Jussi Kivilaakso

Net neutrality in Finland

School of Electrical Engineering

Thesis submitted for examination for the degree of Master of Science in Technology.
Espoo 23.11.2015

Thesis supervisor and advisor:

Prof. Heikki Hämmäinen

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Jussi Kivilaakso
Title: Net neutrality in Finland
Date: 23.11.2015 Language: English Number of pages: 7+48

Department of Communications and Networking
Professorship: Networking Technology Code: S-38

Supervisor: Prof. Heikki Hämmäinen
Advisor: D.Sc. (Tech.) Heikki Hämmäinen

The Internet is increasingly important for modern information society and it has changed the way we communicate and do business. However, the rapid growth of the Internet has become a burden to Internet service providers (ISPs), who must constantly build new infrastructure to keep up. This gives ISPs an incentive to monetize their services in such a way, it may violate network neutrality. The net neutrality is a principle that all Internet traffic should be treated equally to protect consumer rights, freedom of speech and to secure unobstructed network access to new innovative services and businesses.

A literature survey studies the most important written sources especially the recently imposed net neutrality regulations by the United States, the European Union and Finland. An interview study is used to examine the current net neutrality situation in Finland and PEST analysis is applied to ensure that all significant macro-environmental factors are taken into account when key trends and uncertainties are identified. The ideas and the information gathered during the expert interviews work as a basis for Schoemaker's scenario planning method, which is used to develop and analyze possible scenarios that may occur in the future.

The US's, the EU's and Finland's regulations are fairly similar and they all guarantee free access to the content of users' choice, and prohibit blocking and restricting users' access. The network management is allowed to ensure an integrity and a security of the networks, and to maintain quality of Internet access service and other communications services. The Finnish regulation is seen to be sufficient by the experts and no net neutrality violations have been found. The scenarios indicate that permissible regulation, will promote new innovation and do not cause excessive burden to ISPs. Problems may arise from interpretation of the upcoming EU law and whether it allows offering new innovative telecommunication services.

Keywords: Net neutrality, Scenario analysis, Internet, QoS.

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Jussi Kivilaakso
Työn nimi: Verkkoneutraliteetti Suomessa
Päivämäärä: 23.11.2015 Kieli: Englanti Sivumäärä: 7+48

Tietoliikenne- ja tietoverkkotekniikan laitos
Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Heikki Hämmäinen
Ohjaaja: TkT Heikki Hämmäinen

Internet on erityisen tärkeä modernille tietoyhteiskunnalle ja se on muuttanut tapaamme kommunikoida ja harjoittaa liiketoimintaa. Internetin nopeasta kasvusta on kuitenkin tullut taakka Internet-palveluntarjoajille, joiden täytyy jatkuvasti investoida uuteen verkkoinfrastruktuuriin. Tämä antaa teleoperaattoreille syyn muuttaa palveluidensa hinnoittelua ja toimintatapojaan niin, että verkkoneutraliteetti on vaarassa särkyä. Verkkoneutraliteetti on periaate, jonka mukaan kaikkea Internet-liikennettä tulisi kohdella tasa-arvoisesti, jotta voidaan suojella kuluttajien oikeuksia, sananvapautta ja uusien innovatiivisten palveluiden ja yritysten pääsyä verkkoon.

Yhdysvallat, Euroopan unioni ja Suomi ovat hiljattain laatineet uusia verkkoneutraliteettilakeja suojellakseen Internetin avoimuutta. Näitä lakeja ja muita tärkeitä kirjallisuuslähteitä käydään läpi taustatutkimuksessa. Suomen verkkoneutraliteetin nykytilannetta kartoitetaan haastattelututkimuksella ja PEST-mallilla varmistetaan, että tärkeimmät ulkoiset tekijät on huomioitu trendejä ja epävarmuustekijöitä tunnistettaessa. Asiantuntijahaastatteluissa kerättyjä ideoita ja tietoja käytetään perustana Schoemakerin skenaarioanalyysille, jonka avulla luodaan ja tutkitaan mahdollisia tulevaisuudessa esiintyviä skenaarioita.

Yhdysvaltain, Euroopan unionin ja Suomen lait ovat samansuuntaisia ja ne kaikki kieltävät tarpeettoman liikenteen ja Internet-yhteyspalvelun estämisen ja rajoittamisen. Verkonhallintaa saa käyttää verkon luotettavuuden ja tietoturvan säilyttämiseksi, kuten myös verkkoyhteyden tai muiden tietoliikennepalvelujen laadun varmistamiseksi. Asiantuntijat kokevat Suomen lainsäädännön riittäväksi ja verkkoneutraliteettirikkomuksia ei ole esiintynyt. Skenaarioiden mukaan sallivat verkkoneutraliteettilait edistävät uusien innovaatioiden syntymistä, eivätkä aiheuta liiallista taakkaa teleoperaattoreille. Ongelmia voi syntyä tulevan EU-lain tulkintatavoista ja siitä mahdollistaako laki uusien innovatiivisten tietoliikennepalveluiden tarjoamisen.

Avainsanat: Verkkoneutraliteetti, Skenaarioanalyysi, Internet, QoS.

Preface

This Master's thesis studies net neutrality in Finland, and is written for an interest of the Department of Communications and Networking, Professor Heikki Hämmäinen and myself.

I would like to thank my instructor Professor Heikki Hämmäinen for guiding me through the thesis and sharing his expertise. I would also like to thank the experts in this field Sebastian Sonntag, Markus Peuhkuri, Janne Holopainen, Mikko Raito, Markku Lamminluoto, Tapio Haapanen and Klaus Nieminen, with whom I had the interviews to complete the project.

I also appreciate all the support I have received from my family and friends during my studies at the Aalto University.

Espoo, 23.11.2015

Jussi Kivilaakso

Table of contents

Abbreviations

4G	Fourth Generation
BEREC	the Body of European Regulators for Electronic Communications
CAP	Content and Application Provider
CDN	Content Distribution Network
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service
DNS	Domain Name System
DPI	Deep Packet Inspection
EU	European Union
FCC	Federal Communications Commission
FICORA	Finnish Communications Regulatory Authority
FTP	File Transfer Protocol (RFC 959)
HTTP	Hyper-Text Transfer Protocol (RFC 2616)
IAS	Internet Access Service
ICT	Information and Communications Technology
IoT	Internet of Things
IP	Internet Protocol (RFC 791)
IPTV	Internet Protocol Television
ISP	Internet Service Provider
LTE	Long Term Evolution
Mbps	Megabits per second
MP2P	Mobile Peer-to-Peer
NRA	National Regulatory Authority
NSA	National Security Agency
OS	Operating System
P2P	Peer-to-Peer
PEST	Political, Economic, Social, Technological (framework)
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
SDN	Software-Defined Networking
SMS	Short Message Service
SONET	Synchronous Optical Networking
TCP	Transmission Control Protocol (RFC 793)
US	United States of America
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

1 Introduction

The Internet is increasingly important to modern information society. The Internet is constantly growing and it has become a ubiquitous platform for information, communication and entertainment. It has changed the way we communicate and do business. Internet Service Providers (ISPs) own and control most of the networks, so they are in a fundamental position. Governments, private sector and individuals are concerned how the ISPs will monetize usage of their networks and services in the future. This concern has started the net neutrality debate. Trying to figure out the net neutrality via the Internet might be complicated, since it is increasingly hard to find the facts behind opinions, discussions and hidden agendas. [1]

In the beginning, the Internet was only a research network between a couple universities, but it had two fundamental design principles which still apply today. End-to-end principle states that application-specific functions should be in the end hosts rather than in routers. The concept of "dumb pipe" means practically the same thing. Best-effort principle states when packets are send through the network, it should be done as fast as possible. Although the end-to-end principle is seen as a precursor to the net neutrality, we must remember that Quality of Service (QoS) has always been a concern for the Internet as well. The QoS refers to the capability of a network to provide a better service to a selected network traffic by either raising the priority of a flow or limiting the priority of another flow. ISPs can increase their profitability and the efficiency of their network by network management, but since it is not distinct how much network management is too much, there will be net neutrality issues. This leads to one of the key questions in the net neutrality debate how much network management ISPs can legitimately use on their networks. [1]

A typical Internet user buys an Internet access from local an ISP with a certain bandwidth. Similarly, this local ISP will buy an access to the entire Internet from a larger ISP in a service called transit. The price of the transit service increases when more data is sent between these two ISPs. Since bandwidth intensive services like video streaming and online gaming are gaining more popularity, the costs of the ISPs are growing. Also the amount of traffic that is carried over wireless networks increases rapidly and building more capacity to the wireless networks is especially expensive. This gives ISPs an incentive to discriminate some traffic flows, and techniques needed for traffic management are already implemented in the networks. What has fueled the net neutrality debate, is the fact, that some ISPs have signaled that they are going to use these techniques to generate more money for their company.

1.1 Research question and objectives

While the net neutrality debate is going on around the world and the amount of Internet traffic is growing rapidly, various stakeholders are eager to defend their own interests. Some ISPs are trying to keep their competitive advantage over others, while other

stakeholders are interested on defending the individual rights and the fundamental design principles of the Internet. This thesis will study the net neutrality in Finland and tries to provide new perspectives through scenarios, which will illustrate the possible futures of the net neutrality debate and the regulation. The main research question is:

- *What is the current situation of the net neutrality in Finland and what net neutrality challenges may appear in the future?*

In order to answer the main research question, following objectives are recognized and must be solved during the research:

- *Study the latest regulatory situation in the US, in the EU and in Finland.*
- *Identify essential stakeholders, key trends and key uncertainties that are related to the net neutrality in Finland.*
- *Identify the two most important key uncertainties during interviews.*
- *Create four scenarios presenting the possible futures.*
- *Analyze and compare each of the scenarios and their value creation.*

1.2 Scope

This thesis gives comprehensive explanation for the net neutrality and will examine if any major net neutrality violations are occurring in Finland. The net neutrality debate started in the United States and the US also tends to give direction to the rest of the world in Internet related issues, therefore the US is studied more closely. Regulation in the European Union should also be studied in detail, since it has major influence on Finland. This thesis will also present technical aspects of the net neutrality, while keeping its main focus on Finland.

A background research will start from the late 1990s, when the first net neutrality issues appeared [2]. The time frame for scenario planning is ten years, which may be relatively long time period, since the regulation concerning the net neutrality is new and may see some changes in the next few years.

1.3 Research methods

The research methods used in this thesis are:

- literature survey,
- interviews, and
- Scenario planning.

A literature survey studies the most significant written academic publications, articles, books and the regulation concerning net neutrality. The literature survey will present the basic knowledge and information from around the world. Expert interviews are used to deepen the understanding and to provide more practical knowledge from the Finnish

Information and Communications Technology (ICT) field. Results of the interviews will provide a basis to the scenario planning and scenario construction.

1.4 Structure of the thesis

The first chapter introduces net neutrality and the thesis to the reader. The second chapter explains research methods, the Scenario planning and PEST analysis, which are applied in the study. The third chapter explains background to the net neutrality debate and it also presents possible challenges. The fourth chapter studies regulation related to the net neutrality in the US, in the EU and in Finland.

The fifth chapter includes expert interviews and explains the current net neutrality situation in Finland. The scenario planning process is applied in the sixth chapter. Also the achieved scenarios are explained and analyzed in the sixth chapter. Finally, chapter seven will conclude the thesis. The structure of the thesis is presented in Figure 1.

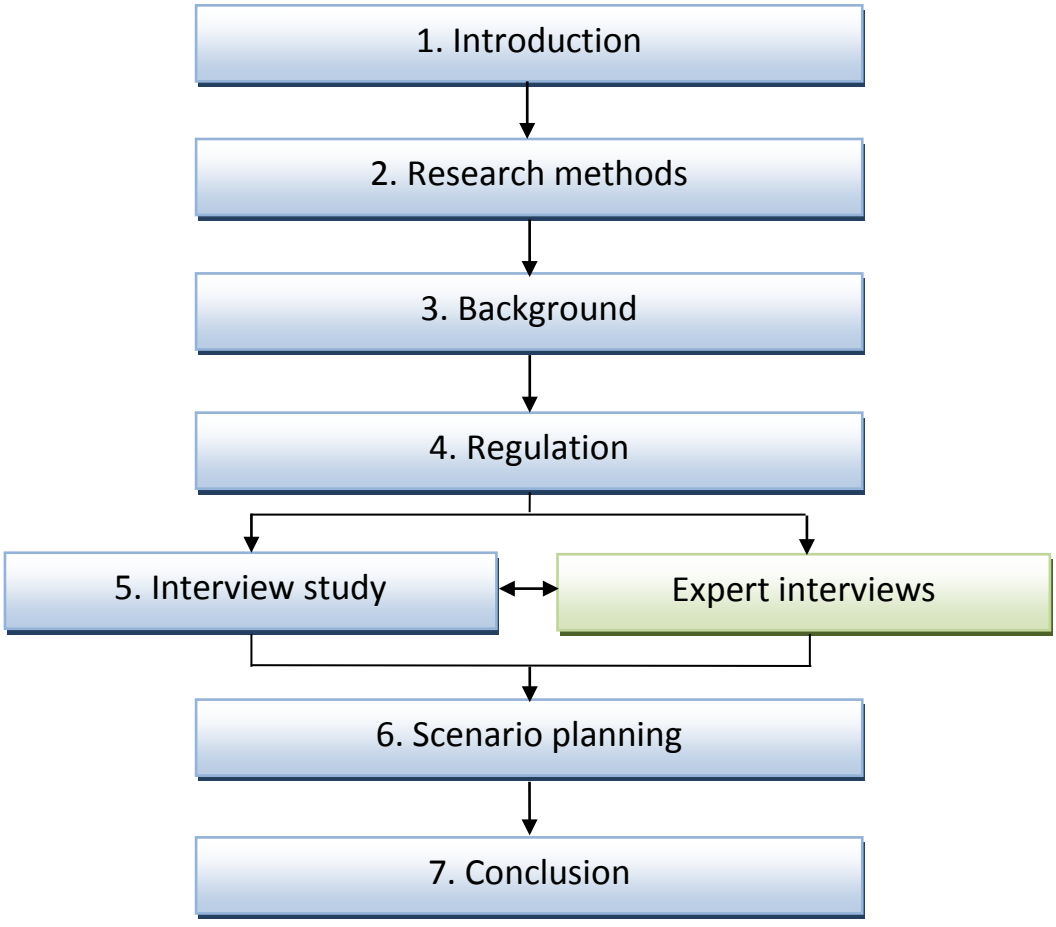

Figure 1: Structure of the thesis

2 Research methods

This chapter introduces research methods to the reader, explains how they are applied in this thesis, and how they are related to each other.

2.1 Scenario planning

Scenario planning is a tool for strategic management and it is used by managers, experts and strategists within organizations. The scenario planning combines various perspectives in order to create possible scenarios besides the generally known forecasts. The scenario planning does not predict the future; it attempts to describe what is possible in complex situations. [3]

Herman Kahn was one of the first that used scenario-based planning in military strategies. In the early 1970s, Pierre Wack transformed scenario planning into business environment and developed a successful scenario planning system to Royal Dutch Shell, which helped Shell to prepare for oil crisis [4]. More recently, scenario planning has been applied in several cases in the ICT field. Heikkinen has used scenarios in his papers to study usage of Mobile Peer-to-Peer (MP2P) services in Finland [5][6]. Smura and Sorri have applied scenario planning to study local area access within mobile services business and Levä made a comprehensive study on the Future Internet evolution in 2009 [7][8].

Scenario planning has an advantage over other planning methods like sensitivity analysis and computer simulations, because it allows you to change multiple variables at the same time, without keeping others constant. Scenarios can also be used to analyze such variables that cannot be specifically modeled by computer simulations, such as new disruptive innovations or value shifts in customer preferences. Scenario planning tries to find a middle ground in decision making, by getting rid of the common mistakes – under- and overprediction of change, tunnel vision and overconfidence. [3]

Schoemaker's comprehensive scenario planning method is chosen to be applied in this study [3][9]. Schoemaker describes the process of developing scenarios as ten step series, but last two steps including quantitative modelling will not be applied in this case. Simplified method is presented in Figure 2. The first step is to define the scope and set the time frame of the analysis. Time frame can depend on a several factors such as technological change. You should assume that even more changes will happen in the future than what has happened in the past. In the second step you will identify major stakeholders and their current roles, interest and involvement. The third step includes finding out what are the key trends and key uncertainties related to the case. In the fourth step you will construct four plausible scenarios by crossing two of the most important uncertainties. Finally, you will check consistency of the scenarios, develop them further and analyze your case with them. [3]

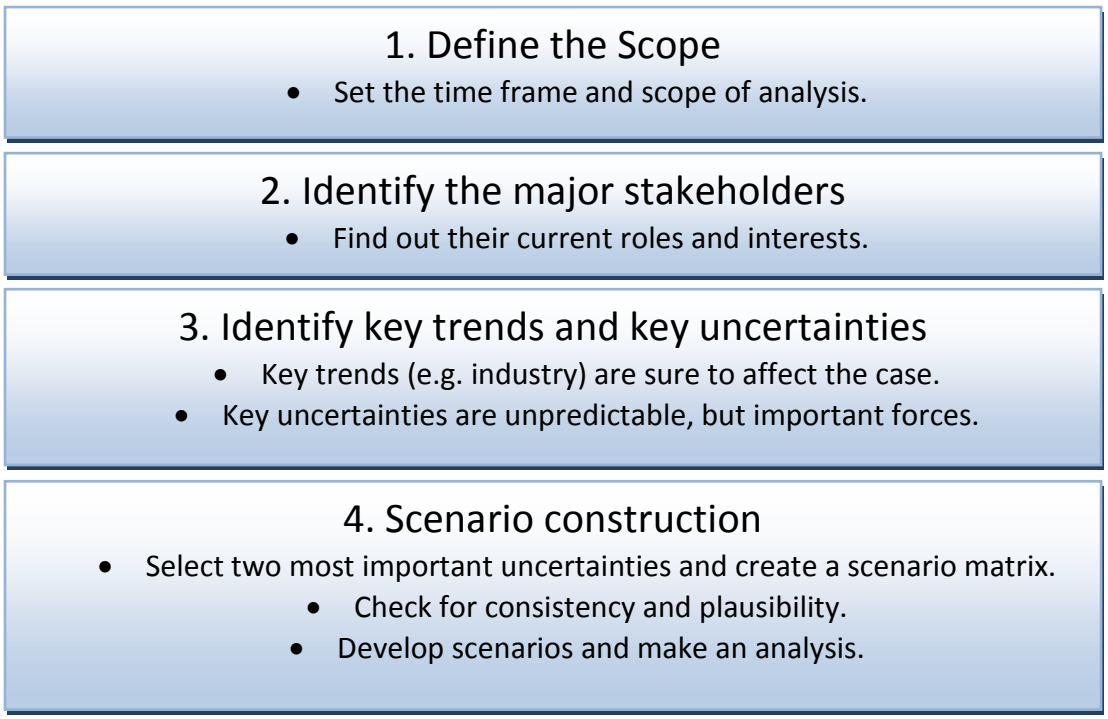

Figure 2: Scenario planning process [3]

2.2 PEST analysis

PEST is a framework of macro-environmental factors that are used to study political, economic, social and technological events and trends which influence an industry or even a global market. The basic PEST analysis includes four factors: Political, Economic, Social and Technological, but also new components like Environmental and Legal can be added to create a PESTEL framework. In this study of the net neutrality the PEST framework is chosen, since the Environmental aspects such as climate and weather does not relate to the study. Also the Legal aspects can be added under Political factors that are basically the acts of the governments and regulatory authorities. The PEST analysis is a useful strategic tool for analyzing different aspects of the net neutrality debate. It is used to identify the key trends and uncertainties for the scenario planning method, and guiding the expert interviews. [10]

2.3 Interviews

Interview is well-known and widely used research method in which researcher attempts to learn what another person knows, feels or thinks about the topic. In this study interviews are conducted face-to-face. Telephone interviews do not provide visual signs of body language or facial expressions, which means you must attend to voice more carefully. Conducting the interview is only one part of the interview-based research. First you must create the questions, decide who to interview and make an extensive back-

ground research. After the interview you need to ensure that your data is correct and only then do the analysis phase. [11]

For a standardized interview questions and order are predetermined. This study uses more open format to gain more in-depth knowledge. In these unstructured interviews conversation is free with a couple of primary research questions, which will change from interview to another. ISPs' interests and knowledge are likely to differ from the regulators'. Interviews are flexible and adaptable to different contexts and will provide insight knowledge that would not be available otherwise. But they also pose some challenges such as an element of unpredictability. Some organizations may not answer all the questions, because the net neutrality is to some extend a political issue or they do not want their motives out in the public. Thus the interviewer-interviewee relationship is important for a successful interview. [11]

3 Background

This chapter presents the background to the net neutrality debate and possible challenges that may appear. Chapter will also present technologies and means to control information networks.

3.1 History

In the 1969, the Internet was only a research network between a couple universities, but it had two fundamental design principles which still apply today. End-to-end principle states that application-specific functions should be in the end hosts rather than in intermediary nodes. This means that the intermediate nodes act individually and do not differentiate packets based on their source or content. Best-effort principle states when packets are send through network it should be done as fast as possible. Packets may take different routes and they are stored in router's queue if they arrive faster than the router can forward them. When the queue gets full packets are discarded and must be resent by the source host. This is the main reason for congestion on the Internet. Although the end-to-end principle is seen as a precursor to the principle of net neutrality, we must remember that Quality of Service (QoS) has always been a concern for the Internet as well. The QoS refers to the capability of a network to provide a better service to selected network traffic over various technologies. The main goal of the QoS is to provide privileged delivery for applications that require it by ensuring a sufficient bandwidth, controlling jitter and latency, and improving loss characteristics. E.g. voice communications requires that the packets are received on time and in particular order (i.e. low latency and low jitter). [1]

The net neutrality debate started in the late 1990s, when Lemley and Lessig published a paper about the possible threats to end-to-end nature of the Internet. They noticed that many cable companies had vertically integrated with ISPs and these cable companies did not allow users to select another ISP [2]. The term net neutrality was first used by law professor Tim Wu in 2003 [12], and it is the principle that ISPs, companies and governments should treat all Internet traffic equally, not discriminating different users, content, services, applications, devices or modes of communication. Wu explains that a neutral public network should deliver most to the world economically, by serving as an innovation platform. Wu also mentions in his paper that many US operators had prioritized their short-term interests over their long-term interests, which had caused a tendency to ban or restrict new innovative applications or network equipment in their networks. Wu thinks laws are most successful when they prohibit harmful acts, therefore net neutrality laws should prevent behavior that creates profits for the ISP, but has negative effects for the economy and the country. [12]

Bandwidth intensive services like streaming media and online gaming are gaining more popularity. Globally, the video traffic (TV, Internet, Video on Demand (VoD) and Peer-to-Peer (P2P)) will be around 85 percent of consumer traffic by 2019 [13]. The Internet

traffic increased 26% percent last year and is expected to grow 23% annually in the next five years [13]. Also the amount of consumers and number of devices are growing. To avoid congestion ISPs have to invest heavily in their networks. These investments are periodical and cause overprovisioning. This is a relentless cycle that the ISPs are trying to avoid. At the same time content providers are benefitting from the increased traffic in the customer access networks. Network infrastructure vendors like Cisco, Nokia and Huawei are constantly improving the efficiency of their hardware by creating new multiplexing methods in such a way that the costs per unit of a bandwidth are decreasing. This slightly reduces the costs of the ISPs when they are upgrading their networks. [1]

A typical end-user buys Internet access service (IAS) from local an ISP to gain access to the whole Internet with a certain bandwidth. Likewise, this local ISP buys an access to Internet backbone network from a higher tier ISP in a service called transit. The transit cost is based on a reservation of a bandwidth, thus the increasing traffic volumes will cause more costs to the local ISP. ISPs and/or content providers may also have peering arrangement with each other. Peering is a service where two interconnection networks agree not to charge each other for the exchanged traffic. The cost of consumers' IAS depends crucially on the number of competing ISPs in the area. Some end-users that face a local monopoly or duopoly have exceedingly high IAS costs. Content and Application Providers (CAPs) are not bound to any specific location and have therefore negotiated relatively cheap Internet access contracts. [14]

The net neutrality debate heated up in 2005 when Ed Whitacre, the CEO of AT&T stated that they need payments from the content providers or he will not let the content providers use their networks for free. For this reason AT&T, Verizon and cable TV companies are asking for removal of the net neutrality. CAPs are not interested of paying extra without any additional benefit. This would lead to a situation where ISPs are offering faster access lanes to their customer CAPs for an additional payment. If some CAPs started paying extra, they would lose their bargaining power. This arrangement would inevitably lead to higher payments and slowing down those CAPs who do not pay. Smaller companies could not compete with giants like Google and Facebook. This would result in monopolized markets and reduction of innovations. [1][14]

3.2 Traffic management

Another main concern related to the net neutrality is ISPs' ability to use various traffic management techniques to limit unwanted traffic. They can prioritize, degrade or even block certain traffic flows, to distort competition or to maximize their profitability. But not all traffic management is counterproductive, ISPs use traffic management to increase efficiency of their networks and to protect their networks' security and integrity. They also manage applications that need higher Quality of Service to work properly (e.g. video conferencing).

3.2.1 Quality of Service

Conventional routers and switches work on a best-effort basis. More complex QoS tools allow you to provide a better service to selected network traffic over different technologies, such as Frame Relay, Ethernet, SONET and IP-routed networks. This can be done by prioritizing a traffic flow over another or reducing the priority of some other flow. Real-time streaming multimedia applications like Voice over IP (VoIP) and IPTV require low latencies and fixed bitrates to work properly. Different QoS mechanisms can be used to guarantee these features. The QoS tools can also mitigate most congestion problems, but sometimes traffic volumes are too high in the network and the only solution is to buy more capacity. [15]

The QoS implementations have various tools. Classification tools are used to identify and optionally mark traffic flows for the use of other QoS tools throughout the internetwork. Congestion management tools queue and manage flows in different ways to offer a desired treatment to a certain flows. Congestion avoidance is handled with queue management tools that prevent a queue from filling. When the traffic comes in bursts that exceed the speed of a link, queue management drops low-priority flows and allows high-priority flows enter the queue. Traffic Shaping and Policing is used to prevent overflow problems by limiting the bandwidth that a flow uses. Shaping buffers traffic above the configured rate for later transmission, while Policing simply discards exceeding traffic. Link efficiency tools are used to mitigate experienced delay for time-sensitive flows. This is done by fragmenting and interleaving packets. Also header compression is used to reduce the overhead. [15]

3.2.2 Content distribution networks

While QoS is purely a technical concept that is used to manage network services and interactions between applications, Quality of Experience (QoE) is solely a subjective measure for overall perceived user value of particular service [16]. When end-users experience delay due to congestion in the network, they will probably associate the low quality directly to the content provider's service. Therefore, content providers are interested to improve their QoE for the end-user. The QoE can be improved by using the QoS tools mentioned earlier or by using a Content Distribution Network (CDN).

The CDN distributes the contents from an origin server to strategically placed cache servers, which are located closer to the end-user. This shortens access delays and reduces bandwidth consumption. CAPs are willing to pay for the commercial CDNs to improve their delivery and host their webpages. Some big companies like Google and Netflix have even build their own CDNs. The CDNs can be found in the CAP's own network, in mobile base stations, at internet exchange points, and in the ISP's customer access networks. The ISPs are willing to cooperate with the CAPs, since they are reducing transit costs and improving the QoE. [17]

CDNs offer own lanes to certain traffic which violates the basic principle of the net neutrality. Also the net neutrality proponents argue that large CAPs can pay for better quality service than other content providers. But, the market for the CDNs is seen as competitive and it is unfair to intervene the market system itself. The tough competition and cooperation between the firms have only increased the consumer benefit. The CDNs also enable the increasing use of the video traffic and congestion problems would be inevitable without them. Other thing to notice is that the current net neutrality regulation does not apply to the interconnection market. [18]

3.2.3 Deep packet inspection

ISPs can use traffic management to limit or block traffic flows that are seen to create unwanted costs. There have been a few net neutrality violations in the past. The first example is Comcast, the second largest ISP in the US that restricted P2P traffic in 2007 and 2008. In P2P technology users share large files like music, movies and games to each other and the ISPs cannot really monetize this traffic. Even though the Comcast stated that they do not block access to any applications, they blocked and restricted uploads in P2P network. The Federal Communications Commission (FCC) decided to sanction Comcast for unfair treatment of the P2P users, but the US Court of Appeals later overruled FCC's decision, since the FCC did not have regulatory power to stop ISPs network management practices at the time. [19][20]

Comcast had implemented a Deep Packet Inspection (DPI) technique Sandvine Policy Traffic Switch model 8210 in its network. The Comcast's DPI implementation disrupted P2P protocols Ares, BitTorrent, eDonkey, FastTrack and Gnutella. The DPI is mainly used to monitoring and traffic shaping. It can identify applications being used in the network, protect against Distributed Denial of Service (DDoS) attacks and even scan for viruses being sent through the network. Some techniques can go even deeper to look inside all traffic from particular IP-address and reassemble e-mails that are sent by the user. Many major ISPs in both US and Canada had started using DPI implementations, and none of them notified customers or regulators and this led to publicity, litigation and major regulatory proceedings. After the public confrontation traffic management was scaled down drastically in the US, even there was no applicable regulation. Canada's system had a stronger regulation against this kind of disruptive behavior, but they still left the DPI usage unchanged. [21][22]

In the Europe, British ISP Plusnet uses DPI to divide end-user data streams to different priority classes, which is a violation of the net neutrality. If you don't have the highest priority connection your online gaming and VoIP experience will suffer. Also the P2P and File Transfer Protocol (FTP) usage is limited during the peak periods. Even if the traffic is prioritized in this manner customer satisfaction is claimed to be great. The people who do not use VoIP or play online games, don't need to pay as much for their internet connection as the heavy users. [21][23]

Although the DPI can be used to violate the net neutrality, it is widely used by most of the ISPs to examine traffic in order to prevent security threats. From 2008 to 2010 the US ISPs test positive for the DPI usage 11% of the time, while the Canadian ISPs test positive 33% of the time [22]. The worldwide usage of DPI to detect and limit the P2P application BitTorrent has been on downward trend between 2009 and 2012. In the second quarter 2009 DPI usage was 24% and in 2012 the DPI usage to throttle BitTorrent was only 15%. [24]

3.3 Challenges

It is problematic to distinguish what can be considered reasonable network management and what violates the net neutrality. The European Commission lists net neutrality challenges in Digital Agenda in the Europe 2020 initiative:

- *Unfair traffic management*. Blocking and throttling (i.e. slowing down the speed) P2P services, VoIP services, gaming or streaming.
- *Weakening the competition*. When ISP provides traditional voice calls in PSTN networks, the access to cheaper or even free VoIP calls offered by competitor may be limited.
- *The decrease of innovation*. CAPs may reduce investments into new services or applications, if ISPs are likely to discriminate against them. Also, ISPs may reduce development and innovation of their own services and applications, if they can just block the competitors out of the market.
- *The potential degradation of QoS*. Congestion may cause degradation of the IAS as a whole or the QoS of particular applications (P2P or VoIP) may be degraded.
- *Privacy issues*. ISPs may access IP packet header information to route the packet through a slower or a faster link. The ISPs can also use even more intrusive method called the DPI to access data within the packet.
- *Lack of transparency.* ISPs tend not to tell what kind of traffic management practices they use. Also, some consumers have little awareness what kind of quality they can expect from their IAS.
- *Threats to quality levels.* ISPs want to avoid network congestion, but they also have to prioritize video services to provide a sufficient quality to the end-users.
- *Insufficient fast broadband coverage.* Only 50% of the population in the Europe have IAS at speed of 30 Mbps or higher. The EU target is that every citizen has an access to a fast broadband by 2020. [25]

The Body of European Regulators for Electronic Communications (BEREC) discusses two more possible threats in their net neutrality positions:

- *Security and Integrity.* Techniques for managing traffic should be implemented carefully by the National Regulatory Authorities (NRAs). Implementations should not degrade network security or integrity.

- *Intentionally degrading the IAS.* Prioritization may give an incentive to degrade the best effort IAS in order to get ISP's customers to pay more from higher quality service. [29]

4 Regulation

In competitive industries we need laws to maintain market competition by regulating the anti-competitive conducts made by companies. The net neutrality regulations are fairly new and may face some changes over time. In this chapter we take a closer look to a regulatory situation in the US, in the EU and in Finland.

4.1 United States of America

The FCC regulates communications in the United States, and it is an independent agency of the US government. The FCC supports net neutrality and FCC's rules and policies have protected the open Internet over a decade. It has been seen that the open Internet supports American economy and allows citizens to communicate, educate and entertain themselves. In 2005, the FCC launched its open Internet principles, which guarantee consumers to have a freedom to use their Internet connections to access any content or use any application. In 2010, the FCC adopted the open Internet rules to protect and promote innovation and investment on the Internet. [26]

In 2015, the FCC adopted new more comprehensive rules to protect free expression and innovation. The new rules apply to both mobile and fixed broadband service. The FCC also reclassified broadband IAS as a telecommunications service under Title II, to gain broader regulatory power. The bright line rules will ban practices that are known to violate net neutrality:

- *No blocking*: ISPs may not block access to legal content, applications, services or non-harmful devices.
- *No throttling*: ISPs may not degrade Internet traffic on the basis of content, applications, services or non-harmful devices.
- *No Paid Prioritization*: ISPs may not favor some lawful Internet traffic over other lawful traffic.

The rules also promote greater transparency and ensure that ISPs can manage the technical and engineering aspects of their networks. These can include preserving security of the networks, optimizing overall network performance and maintaining QoE for consumers. ISPs have the ability to act as gatekeepers between edge providers and end-users, therefore FCC's rules also prohibit unreasonable interference or unreasonable disadvantage to edge providers or end-users. The FCC's order does not apply the open Internet rules to the interconnection market. The rules apply only to a last-mile IAS. [26]

The FCC's rules have an exception for specialized services. These data services may be offered by the ISP like VoIP calls or energy consumption sensors, but these so called specialized services do not offer Internet access. The open Internet rules do not directly apply to the specialized services, but the FCC will reserve the authority to take action if any of these services are used to evade or violate net neutrality. [26]

The United States and the European Union have different regulatory environments and are also remarkably different as market places. In the United States the consumer choice for the ISPs is limited in some areas, while the EU has multiple different ISPs in each country. That is why the ISPs in the US compete in the networks and platforms, while the ISPs in the EU compete in services. [27]

4.2 European Union

In the European Union, BEREC serves as an advisor for the European Parliament, the Council and the Commission in the electronic communications field. BEREC's objective is to develop with the NRAs regulatory best practices, methodologies and guidelines for the EU. BEREC will also assist NRAs in the regulatory field, delivering recommendations and providing advice in the electronic communications sector. [28]

BEREC sees the net neutrality as a principle that all Internet traffic should be treated equally on best effort basis. Increasing mobile traffic may lead ISPs to take measures to manage their networks. To BEREC the most important question in the net neutrality debate is how much network management ISPs can legitimately use on their networks. The BEREC has found that application-specific limitations are not broad in extent, but more blocking and throttling occurs in the mobile networks than in the fixed networks. More than 20 percent of the mobile Internet users in the Europe have some restrictions in VoIP services. Also some mobile operators use data caps and variety of billing policies to control their subscribers. [29]

BEREC has also done a research on interconnections between the ISPs. The interconnection market consists of transit and peering contracts that ISPs create to be able to send traffic to each other at the backbone level of the Internet. There has been a few interruptions in the interconnections, but they have been solved quickly and without regulatory intervention. If end users cannot reach all the destinations on the Internet, it is a violation of the net neutrality. BEREC states in its response to the European Commission that interconnection arrangements between the ISPs are not directly related to the net neutrality, and since all traffic flows are treated equally net neutrality violations should not appear [30]. [29]

ISPs can increase efficiency and profitability by network management, but it is not distinctive how much network management is reasonable. Practices will probably be considered reasonable, when some restrictions apply and their advantages clearly surpass their disadvantages. BEREC has proposed following guidelines to evaluate the situation:

1. *Non-discrimination between stakeholders.* The service is provided by non-discriminatory manner between all content and application providers.
2. *End-user control.* Traffic management practices that end-users can control is an important indicator of reasonableness, and often seen more reasonable than measures taken unilaterally by the ISP.

3. *Proportionality.* The network management practices should have legitimate aim, with an objective justification (i.e. NRAs should impose measures that can fulfill their objectives efficiently with minimal side effects.)
4. *Application agnosticism.* ISPs should not use congestion management to degrade a specific application, if application-agnostic methods can be used instead. The application-agnostic methods treat all IP packets from all applications similarly while application-specific functions treat applications differently (e.g. VoIP or P2P is throttled while other applications are not). [31]

BEREC also gives guidance how NRAs can create proportionate and effective policies to support net neutrality. NRAs should stimulate market forces with regulation at wholesale level. When ISPs face competition at the IAS market, they will have less incentive to degrade the quality of their own services. Competition should keep ISPs in line and end-users would get cheaper IAS. This can only work when end-users are fully aware of the ISPs' prices. BEREC is promoting effective transparency that ensures the price information is accessible, understandable and accurate. The average download and upload speeds in comparison to maximum download and upload speeds should be provided as well. End-users will not benefit from greater transparency, unless they can easily switch ISPs to exercise their consumer power. This may be an area of potential concern and BEREC will be conducting further assessment of switching conditions and user behavior. [29]

NRAs are recommended to monitor quality of the IAS offers over time to detect degradations. The whole IAS may be degraded or the traffic may be prioritized unevenly (e.g. specialized services are provided at the expense of the IAS) or throttling and blocking are degrading individual applications. NRAs should take into account market conditions and behavior of the ISP. When dealing with unrestricted IAS offers, it is important to take network effects into account. The unrestricted group is not able to use all the applications to communicate with the other group that has a restricted Internet access. [29]

When market violations appear, NRAs should handle the situation with the most suitable regulatory tools. If switching to another ISP cannot be done easily, ex-ante regulatory tools may be sufficient response, such as enhancing transparency, competition and ease of switching. If these measures does not solve the issue, NRA can impose minimum QoS requirements. The NRA can force ISP to improve the QoS until the degradation is eliminated. When some specific applications are being throttled or blocked, NRA can just prohibit those restrictions. [31]

4.2.1 Specialized services

BEREC clearly distinguishes an Internet access service and specialized services from each other and its guidelines focus specifically on the Internet access service. An IAS is a service that provides connection to the public Internet, while specialized services are electronic communications services that are designed to provide some specific characteristics such as end-to-end quality or availability. Therefore, specialized services will

rely on extensive use of traffic management and access restrictions. IAS and specialized services are provided over distinct networks, but typically these networks are utilized over the same physical infrastructure. [31]

In the Europe, 35% of the fixed ISPs use traffic management techniques to offer specialized services in a way that the capacity is provided at the expense of IAS. In these cases specialized services should be taken to a closer attention of NRAs. The national situation vary greatly: in some countries none of the ISPs offer specialized services, while in others countries all of the ISPs offer specialized services side-by-side with the IAS. VoIP, IPTV and VoD are the most common specialized services offered in these countries. [32]

4.2.2 Upcoming EU law

On the 30th June 2015, The European Parliament, the Council and the Commission agreed on EU-wide rules on net neutrality. The proposal of the European single market for electronic communications has seen numerous amendments and it will come into effect on 30th April, 2016. The proposal guarantees free access to the content of users' choice, it prohibits blocking and slowing down of their access, and bans paid prioritization. Reasonable network management is allowed to:

1. Preserve the security and integrity of the network.
2. Minimize temporary network congestion.
3. Comply with national legislation related to illegal content or criminal law.

These exceptions must interpreted strictly and otherwise all traffic should be treated equally. The new policy allows existence of specialized services that can be offered to consumers with higher priority, if it is not done at the expense of quality of the open Internet. The Commission gives tele surgery, video conferencing and IPTV as examples of specialized services. The proposal also bans discrimination against encrypted traffic. Even if ISPs cannot classify the content of the encrypted traffic, it does not deserve unfair treatment. The regulation gives NRAs a freedom to choose whether or not allow zero-rating in their countries. [33][34]

4.3 Finland

The regulator in Finland is the Finnish Communications Regulatory Authority (FICORA) and it operates under the Ministry of Transport and Communications. FICORA regulates radio frequencies and television broadcast permits, and manages the .fi domain name. FICORA ensures that every citizen in Finland has access to the basic communications services that are required by law. FICORA also provides information about possible data security threats and supervises operation of ISPs. [35]

FICORA has same point of view to the net neutrality as BEREC. In BEREC's and FICORA's opinion the best practices arise most certainly when markets work efficiently.

This happens when users have possibility to change service providers and markets are transparent. In case of violations regulator must have a way to intervene. FICORA emphasizes that network management is needed to get rid of the congestion problems and guaranteeing network security and the QoS. [36]

FICORA has also remarked that the Internet ecosystem and value networks between ISPs and CAPs are changing. One important factor is ever growing need for bandwidth. In recent years increase in bandwidth consumption has been due to P2P applications and video services, and the capacity issues are especially related to mobile networks. [36]

FICORA states that exceptions are needed to perfect net neutrality. Network management is a necessity for various reasons. ISPs have to monitor and shape traffic by prioritizing, restricting or blocking, in order to offer and develop functional and secure services, maintain IP-networks, be profitable and to fulfil authorities' needs. Some ground rules should still be put in place, so consumers' rights are not restricted without a reason or IPSs won't get unjustified competitive advantage over content providers. [36]

4.3.1 Finnish net neutrality law

In November 2014, the Finnish Parliament confirmed new Information Society Code regulation. The Information Society Code combines all old and new rules and laws related to the electronic communications. The regulation will improve consumer protection, in addition it pays particular attention to protection of privacy and information security. The regulation consists of 350 sections and one of them, section 110 §, concerns net neutrality. This section came into effect on the first of July, 2015. [37]

The Information Society Code states that an ISP cannot restrict a subscriber or a user to use an IAS, except:

1. To implement the essential quality features of an IAS, data transfer rate range or other services that are defined in the communications service agreement;
2. Based on the decision of the authorities or the court;
3. Ensuring information security or to correct interruptions in a way provided in sections 243, 272 and 273 or other similar way provided by law;
4. To fulfil quality requirements of a communications network or an IAS, that are defined in sections 243 and 244.

These restrictions shall be implemented in a non-discriminatory manner and shall not:

1. Limit the intended use of an IAS;
2. Prohibit or restrict a subscriber's or user's ability to use applications and services they wish;
3. Unreasonably slow down the IAS.

An ISP must also ensure that the customer has an access to sufficient information about the possible effects these restrictions stated above may have on the service. FICORA

may issue further regulations to secure sufficient availability and quality of an IAS. FICORA may also decide to oblige the ISP to carry out procedures to prevent interruptions or to refrain from the use of the procedures and restrictions that may cause interruption. Finally, FICORA must take into account the general quality, prices and service features of the IASs available to users, when issuing regulations and orders. [37]

4.3.2 Other regulation

Finland has recently updated two relating electronic communications laws that are explained here. In 2010, Finland became the first country in the world to rule that every resident is entitled to 1 Mbps broadband subscription to home or place of business. This universal service subscription can be fixed or wireless. FICORA has named ten tele operators to fulfil this duty. Seven small ISPs are only obligated to offer subscription in one or two municipalities, while the three biggest ISPs TeliaSonera Finland Oy, Elisa Oyj and DNA Oy are obligated to offer an IAS in 185, 75 and 36 municipalities accordingly. The decree of Ministry of Transport and Communications will be raising the speed of the universal service broadband subscription to 2 Mbps and this degree will take force in the first of October 2015. [38][39]

Attacks against information networks are growing globally and are often linked to organized crime. This constitutes a threat to a modern information society, and, in particular, to freedom, security and justice. Therefore the European Union has created a Directive 2013/40/EY to establish more comprehensive rules against identity thefts, creation and usage of botnets and cybercrime in general. The Directive will also improve cooperation between authorities, including police, law enforcement services of the member states, Eurojust, Europol, European Cyber Crime Center and the European Network and Information Security Agency. [40]

The Finnish Government has proposed HE 232/2014 regulation to put in force the EU's so called Information System Criminal Directive. The regulation will criminalize identity thefts, and perpetrator can be sentenced e.g. from defamation, fraud, forgery or falsification of the personal information. Ticket being the maximum penalty from the identity theft. The perpetrator could be sentenced to jail for maximum of two years from data breach, violation of communications secrecy or hacking. If data breach, disruption of information systems or telecommunications networks is done using botnets, as part of organized crime or if it has been targeted to an essential infrastructure, the offender can be convicted to jail for maximum of five years. The regulation will take force in the fourth of September, 2015. [41]

Although too much regulation is seen counterproductive, regulation is essential in problematic cases i.e. when someone is breaking the law. Companies do not want government to intervene competitive markets, so they can gain the maximum benefits. But when someone is misusing their market power or someone else is doing malicious activities, the government is suddenly needed to correct things. [42]

4.4 Comparison of the net neutrality laws

To summarize the fourth chapter differences of the net neutrality regulation between the US, the EU and Finland are compared in the Table 1.

Table 1: Differences in the net neutrality regulation

	United States	European Union	Finland
Prohibits:	Blocking	Blocking	Blocking
	Throttling	Throttling	Throttling
	Paid Priorization	Paid Priorization	
	Unreasonable disadvantage	Discrimination of encrypted traffic	
Network management is allowed to:	Preserve the security and integrity of the network	Preserve the security and integrity of the network	Preserve the security and integrity of the network
	Optimize overall network performance	Comply with national legislation	Comply with national legislation
	Maintain QoE for consumers	Minimize temporary network congestion	To implement the essential quality features of an IAS or a communications network
			Correct interruptions
Specialized services are:	Allowed	Allowed	Allowed
Zero-rating is:	Allowed	Left NRAs to decide	Allowed
Applies to:	Fixed and mobile	Fixed and mobile	Fixed and mobile
Length of the regulation:	400 pages	49 pages	1 page
Valid from:	26.2.2015	30.4.2016	1.7.2015

5 Interview study

The fifth chapter describes the current net neutrality situation in Finland. It introduces the most important stakeholders, it describes how interview study was made and what the findings were. The results from this chapter will also serve as a basis for the scenario planning.

5.1 Stakeholders

Various stakeholders are motived to influence the net neutrality debate in the Internet. These stakeholders include end-users, network infra vendors, content & application providers, commercial ISPs, backbone ISPs, governments & regulators, standardization bodies and research institutes. In the study of the net neutrality in Finland the most relevant to interview are:

- Research institute: Aalto University
- Content provider: YLE
- Regulator: FICORA
- Commercial ISPs: Elisa, TeliaSonera and DNA

To be noted Elisa, TeliaSonera and DNA are mobile operators and content providers/distributors, and TeliaSonera is also a backbone Internet operator. TeliaSonera also offers budget mobile services in the form of another company, Tele Finland Oy.

5.2 Expert Interviews

Interviews were used as a part of the research to gain more in-depth knowledge and opinions on the net neutrality situation in Finland, which wouldn't have been available otherwise. Interviews were conducted between 25th of August and 30th of September, 2015 in Espoo and Helsinki. List of interviewees is presented at the Table 1 and the question list can be found in the Appendix A. Interviews were conducted using unstructured format, therefore questions had some variation based on the interviewees' expertise and organization, and discussion was free during and after the interview. The interviews and discussions were conducted in Finnish.

Table 2: List of interviewees

Name	Title	Organization
Sebastian Sonntag	Doctoral Candidate	Aalto University, Department of Communications and Networking
Markus Peuhkuri	Laboratory Manager	Aalto University, Department of Communications and Networking
Janne Holopainen	Media Regulation Manager	YLE, Finnish Broadcasting company
Mikko Raito	Legal Counsel	Elisa Oyj
Markku Lamminluoto	Senior Advisor	DNA Oy
Tapio Haapanen	Development Manager	TeliaSonera Oyj
Klaus Nieminen	Communications Network Expert	FICORA

5.3 Findings from the Interviews

The interview study succeeded to provide additional information about the Finnish net neutrality. Following sections will present key findings from the topics that are not yet explained in the thesis.

5.3.1 Regulation

The Finnish net neutrality regulation is seen to be well-written, compact and precise. It is balanced to cover needs of end-users, ISPs and CAPs. The Finnish regulation does not prohibit specialized services or zero-rating, therefore ISPs can offer differentiated services and subscriptions to consumers. Consumers have various needs and it is their benefit the more services are available to match their demand.

The upcoming EU regulation will abolish the Finnish net neutrality section from the Information Society Code, as well as other contradictory regulation. When the EU regulation comes in force all EU countries must follow it. If some cases are not covered in the law, the next policy to obey is BEREC's guidelines, and after that NRA's rules. The BEREC is preparing new guidelines to explain details that the EU law does not clarify.

The current proposal does not clarify how network monitoring should be done by the NRAs, but it clearly states that authorities have obligation to examine ISPs' traffic management practices and provision of specialized services. The EU proposal allows exist-

ence of specialized services, if they are offered without deteriorating the quality of Internet access.

5.3.2 Network management

Traffic prioritization and restrictions with a reasonable cause are not generally seen as net neutrality violations. While blocking and degrading competitors' services to gain competitive advantage and asking for surcharge from a specific competitor's service (e.g. Skype) are seen as net neutrality violations. It is seen that the network management is needed to ensure the quality of customer access networks.

In 2004, DPI was used in Finland and since then it has been on downward trend. In 2008, DPI was hardly used anymore and since 2010 DPI usage has been practically nonexistent. Some P2P restrictions have been used in the past, but those restrictions are relinquished years ago. In 2012, Helsinki District Court ordered that ISPs Elisa, TeliaSonera and DNA have to block access to The Pirate Bay due to music and movie copyright infringements. This was executed so that the domain names used by The Pirate Bay were removed from Domain Name System (DNS) and access was blocked to The Pirate Bay's IP-addresses. Several domains that contain illegal content have also been removed from the DNS servers and access is denied to those IP-addresses. ISPs also block port 25 to reduce the amount of spam that is sent from their networks. Generally the email spam is blocked by the email service provider.

Zero-rating means that customers with limited data plans don't get charged for data consumption by the specific applications or services possibly provided by the ISP. This way ISP can direct consumers to use its own services or some other specific services. Regulation concerning zero-rating is still open and thus far it is allowed, but different zero-rating implementations will be regulated in the future. Some interviewees saw zero-rating as a problematic issue, but we must note that the most of the new mobile subscriptions in Finland do not have data caps and fixed broad bands have never had data caps. Elisa offers post- and pre-paid mobile subscriptions only with unlimited data [43]. DNA offers unlimited data plans to all post-paid subscription, and one pre-paid with data cap [44]. TeliaSonera has one data capped post-paid mobile subscription, while most of them being unlimited as well [45]. Finland differs from the other EU countries not only by the amount of unlimited data plans, but also by offering primarily post-paid subscriptions. Finland has also the highest mobile data consumption in the world [46]. Company mobile subscriptions have higher priority in the network than consumer mobile subscriptions, thus company subscriptions are offered with a higher price. Also, corporate VPNs have slightly higher priority in the networks, but overall there are relatively little prioritized network traffic in Finland.

One interviewee stated that a network is never unbiased. Some people live in the urban environment and other in rural areas. Networks will inevitably have larger capacities and lower latencies in the urban areas, since it is more expensive to upgrade base stations in the rural areas. The challenges concerning networks in the future are related to

the mobility and mobile networks. Also intensive data monitoring in Sweden is seen problematic, since some of the Internet traffic that originates inside Finland and end ups back in Finland circulates through Sweden. This endangers privacy of the Finnish companies and consumers.

Overall, the net neutrality in Finland is seen to be in advisable shape. There has not been any net neutrality infringements in Finland, and it is important to prevent them from occurring in the future.

5.3.3 Other observations

The Finnish net neutrality law is only one page long, thus it is more understandable than the upcoming EU law. The EU law document also includes new roaming regulation that will introduce cheaper roaming prices when you use phone or data services in another EU country. Most of the experts see the upcoming EU regulation as the largest uncertainty in the whole net neutrality debate. Zero-rating was the only other uncertainty that was mentioned more than once. But as noted above, the Finnish ISPs do not offer zero-rated services and the Finnish mobile broad bands have unlimited data. Therefore, zero-rating cannot be taken into account in Scenario planning as one of the most important uncertainties.

Every expert viewed that the Finnish net neutrality has no problems and it is more than likely that the Internet stays open for the next ten years in Finland. This is probably the reason there has not been public net neutrality debate in Finland. In the US cable and IP compete with each other as platforms and ISPs in the US have violated the net neutrality in the past. Thus the FCC received more than 4 million comments on its net neutrality proposal.

Lots of single observations were also listed during the interviews, which are elaborated in this paragraph. Backbone networks do not have congestion, but the networks between continents and mobile networks may become bottlenecks in the future. It is also important to mitigate malicious traffic in the networks. This is done with automatic monitoring systems, which have triggers for certain harmful lists. If the amount of traffic of the specific end-user decreases or increases significantly, it is detected by the ISP or the regulator. The network management can be done when the threat is active. It is not the ISP's benefit to intensively monitor the customer, they would rather focus on business activities. The network management has the highest priority in the network, and the speech is prioritized over the video traffic.

6 Scenario planning

In this chapter industry trends and possible uncertainties are analyzed and the Scenario planning method is used to construct the scenarios. The two most important key uncertainties are chosen to create a scenario matrix. Scenarios will be analyzed at the end of the chapter.

6.1 Key trends

The initial key trends and key uncertainties were collected during the expert interviews. The PEST framework was used as part of the first question to collect important macro-environmental factors from Political/Legal, Economic, Social and Technological stand points. The importance of possible uncertainties were discussed later in the interviews. All identified factors are listed in the Appendix B.

Key trends are forces that have high influence on the future of the industry and the current strategy of the organizations. The scenario planning's objective is to identify essential futures of the net neutrality situation in Finland in the next ten years. The final key trends are assumed to be valid in this time frame and they are presented in the Table 3. The trends are categorized based on the PEST framework and each trend is briefly explained.

Table 3: Key Trends

Political/Legal trends
PT1: Too strict regulative measures are detrimental for an economy.
PT2: The EU and the US are different as market places.
PT3: Everybody has a legal right to 2 Mbps broadband in Finland.
PT4: The Finnish law does not prohibit offering subscriptions with extra services.
PT5: The Finnish net neutrality law is seen to be sufficient and well-written.
Economic trends
ET1: Demand for many different services.
ET2: Netflix causes one third of traffic.
ET3: Internet services are important for modern information society.
ET4: Intensive competition in Finland. 3 large operators.

Social trends
ST1: Need for privacy and security.
ST2: Increasing usage of social networking sites.
ST3: People are online all the time.
ST4: Intimidation with net neutrality threats.
ST5: It's consumers' benefit to have multiple different services to choose from.
ST6: Net neutrality regulation protects consumers.
Technological trends
TT1: Prioritization is needed in the Internet.
TT2: Mobility increases.
TT3: Everything is top of HTTP.
TT4: No net neutrality infringements in Finland.
TT5: Internet of Things.
TT6: ISP cooperation.

6.1.1 Political/Legal trends

- **PT1: Too strict regulative measures are detrimental for economy.** The open Internet has been important for new innovative business models and services that have needed special treatment in form of the network management. In other industries, governments' measures of protectionism such as tariffs and important quotas have been seen to contrast with the free trade in general. Therefore, regulative measures should be balanced, and should not reduce consumer welfare or be counter-productive.
- **PT2: The EU and the US are different as market places.** In the US, consumer choice for a last-mile ISP is limited in some areas and the customers are facing monopolistic markets. Also, some cable companies are reluctant to offer high-speed broad bands to their customers, since streaming services like Netflix may reduce number of their cable TV subscribers.
- **PT3: Everybody has a legal right to 2 Mbps broadband in Finland.** It is required by law that everyone in Finland can have an Internet access to their home or place of business. Building networks to remote areas is expensive to the ISPs

and they will not get their capital expenses covered by only a few customers in those distant areas.

- **PT4: The Finnish law does not prohibit offering subscriptions with extra services.** More diversified mobile subscriptions with services like IPTV are not prohibited. Also zero-rating is allowed in Finland. But, if some of the acts made by the ISP is seen even slightly to violate net neutrality, it could lead to a situation where customers will switch to a competitor.
- **PT5: The Finnish net neutrality law is seen to be sufficient and well-written.** The current regulation prohibits malicious activities in the networks and allows necessary network management, and the law is not counter-productive to companies or economy.

6.1.2 Economic trends

- **ET1: Demand for many different services.** To satisfy consumer demand, plenty of different products and services are entering into the market. Needs and taste vary greatly from consumer to consumer. Some want the fastest possible fixed and mobile broadband, while others are happy with a cheaper and slower IAS with a data cap.
- **ET2: Netflix causes one third of traffic.** In some market areas one content provider may generate excessive amount of traffic. This causes a burden to the ISPs and charging CAPs would be justified from their point of a view. In North America, Netflix generates more than a third of the Internet traffic during peak hours.
- **ET3: Internet services are important for modern information society.** The Internet has changed the way we communicate and do business. Many services could not be implemented without fast Internet access.
- **ET4: Intensive competition in Finland.** There are three major tele operators in Finland, who are trying to outsmart their competition. This keeps consumer prices low and provides new innovative services for customers.

6.1.3 Social trends

- **ST1: Need for privacy and security.** The amount of cyber-attacks, data breaches and snooping personal information of the businesses and citizens have been increasing in a past few years. That's why security and privacy protection is necessary now and will become even more important in the future.
- **ST2: Increasing usage of social networking sites.** Social media sites such as Facebook, Twitter and LinkedIn have introduced mobile and web based platforms which individuals can use to interact with each other. Internet users have started to spend more time in social media sites than any other type of website.
- **ST3: People are online all the time.** More and more people are always connected to social media, email and other messaging applications with their mobile

phones. Large corporations like Facebook and Google are benefitting when people spend more time online.

- **ST4: Intimidation with net neutrality threats.** Only a few major net neutrality infringements have occurred in the Europe, nonetheless extremely strict net neutrality laws were proposed earlier by the EU Commission. Also some articles online are claiming the loopholes in the EU's net neutrality regulation could severely damage technology companies and other end-users.
- **ST5: It's consumers' benefit to have multiple different services to choose from.** If perfect substitute products or services cannot be found in the market, the markets will become monopolistic and the products lack differentiation. Also the prices tend to be higher.
- **ST6: Net neutrality regulation protects consumers.** Since fast lanes are not allowed, innovators can start new businesses and consumers can enjoy their unrestricted Internet access.

6.1.4 Technological trends

- **TT1: Prioritization is needed in the Internet.** To conduct business successfully corporations must ensure availability of some applications and services to all users. The QoS parameters are used to ensure that enterprise resource planning, video conferencing and other critical systems work as intended.
- **TT2: Mobility increases.** People travel more for business and leisure reasons and they need their mobile devices to work during their travel. This increases the need of mobile devices, wireless networks and greater capacity in the mobile networks.
- **TT3: Everything is top of HTTP.** Most of the Internet services are accessed with a HTTP protocol. At first glance it may be hard to see what goes through the network within HTTP packets, but it also gives agencies such as the National Security Agency (NSA) an ability to trace user's HTTP activity.
- **TT4: No net neutrality infringements in Finland.** So far there hasn't been any net neutrality violations in Finland. The situation must be followed to prevent them from occurring in the future.
- **TT5: Internet of Things.** Wide variety of new devices will be connected to the Internet with many different access technologies. Some of the devices may need their own mobile subscriptions, which will open a new market for simple and managed mobile connections.
- **TT6: ISP cooperation.** In some rural areas all ISPs do not build their own networks. In those places ISPs can rent network bandwidth from their competitors and offer subscriptions to consumers via their competitors' infrastructure. DNA and TeliaSonera are building a joint LTE Advanced 4G-network in the eastern and northern Finland to make savings in infrastructure. The area covers half of the Finland, but has only 15 percent of the population.

6.2 Key uncertainties

The key uncertainties in scenario planning demonstrate unpredictable factors that may have significant influence on the future of the net neutrality situation in Finland. Likelihood of them happening and their influence vary from uncertainty to another. Thus, we need to find two most important uncertainties to be able to construct the most plausible scenario matrix.

Table 4: Key uncertainties

Political/Legal uncertainties
PU1: Will the freedom to access any information or freedom of speech suffer?
PU2: Is blocking single sites such as The Pirate Bay going to be regular occurrence?
PU3: What can be considered as a specialized service?
PU4: Will the regulation become obsolete due to rapid industry changes?
PU5: How is the EU regulation going to be interpreted?
Economic uncertainties
EU1: How are the large corporations going to change the industry?
EU2: How will the increasing power of ISPs affect?
EU3: Is zero-rating going to cause problems?
EU4: Vertical integration?
Social uncertainties
SU1: Will the quality of Internet services be preserved?
SU2: What kind of risks consumers are facing?
Technological uncertainties
TU1: How increasing Internet traffic is going to affect?
TU2: Will wireless become a bottleneck?
TU3: How harmful traffic is restricted?

TU4: How OS and Device neutrality will affect?
TU5: How about Content and Service neutrality?
TU6: What effects the rapidly changing high-tech industry will produce?
TU7: Intelligence moves from edges to the network?

6.2.1 Political uncertainties

- **PU1: Will the freedom to access any information or freedom of speech suffer?** Unlikely. The Finnish net neutrality regulation bans access restrictions and so does the upcoming EU law. According to the EU law every European citizen must have access to all content.
- **PU2: Is blocking single sites such as The Pirate Bay going to be regular occurrence?** Unlikely. Even though ten EU countries have blocked The Pirate Bay, the access restrictions are easy to circumvent with proxy servers. Netherlands have stated that the blockade is ineffective, thus ISPs are no longer required to block access to The Pirate Bay [47].
- **PU3: What can be considered as a specialized service?** It is an electronic communication service that needs a higher end-to-end quality or an availability such as tele surgery or IPTV, and it should not be offered at the expense of an IAS. Following questions will hopefully be answered in the upcoming BEREC document: What proportion of a bandwidth specialized services can use and what can be categorized as one?
- **PU4: Will the regulation become obsolete due to rapid industry changes?** The regulation should be comprehensive, but it remains to be seen what kind of revolutionary innovations will happen in the future. The net neutrality regulation should be adjusted, if it is seen necessary.
- **PU5: How is the EU regulation going to be interpreted?** The EU regulation concerning net neutrality is ready and it's unlikely to change before it's in force. The interpretation of some sections is still unclear, but the upcoming BEREC document will hopefully answer to them.

6.2.2 Economic uncertainties

- **EU1: How are the large corporations going to change the industry?** Finland has three large competitive tele operators, thus markets work well. When monopolistic markets or industries appear it tends to rise consumers' prices and reduce amount of innovations. It is hard to enter the market as a newcomer, since barriers of entry are high, especially capital expenditure and economies of scale. Large corporations like Google, Facebook and Akamai are responsible for serving enormous amount of the entire Internet traffic. Their choices will have impact on Internet ecosystem, and their position may be considered similar as

ISPs' gatekeeper position in the net neutrality debate. Traditional mobile services (voice calls and SMS) are being replaced by applications that are no longer controlled by the operator.

- **EU2: How will the increasing power of ISPs affect?** ISPs have an important position in information society, since they provide Internet access to consumers and they act as gatekeepers between CAPs and end-users. Will the ISPs start charging CAPs at some point, since they are causing most of the traffic in their networks? Smaller CAPs may have a little influence on the price, if this happens.
- **EU3: Is zero-rating going to cause problems?** Zero-rating is seen as problematic issue. Customers with limited data plans don't get charged for data consumption by specific applications or services possibly provided by the ISP. In Finland, almost all mobile subscriptions are provided with unlimited data, so zero-rating shouldn't cause problems.
- **EU4: Vertical integration?** When ISP expands its operations to different levels of the supply chain, (e.g. acquires a content provider) it may cause disadvantage to competitors by limiting their access to content. This may give vertically integrated operator a profitable possibility to increase price, to the detriment of end-users.

6.2.3 Social uncertainties

- **SU1: Will the quality of Internet services be preserved?** When traffic is not discriminated, new competitive services can be offered to customers. Also growing bandwidth requirements due to video consumption will cause burden to ISPs.
- **SU2: What kind of risks consumers are facing?** Without competitive markets and strong net neutrality regulation consumers' IAS costs would rise. Also barriers of entry would rise for startups and entrepreneurs. They couldn't reach new customers as easily and launching their businesses would be harder without the open Internet.

6.2.4 Technological uncertainties

- **TU1: How increasing Internet traffic is going to affect?** There will be a need for large network infrastructure upgrades. It remains to be seen will the ISPs able to handle these investments while being profitable.
- **TU2: Will wireless become a bottleneck?** While customers in fixed networks are for the most part immobile, mobile customers can emerge anywhere. This makes offering fast connections more difficult and issues like congestion and interference more likely in mobile networks.
- **TU3: How harmful traffic is restricted?** Large amount of Internet traffic comes from automated sources and some of it is harmful. Attackers try constantly bypass security systems and change their tool set. Botnets and DDoS attacks

pose an immense treat to the Internet, and stopping them is an important task for the network owners.

- **TU4: How OS and Device neutrality will affect?** Since mobile devices have become extremely successful business, mobile OS creators and mobile device manufactures (e.g. Apple) have gained large control over mobile software. Apple can directly decide what applications are approved to AppStore and indirectly decide not to give support e.g. to flash media, thus being able to supervise functionality of the end-users' devices. [1]
- **TU5: How about Content and Service neutrality?** Google is a large service provider and owns the two largest search engines in the world i.e. Google and YouTube. Google could easily abuse its position with non-neutral search results that are crucial for the other companies. Also social networking sites like Facebook can easily modify users' news feeds with their algorithms. If some company partners up with Facebook they could get higher priority in posted links, news feeds and shown advertisements.
- **TU6: What effects the rapidly changing high-tech industry will produce?** New innovations or services related to e.g. IoT or SDN may not necessary be included in current regulatory frameworks. These will create new challenges to regulators as well as companies trying to deploy them.
- **TU7: Intelligence moves from edges to the network?** The Internet was originally a dumb network where most of the intelligence lied at the end-hosts. With the emergence of the cloud computing services, some might say the intelligence is shifting from edges to the network. Regardless, the cloud computing providers must follow the net neutrality regulation without giving unfair treatment or selectively providing better priority to certain customers at the expense of others. But since the cloud computing servers can be located anywhere, even outside the Europe, the regulation may not apply.

6.2.5 The most important key uncertainties

Two final key uncertainties are decided based on how large impact the uncertainty has on the industry and how plausible it is. During the interviews almost every expert perceived the upcoming EU regulation as the main concern for the Finnish net neutrality. The Finnish telecom industry works competitively with the current Finnish net neutrality regulation. The upcoming EU regulation was seen complex and it may cause misinterpretations. Thus, Political uncertainty 5 is chosen as one of the final key uncertainties. The TU6 is closely related and can be included to PU5, since one of the concerns of the upcoming EU regulation is that can new innovative services be productized.

PU1 and PU2 are already ruled out in the brief explanations. Zero-rated serviced (EU3) and specialized services (PU3) can already be offered in Finland and ISPs haven't offered them in a discriminatory manner, thus their significances as uncertainties are low. Also, final uncertainties must be independent from each other, therefore other regulation related uncertainties can be ruled out (PU4 & TU7). Social uncertainties can also be

excluded, since the net neutrality regulation's main goal is to protect the consumer and guarantee the quality of their IAS. Finnish ISPs have some vertical integration in the content market (EU4), but it has not caused detriment to competitors, end-users or the markets in general.

Wireless networks are more likely to face problems like interference and congestion than the fixed networks (TU2). The wireless networks in Finland are among the best in the world and ISPs are investing continuously on them, therefore it is unlikely to encounter congestion problems in the imminent future. The harmful Internet traffic (TU3) is also an increasing problem. Hackers are trying to exploit smartphones and tablets with malware. Google and Apple are investing significant resources in an attempt to stop malicious applications [48]. The amount of mobile malware appears to be insignificant and mobile application markets provide satisfactory security [48]. Only 0.17 percent of mobile devices are affected by security threats [49]. Several other possible methods to commit harmful acts exist, but further assessment of all the possible malicious activities is outside the scope of this study and is not directly related to the net neutrality.

Thus, we are left with ISP and CAP related uncertainties. The Finnish ISPs are seen to offer fair services without discriminating practices. The study may be biased, since all of the interviewees are from Finland, but a clear evidence shows that Finnish ISPs do offer significantly better services than their European counterparts [50]. The device neutrality and service neutrality are uncharted topics, but pose a clear threat to Finnish ecosystem. The fact that multinational companies have such a fundamental position in a society and are exerting more control over widely used devices and service, may cause problems in the future. It is also hard to regulate foreign and multinational companies. The How are the large corporations going to change the industry? –uncertainty (EU1) includes topics of the device and service neutrality, and therefore it is chosen as the second final key uncertainty. The final key uncertainties that are used to form a scenario matrix are:

- How is the EU regulation going to be interpreted?
- How are the large corporations going to change the industry?

The key trends and less important uncertainties are used to add distinct elements to the final scenarios.

6.3 Scenarios

The final scenarios were constructed based on the two most important uncertainties, which are most likely to have the biggest impact on the net neutrality in Finland. The first one is regulation based uncertainty while the other one is actor based, thus providing a wider scope. The first final uncertainty is related to the upcoming EU regulation and its interpretation. The current proposal does not specify how much bandwidth can be reserved to specialized services or can new innovations be productized and offered to consumers. The second final key uncertainty focuses on the large actors in the ICT industry and how they will act on the future, neutral or hostile. The focus is not only the ISPs, but the other significant corporations that have a large control over the devices and services that are being used.

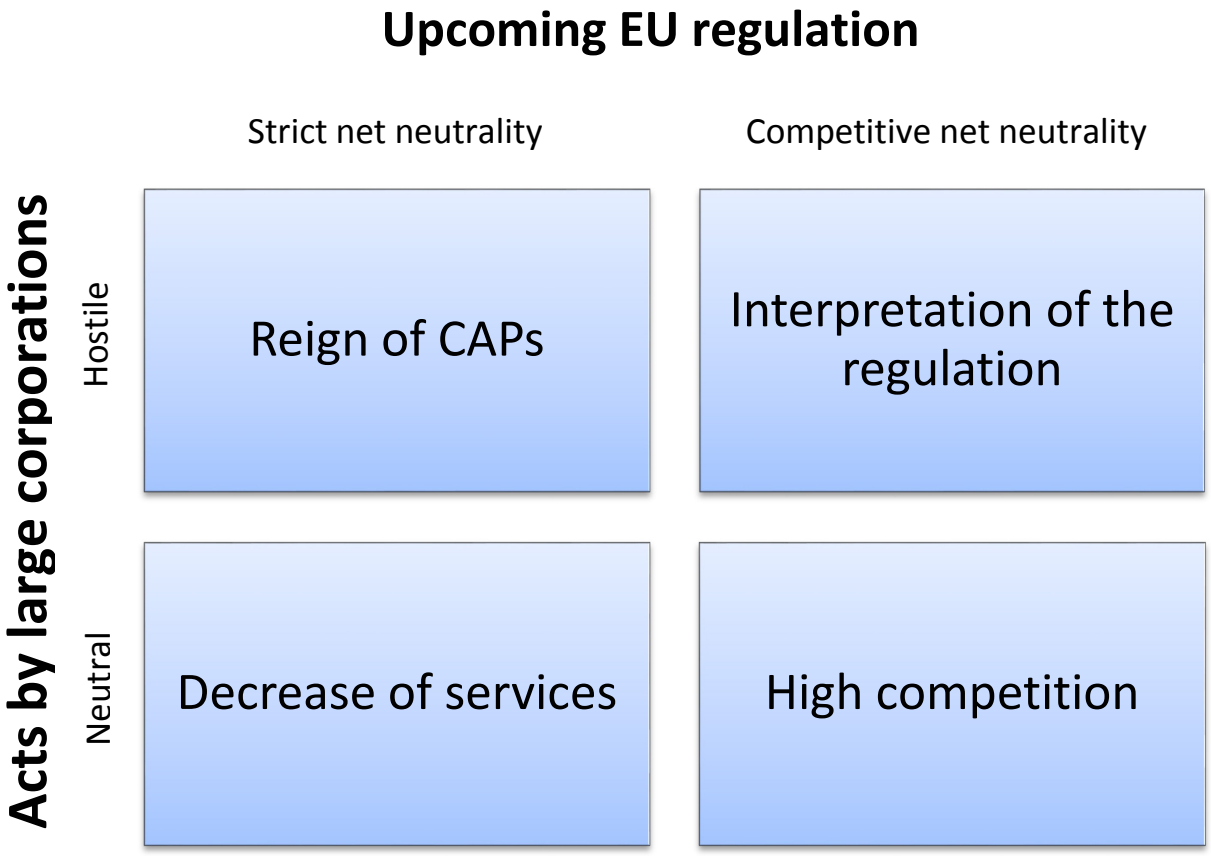

Figure 3: Scenario matrix

6.3.1 Reign of CAPs

The European Union will get strong net neutrality laws in any case, but requirement for perfect net neutrality or setting the regulation too strict would lead to congestion problems. Only way to revise that are heavy network infrastructure investments by the network owners, which would lead to increased consumer prices for an IAS. However, the current proposal by the EU Commission will allow reasonable traffic management and this kind of situation is unlikely to happen. But the tightening regulation may have large

impact on other EU countries such as United Kingdom whose ISPs rely on extensive network management practices.

If the upcoming EU net neutrality regulation is strict about new emerging technologies and services, it will diminish the ability of startups and ISPs to compete in high-tech industries. This will lead to lack of new innovation or at least to a great difficulty to deploy new innovations. The current net neutrality regulation applies only to the last-mile infrastructure that is offered by the ISPs, thus having little to none impact on the content providers.

In market-oriented economies companies tend to seek profitable businesses anywhere without hesitation. Since traditional phone services are being replaced by the applications like WhatsApp, the market power is shifting away from the ISPs. Also the requirement for fast broad band to every household and place of business, causes more expenditure to ISPs. OS manufactures and CAPs have started to gather information about their consumers, and some of the consumers are even unaware of that. The information gathering can be applied to wider scale and to more personal information, when it becomes a clear violation of privacy. If companies such as Google decided to provide non-neutral search results, it would be a great threat to the entire information society. Many businesses rely on that they can be found easily from Google search results.

6.3.2 Interpretation of the regulation

In this scenario, competitive net neutrality means that the EU regulation can be interpreted in a way that it is possible to offer new services related to emerging technologies such as IoT and SDN. This will give more leeway to startups and to other small companies. The regulation will still be strict about clear violations of the net neutrality. Paid-peering, blocking and restrictions are prohibited, but CDNs are allowed. This may give large corporations an incentive to invest heavily on them, which allows offering better QoE to the end-users. Currently CDNs and cache servers allow ISPs and CAPs to diminish congestion in the networks. Although the packets are sent with a best-effort principle, the smaller companies do not have access to this same infrastructure. The interconnection market is not included in the current regulation, but adding it may become necessary in the future, as well as increasing transparency of the interconnections.

When the regulation does not set exact boundaries on how the details should be interpreted, companies tend to handle it the way that suits best for them. Some companies are willing to take some risks in order to find new profitable businesses from unregulated markets. This is likely to cause more legal disputes in the future. BEREC is preparing new guidelines to cover obligations of the NRAs related to the monitoring and enforcement of the net neutrality regulation. Hopefully the guidelines will deliver a common approach to net neutrality rules and take a firm stance against misinterpretations.

6.3.3 Decrease of services

When the net neutrality regulation is set too strict, ISPs in some European countries cannot rely on their network management practices. ISPs must invest heavily in new network infrastructure to keep up with the increasing Internet traffic. This may shift market power from ISPs to the CAPs and to other ICT companies. When the net neutrality regulation is strict in EU level, this will cause more burden to the ISPs and they cannot monetize their new services or products that easily. This situation would lead to decrease of services that are offered to end-user and the prices of mobile subscriptions and IASs would rise. This may cause slight burden to smaller companies which could result in decrease of innovations.

Problems with the net neutrality regulation can also be revised afterwards. It is nearly impossible to cover all the small details in the regulation, since some companies may try to circumvent the rules to seek for an advantageous position. Leaving things like zero rating open for the NRAs to decide can be a smart choice, since some of the EU member countries have already adopted national regulation and other industry practices. The power of the CAPs and OS manufacturers is increasing in this scenario. Google and Microsoft are dominant market powers in nearly monopolistic markets. The Service neutrality or the OS neutrality may become real problems in the next ten years.

6.3.4 High competition

When the regulation is permissible large CAPs, mobile phone manufacturers and OS manufacturers such as Google, Apple and Microsoft face more competition. High competition will give end-users more variety in mobile devices and applications, while the prices stay affordable. New startups will enter the market to focus on niche markets, which increases consumer surplus and decrease the possibility of monopolistic markets from occurring. ISPs are more likely to make profits and offer their own content services that compete against content providers' services.

The regulation should be adjusted, if net neutrality violations appear. High-tech industry changes fast and new innovations appear frequently, therefore it is relatively hard to set regulation to take every possible option into account. Allowing the markets to work competitively will promote new innovation and do not cause excessive burden to ISPs. NRAs must monitor the ISPs and their provision of specialized services regardless how restrictive the regulation is. It is benefit to consumers, ISPs, device manufacturers and content providers that the Internet is open to innovation and experimentation [26].

6.4 Analysis

In Finland there are three major competitive ISPs, services are transparent and switching to another ISP is effortless, thus markets work well. They offer IASs, mobile subscriptions, content services and other corporate services. It is unlikely that any of these players start restricting services in such a way it would violate the net neutrality. The

gain benefit for such an activity is marginal, while getting caught may drive away a lot of customers. Therefore, problems that may arise are likely to come from acts of multi-national companies rather than domestic ISPs. The EU regulation will cover all member countries, therefore it is hard to make perfectly comprehensive. Some countries may need strict rules, in order to govern their ISPs and some might not. It is advisable that some points are left open to NRAs to decide, since one of the regulator's goals is to maximize welfare of the citizens and businesses in a long term [35].

In the first scenario, *Reign of CAPs,* CAPs are aggressively trying to maximize their profits by extensive information gathering or by providing non-neutral search results. ISPs will suffer from strict regulation, competing services like WhatsApp and heavily increasing Internet traffic. The consumers will suffer from increasing IAS prices and violations of privacy. In the second scenario, *Interpretation of the regulation*, large CAPs are trying to find unregulated markets such as building CDNs, which will cause disadvantage to smaller companies. ISPs may try to provide more specialized services at the expense of Internet access which will detriment end-users' QoE of an IAS. In the third scenario ISPs are suffering from too strict regulation which will result in *Decrease of services.* It is regulators mission to balance the regulation to satisfy needs of all stakeholders. While in the final scenario, *High competition*, regulation is balanced and it does not cause major disadvantages to any of the stakeholders.

The value distribution of the scenarios is illustrated in the Figure 4 [51]. To reduce the number of stakeholders, OS and device manufacturers (e.g. Apple, Microsoft) and Internet service corporations (e.g. Google, Facebook) are included in the CAPs. The benefit of end-users is marked with plus or minus signs. The illustration is directional and the number of coins should be examined within and between the scenarios. The advertisers' benefit is not drawn into the picture, but they would be best off in the *Reign of CAPs* scenario, since they would receive end-users' personal preferences from CAPs, thus being able to provide more precise marketing.

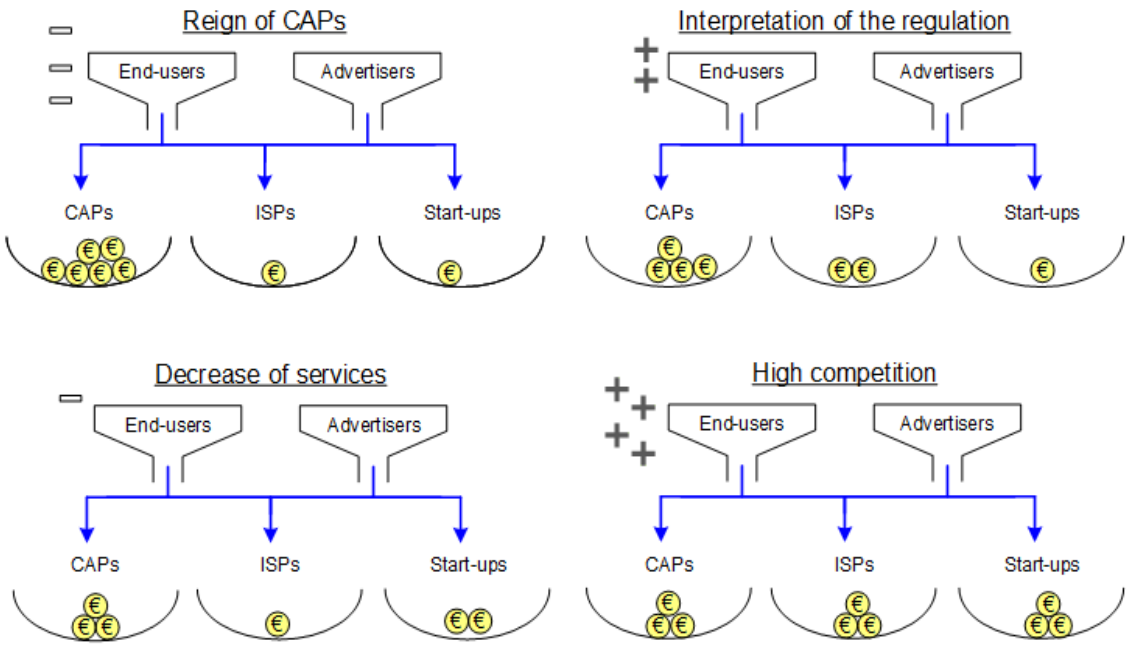

Figure 4: Value distribution of the scenarios [51]

The *Decrease of Services* has the lowest economic benefit to the society, due to the strict regulation. CAPs are offering non-neutral services and gathering personal information to maximize their profits, which is illustrated in the *Reign of CAPs*. The *High competition* provides most benefit to the society, not only by the amount of money, but also from achieved end-user benefit. The *Interpretation of the regulation* reduces revenue from start-ups and shifts it to CAPs, due to the built CDNs. ISPs will get some revenue streams from their specialized services. The end-users are benefitting from the services offered by the ISP, but switching to other content services is harder since some of the specialized services are offered at the expense of the IAS.

7 Conclusion

This chapter describes the results from the study and answers to the main research question. The results are evaluated and plausible exploitations of the results are provided in the discussion. The possible future research topics are suggested in the end.

7.1 Results

The answer to the main research question is that the net neutrality in Finland is in advisable shape, and no net neutrality violations were found. The European Union and Finland have recently imposed net neutrality regulations that ensure free access to the content and services of users' choice and prohibits blocking and restricting their access. ISPs are allowed to use network management, in order to offer and develop functional and secure services, maintain their networks and to comply with national legislation related to illegal content or criminal law.

The Internet is extremely beneficial to a society and it should provide most to the economy when it remains open for innovation, investments and speech [26]. The net neutrality laws are imposed to guarantee the open Internet. The Finnish net neutrality regulation came into effect on the first of July, 2015 and it will be abolished when the EU regulation will come into force on the 30th of April, 2016. BEREC is preparing new guidelines that will cover obligations of the NRAs related to monitoring and enforcement of the net neutrality regulation. The guidelines will hopefully specify how much bandwidth can be allocated to specialized services and what can be categorized as one.

The Scenario planning provides new aspects to the net neutrality debate through identifying important key trends and key uncertainties. The first final key uncertainty relates to the upcoming European Union regulation. Since the regulation is not in force yet, it will be hard to predict does it restrict the emergence of new innovative services. The second final key uncertainty focuses on the large actors in the ICT industry and how they will act on the future, neutral or hostile. Companies like Google and Apple are in a similar gatekeeper position as the ISPs and their actions will have a great influence on the ICT industry.

The first scenario, *Reign of CAPs*, shows a situation where market power is shifting away from the ISPs, resulting in network congestion and increased IAS prices. The *Interpretation of the regulation* presents a situation where the regulation does not restrict companies from entering the market with new innovations. Meanwhile, larger companies try to find new profitable businesses from unregulated market areas (e.g. by building CDNs). The *Decrease of services* scenario may occur when ISPs struggle with strict net neutrality regulation and are unable to offer new services to their customers. In *High competition* markets are allowed to work competitively, which will promote new innovation and provide more services to consumers. The *High competition* scenario has the highest end-user and economic benefit to the society.

7.2 Assessment of the results

No serious net neutrality violations were found in Finland. The DPI usage is practically nonexistent and the Finnish ISPs do not restrict the P2P protocol. Zero-rating should not cause problems in Finland, since almost all mobile subscriptions have unlimited data. The challenges that may appear are related to the upcoming EU regulation. It may not allow productization of new innovative services related to the emerging technologies. The EU law leaves zero-rating question open to national regulators to decide, which may cause problems in various EU countries. Some national regulators have not proposed strict national net neutrality regulation, therefore they may not make changes to the zero-rating practices either.

Scenario planning challenges a prevailing mindset by identifying early warning signals and by awakening new ideas. The more control stakeholders have over a trend or an uncertainty, the quicker it may vanish. Each constructed scenario studies a peculiar business architecture, which may initiate advantageous discussions among the experts. The target for the Finnish net neutrality is clearly similar as the *High competition* scenario. The scenarios can also reveal unrecognized opportunities or an ideas of new businesses.

7.3 Discussion

The EU regulation has experienced numerous amendments and one of the proposals was going to allow paid prioritization, thus it should be noted the older news articles, that do not discuss the latest proposal, are with a high probability irrelevant. Also some articles that are directly translated from English to Finnish are focusing situation in other countries like the UK, therefore they may not have nothing to do with situation in Finland.

Finnish mobile market is different than the market in most of the European countries. The competitive market in Finland provides affordable mobile IAS prices with unlimited data, thus zero-rated services have hardly any effect in Finland. While ISPs in countries like Spain, Germany, Belgium and the United States zero-rate their own IPTV or their partners' services and sell mobile internet with a remarkably high price [50]. Zero-rating is harmful in those countries and should be regulated carefully by the national regulators.

The scope of the research was to study net neutrality in Finland, therefore the results are obviously the most useful to the Finnish audience. The facts are presented in the fifth chapter, while the conducted scenario analysis provides possible problems that may arise in the future. The scenarios can also be applicable in other countries where zero-rating cannot be reckoned as one of the key uncertainties. These countries are Poland, France, other Nordic countries or Baltic countries, where mobile data is affordable [50]. In Poland, fourth challenger tele operator has started offering inexpensive unlimited

data plan and has gained 22% of the market [50]. This raises a question: Could Finnish tele operators expand their business to other EU countries such as Germany?

7.4 Future Research

In the future, it would be interesting to see papers that study how much detriment these price discrimination practices such as zero-rating cause to content providers and consumers in other EU countries. And how hard is it for a new content provider to enter the market, where ISPs are vertically integrated providing their own content? It is also intriguing to follow how each of the EU countries are going to adopt the regulation and what will be the final form of the upcoming EU law.

The net neutrality debate will continue until the EU regulation is in force, BEREC guidelines are finished and the EU member countries have successfully adopted the regulation. After that the debate will continue outside the EU where the net neutrality regulations are not yet in force. In the future, the debate may shift to new related topics such as service neutrality or device neutrality.

References

[1] Krämer, J., Wiewiorra, L. and Weinhardt, C. Net neutrality: A progress report. Telecommunications Policy, 2013. Vol. 37, No. 9, pp. 687-814.

[2] Lemley, M.A. and Lessig, L. The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era, 2000. UCLA Law Review, Vol. 48, p. 925; Stanford Law and Economics Olin Working Paper No. 207; UC Berkeley Public Law Research Paper No. 37.

[3] Schoemaker, P.J.H. Scenario Planning: A Tool for Strategic Thinking, Sloan Management Review, 1995. Vol. 36, no. 2, pp. 25-40.

[4] Wack, P. Scenarios: Uncharted Waters Ahead, Harvard Business Review, 1985. Vol. 63, no. 5, pp. 73-89.

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

[6] Heikkinen, M., Matuszewski, M. and Hämmäinen, H. Scenario planning for emerging mobile services decision making: mobile Peer-to-Peer Session Initiation Protocol case study, Int. J. Information and Decision Sciences, 2008. Vol. 1, pp. 26-43.

[7] Smura, T. and Sorri, A. Future Scenarios for Local Area Access: Industry Structure and Access Fragmentation. Proceedings of the 8th International Conference on Mobile Business (ICMB) in Dalian, China, 2009.

[8] Levä, T. Scenario Analysis on Future Internet. Master's Thesis. Helsinki University of Technology, Espoo, 2009.

[9] Schoemaker, P.J.H. When and How to Use Scenario Planning: A Heuristic Approach with illustration, Journal of Forecasting, 1991. Vol. 10, no. 6, pp. 549-564.

[10] Johnson, G. Whittington, R. Scholes, K. Angwin, D. and Regnér, P. Exploring Strategy Text & Cases. London, Pearson, 2013.

[11] Arthur, J., Waring, M., Coe, R. and Hedges, L. Research Methods & Methodologies in Education. London, UK, SAGE Publications Ltd, 2012. 456 p. ISBN 978-0-85702-038-3.

[12] Wu, T. Network Neutrality, Broadband Discrimination. Journal on Telecommunications & High Technology Law, 2003. Vol. 2, pp. 141–178.

[13] Cisco. Cisco Visual Networking Index: Forecast and Methodology, 2014-2019. White Paper, 2015.

[14] Economides, N. and Tåg, J. Network neutrality on the Internet: A two-sided market analysis. Information Economics and Policy, 2012. Vol. 24, pp. 91–104.

[15] Cisco. Quality of Service Networking, 2012. [Accessed 17.7.2015]. Available at: http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

[16] Kilkki, K. Quality of Experience in Communications Ecosystem. Journal of Universal Computer Science, 2008. Vol. 14, no. 5, pp. 615-624.

[17] Peng, G. CDN: Content Distribution Network. Technical Report, Stony Brook University, 2008.

[18] Layton, R. Content delivery networks safe from net neutrality… for now. TechPolicyDaily.com, 21.3.2014. [Accessed 29.7.2015]. Available at: http://www.techpolicydaily.com/communications/content-delivery-networks-safe-net-neutrality-now/

[19] Swansson, P. Comcast blocks some Internet traffic. NBC news, 19.10.2007. [Accessed 30.7.2015]. Available at: http://www.nbcnews.com/id/21376597/#.VbpQmWN3YtF

[20] McCullagh, D. Court: FCC has no power to regulate Net neutrality. Cnet, 6.4.2010. [Accessed 31.7.2015]. Available at: http://www.cnet.com/news/court-fcc-has-no-power-to-regulate-net-neutrality/

[21] Anderson, N. Deep packet inspection meets Net neutrality. Ars Technica, 26.7.2007. [Accessed 31.7.2015]. Available at: http://arstechnica.com/gadgets/2007/07/deep-packet-inspection-meets-net-neutrality/1/

[22] Mueller, M.L. and Asghari, H. Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States. Telecommunications Policy, 2012. Vol 36, No 6, pp. 462–475.

[23] Plusnet. All about traffic management, 2015. [Accessed 20.8.2015]. Available at: http://www.plus.net/support/broadband/speed_guide/traffic_management.shtml

[24] Mueller, M.L. Social Science Research on Deep Packet Inspection. Using Network Data to Detect DPI. [Accessed 20.8.2015]. Available at: http://dpi.ischool.syr.edu/MLab-Data.html

[25] European Commission. A Europe 2020 Initiative. Net Neutrality Challenges. [Accessed 2.7.2015]. Available at: http://ec.europa.eu/digital-agenda/en/net-neutrality-challenges

[26] Federal Communications Commission. Protecting and Promoting the Open Internet, GN Docket No. 14-28, 2015.

[27] Donck, F. Net Neutrality in Europe: Overview and Challenges. Internet Society, NN Debate, Lisbon, 2015.

[28] Council Regulation (EC) No 1211/2009. Establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office. OJ L 337/1.

[29] BEREC. Summary of BEREC positions on net neutrality. BoR (12) 146, 2012.

[30] BEREC. An assessment of IP-interconnection in the context of Net Neutrality. BoR (12) 33, 2012.

[31] BEREC. Guidelines for Quality of Service in the scope of Net Neutrality. Bor (12) 131, 2012.

[32] BEREC. A view of traffic management and other practices resulting in restrictions to the open Internet in Europe. BoR (12) 30, 2012.

[33] European Commission. Press release. Commission welcomes agreement to end roaming charges and to guarantee an open Internet, 30.6.2015. [Accessed 24.8.2015]. Available at: http://europa.eu/rapid/press-release_IP-15-5265_en.htm

[34] Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, 2013/0309/COD.

[35] FICORA. Presentation and duties, 2015. [Accessed 23.6.2015]. Available at: https://www.viestintavirasto.fi/en/ficora/presentationandduties.html

[36] FICORA. Viestintäviraston muistio verkkoneutraliteetin (net neutrality) sääntelytilanteesta, Suomi ja EU, 2012. 1800/69/20.

[37] Ministry of Transport and Communications, Finland. Information Society Code. L 7.11.2014/917. [Accessed 23.6.2015]. Available at: https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

[38] FICORA. Internet-yhteyspalvelujen tarjontaa koskevat yleispalvelupäätökset, 2015. [Accessed 31.8.2015]. Available at: https://www.viestintavirasto.fi/ohjausjavalvonta/yleispalvelu/yleispalvelupaatokset/internetyhteyspalveluidenyleispalvelupaatokset.html

[39] FICORA. Everyone is entitled to telephone and internet access, 2015. [Accessed 31.8.2015]. Available at: https://www.viestintavirasto.fi/en/internettelephone/righttoatelephoneandbroadbandsubscription.html

[40] European Parliament and the Council Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. L 218/8.

[41] Finnish Government Proposal. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi. HE 232/2014. [Accessed 5.9.2015]. Available at: https://www.finlex.fi/fi/esitykset/he/2014/20140232

[42] Goldsmith, J., Wu, T. Who Controls the Internet? Illusions of a Borderless World. Oxford University Press, 2006.

[43] Elisa Oy. Matkapuhelinliittymä hinnasto henkilöasiakkaille 1.3.2015. [Acces-sed 2.11.2015]. Available at: http://elisa.fi/attachment/content/Elisa_Mobiili_hinnasto_ha_01032015.pdf

[44] DNA Liittymät. [Accessed 2.11.2015]. Available at: https://www.dna.fi/liittymat

[45] Sonera. Liikkuva Netti mobiililaajakaista. [Accessed 2.11.2015]. Available at: https://kauppa.sonera.fi/yksityisille/tarjooma/nettiliittyma.aspx

[46] Tefficient. "Peak data" in sight. Industry analysis #7, 2014. [Accessed 2.11.2015]. Available at: http://media.tefficient.com/2014/12/tefficient-industry-analysis-7-2014-mobile-data-usage-peak-ver-2.pdf

[47] RT.com. Dutch court rules in favor of unblocking Pirate Bay as ban 'ineffective', 28.1.2014. [Accessed 16.10.2015]. Available at: https://www.rt.com/news/court-unblock-pirate-bay-308/

[48] Lever, C., Antonakakis, M., Reaves, B., Traynor, P. and Lee, W. The Core of the Matter: Analyzing Traffic in Cellular Carriers, 2013. In proceedings of NDSS 2013.

[49] Raghuramu, A., Zang, H. and Chuah, C-N. Uncovering the Footprints of Malicious Traffic in Cellular Data Networks, 2015. 16th International Conference, PAM 2015, New York, US. pp. 70-82.

[50] Digital Fuel Monitor. Consolidated tight oligopolies versus competitive mobile markets – Digital Fuel Monitor 4th release 2H2015, 2015. [Accessed 11.11.2015]. Available at: http://dfmonitor.eu/downloads/2H2015_DFMonitor_fourth_release_09112015.pdf

[51] Christensen, C.M., Raynor, M. and Verlinden, M. Skate to Where the Money Will Be, Harvard Business Review, 2001. Vol. 79. pp. 72-81.

Appendices

Appendix A. Basic question list used in the interviews. Variations were applied based on the interviewee's organization and the problem at hand.

1. Scenario planning: Factors affecting the net neutrality?
    - Political/Legal
    - Economic
    - Social
    - Technological
2. How and why is network management done?
3. How is malicious activity prevented in information networks?
4. Does the situation differ between fixed and mobile broadband?
5. What do you think about Finnish Information Society Code- regulation?
6. What are the differences in between the European Union's and the Finnish net neutrality regulation?
7. Will the European regulation overrule the Finnish regulation?
8. What do you think about specialized services?
9. Does business mobile subscriptions have a higher priority?
10. In what relation there are mobile subscriptions with unlimited data and data cap?
11. Has there been any traffic restrictions or net neutrality infringements in Finland?
12. Is zero-rating allowed in Finland?
13. When is the net neutrality violated/broken in your opinion?
14. How do you see the net neutrality situation in Finland?
15. How will the net neutrality situation develop in next 10 years?
16. What factors will cause most uncertainty or problems concerning the net neutrality?
17. Anything else?

Appendix B. Important forces affecting the net neutrality based on the interviews. Grouped as trends (T) or uncertainties (U):

Political/Legal forces	Group
Freedom to access any information and freedom of speech.	U
Too strict laws may decrease competition.	T
The EU and the US are different as market places.	T
Blocking The Pirate Bay was a radical decision.	U
Everybody has a legal right to 2 Mbps broadband in Finland.	T
Unclear what can be considered as specialized service.	U
Finnish law does not prohibit offering subscriptions with extra services.	T/U
Finnish net neutrality law is seen to be sufficient and well-written.	T
EU Parliament's was in favor of very strict net neutrality.	U
Hard to set regulation that doesn't become obsolete, due to rapid industry changes.	U
EU regulation isn't ready or in force yet.	U

Economic forces	Group
Demand for many different services.	T
Large companies have a lot of power -> Own CDNs.	U
Netflix causes one third of traffic.	T
Content providers can't influence on the price.	U

ISPs' power increases.	U
Internet services are very important for modern information society.	T
Startups have little influence.	U
Intensive competition in Finland. 3 large operators.	T
Zero-rating.	U
Vertical integration of ISPs and CAPs.	U

Social forces	Group
Consumers have very little influence.	U
Need for privacy and security.	T
Consumer's risk.	U
Increasing usage in social networking sites.	T
People are online all the time. Part of everyday life.	T
Intimidation with net neutrality threats.	T
It's consumers' benefit to have multiple different services to choose from.	T
Net neutrality regulation protects consumers.	T
Quality of Internet services must be preserved.	U

Technological forces	Group
Internet traffic increases due to video consumption.	U
Wireless may become bottleneck.	U
Prioritization is needed.	T
Mobility increases.	T
Everything is top of HTTP.	T
Restricting harmful traffic.	U
No net neutrality infringements in Finland.	T/U
Internet of Things.	T
OS and Device neutrality.	U
Service and Content neutrality.	U
Proactive network infrastructure investments.	U
ISPs rent network bandwidth to each other.	T
Rapidly changing high-tech industry.	U
Cloud services, cloud computing. Intelligence moves from edges to the network.	U