⁶, NGN³⁷
 - increased production and dissemination of local content
 - expected growth of machine to machine communication requiring an ONS³⁸

All these are to some extent discussed in IGF39. The understanding and the analysis although always within the remit of the Internet user society, are in many instances adequate. However, the implementation power is of course insufficient. The public discussion in media, particularly the digital media, is to a large extent subject to uninformed enthusiasm for oversimplified solutions that quite often express elements of anarchy. This is provocatively the case in the recent debate on file sharing.

The Internet Governance dilemmas following WSIS

The political process of WSIS, including strong elements of foreign politics and regional economic development considerations gave an enormous lift in understanding and competence in this rather new policy sector. Unfortunately, this lift happened mainly within rather narrow circles. The documents from the summits in Geneva and Tunis are warmly recommended: The Geneva Declaration and Principles, The Geneva Plan of Action, The Tunis Commitment and The Tunis Agenda for the Information Society blend very high level diplomacy language with rather concrete objectives and strategy elements for a democratic Internet Governance structure based on transparency, openness, democratic representation, and accountability. The apparently great concept of multi-stakeholderism deserves special reflections.

The Tunis Agenda states in paragraph 61: We are convinced that there is a need to initiate, and reinforce, as appropriate, a transparent, democratic, and multilateral process, with the

³⁴ ISP: Internet Service provider

³⁵ IPv&: Internet Protocol version 6

³⁶ IDN: International Domain name system

³⁷ NGN: Next Generation Networks

³⁸ ONS: Object naming System

³⁹ IGF: Internet Governance Forum

participation of governments, private sector, civil society and international organizations, in their respective roles.

The WSIS process itself became a multi-stakeholder process, to the great surprise and joy of the "civil society" that, for the first time in a UN process, were allowed in at the tables together with governments and private sector. The key challenge, that never was resolved in the circles of ICANN40 and the associated operational management of Internet critical infrastructure, is the role of civil society. In these circles, this could be NGO41s, idealistic organizations like Human Rights and Freedom of Expression initiatives, but also Academia itself. It seems to me, particularly concerning the academics, many do not fully understand who they are, who they represent and who they are accountable to. While nobody questions the "technical" expertise and intellectual capacities of these academics, why they should be heard and consulted – a procedure common in the Nordic countries – many academics from other regions of the world, notably from the US enthusiastically mix this role with ambitions for operational decision powers in the Internet society including the ICANN realm.

Among many dilemmas in Internet Governance are these:

- 1. The multi-stakeholder concept implementation, specially the role of "civil society", is intriguing from an idealistic point of view, but does not add to operational efficiency and introduce democratic deficiencies.
- 2. "If it ain't broken, don't fix it" is usually a slogan preventing progress! On the other hand, there is some management wisdom in it. And it is of course of utmost importance not to allow "fixes" and changes to jeopardize the stability of the net.
- 3. The roles of governments and their public policy influence versus micro management incompetence has not been defined and is far from a suitable implementation. Since it seems that the UN track has failed, many believe that the GAC⁴² should be removed from the ICANN management structure, and that governments should take an oversight role developed through cooperation between USG⁴³, EU and other regional multilateral alliances.
- 4. ICANN has in fact global monopoly in management of DNS and further IDN and ONS. Although they often claim to be very liberal, open, transparent, etc., monopolies never provide nice solutions in the interest of users. The issue should be seriously studied by international competition authorities.
- 5. The non-ICANN issues are governed weakly and very fragmented at an international level; on the other hand: the net works! Redistribution of mandates and powers between ICANN, ITU and others is hardly feasible, but clarity of responsibility and mandate would help.
- 6. As recently admitted by many, a government oversight within the UN system/family does not seem to be a realistic solution. For some governments, notably the Norwegian, which has UN as the pillar for international cooperation, this is sad and frustrating. We will nevertheless seek viable and effective international governmental oversight structures outside the UN system, see also below.

⁴⁰ ICANN: Internet Corporation for Assigned Names and Numbers

⁴¹ NGO: Non Government Organisation

⁴² GAC: Government Advisory Committee to the ICANN board

⁴³ USG: United States Government

Dilemmas are hard to resolve, but they enhance the understanding of the issues, and they should contribute to risk analysis and search for the right balances between buckets of compromises.

Some observations

In the ongoing discussion on Internet Governance and in particular the future role of governments, some observations or opinions are offered for consideration:

- 1. The operational quality and stability of Internet is good; the USG implementation of their oversight role of IANA44 functions and of the JPA45 has been well balanced.
- 2. The level of political awareness and the professional and social atmosphere between stakeholder groups have improved substantially through the WSIS process and in particular as a consequence of IGF.
- 3. The fragmented governance of international non-ICANN issues is worrying; although a number of relevant multilateral organisations, like ITU, WIPO46, WTO47, OECD48, in fact do cooperate and communicate well. I believe that the mutual understanding of mandates and roles is inadequate.
- 4. The ICANN management structure is still inadequate with respect to accountability, transparency, representation and participation and gender distribution. The ICANN constituency concept should be re-evaluated. The internal committee structure contributes to an opaque situation where the risk of organizational capture is significant. Some of the constituencies in particular concerning "civil society" are questioned by many. The role and transparency of the NomCom49 is doubtful from a transparency and democracy point of view.
- 5. The developing countries with all their not-yet-Internet-users are hardly present at all in the work and management of ICANN. The efforts made have been insufficient.
- 6. Notwithstanding improved performance by GAC with Janis Karklins as chair, the government influence non voting member of the ICANN board and unclear formal role make the GAC a weak element in ICANN! The issues discussed and the delegate level in GAC is most probably not yet appropriate. The risk that governments get involved in day to day operational issues would be remedied by lifting the issues of governmental concern to higher strategic and political level. Also, the role of the private sector should be strengthened and the governments should concentrate on oversight and competence for last resort roles.
- 7. The definition and role of civil society is inadequate and contributes to inefficiency due to the often academic nature of their forums and rhetoric. The civil society which in the ICANN experience is academic and operates outside defined democratic structures, should be heard in IGF and in wide consultations, but should not have formal power in decision arenas.

⁴⁴ IANA: The Internet Assigned Numbers Authority

⁴⁵ JPA: Joint Project Agreement between ICANN and Deptartment of Commerce, USG

⁴⁶ WIPO: World Intellectual property rights Organisation

⁴⁷ WTO: World Trade Organisation

⁴⁸ OECD: Organisation for Economic Development

⁴⁹ NomCom: ICANN Nomination Committee

Over the last decade, and in particular following the WSIS, many books50, conferences, forums and discussions51 have analysed the weaknesses and strengths of the present management and governance structure of ICANN and other elements of Internet Governance. Unfortunately, fewer proposals for change have been seriously offered. This is obviously due to lack of flexibility and cemented positions among some of the stake-holders, e.g. the USG could not accept to share political influence with other states (arguing on homeland security), and ICANN and the civil society could not accept additional governmental influence in Internet Governance.

Possible steps toward a better governance structure

The Internet Governance principles resulting from WSIS, like openness and net neutrality, stability, accountability, transparency, democracy, legitimacy, multi-stakeholder influence and lawful use of Internet must be kept. The management quality and structure of ICANN should be improved with respect to transparency and accountability. The complexity as depicted below could in itself be a democratic problem. ICANN itself is afraid to be captured! With the present structure nobody can see who has captured who. Many will today claim that ICANN is captured by its staff, i.e. by itself. Is that good corporate governance? The obscure constituency concept, the equally obscure NomCom, the uneven composition of the enormous number of committees with respect to gender, positions, geography, etc., should be modernized and significantly simplified.

The governments, representing democratically all citizens, even including the-not-yet-Internet-user, should leave all the day to day operation to the private sector acting according to the best standards of corporate governance, but must take its responsibility to guarantee stability, openness, accountability and lawfulness of Internet operation and use. The present GAC is nowhere near this position.

Commissioner Reding, in her video message52 this spring, suggests several measures that I view as interesting and an excellent starting point for an evolution which certainly is in the spirit of WSIS. A small international, independent tribunal with legal competence should be established. Anyone affected by ICANN decisions should have the right to request full judiciary review by the tribunal of the relevant decisions. This would bring the rights of law factor into the global scene with a broader legal framework than the Californian one alone and replacing or cooperating with, the ICANN Ombudsman.

For the more general oversight pertaining to public policy issues relevant to, but also outside, ICANN, a multilateral government forum or body should discuss, advice and, if judicially possible, decide on issues. Whether this oversight body – also with "last resort" functionality – is a G-12 or G-15 is of less relevance. The important element is that there is a reasonable global distribution of nations in the group including developing countries, that it meets

⁵⁰ E.g. Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG), ed. William J. Drake, UN ICT Task Force, 2005;

The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment, ed. Wolfgang Kleinwachter, Germany land of ideas, 2007;

Internet Governance Forum (IGF). The first two years, ed. Avri Doria and Wolfgang Kleinwachter, UNESCO, ITU, 2008

⁵¹ Report on a meeting towards good Internet Governance in the 21st century, by Marten Botterman, Constantijn van Oranje and Jonathan Cave, the Dutch Ministry of Economic Affairs (March 2009)

⁵² Commissioner Reding's weekly video message 4th of May 2009 on "The future of Internet Governance: Towards an Accountable ICANN"

regularly, e.g. once a year, and that it meets at appropriate high level (to avoid micromanagement). The forum shall not only check out ICANN decisions, but would naturally look at political questions like whether we collectively could benefit from additional and specific law instruments for Internet (usage), ref the idea of an Internet Charter, and analyze how the ICANN monopoly could be suitably regulated.

<u>Remarks</u>

I believe everybody understands that some interesting and challenging work remains before a new government oversight structure for Internet is operational and we see an improved ICANN. Presumably IGF would be a good complement and a vehicle to sound out the implementation steps, preferably to be organized only every second year after 2010. The process must carefully keep industry as operators, service- and content providers in the loop. And, as we all learned during WSIS, we should show patience, listen to the view of many if not all in order to anchor the improved Internet Governance and to ensure that the best qualities of Internet are preserved. The governments will ensure an open, inclusive, robust and innovative Internet, where the further development of content and communication take place in an atmosphere of mutual respect and lawful behaviour.

10.4. Internet – part of Universal Service Obligation package?

Should broadband and Internet access belong to the Universal Service Obligation? If so, what kind of service should it be? Provided by whom? And who should pay for it? The concept of Universal Service is believed to originate from Theodore Vail, then CEO of AT&T in 1907 [Reil09]. This was in the context of providing telephone services. Now it is generally related with *providing basic service level(s) and at a subsidised price for certain regions*.

A number of criteria have been used by regulators to decide what should be within the scope of USO and what should be excluded. The EU criteria are whether

- The service has to be used by a majority of users,
- The use of the service is conductive to social inclusion
- Quasi-ubiquitous availability of the service generates "general net benefits to all consumers"

As broadband has passed the 50 % penetration level in Europe, the first criterion should be complied with. The remaining two are less quantitative, but there seems to be a growing support that broadband and Internet access contribute to social inclusion and generate net benefits.

The question of USO and how it should be funded has always been political. Currently it is largely financed by the telecommunication industry and in most cases the incumbent operator in the market. Considering the increasing competition and general service benefits, it could be argued that these costs should be more widely distributed. Many argue that governments should directly finance this public service offering.

10.5. End-point responsibilities

Which responsibilities should be carried by users/customers (also referred to as end-point responsibilities)? This has been a subject for lengthy discussions. What is commonly lacking from these discussions is the concerns regarding the quite wide capabilities of the end-users/end-points; some are quite advanced while others are rather basic.

For Internet-based service offerings this area grows in complexity as *the market is global, liberated and diversified service offers*. Several market players are also commonly involved. Their relationships could be fairly complex. In addition, several countries could be involved with their own laws and regulations. Just look at the case where the Internet radio station is located in Malaysia while the user listening-in is located in Norway.

In the *trading regulations* the first responsibility usually lies with the provider and consists of the compliance to the respective national legislation in force. National legislation in most European countries is based on the European parliament and the council of European Union legislation.

Directive 2000/31/EC describes some of the providers' responsibilities when the provisioning information society services. That is in particular what concerns electronic commerce across the internal market. The main goal of this directive is to contribute to the proper functioning of the internal market by ensuring the *free movement of information society services* between the Member States over the Interne. This Directive is an important milestone permitting *virtualisation of commerce and e-business among European countries* with well-defined policies and rules, particularity for providers. The Directive 2000/31/EC does not offer a global solution for today's or future disputes concerning responsibilities.

There are several users showing interest in end-to-end control of Internet sessions. This is mainly due to the increasing complexity of home networks and devices. In addition comes the increasing awareness of security challenges. The home/business premises management and control pose several challenges specifically related to adequate service monitoring and to detect failures and security attacks.

Information security is a particular problem. This includes spam, virus etc. It also addresses Intellectual Property Rights (IPR), piracy and improper information or content use. Some providers are usually caught in the middle of the battle due to their intermediary relationship with content providers.

Although awareness raises on these issues, several users are still uninformed of all risks related to piracy. The European Commission is deliberating on this subject. The European Economic and Social Committee (EESC) presented its strategy for a Secure Information Society. This aims to be compatible with the freedom of information, communication and expression. It is anticipated that in the near future there will be more and more control actions, enforced by European laws, and that the involved multiple actors come together in the value chain of responsibility.

10.6. Network neutrality

The term network neutrality has been intensely debated. The concept arouse around 2003 in opposition to the possibility that Internet Service Providers could propose new services while controlling and discriminating certain Intent traffic and content. This gives rise to an unfair situation between network operators and service providers who do not possess their own access lines. There is however today no clear definition for network neutrality but a minimal set of requirements can be identified. Firstly, a network should be able to connect any kind of equipment. Secondly, the network should not impose any restriction on how equipment can communicate. Thirdly, a network should not make any discrimination between flows of data.

Different perspectives can be recognized related to different arguments, see Figure 23.



Figure 23 Different perspectives and argument types related to Internet governance

10.7. Norway

Opening the conference on "Internet Governance at Crossroads" in Oslo, January 2009, Eva Hildrum, Ministry of Transport and Communications referred to the following key topics guiding the governance models (ref. [Hild09]):

- *Information sharing*: Information being essential for our daily work and functioning. Internet as information source has moved from "nice to have" to "need to have" status. Free flow of information is also an essential element in a democratic society.
- *Freedom of expression*: This is often seen as a human right and plays a significant role in the evolvement of today's societies.
- Access to content: Internet is increasing its position for providing access to requested content. A key challenge since the last Internet Governance Forum is how to ensure access to the rest of the world when moving the Internet society forward. This has already been experienced through several events during the latest years. On the other hand, quality and neutrality may sometimes be questioned.

Ministry of Transport and Communications in Norway considered it important to protect the Internet so that it will stay as open as possible. This is also behind the necessity to separate the regulation of transmission and access from the regulation of content.

• *Net neutrality*: The current regulation may not adequately protect the equal treatment of all services and content. That is, certain Internet providers might act as gatekeepers with respect to content and applications within their own networks. Other sources may claim that regulation will harm innovation and the development of the Internet.

Traditionally, minimum regulation has been applied on Internet actors. A key motivation is to preserve the dynamics and power of innovation among the many actors involved in the development of new services based on the Internet. Hence, it is The Norwegian law on electronic communication regulates provisioning of electronic communication services [eCom02]. Its objective is that all households and enterprises throughout Norway shall have access to basic telecommunication service of high quality for a low price as possible. It is also part of the objective to enable highest possible value creation and efficient utilization of resources within the telecom sector by effective competition.

The law and implementation of is aim to gradually reduce the telecom sector specific regulation and replace it with a more general regulation according to competition. As a consequence of this the following principles are used as foundation:

- Minimum level of regulation; sector-specific regulation shall not be introduced if the objectives of the law can be achieved by common competition regulation.
- Technology neutrality; no technology shall be preferred. Market actors shall themselves select ways of establishing and technology that are more cost effective
- Non-discrimination between actors; actors with significant market power shall not take advantage of their position.

In order to achieve effective competition there are some principle means:

- Regulation of price (e.g. price caps, cost-based pricing)
- Non-discriminating actors (e.g. actors with and without infrastructure could be given similar terms)
- Open access (e.g. operators may allow providers to utilize the infrastructure for service provision)

[eCom02] also states that any provider of public electronic communication services shall measure and communicate service quality that is provided to end users. The authority shall provide regulations for how to measure and what levels of information to provide.

important to balance between the i) network providers' need to bundle network and services to get return on their investments, and, ii) the consumer's right to access the services they choose.

The Norwegian government endorses the European Commission's approach, but believes that it needs to be more substantial. In short the challenge for the regulatory authorities is to ensure this power of innovation, technological development, freedom of choice and the right to "freedom of speech", without suffocating or limiting the incentives to continue with capacity development, service development and investments in infrastructure.

- *ICANN domain names*: The number of languages represented on the Internet is increasing. ICANN has initiated a "fast track" process for the implementation of domain names in other scripts than Latin. This will benefit any community that would like to promote individual characteristics of traditions and diversity.
- *Broadband access*: Different governments take active roles in providing access to Internet. Norway has one of the highest percentages in the world regarding broadband access to households. This is motivated by believing that broadband access is an important driver for growth, trade and information and thereby welfare.

The Norwegian eTrade law [eTra02] is an implementation of the European Directive on electronic trade. This refers to information society services, which is defined as

- a service that ordinary is paid for, over distance and distributed electronically and by individual request by a receiver, and,
- any service consisting of providing access to or transferring information over an electronic communication network, or being a networked host for data that is delivered to a service recipient.

This directive is based on a set of principles, including:

- Home country's regime regulates service providers. The service provider must obey regulation in its home country. Any service provider located within the EEA has right to offer services in Norway without any hinders by Norwegians regulations. A country, however, may terminate certain services in order to protect general health, public security, etc.
- Obligation to provide information. Relevant information about a service provider must be available, such as name, address, and so forth.
- Unsolicited e-mail: Any service provider that distributes marketing information by electronic mail must consult national registries where users have reserved the right to not receive such commercial mails.
- Electronic agreement establishment: It must be possible to establish agreements by electronic means. These agreements must have the same legal status other agreements.

The Norwegian Post and Telecommunications Authority have issued a document on principles for Internet neutrality [PT-nn09]. Overall objective by the network neutrality is that Internet provides *an open and non-discriminating platform for all forms of communication and content distribution*. The document summarises a set of principles addressing how every Internet Service Provider should handle the traffic (translated from Norwegian):

- 1. Internet users have rights to get an Internet access with specified capacity and quality. This implies that:
 - a) Internet access capacity and quality shall be clearly specified.
 - b) In case the physical access is shared between services, is shall be described how the capacity is divided between the Internet traffic and the other services.
- 2. Internet users have rights to get Internet access able to:
 - a) Fetch and deliver content as wanted
 - b) Use services and applications as wanted
 - c) Connect equipment and user programs that do not harm the network, as wanted

This does not legitimate access and distribution of illegal and harmful services and content. It is also open for an ISP to levy additional charges for heavy use of capacity.

3. Internet users have rights to access without discriminating types of applications, service, content and who is the sender or receiver.

This implies that individual data flows using the basic Internet service shall not be discriminated. Traffic control to prevent harmful behaviour, comply with lawful conditions, ensuring service quality, prevent temporary congestion and prioritize traffic according to users' requests are allowed.

The document also elaborates on how to define network neutrality. An idealistic definition is "an electronic communication network where all traffic is equal independent of application, service, content and sender and receiver address. It is possible to differ between different service classes. A fair capacity, however, should always be available for the basic service class ("best effort class").

The first principle implies that capacity and quality of the access must be clearly specified. In case the access is shared among a number of services, how the capacity is divided between the Internet traffic and the other services must also be specified. This addresses the so-called "walled garden" versus the "open garden" as some ISPs provide.

- Which governance models to apply for different aspects of the Internet is high on various agendas.
- Society, business and human rights to be balanced in multi-stakeholder model.
- Internet being an open and non-discriminating platform for all forms of communications and information sharing.

11. Selected national initiatives

The *Western economies*, headed by the US, have *dominated the word markets in the last century*. In recent times, however, we fined the more rapid growing economies in Brazil, Russia, India, and China (also referred to as the BRIC countries). The collective GDP from the BRIC countries is expected to surpass the GDP of the 6 richest countries within a few decades (the USA, the UK, France, Japan, Germany, and Italy).

In result the *geopolitical and economic power may shift from the West to the East.* Even if the current recession shaves two to three percentage points off its current 12 % GDP growth rate, China's economy will overtake all the European countries by 2015. Similarly, India's tech market is expected to grow at 20 %. One example of this is the current additions of 8 to 12 million new mobile subscribers every month. This places India in the word's fastest-growing technology market along with China.

So, how should any nation respond to such effects? Or, should one simply enjoy others countries' emerging dominance? In the following a few of the national Internet initiatives are summarized. There are also other national initiatives in Europe as summarised in [NIDwg08].

11.1. Australia

The Australian government has announced that it will drive the construction of a \in 23 billion nationwide fibre to the premises (FTTP) network. This is planned to be done by a company in which the government in will hold a minimum 51 % stake.

In effect, over the following 8 year period, about 90 % of all Australian homes, schools and work places should be connected with *bit rates up to 100 Mbit/s*. The remaining 10 % is to be connected by wireless and satellite at bitrates of 12 Mbit/s.

The government states that this "will be the single largest nation-building infrastructure project in Australian history".

11.2. Finland

In Finland, a number of *strategic Centres of Science, Technology and Innovation* (SHOKs) have been defined. Future Internet is within the ICT SHOK.

Key emphasis is placed on innovation, novel network management schemes, security ad native support of mobility.

11.3. Italy

In June 2009, the Italian government announced that it would spend \in 1.47 billion on upgrading infrastructure. This was to provide all citizens with access to broadband bit rates of 2 - 20 Mbit/s by 2012.

11.4. Japan

The UNS strategic programs, released in 2005 by the Ministry of Internal Affairs and Communications in Japan, opened for a *new generation network* based on innovative concepts. An idea was to ensure that the network architecture was defined with a *long-term perspective* in mind.

This was the trigger for launching the New Generation Network Initiative. This is complemented with a forum consisting of 200 members across industry and academia.

This is also supported by the *AKARI initiative* – several research projects exploring research paths. Main focus areas address aspects of network technologies, in particular optics, sensor networks and security. The projects also include experiment research projects that can be made available for experiments and applications. The AKARI initiative was launched in 2006.

The AKARI initiative has allowed for a so-called *clean slate approach*, assuming at time-tomarket horizon around 2015 - 2020. The point is to avoid limitations following from existing implementations. The goal is to create an overarching design for how the network should look like. The design principles are related to societal trends.

The primary goal the AKARI project is to design a network of the future, [AKAR08]. By year 2015 technologies for a new generation network should be available. A network architecture is also be developed and corresponding network design to be created. Conceptual design was made in 2007.

After having defined the new architecture, the challenge of migrating today's networks and systems is to be looked into.

Factors to be considered for the new generation network are (from [AKAR08]):

- Peta-bit/s class backbone network, 10 Gbit/s fibre to the home, e-Science
- 100 billion devices, machine to machine, 1 million broadcasting stations
- Principles of competition and user-orientation
- Essential services (medical care, transportation, emergency services), 99.99 % reliability
- Safety, peace of mind (privacy, monetary and credit services, food supply traceability, disaster services)
- Affluent society, disabled persons, aged society, long-tail applications
- Monitoring of global environment and human society
- Integration of communication and broadcasting, Web 2.0
- Economic incentives (business-cost models)
- Ecology and sustainable society
- Human potential, universal communication

These factors are considered to be derived from the following general requirements, [AKAR08]:

- *Large capacity*. Increased speed and capacity are required to satisfy future traffic needs, which are estimated to be approximately 1000 times current requirements in 13 years.
- *Scalability*. The devices that are connected to the network will be extremely diverse, ranging from high-performance servers to single-function sensors. Although little traffic is generated by a small device, their number will be enormous, and this will affect the number of addresses and states in the networks.
- *Openness*. The network must be open and able to support appropriate principles of competition.

- *Robustness*. High availability is crucial because the network is relied on for important services such as medical care, traffic light control and other vehicle traffic services, and bulletins during emergencies.
- *Safety*. The architecture must be able to authenticate all wired and wireless connections. It must also be designed so that it can exhibit safety and robustness according to its conditions during a disaster.
- *Diversity*. The network must be designed and evaluated based on diverse communication requirements without assuming specific applications or usage trends.
- *Ubiquity*. To implement pervasive development worldwide, a recycling-oriented society must be built. A network for comprehensively monitoring the global environment from various view points is indispensable for accomplishing this.
- *Integration and simplification.* The design must be simplified by integrating selected common parts, not by just packing together an assortment of various functions. Simplification increases reliability and facilitates subsequent extensions.
- *Network model.* To enable the information network to continue to be a foundation of society, the network architecture must have a design that includes a business-cost model so that appropriate economic incentives can be offered to service providers and businesses in the communications industry.
- *Electric power conservation*. As network performance increases, its power consumption continues to grow, and as things stand now, a router will require the electrical power of a small-scale power plant. The information-networked society of the future must be more Earth friendly.
- *Extendibility*. The network must be sustainable. In other words, it must have enough flexibility to enable the network to be extended as society develops.

11.5. New Zealand

A few days before the announcement by the Australian government, it was announced in New Zealand that they plan an investment project for about \in 600 million. This is to provide a *broadband network with access bit rates of 100 Mbit/s*. It has been proposed to establish a joint government and private company initiative.

The New Zealand government has estimated *economic benefits* in the range $\in 1 - 1.8$ billion per year from having a new national broadband network.

11.6. Sweden

The Royal Swedish Academy of Engineering Sciences Sweden has completed an Internet Foresight project as documented in [IVA08]. A number of recommendations have been delivered to *allow Sweden taking a prominent Internet nation role by 2015*. The approach proposed is based on strong involvement from the industry and named *Ambient Sweden*.

They summarise the following proposed measures to make Sweden a top Internet nation in 2015:

• New *opportunities for business and the public sector* – become a pioneer within digital media distribution, use of e-administration systems and green IT. This requires targeted initiatives and investment building on current projects in Sweden.

- Raise the *level of trust in the Internet* increase awareness of importance of information security. Internet infrastructure must be robust allowing service with high quality and without interruptions. Introducing a national e-identification system could also raise the trust level.
- A *common service market* access to services independent of access and networks. Could involve creating common services that follow the user and not the provider. Two examples are email addresses and access to on-demand content.
- *Infrastructure for future Internet services* ensure long-term and predictable regulation not placing obstacles on investing in infrastructure. Buying and selling services in a flexible and competitive manner should be encouraged.
- A *business-friendly climate* Sweden to provide better environment for starting, expanding and operating business compared with other relevant countries. This need to encourage foreigners with relevant skills to desire to work and live in Sweden.
- The distance between *steps on the digital ladder* (see Figure 24) will be reduced through increased competence making effort to help and inspire people to climb the digital ladder. This required joint effort of the public sector, school, labour market players and citizens' organization. The different steps in the ladder will evolve according to technology being developed.
- A *flexible working life* new forms of communication support remote and nomadic working places. This will support regional development. Systems and applications that facilitate personal contact independent of distance allow climbing the digital ladder. This attracts competence, reduces need for physical meetings, frees up resources and reduces personal stress levels. Environmental benefits will also follow. Internet can be utilised to support a more flexible working life. This needs to be captured by the labour market players.
- Introduce *computer studies and IT-based teaching* in schools this includes pedagogical research, teacher training in technology use and development of the appropriate tools. Swedish innovation companies could play an important role, both nationally and internationally. Computer studies could also be made compulsory in the curriculum. These studies should cover technology, ethics and media scrutiny, considered to be important skills to climb the digital ladder.
- Research and innovation that *places Sweden at the top* maintaining and expanding teams of world class researchers. An "Internet of the Future" committee could be established. This could serve different duties including producing the basis for a research budget. Internet foresight must help to ensure that Swedish industry is competitive and stimulate the creation of new enterprises.
- *International profiling* participating in international organisations that focus on Internet use and standardisation. Particular areas are mobile Internet, e-administration, green IT and digital media distribution. A network of people could be established to achieve coordination at the national level. This is to stimulate activities going on in Sweden both by Swedish and by foreign companies. Main purpose of the network is to work with initiatives that are structured, long-term and predictable.



Figure 24 Digital ladder illustration (adapted from [IVA08])

In order to this to happen, [IVA08] proposes as programme – Ambient Sweden – to realise the proposals. The programme gets the mandate to drive development and implementation of the proposals. The interpretation of leading Internet nation is illustrated as three areas, see Figure 25:

- *Application* implying high level of usage and high usability. This implies value for the users by simpler communication, more services or improved efficiency.
- Access to internet by sufficient capacity, security and quality. Open market for providing Internet services not preventing investments in capacity.
- *National collective leadership in international organizations* setting the scene for Internet's organisation, control and development. This also implies research and enterprises in world class.

	Advanced appli	cation - usability		
High usage by enterpri and private persons	High usage by enterprises, governments and private persons		el of integration into	
	Access to	broadband		
Broadband access ove copper	Broadband access over fibre, wireless, copper		Efficient and sustainable market in balance	
	Collective lead	ership of the nation		
Leading in international organizations for applications	Leading in internati standardisation	onal organization for	Research and product development tha results in flourishing businesses.	

Figure **25** *Three areas for placing Sweden among the leading nations (adapted from [IVA08])*

In order to achieve the goals, [IVA08] underlines the need for having *competent technical research activities*. This is to allow Sweden to utilise and influence the development. Within the technical area topics like network architecture, system architecture, operation and maintenance, security, routing and distributed storage are mentioned.

Regarding specific actions, it is recommended to establish a "Future Internet" committee that is allocated a budget from year 2009. By 2015 the ambition is to have at least three Swedish research groups at world class level within Internet research.

To address the European initiatives, it is recommended that Sweden achieves a main hub of one of the *Knowledge and Innovation Communities*⁵³, to be located in Stockholm.

11.7. UK

Early in 2009 the UK government confirmed a 2 Mbit/s universal service obligation by year 2012. The networks could be partly funded by money not spent from facilitating the digital switch-over. The government also approved a £ 100 million project to roll out next generation broadband across the South Yorkshire region

11.8. The USA

A NewArch project was started in 2000. Somewhat later a workshop on Future Directions in Network Architecture was held. This was linked with the two NSF projects:

- The FIND umbrella for support of research. This is replaced by the initiative Network Science and Engineering (NetSE), launched in September 2008. Funding is about 20 mill. USD per year over 4 years.
- *The GENI umbrella* for support of experimental research and test beds facilities. Funding is about 5 mill .USD per year over 5 years.

In the beginning of 2009 the Obama administration got through a stimulus plan including 7.2 billion USD for *broadband service development*. This is roughly divided between the National Telecommunications and Information Administration (NTIA) part of the Department of Commerce (4.7 billion USD) and Department of Agriculture (2.5 billion USD). The former is to carry out the "Broadband Technology Opportunities Program", while the latter follows the Rural Utilities Service (RUS). In addition the Federal Communications Commission (FCC) was given a year to make a national broadband plan including "an analysis of the most effective and efficient mechanisms for ensuring broadband access by all people of the United States.".

The plan includes ambitions for rapid impact. The departments must earmark funds by end of fiscal year 2010 and chosen projects must be "substantially complete" within two years after that. It does not, however, define what broadband means. This opens for the race among cable network, copper network, fibre network, wireless and other operators.

A critical emphasis is placed on serving rural and other under-served areas. The US congress added a remark that the RUS funds gives priority to projects that allows users a choice of service provider. This could be to limit the attractiveness of such projects to the (local) incumbents.

⁵³ Knowledge and Innovation Community is an EU initiative.

An argument for this may be the ten-fold return in investment that the US government expects for every dollar invested in broadband.: US Congress January 2009 remark: "For every dollar *invested in broadband*, the economy sees a *tenfold returns on that investment*".

In the USA, around 55 % of adults used broadband Internet connections at home in April 2008, this was up from 47 % April 2007.

- Several countries have stated certain ambitions regarding broadband deployment and usages.
- Internet initiatives have been launched by several of the dominating countries.
- Political attention regarding the crucial position of Internet in the further wealth of the society.

12. Summarising selected prospectives

12.1. Broadband versus Internet

Although not strictly true, several relate the Internet usage to broadband. However, Internet access can in fact be provided on any communication means as long as it is capable of sending IP traffic. Still, the broadband access allows improved user experience regarding response times. There are also several services that require higher bit rates, such as transfer of video.

Broadband in Norway

Norway is a cost-intensive country for telecom infrastructure deployment. This is due to disperse population and mountainous geography. Still the broadband coverage has increased from almost nothing to almost 100 % during a decade. Note that this assumes broadband capable of supporting 640 kbit/s (down stream direction towards terminal).

Somewhat more than 99 % of all households in Norway are covered by wired broadband access (copper, fibre, coax). In fact, by end-2009 it is estimated that about 2 800 households have not been covered by a broadband services with at least 640 kbit/s down stream bit rate (from [FADbb98]).

A distribution on different technologies is given in Table 3. Note that different access technologies will naturally overlap. A trend towards users shifting from xDSL to fibre has also been recognized during year 2009.

Table 3 Estimates of access technology distribution for Norwegian households by end-2009(adapted from [FADbb98])

Technology	xDSL	Mobile broadband	Coax	Radio	Fibre
Fraction households covered	94 %	94 %	49 %	37 %	21 %

Which bit rates would be then be expected in the future? There is no unique answer to this question. Some say that within 5 years common bit rates will be within the range of 8 Mbit/s to 50 Mbit/s (down stream). However, this is very much driven by the usage of applications requiring more bandwidth, such as video. In particular high definition TV/video will place requirements on the bit rates to be provided. A key driver for this may also be ambitions stated by the Norwegian government.

Another discussion is to what degree the bit rates required will be symmetric (that is up stream versus down stream). Common examples are found for the relation 1 : 4 to 1 : 8 between up and down stream. However, inspired by the trend towards user-generated content and user involvement, more symmetry would be expected. Several points to the optical fibre access as the wired access form to provide the long-term bit rates. Correspondingly on wireless access, WLAN and 3G/4G systems may prevail.

To address these questions, a study was launched by the Ministry of Government administration and reform [FADbb09]. They raise a set of questions impacting the demand for bit rates and coverage, including:

- Which *political goals and ambitions* shall be defined regarding deployment of high capacity broadband network in Norway in the near future?
- Shall the *digital dividend* be used for mobile broadband or TV?
- Shall access to high capacity broadband network be *regulated* before the networks are deployed, or shall *clear incentives* be given for as much commercial deployment as possible?
- Shall local municipals, road authorities, etc, be allowed to place strict limitations regarding *ducting for pipes and cables*, or shall there be a common national policy regarding broadband infrastructure cabling that stimulates as much deployment of high capacity broadband network as possible?
- Will improved efficiency of *health and elderly care* by use of video-based means become a prioritized task?
- Will development of *education arenas on all levels* utilizing digital, video-based means become an important task to further develop Norway as a knowledge nation?

Regarding the first item, a communiqué to the Norwegian parliament dated April, 17th 2009, the following could be read:

"Primary goal is that a full national broadband coverage shall be realized. As this goal is almost achieved, further effort will be spent on the following challenges:

- persons should make use of the broadband network
- increasing capacity of the broadband network"

It is further stated in the report that a nationally covering, future-oriented broadband network can be implemented for a relative low cost by smart and consistent regimes for regulating infrastructure deployment. It is also stated that the sooner such a network is established the greater value it will contributed to the society.

Drivers for increased broadband include:

- *Higher demands* following from servicing involving users. This includes for example sites for user-generated content and allowing social interactions. Mid 2009 about 40 % of all Internet users are part of a network-based society (e.g. Facebook, Twitter, LinkedIn). More video content is also available driving the bandwidth consumption.
- Request for *more flexible and adaptable "always on, always in sync, always within touch"*. In particular this drives demands for mobile broadband coverage and capacity.
- Competition between network operators. That is, there will be a fight to offer the "best" Internet and broadband services.
- Innovation of new services and business models. In particular related to Internet, the service innovation is assumed to keep up and even increase. This is for example inspired by the sheer volume of users available when launching services based on Internet.
- *Governmental concerns and incentives* related to green solutions (reduction of energy consumption and pollution), health services and education.

Going forward, it will become a political discussion whether Norway should find a place in the Internet and broadband front or leave the innovation and early gains to other countries? [FADbb09] concludes that experiences from other countries demonstrate that the *nations*

stating the most ambitious political goals and visions are also leading in this evolution. This refers to evolution both in terms of infrastructure capacity and user behaviour.

Samples from other countries

Several countries and municipal governments have stated fairly ambitious goals. Some of these are (from [FADbb09]):

- Finland: every inhabitant shall have access to high capacity broadband with bit rates greater or equal to 100 Mbit/s by year 2015.
- Australia: 90 % of the population shall have access to 100 Mbit/s based on optical access within 8 years.
- Greece: 100 Mbit/s for every one within 7 years.
- South Korea: 1 000 Mbit/s to everyone by 2013.
- China: 100 Mbit/s for everyone as a target.
- Singapore: 100 % coverage of optical access by 2015.
- Stockholm (Sweden): 90 % of the households shall be covered by optical access by year 2012.
- Catalonia (Spain): funding of optical deployment to every public office.

For several countries we can observe emerging local and regional infrastructure operators. There may be different drivers for this trend, however. For example, in several European countries the main motivation seems to be to promote the development of under-developed regions. Such cases are found in France, Ireland and Sweden.

The risk of a digital divide between different regions in the same country is typically behind such initiatives. This is why some governments explore incentives that encouraged deployment of broadband beyond urban areas. For the three countries mentioned, the governments invested in telecom projects with some common characteristics; i) third party infrastructure provider that leased the infrastructure to several providers on a cost-oriented basis, ii) competition neutral infrastructure to fuel competition on services.

For USA the primary motivation seems to be the risk to fall behind other countries. This is to achieve a "critical mass" of residential users to further drive innovative solutions. Some state that the broadband access should be built and owned by public entities, similar to public roads. These should then be completely open access to all on non-discriminatory conditions and on cost-recovery principles. The analogy is brought further by comparing telecom and basic Internet services with public infrastructure like roads and water and sewer systems (and even power supply in some regions). Some consider information networks just as new types of infrastructure. Note that public ownership of the physical network does not necessarily mean that the authority manages the network or provides services. Users could then choose which service providers to engage with regarding service in the relevant areas.

12.2. Future Internet issues

Corresponding to various national initiatives, there are also different European initiatives. As proposed in [NIDwg08] such initiatives must consider a number of characteristics. One of the key elements is collaboration and networking.

The *right mix of players* should be planned. This means that different industry, governmental, academic and user groups must be included. This mix will also nurture innovative ideas. Different aspects should be covered such as:

- Players of different types several collaborative arenas are already present in Europe, e.g. Research Framework Programmes, Eureka.
- Knowledge across different disciplinary dimensions covering both "hard sciences" and "soft sciences".
- Skills creation and exploitation of knowledge concerning the development of the necessary skills; recent initiatives in Europe is definition of Knowledge and Innovation Communities (KICs)⁵⁴.
- Users involving users in the creation of content and services/applications. Networking between users should provide innovative solutions and working arrangements.

These must consider the globalisation trend, meaning i) global experiments and testbeds allowing large scale validation of research results, ii) support of global standards, and, iii) early identification of usage requirements from prospective user countries and regions.

Testbed initiatives have been described by several national initiatives (see Chapter 11). It would be natural to relate these for certain topics in order to gain from common activities and observations. In effect, the testbeds can be deployed across several countries to include relevant research and development environments in a simpler manner. In general, experimenting based on technology and application oriented results allows for a "proof" of usefulness of available results.

Basic motivating factors for establishing testbeds include:

- i) *Hands-on supported education*. Currently most students learn mainly from a text book with few practical experiences. Building a running test facility would allow to get hand-on experience with large-scale deployments. This impacts both the training of future work force and the quality of research.
- ii) *Outreach*. An open test facility would be available to anyone. This lowers the barriers to entry and broadens the community of students and others to engage in cutting-edge research.
- iii) *International co-operation*. May support federation of facilities, thereby enabling other countries and organizations to offer resources to a broader experimental facility.
- iv) *Industrial involvement*. Immense opportunity for industrial participation, ranging form equipment manufacturers, service providers and other development groups as well as different user categories, including governmental offices.

A number of common topics have been outlined in [NIDwg08]. These might be addressed related to activities on future Internet:

- *Rethinking network operation* aspects, management and resource control approaches to fit the widest possible application requirements.
- Progressing towards mobility and end to end very high speed rates, in a native manner.

⁵⁴

See http://eit.europa.eu/kics-call.html for Calls for Proposals of Knowledge and Innovation Communities

- Supporting the network and service functionalities coupled with sensors and edge devices, enabling the emergence of *Internet of things*.
- Creating the *networked service architectures* favouring user controlled service creation and mash ups and hence an Internet of services.
- Providing the need functionalities for the emergence of *massive 3D usages*, for entertainment or public applications such as health.
- Understanding *information networking* methods for saving, sharing and delivering information.
- Addressing *security/trust/identity* as horizontal issues from both the research and the experimental/infrastructure perspective.
- Advancing the *federated testbeds* experimental infrastructure enabling Europe to run its own research and experimental facilities whilst at the same time building the capability for interconnection with other infrastructures existing in other regions, such as initiatives in the USA and Japan.

12.3. Example applications and functionality

Browsing the list of application ideas related to Internet is more than a full-day activity. Steadily new ideas are mentioned and quite a few are launched as a public service offer. Several of the traditional telecom players are also engaging in this, such as the service providers and the manufacturers.

A brief sample of some applications belongs to the groups of:

- *Home automation*: automation solutions for control of home security and comfort. These include air conditioning, lights control, window closing, surveillance, plant watering, pet feeding, controlling digital multi-media home systems etc. A future home may combine all these and other functionalities under a common interface for control.
- *Entertainment*: control over media library for sharing and distributing content outside home. This could be to make media library accessible to other home networks.
- *Infotainment*: allows for example a user to make his programme/information guide, selecting among a set of media types and contents.
- *Education*: used for various age groups and at different levels.
- *Social inclusion and health services*: various assistance solutions allowing persons to continue to live at home. This also covers any e-Care services.
- *E-business*: including home shopping and home offices.
- *Car communication*: including reporting from a car on varying driving conditions, slippery, congestion, accident, etc. Entertainment and logging applications in cars have also been developed.

To gain from economy of scale and scope additional requirements relevant aspects to consider include:

- technology-independent
- allow seamless interworking

- support different service levels, including resilience and response times
- support different business models
- offered in various regions, even on a global scale

It is typically fundamental to take into account individual requirements of users in an early phase. This is both to get feedback on early implementations and to examine and adapt the applications based on user behaviour. Approached in a proper way, the Internet provides a means for experimenting with such service cases.

This could also include basic capabilities that typically are found within the service providers, such as:

- Mechanisms for *authentication and identity* management: this is a key strength, e.g. utilising SIM cards found in mobile systems.
- Knowledge about *locations*: to some level of granularity whereabouts of certain objects are known. For example a cell for a mobile system and an access line for a fixed broadband system. Built-in GPS functionality may add to the accuracy.
- Information about certain *preferences*, service profiles, etc.
- Mechanisms for *billing and accounting*: a billing relationship is a pivotal asset. Different billing arrangements exist, which support different business models.
- Service outlets making the applications and service offers known to a wider set of users.
- *Traffic inspection and data collection* mechanisms for monitoring, security attack prevention, etc.
- Mechanisms for *ensuring service levels*, configuring, fault handling, etc.

Utilization of location information and more complex types of context can enable new types of application and services. *Context-awareness* deals with the ability of applications to utilize information about the user's environment (context related to time, location, network connections, applications, sensors, remote sources) as well as higher levels like being with a group of friends or family members.

Such information can be used to tailor services to the user's current situation and needs. Building context-aware systems involves the consideration of several new challenges mainly related to the gathering/sensing, modelling, storing, distributing and monitoring of contextual information. These challenges justify the need for proper architectural support. Platforms for context-aware application should facilitate the creation and the dynamic deployment of a large range of applications, including those that have not been anticipated at time of designing the delivery system.

To improve user expectation, network-aware services and service-aware networks have been proposed. This includes higher levels of automation, including self-management. This areas also collects several features into an orchestrated whole, such as context-awareness, robustness, mobility, reliability, security and Quality of Service support.

12.4. Example: contributions to poorer regions

The Norwegian Public Clarification [NOU08:14] addresses several opportunities for a coherent Norwegian policy to promote development in less developed countries. As one out of seven policy areas, knowledge is further elaborated on.

Information technology is an enabler for distributing knowledge rapidly and effectively. The report states that different national and regional governments compete on leading research and innovation in order to ensure future economic growth. Within the OECD enterprises make up a steadily higher fraction of the research effort.

Awareness of knowledge being a strategic economic resource for enterprises and governments has increased. This has again lead to *growing interests for privatisation and commercialisation of knowledge*, e.g. through the number of patents. There are, however, counter-forces driving towards openness and sharing.

[NOU08:14] goes on by referring to South Korea as one country that has successfully grown by placing intense effort on education, research and importing technology knowledge. Mass production allows reduced costs and access to technologies for groups with lower levels of willingness to pay.

One of the global trends is more *openness and sharing of knowledge and technology* (e.g. Open access, Open source, etc.). This may lower the costs and make it easier for less developed countries to receive and take part in knowledge sharing.

Mobile telephony is mentioned as one technical solution that has taken a position as enabler for wealth, sustained living conditions and income. End 2008 about 80 % of the world's population lived within coverage of a mobile network. The situation is rather specific in certain countries. For example in Tanzania, about 10 % of the households have electricity. On the other hand 97 % of the population has access to a mobile phone. Mobile services can also be a fundament for business, such as payment, banking and market place for groceries and fish.

A real danger is that the poorest countries may be marginalized within the knowledge economy area. As they currently do not make up an attractive market, there will likely not be enough knowledge and technological solutions that are tailored for their situations and taking care of their peculiarities.

- Internet chosen as vehicle for launching several business ideas due to the fairly low entry barrier and the great market potential.
- Long list of ideas for applications can be found in various fora.
- Fundamental functionality present in different parts of the network and in the end-systems to provide user-friendly services.

13. Concluding remarks

Within two decades Internet has moved from a small academic network to a widely used arena for various types activities. Today, these activities include trade, payments, reporting, education, entertainment, games and social interaction. More types of activities are expected in a future Internet. And the society will depend even more on an operational Internet. It is expected to deliver predictable and secure services to users in a flexible manner. In fact, this will become essential for any modern society.

To support such a future Internet, several initiatives have been launched in different regions. One motivation is the *basic shortcomings of the Internet design*. These were identified already in the beginning of the 1990s. It is perhaps quite a paradox that today's version of Internet has been able to go through this phenomenal growth despite such basic design challenges.

Another motivation for the initiatives is the request to take on leading positions on the question of how a future Internet should look like, and how it should be managed. Major *business opportunities* are expected to emerge during this work.

Severe limitations are faced, such as the limited addressing space. These will become even more evident as more users and applications are added. Key issues have also been identified regarding *security and predictable service levels*.

More nations recognize the essential role Internet can play in society's prosperous situation. Correspondingly, national programmes and projects have been initiated. Some of the national ambitions are also quite clear and intended for bringing together groups from different players. The research on future Internet has started by several research groups.

So, what should be the Norwegian approach to the future Internet? Two well-known options are i) to wait for solutions developed by others and import the working ones when needed, or, ii) to define our own areas and way of working to seize the opportunities revealed.

An obvious motivation for the development related to Internet is the size of the market. As common solutions are available across the globe, services offered at one place could be accessed from any place having Internet access. This has been recognized by many of the political groups already defining their ambitions.

This report addresses various aspects of the Internet; History, status and future options are discussed. One motivation is to relate the technology challenges and objectives to societal needs and trends. In that respect, critical issues with today's Internet are presented; several technical areas have to be improved. Again, these are motivated by requirements following from current demands and trends.

Main objective of the report is to provide background and some arguments related to current challenges and future options in the Internet space. It is believed that a broader discussion should be undertaken also in *Norway to seize the opportunities revealed*. A balanced portfolio of *governmental and private activities must be started*. In particular the national initiatives will is most cases work as a key driver for other activities.

A key point is to maintain the *innovation force* related to Internet at the same time as sustainable *commercial operations* are fuelled. Today's dependency of Internet regarding key society and business functions will become even stronger in the future.

To further allow for increased societal welfare, therefore, it is essential to ensure that the Internet evolves correspondingly. Selected areas are described in this report, together with illustrations of how these could be pursued.

Act locally – think globally \rightarrow Applicable even for the Internet evolution.

14. References

[Afua01]	A. Afuah, C. Tucci: Internet Business Models and Strategies. McGraw Hill 2001.
[AKAR08]	AKARI Architecture Design Project: New Generation Network Architecture AKARI Conceptual Design (ver. 1.1). October 2008.
[AmSw08]	Ambient Sweden: Internet predictions – how to make Sweden a leading Internet nation in year 2015 (in Swedish). Available on www.iva.se/internetframsyn
[CELT09]	CELTIC purple book: New challenges for Celtic. Issues 2009. [on-line: www.celtic-initiative.org]
[Davi09]	Charlie Davies: Bridging the broadband divide: challenge and solutions. Ovum straighttalk. April 2009, p.16-17.
[EC97/21]	Official Journal of the European Union: Opinion of the European Economic and Social Committee on the Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – A strategy for a Secure Information Society – Dialogue, partnership and empowerment. 2007/C 97/09
[Eci2010-05]	Commission of the European Communities: i2010 – A European Information Society for growth and employment (SEC 2005/717). June 2005. [on-line: http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229: FIN:EN:PDF]
[eCom02]	Norwegian law on electronic communication. (ekomloven). Ot.prp. no. 58. 2002-2003. (in Norwegian)
[ENIS08]	European Network and Information Security Agency: Resilience features of IPv6, DNSSEC and MPLS. Greece. 2008.
[eTra02]	Norwegian law on certain aspects of electronic trade and other information society services. (ehandelsloven). Ot.prp. no. 31, 2002-2003. (in Norwegian)
[FADbb09]	Ministry of Government administration and reform: Broadband 2.0 – status and development towards 2015 (in Norwegian). On-line: <u>http://www.regjeringen.no/en/dep/fad/Documents/Reports-and- plans/Reports/2009/bredband-20.html?id=570961</u>
[GENI07]	Global Environment for Network Innovations Research Plan. 2007
[Haus09]	David Hausheer, et al.: Future Internet Socio-Economics – Challenges and Perspectives. Toward the Future Internet. IOS Press. 2009.
[Hild09]	Eva Hildrum: Opening speech at "Internet Governance at the Crossroads" conference. Oslo, Norway. 29-January-2009.
[ITU-IDX09]	International Telecommunication Union: Information and Communication Technologies Development Index. Geneva. March 2009
[IVA08]	Royal Swedish Academy of Engineering Sciences: Ambient Sweden. April 2008 [on-line:

	http://www.iva.se/upload/Verksamhet/Projekt/Internetframsyn/internetframs yn-syntesrapport.pdf]
[Jans08]	Dean Jansen: Miro – open and decentralized Internet TV. EBU Technical Review. 2008 Q3.
[Juni09]	Juniper: Deploying IPv6: Issues and Strategies. January 2009.
[Lein07]	Barry M. Leiner, et al.: A brief History of the Internet. 2007. [on-line: <u>www.isoc.org/internet/history/brief.shtml]</u>
[Liot08]	A. Liotta, A. Liotta: P2P in a regulated environment; challenges and opportunities for the operator. BT Technology Journal. Vo. 26, no 1. September 2008. p.150-157.
[Lund01]	Yngvar Lundh: Computes and Communication. Early Development of Computing and Internet-technology – a Groundbreaking Part of Technical History. Telektronikk 2/3 2001, p.3-19.
[NIDwg08]	Report from the National ICT Research Directors Working Group on future Internet (FI). July 2008 – November 2008. [on-line: http://www.future- internet.eu/fileadmin/documents/reports/FI_Rep_final281108pdf]
[NOU08:14]	Norwegian Public Clarification (in Norwegian Norsk Offentlig Utredning): Coherent for development? How coherent Norwegian policies can assist development in poor countries. NOU 2008:14.
[NOU09:1]	Norwegian Public Clarification: Individuals and integrity: Privacy in the digital society. NOU 2009:1. (in Norwegian)
[NYTI08]	New York Times: Internet Traffic Begins to Bypass the U.S. 30 August 2008. [on-line: http://www.nytimes.com/2008/08/30/business/30pipes.html]
[OECD07]	OECD report: Broadband and ICT Access and use by Households and Individuals, DSTI/ICCP/IE (2007)4/FINAL
[OECD09]	OECD Ministerial Meeting: The Seoul Declaration for the Future of the Internet Economy. Seoul, Korea. 17-18 June 2008. [on-line: http://www.oecd.org/dataoecd/49/28/40839436.pdf]
[Pear09]	Chris Pearson, Rob van den Dam: The changing face of communications. European communications. Spring 2009, p.14-17.
[PT-nn09]	Norwegian Post and Telecommunications Authority: On network neutrality. Principles for neutrality of Internet. 16 April 2009 (in Norwegian) [available on-line
[Redi09]	Niviane Reding: Internet of the future: Europe must be a key player. Manuscript for speech delivered during "Future of the Internet initiative of the Lisbon Council" February 2009
[Rei109]	Benoit Reillier: Broadband for all European communications Spring 2009
[RFC1287]	D. Clark et al.: Towards the Future Internet Architecture. IETF RFC 1287. December 1991.
[Tsel09]	Georgis Tselentis, et al.: Towards the Future Internet. A European Research Perspective. IOS Press 2009.

[Twat08] ITU-T Technology Watch Report no 7: NGNs and Energy Efficiency. August 2008.