FLAMINGO

European Seventh Framework Network of Excellence

`http://www.fp7-flamingo.eu/`

WP7 — Economic, Legal and Regulative Constraints

Deliverable D7.2 — Design and Selected Mechanisms

University of Twente, The Netherlands (UT)
Institut National de Recherche en Informatique et Automatique, France (INRIA)
University of Zurich, Switzerland (UZH)
Jacobs University Bremen, Germany (JUB)
Universität der Bundeswehr München, Germany (UniBwM)
University Politecnicà de Catalunia, Spain (UPC)
iMinds, Belgium (iMinds)
University College London, United Kingdom (UCL)

Project funded by the European Union under the
Information and Communication Technologies FP7 Cooperation Programme
Grant Agreement number ICT-FP7 318488

Document Control

Title:	WP7 — Economic, Legal and Regulative Constraints
Type:	Public
Editor(s):	Radhika Garg, Burkhard Stiller
E-mail:	garg@ifi.uzh.ch, stiller@ifi.uzh.ch
Doc ID:	D7.2
Delivery Date:	31.10. 2014
Authors:	Andri Lareida, Anna Sperroto, Anuj Sehgal, Bram Naudt, Burkhard Stiller, Christos Tsiaras Corinna Schmitt, Daniel Dönni, Daphne Tuncer, Guilherme Machado, Joan Serrat, Javier Rubio Loyola, Marinos Charalambides, Maxim Claeys, Niels Bouten, Mario Flores, Patrick Poullie, Radhika Garg, Rashid Mijumbi, Sebastian Seeber, Sofie Verbrugge, Thomas Bocek

For more information, please contact:

Dr. Aiko Pras
Design and Analysis of Communication Systems
University of Twente
P.O. BOX 217
7500 AE Enschede
The Netherlands
Phone: +31-53-4893778
Fax: +31-53-4894524
E-mail: <a.pras@utwente.nl>

Legal Notices

Contents

1 Executive Summary

WP7 focuses on finding, determining, and practically achieving cross-disciplinary methodologies so that technological dependency on economical, legal, and regulative aspects can be studied. Therefore, the purpose of this document is to analyze and discuss key scenarios (in close collaboration with WP5 and WP6) in a use-case-based manner from these perspectives. The goal of these analysis is to enable the formalization of fine design of architecture, methods, and mechanisms for stakeholders involved in an integrated manner.

WP7 is driven by the underlying understanding that the development, operations, and maintenance of a technology proves to be more beneficial, when it is developed with a consideration of three integrated pillars: (a) business goals, (b) economic goals, and (c) legal and regulative constraints. In detail, the analysis of business indicators, policies, and their interrelations for network and application optimization helps in identifying the dependency of underlying technology on economic and initial legal and regulative requirements. Therefore, assisting the design of technologists in comprehending limiting factors from the above mentioned perspectives is the prime focus of this deliverable. To this end and with the experience and engagement in the second year of FLAMINGO with those technologies under the umbrella of the Future Internet (FI) this deliverable D7.2 identifies major facts and achieves major findings for answering the three major questions:

1. What are possible constraints of management technology and solutions from the economic, legal, and regulative domains that enable, border, or restrict operations and management of networks and systems?

2. How can a business-oriented management be designed and carried out for diverse technologies with efficiency?

3. How are business goals, policies, and economic considerations of a technology interdependent?

In reply to these questions, WP7 identified constraints and considerations from those three perspectives determined relevant, which include by definition business, economics, and legal and regulative constraints. Business considerations include the identification of business indicators, policies, and their mapping functions, which serve as a means to operate and maintain a network or system successfully. The economic analysis comprises of the following major facets: multi-actor analysis, cost modeling, pricing schemes, a Service Level Agreements (SLA) analysis, and, where applicable, an incentives discussion. Additionally, the discussion of the status quo of highly debated regulations impacting network and service management in the field of data storage, data retention, cross-border data flow, network neutrality, incentive auctions, and cloud federations and resource allocations form an integral part of this deliverable.

In order to validate the current status of the work within WP7, three validation mechanisms have been identified in Y2 and have been applied where possible. First, the meta method termed “Tussle Analysis” allows to perform a socio-economic aware analysis of future networks; this has resulted in the newly standardized ITU-T recommendation Y.3013. Second, the validation by value networks and business models enable the visualization on how a technology will influence explicitly the economic and the business landscape. Third, in collaboration with external experts, an interview-based verification of WP scenarios’ assumptions, methodologies, and mechanisms had been performed.

Therefore, the design, analysis, and discussion of scenarios (in close collaboration with WP5 and WP6) within the scope of WP7 was able to verify initial assumptions of a general inter-dependency of technological requirements and economic, legal, and regulative constraintsánalysis. As shown,

in order to efficiently operate and maintain the technology in the field, cross-disciplinary methods and approaches are required. In the same line, business indicators, policies, and their interrelations have been identified for those scenarios under investigation. Finally, economic interdependencies of these indicators have been identified. This does form the basis to apply further optimization-driven economic approaches as well as legal and regulative constraints analysis to networks and (telecommunications) services of the Future Internet in the next two years of FLAMINGO to come.

2 Introduction

The rapidly growing penetration of the Internet in business and society always requires efficient networks. For a policy based management of networks incentives must be created for every stakeholder involved. This will also see management decisions that are taken based on the complement of economic optimization with legal and regulative constraints.
The three pillars for successful deployment and operation of networks and services comprises of goals and constraints from the business, economical, and legal and regulative perspective. While the business perspective addresses the business indicators and business policies as a mechanism to track the business goals, the economic dimension addresses incentives, pricing, and cost benefit analysis. The integrated legal dimension will address major stakeholders imperatives in a certain country or region, and the integrated regulative dimension will address impacts and effects of country- or region-specific regulations.

2.1 Goals of D7.2

The first goal of this deliverable D7.2 is to cover the fine design of architectural aspects or those mechanisms selected for all three tasks of WP7. To this end, the relevant scenarios are analyzed from three perspectives, which are identified as the pillars of analysis within WP7. The three pillars of this work are the business, economic, and legal and regulative constraints and considerations. Second goal is to identify the interdependencies of these three pillars in order to ensure successful deployment and operation of respective network and service management scenarios. Third goal of this deliverable is to identify and apply validation mechanisms in order to validate assumptions, approach, and results of all the scenarios within WP7. Details of several validation approaches developed and applied in WP7 are available in Section 6.

Thus, this section recalls the three tasks of WP7 along with their current status, introduces the methodology developed and to be applied for all investigations, and finally outlines the full deliverable structure.

2.2 Tasks of WP7

As mentioned in Description of Work, WP7 is divided in three major tasks as follows. The following section describes the status and outcome of these task in Y2 of FLAMINGO.

- **Task T7.1: Outcomes for Economic Analysis**
  This task identifies detailed insights into economic analysis in the area of network and service management. The aim of to develop pricing models and cost models, identify incentives for stakeholders, and perform cost-benefit analysis for relevant scenarios in the field of network and service management. The set of current and detailed outcomes of T7.1 is summarized in Table 1.

- **Task T7.2: Outcomes for SLA and Policy Management**
  This task concentrates on defining a new methodology or complementing an existing methodology in policy refinement and analysis. The set of current and detailed outcomes of T7.2 is summarized in Table 2.

- **Task T7.3: Outcomes for Legal and Regulative Constraints**
  This task aims to identify constraints from a legal and regulative point of view; specially in the area of data storage, retention, and sharing, cross border data flow, network neutrality, incentive auctions, and cloud federations and resource allocations. The set of current and detailed outcomes of T7.3 is summarized in Table 3.

Table 1: Task T7.1-Outcomes for Economic Analysis

No.	Task Activities	Status as of Y2	Description	Section	To be Addressed in Y3–Y4
1.1	Muti-actor cost-benefit analysis for network management and operations	IN PROGRESS	Cost model of Internet Service Providers is being studied (including caching infrastructure), multi-actor analysis is used to incorporate the interests of all actors	Section 4.2.1-4.2.2	Code implementation and results
1.2	Trade-offs between cost of operations and obtained Quality-of-Experience (QoE)	IN PROGRESS	QoE measures are gathered via custom developed mobile application.	Section 4.2.4	Generate more widespread use of the application
1.3	Pricing approach as a trade-off to match user's demand, Quality-of-Service (QoS), and resource availability	IN PROGRESS	Pricing model for virtualized resources is being studied	Section 4.2.1	Code implementation and results

Table 2: Task T7.2-Outcomes for SLA and Policy Management

No.	Task Activities	Status as of Y2	Description	Section	To be Addressed in Y3–Y4
2.1	Presentation of monitoring information of the managed system	DONE	Finding appropriate observables directly related to business indicators	Section 4.1	–
2.2	Manipulation of managed system to maintain expected service performance	DONE	Policy enforcement to optimise the identified business indicators	Section 4.1	–
2.3	Policy refinement and analysis	DONE	Relating the business indicators with the management policies by means of mapping functions	Section 4.1	–

Table 3: Task T7.3-Outcomes for Legal and Regulative Constraints

No.	Task Activities	Status as of Y2	Description	Section	To be Addressed in Y3–Y4
3.1	Determining QoS fulfillment aspects	FUTURE	-	-	Fulfillment aspects of QoS will be studied from legal and regulative perspective
3.2	Policy-based aspects in view of legal or regulative limitations	FUTURE	-	-	Legal and Regulative implications on business modeling will be studied
3.3	Cost and accounting models in view of legal or regulative limitations	IN PROGRESS	Regulative aspects of incentive auctions are being studied	Section 5.5	Legal and Regulative implications on cost and accounting models will be studied
3. 4	Network neutrality aspects for management	IN PROGRESS	Regulative aspects of network neutrality are being studied	Section 5.4	Legal and regulative aspects of network neutrality will be studied in more depth
3. 5	Investigating adoption of cloud-based solutions from legal and regulative perspective	IN PROGRESS	Regulative aspects of cloud storage and resource allocation are being studied	Section 5.5	Constraints from legal and regulative point of view in cloud adoption process will be studied
3. 6	Investigating legal and regulative constraints of data sharing due to the analysis of data in network and service management	IN PROGRESS	Legal and Regulative aspects of data storing, data sharing, data retention are being studied	Section 4.3.1 to 4.3.2, Section 5.1 to 5.3	Legal and regulative aspects in these areas will be studied in more depth

By addressing the overall goal, the following three targets are addressed by the methodology chosen: First, to understand the considerations from the business, economic, legal and regulative perspective so that interdependencies can be established. Second, to establish guidelines for suitable models for techno-economic interdependencies, legal, and regulative recommendations. Third, to perform detailed analysis of scenarios that are part of FLAMINGO's technical scope, especially from WP5 and WP6.

Taking the analysis ahead, as done in Y1 of FLAMINGO, appropriate and relevant scenarios, which in terms of their technical content are based on the objectives of WP5/WP6, the area of research focusses on network and service monitoring, which also addresses virtualization strategies, content delivery, and automated configuration and repair of managed objects. To this end, six major scenarios are identified and analyzed (as described in Section 3). Based on the relevance and scope four of these scenarios (iMinds-UPC-NetVirt, UCL-iMinds-Cache, UCL-UPC-BOSM, UZH-UniBwM-JUB-M2) were already part of WP7 since the beginning of the project. In Y2, these four scenarios, have covered more in-depth analysis as compared to the newly included scenarios. For project Y2, the focus has been laid on the scenarios to identify the interrelations between the three pillars, which form the basis of the work within WP7.

2.3 Document Structure

The remainder of Deliverable D7.1, entitled "Design and Selected Mechanisms", is structured in the following manner. Section 3 "Scenario Descriptions and Design Constraints", summarizes and describes scope of the scenarios involved in WP7. This is done based on boundary map, stakeholder analysis, and risk analysis. Section 4 "Goals and Considerations driving Selected Scenarios of Network and Service Management', addresses the business, economic, and legal considerations in the field of network and service management. Section 5 "Status-quo of Selected Current Regulations Impacting Network and Service Management", discuses the current status quo and open issues in regulations impacting the field of network and service management. Section 6 "Validation of Scenarios and Mechanisms" concentrates on validating the work within WP7 through several mechanisms. Section 7 finally summarizes, concludes the current work and discusses the work foreseen. Section 8 "WP7 Objectives", lists the objectives of WP7 as stated in the FLAMINGO Description of Work and reports their status. Section 9 "Abbreviations", lists all the abbreviations used in the deliverable D7.1. Section 10 "References", contains details of all the references used within the deliverable. Section 12 "Appendices", contains all filled in questionnaires from the external partners collected during the interview-based validation approach.

3 Scenario Descriptions and Design Constraints

The overall WP7 work as well as all WP7-related tasks had been structured efficiently by applying project management and research techniques. Especially for describing the clear design scope of a scenario and to work within each scenario with appropriate techniques and valid assumptions (1) a Boundary Map, (2) a Stakeholders' Analysis and Stakeholders' Map, and (3) a Risk Analysis have been applied. This leads to a well-determined set of boundaries, which are essential to carefully target the scenarios' findings.

3.1 Techniques

To provide a a brief overview on these techniques, the basic principles of the Boundary Map, the Stakeholders' Analysis and Stakeholders' Map, and the Risk Analysis are outlined here. In turn in subsequent subsections those three techniques have been applied to all WP7 scenarios ensuring a determination of key assumptions, stakeholders involved, and the related risks.

Boundary Map: Research projects are in their nature never-ending. New questions appear as results are generated. Thus, defining the boundaries is an important step towards managing such projects. With the project group discussions are done to identify where are the boundaries of the project as seen from the scenario today.

"The boundaries of a project are measurable and auditable characteristics that define what belongs to the project and what does not belong to it. Project boundaries are closely linked to project objectives, they create a holistic perception of project work, and they define the content of the project in terms of expected results. A clear boundary statement helps direct the things that are applicable to those areas within the project scope" [4].

Stakeholders' Analysis and Stakeholders' Map: The purpose of this is to visualize (i) the interest, (ii) the influence, and (iii) the attitude of each stakeholder that is involved in a scenario.

Approach:

1. Create a list of all stakeholders
2. Define their interest in the project (Low, Medium, High)
3. Define their influence in the project (Low, Medium, High)
4. Define their attitude in the project (Positive, Neutral, Negative)
5. Draw the stakeholder map

Risk Analysis: The risk analysis helps to define what are the potential problems that might occur, and help to think in advance of possible measures to eliminate, or reduce the risk. Stakeholders that identified during the stakeholders' analysis to have a negative attitude should be also reflected in the risk analysis.

Approach:

1. Collect possible risks that are related with (a) Content, (b) Resources, (c) Time dependencies, (d) Stakeholders, and (e) Context
2. Estimate the probability (PB_R) of a risk (Low=1, Medium=2, High=3)

3. Estimate the impact (IMP) of a risk (Low=1, Medium=2, High=3)
4. Calculate the risk factor $R = PB_R \cdot IMP$
5. Identify A-risks, B-risks, C-risks according to the risk matrix (cf. Figure 1)
6. Identify the possible causes of each risk
7. Propose possible measures that can eliminate or reduce the risk
8. Address first risks with high risk factor R

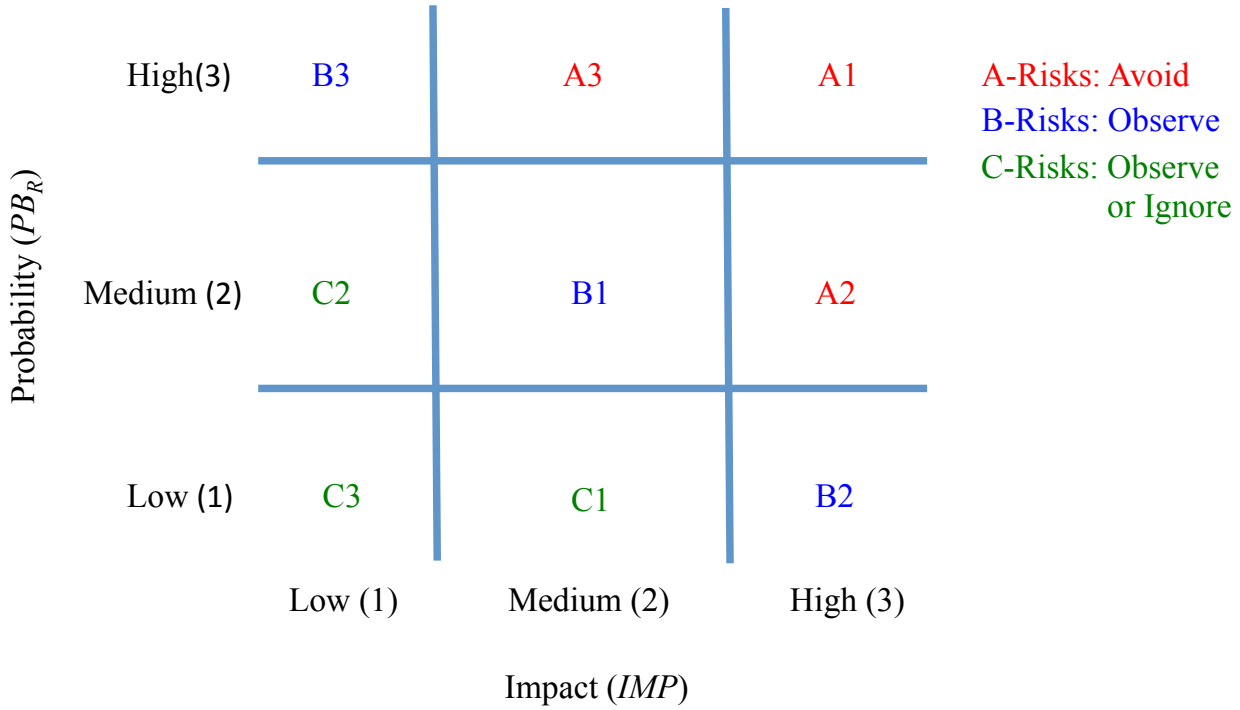

Figure 1: Risk Table.

Approach:

1. Ask yourself:
   What is the project all about?
   What do we have to know?
   What is interesting for us?
   What does this scenario have to deliver?
   What are the possible applications of the outcome of this scenario?
   Which topics have to be worked on in the scenario to reach the scenario's/FLAMINGO's objectives?
   Which not?
   Where could we limit the scope?
2. Draw the project's boundary to include the topics that (a) definitely, (b) maybe, and (c) certainly not belong to the project.

These approaches of project management are used in the following sections to describe the scenarios, which are studied within WP7. These approaches provide a unified and homogeneous method to describe the scenarios under the umbrella of WP7.

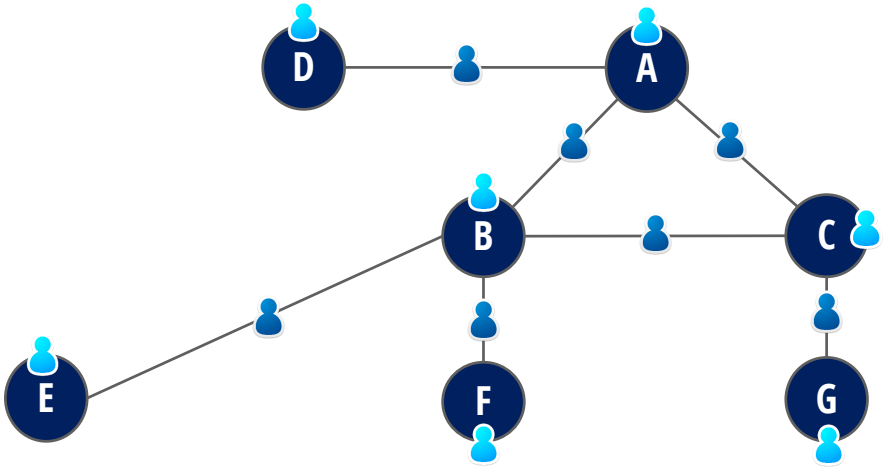

Figure 2: Substrate Network Represented by Agents

3.2 Resource Management in Virtualized Networks

This joint research activity, is a collaboration between iMinds and University Politecnicà de Catalunia (UPC), and is referred by iMinds-UPC-NetVirt. Network virtualization provides a mechanism for allowing multiple Virtual Networks (VN) to share resources from one or more Substrate Networks (SN) [10]. These resources - for any given VN - are completely isolated from the others, and appear as though they belong to different physical networks. VN operators can then lease these resources to other VNs, or use them to provide services to end-users, allowing them to establish multiple specialized and flexible networks that are driven by end user requirements. One key requirement in network virtualization is the allocation of resources. This can be divided into two stages: Virtual Network Embedding (VNE), and Dynamic Resource Management (DRM). VNE involves embedding virtual nodes and links to substrate nodes and links respectively, while DRM includes the adaptation of actual resources allocated to virtual nodes and links to the actual needs of the virtual networks, aimed at achieving efficient resource utilization. Efficiency, optimality and flexibility of resource allocation are fundamental factors for network virtualization to be successful. While VNE is a well studied problem [35], most current approaches to DRM allocate a fixed amount of resources to the virtual nodes and links for their entire lifetime irrespective of actual utilization [64]. As Internet traffic is not static, this could lead to an inefficient utilization of overall network resources, especially if a substrate network rejects requests to embed new VNs while reserving the resources for VNs that are lightly loaded. In this research, we propose two dynamic resource management approaches for network virtualization, described as follows:

The first approach opportunistically allocates resources to virtual nodes and links depending on the perceived needs. The opportunistic use of resources involves carefully taking advantage of unused virtual node and link resources to ensure that VN requests are not rejected when resources reserved to already embedded requests are idle. Therefore, we use a demand-driven dynamic approach [64] that allocates resources to virtual nodes and links using Reinforcement Learning (RL) [90]. Our proposal is that after the initial VNE step, resources allocated to each virtual node and link should be monitored and adjusted to reflect both actual resource need by the virtual network, and resource availability in the substrate network. To this end, as shown in Figure 2, we represent each substrate node or link as an agent. These agents are tasked to monitor the resource utilization of all mapped virtual nodes and links, and comparing this with the available substrate resources, re-allocations are performed. The agents then monitor the network to determine its performance, for example through parameters such as packet delay and drop ratio, and based on these statistics, the agents use machine learning techniques to make better actions for future resource allocations.

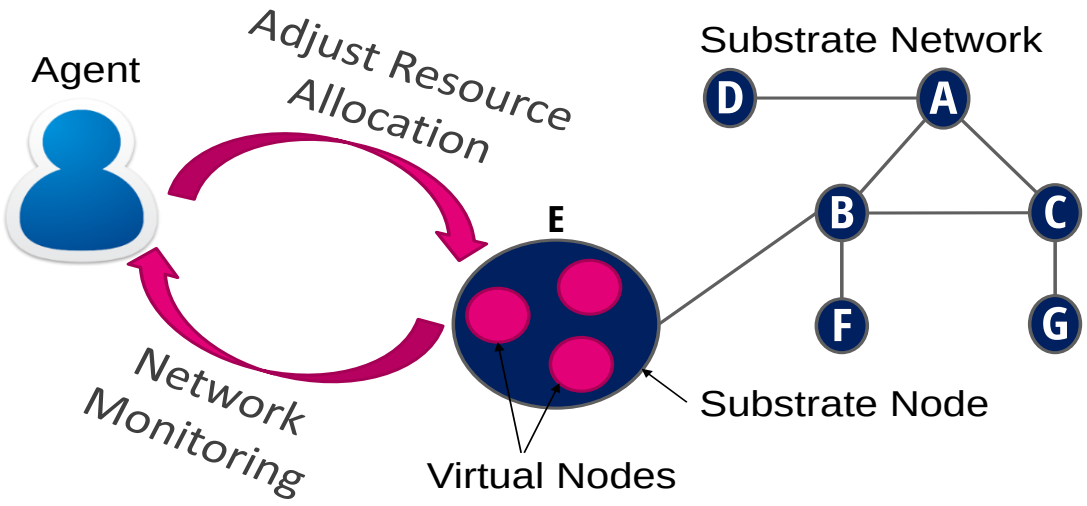

Figure 3: Proposed Dynamic Resource Management Approach

We show in Figure 3 the general process involved by each agent. Detailed information about the current status of this research may be found in [64], [65] and [66].

Our second approach is based on the observation that it is possible to over-sell the substrate network resources with the objective that the mapped virtual networks load the substrate network in an efficient way, and hence improve the profitability of infrastructure providers. To this end, the proposal is to continuously forecasts expected demand for substrate network resources, and based on this makes decisions the respective percentages by which each substrate node and link can be over provisioned. The task is to strike a balance between the conflicting objectives of over-selling the substrate resources as much as possible, yet ensuring that at any time, each of the virtual network is able to use its maximum reserved resources when needed.

The contributions of collaboration work will be three-fold:

1. A substrate resource forecasting approach that learns from the history of virtual network resources requests to predict future resource requests.
2. A dynamic pricing scheme that uses virtual network traffic predictions and hence expected opportunity cost (with respect to Infrastructure Provider (InP) profit from VNE) to price substrate nodes and links.
3. A virtual network embedding algorithm that uses future demand forecasts other than actual resource constraint to accept or reject virtual network requests.

Boundary Map: The boundary map that has been identified between this collaboration's members is illustrated in Figure 4. Any task that is out-of-scope, can become the start point of either a new collaboration, or an extension of this collaboration for the future.

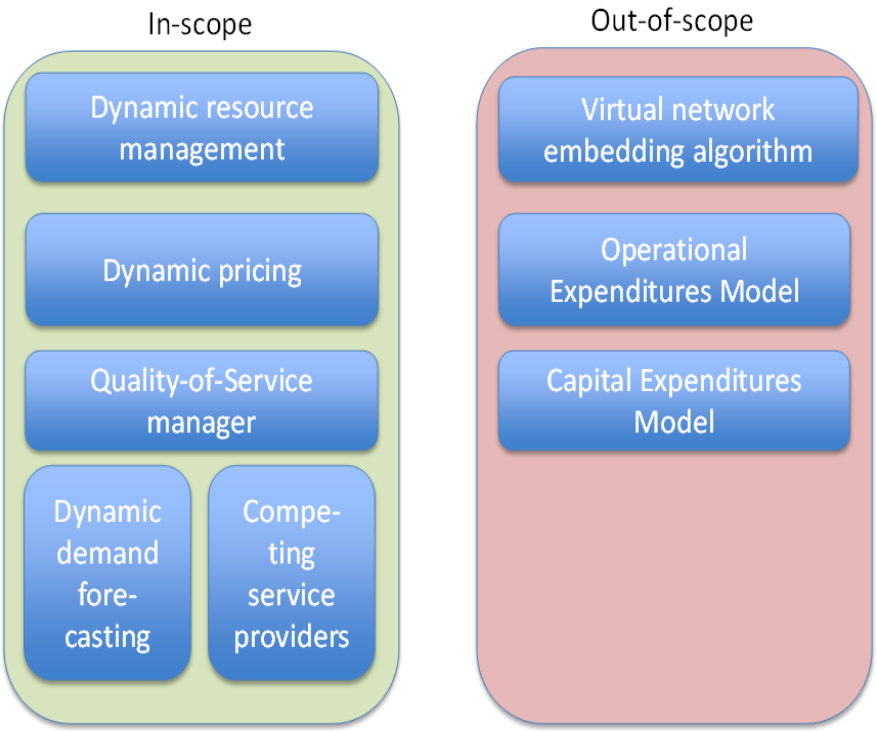

Figure 4: The Boundary Map of Resource Management of Virtualized Networks

Stakeholders' Analysis and Stakeholders' Map: The stakeholders list is summarized in Table 4 and the stakeholders map is illustrated in Figure 5. The goal is (a) to increase as much as possible the interest of every stakeholder, and (b) to change, if possible, negative to neutral, or even positive, the attitude of stakeholders with high influence.

Table 4: Stakeholders Analysis of the Resource Management of Virtualized Networks

Stakeholders	Interest	Influence	Attitude
Service Provider (SP)	Medium	Low	Neutral
Virtual Network Provider (VNP)	High	Low	Positive
Infrastructure Provider (InP)	Medium	Low	Neutral
Regulator (REG)	Low	Low	Neutral
FLAMINGO partners (FP)	Medium	High	Positive

Risk Analysis: The list of the potential risks that has been identified during the risk analysis phase are in Table 5. The risk analysis shows that the main risk that this collaboration is facing is to not be able reliable cost data from the InP.

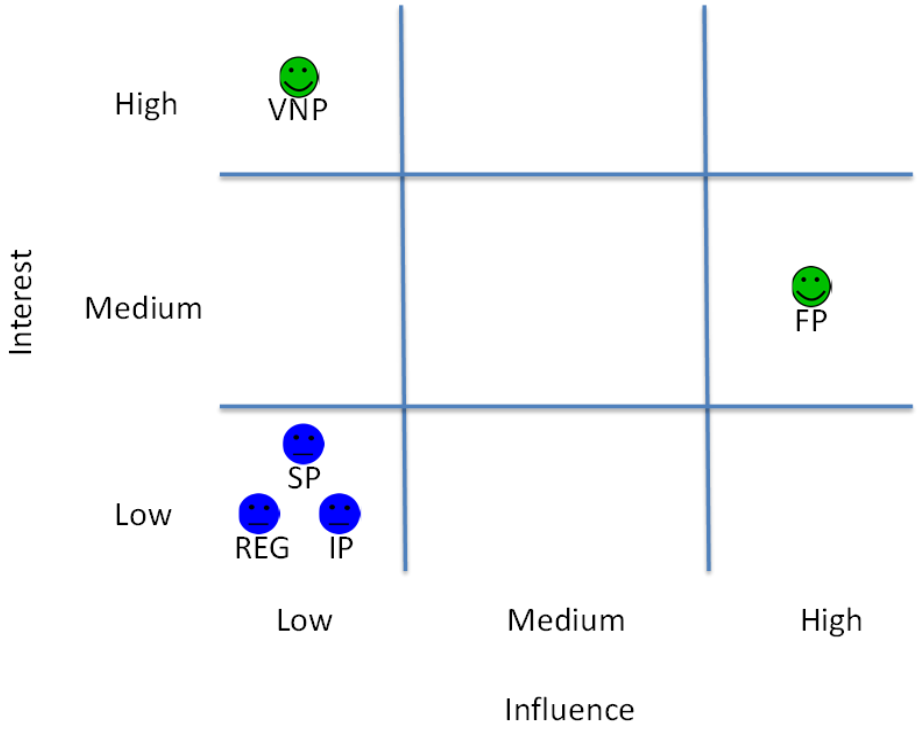

Figure 5: The Stakeholders Map of the Resource Management of Virtualized Networks

Table 5: Risks of the Resource Management of Virtualized Networks

Risk	PB_R	IMP	R	Priority	Possible Cause	Measure
Lack of reliable cost data	1	2	4	B1	Data is sensitive	Collect early and work with relative values

3.3 ISP-oriented Content Delivery

This joint research activity, is a collaboration between University College of London (UCL) and iMinds, and is referred by UCL-iMinds-Cache. Content Distribution Networks (CDN) are distributed systems of servers spanning different geographic locations. The goal of a CDN is to serve content to end-users across the Internet. Current content delivery services operated by large CDN providers can exert enormous strain on Internet Service Provider (ISP) networks. This is mainly attributed to the fact that CDN providers control the placement of content in surrogate servers spanning different geographic locations, as well as the decision on where to serve client requests from (*i.e.,* server selection). In contrast, CDNs lack knowledge of the precise network topology and state in terms of traffic load. This may result in network performance degradation.

In this joint research activity, a scenario where ISPs deploy its own caching infrastructure is being investigated. The service, ISP oriented content delivery, is an extension to the traditional role of an ISP. To this end, as shown in Figure 6, The ISP provides both caching space and connectivity infrastructure for the distribution of content to end users.

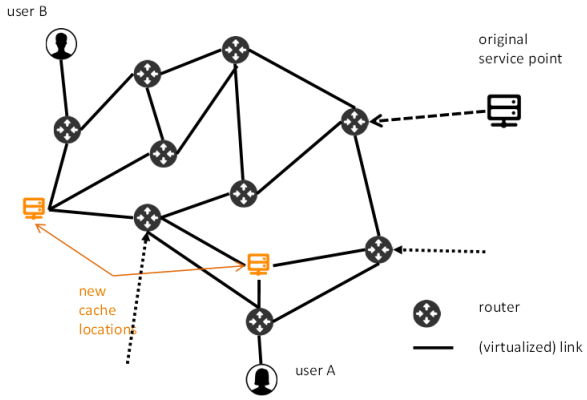

Figure 6: The ISP-oriented Cache Management

The objective of the work is to develop a model to quantify the benefits for an ISP of deploying its own caching infrastructure. These benefits are expressed as business indicators (BI). The BI considered in the ISP oriented content delivery scenario are: (1) the (long-term) investment cost for the ISP and (2) the Quality-of-Experience (QoE) for the end user and service provider.

To analyze the investment cost for the ISP, we determined the network setting to consider. This concerns the physical topology to use, the configuration of the caching infrastructure, the traffic demand to consider, as well as the routing and cache management policies. Next, we have started on collecting data to build a cost model for the different network elements. In this context those are IP/MPLS routers, transponders, photonic switching gear, fiber links, caching equipment and peering rates. To analyze the effect on the QoE the delay between requesting content and consuming it will be considered. The deployment of caching infrastructure operated by the ISP will allow some requests to be directly served from within the network. This can, therefore, affect the delay in accessing content and a such the QoE as perceived by the end user. To further analyze this scenario a boundary map, stakeholders' map and risk analysis were conducted.

Boundary Map: The boundary map that has been identified between this collaboration's members is illustrated in Figure 7. Any task that is out-of-scope, can become the start point of either a new collaboration, or an extension of this collaboration for the future.

Table 6: Stakeholders Analysis of the ISP-oriented Cache Management

Stakeholders	Interest	Influence	Attitude
Content Producer (CP)	Medium	Low	Neutral
Content Delivery Network (CDN)	High	Low	Negative
Internet Service Provider (ISP)	High	Medium	Positive
Regulator (REG)	Medium	Medium	Neutral
FLAMINGO partners (FP)	Medium	High	Positive

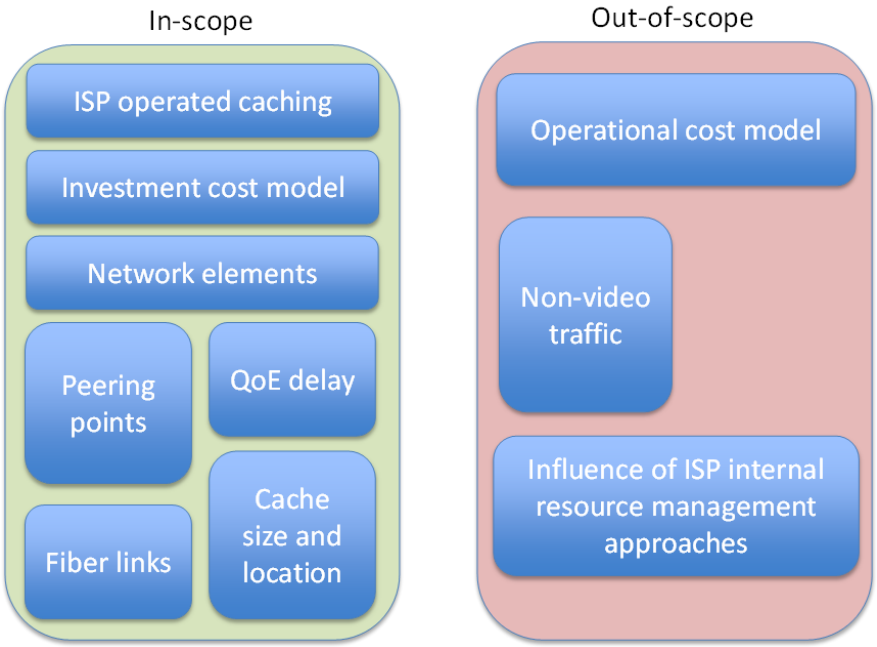

Figure 7: The Boundary Map of ISP-oriented Cache Management

Stakeholders' Analysis and Stakeholders' Map: The stakeholders list is summarized in Table 6, and the stakeholders map is illustrated in Figure 8. The goal is (a) to increase as much as possible the interest of every stakeholder, and (b) to change, if possible, negative to neutral, or even positive, the attitude of stakeholders with high influence.

Risk Analysis: The list of the potential risks that has been identified during the risk analysis phase are in Table 7. The risk analysis shows that the main risk that this collaboration is facing is to not be able reliable cost data from the infrastructure provider.

Table 7: Risks of the ISP-oriented Cache Management

Risk	PB_R	IMP	R	Priority	Possible Cause	Measure
Lack of reliable cost data	2	2	4	B1	Data is sensitive	Collect early and work with relative values
Unpredictability of the traffic dynamics	1	2	2	C1	Demand dynamics	Favor reactive approaches compared to proactive ones

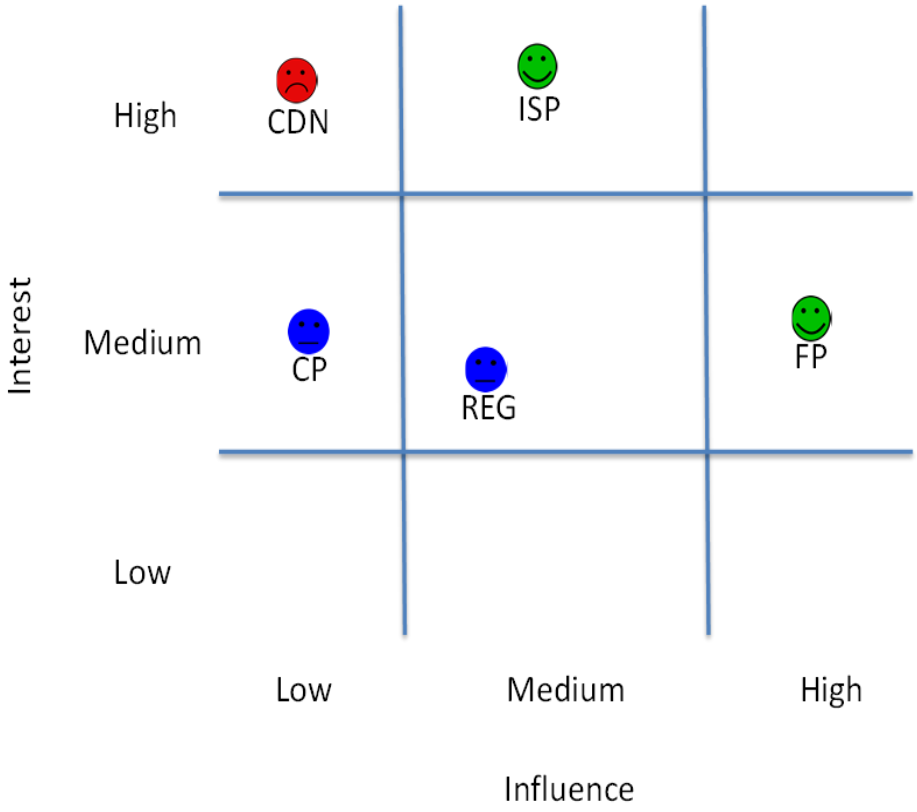

Figure 8: The Stakeholders Map of the ISP-oriented Cache Management

3.4 Business-oriented Service Management

The performance of services offered by network operators has direct impact on its reputation, on its revenue due to new customer subscriptions, but also on penalties that can apply when services are not provided to an acceptable quality level. Previous research on business-oriented network and service optimization (*e.g.,* [82]) has mainly focused on optimizing individual business indicators, such as profit and revenue, in isolation without analyzing the effect on network configurations and the subsequent impact on other indicators. Given that different business objectives are usually incompatible, a single network configuration cannot optimize them simultaneously.

As an example, consider two representative BIs that relate to: (a) the volume of service subscriptions, and (b) the level of service satisfaction. A network operator prioritizing the former BI will have a higher economic benefit by taking actions to maximize the number of subscribers. These actions, however, could have a negative impact on service satisfaction since an excessive number of users could eventually cause resource starvation by injecting too much traffic in the network. Consequently, it is necessary to develop appropriate mechanisms that can determine trade-offs between BIs and also to ensure that the underlying policy-based control mechanisms optimize the BIs according to administrative strategies. The objective of the collaboration between UPC and UCL is to bridge this gap and develop an approach for deriving policy configurations that optimize the business value of the network infrastructure. This scenario is referred as UCL-UPC-BOSM.

To achieve this objective our approach relies on the representation of business strategies as business indicators that have been modeled as objective functions of measurable parameters of the

network infrastructure. These are quantified according to the network state and service usage and are used to drive the optimization process. To determine the trade-offs in the presence of multiple objectives evolutionary algorithms are used. These take as input the range of possible parameter values and their relationships with BIs, and fine-tune the configuration according to network state feedback. The proposed approach is validated in the context of DiffServ QoS management and more specifically admission control, where the developed mechanism determines policy parameter values that best reflect business-oriented service management preferences.

To further analyze this scenario a boundary map, stakeholders' map, and risk analysis were conducted.

Boundary Map: The key areas of in-scope versus out-of-scope for this scenario are listed in the scenario's boundary map as shown in Figure 9.

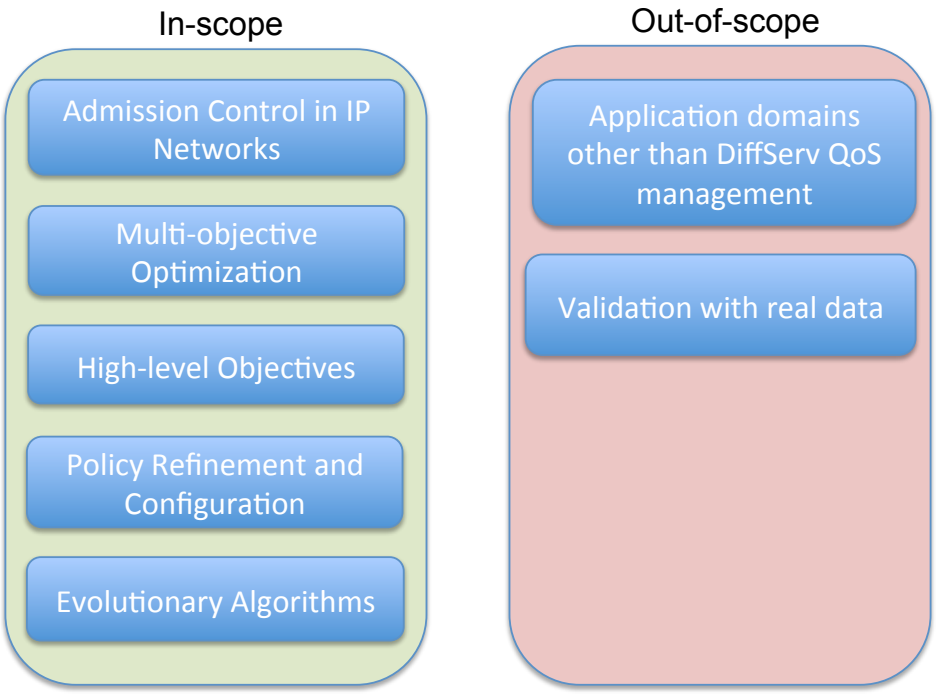

Figure 9: The Boundary Map of Business-oriented Service Management

Stakeholders' Analysis and Stakeholders' Map: The stakeholders list is summarized in Table 8, and the stakeholders map is illustrated in Figure 10.

Table 8: Stakeholders Analysis of Business-oriented Service Management

Stakeholders	Interest	Influence	Attitude
Network Operator (NO)	High	Medium	Positive
End-user (EU)	High	Low	Positive
Regulator (REG)	Medium	Medium	Neutral

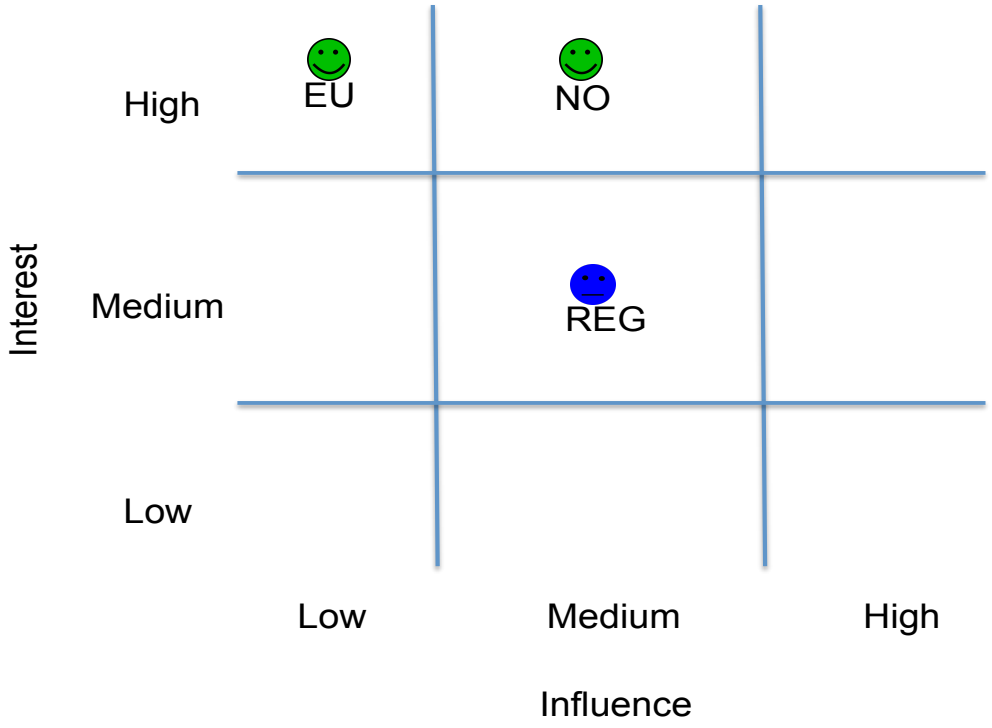

Figure 10: The Stakeholders Map of Business-oriented Service Management

Risk Analysis: Table 9 lists the main risks that have been identified during the risk analysis phase. These concern the data availability (topology, traffic traces, service invocation patterns) from the network operator, which could allow a more realistic evaluation of the developed approach, and also the unpredictability of service invocations due to user behavior.

Table 9: Risks of Business-oriented Service Management

Risk	PB_R	IMP	R	Priority	Possible Cause	Measure
Lack of real NO data (topology, traffic traces, service invocation patterns)	3	1	3	B3	Data sensitivity	Work with synthetic data
Unpredictability of service invocations	1	3	3	B2	User behavior	Improved prediction

3.5 Mobile Measurements

FLAMINGO's Mobile Measurement scenario will be conducted by a mobile application, which gathers technical parameters such as latency, jitter, packet-loss, and bandwidth. This is joint collaboration between University of Zurich, Universität der Bundeswehr München (UniBwM), and Jacobs University Bremen (JUB), and is referred as UZH-UniBwM-JUB-M2. The collection of those parameters is initiated by the end-user and the results are fed into a QoE model that generates a ITU-T compliant MOS. Based on this data, QoE for services in MNOs for this user is quantified.

The USA regulator Federal Communications Commission (FCC) does something similar concerning ISPs quality by asking a company to perform some measurements. Those measurements are

publicly available to the respective users so that they know what quality they can expect when selecting a specific ISP. The same idea is transferred to mobile networks so end-users can use this service to estimate the QoE of a given MNO at a given location. Such an approach can be seen as an incentive for MNOs to provide better and more reliable services.

Quality-of-Service metrics have been traditionally used to evaluate the perceived quality of services delivered by network operators. However, these metrics are not suitable for evaluating the experience of an end-user. The experience of a user is quantified based upon different activities, such as speed of Web page loading, quality of video streaming, or voice quality of an Internet-telephony.

Due to the temporal and geographical nature of mobile networks, the perceived experience of a user may change based on location and time. Mobile operators may prioritize certain services over others, leading to a service type dependent QoE. In this work FLAMINGO presents a mobile application developed to gather metrics necessary to evaluate QoE in a mobile environment. The approach towards obtaining not just a general, but service-specific Mean Opinion Score (MOS) to quantify QoE is also discussed.

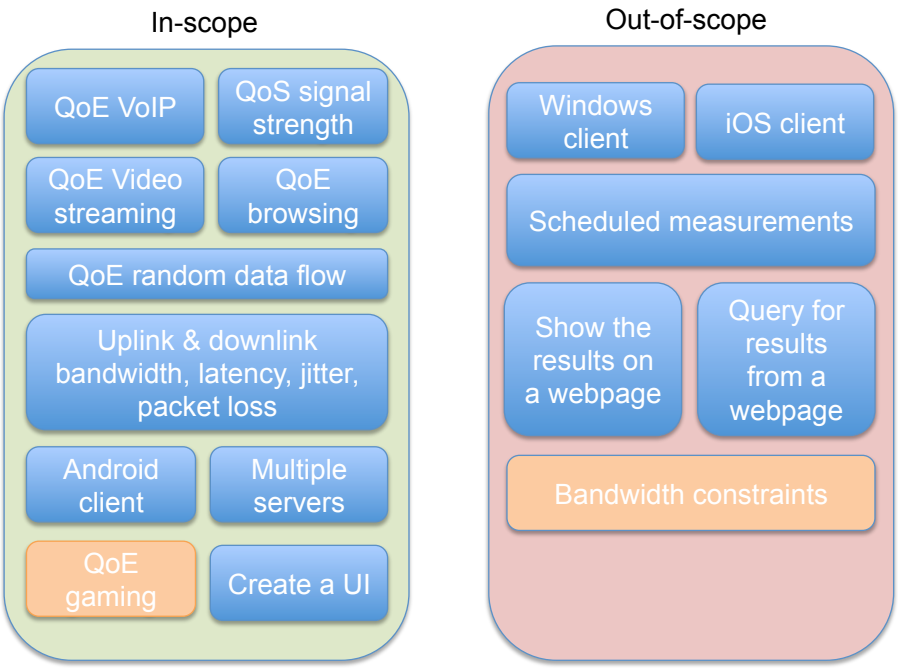

Figure 11: Boundary Map of the Mobile Measurement

For this purpose FLAMINGO measures technical parameters, such as, uplink and downlink bandwidth, and latency of specific protocols data such as, RTSP, SIP, RTP, HTTP, and torrent. Then an expected MOS is created, considering major requirements of each protocol, and this MOS is illustrated on a map.

Boundary Map: The key areas of in-scope versus out-of-scope for this scenario are listed in the scenario's boundary map as shown in Figure 11.

Stakeholders' Analysis and Stakeholders' Map: Concerning the stakeholders analysis and the respective stakeholders map, stakeholders of relevance are listed in the following Table 10.

Table 10: Stakeholder Analysis of the Mobile Measurement

Stakeholders	Interest	Influence	Attitude
MNOs	High	High	Negative/Positive
Regulators (REG)	Low/Medium	Low	Neutral
Similar App developers (SAD)	Medium	Low	Negative
End-users (EU)	High	High	Positive/Neutral
FLAMINGO partners (FP)	Medium	High	Positive

The respective stakeholders map, as illustrated below, identifies the cross-check on interest versus influence (all in a “low”, “medium”, or “high” characteristic). The goal is (a) to increase as much as possible the interest of every stakeholder and (b) to change, if possible, negative to neutral (or even to positive), the attitude of stake-holders with a high influence. This change can only be arranged for if the mobile measurements data provided assure the stakeholder involved that a change of behavior is deemed necessary.

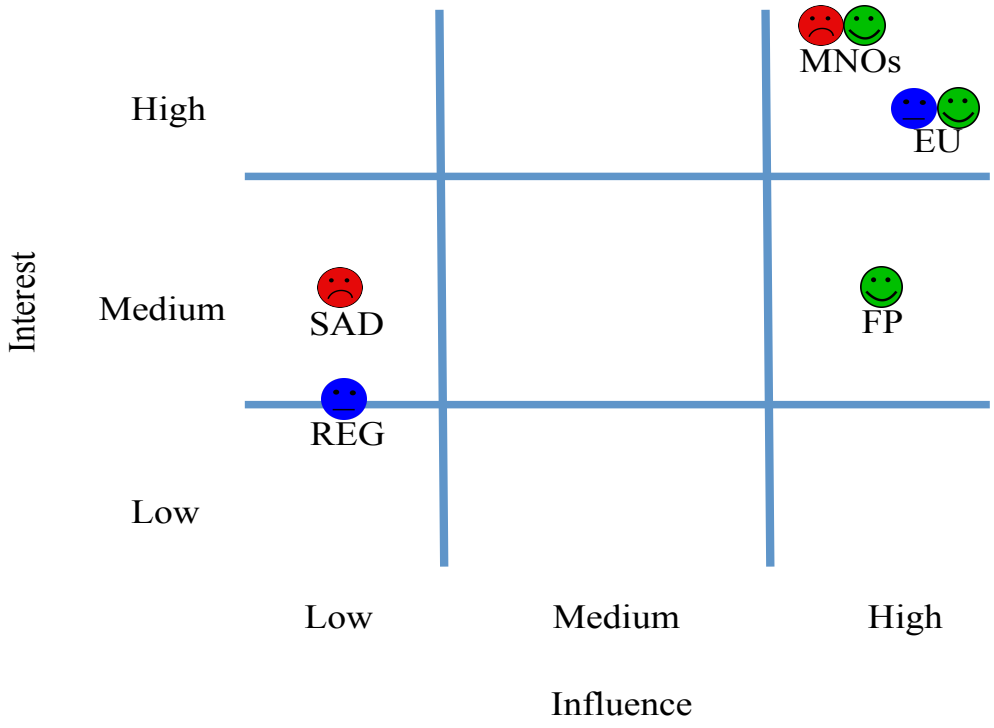

Figure 12: The Stakeholders Map of the Mobile Measurement

Risk Analysis: The list of the potential risks that has been identified during the risk analysis phase are shown in the following table. The risk analysis reveals that the main risk is to be unable to collect a sufficient amount of data from end-users to provide the basis for a thorough understanding if there exists any correlation between the type of traffic, the time and the day, and end-users’ QoE, which are relevant for data services of mobile networks.

Thus, the main goal once the data collection application is released, is to put major effort on the increment of the application’s user-base. Finally, effort is needed to be invested on making the measurable data and evaluation method transparent to every stakeholder involved, especially to avoid conflicts with MNOs.

Table 11: Risks of the Mobile Measurement

Risk	PB_R	IMP	R	Priority	Possible Cause	Mesure
MNOs block traffic to our servers	1	3	3	B2	They feel that our result harm their reputation	Make clear what and how is measured and why is accurate
Not enough data	3	3	9	A1	End-users don't use the App	Advertise?
The servers are not responding	1	2	2	C1	Too many users use the App	Update the H/W
The App drains end-user's data	2	2	4	B1	Too many measurements	Notify the user about the volume of data needed prior to a measurement

3.6 Legal and Ethical Facets of Data Sharing

The scenario and the collaboration described in this section is born in the context of the Dagstuhl seminar "Ethics in Data Sharing" [17], which took place in January 26th – January 31st 2014. The seminar, which accounted among the organizers also A. Pras (UT), brought together experts from the legal, ethical and technological aspects of data sharing and data consuming, and it started fruitful discussion about the pro and cons of data sharing and the options and needs of the various involved parties. A follow-up effort from the Dagsthul seminar is the collaboration between SURFnet BV (the Dutch National Research and Education Network), University of Twente, University of Amsterdam, Tilburg University and University of Zurich, and is referred as UT-UZH-Ethics.

Scientists, often face the need for data on which the investigations and validation of approaches is based. A chief example of such data is, for the research conducted in this Network of Excellence, various flavors of network data. However, such data is not always directly accessible to researcher. For example, not every researcher has the possibility, equipment or is allowed to measure network data on his/her institution infrastructure; or the type of research calls for a larger measurements than an institution network; or again, the type of data needed for the research have to be collected with the permission of the end-users.

A pivotal role in data sharing and acquisition is played by ISPs and Network Operators (NO). However, sharing network data with third parties, although for academic research purposes, carries intrinsic ethical and legal concerns. This is because, although data are often aggregated, in some case they may still contain user-identifiable information, or the type of data is by law considered personal information.

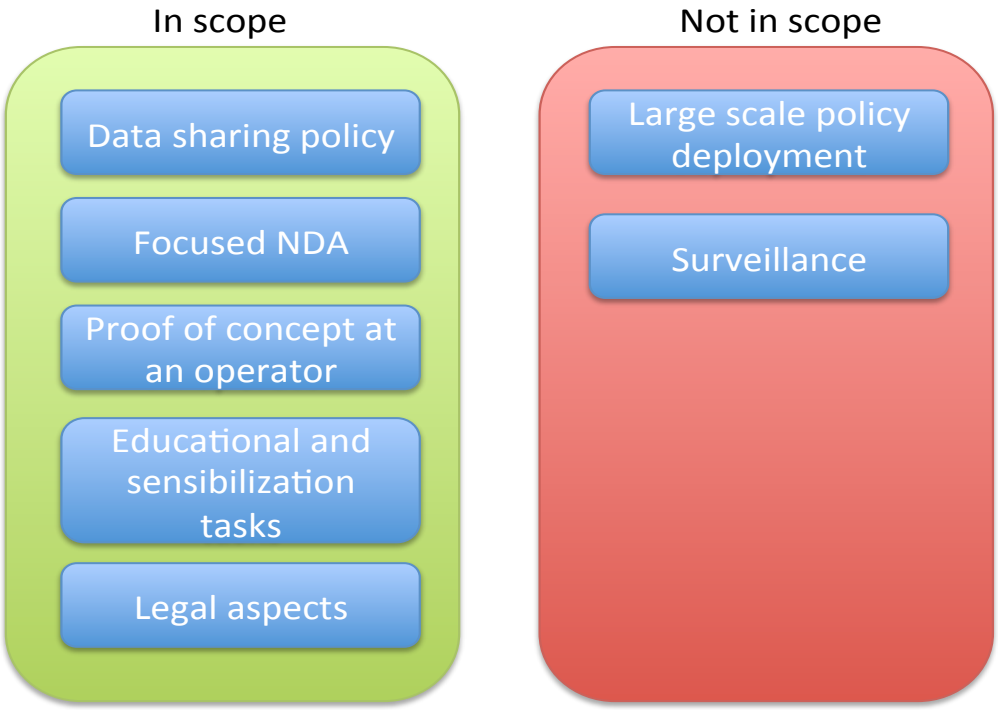

Figure 13: The Boundary Map of Legal and Ethical Facets of Data Sharing

The goal of this collaboration is to establish an ethical guideline for facilitating data sharing between operators and researcher. Such a guideline will provide a step forward from the current practice of data sharing, which is ad-hoc and essentially based on the idea of sharing with "trusted parties",*i.e.,* with researcher we know and we can reasonably assume will conduct proper research. However, the current situation is far from optimal from several aspects. A strategy of establishing a common knowledge between the data provider and the data consumer is missing, the ethical aspects are left to the separate consideration of data provider and data consumer, Non-disclosure Agreements (NDA) are often too generic, and reproducibility of results by other researcher can become difficult.

Table 12: The Stakeholders Analysis of Legal and Ethical Facets of Data Sharing

Stakeholders	Interest	Influence	Attitude
Data provider/Network Operator (DP)	High	High	Positive
Data Consumer/Researcher (DC)	High	Medium	Positive
Ethical Committee (EC)	High	High	Positive

The partners involved in this scenario are currently working on several aspect of the data sharing problem. From the one side, they are working on the creation of a policy for facilitating data sharing between operators and researcher. SURFnet is strongly leading this task and will implement the policy in its data sharing procedure. On the other hand, the partners are working towards educational measures to raise researcher awareness to the problem of consciously frame their research scope, structure their data requirements and identify ethical concerns.

Boundary Map: The boundary map in Figure 13 describes the activities that will be carried on in this scenario, and the ones that are out of scope at this point in time. The legal aspects of the scenario will be taken into consideration at a further moment in time.

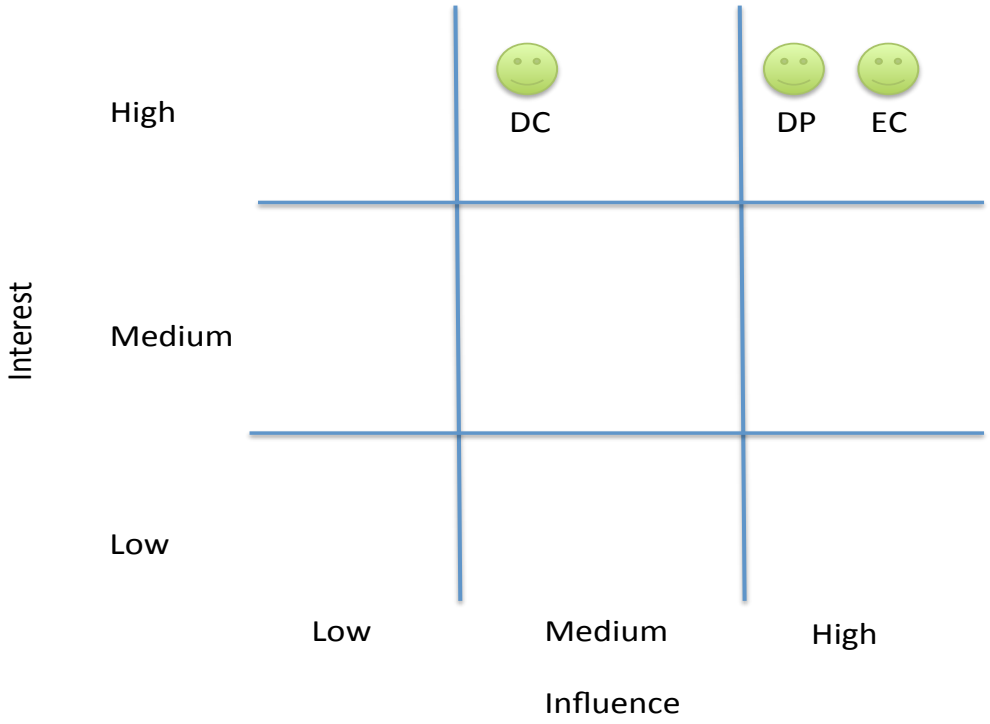

Figure 14: The Stakeholders Analysis of Legal and Ethical Facets of Data Sharing

Stakeholders' Analysis and Stakeholders' Map: Table 12 summarizes the stakeholder analysis for the scenario, while Figure 14 depicts in graphical form the stakeholder analysis.

Table 13: Risks of the Resource Management of Legal and Ethical Facets of Data Sharing

Risk	PB_R	IMP	R	Priority	Possible Cause	Measure
Ethical concerns	3	3	9	A1	Research not properly framed	Policy and guidelines
Un-responsible disclosure	1	3	3	B2	Lack of communication; mis-aligned expectations; lack of carefulness	Policy and guidelines
Issues with data curation	1	2	2	C1	Lack of resources; lack of carefulness	Policy and guidelines
Lack of timeliness	2	1	2	C2	Lack of resources	No solution

Risk Analysis: The list of potential risks for the considered scenario is listed in Table 13. The identified risks concern the possible side effects of the performed research in terms of ethical concerns. This is considered the risk with the highest impact, and the motivating one for the development of this scenario. The remaining risks cover issues such as how the results of the research can be disseminated and how the data should be stored and preserved (if necessary). Finally, the lastly identified risk cover the interaction between the researcher data consumer and the data provider, in case the data consumer need data with urgency (e.g., to capture a transitory phenomenon on the Internet).

4 Goals and Considerations driving Selected Scenarios of Network and Service Management

Network and service management have been tradditionally devoted to develop mechanisms to deliver end-to-end QoS in the Internet. Network monitoring, congestion prevention and solving, service subscriptions and invocations control, traffic engineering, resource management, mobility management, and other functions have been the centre of study in the network and service management area in wired and wireless networks. Although these functions have been proved to be efficient to control QoS delivery, the requirements, implications, and the incremental efforts to elevate the business value of network infrastructures aligned to legal and regulative constraints, have remained almost unexplored. This section, therefore, discusses the major aspects of business and economical goals/considerations and the legal and regulative status in the area of network and service management, focusing on key management scenarios considered in the FLAMINGO project.

4.1 Business Goals and Related Considerations

The ability to carry out business-oriented management introduces several challenging problems. Initially, business strategies must be properly modeled with appropriate business indicators, pivotal for the management of policies. Second, business indicators should be monitored and modeled as functions of measurable parameters of the managed systems. Third, the dynamicity of events occurring in the managed network should be constantly evaluated as to define proactive and corrective management actions enforced through policies. There is a need to define three main elements to carry out business-oriented management: i) business indicators, ii) enforceable policies that drive the business strategies, and iii) there is a need to relate the business indicators with the management policies by means of mapping functions.

Business Indicators (BI) are indicators that reflect the business strategies of a managed system's administrator. They can be used by service providers to define their preferences in achieving specific goals. They may relate to Service Management Objectives (SMO) and subsequently they can control the configuration parameters of the enforceable policies. Each BI can be relevant for the operator to some degree of importance and hence, the underlying management policies should control the network aligned to the importance the operator gives to each BI.

Configuration policies or enforceable policies are business-agnostic elements that are executed at the network or system elements to control their behavior and lifecycle. They are lowest-level policies committing to the actual implementation of the system.

Mapping functions are the analytical elements that can be used to bring the gap between business value and configuration management by considering the influence of BIs when generating enforceable policies. Mapping functions can that take into account the impact of BIs over management policies and they can be used to identify conflicts on contradictory business indicators. Consider, for example, two representative BIs that relate to: (a) The volume of service subscriptions, and (b) the level of service satisfaction. A network operator prioritizing the former BI will have a higher economic benefit by taking actions to maximize the number of subscribers. These actions, however, could have a negative impact on service satisfaction since an excessive number of users could eventually cause resource starvation by injecting too much traffic in the network.

The remaining of this section will elaborate on these three main aspects for representative scenarios of FLAMINGO: Management of Differentiated Services, Resource Management in Virtualized Networks, Quality Improvement, ISP-oriented Content Delivery, and Mobile Measurements.

4.1.1 Resource Management in Virtualized Networks

Business Indicators: In the context of resource management in virtualized networks, we define two BIs: Losses due to virtual network blocking (l_{vnb}) and losses due to degradation in VN QoS, l_{qos}. In following sections, we define these BIs.

Losses due to VN Blocking, l_{vnb}: It is a measure of the revenue that the infrastructure provider looses by failing to embed virtual network requests due to resource constraints. This business indicator is important in two ways: First, it directly affects the bottom line of the infrastructure provider, and second, continuously rejecting virtual network requests could have a negative impact on the good will of the resource provider. If β is the average income earned from a successfully embedded virtual network, l_{vnb} is given by equation 1:

$$l_{vnb} = \beta \times \Big(\text{Total Requests} - \text{Accepted Requests}\Big) \tag{1}$$

Losses due to degradation in VN QoS, l_{qos}: It is the total amount of money that the substrate network would pay to the virtual networks as a result of violations in QoS requirements. This BI is affected by two aspects: the penalties due to packet drops (l_{pd}), and losses due to link delays (l_{ld}). l_{pd} is the penalty paid by the substrate network due to packets dropped by the virtual networks resulting from failing to avail the contracted node queue sizes, while l_{ld} is the penalty due to virtual network packets experiencing longer delays than contracted, resulting from the virtual links being assigned less than the contracted data rates.

$$l_{qos} = l_{pd} + l_{ld} \tag{2}$$

Configuration Policies: The management of both l_{vnb} and l_{qos} requires a careful balancing approach. If a high importance is attached to l_{vnb} over l_{qos}, the substrate network would increase its income from accepting virtual network requests. However, the high number of mapped virtual networks would compete for the available substrate resources, hence leading to more packet drops and high delays. This would lead to high penalties, hence increasing l_{qos}, which ultimately affects the profitability of the substrate network.

$0 \leq R_u^s \leq 1$ is defined as the percentage of a substrate resources, s (a substrate node or link) that are currently utilized (by mapped virtual nodes and links) at any time. In Figure 15, we define three important ranges for R_u^s. In particular, when $0 \leq R_u^s \leq R_A$ *i.e.,* the green region, the substrate node/link is lightly loaded, and can therefore map more virtual nodes/links with a high confidence that the QoS requirements of all mapped nodes/links will not be violated. However, the range $R_B \leq R_u^s \leq R_C$ *i.e.,* the red region presents a possibility that some of the virtual nodes/links could have their QoS violated. The actual values of R_A, R_B and R_C are set dynamically by monitoring and making comparisons of the actual virtual network packet drops and link delays with the actual contracted values. Even if the objective is to accept more virtual network requests, there is a need to regulate the number of accepted virtual network requests. Four policies are defined, as shown in Table 14, two for each substrate node and two for a link. These policies regulate the number of virtual nodes/links that are mapped onto a given substrate node/link, as well as the maximum amount of resources that can be used by the mapped nodes/links. The polices are explained as follows:

Policies NP.1 and LP.1 define critical resource utilizations (CRU), $R_A \leq R_{cru}^u \leq R_C$ and $R_A \leq R_{cru}^{uv} \leq R_C$ for each substrate node u and link uv respectively. A CRU defines a point when a notification is triggered for a proactive action to be taken so as to prevent violations in virtual node and link quality of services. Therefore, if CRU is close to R_A, a notification is always issued early,

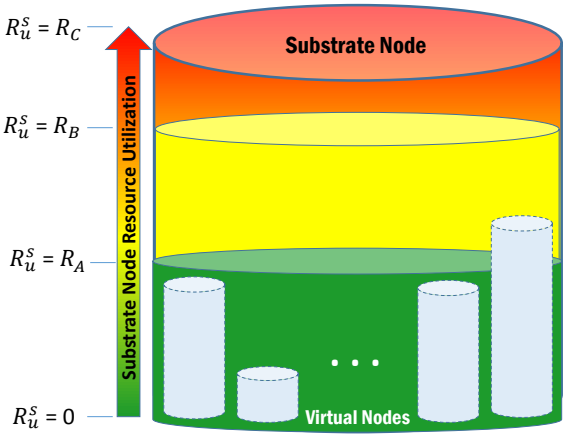

Figure 15: Definition of Substrate Resource Levels

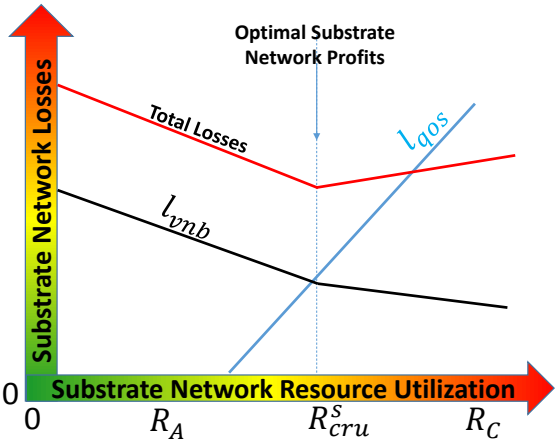

Figure 16: Business Indicator to Policy Mapping Functions

whereas values close to R_C result in delayed proactive actions. The run-time operation of the dynamic control is triggered by the CRU a set point, which activates policies polices NP.2 or LP.2 for adjusting the dynamic virtual network admission control (VNAC) values $R_A \leq R_{ac}^u \leq R_C$ and $R_A \leq R_{ac}^u v \leq R_C$ for substrate node u and link uv respectively. The values of $R_A \leq R_{ac}^u \leq R_C$ and $R_A \leq R_{ac}^u v \leq R_C$ control the acceptance of more virtual nodes or links by a given substrate node or link. The lower they are, the less the chances are of an incoming virtual network request being mapped onto the substrate node or link in question. A new virtual network request will be accepted only if the current utilization of the relevant Node or Link does not exceed $R_A \leq R_{ac}^u \leq R_C$ and $R_A \leq R_{ac}^u v \leq R_C$ respectively.

Mapping Functions: The mapping functions are represented in Figure 16, where three functions are shown. As the resource utilization increases, l_{qos} is initially 0 since the substrate network has enough resources to exceed the QoS requirements of the virtual network, while l_{vub} continuously reduces since the resources are used up by mapping more virtual networks. During this period, the total losses derived from both BIs continuously reduce, and hence it pays for the substrate network provider to continue accepting more requests. After some time, the virtual networks start competing for resources, and as a result, the losses due to QoS degradation start increasing. In the same way, since we have fewer resources, the mapping algorithm uses up more resources for mappings, leading to a reduction in the number of actual virtual network mappings per resource, and hence a reduction in the rate at which l_{vub} reduces. At this point, the rate at which the total losses for the substrate network reduces reduces, and this continues, until the losses start reducing. Therefore, if the CRU, R_{cru}^s is set close to R_C, it prevents a degradation in the QoS of VNs. This may allow currently mapped virtual networks to enjoy higher than contracted QoS values in terms of packet drops and delays (but without paying higher than the contracted costs), in addition to increasing the losses due to VN blocking, l_{vnb}. This would ultimately lead increased losses for the infrastructure provider. On the other hand, a CRU close to R_A would have the opposite effect on l_{vnb} since it allows the substrate network to accept a high number of network requests. This would increase the losses due to degradation in VN QoS, l_{qos} since many virtual networks would be competing for the substrate network resources. The aim is therefore to determine a value $R_A \leq \bar{R} \leq R_C$ which is the optimal CRU that allows for just the contracted quality of services for the virtual networks, while at the same time minimizing the losses due to rejected virtual network requests.

Table 14: Network Virtualization Policy Actions

Policy ID	Policy Action	Description
NP.1	setCRU(Node, R^u_{cru})	Sets the critical resource utilization, R^s_{cru}, for a Substrate Node, u
LP.1	setCRU(Link, R^{uv}_{cru})	Sets the critical resource utilization R^s_{cru} for a Substrate Link, uv
NP.2	setVNAC(Node, R^u_{ac})	Sets the admission control for accepting new virtual nodes onto Substrate Node u
LP.2	setVNAC(Link, R^{uv}_{ac})	Sets the admission control for accepting new virtual links onto Substrate Link with uv

4.1.2 ISP-oriented Content Delivery

Business Indicators: As described in deliverable D7.1, UCL and iMinds are investigating a scenario where ISP operate a small-scale content delivery network service by maintaining their own caching points in the network [101], [11], [12]. Apart from the additional revenue stream, ISPs can gain from improved control of network resources, while users benefit from the close proximity of content. The business indicators considered in this scenario are (i) QoE, which is expressed in terms of content access delay (*AccDelay*), and (ii) Bandwidth consumption (*BWcons*) within the ISP network.

Due to resource constraints only a subset of all available contents can be accommodated in the caching infrastructure operated by the ISP. While the requests for these contents can directly be served from within the network, all others need to be redirected to the origin servers (*i.e.* to the source of the content). This can, therefore, affect the delay in accessing a content item and, as such, the QoE as perceived by the user. Furthermore, a copy of a specific content item can be stored at more than one caching location in the network, i.e. content can be replicated. A high replication degree implies that a bigger portion of requests can be served from network edges, which will reduce the BW consumption in the network core.

Configuration Policies: The cache management algorithms proposed in [101], [11], [12] determine where to store which content, from where to serve user requests, as well as the path used to deliver the content. The decisions take into account the popularity of content and its geographical distribution, which are acquired by a central manager responsible for the management decisions. In this way, the ISP aims to minimize its network resource consumption, while simultaneously reducing the number of requests that have to be served from outside the ISP network.

The approach involves two tunable parameters that control the resulting cache configuration. These influence the number of requests that are redirected to the origin server (details for computing the number of redirections can be found in D7.1) and the utilization of core network links:

1. *Server link parameter* α: The server link represents the external link that leads to the origin server, and the associated parameter α defines the penalty of accessing content from the origin server. The value of α regulates the replication degree of content stored in the network.
2. *Cache hit ratio threshold* th_{chr}: Another factor that affects the access delay is the reconfiguration frequency, which determines how often the proactive algorithm computes new content placement. Given that request patterns can change over time, a given configuration may not

accurately reflect the current demand, which can result in more request redirections. To control the reconfiguration frequency we define a cache hit ratio threshold th_{chr} that will trigger a reconfiguration when crossed downwards. This is expressed as a percentage of the total number of requests.

Mapping Functions: The value of parameter α can range between 0.5 and 1. Low values of α lead to the placement of more popular content items at multiple locations (i.e. higher replication degree), which results in shorter delivery paths for most requests (*e.g.,* served from edge nodes) and, thus, lower bandwidth usage inside the ISP network. However, the average access delay can increase given that a smaller number of unique content items will be stored in the network (less popular items have to be fetched from the origin server). In contrast, high values of α force the algorithm to place a bigger number of contents inside the ISP network, but with a lower replication degree. This causes a traffic increase in the core network but reduces the overall number of redirections to the origin server and thus the access delay.

The cache hit ratio threshold th_{chr} can take a value between 50-100%. A high threshold, (*e.g.,* 90%) will result in more frequent reconfigurations, which will reduce the access delay given that the number of redirections to the origin server will be less. The tradeoff is the overhead associated with content migrations during reconfigurations; the more frequent the reconfigurations are, the more the BW consumed.

The weight assigned to the two BIs (*BWcons*, *AccDelay*) influences the configuration of both parameters (α, th_{chr}). These share a linear relationship as follows: *BWcons* is inversely proportional to both α and th_{chr}, while *AccDelay* is directly proportional to both α and th_{chr}.

4.1.3 Business-oriented Services Management

Differentiated Services (DiffServ) have been proposed as a scalable approach for providing QoS in IP networks. The core philosophy is grouping traffic with similar QoS requirements into a limited number of service classes, allocating bandwidth to these classes, and differentiating their forwarding treatment throughout the network. While different QoS levels can be provided, the absence of advanced control (based on, for example, pricing, service admission) can result into resource starvation and network congestion.

Business Indicators: In the context of a DiffServ scenario three BIs are considered that can potentially be used by a service provider: Losses due to service invocation rejections *(lossInvRjct)*, Losses due to performance degradation *(lossSvcDgd)* and Service satisfaction *(satisfSvc)*. These three BIs are formally defined as follows:

Losses due to service invocation rejections: This indicator correlates the losses of a network operator with the rejections of service invocations. When subscribed services are rejected the operator usually suffers economic penalties. Assigning the highest importance to this BI over others would imply that the operator prioritizes the acceptance of all subscribed services irrespective of the network conditions. This can eventually result in network congestion due to an excess of active services injecting traffic to the network. Congested links can degrade the performance of active services and thus adversely affect the *lossSvcDgd* and *satisSvc* BIs.

Losses due to performance degradation: Congestion is a result of the network resources not being able to accommodate the volume of injected traffic. Under such conditions performance degradation of active services can occur and subsequently losses for the network operator in the form of penalties since services may not receive their contractual rates. The *lossSvcDgd* indicator correlates these losses with the performance of active services at times of network congestion. Prioritizing this BI over others would result in scenarios where proactive actions prevent network

Table 15: SLS-I Policy Actions

ID	Policy action	Description
P1.1	setTCL(TT,TCL)	Set the target critical level threshold w.r.t. RAB per TT
P1.2	setSR(TT,SR)	Sets the service rate of a TT
P2.3	setACth(TT,AC)	Sets the admission control limit w.r.t. RAB per TT

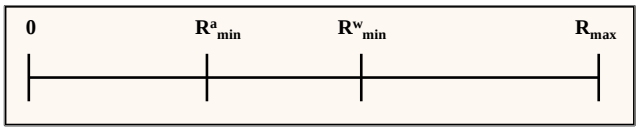

Figure 17: The Resource Availability Buffer (RAB)

congestion. This would negatively affect the *lossInvRjct* BI as few active services will be maintained due to high invocation rejection rates. In contrast, the BI service satisfaction would be favored as the network would never have congestion, and it would be more probable that the resulting few active services would be fully satisfied most of the time.

Service satisfaction: Contrary to the *lossSvcDgd* indicator that correlates losses with the performance of active services only during network congestion, the *satisSvc* indicator correlates the business impact of the level of service satisfaction during the whole life cycle of services, namely since services invocations are accepted until their life time has ended. Prioritizing this BI over the others would imply that services receive high rates for most of the time at the expense of sacrificing the number of accepted services and hence, affecting the *lossInvRjct* BI. In contrast, prioritizing this BI would have a positive effect on the *lossSvcDgd* BI since service rates would rarely be degraded and hence congestion would be highly unlikely.

Configuration policies: This section describes the low level enforceable policies that manage the DiffServ network. The final aim is that the policy values should implement the business policy of the operator.

In DiffServ scenario the service invocation logic is based on run-time events to regulate traffic entering the network. The policies used here are shown in Table 15. They perform dynamic admission control on the number of active services, as well as on the volume of admitted traffic.

The Service Level Specifications-Invocation (SLS-I) policy values are defined with respect to a *Resource Availability Buffer (RAB)*, which maintains the aggregate demand of subscribed services per *Traffic Trunk* (TT). TT is defined as aggregated traffic flows with the same origin-destination and the same performance requirements. As illustrated in Figure 17, the *RAB* has two main ranges: traffic injection up to $R^{a}_{\min}$ can be used with high confidence even at times of congestion, whereas the area between $R^{w}_{\min}$ and $R_{\max}$ is risky, because the network cannot provide QoS guarantees [70]. The calculation of the RAB values $R^{a}_{\min}$, $R^{w}_{\min}$, $R_{\max}$ considers Almost Satisfied ($Fctr_{\mathrm{AS}}$) and Fully Satisfied ($Fctr_{\mathrm{FS}}$)) factors and the average rates of the offered services.

The policies are three for each TT as shown in Table 15. These policies perform dynamic control on the number of active services, as well as on the volume of injected traffic. Policy P1.1 defines a threshold that signals *Target Critical Levels* (TCL) of traffic and TCL $\in[R^{a}_{\min}, R_{\max}]$. The closer the TCL is to $R^{a}_{\min}$, the earlier a notification is issued, whereas values close to $R_{\max}$ result in delayed proactive actions. The run-time operation of the dynamic control is triggered by TCL crossing

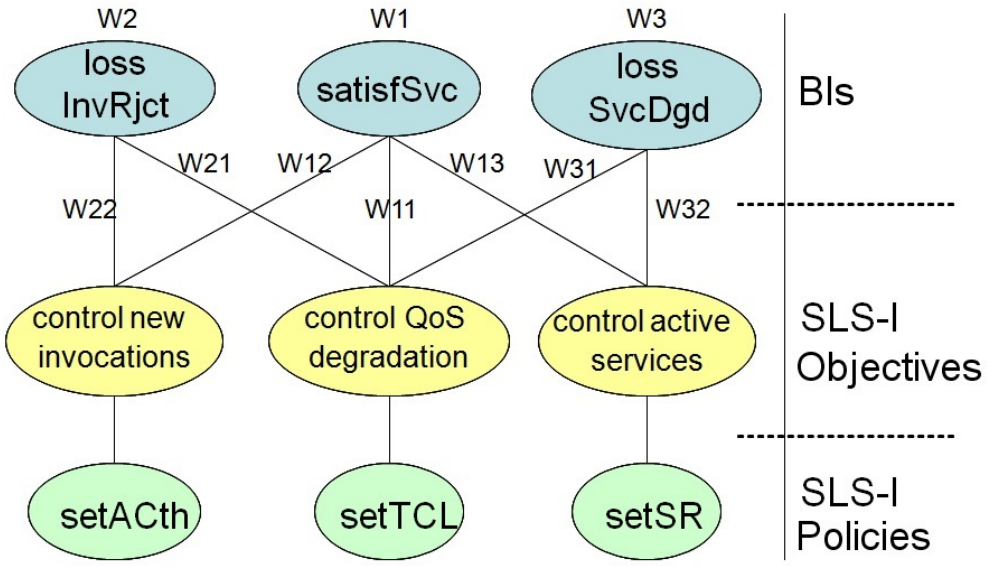

Figure 18: Relationships Between SLS-I BIs, Objectives, and Policies.

alarms, which activate policies P1.2 and P1.3 for adjusting the *Service Rate* (SR) and the dynamic *Admission Control (AC) threshold* (AC_{th}) of a TT. The AC_{th}) which is in the range [R^a_{min}, R_{max}] controls invocations of already subscribed services. The lower it is, the less the chances are of an incoming service being successfully invoked. A new service request will be accepted only if the current utilization of the relevant TT together with the average rate of that service does not exceed AC_{th}. Finally, the SR parameter, which is in the range [R^a_{min}, R_{max}] adjusts the service rates of active services. The lower the rate, the more the degradation experienced by active services.

Mapping functions: This section describes the impact of service management policies on the BIs and provides the mapping functions that are used to quantify the policy parameters [82]. BIs can be used by service providers to define their preferences in achieving specific goals. BIs relate to service management objectives (SMOs) and subsequently control the configuration parameters of derived policies. In the example of a DiffServ scenario, Figure 18 depicts the relationships of the BIs applying to dynamic service management with the associated objectives and the policies that influence them. Setting TCL achieves the *control QoS degradation* objective, which is influenced by all three BIs. A TCL close to R_{max} results into delayed QoS degradation prevention actions. This can allow active services to enjoy higher than average service rates for longer and sustain a high probability of accepting new invocations. As such, BI *satisfSvc* is maximized, and the BI *lossInvRjct* is minimized. These conditions, however, may eventually cause network congestion and performance degradation, it resulting into potential heavy penalties, negatively affecting the BI *lossSvcDgd*. A TCL close to R^a_{min} can have the opposite effect on BI *satisfSvc* and negative effect on BI *lossInvRjct* since proactive actions are enforced too early. *lossSvcDgd* is also negatively affected in this setting because services are likely to receive less than their contracted average rates. R^w_{min} is considered the optimal TCL value for minimizing *lossSvcDgd*. This can result into average levels of service satisfaction and positive effect on BI *lossInvRjct*. Equations 3 to 8 take into account the weights of the three BIs and derive the appropriate TCL value. Two functions are provided per BI reflecting the mapping zones between R^a_{min} - R^w_{min} and R^w_{min} - R_{max}. The final TCL value is derived by using the appropriate function based on the weight, and determining the mean of the three resulting TCL instances. Figure 19 a plots the TCL mapping functions.

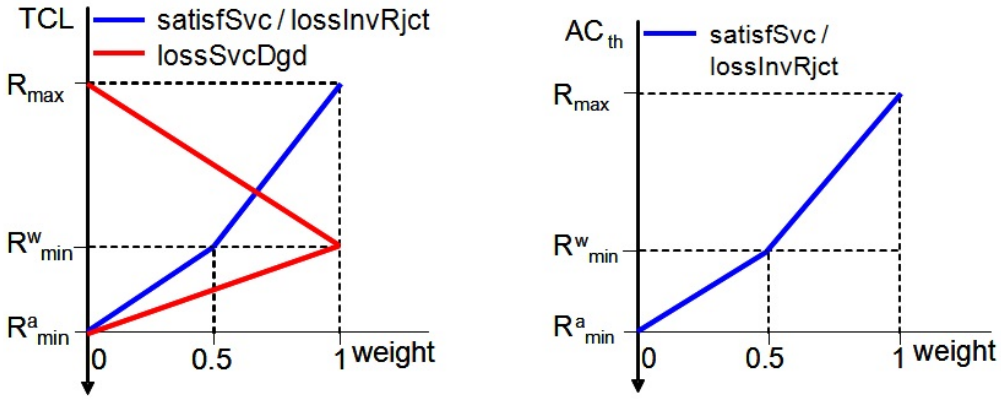

Figure 19: Impact of SLS-S BIs Weights on (a) TCL, and (b) AC Threshold.

$$TCL_1 = R^a_{\min} + 2W_{11}(R^w_{\min} - R^a_{\min}), \text{when } W_{11} \leq 0.5 \tag{3}$$

$$TCL_1 = (2R^w_{\min} - R_{\max}) + 2W_{11}(R_{\max} - R^w_{\min}), \text{when } W_{11} > 0.5 \tag{4}$$

$$TCL_2 = R^a_{\min} + 2W_{21}(R^w_{\min} - R^a_{\min}), \text{when } W_{21} \leq 0.5 \tag{5}$$

$$TCL_2 = (2R^w_{\min} - R_{\max}) + 2W_{21}(R_{\max} - R^w_{\min}), W_{21} > 0.5 \tag{6}$$

$$TCL_3 = R^a_{\min} + W_{31}(R^w_{\min} - R^a_{\min}), \text{when } W_{31} > 0.5 \tag{7}$$

$$TCL_3 = R_{\max} - W_{31}(R_{\max} - R^w_{\min}), \text{when } W_{31} \leq 0.5 \tag{8}$$

The policy relating to the *control new invocations* objective sets the AC threshold, which is influenced by the *satisfSvc* and *lossInvRjct* loss indicators. Values close to $R_{\max}$ imply low probability of invocation rejections resulting to minimal losses and increased satisfaction. Low threshold values result to higher losses and less satisfaction due to the increased probability of invocation rejections - $R^a_{\min}$ represents the extreme case. Figure 19b depicts the effect of the BIs weights on the threshold value, which can be determined by taking the mean of AC_{th1} and AC_{th2} from the functions below.

$$AC_{th1} = R^a_{\min} + 2W_{12}(R^w_{\min} - R^a_{\min}), \text{when } W_{12} \leq 0.5 \tag{9}$$

$$AC_{th1} = (2R^w_{\min} - R_{\max}) + 2W_{12}(R_{\max} - R^w_{\min}), W_{12} > 0.5 \tag{10}$$

$$AC_{th2} = R^a_{\min} + 2W_{22}(R^w_{\min} - R^a_{\min}), \text{when } W_{22} \leq 0.5 \tag{11}$$

$$AC_{th2} = (2R^w_{\min} - R_{\max}) + 2W_{22}(R_{\max} - R^w_{\min}), \text{for} W_{22} > 0.5 \tag{12}$$

Table 16: Measurable Parameters for the Supported Services and Protocols

Services	Protocol(s)	Measurable Parameters
Browsing	HTTP	Uplink and downlink throughput
Video streaming	Flash, RTSP	Jiter
Voice Over IP (VoIP)	SIP, RTP	Latency
General traffic	Random data	Packet loss
Network coverage	-	Signal strength

The last SLS-I policy involves service rate adjustments of active services, which have an impact on the user's perceived service quality and on the penalties applying as a result of performance degradation. Values close to SR_{FS} imply high levels of satisfaction and prevention of penalties. AS rates can lead to the reverse due to unfulfilled contracted rates. The impact of the two BIs are quantified by the functions bellow:

$$SR_1 = SR_{\mathrm{AS}} + W_{13}(SR_{\mathrm{FS}} - SR_{\mathrm{AS}}) \tag{13}$$

$$SR_2 = SR_{\mathrm{AS}} + W_{32}(SR_{\mathrm{FS}} - SR_{\mathrm{AS}}) \tag{14}$$

By specifying the importance of BIs with weights and using the described mapping functions, a network can be configured according to the business objectives. An ISP may, for example, opt to minimize at the most the penalties for high revenue-generating services, or to build up its reputation through good levels of service satisfaction.

4.1.4 Mobile Measurements

Business Indicators: Based on the current research interest of the partners, the collaboration scope has focused in the mobile measurements on mobile networks. The goal of the collaboration is to estimate the expected QoE of end-users at a given location, on a given Mobile Network Operator (MNO), for specific types of traffic. Thus, a client-server architecture to perform measurement tests has been developed. The client, which is an Android application, gathers the measurable technical parameters, which are network performance metrics, by connecting to and sending data to the server. Since it is possible for MNOs to have protocol based traffic shaping policies applied, just measuring throughput of a link using random data is not enough. As such, the client presents to users a list of services they would like to test. Each service supports multiple protocols. Thus, the protocol description files for the chosen protocols are then downloaded from the server and the technical parameters measurement is performed. The measurable parameters that define the MOS, as well as the services and protocols that are supported are listed in Table 16.

After performing the measurement of the technical parameters the results are stored in a database. However, the performance of each parameter cannot deliver much information neither about the performance of the MNO, nor about the QoE, because it depends what the end-user is aiming to do. *E.g.*, 500 ms latency is affecting critically VoIP services but not browsing. Thus, a Mean Opinion Score (MOS) is calculated for each type of service, using the measured technical parameters.

The MOS is a number that reflects the end-users' QoE. The Telecommunications Standardization Sector of the International Telecommunications Union (ITU-T) has defined in recommendations P.800 [46], P.800.1 [45] and P.805 [47], a five-point scale that illustrates the QoE of the end-user. The ITU-T MOS scale is summarized in Table 17 and it is used here for all MOS calculations.

Table 17: The MOS scheme recommended by the ITU-T [46]

MOS Value	Quality
5	Excellent
4	Good
3	Fair
2	Poor
1	Bad

Table 18: Technical Parameters Service-related Values

Service	Protocol(s)	Parameter	Desired value	$MOS = 3$	$MOS = 5$
Browsing	HTTP	downlink throughput	$1330\ Kbps$	-25%	$+100\%$
		latency	$523\ ms$	$+15\%$	-50%
Video	Flash, RTSP	downlink throughput	$1.5\ Mbps$	-20%	$5\ Mbps$
			480p		720p
VoIP	SIP, RTP	uplink throughput	$8\ Kbps$[3]	$5.3\ Kbps$[2]	$64\ Kbps$[3]
		downlink throughput	$8\ Kbps$[3]	$5.3\ Kbps$[2]	$64\ Kbps$[3]
		latency	$150\ ms$[4]	$+50\%$[3]	-50%

The $M2$ collaboration considers two BIs. (a) *lossSvcDgd* which is represented by the number of times were $MOS < 3$, divided by the total number of cases that the MOS of a service across all competitive MNOs were $MOS < 3$ and (b) *satisSvc* which is represented by the MOS value itself.

Configuration Policies: In [98] the desired and lower values for (a) uplink throughput, (b) downlink throughput and (c) latency for Browsing, Video streaming and VoIP are identified. The results are summarized in Table 18. For the calculation of the *satisfSvc* the Deterministic QoE (DQX) [100] model has been used. In case that the values of technical parameters are below the desired value the *lossSvcDgd* is increasing.

Mapping Functions: A precise QoE formalization that will be used to calculate the *satisfSvc* and the *lossSvcDgd* demands a mathematical model that is able to consider multiple and diverse variables, such as priority, price, and bandwidth that can affect the end-user QoE positively or negatively on a given situation. Furthermore, each variable might affect QoE in a different way in each scenario. Those characteristics are encapsulated in the DQX model [100]. Thus, Equation 15 is used to calculate the MOS of uplink and downlink throughput for every service, as well as for the signal strength. Equation 16 is used to calculate the MOS of jitter, latency and packet loss for every service as it is described in the DQX model.

$$e_i(x) = 4 \cdot \left(1 - e^{-\left(\frac{x}{x_0}\right)^m \cdot \ln 4}\right) \tag{15}$$

$$e_d(x) = 4 \cdot e^{-\left(\frac{x}{x_0}\right)^m \cdot \ln \frac{4}{3}} + 1 \tag{16}$$

Finally, Equation 17 generates the generic ITU-T MOS-compilant MOS $E(X)$ considering the set of technical parameters affecting a service.

$$satisfSvc = E(X) = 1 + 4 \cdot \prod_{k=1}^{N} \left[\frac{e_{(i \vee d)}(x_k) - 1}{4}\right]^{w_k} \tag{17}$$

For the *lossSvcDgd* calculation a set S of *satisfSvc* calculations will be considered for a given service v, or set of services Υ for every MNO. Calculations $satisfSvc \in S$ will take place in a time-frame T and a given area G. Thus Equation 18 is used to calculate *lossSvcDgd*.

$$lossSvcDgd = \int_T \int_G \left(\frac{|\{satisfSvc \in S | satisfSvc < 3\}|}{\sum_{i \in MNO} |\{satisfSvc \in S | satisfSvc < 3\}|} \right) \mathrm{d}g \, \mathrm{d}t \tag{18}$$

4.2 Economical Goals and Related Considerations

The business goals and considerations of Section 4.1 and the economical goals and considerations in this section impact each other. For example, the business strategies and business indicators of Section 4.1 are defined based on careful analysis of the goals and expectations of the actors involved. The chosen business strategy raises several economical questions such as: “How to ensure that the provider’s client receives the most appropriate type and level of service?”, “What is the impact when deviations from the agreed service specifications occur?”, “What is the impact of the chosen pricing scheme?” and “How does the business strategy impact the provider’s costs?”. As such it would be interesting to try to answer (some of) these question for each of the FLAMINGO scenarios.

Business goals and considerations of 4.1 and economical goals and considerations in this section here impact each other. For example, business strategies and business indicators of 4.1 are defined based on a careful analysis of goals and expectations of all actors involved. Especially the business strategy chosen raises several economical questions, such as (1) “How to ensure that the providerś client receives the most appropriate type and level of service?”, (2) “What is the impact when deviations from agreed upon service specifications occur?”, (3) “What is the impact of the chosen pricing scheme?”, and (4) “How does the business strategy impact providerś costs?”. Thus, it is more than interesting to answer these questions or parts thereof for each of the FLAMINGO scenarios.

An economic analysis of network management solutions introduces several challenges. Initially the interaction between different actors must be properly modeled to evaluate if goals of each actor are met or possibly violated by the network management solution. Second, service level specifications have to be defined to ensure that a client’s organization receives the most appropriate type and level of service for its needs. Two of the main components of a service level encompass the pricing schemes and the reaction on deviations from quality and performance-related targets. Third, the offering of a network management solution can have an effect on the cost structure of several actors.

The economic analysis of network management solutions can focus on each of these four aspects, the (1) multi-actor analysis, (2) service level agreements (*i.e.,* quality and performance-related targets), (3) pricing mechanisms, and (4) cost modeling. The economic analysis can reenforce business goals and considerations of this 4.2 here and legal and regulative constraints and considerations of 4.3 afterwards.

The multi-actor analysis evaluates a solution from the perspective of different actors. In this way, actors are explicitly included in the analysis. The multi-actor analysis makes goals of different actors explicit, which leads to a better knowledge of different parties involved. The involvement of important actors in the analysis increases the chance on an acceptance by all parties involved for the proposed network management solution. In general, the multi-actor analysis has two main phases. The first phase determines the exploration phase and gathers data for the analysis phase. The information can be gathered via (a) interviews and (b) a structured value network analysis.

The second phase is the analysis phase. The outcome of this phase results in a clear overview of benefits and drawbacks of the network solution proposed and this can be achieved for different groups of actors. Thus, during the first year of the FLAMINGO project for each of the scenarios a value network was drawn as documented in D7.1. Within the second year of the FLAMINGO project, it has started to perform interviews with industrial and regulatory experts to include their feedback into ongoing work and to validate scenarios proposed as documented in Section 6.

Service Level Agreements (SLA) ensure that a client receives the most appropriate type and level of service. To implement SLAs, first, critical success factors and key performance indicators in assessing the performance of service providers have to be identified. Second, tools must be set up to collect and assess performance data. Third, rewards and penalty incentive system have to be set up to to drive adherence to service level specifications. SLAs ensure that performance aims are directly related to the client organization's business objectives.

Pricing schemes define the function of mapping financial units onto resource usage, which determines provider charges for their customers in exchange for their product or services. The pricing scheme defines the exact calculation and parameters to use in the price calculation. In general, different pricing schemes are possible such as fixed- and dynamic pricing. Dynamic pricing schemes can be used to shift the demand for a service in time in order to reduce peak demand. The outcome of a pricing study ensures that the service provider can maximize its profit for a certain SLA.

Cost modeling defines the process of estimating the cost of specific products or services. The respective steps include defining the scope of the cost model and gathering input data. Next, the cost model itself must be defined by modeling capital investments and operational processes that are involved in processing products and services. Lastly, the total cost must be attributed to a single product or service. The outcome of a cost study provides interesting information for pricing decision and can identify where there is room for improvement.

Table 19: Overview of the scenarios and economic considerations

Scenarios	**Multi-actor analysis**	**SLAs**	**Pricing**	**Cost modelling**
Resource management in virtualized networks	D7.1	l_{qos}	l_{vnb}	
ISP-oriented content delivery	D7.1			th_{chr},α
Business-oriented Service Management	D7.1			
Mobile measurements	D7.1		$lossSvcDgd$	$lossSvcDgd$, $satisSvc$

The reminder of this section will elaborate on these four main aspects for those scenarios of FLAMINGO considered representative for WP7: Management of Differentiated Services, Resource Management in Virtualized Networks, Quality Improvement, ISP-oriented Content Delivery and Mobile Measurements. Not all of these four aspects are of equal importance for each of the scenarios while other aspects were already (partly) covered in D7.1 as indicated in Table 19.

4.2.1 Resource Management in Virtualized Networks

In the context of resource management in virtualized networks, focus is on two economic topics: a dynamic pricing mechanism and the impact of penalties when a service level agreement is violated.

Two types of business indicators are defined for this scenario: Losses due to virtual network blocking (l_{vnb}) and losses due to degradation in VN QoS, l_{qos}. In following section each of these business indicators are related to the economic topics.

Dynamic pricing

Dynamic pricing is a pricing strategy in which the service provider adapts the price based on the current market demand. A prototype example of a dynamic pricing scheme are the pricing schemes of airline carriers. They often change prices throughout the day of the week or even the time of day. The goal of dynamic pricing is to optimize the total profit of the service provider.

In this scenario the goal is to optimize the profit of the virtual network provider, to this end we use a dynamic pricing approach that is demand driven. When demand is high (low) for a resource the price charged will also be high (low). The goal of this approach is to maximize resource utilization by balancing the demand throughout time by decreasing the highest peaks and increasing the lowest dips.

To this end, this proposal continuously forecasts expected demand for substrate network resources, and based on this makes decisions on the pricing of a resource. The dynamic pricing decision immediately impacts the first business indicator, l_{vnb}, because a higher (lower) level of pricing will decrease (increase) the attractiveness of the resources for the consumer (as it is assumed that the price elasticity of demand is elastic).

Given the dynamic pricing approach and based on demand forecasting opportunity costs have to be taken into account as well. An opportunity cost is the cost of making an economic choice expressed in terms of missed revenue. For example, it can be economically optimal to reserve resources for future use at a higher price than accepting demand now at a lower price level. Taking into account opportunity costs also impacts the first business indicator, l_{vnb}, because when an opportunity cost is identified the level of virtual network blocking may temporarily increase to allow to sell the resources in the future at a higher rate.

SLA violation

Another consideration is that user traffic is non-uniform, different virtual networks would demand for their maximum resource requirements at different times. This way, it is possible to over-sell the substrate network resources with the objective that the mapped virtual networks load the substrate network in an efficient way, and hence improve the profitability of infrastructure providers.

To this end, this proposal continuously forecasts expected demand for substrate network resources, and based on this makes decisions the respective percentages by which each substrate node and link can be over provisioned. The task is to strike a balance between the conflicting objectives of over-selling the substrate resources as much as possible, yet ensuring that at any time, each of the virtual network is able to use its maximum reserved resources when needed.

As with any forecast, their is some uncertainty about the reliability of the predictions. Therefore, it is possible that the promised service level specifications cannot be guaranteed. In that case a penalty has to be paid. A prototype example is the overbooking of airline carriers based on a forecast of the number of no-shows. When the forecast is not in line with the real amount of no-shows, the carrier may need to pay some passengers a fee to convince them to take another flight. For this scenario, wrong predictions will result in a degradation of the QoS which is measured by the second business indicator, l_{qos}.

4.2.2 ISP-oriented Content Delivery

In terms of economic impact, the ISP-oriented cache management scenario focuses in the first place on cost modeling and cost optimization. In general, ISPs are interested in opening new revenue opportunities by offering their own caching infrastructure. Still, keeping the cost low is also in their advantage to remain competitive and maximize profit. Therefore, this problem is studied from a cost optimization perspective for the caching infrastructure inside the ISP's network.

Two types of business indicators are defined in this scenario: (i) Quality of Experience, which is expressed in terms of content access delay (*AccDelay*), and (ii) BW consumption (*BWcons*) within the ISP network. Both business indicators have an impact on the cost modeling topic.

Cost modeling
The analysis of the optimal placement of cache locations and the optimal size of cache locations requires a rough estimate of the investment cost in network infrastructure. Therefore, the cost of the following most relevant cost categories in a network is modeled: (1) the investment cost in network nodes (i.e. a multilayer node), (2) the cost of connectivity (i.e. leasing links) and (3) the cost of peering (i.e. inter-domain connectivity). For this particular scenario we also need to take into account (4) the cost of caching infrastructure (i.e. data centers).

In this scenario the goal is to optimize the profit of the internet service provider by minimizing the cost without taking into account the possibility for extra revenue generation. Several parameters have a direct impact on the cost optimization. These parameters are captured in the business indicators.

The first business indicator of content access delay, involves two tunable parameters that control the resulting cache configuration.

The server link parameter α represents the external link that leads to the origin server. Parameter α defines the penalty of accessing content from the origin server. The value of the parameter α immediately impacts the amount of peering traffic because when more content is accessed from the origin server (which is likely to be outside the ISP's own domain) the higher peering costs will be. At the same time, node- and link utilization will be higher as content will have to cross more nodes and links between origin server and the user. On the other hand, storing more content inside the network will involve a higher cost for caching infrastructure.

The cache hit ratio th_{chr} affects the access delay in the reconfiguration frequency. A low threshold will result in infrequent reconfigurations. This will lead to higher access delays and a more redirections to the origin server. On the other hand, a high threshold will lead to a lower number of redirections but a higher bandwidth consumption (overhead due to content migration). Just like the server link parameter α, parameter th_{chr} has a direct impact on the cost modeling and cost optimization. For example, more redirections will increase the bandwidth consumption as more requests are redirected to the origin server. Peering traffic may also rise considerably. Too frequent reconfiguration may undo the effect because the overhead is larger than the possible savings in terms of bandwidth consumption. The amount of peering traffic may still be reduced.

The second business indicator, bandwidth consumption, (partly) determines the timing of an upgrade of the network. When the bandwidth consumption of a certain link ((*e.g.,* 1GbE link) is higher than the bandwidth threshold a parallel link ((*e.g.,* another 1GbE link) has to be added or the existing links need to be replaced and updated ((*e.g.,* from 1GbE to 10GbE link). Other factors that will determine the timing of an upgrade are traffic forecasts, the used protection schemes and non-technical decisions such as the investment horizon of the ISP.

For this scenario both business indicators immediately impact the economic analysis and therefore our research collaboration will focus on the optimization of each of them.

4.2.3 Business-oriented Service Management

The business-oriented policy refinement process outlined in Section 4.1.1 has taken an important step towards bridging the gap between business value and configuration in the DiffServ management domain. However, due to its analytical basis that considers the definition of policies for TTs in isolation, the approach lacks of operational means to guarantee the optimization of the business

indicators under dynamic network conditions, traffic management operations, the run-time execution of policies, and service invocation dynamics, all in all, for multiple TTs in a functional network. These are some of the key elements that should be taken into account when deriving policies that would have economic impact in practice.

In this scenario concentration lies on a framework to optimize the business indicators of the DiffServ management scenario as an illustrative example of how optimization techniques could be applied to optimize the business indicators, which eventually would have a positive economic impact. This section describes a BI optimization solution for the business-oriented DiffServ management scenario, which includes the policy optimization framework, a concrete methodology to evaluate BIs quantitatively, the features of the selected optimization technique and examples of the result of the optimization process.

Optimization framework

The proposed solution is based on an offline policy optimization framework whose main objective is to generate a catalogue of service management policies that optimize the business value of the network infrastructure. The various components of this framework are depicted in Figure 20.

The core component of the framework is the *policy optimization* module, which searches the most optimal policies within the policy values' search space to locate solutions that optimize the business objectives. Policy optimization is an iterative process, supported by *evolutionary algorithms* that are in charge of finding the most optimal values of the service management policies. During their execution, the algorithms produce candidate policies whose optimality in comparison with the business objectives is evaluated iteratively until no better solution can be determined. The evolutionary algorithms are in turn supported by a process that provides numerical values of the objectives to-be-optimized. Quantifying the BIs is pivotal for the algorithms search activity and it is the responsibility of the *BI evaluation* module. The latter follows novel and well-defined methods that consider network and service performance information. By correlating such information with business-aware data they assign numerical values to the business indicators accordingly. BI evaluation is supported by the *Performance measurements processing* module, whose main responsibility is to handle and manage raw monitoring data from the network simulator such as injected traffic, service invocations, service rejections, or quality of service enjoyed by active users.

The *policy optimization* component is configured with the parameters shown in the left part of Figure 20, namely the *BI Preferences*, the *Resource Availability Buffers* and the *SLA Repository*. *BI preferences* define desirable BI levels, which are taken into account when generating the policy configurations. In other words, the enforcement of the policies derived by the optimization process would result in the most ideal configurations to reach the desired preference levels of the BIs. Another configuration set concerns the *Resource Availability Buffers (RABs).* The *policy optimization component* considers the *RAB* to define the search space of the policy values. Finally, the *SLA Repository* is another configuration set for the policy optimization component. The number of service types and their technical specifications formalized therein represent the basis to quantify the BIs during the optimization process. For example, based on the contractual service rates the *policy optimization* can define whether a service is degraded, at which extent and for how long. This way the effect of degradations (and other SLA-aware aspects) can be correlated with appropriate BI numerical values.

During the search process the *policy optimization* produces candidate policy values which are fed to the *policy-based simulator*. The latter is a modified OPNET toolkit with enhanced functionality to support the execution of the service management policies on the fly, with capabilities to produce network and service monitoring information during its simulation runs and also with capabilities to be configured on the fly. When performing simulations the two configuration data shown in the lower-left part of Figure 20 are considered. The *network topology & features* consist of the access

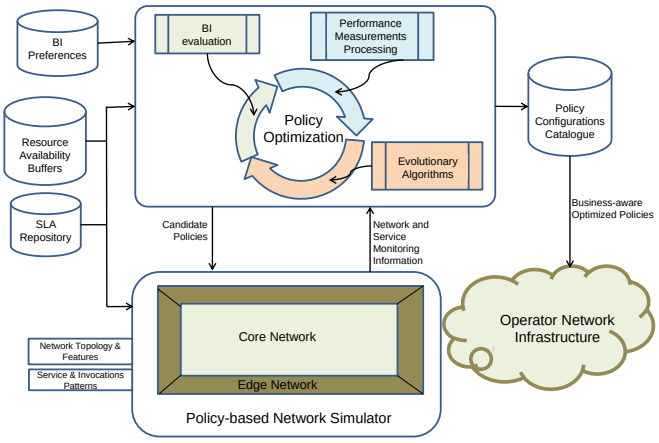

Figure 20: Policy Generation Framework

and core routers, links with specific capacities, the TTs of the network and the DiffServ mapping configurations of the network infrastructure. The simulation of dynamic network conditions and run-time policies execution is performed by considering service invocation dynamics. These are provided as inputs to the simulator in the form of *service & invocation patterns*, which consist of the services characteristics, and the service invocation periods including durations (service life cycle of observation times ranging from minutes to hours). This information represents the traffic patterns injected to the network ingress points. With all these inputs, the *policy-based simulator* provides to the policy optimization component raw network and service monitoring information that represent the result of the deployment of the candidate policies generated by the optimization component.

The *policy optimization* component produces optimal policy value sets that are stored in the *Policy Configurations Catalogue*. Table 20 illustrates the structure of the catalogue. For a given set of *BI preferences*, the *policy optimization* produces a Pareto front [76]. Each point in a Pareto front is defined by numerical values of the BIs. These points render the closest optimal BI values in comparison to the desired levels defined by the *BI preferences*. For each Pareto point, the optimization process produces the service management policies for all TTs in the network, which represent the configurations most aligned to the *BI Preferences*. The operator can thus select from the catalogue the most appropriate policy configurations for the traffic trunks to manage its network infrastructure.

The service management policies considered are three for each traffic trunk as described earlier and shown in Table 15.

A key challenge in the proposed framework is the process of evaluating BIs as this has a number of dependencies including the nature of individual BIs, the network and service measurements, the technology used to deploy the services, the injected traffic, the amount and dynamics of service invocations, and the enforcement of service management policies. The next three sections elaborate on the description, relevance and most importantly, the methodology to evaluate the three BIs considered in this work: Losses due to service invocation rejections (*lossInvRjct*), losses due to performance degradation (*lossSvcDgd*), and service satisfaction (*satisSvc*).

Evaluation of BI losses due to service invocation rejections

This indicator correlates the losses of a network operator with the rejections of service invocations. When subscribed services are rejected the operator usually suffers economic penalties. Assigning the highest importance to this BI over others would imply that the operator prioritizes the acceptance of all subscribed services irrespective of the network conditions. This can eventually result in

Table 20: Structure of the Policy Configurations Catalogue

BI Preferences Set *a*	Pareto Front for BI Preferences Set *a*	Pareto Point *a*1:BI Values	Service management policies for TT_{a11}
			...
			Service management policies for TT_{a1c}
		...	...
		Pareto Point ab:BI Values	Service management policies for TT_{ab1}
			...
			Service management policies for TT_{abc}

network congestion due to an excess of active services injecting traffic to the network. Congested links can degrade the performance of active services and thus adversely affect the *lossSvcDgd* and *satisSvc* BIs.

The *lossInvRjct* BI tracks the ratio of rejected to accepted services and is influenced by the TCL and AC thresholds. It should be noted that the policies setting these thresholds are executed at the ingress points of each TT, so that the BI is measured taking into account all TTs in the network and all service invocations in each TT for a period of time, i.e. observation times ranging from minutes to hours.

In order to evaluate this BI we propose the following methodology, which applies to each TT i in the network:

1. The default behavior of the adopted service management approach considers that when the injected traffic reaches the TCL policy threshold, corrective actions are executed to prevent network congestion. A default corrective action is the execution of the AC policy, which results in the rejection of new service invocations.
2. When the TCL is crossed upwards and the AC policy is enforced a count of the number of service rejections is maintained.
3. Service rejections eventually result in the reduction of injected traffic. When the traffic volume falls below the TCL, new invocations are accepted and the count for rejected services is stopped.
4. The methodology prescribes to return to step 2 and continue the monitoring of the BI until the BI evaluation takes place when the observation time has completed.
5. The following expression quantifies this BI at the evaluation phase:

$$lossInvRjct = \sum_{i=1}^{n} \frac{rjctSvc_{TTi}}{rjctSvc_{TTi} + accSvc_{TTi}} \tag{19}$$

where n is the number of TTs, and $rjctSvc_{TTi}$ and $accSvc_{TTi}$ are the total number of rejected and accepted services in the respective traffic trunk. The value of the *lossInvRjct* indicator

lies between zero and n. A value equal to zero represents that all service invocations are accepted, while a value equal to n would represent that all service invocations are rejected.

Evaluation of BI losses due to performance degradation

Congestion is a result of the network resources not being able to accommodate the volume of injected traffic. Under such conditions performance degradation of active services can occur and subsequently losses for the network operator in the form of penalties since services may not receive their contractual rates. The *lossSvcDgd* indicator correlates these losses with the performance of active services at times of network congestion. Prioritizing this BI over others would result in scenarios where proactive actions prevent network congestion. This would negatively affect the *lossInvRjct* BI as few active services will be maintained due to high invocation rejection rates. In contrast, the BI service satisfaction would be favored as the network would never have congestion, and it would be more probable that the resulting few active services would be fully satisfied most of the time.

This BI is influenced by the TCL and SR policy settings. The evaluation of this BI as a result of enforcing these policies considers a given observation time ranging from minutes to hours. To evaluate this BI the following methodology is proposed, which applies to each TT i in the network:

1. When the volume of traffic is below the TCL the network is not congested and the BI is thus not quantified. When the TCL is exceeded a default corrective action is adopted to adjust the rate of active services by means of the SR policy. However, this can result in active services receiving lower rates than the contracted ones and consequently in service degradation.

2. When congestion occurs the total number of active services and the volume of injected traffic are quantified at periodic rates (*e.g.,* based on a monitoring interval $>$ 10 seconds).

3. The number of active services and injected traffic are used to measure the ratio between the average rate of the services currently served and the average service rates for the SLAs allocated in the RAB, which is calculated as follows:

$$lossSvcDgd_{TTi} = \frac{(TR_{in})(numSLAs)}{(actSvc)(SR_{SLAs})} \tag{20}$$

   where *lossSvcDgd*$_{TTi}$ quantifies the BI in TT i, TR$_{in}$ is the total volume of traffic injected to the TT and *actSvc* is the number of active SLAs in the TT, both measured at the time of the evaluation. Finally, *numSLAs* and *SR*$_{SLAs}$ are the number of SLAs and the sum of the contractual service rates allocated in the RAB of the TT i respectively.

4. The BI is quantified only when the injected traffic is above the TCL. When the volume of injected traffic falls below TCL, the SR is changed to its original value and the BI quantification BI is stopped.

5. The system keeps a record of all BI quantifications. Using all BI evaluation records produced during the simulation (step 4), the average value of *lossSvcDgd*$_{TTi}$ is computed, which is denoted as *lossSvcDgd*$_{avgTTi}$. The value of this BI over all TTs in the network is given by:

$$lossSvcDgd = n - \sum_{i=1}^{n} lossSvcDgd_{avgTTi} \tag{21}$$

where n is the number of TTs. The value of the *lossSvcDgd* lies between zero and n. A value equal to zero represents that all services have enjoyed at least the average contracted service rates allocated in the RABs of the network during congestion, while a value equal to n would represent that none of the services have enjoyed at least the average contracted service rates allocated in the RABs during congestion as well.

Evaluation of BI service satisfaction

Contrary to the *lossSvcDgd* indicator that correlates losses with the performance of active services only during network congestion, the *satisSvc* indicator correlates the business impact of the level of service satisfaction during the whole life cycle of services, namely since services invocations are accepted until their life time has ended. Prioritizing this BI over the others would imply that services receive high rates for most of the time at the expense of sacrificing the number of accepted services and hence, affecting the *lossInvRjct* BI. In contrast, prioritizing this BI would have a positive effect on the *lossSvcDgd* BI since service rates would rarely be degraded and hence congestion would be highly unlikely.

In order to measure this BI the following methodology is proposed, which applies to each TT in the network:

1. The BI is quantified during the whole service life cycle and it is quantified considering two network states: 1) When network resources are not highly utilized, and 2) when network resources are heavily utilized.
2. In order to define the state of the network the methodology considers the percentage of utilization of the shared links supporting a given TT. The link utilization is periodically monitored at intervals $>$ 10 seconds, which is the granularity of BI evaluations on each TT. The link monitoring functionality on which this methodology relies is supported by the policy-based network simulator.
3. Contracted service rates are formalized in SLAs. In the case where services inject traffic at rates lower than the contracted ones, they are considered fully satisfied. When the utilization of all shared links along a given TT is below 85% we consider that the network is not highly utilized, that services are injecting the desired traffic and that they are fully satisfied. In these conditions the BI is assigned with the maximum value when it is evaluated.
4. Services may be prevented from sending traffic at their desired rates due to over utilized network links that are shared between multiple TTs. When the network resources are heavily utilized the BI is evaluated considering the ratio between the average rate of the services currently served and the average service rates for the SLAs allocated in the RAB. This ratio is periodically computed and the results are used for deriving the average value of the BI over a simulation execution.
5. Taking into account all the above considerations, this BI is evaluated by a combination of the maximum values corresponding to periods of full satisfaction and also when the network is heavily utilized as follows:

$$satisSvc = \begin{cases} 1, & \text{if any shared link's capacity in TT} < 85\% \\ \frac{(TR_{in})(numSLAs)}{(actSvc)(SR_{SLAs})}, & \text{if any shared link's capacity in TT} >= 85\% \end{cases} \quad (22)$$

where TR_{in} is the total volume of traffic injected to a TT and *actSvc* is the number of active SLAs in the TT, both measured at the time of the evaluation. On the other hand, *numSLAs* and SR_{SLAs} are the number of SLAs and the sum of the contractual service rates allocated in the RAB respectively.

6 Taking into account the latter considerations, step 5 certainly implies that BI *satisSvc* is evaluated periodically until the observation time ends. Considering the number and value of each BI evaluation recorded during the simulation, the average of the *satisSvc* is calculated and it is denoted as $satisSvc_{\mathrm{avg}}$.

(7 Finally, the value of this BI over all TTs in the network can be computed by the following expression:

$$satisSvc = n - \sum_{i=1}^{n} satisSvc_{avgTTi} \tag{23}$$

where n is the number of TTs in the network. The value of the *satisSvc* indicator lies between zero and n. A value equal to zero represents that all services have enjoyed at least the average contracted rates allocated in the RABs during the whole service provision. A value of *satisSv* equal to n would represent that none of the services have enjoyed at least the average contracted service rates allocated in the RABs during their provisioning cycle.

Features of the optimization technique

In order to derive optimized policy configurations, the framework uses optimization techniques. Optimization is the procedure of finding and comparing feasible solutions until no better solution can be found [21]. More specifically, this framework uses multi-objective optimization (MOO) techniques since multiple objectives need to be optimized simultaneously. In this work the term *objective* refers to a BI and the term *solution* refers to policy values that optimize one or more BIs according to administrative preferences. Determining the most optimal solutions relies on search techniques from which Evolutionary Algorithms (EAs) have been found to be efficient in locating solutions close to the global optimum even in highly rugged search spaces [16].

Evolutionary Algorithms (EAs) are population-based techniques that perform multidimensional search and can find more than one solution within an execution. In this work the term *population* refers to policy configuration values that are considered in the search space. However, despite their success, EAs have limitations when solving computationally expensive optimization problems. Due to the dynamics of network events and service provisioning as well as the range of values configuration policies can take, the optimization of multiple BIs falls under this category of problems. This issue can be addressed by surrogate[1] models such as the ones proposed in [104], [28], [55] and [8]. Most of these solutions have been developed to solve specific problems, the most successful of which is ParEGO [28] as it has managed to solve problems that cannot be solved with the other models. Nevertheless, existing techniques are only effective when the number of functions evaluations have at most 10 variables [28], which are not adequate for the problem addressed in this work, *e.g.,* more than 10 policy variables may need to be evaluated in an operational network in practice.

The simulation process on which the optimization procedure relies can be very time-consuming. BIs are evaluated considering the results of observations made through network simulations, which can take dozens of minutes per simulation run depending on observation time, network topology, service features and the computational resources available to execute the simulations. An appropriate surrogate-based optimization approach that could easily deal with the above complexity and that can provide efficient results for more than ten variables, has been adopted. The Tune-adaptive Metamodel Assisted Algorithm TAMAAL [9] has been applied to solve the policy optimization problem addressed in this research. TAMAAL intersperses evaluations in its metamodel and

[1] Also known as metamodels, emulators, reduced models, approximate models, and response surface models

Table 21: Values for Policies of the Knee Point

Policy value	Policy Values for TT1 to TT6 (bps)					
TCL	1,383,730	1,546,095	1,187,704	663,278	1,500,438	805,318
SR	1,270,876	729,770	1,024,479	534,309	705,286	1,163,111
AC_{th}	1,029,852	1,110,586	1,203,230	723,575	1,432,216	489,520

the evaluation of BIs, and it uses the results of the BIs evaluation to feed back the metamodel, thus improving its accuracy. Previous research [68] compared four meta-modeling techniques: Radial Basis Functions, Support Vector Regression, Kriging-DACE, and Polynomial Regression, according to their accuracy, robustness, efficiency, and scalability with the aim to identify advantages and drawbacks of each meta-modeling technique. This work did not identify a clear winner among the meta-modeling techniques considered, but each meta-model outperformed the others in specific test functions. Eight scalable unconstrained global multi-objective test function problems were used from the specialized literature that consider both, the number of local minima and the shape of the Pareto front, containing characteristics that are representative of what can be considered ”difficult” in multi-objective optimization research problems. Therefore, TAMAAL was designed to find the best surrogate approach to be used at a given time for a given problem. This goal is achieved through online adaptation. TAMAAL starts with several meta-modeling techniques and selects the best one according to a metric responsible to measure the performance of each technique.

Example of BIs optimization

The above framework and the optimization technique have been put in place. This section describes an example of the results achieved with the optimization solution in the context of DiffServ management. The typical setup for the optimization of BIs consists of a Network Topology and Features, SLA Repository, Resource Availability Buffers and Service & Invocation Patterns as described in Section 3.4.1. The results targeting the optimization of *all* BIs being treated equally result to a *Pareto front* with the points defined by the closest BI values to the origin coordinates [0, 0, 0]. An example of the Pareto front obtained is shown in Figure 21, which includes the most optimal solutions found by the optimization framework after 31 execution runs, for which in each execution run the framework’s TAMAAL algorithm has performed 1,000 evaluations over the real function (OPNET-based simulation), rendering a total of 31,000 simulations.

In the example whose results are plotted in Figure 21 the optimization process produced a total of 460 service management policy sets grouped in the 41 Pareto front points shown therein. This means that points with identical numerical BI values may result to different policy sets. The most important point in the Pareto front is that of the knee point, i.e. the point with the lower Euclidean distance to the origin (*BI Preferences* [0,0,0] in BIs *satisSvc, lossSvcDgd, lossInvRjct*). The knee point in the Pareto front of our example has a Euclidean distance to the origin equal to 0.39836587 and it outperformed the rest 460 points. This point has only one set of service management policies. From this we conclude that very popular points in the Pareto front do not necessary coincide with the best alternative to maximize the network business value. The operator would deploy the policy set of the knee point in the real network to optimize equally all the BIs. The associated policy values of the knee point are shown in Table 21.

4.2.4 Mobile Measurements

Mobile Measurements (M2) collaboration aims to create a tool that estimates the performance of Mobile Network Operators (MNOs) considering the following three dimensions: (a) Location, (b) timeframe, and (c) Type-of-Service (ToS). The roadmap to this estimation involves measurements

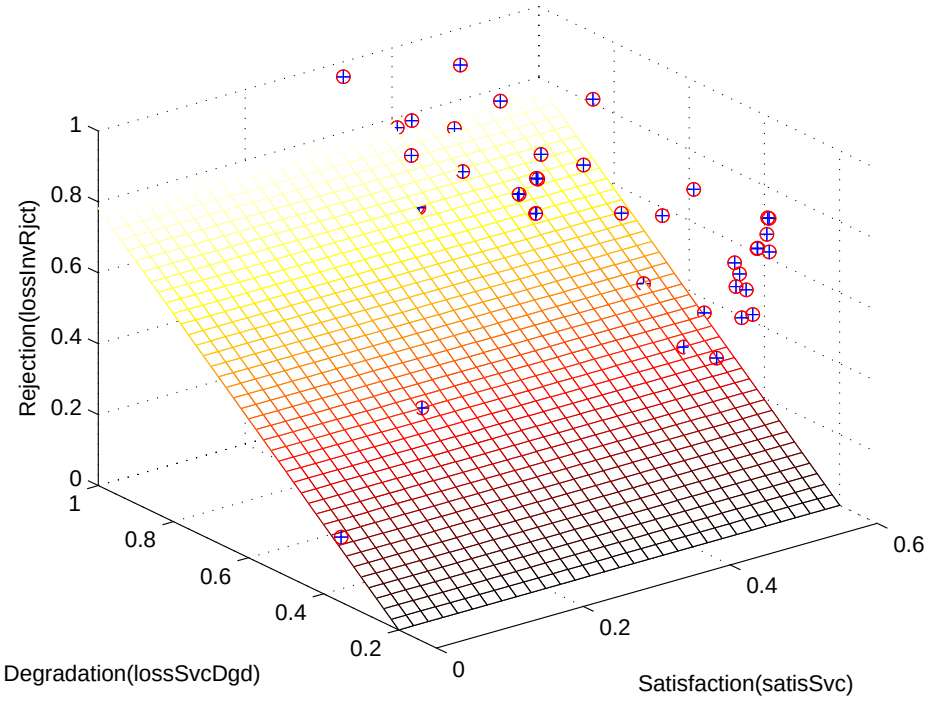

Figure 21: Pareto Front Points Optimizing *all* BIs: *satisSvc, lossSvcDgd, lossInvRjct*

on mobile devices that will emulate data traffic according to specific services and protocols. Technical parameters such as bandwidth, latency, and jitter will be measured and based on the service requirements an MNO Quality-of-Experience map will be created. Such tool will enable end-users to have an overview of their MNO's performance in locations of their interest, such as their home, or work address. Having such information available can be used as an input in QoE-based charging models [80]. However, nowadays in the mobile communication area customers are paying a fix rate and the MNO is expected to provide best-effort IP-based services without considering end-users location.

What is QoE estimation? The performance of technical variables does not hold significant information since each service has specific performance demands. Estimating QoE demands service-specific calculations. *E.g.*, $500\ ms$ of delay will not affect browsing QoE, but it will make VoIP services unusable in practice. Thus, when estimating QoE all the service related constraints should be also taken in to account.

What are the contributions of our work? This collaboration provides a tool that can be provide economic-related input into both stakeholders in mobile communications: (a) End-users to select the MNO that performs better in services and locations that they are interested. (b) MNOs can get a feedback about their networks performance and arrange potential future infrastructure updates.

Economical Goals/Considerations Two types of BIs are defined for this scenario: Losses due to performance degradation ($lossSvcDgd$) and Service satisfaction ($satisSvc$). $satisSvc$ is relevant for the MNOs that could monitor the QoE of their networks at a given location, compare it with other

MNOs and decide whether take an action and invest further on network infrastructure. Thus, a continuous monitoring of $satisSvc$ is essential to maintain, on improve, MNOs reputation. In such approach, decreasing values of $satisSvc$ could follow increasing values of infrastructure investments. $lossSvcDgd$ is relevant to both end-users and MNOs since increasing values of this BI result a constant underperformance of a MNO compared to its competitors. Thus, a QoE-based charging scheme could be adopted from a MNO, either to minimize losses in case of underperformance, or maximize revenue in case of high credibility. Last but not least QoE-related measurement data might be of interest of MNOs. There is a demand for such data and companies like OpenSignal [72] are already collecting data that sell to MNOs who are interested to monitor the performance of their networks. Currently, the Mobile Measurements collaboration as OpenSignal acknowledged after reviewing [98] and [100] meet advanced modeling and measurement techniques (a) to estimate QoE for a given service and set of services and (b) to detect traffic shaping. Thus, a collaboration with OpenSignal has been initiated for the next phase of the collaboration.

4.3 Legal and Regulative Constraints and Related Considerations

In the field of network and service management sharing, transferring, storage of data forms a crucial part for network operation, administration, maintenance, and configuration of resources. This however, entails various legal and regulative constraints and requirements, that should be considered while performing any of these tasks. The following section discusses two major aspects of such constraints.

4.3.1 Schengen Routing

After the magnitude of NSA electronic surveillance was made public, industry organizations and politicians got worried about security and privacy of their data and other business and privacy related data in Europe (*e.g.,* private mail exchanges or worthy protecting company data). Since the path through which data traveling through the Internet is not known, even when source and destination are geographically nearby, the possibility of getting captured by industrial competitors or security agencies for the purpose of industrial espionage or military intelligence service is always present. For the reason that data traveling outside law frontiers is not covered by the source countries law, there is nothing to use as a lever against the opponent, no matter if this is an industrial competitor or a military intelligence service opponent.
Due to these threats, politicians and industrial organizations started various initiatives to protect the data. The first operation was started by Deutsche Telekom marked with public statement from Philipp Blank, spokesperson and corporate blogger of Deutsche Telekom: ”Internet data made in Germany should stay in Germany” [84]. The following sections aim to give an overview of Schengen Agreement, reasons for implementing *Schengen Routing*, and details about possible implementation strategies.

Schengen Agreement: The first Schengen Agreement was signed in 1985 between five member states of the European Economic Community (EEC) with an initial idea to harmonize visa policies within the EEC and allow cross boarder traffic of residents without stopping at fixed checkpoints. The name was derived from the town nearby the agreement was signed. Later in 1990 the Schengen Convention was initiated as a supplementary to the Agreement, which proposed the complete abolishment of internal border controls. With this Convention the area of countries participating in Schengen Agreement operates like a single state for international visitors, with external boarder controls while entering or leaving the Schengen Area and common visa policies, but without border controls within the area. The current Schengen Area consists of 26 European countries of which

22 are European Union states [31]. Before 1999 the Schengen contracts operated independent from the European Union. In 1999 the Amsterdam Treaty incorporated the Schengen Agreement into European Union law with two exceptions: United Kingdom and Ireland (special opt-out). Since this time Schengen is a part of European Union law where all European Union member states are obliged to implement the Schengen Agreement.

Reasons for Schengen Routing: The reasons arguing for *Schengen Routing* are manifold, but all are based on security and privacy issues of data. Data can be divided into industrial relevant and personal relevant data. The former represents a target for industrial espionage by a competitor, whereas the latter focuses more on surveillance by security agencies which try to get personal data from possible criminals. These two aspects are covered in general by national law, so that everyone who feels affected can call the justice for further investigations, if sensible data seems to be in the wrong hands.
Since the data traveling through the Internet has the opportunity to leave the area protected by the national law of the data owner, the legal situation is unclear. The removal of this lack of clarity is a main goal of *Schengen Routing*. The legal situation is much clearer and the justice can easily protect the national law, if transferred data, when source and destination of data are in the same country, is not leaving the national area. For the reason that most of the data traveling trough the Internet is routed through neighbor countries, because of the nature of the Internet to connect people and data, a bigger area than a national wide one would be more reasonable. Furthermore a Schengen wide routing policy, which has to be implemented e.g., rearranging routing policies is an opportunity to include data protection and reduce network neutrality aspects at the same time). Also the technical aspects of such routing restrictions have to be taken into account. Expanding the area from national wide to the European Union area enhances the trade-off between network neutrality and data protection, thereby the idea of *Schengen Routing* was born. If routing policies manipulate the traffic flow to remain inside the European Union, they can also manipulate other types of traffic or their QoS behavior.

Idea of Schengen Routing and its applicability: The main idea is to apply a European wide routing system in a sense that data, when sender and recipient are inside Schengen area, is not sent via another country. There is no need to isolate users or restrict the access to the Internet. Seen from another perspective users accessing data in countries outside the European Union will have no profit from this solution since the communication partner (no matter if source or destination) is not covered by *Schengen Routing* Agreement. Currently the main contributor seems to be Deutsche Telekom, as depicted from an interview of Philip Blank [84] where they describe that ”data running over Telekom’s German networks stays in this country”. This could be seen only as a starting point, because if only one provider supports *Schengen Routing* the traffic to other providers may leave the country. In addition most users do not know which providers are connected. They should only have the goal to use national services and the rest has to be done by the providers.
Routing traffic only in a providers network might be easily achievable for the simple reason that a provider can control their own network, but how can a European wide *Schengen Routing* be implemented. There must be an exchange between routing possibilities and much more sensible network provider informations to ensure that data, sent from one provider to another, originating not to leave *Schengen Routing* area really stays with these boundaries. For example these aspects lead to the fact that QSC, a Telekom competitor, raised the question about the possibility of protecting traffic with this approach, since it might be impossible to determine data that would travel nationally or internationally.
In the latest news the governments of France and Germany could act as a key player in introduc-

ing *Schengen Routing*. The German Chancellor Angela Merkel and the French President Francois Holland picked up the topic in order to establish a European communications network that is beyond the reach of US security officials. An initiative from the government might push the development of a *Schengen Routing* area. However more and more people doubt that a European communications network would indeed lead to more security, because they argue that it would not be a problem for security agencies to set up more surveillance stations within Europe to capture data [86]. Since this is true several politicians (e.g. Jan Philipp Albrecht - German member of the European Parliament) stated the fact that a legal framework to secure the fundamental rights in Europe, especially in the market area, is much more important.
In the scope of economics *Schengen Routing* seems to be a big chance the generate revenues, since every provider can provide special offers for data storage with the European Union or selected countries. In addition special rates can be introduced to guarantee *Schengen Routing* at your Internet connection.
The goal for the research community from this *Schengen Routing* discussions might be a sensitization of companies and users to protect their data by supporting and using recently developed approaches reasonable for secure data storage and secure data exchange.

4.3.2 Legal and Ethical Facets of Data Sharing

Data sharing does play an important role for a scientific evaluation and assessment (often termed analysis) of data from operational systems, which determine amongst others the usage of services, protocols, systems, or software components by machines or individuals, which typically foresee a privacy constraint. Such analysis can lead to basic network, traffic, or operation know-how and optimizations, essential for today's Internet Service Providers in a highly competitive and challenging environment, in which efficiency gains may decide on success or failure for a provider or its services.

As discussed briefly in Section 3.5 the view of such data sharing from an Internet Service Provider's perspective contains a larger set of individual-and privacy-related information and data fields, which can lead to a personalized identification of an individual, who has generated certain events, who has utilized certain services, and who has undertaken certain actions within a network at a given point in time and at a given location. For example, accounting data for the sake of charging in form of Charging Data Records (CDR) or monitoring data for network and service management purposes in general in the form of NetFlow records determine two examples: they are needed to be individualized to charge the right user or to determine the right network access point, which suffers a performance degradation. Furthermore, Section 3.5 outlines the prospects on the ethical side, which are no settled these days and which do not typically follow detailed legal acts, but only can follow a common (if at all) understanding of data usage in shared cases.

Thus, besides the broader discussion on ethics of such data sharing, the legal facets of data sharing have not yet seen too much attention, since a typical approach of preventing any legal problems in case of data sharing plans is to deny any sharing request, either coming from the research community to a provider or even between departments within a provider's organization. As such, no legal questions have to be studied, as the data privacy is guaranteed - in the light of a planned for sharing activity - due to a non-revealing of those.

However, this very limited approach and less constructive case does not always apply, since (a) formal requests by a court can make data sharing legally demanded for and (b) provider's willingness to share data for external data analysis and optimization may be seen as a support for an operator's network operation. Thus, the demand for a viable and legal framework, being compliant with overall regulations, arises. Note that the case (a) does not relate only to the directive 2006/24/EC

[92], which addresses data retention, since other operations and usage data are available within a provider's affiliation, such as CDRs for charging and billing purposes that had been stored in the past and will be stored in the future, too, at least for a certain period of time.

As of today and to the best knowledge of the current situation, there does not exist a formal legal basis (either on the European, Swiss, or US American level), which would determine a clear approach for the case (b). Of course, due to Communication Commissions (*e.g.,* the Swiss BAKOM - Bundesamt fuer Kommunikation - or the US American FCC - Federal Communication Commission) regulations, embedded into national - typically - Telecommunication Acts (*e.g.,* by the Swiss proposal for a Federal law on the surveillance of postal and tele services [23]), the issuing of operator data for court cases is defined and applied in case (a). Additionally, a number of national telecommunication acts define quite restrictive rules for monitoring and analyzing such usage data, especially from the privacy perspective. This is due to the fact that, *e.g.,* with the knowledge of an IP address used for a certain communication the personal or human identity behind this technical identifier could be tracked, traced, and in turn revealed to the public or elsewhere, resulting in a break of privacy regulations.

Furthermore, in case of the Swiss Telecommunications Act [24] Article 26 on "Technische Kontrolle (technical measures)", which applies to wireless communications, in case of interferences observed in those wireless communications (a) "the BAKOM is legally allowed to monitor and store wireless communications" to ensure that an interference-free communication can be offered. Additionally, it states clearly as well that (b) such "information stored may only be used to identify the root cause of the interference (in the wireless communications)", complemented with the requirement to (c) "hand over such information monitored - in case of a suspicion that a criminal offense had been performed - to relevant authorities. All other information stored have to be deleted". In this case data sharing is well defined in principle, however, the interpretation on "which information" is considered to be relevant to detect such an interference is not determined in this law.

Finally, at the current stage of investigations of data sharing for network and service management purposes a multitude of facets exist, which are either fully interpreted by (1) a legal expert or lawyer or (2) a networking expert or engineer. However, a clear mapping of terminology or functionality between the two domains tends to be very blurry, if not even considered undefined from a scientific point of view. One reason for this situation may be seen in the fact that technology typically determines re-appearing, unchanged terms and conditions, which are always applicable in a given network or topology, while legal aspects, although governed by general or specific laws and regulations, are discussed and debated typically on a case-by-case basis.

Thus, a general conclusion on the validity or ineligibility of a certain procedures, measurements, or data analysis methods requited in the case of data sharing tends to remain impossible as of today.

5 Status-quo of Selected Current Regulations Impacting Network and Service Management

New technologies and realities of network and service management tasks place increasingly diverse demands on regulatory authorities. These European, Swiss, or American regulatory bodies plan to protect the consumer and enable a fair competition in the communications market to ensure growth of the economy by means of technology-neutral and transparent policies.

For instance, developments in the field of network and service management with respect to moving traditional in-house data storage to cloud-based globalized data storage with an international flow of data has lead to many regulative constraints due to the lack of transparency in a clear jurisdiction breakdown of such data flows. Also, regulation of data, services, and applications with the perspective of network neutrality has become increasingly important, especially to ensure fair competition and growth in the telecommunications and applications market.

This section, therefore, discusses the current and major aspects of regulative status in the area of network and service management, namely (1) data retention, (2) data storage, (3) cross border data flows, (4) network neutrality, (5) incentive auctions, and (6) cloud federations and resource allocations. For each of those aspects - as far as possible - the key technology at hand is presented, stakeholders involved are outlined, and regulation (if in place explicitly) is described. Subsequently, a brief analysis, the determination of open or unsolved issues, is followed by an overall discussion.

5.1 Data Retention

The field of telecommunications data retention covers the retention or storage of telecommunications metadata, such as call detail records, IP addresses, and locations. Among the data retained are typically the user IDs or IP addresses, user's location, webpages visited, email addresses, and time. The exact implementation of telecommunications data retention regulations varies between countries [40], [93], [94]. The European Parliament and the Council of the European Union agreed on a directive 2006/24/EC in 2006 [92], which regulates the retention of telecommunications data across Europe. This directive was declared invalid by the Court of Justice of the European Union (CJEU) April 8. 2014 [95].

The ongoing discussion on telecommunications data retention legislation in Europe determines an important facet in network and service management of today's networks and their usage as well as deployment.

5.1.1 Technology

Telecommunications data retention involves all electronic communication networks, which are publicly accessible. This includes telephony as well as data networks that citizens use every day for their telecommunication needs. Providers of such service collect certain meta data mainly used for billing, a few examples of metadata are caller ID, called party ID, and call duration. Legislation in some countries forces providers to retain this data for differing periods of time.

The European directive 2006/24/EC defines a retention period of maximum 2 years [92]. From a technological point of view it is not a challenge to retain that sort of data since storage capabilities are available. However, the retention of metadata will imbue a certain cost to providers if they are not retaining this kind of data already for the required period. The Australian Mobile Telecommunications Association (AMTA) states that the cost of retaining data beyond the usual period would have to be paid by the agencies requiring it [93].

5.1.2 Stakeholders Involved

Since the area of telecommunications data retention touches basic human rights all citizens of earth are stakeholders in this matter. Due to the heterogeneity of forms of government and different federations this section presents stakeholders on the example of the European Union:

- European Parliament / European Council: The regulator of the union is interested in harmonizing legislation among its member states thus it will pass regulations to reach this goal as shown by the European directive 2006/24/EC [92]. Furthermore, it has an incentive to prevent and successfully investigate cases of crime and terrorism.
- Member State: A member state of the European Union shares the incentives of the union. However, a state might have its own legislation which stands in conflict with the legislation passed by the union. Furthermore, a state, representing its citizens, might have a different approach to reach the aforementioned goals than the union. In fact, some European Union member states were sued by the European Union for not implementing directive 2006/24/EC [92], among those one example is that of Germany.
- Citizens: Citizens also have incentives to prevent and investigate crime and terrorism but at the same time they aim to safeguard their human rights. The human right, which is at stake in this topic is the right to respect for private and family life granted by the European Convention on Human Rights [32]. Citizens are sometimes represented by a commissioner for data protection.

5.1.3 Regulation Areas Affected

The field of telecommunications data retention is mainly an issue of data protection. The large scale collection of data, as intended by the directive 2006/24/EC [92], can be considered mass surveillance. The problem is that the retention of this data restricts privacy rights of citizens. Although, the European Convention on Human Rights [32] allows for exceptions to this right if *i.e.,* national security is affected. The differentiation between necessary restrictions and unproportional measures is a delicate and controversial issue. Another regulative aspect of telecommunications data retention is the usage and access of the retained data.

5.1.4 Open Issues

There are some open issues, as explained below, in this field of regulation:

- **Utility of retained data:** The general justification for retaining telecommunications data is the investigation of crime, directive 2006/24/EC [92] mentions serious crime in particular. Data published by the Austrian judicial authority [5] for 2013, after the directive has been implemented, shows that in 53.7% of the cases where retained data was accessed it was of no benefit to the investigation. For the 105 cases where the retained data helped to solve crime the type of crime was published with the number of cases. These are: theft (113), drug abuse (59), robbery (52), stalking (43), fraud (38), and dangerous threat (16). There were no cases of organized crime of terrorism recorded which are the main arguments for data retention in directive 2006/24/EC [8]. Switzerland has no legislature that requires the retention of data in general. A new draft law [23] that gives authorities the option to retain data of specific individuals which are part of a trial, a suit, or have gone missing to an extent of maximum 30 years but not longer than necessary.

- **Access to data:** In the press release of the ruling of the CJEU [95] directive 2006/24/EC [92], the court criticizes the lack of an objective criterion which would ensure that the competent authorities can access data only for investigation of crime serious enough to justify the interference with fundamental rights. The directive leaves the definition of "serious crime" to the member state's legislature. Furthermore, the directive does not define procedures, which involve the decision of a court before access to the data can be granted, like in case of search warrants this is a common practice.

  The Electronic Frontier Foundation (EFF) raises the issue of vulnerability of the databases to theft and accidental disclosure [27]. Essentially the argument states that even if appropriate procedures are in place, threats like malicious employees, hackers, or accidents can only be ruled out by not storing that type of data. Additionally the court states that the directive lacks clear rules or safe-guards to ensure the security of the data and prevent unlawful access or abuse. Furthermore, the irreversible destruction of the data is not ensured.

- **Type of data to retain:** Article 5 of Directive 2006/24/EC [92] lists in detail what data has to be retained, this data is categorized in these categories:

  - Data necessary to trace and identify the source of a communication
  - Data necessary to identify the destination of a communication
  - Data necessary to identify the date, time, and duration of a communication
  - Data necessary to identify the type of communication
  - data necessary to identify users' communication equipment or what purports to be their equipment
  - Data necessary to identify the location of mobile communication equipment

  It is debatable if it is necessary to retain all this data or if it is of use. To identify a source of communication in the Internet, the IP address is used which does not actually identify a user but only the person that signed the contract with the ISP. It is easy for criminals to circumvent being identified by using anonymizing services such as Tor [95] or even a simple VPN Server which resides in a country without data retention regulation.

- **Time of retention:** Directive 2006/24/EC [92] mentions a period between 6 and 24 month for which the data must be retained, Australian politicians are talking about 2 years [93]. The CJEU criticized that there is no distinction made between different categories of data and that all data would have to be treated the same way. Furthermore, the directive does not oblige the owner of the data to irreversibly destroy it at the end of the retention period.

5.1.5 Status

The status of telecommunications data retention differs among states. Therefore, examples are given with concrete cases.

In European Union, after the CJEU declared directive 2006/24/EC [92] invalid, there is no European Union legislation which regulates telecommunications data retention. States that implemented the directive already have to change their legislation again to comply with the court's decision.

Austria had implemented the European Union directive, which motivated case in the CJEU. After the European Court's ruling the Constitutional Court of Austria followed and declared the Austrian data retention law as unconstitutional [41] .

Germany, which has not adopted directive 2006/24/EC, declared that there is no intention on passing general data retention regulations. In Germany data can be retained in cases where certain citizens are under suspicion of crime.

Britain, in reaction to the CJEU's ruling from April 8. 2014, passed a bill July 17, 2014 to keep the status quo in Britain [94]. The parliament is still in dispute about the legality of this bill, which will expire at the end of the year 2016. The parliament is working on new legislation that complies with CJEU's ruling.

Australia is seeing a discussion about data retention legislation between its political parties [93]. So far Australia does not have a telecommunications data retention law, however, state agencies and departments can access data retained by telecommunications providers without a search warrant.

5.1.6 Discussion

There is one argument for telecommunications data retention, the prevention and investigation of crime and terrorism. History has shown that such retained data can be helpful in solving cases of crime [40]. It is undisputed that metadata can be an important investigative instrument. However, this comes at a certain price. For nation wide data retention citizens give up a big amount of their fundamental right to privacy. Since existing legislation typically does not require a court order or search warrant to access the data citizens are de facto under constant surveillance by different government agencies. Another dimension to this price is the actual cost involved in collecting and retaining the data. Either governments or telecommunication customers have to pay the bill in the end, which are citizens and business in both cases. With data retention comes a general risk of abuse or unauthorized access to the data. Investments in security measures to protect the data will further drive up total cost but cannot guarantee total security.

The issue of telecommunications data retention is not on a technical level but on a political. States or societies have to weigh its benefits and cost against each other and decide how far they want to go. The CJEU has declared one approach as unlawful and with this act has defined some limits for member states' data retention laws. There is still no final answer to the question of what extent of data retention is proportional to its cost. Discussions are ongoing, also outside the European Union.

Concluding, telecommunications data retention is a field without clear answers. Whatever is decided in that matter is a trade-off between national or personal security and the cost, such as giving up private freedom. It yet to be seen if the CJEU's decision will have a signaling effect to other states like Australia where the discussion is ongoing. Organizations, like the EFF, will argue with the decision of the CJEU in other states as well. member states, which have implemented the invalid directive, will have to rethink their data retention legislature which will take time. Telecommunications data retention is currently a hot topic and will very likely continue to spark debate as technology evolves and new forms of metadata appear.

5.2 Data Storage

The field of data storage covers the practice of storing information in multiple storage media, by different parties (*i.e.,* users, providers), which may or may not be geographically dispersed. Data storage is essential in the modern era, since it is present in any application, service, or technology that deals with computation of information.

As will be shown in this section, different regulative problems arise when data storage is evaluated from different perspective, and it becomes even more critical with the recent use of Clouds, storage overlays, and systems that represents data in a finer level of granularity.

5.2.1 Technology

Data is a set of values, symbols, or variables that, coupled together, forms information. Data is a concept that is considered to be the lowest level of abstraction. Such set of values, symbols, or variables follow a well-defined structure in which data is represented. These structures are often described in standards, since multiples entities (*i.e.,* software) must write and read data following such data structure.

A computer file (or just a *file*) is an abstract representation used by file systems to express data, following a file format (*e.g.,* JPG, AVI, MP3). File formats are data structures (standardized or not) to represent files of a certain type [61].

It is important to note that a file (*i.e.,* data, with a sequence of bytes) that does not follow a certain file format is not meaningful to whom is reading/interpreting it. Both writer (*i.e.,* who generated a file) and reader (*i.e.,* who is reading/interpreting a file) must be aware on which file format and structure the file data is represented. Therefore, if the reader can interpret the file data and generate the expected output by the writer, thus, the data is considered *intelligible*.

A user can store files in multiple places: (1) Private media, such as hard disks, USB drives, or SD cards, (2) on the Cloud, such as Dropbox or Amazon, not being aware where exactly the files are being stored, and (3) on other users' devices, such as computers equipped with hard disks, in a Peer-to-Peer network. In these three cases the files can be privately stored, not allowing third-party access from anyone else except from who is storing it (*e.g.,* using cryptography); or shared, allowing that other users retrieve the stored files. In (2) and (3), the file sharing process is made through the network and enabled by a software – available by a Cloud provider or a software which enables a Peer-to-Peer (P2P) application (*e.g.,* BitTorrent).

Looking from the Cloud provider perspective, it is up to the provider to decide where and how users' files should be internally stored. The files can be re-organized (*e.g.,* fragmented, encrypted) in order to suit internal restrictions, requirements, and optimization levels set by the Cloud provider. Even though files may be internally distributed or re-organized, user's files are provided in its original format when requested by someone (download). Thus, users downloading and uploading data are not aware of how files were fragmented or where the actual data fragments are located. Such process is invisible to the end-user. The majority of Cloud providers and services, such as Dropbox, Google Drive, Imgur, or Amazon S3, employ internal data storage that are not totally transparent to the end-users [42].

The same happens when looking from a P2P application perspective, but with a more transparent process. Every user runs a file sharing P2P application being part of a decentralized network which every node has the same software characteristics. In other words, how a file is re-organized in order to suit the P2P application requirements is performed homogeneously by every participant of the network. Thus, if files/data should be fragmented, the process happens using rules implemented in every P2P application. It means that all other users part of this network are aware of how the fragmentation happened and where the fragments are located. BitTorrent is a typical example of such a process.

There are applications/services that act as a storage overlay, also adopting hybrid mechanisms in order to manage and store data, such as PiCsMu [60] and Otixo [74]. Storage overlay applications manage how and where data is stored, but they use underlay services (*e.g.,* Cloud providers and/or Peer-to-Peer networks) to actually store the data. The overlay application implements algorithms to decide, *e.g.,* whether data should be fragmented, how to fragment it, which encryption scheme to use, apply error correction codes to ensure minimal levels of data reliability and, at the end, decide where to actually store the data. The particularity of storage overlay systems rely on being aware of the whole metadata information, but not being actually responsible for storing the data,

i.e., keeping data with a meaningful representation under its premises. Storage overlay systems may decrease the granularity of how data is represented, thus storing a sequence of bytes that may not have a meaning for whom is storing it.

Another characteristic of storage overlay systems is the capability of transforming data for storage purposes. For example, the storage overlay system may encode parts of a file into other well-known files in order to enhance security/privacy (i.e., encoding encrypted data fragments within a JPG file). Therefore, the actual file stored in a Cloud service or in a Peer-to-Peer network does not characterize the original file format that the end-user aims to store.

5.2.2 Stakeholders Involved

Stakeholders involved in the area of data storage are:

- End-User (EU): End-Users provide data or files to be stored, share files, and also perform file download, using or not a Service Operator. EUs express their will to which storage action related to the data should be performed. The EU has the file to be stored, in a well-known file format.
- Cloud Service Provider (CSP): CSP provide Cloud services that accept data storage in any file format (raw data, without necessarily have formats), or only in specific file formats (e.g., JPG, PNG, MP3). CSPs can also be contracted by other CSPs, since sub-contracts can be fixed to provide a broader range of services – e.g., Dropbox contracts Amazon S3.

  CSPs should employ technical mechanisms in order to:

  - Prevent Cloud Costumers (CC) to store data in CSPs' infrastructure that does not comply to the service agreement or term of service, which were established and accepted beforehand. The prevention can occur in the moment that CCs specify what kind of data they want to store, employing, e.g., strong data validation mechanisms [ref] GSMachado:DataValidation.
  - Audit its own CSP storage infrastructure anticipating possible legal issues due to data stored by CCs.
- Cloud Customer (CC): Cloud Customers have a relation to CSPs since a service agreement or a term of service was accepted beforehand. CCs can also be EUs, since EUs might have user accounts in one or multiple CSPs.
- Legislator (LE): Legislators take regulatory means to resolve conflicts between stakeholders and judicial uncertainties.

5.2.3 Regulation Areas Affected

Below is the list of major areas, which are effected by the regulations:

- Data granularity:

  The authors in [67] provide a response to a project proposal evaluation, which was published by the UK Parliament. In this document, the authors highlight the problematic about intelligible data versus distributed storage:

> Given distributed storage and proprietary file formats, access to physical media, e.g. storage hardware in a third country, does not necessarily afford access to intelligible data. The only sure way to access intelligible data is through the user logging in to reunite fragments into intelligible form automatically. Fragments are distributed automatically; providers may or may not know in which hardware all fragments comprising one data set are stored. Some fragments may be intelligible, others not. Some providers can bypass or use customer logins, others cannot. Even providers bypassing customer logins cannot, without decryption keys, decipher data securely encrypted by controllers. Similarly, after deletion operations, fragments may or may not be intelligible or re-unitable. Again, these depend on service type and design.

In [87] the authors discuss the legal difficulties in the Swedish perspective. Although, the text is dated back to 1998, the authors emphasize the emerging focus on minimal data fragments:

> A data store-space contains "units" of data. In a traditional store one deals with units such as "books", "letters", "index cards", "formularies", and "contracts". In a comfortable, traditional situation there is a close correspondence between the unit that is asked for and retrieved and the physical object that is and can be handled as a unit. Consider, for example, a request to obtain access to the correspondence of an individual during a certain period of time. In the digital world new information handling principles begin to apply to the units of data. Fragments can be retrieved, combined, restructured, excluded, compared etc. to an extent that is simply not possible in a traditional, paper-based environment. The limits are pushed downwards so that individual micro units – a single alphabetical or numeric sign, an isolated picture element, a momentary breathing – can be identified, singled out and used. Basically, we begin to deal with patterns of ones and zeros (bit patterns) and the pattern delimiters are logical rather than physical in nature.

A further issue is the possible ability of the provider (and of any sub-provider, *e.g.,* IaaS provider) to access cloud users' data:

> As discussed [...], where data stored with providers are not encrypted, or only weakly encrypted, most providers have the technical ability to access the data in intelligible form. Most providers also contractually reserve the right to do so, e.g. for service/support reasons or if disclosure is compelled or requested by law enforcement authorities. If the controller/cloud customer knows that the provider has the ability and legal right to access its data, and the provider is established outside the EEA, does this mean that the controller "intended" to allow non-EEA entities to access its data? Must the controller investigate the extent of the provider's ability to access its data?

Storing non-intelligible data may raise legal problems due to:

- The lack of knowledge of what someone intended to store, but allowing to store on someone's premises without any kind of inquiries;
- Privacy reasons, since non-intelligible data can be classified as personal data even not being encrypted or annonymized. Thus, storing and disclosing non-intelligible data should be faced as sensitive.

- Fragments in different locations versus data protection laws:

A CSP may be characterized as an entity that process and modifies data (or, personal data) if its services/applications perform data replication or data fragmentation [43]. Thus, splitting personal data into fragments may itself constitute processing personal data, even if the resulting fragments may not be considered personal data. However, arguably, if personal data is fragmented into non-personal data, then subsequent storage of the fragments should not be processing.

Even where unencrypted data stored is clearly considered personal data, might be justification to argue that the CSP itself is not, or should not be considered, a processor, as long as it takes the suitable means to prevent access to the data by anyone other than the relevant user [43].

- Terms of Service and Data Storage:

  Usually, CSPs have Terms of Services with the following sentence:

  > CSP's terms of service do not allow the sending of automated queries of any sort to our system without express permission in advance from the CSP.

  It means that the CSP does not allow any kind of automated software to interact with its services without previously being registered to perform specific queries. Thus, storage overlay systems may have legal issues since they use automated means, through registered APIs or not, to persist data in CSPs infrastructure.

  Related to content, CSPs' terms of service often mention that the service should be used accordingly to its purposes: for example, a service to store images, of different types (JPG, PNG, etc), should only store personal data related to images. Therefore, CSPs should employ strong data validation algorithms [61] in order to:

  – Verify if data pushed to CSPs infrastructure complies to the terms of service;
  – Detect any kind of data transformations (e.g., data injection within well-known data formats) that could hide illegal material.

5.2.4 Status

Naturally, the status of legal decisions of data storage depends a lot on the case. One could compare the BitTorrent metafiles to storage overlay systems, which in fact do not actually store file data. Whether who holds the metadata violates, e.g., copyrights by linking to copyrighted material, without the authorization of copyright holders, is highly controversial. Recently, Suprnova.org, TorrentSpy, LokiTorrent, BTJunkie, Mininova, Demonoid, and Oink's Pink Palace, and, most notoriously case, The Pirate Bay, faced serious legal issues. All of them were shut down, but The Pirate Bay remained online since its owners/authors are still appealing from the initial court decision.

Even though BitTorrent presents some similarities to storage overlay systems, the fundamental difference is that storage overlay systems use CSPs to store data, and not individuals' storage – how it happens with BitTorrent. Therefore, CSPs are responsible, as a company, to what is being stored and to what is shared from their infrastructure. There is no legal decision, until this moment, that consider such a storage overlay system. However, with the massive exploiting of, e.g., PiCsMu [60], for illegal purposes the CSPs and LEs should be pay attention on the intent of each user to based their decision upon.

5.3 Cross Border Data Flow

This section discusses the topic of cross-border data flow in detail. After a brief introduction, the involved stakeholders are analyzed and the requirements for an adequate regulation are provided. An in-depth analysis of the field will discuss technical and political aspects of the subject. Solved, unsolved, and debated issues are provided subsequently. The final section summarizes the pros, and cons and draws conclusions.

5.3.1 Technology

The term ”cross-border data flow” refers to the very common scenario where data packets traveling from a source IP address to a destination IP address cross country borders on their way, often without the knowledge of the involved end points [57]. Cross-border data flows support research and development activities [63] and are understood to have a positive impact on economic efficiency and productivity. On the other hand, cross-border data flows are also subject to intense debate, due to the reasons described in [63]:

- Privacy and Data Protection: Different governments have different and often incompatible policies in place to protect their citizen’s personal data.
- National Security: Some politicians see future wars moving from the real to the virtual world [75]. Controlling the data flows in such a scenario is, therefore, key.
- Political Restrictions: Social media technology can be used to mobilize large amounts of people, as could be seen during the Arab Spring [29]. Oppressive governments have a vested interest in preventing certain data flows from reaching their destination.
- Morality-based Internet Restrictions: Some governments may want to ban morally questionable content, such as pornographic, religious, or gambling sites.
- Intellectual Property Protection: Protecting Intellectual Property (IP) rights is still an unresolved issue in today’s Internet world.
- Commercial Restriction: Commercial restriction refers to the practice of blocking Internet-based companies from doing business in a particular country.

The above points alone provide ample room for debate. What is more, any attempt to control data flows that does not serve a purely technical purpose such as load balancing, is a violation of the network neutrality principle, which stipulates that all packets must be treated equally. The question from a service management point of view is, therefore, whether political aspects will have to be taken into consideration in the future also.

5.3.2 Stakeholders Involved

The set of stakeholders affected by cross-border data flows can be divided into three major categories: End-users, government, and corporations. Each of which is characterized in more detail below:

- End-Users: By engaging in typical Internet activities such as searching for information, engaging in social media activities, or executing a transaction in an online store, end-users leave traces that can be used or abused by corporations, governments, or other end-users.

- Government: Governments are responsible for regulating local and cross-border data flows such that the interests of end-users, corporations, and the government are protected.
- Corporations: Most corporations are connected to the Internet and therefore at risk to have secret information exposed to third parties in case of a successful attack or careless employees. Moreover, corporations are often interested in detailed information about end-users so they can distribute their products more efficiently.

On the one hand, the individual stakeholders have a responsibility themselves to protect sensitive data to the extent they can. On the other hand, governments are responsible for designing and enforcing regulations such that the interest of the stakeholders are protected. This task is challenging, because the interests of the stakeholders are often at odds.

5.3.3 Regulation Areas Affected

A regulatory framework with respect to cross-border data flow must encompass the areas security, privacy, fees and costs, interconnection, and universal service. The requirements are detailed below:

- Security: The framework must define how access to sensitive data can be restricted to authenticated and authorized parties even if it is sent across political, legal, or economic borders.
- Privacy: The framework must define how the privacy rights of end-users and corporations are or must be protected if privacy-relevant data crosses political, legal, or economic borders.
- Fees and Costs: The framework must define how fees and costs are handled for cross-border data flows. This will also include the definition of abusively high and low prices [53].
- Interconnection: The framework must define whether and – if so – to what extent routers residing in different political, legal, or economic areas can be interconnected.
- Universal Service: The framework must define to what extent service providers are required to provide universal service to end-users.

5.3.4 Analysis

This section provides an in-depth analysis of cross-border data flow issues. It is subdivided into a technical part, which discusses technical possibilities and challenges with respect to cross-border data flows and a political part that focuses on the political aspects.

- **Technical Aspects:** The Internet was designed with scalability and decentralization in mind. The sender of a data packet specifies the target address and routers forward the packet towards the destination. This makes the network scalable, because there is no need for any node to know the topology and state of the network and resilient because packets can be rerouted in case of node failures. Furthermore, the Internet was designed to be network neutral, *i.e.*, all packets would be treated equally, irrespective of their source, destination, or content.

  Introducing cross-border data flow regulations breaks with these design principles. A law stipulating that certain traffic must not leave a country or economic area implies that the routers of the Internet take additional information into consideration. In particular, they need information about

  - the political policy and
  - the location of routers

  but also information about

  - the source
  - the destination, and
  - the content

  of the data packet.

  First of all, routers need fine-grained policy information such that they can take routing decisions that are in line with existing policies. Second, they need geographic location information about their neighbor routers so they know what forwarding decisions will cause a packet to be sent over a border. Then, routers need information about the source, the destination, and the content of the packet to know what policies apply for a packet in question.

  Some of the required routing policies may be implemented implicitly, *e.g.,* by establishing peering agreements such that packets never leave a country or economic zone unless the packet destination address lies outside [106] or by making use of the dynamic routing features of IPv6 [38]. Others, such as geographic location and policy information will require hard- and software modifications of Internet routers, possibly even changes in routing protocols.

  In any case, the transition costs (*e.g.,* hardware, software, migration) as well as the cost for enforcing the new policies would be substantial.

- **Political Aspects:** Political aspects boil down to the design, implementation, and enforcement of regulatory frameworks that balance the interests of the stakeholders (*i.e.* end-users, corporations, and government). A suitable regulation framework must take different kinds of traffic into consideration:

  - Uncritical data traffic: This is data traffic in which neither end-users, nor governments, nor corporations have a specific interest in. Examples are configuration traffic or software update traffic.
  - Critical data traffic: This is data traffic in which at least one stakeholder has a particular interest in and for which there is a certain abuse potential. Examples are medical records, corporate secrets, or information concerning national security. Regulations concerning this kind of data traffic must specify whether producing such data flows is permitted in the first place (*e.g.*, Should it be legal or illegal to send medical records via the Internet?) and - if it is - whether it must be treated in a special way (*e.g.*, encryption or routing restrictions).
  - Illegal / Inappropriate data traffic: This is data traffic, which is considered unsuitable or illegal according to a country's regulations or policies. It can be divided into content that is considered illegal globally (*e.g.*, websites facilitating human, weapons, or drug trafficking) but also content that is only considered to be harmful by certain jurisdictions (*e.g.*, religious sites).

  There are several challenges when it comes to classifying data traffic. The first one is that end-users, corporations, and governments – but also the aforementioned stakeholders among themselves – are likely do disagree substantially concerning the questions what data belongs into what category. The second one is that classifications will vary from country to country. This is an issue, because hardware and software requirements may differ from

country to country and configuration and maintenance tasks can possibly not be standardized. The third one concerns the question of how to find out what category a data packet belongs to.

In any case, any form of content-based data traffic management violates the principle of network neutrality, which stipulates that all traffic must be treated equally by the network devices.

5.3.5 Solved, Unsolved, and Debated Issues

Table 22 summarizes whether issues concerning the regulation of cross-border data flows are solved, unresolved, or debated. An (X) means that the issue is pending, an X means that the issue is addressed.

Table 22: Status of Issues Concerning the Regulation of Cross-border Data Flows

Topic	Solved	Unsolved	Debated
Security		X	X
Privacy		X	X
Fees and Costs	X		X
Interconnection	X	(X)	X
Universal Service	X		

Security aspects remain unsolved so far. This is not because suitable technologies do not exist but rather because they are not deployed. Exceptions do exist, such as online payment systems or secure chats; the bulk of all traffic is transmitted without encryption though. The issue of encryption is also highly debated because it is a two-edged sword. On the one hand, a complete end-to-end encryption of all Internet traffic would make Internet traffic secure; on the other hand, it will also make it more difficult to fight cyber crime and terrorism [38].

Privacy aspects remain both unsolved and highly debated so far. The debate has not reached a mature stage yet.

The details relating costs and fees between end-users and service providers are agreed upon in a contract. The same applies for data traffic between service providers, although these contracts are substantially more complex. The subject is still strongly debated because costs for end-users tend to be high, because there is a lack of competition in the last mile in most countries. As far as peering and transfer agreements are concerned, alternative billing and charging models are currently being discussed, because the quantity of data produced by end-users and content providers keeps increasing but the revenues for service providers tend to shrink. An overview of such models can be found in [56].

Service providers are currently interconnected via peering and transfer agreements. What agreements a service provider enters into depends on economic and performance aspects but will usually also reflect the service provider's corporate strategy. Aspects of interconnection can be considered to be solved with respect to current policies. Should regulatory requirements, which demand that packets must be routed within political or economic borders, become reality, the issue of interconnection must be considered to be unsolved.

Guildeline 2002/22/EG of the European Union demands that member countries must ensure that all end-users have adequate access to telecommunication services [25]. This issue can, therefore, be considered to be solved.

Table 23 shows whether technical and political aspects with respect to cross-border data flow are solved, unsolved, or debated. An (X) means that the issue is pending, an X means that the issue is addressed.

Table 23: Status of Issues Concerning the Analysis of Cross-border Data Flows of Technical and Political Aspects.

Topic	Solved	Unsolved	Debated
Technical Aspects	X	(X)	X
Political Aspects		X	X

In the European Union, technical aspects of cross-border routing can be considered to be solved for now because there is no regulation in place that requires packets to remain within the country or economic borders. Should the debate result in policy requirements that requires packets to remain within country or economic borders, the technical aspects are at least partially unsolved (*c.f.* Section 5.3.4). The political aspects are unsolved and probably will remain so until the debate about cross-border data flows has become more mature.

5.3.6 Discussion

The pros of unregulated cross-border data flows are as follows:

- Network neutrality is preserverd.
- End-users have access to an uncensored Internet.
- Business and communication accross country and economic borders is facilitated.
- The cost for hardware, software, and maintenance remains low because the status quo is preserved.

The cons of an unregulated cross-border data flow are as follows:

- The privacy of end-users and corporations can be compromised more easily.

As can be seen from the above list, the advantages of the status quo are substantial whereas the disatvantages are limited. A better protection of end-user privacy and security could be achieved but only at the expense of current advantages.

5.4 Network Neutrality

Network Neutrality is the principle that each data packet is treated the same way. It does not matter what the content of the packet is, what the source of the packet and its destination is. With network neutrality, the user is not discriminated or charged differently than other users. Technically it is possible to distinguish between the content, source, or destination of a packet, and some providers partially implement this already [59]. ISPs claim that P2P, online gaming, and video on demand degrades the performance and experience of other users as these types of application consumes a lot of bandwidth. An ISPs typically over utilizes its network especially during peak

times. Thus, ISPs that cannot serve all requests at peak times seek to prioritize the traffic in order to use their bandwidth more economically. Such a prioritization can be done in different ISO-OSI layers [91]: While the source and destination prioritization can be done in layer 3, the identification of applications is either done in layer 4 (ports), or even in layer 7 with deep packet inspection.

Regulators now have the task to discuss and propose regulations to provide a consistent handling of network neutrality, how it should be implemented, and how to handle traffic prioritization. The technical implementations for either way (prioritization or no prioritization) already exists. Thus, the remaining task is to regulate it.

5.4.1 Technology

The most important task for traffic prioritization is to identify traffic. Different characteristics can be used for traffic prioritization: Source or destination can identify the user or the service. The IP header contains these information, thus only the headers need to be inspected. To detect applications, ports can be used which requires to inspect the TCP or UDP header. However, applications sometimes try to hide due to either unwanted traffic prioritization or due to firewall restrictions. In that case deep packet inspection can be used where the payload is being analyzed. Compared to IP, TCP, or UDP header inspection, deep packet inspection is more resource intensive as more data has to be analyzed. Thus, the remaining challenge is to find mechanisms or algorithms how to detect protocols and applications in high speed Internet more efficiently. However, network neutrality as discussed in [36], [71] often mention destination prioritizing. For example that Netflix might have to pay additional fees to provide the same quality of experience as they generate lots of traffic.

5.4.2 Stakeholders Involved

Following stakeholders are involved:

- Regulators: Regulators should provide a consistent ruling. They need to understand the conflict of interests of the other stakeholders. They have the threat of over regulating, with endless discussions and no substantial results.
- Internet Service Providers: They need to generate income to provide infrastructure to its end users. To demand use bandwidth more efficiently, to charge for high volume services. They have the possible threat of loosing customers for providing bad quality of service and to have massive over provisioning of bandwidth.
- Service Providers: Service providers need good infrastructure to the end user. They have a threat that a competitor will provide the service earlier to the end-user.
- End-users: End user demand to have a good quality of service. If all users use bandwidth in peak times, the user may not have a fast connection.

5.4.3 Regulation Areas Affected

Network Neutrality is an active regulation area and currently much discussion is going on. Google, Facebook, Amazon, Reddit, Mozilla, Netflix, and Kickstarter are teaming up with civil rights organizations to fight for net neutrality in the US. Recently the second round for statements of the FCC ended, with many statements arguing in favor of net neutrality. In EU, discussions are ongoing and the European parliament recently voted for net neutrality with a few exceptions [89]. However, a final decision was not made. In Switzerland, a motion passed in the parliament where net neutrality should be explicitly mentioned in the new and upcoming telecommunication law.

5.4.4 Discussion

There are two aspects of Network Neutrality: Either the traffic gets prioritized based on the type of application (BitTorrent gets lower priority than VoIP), or traffic gets premium priority if service providers pay for it (*e.g.,* Netflix pays to get the best service). Both aspects are problematic, as for example in gaming, low network lag is essential to get a good quality of experience. Such a user, would be discriminated even when this user does not play that often (but others do). The other aspect that service providers have to pay for premium services is problematic as well as this would add an higher market barrier for new and innovative service providers.

On the other hand, ISPs are confronted with over provisioning and need to have enough bandwidth for peak times. Nowadays, IPS users typically have flat rates where the user expects to have the bandwidth available at any time. Although many ISP users consume their bandwidth in fair manner, some heavy users can degrade the quality of service for the other users. Thus, the traffic prioritization makes sense to have in place for traffic with real-time characteristics such as VoIP. Other means of ISPs is to terminate its subscription with the reason of misuse the fair usage, or cap the bandwidth if a certain threshold was reached.

On the other hand, it can be also argued that the Internet service is booming and new and innovative services are being developed due to lack of regulations. Having new regulations in place could slow down the innovation.

The status work performed in this field can be divided into three major categories, which are listed below and which cover the major views as outlined in literature.

- Solved issues: Technical aspects of traffic identification, layer 3, 4, and 7 identification has been already developed and implemented.
- Unsolved issues: Deep packet inspection with high speed Internet can be improved and decision about if network neutrality should be regulated and how.
- Debated issues: There is a conflict of interest between ISPs, service providers, and end-users.

The problem to solve is mainly on the political and regulatory level as on the technical level, solutions exist. They can be improved, but technology exists that can be implemented right way. Thus, the main challenge is to find a regulation with a benefit for all.

5.5 Incentive Auctions

This section discuss the topic of incentive auctions in networking domain. In such environment achieve revenue maximization for service providers, or increment of the social wealth-fare, via auctions is challenging due to dynamic decision-making demand in todays networks. Thus, first the concept of dynamic auctions is discussed and then the current state of research regarding dynamic auctions with a fixed population and dynamic information is presented. Finally, the value of Dynamic auctions is discussed beyond the IT domain.

5.5.1 Dynamic Auctions

Most of the research on auctions has been done on static, one-time auctions, *i.e.*, auctions which are executed once to fulfill a certain purpose. These auctions range from single-item auctions like

the English Auction [62] or the Vickrey's Auction [103] to combinatorial auctions where a combination of items and even parts of items are being auctioned off [18][19]. In the specific setting of the Auction-based Charging User-centric System (AbaCUS) [99], a single item, a call, is being auctioned off repeatedly. Therefore the auction cannot just make a single decision, but a sequence of decisions has to be made. This is called a dynamic auction and the decisions of the dynamic auction imperatively depend on the environment of the system where it is in place. Static one-time auctions are not suitable in many dynamic situations, as demonstrated by [83], where it is shown that the second-price sealed-bid auction, which is equivalent to a Vickrey's auction in setups with single items, is not truthful if losing bidders have the opportunity to win future auctions for the same item. This concept is called the "option value" associated with losing an auction by the author. Further findings are that the second-price sealed-bid auction does not only lack truthfulness but fails to yield an explain efficient outcome in some situations.

Two dimensions exist to distinguish dynamic auctions. The population of agents, *i.e.*, there is always the same amount of bidders throughout time or there is the possibility that bidders join or leave over time which is referred to as a fixed or dynamic population, respectively. The second dimension is the private information of the agents. Agents can either have fixed information, i.e. their private information does neither change with time, nor with the allocation of items throughout the history of the dynamic auction. Or agents can have dynamic information which means their valuation for the items at stake can change during time, affected either by time itself or by past allocations. The call termination market is a setup with a fixed population with dynamic information considering Mobile Network Operators (MNOs) are joining or leaving markets in intervals far larger than the timespan of interest for the auction. The information is dynamic due to the fact that the MNOs valuation for terminating calls is linked to the load of their network, which is neither known by competing MNOs nor by authorities.

5.5.2 A Fixed Population with Dynamic Information Example

The call termination market consists of a fixed population with dynamic information. The revelation principle for dominant strategy equilibria justifies focussing on truthful, direct revelation mechanisms [37]. Therefore only mechanisms with a focus on truthful revelation of changing private information in dynamic environments are considered. Also, both efficient as well as revenue maximizing auctions are considered relevant due to the fact that one of the goals of this thesis is to outline the effect of both concepts on the call termination market. There has been a lot of research in this field lately. The first example is the auction in the system on which this thesis is based. There, an alteration of the Vickrey-Clarke-Groves (VCG) without monetary compensation and a draw resolution mechanism is proposed [99]. The draw resolution mechanism also prevents a single agent from overpowering other agents in the auction and gives incentives to participate in some low revenue situations. A social welfare maximizing generalization of the VCG mechanism [14], [39], [103] for dynamic settings, the Dynamic Pivot Mechanism, has been proposed by [3]. That is, after each history, the expected payment for each agent coincides with the dynamic externality cost he imposes on the other agents. This is done as in the classic VCG mechanism by calculating for each agent i the optimal allocation when agent i is not present in the mechanism. Therefore, each agent is willing to truthfully report his information in every period. The mechanism is modeled in discrete time and all agents share a common discount factor. The private information is an agent's perception of his future payoff path based on the public history of allocations and his private history of realized signals. Another similar mechanism is proposed in [6]. The agent's private type evolution is modeled as a Markov decision process in discrete time in both mechanisms [78]. The same authors also extended the dynamic VCG mechanism to work in domains with a dynamic population and dynamic information [7]. Although this is a powerful extension for many applications, *e.g.*, in a

networking environment where the population of agents can change because some are unreachable or when end-users are involved in the bidding, it brings unnecessary complexity into the call termination domain.

5.5.3 Dynamic Auctions Applied to Similar Domains

The auction introduced in [105] aims at maximizing the revenue of a cloud computing provider by deviating from fixed prices towards dynamic prices set by a dynamic auction. Users can bid their value to receive a cloud instance and get priced according to the demand, *i.e.*, the amount of other users competing to use cloud instances and their value to do so. The auction introduced is similar to the work in AbaCUS in the way that it faces many of the same constraints, such as favoring a direct revelation mechanism because the decision has to be perceived as instantaneous by the users and it is revenue maximizing and truthful. Keep in mind that revenue maximization in normal auctions is equivalent with expenditure minimization for the user in the reversed setting of the call termination market. Cloud computing providers face the same maximization problem when deciding how many instances to to sell at each point in time as the MNOs face when choosing how much cell capacity they intend to allocate to users during a certain time frame. Because both face opportunity cost from rising prices in the future, but also from not allocating all available resources in the present. On closer examination it becomes obvious that the two domains differ quite fundamentally by the fact that in one case the bidder is facing the optimization problem and in the other case it lies with the auctioning party for the call termination market and the cloud market, respectively. When classifying the auction according to the population and information dimensions it would be an auction with a dynamic population with fixed information as modeled in REF50 and de facto probably also dynamic information.

The power grid market is similar to the call termination market in the way that power providers compete against each others in an auction. There is a dynamic population of power providers, and due to the fact that some power sources can only be operated depending on external factors like the weather, these power providers have dynamic information on their power production cost. Although this market could be modeled as a dynamic reversed auction it is, in practice, conducted in a continuous double auction. In double auctions buyers and suppliers submit their values, a clearing price is set depending on all submissions and buyers and suppliers are then matched according to their bids. This mechanism is, of course, not strategy-proof and there is work on possible bidding strategies including automated bidding based on algorithms to improve an agent's outcome compared to truthful bidding [20]. Other auction mechanisms have been proposed with focus on lowering user payments [107] or a more efficient usage of available fuel resources [79]. Neither of which are truthful according to the authors.

5.6 Cloud Federations and Resource Allocations

The field of cloud federation covers the practice of interconnecting data centers of different operators for live migrating virtual machines and data between these for the purpose of balancing traffic and workloads, especially during peak times. Therefore, cloud federations determine an important facet in network and service management of today's networks and their usage as well as deployment. As will be shown in this section, regulative problems that already arise for a single cloud become more severe in clouds federate and new problems arise.

5.6.1 Technology

A cloud efficiently processes unpredictably changing workloads by virtual machines (VMs), which are dynamically started on the cloud's physical machines. Thereby cloud computing allows private persons or business organizations to have their workloads processed without owning the according physical infrastructure. Since virtual machines can be executed by any physical machines with a chipset that allows for resource virtualization, virtual machines of cloud customers can be moved within the physical infrastructure, i.e., live migrated between the data centers physical machines. Since a cloud provider has several customers, the size of its infrastructure usually far exceeds the size of infrastructure an individual customer would have to afford for hosting the workloads himself. Therefore, cloud providers can partition their infrastructure over several data centers, which increases resilience and offers customers access with greater spatial diversity. These positive properties enabled by infrastructure distribution also allows clouds to federate by hosting virtual machines for one another. Therefore, "Cloud federations comprise services from different providers aggregated in a single pool supporting three basic interoperability features resource migration, resource redundancy and combination of complementary resources resp. services" [58]. A federated cloud is the deployment and management of multiple services to match the business needs and allows the customer to choose best possible services, in terms of cost, availability, and performance to meet their requirements. However, in order to comply with the service level agreements between a cloud provider and a customer, the cloud may also federate with other clouds transparent to the customer, i.e., the cloud provider may outsource the customer's virtual machines to the data center of another cloud provider without implicitly informing the customer. While data may already get distributed across national borders, when the cloud provider owns data centers in different countries, this likelihood further increases in case of federations. This is critical, as will be shown subsequently, many of the legal issues in cloud computing arise from distributing cloud data internationally.

5.6.2 Stakeholders Involved

Stakeholders involved in the field of cloud federation are as follows:

- Data Center Operator (DCO): DCOs provide cloud capabilities, i.e., own and operate a physical cloud infrastructure. They have the responsibility of setting up and maintaining any service that they offer. They also have to adhere to any legal requirement for data protection and privacy. Cloud federations offer two substantial benefits to DCOs. First, it allows DCOs to earn revenue from computing resources that would otherwise be idle or underutilized. Second, cloud federations allows DCOs to expand their geographic footprints and absorb demand spikes.
- Cloud Service Provider (CSP): CSPs deploy the infrastructure offerings by DCOs to offer services to cloud customers. In case of big players such as Google and Amazon the roles of DCO and CSP coincide.

  Some CSPs and DCO form coalitions to develop guidelines for certain aspects of cloud computing or better represent their interests towards political bodies. For example, in 2008, the Cloud Security Alliance (CSA) was founded to develop guidelines for secure cloud computing and to improve communication between CSPs, DCOs, and customers. In Europe the interests of DCOs and CSPs are represented by the umbrella association EuroCloud Europe.
- Cloud customers (CC): include end-users and companies that deploy cloud-based infrastructure for their IT requirements. Cloud computing enables an end-user to purchase computing

infrastructure as needed without a start-up investments. Since the CC often uploads private data to the cloud infrastructure and depends on it for computational capabilities, the following aspects are critical for the CC and, if not resolved sufficiently, may prevent him from moving to cloud based services.

1. The CC has to entrust his data to the CSP and therefore also DCO and thus effectively loses control over his data.
2. The CC has to trust that the DCO is able to provide the agreed cloud capacities. In particular, if the CC is a company, which has customers itself, these customers will hold the CC liable, if the agreed services are not provided, even if this is due to insufficiencies of the DCOs resource planning.
3. Especially if the CC is an end-user he may be overstrained with the extent of the contract between him and CSP and unable to comprehend or prove if the any license or service agreements are violated.
4. The DCO may operate data centers in different countries. Therefore, if data of a CC is exported to another country, different legal requirements and jurisdiction may become applicable.

- Legislators: Legislators have to take regulatory means to resolve conflicts between stakeholders and judicial uncertainties. A task of the legislator is to alleviate the threats to CCs [85], as this is the entity who depends on the other stakeholders and potentially discloses sensitive data to them. It is important that the legislator shapes the legal framework, such that CCs needs are respected but also that other stakeholders do not have incentive to leave a certain market. For example, if a national legislator shapes the legal framework to strictly, compared to neighbor countries, DCOs will build data centers only in neighbor countries and export customer data to these countries. Similarly, CSP will then only contract DCOs in these countries. To alleviate the pressure DCOs and CSPs can apply my threatening migration to other countries coordination between countries judicial bodies may be reasonable, as undertaken by the EU [33].

5.6.3 Regulation Areas Affected

From a regulative perspective, cloud federations are delicate for several reasons. In particular from aspects that are critical for CCs (cf. cloud customer definition) several regulative issues arise. These issues become even more complicated in case of cloud federations, as this moves in-house responsibilities away from one DCO to another and therefore raises further legal questions, as a third party is involved. More precisely, the CC has to entrust more then one DCO his data, more DCOs are responsible for the service provisioning, the contracts become more complex, and the likelihood that incorporated data centers are spread over several countries rises. Subsequently, two major areas that give rise to legalizes in cloud computing are discussed.

- **Entrustment of Data:** Data protection legislation is fundamental to Cloud Computing as the customer looses a degree of control over personal artifacts, when they are submitted to the CSP or DCO for storage and possible processing. In particular, this legislation has to address the following issues.
  - The infrastructure is shared between multiple customers, wherefore customers may gain unauthorized access to the data of other customers.
  - The cloud provider's servers or data centers are located in more than one jurisdiction.

  - Data is transferred between multiple locations based on the availability, wherefore the data can be eavesdropped while in transfer.

  EU Data Protective Directive is a directive adopted by European Union designed to protect the privacy and protection of processing, use, or exchange of personal data collected for or about citizens of the EU. Switzerland has partially implemented this directive and US has voluntary registration to the "Safe Harbor", so that private companies adhere to this directive.

  Therefore, privacy of data exchange and processing is a big issue. The responsible stakeholder, who must adhere to any regulation, for data protection the privacy must be clearly identified.

- **National vs. International Regulation:** When data of customers is stored abroad (relative to the customer) or services are offered to the customer from cloud providers abroad, the question arises, which law is applicable: the law of the DCO's, CSP's, or CC's country, or the law of the country where the data center is located (this may differ from the other three countries). In case of a federation, this case may get even more complicated, if the different DCO's are located in different countries and run data centers in other countries. For the EU no international judicial norm is present (though under development) wherefore most judicial issues have to be solved before hand in the contract, where it is often agreed on the judicial framework of one of the countries. Although for many offers CCs are not on an equal footing with DCOs and CSPs, CCs can choose the applicable law freely [102]. Although in the EU, data protection is determined by the country where data is processed, [33] ensures that the data is protected by the owner's domestic applicable law. If personal data is processed on behalf, the instructing party is responsible for choosing a processor that can provide appropriate security measures [33]. Such issues are in particular relevant for doctors, psychologists and insurance companies who work with highly sensitive data [22]. Since all cloud computing is data processing on behalf, the CSP is responsible for ensuring that the DCO takes according means. However, since this would imply that the CSP is fully aware about all processing techniques and location of data centers, the DCO would have to provide total transparence of his technical setup. Since this would imply an immense burden for the DCO, cloud computing's easy deployment and favorable price would be greatly degraded. Thus, the CSP is ensured usually by contract that the DCO meets the characteristics the CSP has to ensure. In particular with respect to data privacy this excludes certain countries as hosts for data processors for data of EU citizens. However, the EU approved for example Argentina, Switzerland, Canada as admissible hosts of such data processors. The trust in DCOs or CSPs can further be increased by certificates, such as [1], or the compliance with standards, such as [44].

- **Security and other issues:**

  Due to the technical organization of cloud computing, new security models are necessary. These may overcome at least partially issues with respect to the entrustment and international distribution of data. Due to the high relevance, impact, and complexity of security in cloud computing [77], which also relates to cross-border transfer of data, Security-as-a-Service, is nowadays offered in addition to the standard cloud business models (IaaS, SaaS, PaaS) [22]. Furthermore, security may also have to become a substantial part of SLAs [51] or be increased by submitting less sensitive data to the cloud [69]. As a CC can suffer considerable economical (when data is lost or damaged) or privacy impairment by deploying cloud infrastructures, [33] regulates compensation claims.

5.6.4 Status

The status work performed in this field can be divided into solved and unsolved issues as follows.

- **Solved issues:** According to the article 2 of European Directive a *data controller* is a neutral person or legal body, which determines means to process the data. While *data processor* is a neutral or legal body, which processes the data on behalf of the data controller. According to the European Directive, as data in the cloud crosses multiple borders, it falls in multiple jurisdiction. It is therefore, important to identify a) jurisdiction that is applicable, and b) a stakeholder that is responsible for compliance to the requirements imposed by regulations [26]. As the per case study done in [52], based on European Directive, it is the responsibility of the data processor to adhere to the compliance of regulations. Also, if the roles are clearly identified for data controller and data processor, the location of the data processor determines the applicable national law.

- **Unsolved issues:** For companies it is problematic to apply or identify laws at European scale, because member states implemented the European directive in different ways. Therefore, when the roles of data processor and data controller are not clearly identified, it is hard to find the applicable national law and responsible stakeholder.

  As identified by the European Commission in 2012, there is another key issue to be tackled in terms of “Problems with contracts were related to worries over data access and portability, change control and ownership of the data [96]. For example, there are concerns over how liability for service failures such as downtime or loss of data will be compensated, user rights in relation to system upgrades decided unilaterally by the provider, ownership of data created in cloud applications or how disputes will be resolved.” An expert group on model contract terms and conditions for cloud services for consumers and small firms and a working group with industry stakeholders on service level agreements for professional users were established in order to identify and disseminate best practices in respect of model contract terms for cloud services and to increase trust of prospective customers. Deliverables from this working group will be published by the end of 2014.

  Since large scale cloud computing is exclusively offered by American companies, it is questionable if these can forced to comply with European law. As noted in [22] companies like Amazon, Microsoft, Google may use their dominant market position to guide legislation in their interests and retreat from national markets if their interests are not met. It is further noted that this retreat would create room for local companies, which then would have to comply with the legislations to remain competitive.

  Another legal issue, that is still open, evolves around liability: If CCs conduct illegal activities from within a cloud, i.e., send spam or operate botnets, the CC should be held liable and not the DCO [2]. However, to appropriately phrase this into legislation is not straight forward, as a cross-disciplinary approach of legislators and technical experts is required.

6 Validation of Scenarios and Mechanisms

The current validation of work on scenarios within WP7 includes two approaches, since besides the technology especially economic, legal, and regulatory constraints determine the key facets. Thus, the first, WP7-internal validation includes approaches, which are based on well-known and accepted methodologies, which all WP7 FLAMINGO partners apply to each and every scenarios in scope of WP7. The second and external validation follows an interview-based methodology, based on a general template, which includes both generalized and specific questions. These questions allow for a discussion, evaluation, and validation of the scenario, while getting help from interview partners of external industrial and regulatory experts.

Both of these well-established validation approaches – internal and external – (a) provide an overview of possible limitations, (b) validate assumptions, either based on external partners' views or by the validation approach adapted for WP7 and being part of the internal validation, (c) validate the approach of the scenario and results of the same, and (d) validate the applicability in the real world.

Specifically, the validation method "Tussle Analysis" is considered as a value-added meta-method, since it was developed – based on its basic principles - to be applicable especially for Future Networks. This resulted in the completion and formal acceptance of the ITU-T Recommendation Y.3013 termed "Socio-economic Assessment of Future Networks by Tussle Analysis" [48] within FLAMINGO's Y2 work and in collaboration with the SmartenIT STREP [81], which was started a bit over two years ago within the CSA SESERV [34].

Although, the FLAMINGO Y2 focuses on validating WP7 scenarios from external experts, WP7 also had applied and developed approaches that are applied to relevant scenarios now and in future years of FLAMINGO. Therefore, the following subsections discuss two such approaches, which are to be applied in Y3 and Y4 of FLAMINGO and contains the respective discussion based on interviews conducted with external experts.

6.1 Socio-economic-aware Design of Future Networks by Tussle Analysis

Since the Internet enables the interaction of countless stakeholders of virtually all commercial, industrial, and private sectors, it is carrier for innumerable conflicting interests. Due to the constantly growing technological diversity of connected devices and the Internet's market penetration, these conflicts are settled by technological, economical, or judicial means that can hardly be foreseen during technology design time. Therefore, these colliding socio-economic interests make the Internet a rather unpredictable system, which was pointed out first by [13], which termed these conflicts tussle, the notion also adopted in this deliverable. Accordingly, [13] postulated the "Design for Tussle" of Internet technology, to preclude these conflicts or at least mitigate their effects for the Internet ecosystem. The rising relevance of socio-economic factors for the design of Future Network (FN) technology was also recognized by the ITU-T Recommendation Y.3001 [49] (to which members of FLAMINGO have contributed to) as a need for "social and economic awareness", which is one out of four objectives for FNs. In particular, in the framework of this objective, Recommendation Y.3001 identifies the design goal of economic incentives for FNs, which postulates that FNs are to be designed to provide a sustainable competition environment for solving tussles among the range of participants in the Information and Communication Technology (ICT) and telecommunication ecosystem. In the light of this objective of social and economic awareness and the related design goal of economic incentives, the recently released ITU-T Recommendation Y.3013, where FLAMINGO partners were the only contributors, suggests that the technically-driven FN design and standardization has to be complemented by a clear socio-economic assessment of

FN technology [48]. In particular, [48] proposes tussle analysis as a meta-method to assess, if a technology or a standard for FNs is designed in a socio-economic aware and incentive-compatible manner. This standardization effort is the first of its kind, since the need to investigate socio-economic factors in the design of FN technology is greatly overlooked in research and except [48] not even addressed in standardization (be it standards on how to address socio-economic factors or the consideration of socio-economic factors in standards). Therefore, this work here resulted in the ITU-T Recommendation Y.3013 as developed [48].

6.1.1 Tussle Analysis

The Tussle Analysis was developed in the framework of efforts to design the Future Internet [50] and is considered to be a meta-method, *i.e.,* it describes steps to be implemented by specific methods, to assess and improve a FN technology's or standard's compatibility with socio-economic interest conflicts, *i.e.,* tussles. In other words, the Tussle Analysis defines a systematic socio-economic assessment to be performed during technology design and/or standardization phases in order to anticipate the extent to which this technology is "designed for tussle" [13]. The Tussle Analysis is illustrated briefly in the Figure 22 and constituted mainly by the following three steps. Methods to implement the three steps can be found in [48].

1. Identification of all stakeholders, who are actively or passively affected by the technology.
2. Identification of all stakeholders' interests, conflicts between these interests (tussles), and all means available to them.
3. For each tussle:
   (a) Assessment of the impact to each stakeholder (short-term, mid-term, or long-term depending on the context).
   (b) Identification of ways for stakeholders to circumvent negative impacts (or gain unwarranted advantages), and consequences for the ecosystem, e.g., effects on other stakeholders. These may also include stakeholders, who have hitherto not been affected, i.e., who are not in the set of stakeholders compiled in step 1.
   (c) Iterative application of tussle analysis for each such manipulation technique, identified in step 3b.

In the ideal scenario the tussle outcome (constellation anticipated in step 3) is an equilibrium point, where the following two conditions hold:

1. All stakeholders identified in step 1 derive a payoff that is considered fair and have no means to increase their payoff, wherefore they will not take means to change the outcome, i.e., step 3c does not need to be applied and, thus, the tussle will not evolve further, and
2. No stakeholder of another technology, who was receiving a fair payoff before, gets an unfair payoff after this tussle equilibrium has been reached, i.e., step 3c does not need to be applied.

If both conditions hold the analysis of this particular tussle is completed and the focus should be shifted to remaining tussles as identified in step 2. In case, at least one of the conditions is not met, it has to be investigated, how technology specification, implementation, or standardization details can be changed, such that both conditions are met. If no such changes are possible, a new iteration of the methodology must be performed (step 3c) by making assumptions on the most

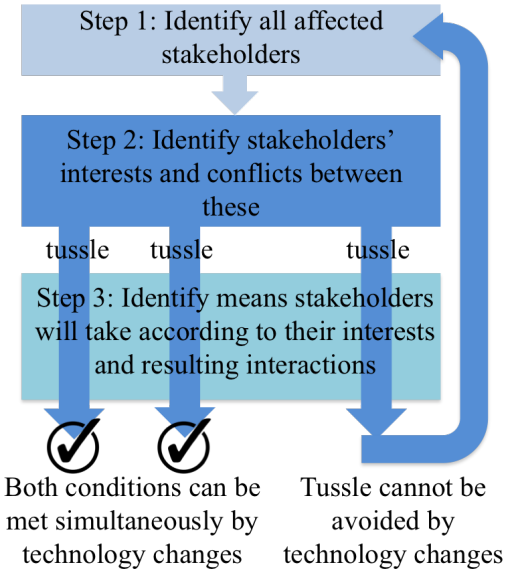

Figure 22: Illustration of Tussle Analysis

probable policies adopted by unhappy stakeholders, i.e., it has to be investigated, how the tussle will evolve. Since this subsequent iteration will again reach step 3, it will be investigated repeatedly, whether the evolved tussle can be stabilized by specification, implementation, or standardization changes. Theoretically, this allows for stabilizing a tussle after it evolved multiple times. However, due to imponderability and disturbance of the ecosystem it is always desirable to stabilize a tussle as early as possible. Thus ideally, a new technology should immediately lead to a stable outcome, i.e., both conditions are met without any tussle evolutions.

6.1.2 Example

The example of a tussle and its evolution here (i.e., an iterative interaction of stakeholders through technological, economical, or judicial means to influence a tussle outcome in their favor) clarifies the concept of tussles. The tussle presented here addresses TCP's (Transmission Control Protocol) bandwidth sharing algorithm and is illustrated by Figure 23. Circles correspond to (temporary) tussle outcomes. The vertical positioning of a circle denotes which of the stakeholders shown on the left favors the outcome. In particular, if the circle is vertically centered, all stakeholders consider their share appropriate/fair.

TCP's bandwidth sharing algorithm is considered fair, because when k TCP connections are instantaneously active in a bottleneck link, then each of them will receive $1/k$ of the bandwidth. Since each user of the bottleneck link desires to increase its share of the link, interests of users of a bottleneck link collide. Thus, with the introduction of the Peer-to-Peer (P2P) technology, TCP's bandwidth sharing algorithm lead to instabilities, since P2P users opened multiple TCP connections for the same file and, therefore, got disproportionate bandwidth share in relation to traditional users. While not fair, this outcome was not stable either, since the ability of an ISP to offer other services was threatened by the increase of P2P traffic. Therefore, ISPs responded by introducing middle boxes for inspecting data packets. These dedicated machines used advanced technology, such as Deep Packet Inspection (DPI) techniques, in order to identify and throttle P2P traffic. Even though this allowed for enforcing fair bandwidth sharing in links once more, it was not a stable outcome again: P2P applications started performing traffic obfuscation, e.g., by encryption, in order to decrease the download time. At the same time, DPI technology, which was installed to throttle

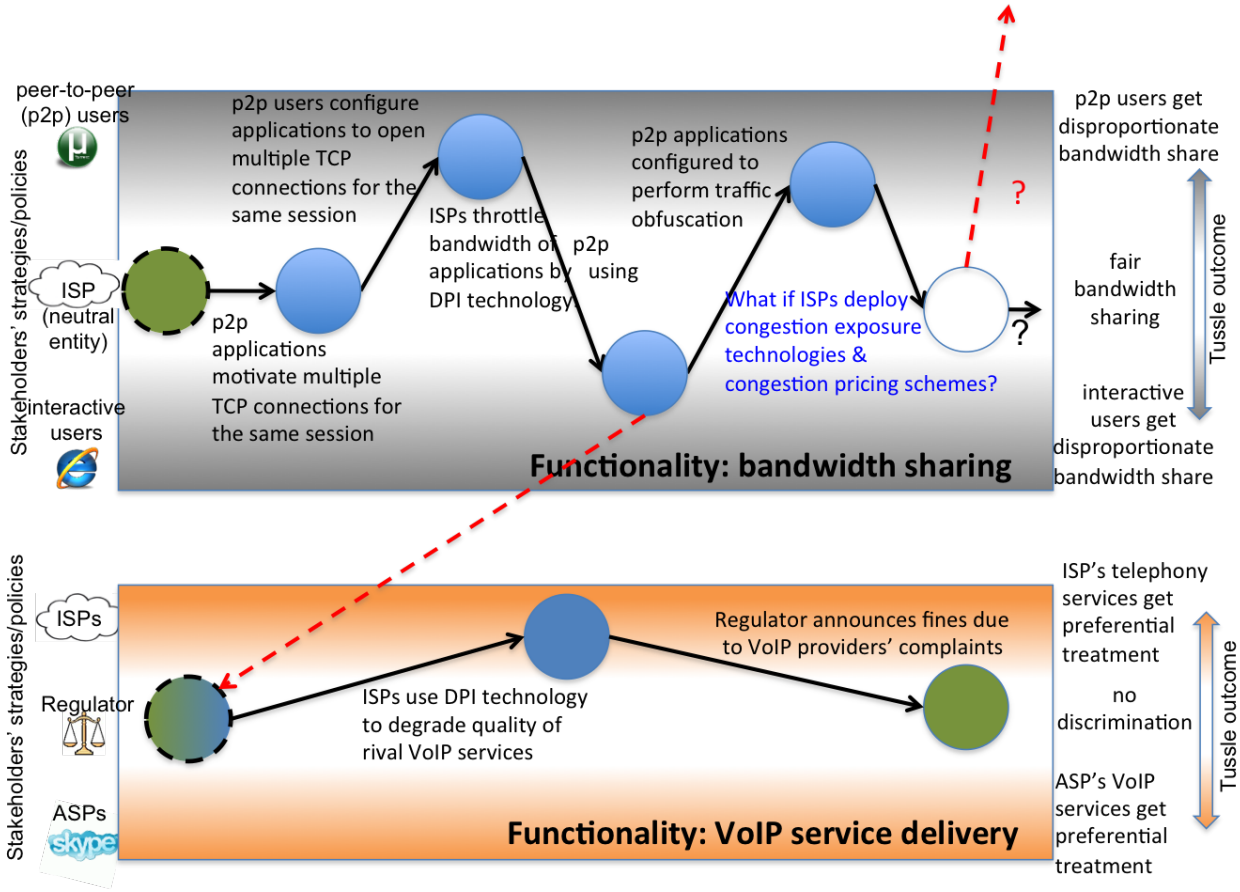

Figure 23: Example of a Tussle for Bandwidth Sharing [48]

P2P traffic, allowed ISPs to identify traffic that directly competes with complementary services they offer. A famous example has been an ISP's attempt to degrade the quality of third-party Voice-over-IP services offered by Application Service Providers (ASPs) that threatened traditional telephony services often offered by an affiliate of the ISP. This is an example of a spillover to another functionality, which was solved by affected users asking the regulator to intervene (judicial means) for discouraging anti-competitive tactics.

6.2 Validation by Value Networks and Business Models

Tussle analysis allows to assess, if a technology or a standard is designed in a socio-economic aware and incentive compatible manner. Value network analysis allows to investigate and visualize how a technology or a standard will change the economic landscape after the introduction of a new technology. Business model analysis focuses on a single actor and allows to investigate how the different blocks of the business model canvas will react on the introduction of a new technology or standard.

6.2.1 A Value Network

How a value is exchanged between involved business actors is indicated by a value network. First, the main roles (responsibilities) taken up in the market are indicated. These roles are then mapped to actors (market players) that really take up the indicated responsibility (by grouping one of more

roles in a single actor). Furthermore, value streams between roles or actors are identified. These streams can take different forms like monetary or non-monetary, tangible or intangible assets. Therefore, a value network gathers a broader multi-actor view on the market.

A sample model of value Network is shown in Figure 24. Those Value Networks developed for each of the scenarios concentrate on streams of legal implications, tussles, and incentives of the players.

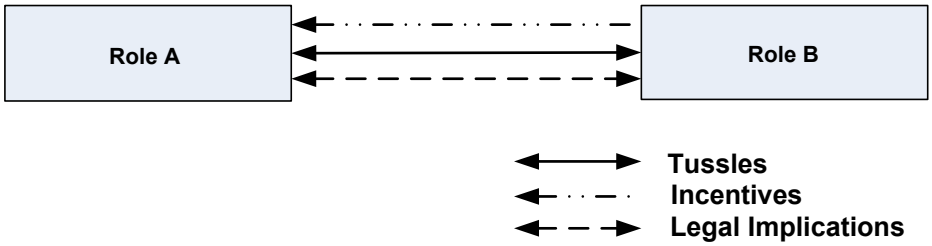

Figure 24: Template for Value Network

Example

The example of a value network and its evolution here (*i.e.,* how the market reacts on new technologies) clarifies the concept of evolutionary value network analysis and how it will be used to validate the scenarios in the future. The value network presented here addresses how the introduction of Software-Defined Networking (SDN) will influence the carrier-grade telecommunication network market and is illustrated by Figure 25. The rectangles contain the roles, the size of the rectangle indicates the market importance of the player and the arrows show the (in)direct value flows.

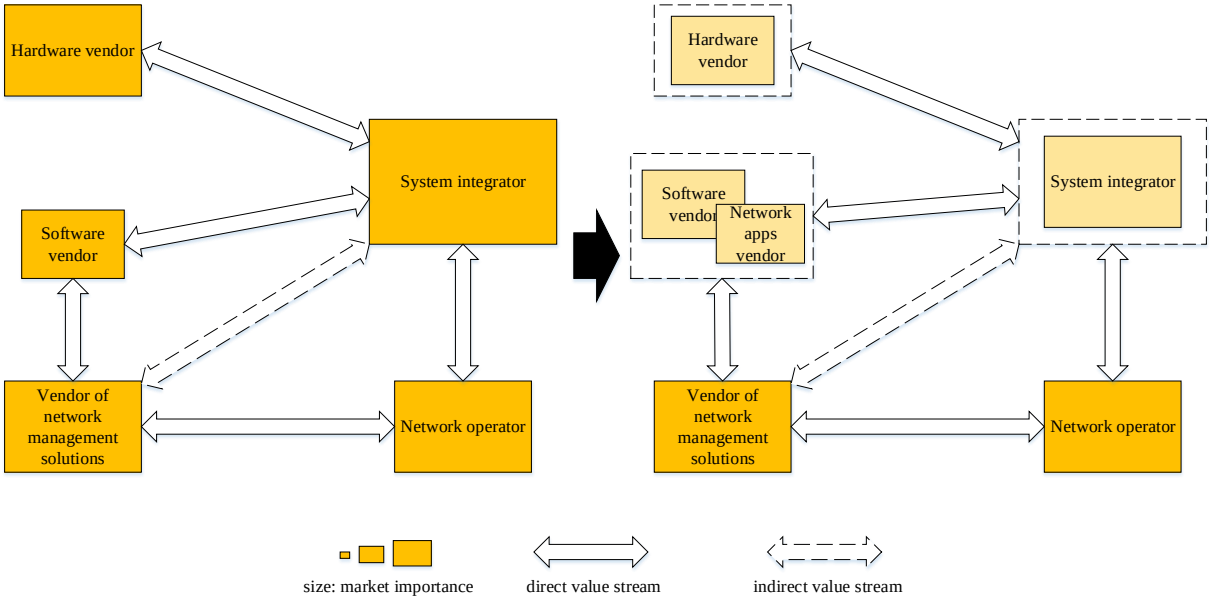

Figure 25: Example of evolutionary value network analysis

Today, system integrators have a dominant market presence. They obtain chips, aerials, line cards and other hardware from a hardware vendor who is specialized in their development and production. Software vendors develop proprietary software solutions, network stacks and handle the

adaption to different hardware platforms. They are linked to vendors of network management solutions who develop dedicated solutions. All these hardware and software components are assembled by system integrators in their own proprietary solutions. Network operators focus on the operation of various networks, e.g. telecommunication networks and purchase network solutions from the system integrators.

SDN impacts the ecosystem for a carrier-grade network set-up in several ways. On the one hand, more standardized interfaces and software solutions emerge. Software vendors take on new business, *e.g.,* operating systems for different hardware as well as OpenFlow-controllers. The software market splits up and a separate market for network applications arises “Network application vendor”). On the other hand, hardware vendors and system integrators lose ground as network operators can assembly their own solutions directly with commodity hardware and network applications.

6.2.2 A Business Model

The way value (monetary and non-monetary benefits) is being generated in the market is indicated by Business Model (BM). BM describes what is actually being offered (value proposition), how this is implemented (used resources, both equipment and activities), to whom it is offered (customers), and what is the financial situation (costs versus expected revenues). A BM, therefore, looks from the perspective of a single actor putting some offer in the market.

BMs for all FLAMINGO scenarios are created based on the Osterwalder’s Business Model Canvas as illustrated in Figure 26 [73]. It defines the framework for designing and presenting BMs. It helps to ask the relevant and right questions, but does not answer them. Thus, an overview of the scenario is developed and presented to ensure a comparable analysis afterwards (see D7.1).

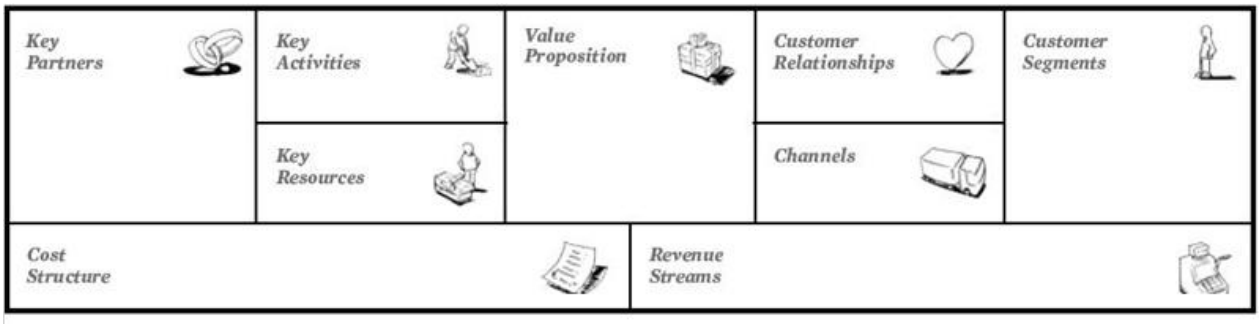

Figure 26: Business Model Canvas [73]

6.3 Interview-based Validation (Questionnaires)

Interview-based validation approach is a qualitative method that aims to have an in-depth analysis of the topic under consideration. As per the generality of interview-based approach, the scenarios within WP7 followed following sequence: (1) Identification of relevant questions in order to achieve the target (in this case validation of assumptions, approach, and results of scenarios), (2) conduct an interview, with relevant experts, and (3) analyze the collected information in terms of relevance, reliability, and validity.

In consequence, the application of an interview-based method on WP7 scenarios was based on a specifically developed questionnaire, which included general and scenario-specific questions. These questionnaires guided the interviews with external experts, in order to validate the work done within WP7 scenarios. In turn, the outcome defines a validation of those approaches, assumptions,

and partial/final results of those WP7 scenario. While this Section 6.3 here summarizes the major findings on a per interviewed scenario basis, the detailed outcome of each interview performed is documented within the appendix to D7.2 in Section 12.

6.3.1 Network Virtualization

The scenario of resource management in virtualised networks was discussed, with Telefonica, S.A., a Spanish broadband and telecommunications provider with operations in Europe, Asia, North America and South America. Operating globally, Telefonica is the sixth-largest mobile network provider in the world.

The validation was performed in a face-to-face meeting in Madrid, Spain, between Joan Serrat and Juan-Luis Gorricho from the Universitat Politecnica de Catalunya (UPC), and Javier Ramon and Alfonso Tierno from Telefonica (I+D).

The industry experts noted that Telefonica as a company was not specifically currently dealing with a virtualisation problem that requires dynamic resource allocation. In general, their resources are statically allocated to virtual network owners. They however observed that the problem considered in the scenario exposes a relevant problem, and that the assumptions made for the formulation were realistic, and led a complete approach or solution to the problem. They also proposed that as the problem of this scenario was very closely related to a similar problem - Network Function Virtualisation - which they are currently working on, there would be possibilities of collaborations between Flamingo and them in this regard in the near future.

6.3.2 ISP-oriented Content Delivery

The ISP-oriented content delivery scenario has been discussed, according to the questionnaire provided by WP7, with several industry contacts. This section will briefly introduce each of the industry contacts and summarize their feedback.

A one hour conference call was set up with two representatives from Belgacom. Belgacom is the Belgian incumbent ISP. With regard to relevance of the scenario, two different aspects were discussed: (1) improving quality-of-service and (2) monetary benefits. In case of the Belgian network the possibility to reduce delays (and as such to improve QoS) are very small due to the small distances that the Belgian network has to cover. For larger networks, *e.g.,* European scale, the reduction in delay can be considerably higher. In terms of monetary benefits, the main content producers (*i.e.,* Google, Netflix and Facebook) have already integrated or are in the process of integrating caches inside the network of Belgacom. Each of the content producers has their own proprietary system. As such an ISP operated cache would only be used for a small part of the total content.

Each of the main cost factors was also discussed during the interview. The cost of inter-domain traffic varies widely among the region (*e.g.,* cost Europe $<$ cost Africa $<$ cost Australia and New Zealand) and the type of link (IP transit- or submarine link). With regard to the upgrade of network infrastructure a number of factors were identified that influence the investment decision to upgrade the capacity. These include technical factors such as the chosen protection scheme, traffic forecasts and economic factors. Upgrading the network does not happen in one shot but in several phases across the network over several years. Link capacity is first increased by adding parallel links (*e.g.,* from 1 x 1GbE to 2 x 1GbE), before an upgrade is considered to a next level (*e.g.,* 5 x 1GbE to 10 x 1GbE). Our work will take these factors into account.

The considered scenario was also discussed with a second industry contact working at Sky, which is a major satellite broadcasting, broadband and telephone service provider in the United Kingdom.

The objective of this interview was to assess the relevance of the ISP-oriented content delivery solution for the service offered by the company.

Video on Demand (VoD) is a key service provided by Sky and as such, the company has strong interests in content. While a caching infrastructure has already been deployed in order to improve the service offered to their customers, their content traffic is currently mainly served by CDNs. According to the interviewee, there do exist business opportunities for such a scenario. However, the interviewee insisted on the fact that, in addition to technical challenges, the research questions to tackle should also take into consideration the existing business relationships between the different stakeholders. It was also highlighted that evaluating the investment cost required to support the proposed service was essential. According to the interviewee, comparing the cost of deploying a content service infrastructure to the cost of peering is not a simple issue and is not dominated by a single side of the argument. As such, it was recommended that, for future research efforts, experimentation with a set of real VoD request traces would be beneficial to evaluate the actual benefits in terms of resource utilization of the proposed solution.

From a more technical point of view, it was also suggested that contents should be categorized. They may have different characteristics, which may imply different requirements in terms of caching. For example, for content belonging to Sky's own library of media assets or for globally very popular content, deploying caches close to the subscriber is extremely useful. In contrast, off-network storage appears as more recommendable option for unpopular and infrequently requested contents.

The feedback from Belgacom and Sky showed that Internet Service Providers may have different interests in terms of content services, and as such, the relevance of the proposed scenario may not be similar for all providers. In the future, we will focus on large scale Internet Service Providers with strong interests in content, while taking into account the recommendations provided from the different industry contacts.

6.3.3 Mobile Measurements

The regulator in this scenario could not provide a clear statement concerning any legal conflicts since there is no legislation concerning the QoE field. The lack of legislation expected since QoE estimation do not examine which is the actual reason in case of underperforming services. The main focus of this work is to estimate the End-to-End (E2E) QoE in the domain of specific services and make available this information to end-users and MNOs. Thus, the main focus of this collaboration will be the end-user data protection and privacy, since this was the main concern of the regulator concerning measurements initiated by the end-user that become publicly available.

6.3.4 Legal and Ethical Facets of Data Sharing

The formalization of the scenario of Legal and Ethical Facets of Data Sharing has been discussed, according to the questionnaire provided by WP7, with the industry contact identified for this scenario, i.e., Roland van Rijswijk-Deij from SURFnet, the Dutch National Research and Education Network.

Since SURFnet is highly involved in this scenario, the picture that we can retrieve from the questionnaire is in line with the original expectations. In particular, van Rijswijk-Deij has highlighted the relevance of identifying com- prehensive policies for enabling ethical data sharing between data providers and data users. The clearly identified goal of achieving a workable policy before the end of 2014 will have impact on both legal and regulatory constraints, for the moment in the Dutch

context. can Rijswijk-Deij also highlighted the impor- tance of creating venues where researchers and operators will be able to further discussing the topic at hand, as for example a follow-up of the Dagstuhl seminar on Ethics in Data Sharing that has taken place in the early 2014.

6.3.5 Auction-based Charging User-centric System

An Auction-based Charging User-centric System (AbaCUS) [97] solution is a solution proposed to overcome the obstacle of the mobile termination service. AbaCUS defines an approach where the Calling Party Pays (CPP) principle is applied. In AbaCUS a call can be terminated by every Mobile Network Operator (MNO) who provides network coverage in a specific location and who is willing to terminate any mobile communication subscriber's call or data session, irrespective of the provider the callee belongs to. Since the modern mobile terminal devices are multiband-compatible, there does not exist any technological boundary for this functionality anymore. Furthermore, no SIM change is required from the callee so there is no SIM-lock interference with the AbaCUS call-termination MNO-independent system. Similarly to roaming users, whom can use the same device for domestic as well as abroad usage without replacing their SIM card, in AbaCUS the callee can receive a call by any MNO that provides network coverage in his location, without the need of additional equipment.

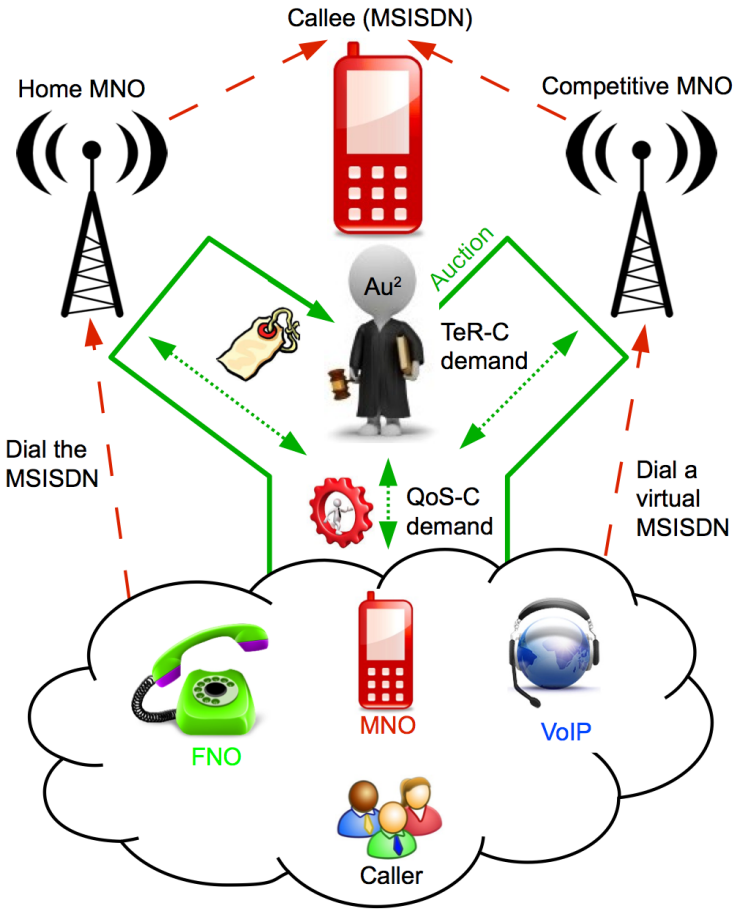

Figure 27: Key Elements of AbaCUS

Figure 27 illustrates the key elements of AbaCUS. A caller is flexible to use the voice-service provider of his choice, such as Voice over Internet Protocol (VoIP), MNOs, and Fixed Network

Operators (FNOs), to place a call. The caller can reach the callee by dialing directly his Mobile Station International Subscriber Directory Number (MSISDN). In this case the host MNO will collect the call-termination rate. However, a competitive MNO may generate a virtual MSISDN and allow to the callee to register temporarily in his network. Thus, the caller may dial the virtual MSISDN and reach the callee. In that case the guest MNO will profit from the termination rate. Multiple MNOs can participate in an auction, where the caller will request to place a call, reach a callee in a specific location, and demands a certain QoS-guarantee for the duration of this call. This demand is expressed by QoS Classes (QoS-Cs), which contain parameters related to the sound quality and the network-access waiting-time. MNOs bidding in the auction will reply to this request by proposing their charging demand. The charging demand is expressed by the Termination Rate Classes (TeR-Cs), which contain a potential start-up cost and the desired charging rate. Finally, on a referee role during the AbaCUS auction is the Auction Authority (Au2), which receives call requests from callers and from MNOs the selected TeR-C preference per QoS-C.

The regulator confirmed that to break a de facto market-defined monopoly, even if it is technically feasible, is hard unless the market players have an incentive to give up the monopoly. The reason is that a regulator would need a lot of time to enforce new policies that demand from the players more investments, either in terms of infrastructure or working-time. Furthermore, in AbaCUS case political action might be needed in special cases such as the Swiss market to enforce a new law. The latest complicates and slows down more a potential attempt to initiate of such process. However, AbaCUS shows a clear impact not only on social wealth fare increment but also on MNOs opportunity to monetize unused infrastructure. Thus, the flexible mobile termination service proposed by AbaCUS might lead to better services in the future and more reliable services from MNOs. For this purpose the main goal of AbaCUS approach will be to strengthen on benefits for MNOs to increase the chances of a voluntary adoption of such system with a minimum regulatory and legislative demand.

7 Summary, Conclusions, and Future Work

The work performed in project year Y2 within FLAMINGO's WP7 on "Economic, Legal, and Regulative Constraints" has lead to relevant observations, results, and conclusions, especially with respect to those WP7 scenarios, which show a close collaboration with WP5 and WP6.

The overall approach taken covers scenarios addressing both (1) a cross-disciplinary approach to technology and (2) economic, legal, and regulative aspects. A selected set of areas in terms of specified use cases have been discussed in terms of (a) a business policy-driven specifications, (b) a multi-actor analysis and cost modeling, and (c) an investigation of regulative boundaries and constraints for the field of network and service management. Thus, the major findings of this deliverable D7.2 are summarized as follows:

1. In order to test the feasibility of deployment and operation of respective network and service management scenarios, business indicators are identified (as a continuation of work performed in D7.1). Business Indicators properly defined for a given scenario constitute a suitable mechanism to determine policies that can optimize the network behavior. The most difficult step is to find mapping functions that relate business indicators and enforceable policies. Once done, optimization techniques can be used to determine optimum values for the parameter-dependent policies. This last step is also particularly difficult, because it is scenario-dependent and the solution has to be studied carefully. Enforceable policies are identified for each of these WP7 scenarios, which enable controlling the behavior and lifecycle of network and system elements. Also, mapping functions are identified to bridge the gap between business value and configuration management by considering the influence of BIs when generating enforceable policies.

2. The economic analysis of technology-driven research is often not receiving the attention it deserves. This can result in low interest from potential users and an end result that does not match their need(s). However, these results and application domains of research can often be hard to predict. To find a middle ground, Section 4.2 of this deliverable links business indicators chosen for each of the WP7 scenarios to economic consequences.

3. Economic consequences were researched using a multi-actor analysis and cost modeling. Several of these scenarios included research into the effects of pricing strategies and Service Level Agreements. Two existing scenarios were extended to include economic analysis (ISP-oriented cache management scenario and the Network Virtualization scenario). In Y3-Y4 of FLAMINGO the ISP-oriented cache management scenario will be used to research the cost-effect of adding caching infrastructure inside a network operator's infrastructure. Optimization of pricing strategies under uncertainty is the focus of the network virtualization scenario. Two other scenarios (the gathered measurement data from the mobile measurements scenario and the policy refinement process from the business-oriented service management scenario) have progressed and presented their first results. Each of these scenarios were ex-ante investigated using stakeholders' analysis and risk analysis.

4. The attempt of stakeholders (*e.g.,* service provider, operator, and network provider) to provide a better service to the end-user, or to improve the performance of the network are in some cases considerably restricted by regulators. Major reasons of such constraints are laws, polices, and mandates on the way data is treated. There are various regulative considerations in terms of data retention, storage, and cross-border data flow, and sharing of data.

5. Three approaches to validate WP7 scenarios were identified. The approach of a Socio-economic-aware Design of Future Networks by Tussle Analysis resulted in the ITU-T Recommendation Y.3013. The second approach validates the economic impact of WP7 scenarios

by applying value networks and business models. The third approach applies an interview-based method for validating the scenarios' approach, their assumptions, and related results with the help of external industrial experts.

7.1 Conclusions

The conclusions drawn after the second project year identifies three major observation: First, in order to monitor, manage, and operate the Future Internet, Business Indicators, policies, and mapping functions serve as a key step to ensure a possible success. Secondly, a clear inter-dependency between business goals and the economic impact has been shown. Therefore, bridging the gap between these two aspects does form the basis for a successful introduction and operation of any technology in practice. Thirdly, the combination of all relevant areas in an integrated manner, especially technical, economic, legal, and regulative perspectives, lead to a better positioning and understanding of services and functions in the communications market.

In general, this work lead to the identification of inter-dependencies in these aspects for the Future Internet and related network and service management tasks. While the analysis is based on investigations performed for scenarios of various network and service monitoring approaches, virtualization methods, and automated configuration and repair of managed resources, FLAMINGO's Y2 end also marks the completion of Task T7.2 with the full identification of business indicators, policies, and their mapping functions for all relevant scenarios.

In turn, this work of WP7 and its related documentation within this deliverable D7.2 act as a basis for certain network and service management decisions, multi-actor and cost modeling analysis, country-specific, partially region-specific regulative settings and frameworks, and business policy-driven mechanisms.

7.2 Future Work

All of these findings in D7.2 will be refined in the FLAMINGO Network of Excellence in years 3 and 4 to come, mainly due to the very close combination of technology, networking, and economic expertise with and applied legal and regulative know-how. This will continue in line with T7.1 and T3.1 descriptions.

Thus, FLAMINGO's WP7 will address an analysis of scenarios with respect to techno-economic inter-dependencies and legal and regulative constraints. From the economic perspective existing scenarios will be validated using the value network analysis and Osterwalder's business model canvas. While the value network analysis will be used to visualize the impact of each of the scenarios on the interaction between actors, the business model canvas will be used to quantify the economic impact of a scenario for a single actor.

Also, an analysis will be performed in terms of cost and price modeling for selected scenarios. From the legal and regulative view point,the key aim of the coming two years of FLAMINGO will be to prepare and partially establish guidelines of legal and regulative constraints in a cross-disciplinary methodology applicable to the network and service management area.

8 WP7 Objectives

FLAMINGO's WP7 objectives are determined by the key areas of networking systems in which relevant stakeholders interact in a cross-disciplinary manner. The focus of WP7 is on the challenges of economic, legal, and regulative constraints of selected network and service management technology, mechanisms, and solutions. Core objectives concentrate on the integration of those dimensions, the respective dissemination of results, and joint Ph.D. works. Therefore, the objectives are summarized, as defined in the Description of Work (DoW), in the following sections.

8.1 WP7 Objectives

WP7 objectives focus on achieving cross-disciplinary methodologies so that technological dependency on economical, legal, and regulative aspects can be studied. The progress in this scope of these objectives is summarized in Table 24. This section provides a high-level summary of the WP7-specific objectives. These objectives have been grouped into two categories: Section 8.1.1 describes the status of the objectives in which WP7 researchers are currently active. We refer to these as *ongoing and completed-objectives*. Section 8.1.2 includes the objectives for which so far no progress has been made. Activities related to these objectives will be part of Y3-Y4 of FLAMINGO. These are termed as *open objectives*.

8.1.1 Ongoing and Completed Objectives

Objective 1: To integrate European network and service management research regarding Economic, Legal and Regulative constraints – WP7 works with a close collaboration with work packages WP6 and WP7 that deal with various research activities regarding network and service monitoring, and automated configuration and repair of Future Internet. In Y1, 9 scenarios were identified, which were analyzed within WP7. In Y2, based on scope, relevance, and in order to deepen then analysis from economic, legal, and regulative view point, 6 scenarios are identified and studied within WP7. On one hand business and economic side includes the identification of business policies, service-level agreements, pricing, and cost modeling. On the other hand, the regulative side includes the study of various constraints in data sharing, storage, retention, and cross-border flow.

Objective 2: To create and maintain articles within Wikipedia and other online systems in this area – The research conducted in Y1 and Y2 has allowed us to generate valuable knowledge that can be used for contributing to Wikipedia. In collaboration with WP2, WP5, and WP6, WP7 has identified a set of Wikipedia articles where a contribution would be beneficial. For more information on this topic, we refer the reader to D2.2.

Objective 3: To address in an integrated manner operations, management, and maintenance with respect to economics, legal, and regulative constraints coherently – In order to facilitate operations and management of various technologies of Future Internet, three aspects have been studied in Y2. These are the a) identification of business indicators and policies, and their mapping functions, b) economic interdependencies of the business indicators and goals, and c) regulative frameworks, which decide the boundaries and constraints for the operations of these technologies. The methodologies for operations, management, and maintenance of technologies within network and service management are completely identified with the end of Y2. Thus, marking the end of Task T7.2. For details, please refer to Section 4.

Objective 4: To apply cross-disciplinary methods and approaches on technology as well as economic, legal, and regulative dimensions – In Y1, WP7 has proposed a joint management architecture that provides a consistent view of the methods and approaches followed by WP7 in studying economic, legal, and regulative dimensions for network and service monitoring and on configuration and repair. In Y2, this architecture was followed and business indicators for monitoring the business objectives were identified. Also, economic dependencies, were identified. Y2 also includes identification of regulative constraints for these methods. Therefore, this objective is marked as completed with end of Y2. For details, please refer to Section 4.

Objective 5: To define a model, architecture, and mechanisms for three stakeholders in an integrated manner: especially covering the operator, the application provider, and the end-user – In Y1, various stakeholders for all the relevant scenarios have been identified. these stakeholders, were also studied with respective to value networks and business models. While the value networks, identified relations amongst stakeholders in terms of incentives, tussles, and their legal and regulative obligations, the business model described goals, cost and revenue modeling of these identified stakeholders. In Y2 these value models and business models have been identified as one of the validation approach, and will be applied in depth in future years of FLAMINGO. Therefore, this objective is marked as completed with end of Y2. For more information please refer to Section 6.2.

Objective 6: To support an integration of the following five factors: (a) cost-awareness, (b) incentives for service provisioning, (c) fulfillment schemes, (d) business policies, and (e) legal/regulative frameworks – Y2 includes analysis with respect to multi-actor analysis, service level agreement, pricing and cost modeling for relevant scenarios. Also, various regulative frameworks have been studied with country-specific, partially region-specific settings. Business policies are also completely identified for all relevant scenarios, as shown in Section 4.1, hence marking the completion of Task T7.2. Please refer to Section 4.2 and Section 5 for details.

Objective 8: To evaluate mechanisms under scenarios determined and derive guidelines for stakeholder defined – Y2 includes identification of validation approaches, in order to evaluate the approach, assumptions and results of the scenarios. This year also includes, validation of scenarios with the help of external industrial partners. This validation approach was in form of interviews conducted for each scenario with an external partner. More information about this is available at Section 6.

8.1.2 Open Objectives

Objective 7: To investigate related operational costs for service offerings by Internet Service Providers (ISP) and telecommunication system providers – Even though the cost modeling for various scenarios is part of work done in Y2 of FLAMINGO, operational cost from the perspective of ISPs and telecommunication system providers will be part of research that will be done in Y3-Y4 of FLAMINGO.

Table 24: WP7 Objectives

No.	Objective	Status as of Y2	Description	Section/Deliverable	To be Addressed in Y3-Y4
1.	Integrating network and service management research regarding economic, legal, and regulative constraints	IN PROGRESS	Analyzing various scenarios in these dimensions. Economic analysis focuses on multi-actor analysis, service level agreements, pricing and cost modeling.	Section 4.2	To be refined and studied in further depth
2.	Maintaining Online Informative Systems	IN PROGRESS	Details of content and topics included in D2.2	D2.2	To maintain articles online *e.g.,* Wikipedia, once terminology in this cross-disciplinary area has settled.
3.	Integrating operations with economic, legal and regulative constraints	IN PROGRESS	Identifying Business Indicators for scenarios to monitor the operations as per business objectives. The business indicators are integrated in the economic goals of several scenarios. Also regulative constraints are being studied	Section 4	To be refined and studied in depth.
4.	Methods and approaches for economic-legal analysis	DONE	Joint architecture defined	D7.1	Can be adapted, if required.
5.	Models, architecture for stakeholders (operator, application provider, end-user)	DONE	Refined and studied in value networks	D7.1	Inter-relations between stakeholders studied as part of Value Networks in D7.1. Future year will see this work as part of validation mechanism.
6.	Integration of cost, incentive, business policies and legal/regulative frameworks	IN PROGRESS	Refined and studied in constraint analysis and BIs identification. Business policies and business indicators are integrated in economic goals of several scenarios. Also, regulative constraints for various fields of network and service management have been studied.	Section 4.2, Section 5	To be adapted with progressing work.
7.	Operational costs for Internet Service Provider and telecommunication system providers	FUTURE	To be defined in Y3-Y4	-	Cost models to be investigated for stakeholders.
8.	Evaluate mechanisms under scenarios determined and derive guidelines for stakeholder defined.	IN PROGRESS	Validation work of all scenarios has been done with external partners	Section 6	To determine guidelines, keeping economic, legal and regulative constraints in consideration.

8.2 Project (S.M.A.R.T) Objectives

Progress on two Specific, Measurable, Achievable, Relevant, Timely (S.M.A.R.T) Objectives, which WP7 focuses on, are defined in the DoW and their respective achievement degrees after second project year in total reads as follows:

1. **Writing of joint scientific papers:** The Description of Work (Section B.1.1.5) states that "after 18 month at least 20 scientific papers will be submitted / published". In Y1, the project had fulfilled and exceeded the expected number of publications. In Y2, the research work packages have published 50 papers, both at major conferences and in journals. In addition, several other papers are currently under review. The complete list of published papers, is listed in D8.2.

   In addition FLAMINGO has participated in writing internet-drafts and RFCs, and contributed in standardization forums like ITU-T, IETF. The complete list of such participation in listed in D4.2.

2. **Integration of Ph.D. students:** The Description of Work (Section B.1.1.5) states that "after 9 months each research WP will have identified at least two fully integrated Ph.D. students, which means that these students will be jointly supervised and financially paid by FLAMINGO". For the FLAMINGO project, PhD students are encouraged to work in collaboration with partner institutions, which is at basis of research. For this reason, there is not a one-to-one match between a Ph.D. student and a single WP. In addition, it is important to mention that Ph.D. collaborations are taking place not only among fully integrated Ph.D. students, but also with students that are not financially paid by FLAMINGO but that are actively contributing to the WP work. These students, their affiliation and the co-supervising institution are listed in D8.2.

9 Abbreviations

Au^2	Auction Authority
$AbaCUS$	Auction-based Charging User-centric System
AC	Admission Control
$AccDelay$	Access Delay
$AMTA$	Australian Mobile Telecommunications Association
ANN	Artificial Neural Network
BI	Business Indicator
BM	Business Model
BW	BandWidth
CDR	Charging Data Records
$CJEU$	Court of Justice of the European Union
CPU	Central Processing Unit
CC	Cloud Customer
CDN	Content Distribution Network
CPP	Calling Party Pays
CSP	Cloud Service Provider
$D7.1$	Deliverable 7.1
DCO	Data Center Operator
$DiffServ$	Differentiated Services
DPI	Deep Packet Inspection
DRA	Dynamic Resource Allocation
DRM	Dynamic Resource Management
DQX	Deterministic Quality-of-Experience
$E2E$	End-to-End
EA	Evolutionary Algorithms
EEC	European Economic Community
EU	End-Users
FCC	Federal Communications Commission
FNo	Fixed Network Operator
FP	Flamingo Partners
GbE	Gigabit Ethernet
$HTTP$	HyperText Transfer Protocol
InP	Infrastructure Provider
IP	Internet Protocol
ISP	Internet Service Provider
$ITU-T$	International Telecommunication Union–Telecommunication Standardization Sector
JUB	Jacobs University Bremen
LE	Legislator
$lossSvcDgd$	Losses due to performance degradation
$lossInvRjct$	Losses due to service invocation rejections
$M2$	Mobile Measurememnts
MAS	Multi Agent Systems
MCF	Multi Commodity Flow
MOO	Multi-Objective Optimization
MNO	Mobile Network Operator
MOS	Mean Opinion Score

$MPLS$	Multi-Protocol Label Switching
NDA	Non Disclosure Agreement
NFS	Neuro-Fuzzy System
NN	Neural Network
NO	Network Operator
NSA	National Security Agency
NVE	Network Virtualisation Environment
PLR	Packet Loss Rate
QoE	Quality-of-Experience
QoS	Quality-of-Service
$QoS-C$	Quality-of-Service Class
REG	Regulator
RAB	Resource Availability Buffer
REG	Regulator
RL	Reinforcement Learning
RTP	Real-time Transport Protocol
$RTSP$	Real Time Streaming Protocol
$satisfSvc$	Service satisfaction
SDN	Software-Defined Networking
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specifications
$SLS-I$	SLS-Invocation
$SLS-S$	SLS-Subscription
SMO	Service Management Objective
SN	Substrate Network
SP	Service Provider
SR	Service Rate
$TAMAAL$	Tune-Adaptive Metamodel Assisted ALgorithm
TCL	Target Critical Levels
$QoS-C$	Quality-of-Service Class
$TeR-C$	Termination Rate Class
TT	Traffic Trunk
$UniBwM$	Universität der Bundeswehr München
UCL	University College London
UPC	University Politecnicà de Catalunia
UT	University of Twente
UZH	University of Zürich
VCG	Vickrey-Clarke-Groves
VN	Virtual Network
VNO	Virtual Network Operator
VNP	Virtual Network Provider
VNE	Virtual Network Embedding
$VoIP$	Voice over Internet Protocol

10 References

[1] American Institute of Certified Public Accountants (AICPA). Statement on Auditing Standards No. 70: Service Organizations. Auditing Standards Board, http://sas70.com/, Accessed in August, 2014.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. *Commun. ACM*, 53(4):50–58, Apr. 2010.

[3] D. Bergemann and J. Välimäki. The Dynamic Pivot Mechanism. *Econometrica*, 78(2):771–789, 2010.

[4] Boundary Map Definition. http://www.mymanagementguide.com/, Accessed in September, 2014.

[5] Bundesminister für Justiz Österreich, Zur Zahl 1292/J-NR/2014. http://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_01179/imfname_353625.pdf. Accessed in September, 2014.

[6] R. Cavallo, D. C. Parkes, and S. Singh. Optimal Coordinated Planning Amongst Self-interested Agents with Private State. *In Proceedings of the 22nd Annual Conference on Uncertainty in Artificial Intelligence UAI'06*, pages 1–8, 2006.

[7] R. Cavallo, D. C. Parkes, and S. Singh. Efficient Mechanisms with Dynamic Populations and Dynamic Types. *Harvard University, Division of Engineering and Applied Physics*, 2009.

[8] D. Chafekar, L. Shi, K. Rasheed, and J. Xuan. Multiobjective GA Optimization using Reduced Models. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 35(2):261–265, 2005.

[9] D. Chafekar, L. Shi, K. Rasheed, and J. Xuan. On the Use of Surrogated Models in Multiobjective Evolutionary Algorithms. *Master thesis, Center for Research and Advanced Studies of the National Polytechnical Polytechnic Institute*, 2011.

[10] N. M. K. Chowdhury and R. Boutaba. A Survey of Network Virtualization. *Computer Networks*, 54(5):862–876, Apr. 2010.

[11] M. Claeys, D. Tuncer, J. Famaey, M. Charalambides, S. Latre, F. De Turck, and G. Pavlou. Towards Multi-tenant Cache Management for ISP Networks. In *2014 European Conference on Networks and Communications (EuCNC)*, pages 1–5, June 2014.

[12] M. Claeys, D. Tuncer, J. Famaey, M. Charalambides, S. Latre, G. Pavlou, and F. De Turck. Proactive Multi-tenant Cache Management for Virtualized ISP Networks. In *10th International Conference on Network and Service Management (CNSM), 2014*, 2014.

[13] D. Clark, J. Wroclawski, K. Sollins, and R. Braden. Tussle in Cyberspace: Defining Tomorrow's Internet. *IEEE/ACM Transactions on Networking*, 13(3):462–475, June 2005.

[14] E. H. Clarke. Multipart Pricing of Public Goods. *Public choice*, 11(1):17–33, 1971.

[15] U. Clauss. So Wuerde Europas "Schengen-Internet" Funktionieren. http://tinyurl.com/noktusx, Accessed August 15, 2014.

[16] C. A. C. Coello, D. A. Van Veldhuizen, and G. B. Lamont. *Evolutionary Algorithms for Solving Multi-objective Problems*, volume 242 of *Genetics and Evolutionary Computation*. Springer, 1st edition, 2002.

[17] J. E. Cohen, S. Dietrich, A. Pras, L. D. Zuck, and H. Mireille. Ethics in Data Sharing (Dagstuhl Seminar 14052). *Dagstuhl Reports*, 4(1):170–183, 2014.

[18] P. Cramton. Spectrum auctions. In *Handbook of Telecommunications Economics*, chapter 14, pages 605–639. Elsevier Science, 2002.

[19] P. Cramton, Y. Shoham, and R. Steinberg. *Combinatorial auctions*. MIT Press, 2006.

[20] R. Das, J. E. Hanson, J. O. Kephart, and G. Tesauro. Agent-Human Interactions in the Continuous Double Auction. *In Proceedings of the 17th International Joint Conference on Artificial Intelligence*, 2:1169–1176, 2001.

[21] K. Deb. *Multi-objective Optimization Using Evolutionary Algorithms*, volume 16. John Wiley & Sons, 2001.

[22] A. Deobald, M. Oehme, P. Staudenrauß, P. Schaffrath, and A. Fischbach. *Seminar IT-Sicherheit - Sicherheit und Vertrauen in Cloud Computing*. Universität der Bundeswehr München - Fakultät für Informatik, April 2011.

[23] Die Bundesversammlung der Schweizerischen Eidgenossenschaft: "Entwurf: Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)". 2014.

[24] Die Bundesversammlung der Schweizerischen Eidgenossenschaft: "Fernmeldegesetz (FMG) 784.10". April 30, 1997 (Status as of July 1, 2010).

[25] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), March 2002.

[26] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, October 1995.

[27] Electronic Frontier Foundation, Mandatory Data Retention. `https://www.eff.org/issues/mandatory-data-retention`. Accessed in September 2014.

[28] M. T. Emmerich, K. C. Giannakoglou, and B. Naujoks. Single-and Multiobjective Evolutionary Optimization Assisted by Gaussian Random Field Metamodels. *IEEE Transactions on Evolutionary Computation*, 10(4):421–439, 2006.

[29] B. Etling, R. Faris, and J. Palfrey. Policital Change in the Digital Age: The Fragility of Online Organizing, Summer-Fall 2010.

[30] EUR-Lex. Treaty of Amsterdam amending the Treaty of the European Union, the Treaties establishing the European Communities and certain related acts. `http://europa.eu/legislation_summaries/institutional_affairs/treaties/amsterdam_treaty/index_en.htm`, Accessed in May, 2014.

[31] European Comission. Schengen area. `http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/index_en.htm`, Accessed in May, 2014.

[32] European Court of Human Rights, European Convention on Human Rights. `http://www.echr.coe.int/Documents/Convention_ENG.pdf`. Accessed in September 2014.

[33] European Union. EU-Datenschutzrichtlinie (EU-DSRL). Amtsblatt, November 1995.

[34] First Report on Economic Future Internet Coordination Activities; SESERV Deliverable D2.1. M. Waldburger and P. Poullie (Eds.), September 2011. http://www.scribd.com/doc/65070802/D2-1-First-Report-on-Economic-Future-Internet-Coordination-Activities.

[35] A. Fischer, J. Botero, M. Till Beck, H. de Meer, and X. Hesselbach. Virtual Network Embedding: A Survey. *IEE, Communications Surveys Tutorials*, 15(4):1888–1906, Fourth 2013.

[36] J. Fritsche. Alle Daten sind gleich. News and Trends, EU-Report. `http://www.eu-info.tradepress.eu/2014/06/30/netzneutralitaet-alle-daten-sind-gleich/`, Accessed in October, 2014.

[37] A. Gibbard. Manipulation of Voting Schemes: A General Result. *Econometrica: journal of the Econometric Society*, pages 587–601, 1973.

[38] F. Greis. Experten fordern Verschlüsselung und Schengen-Routing, Juni 2014.

[39] T. Groves. Incentives in Teams. *Econometrica: Journal of the Econometric Society*, pages 617–631, 1973.

[40] Heise.de, Justizminister: Kein Nationaler Alleingang zur Vorratsdatenspeicherung. `http://tinyurl.com/heise-de-justizminister`. Accessed in September 2014.

[41] Heise.de, Österreich: 354 Anfragen Nach Vorratsdaten, Keine Wegen Terrorismus. `http://tinyurl.com/heise-de-oesterreich`. Accessed in September 2014.

[42] W. K. Hon and C. Millard. Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4. *Script-ed*, 9(25):29–63, 2012.

[43] W. K. Hon, C. Millard, and I. Walden. Who is Responsible for Personal Data in Cloud Computing? – The Cloud of Unknowing, Part 2. *International Data Privacy Law*, 2(1):3–18, 2012.

[44] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27001. Standard, October 2005.

[45] International Telecommunications Union. *Mean Opinion Score (MOS) Terminology (ITU-T Recommendation P.800.1)*. November, 2006.

[46] International Telecommunications Union. *Methods for Subjective Determination of Transmission Quality (ITU-T Recommendation P.800)*. June, 1998.

[47] International Telecommunications Union. *Subjective Evaluation of Conversational Quality (ITU-T Recommendation P.805)*. October, 2007.

[48] International Telecommunications Union. *Socio-economic Assessment of Future Networks by Tussle Analysis (ITU-T Recommendation Y.3013, M. Waldburger, P. Poullie, C. Schmitt, and B. Stiller (Eds.))*, August, 2014.

[49] International Telecommunications Union. *Future Networks: Objectives and Design Goals (ITU-T Recommendation Y.3001)*, September, 2012.

[50] C. Kalogiros, C. Courcoubetis, G. Stamoulis, M. Boniface, E. Meyer, M. Waldburger, D. Field, and B. Stiller. An Approach to Investigating Socio-economic Tussles Arising from Building the Future Internet. In J. Domingue, A. Galis, A. Gavras, T. Zahariadis, D. Lambert, F. Cleary, P. Daras, S. Krco, H. Müller, M.-S. Li, H. Schaffers, V. Lotz, F. Alvarez, B. Stiller,

S. Karnouskos, S. Avessta, and M. Nilsson, editors, *The Future Internet*, volume 6656 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2011.

[51] B. R. Kandukuri, P. V. Ramakrishna, and A. Rakshit. Cloud security issues. In *Proceedings of the 6th IEEE International Conference on Services Computing*, SCC '09, pages 517–520, Washington, DC, USA, 2009. IEEE Computer Society.

[52] A. Kertesz and S. Varadi. Legal Aspects of Data Protection in Cloud Federations. *Security, Privacy and Trust in Cloud Systems, Springer*, pages 433–455, 2015.

[53] T. Kiessling and Y. Blondeel. The {EU} regulatory framework in telecommunications: A critical analysis. *Telecommunications Policy*, 22(7):571 – 592, 1998.

[54] J. P. Kleinhaus. Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets. `http://tinyurl.com/netzpolitik-schengen-routing`, Accessed in May, 2014.

[55] J. Knowles. ParEGO: A Hybrid Algorithm with On-line Landscape Approximation for Expensive Multiobjective Optimization Problems. *Evolutionary Computation, IEEE Transactions on*, 10(1):50–66, 2006.

[56] J. Kraemer, L. Wiewiorra, and C. Weinhardt. Net Neutrality: A Progress Report. Technical Report 37(9):794–813, Telecommunications Policy, October 2013.

[57] C. Kuner. Regulation of Transborder Data Flows under Data Protection and Privacy Laws; Past, Present and Future, 2011.

[58] T. Kurze, M. Klems, D. Bermbach, A. Lenk, S. Tai, and M. Kunze. Cloud Federation. In *Proceedings of The 2nd International Conference on Cloud Computing, GRIDs, and Virtualization* , pages 32–38, 2011.

[59] T. B. Lee. Comcasts Deal with Netflix Makes Network Neutrality Obsolete. `http://tinyurl.com/comcast-network-neutrailty`. Accessed in September 2014.

[60] G. Machado, T. Bocek, M. Ammann, and B. Stiller. A Cloud Storage Overlay to Aggregate Heterogeneous Cloud Services. In *IEEE 38th Conference on Local Computer Networks (LCN)*, pages 597–605, October 2013.

[61] G. S. Machado, F. V. Hecht, M. Waldburger, and B. Stiller. *Bypassing Cloud Providers' Data Validation to Store Arbitrary Data*. IFIP/IEEE, May 2013.

[62] R. P. McAfee and J. McMillan. Auctions and bidding. *Journal of economic literature*, 25(2):699–738, 1987.

[63] J. Meltzer. The Internet, Cross-Border Data Flows and International Trade, February 2013.

[64] R. Mijumbi, J. Gorricho, J. Serrat, M. Claeys, F. De Turck, and S. Latr´e. Design and Evaluation of Learning Algorithms for Dynamic Resource Management in Virtual Networks. In *Proceedings of the 14th IEEE/IFIP Network Operations and Management Symposium (NOMS), NOMS2014.*, NOMS2014. IEEE Press, 2014.

[65] R. Mijumbi, J.-L. Gorricho, J. Serrat, M. Claeys, F. De Turck, and J. Famaey. Neural Network-based Autonomous Allocation of Resources in Virtual Networks. In *Proceedings of the European Conference on Networks and Communications (EuCNC)*, EuCNC2014. IEEE, June 2014.

[66] R. Mijumbi, J. L. Gorricho, J. Serrat, K. Xu, M. Shen, and K. Yang. A Neuro-Fuzzy Approach to Self-Management of Virtual Network Resources. *Journal of Expert Systems With Applications*, Sept 2014.

[67] C. Millard, A. Cunningham, and K. Hon. UK Parliament, Justice Committee: Written evidence from Christopher Millard, Alan Cunningham and Kuan Hon, Cloud Legal Project, 2012, Accessed in October, 2014. http://tinyurl.com/p48ap99.

[68] G. Montemayor-Garcia and G. Toscano-Pulido. A Study of Surrogate Models for their Use in Multiobjective Evolutionary Algorithms. In *8th International Conference on Electrical Engineering Computing Science and Automatic Control (CCE), 2011*, pages 1–6. IEEE, 2011.

[69] M. Mowbray and S. Pearson. A Client-based Privacy Manager for Cloud Computing. In *Proceedings of the 4th International ICST Conference on Communication System Software and Middleware*, COMSWARE '09, pages 5:1–8, New York, NY, USA, 2009. ACM.

[70] E. Mykoniati, C. Charalampous, P. Georgatsos, T. Damilatis, D. Goderis, P. Trimintzios, G. Pavlou, and D. Griffin. Admission Control for Providing QoS in DiffServ IP Networks: the TEQUILA Approach. *Communications Magazine, IEEE*, 41(1):38–44, 2003.

[71] G. Nagesh. Court Tosses Rules of Road for Internet. `http://online.wsj.com/news/articles/SB10001424052702304049704579320500441593462`. Accessed in September 2014.

[72] OpenSignal. `http://www.opensignal.com/`. Accessed in September 2014.

[73] A. Osterwalder. Business Model Canvas. `http://www.businessmodelgeneration.com/downloads/business_model_canvas_poster.pdf`, Accessed in October, 2014.

[74] Otixo Website. Access All Your Online Files with a Single Login, Accessed in September, 2014. http://www.otixo.com.

[75] L. Panetta. Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, October 2012.

[76] V. Pareto. *Cours d'economie politique*. Librairie Droz, 1964.

[77] S. Pearson. Taking Account of Privacy when Designing Cloud Computing Services. In *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing*, CLOUD '09, pages 44–52, Washington, DC, USA, 2009. IEEE Computer Society.

[78] M. L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*, volume 414. John Wiley and Sons, 2009.

[79] B. Ramachandran, S. K. Srivastava, C. S. Edrington, and D. A. Cartes. An Intelligent Auction Scheme for Smart Grid Market Using a Hybrid Immune Algorithm. *Industrial Electronics, IEEE Transactions on*, 58(10):4603–4612, Oct 2011.

[80] P. Reichl, P. Maille, P. Zwickl, and A. Sackl. A Fixed-point Model for QoE-based Charging. In *2013 ACM SIGCOMM workshop on Future human-centric multimedia networking (FhMN '13)*, pages 33–38, 2013.

[81] Report on Stakeholders Characterization and Traffic Characteristics; SmartenIT Deliverable D1.1. I. Papafili and G. D. Stamoulis (eds.). `http://tinyurl.com/delieverableD1-1`, August 2011.

[82] J. Rubio-Loyola, M. Charalambides, I. Aib, J. Serrat, G. Pavlou, and R. Boutaba. Business-driven Management of Differentiated Services. In *Network Operations and Management Symposium (NOMS), 2010 IEEE*, pages 240–247. IEEE, 2010.

[83] M. Said. Auctions with Dynamic Populations: Efficiency and Revenue Maximization. *Auctions, Market Mechanisms and Their Applications*, pages 87–88, 2009.

[84] J. Schaefer and P. Blank. Deutsche Telekom: 'Internet data made in Germany should stay in Germany'. `http://tinyurl.com/deutschetelekom-internet-data`, Accessed in May, 2014.

[85] L. Schubert and K. Jeffery. *Advances in Clouds*. European Commission, Publications Office of the European Union, Luxembourg, 2012.

[86] J. Seiffert. Weighing a Schengen Zone for Europe's Internet Data. `http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482`, Accessed in May, 2014.

[87] P. Seipel. Borderline Technology: Its Difficulties in a Swedish Perspective. `http://www.juridicum.su.se/iri/docs/Borderline_Technology/`, September 1998.

[88] U. Sievers. Ein Schengen-Routing ist Faktisch Schon Da. `http://www.vdi-nachrichten.com/Technik-Wirtschaft/Ein-Schengen-Routing-faktisch-da`, Accessed in May, 2014.

[89] H. Steier. Grosse Gefahr fuer das Gesamte Internet. `http://www.nzz.ch/mehr/digital/internet-slowdown-netzneutralitaet-fcc-aktionstag-1.18380788`. Accessed in September 2014.

[90] R. S. Sutton and A. G. Barto. *Introduction to Reinforcement Learning*. MIT Press, Cambridge, MA, USA, 1st edition, 1998.

[91] A. S. Tanenbaum. Network protocols. *ACM Comput. Surv.*, 13(4):453–489, Dec. 1981.

[92] The European Parliament and Council, DIRECTIVE 2006/24/EC. `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF`. Accessed in September 2014.

[93] The Guardian. `http://tinyurl.com/guardian-data-retention`. Accessed in September 2014.

[94] The Telegraph, Emergency legislation giving police access to phone records becomes law. `http://www.telegraph.co.uk/news/10974818/Emergency-legislation-giving-police-access-to-phone-records-becomes-law.html`. Accessed in September 2014.

[95] Tor Project, Anonymity Online. `https://www.torproject.org/`. Accessed in September 2014.

[96] Towards an EU Cloud Computing Strategy. `http://www.eesc.europa.eu/?i=portal.en.ten-opinions.24758`, April 2012.

[97] C. Tsiaras. AbaCUS Project. `http://www.abacusproject.eu/`. Accessed in October 2014.

[98] C. Tsiaras, A. Sehgal, S. Seeber, D. Dönni, B. Stiller, J. Schönwälder, and G. Dreo. Rodosekn. Towards Evaluating Type of Service Related Quality-of-Experience on Mobile Networks. In *7th IFIP Wireless and Mobile Networking Conference (WMNC)*, WMNC2014. IEEE, May 2014.

[99] C. Tsiaras and B. Stiller. Challenging the Monopoly of Mobile Termination Charges with an Auction-Based Charging and User-Centric System (AbaCUS). In *Proceedings of the Conference on Networked Systems (NetSys 2013)*, NETSYS '13, pages 110–117, 2013.

[100] C. Tsiaras and B. Stiller. A Deterministic QoE Formalization of User Satisfaction Demands (DQX). In *39th IEEE Conference on Local Computer Networks (LCN)*, LCN2014, pages 227–235. IEEE, September 2014.

[101] D. Tuncer, M. Charalambides, R. Landa, and G. Pavlou. More Control Over Network Resources: An ISP Caching Perspective. In *9th International Conference on Network and Service Management (CNSM), CNSM2013*, pages 26–33, Oct 2013.

[102] Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates. Amtsblatt der Europäischen Union, June 2008.

[103] W. Vickrey. Counterspeculation, Auctions, and Competitive Sealed Tenders. *The Journal of finance*, 16(1):8–37, 1961.

[104] I. Voutchkov and A. Keane. Multiobjective Optimization using Surrogates. *Adaptive Computing in Design and Manufacture*, 9(167-175), May 2006.

[105] W. Wang, B. Liang, and B. Li. Revenue Maximization with Dynamic Auctions in IaaS Cloud Markets. In *IEEE/ACM 21st International Symposium on Quality of Service (IWQoS), 2013*, pages 1–6, June 2013.

[106] P. Welchering. Daten im Land halten bringt nicht viel. `http://www.faz.net/aktuell/technik-motor/computer-internet/europaeisches-netz-daten-im-land-halten-bringt-nicht-viel-12690332.html`, Accessed in July, 2014.

[107] F. Zhao, P. Luh, Y. Zhao, J. Yan, G. Stern, and S.-C. Chang. Bid Cost Minimization vs. Payment Cost Minimization: A Game Theoretic Study of Electricity Markets. In *Power Engineering Society General Meeting, 2007. IEEE*, pages 1–8, June 2007.

11 Acknowledgements

This deliverable was made possible due to the large and open help of the WP7 Partners of the FLAMINGO consortium. Also, feedback and comments from reviewers were highly valuable and enriching for the quality of deliverable. Many thanks to all of them.

12 Appendices

The interview-based validation approach was based on a general template of questionnaires, prepared by WP7 of FLAMINGO. This template consisted of four major categories of questions- (1) General Questions to identify the validity of assumptions, problem, and approach followed, (2) Scenario Specific Questions to perform in-depth analysis of scenarios with experts in terms of implementation and practicality, (3) General Recommendations to identify areas of changes and/or improvements for the scenarios, and (4) Applicability and Limitations Questions, where there relevance of scenario in real world is being discussed.

As a result, these questionnaires were used in the interview and were consequently filled off by scenario owners. This section presents all these questionnaires for the scenarios within WP7.

12.1 Network Virtualization

FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: Network Virtualization

Scenario Owner: UPC-iMINDS

Expert's Name: Javier Ramón (Telefónica I+D), Alfonso Tierno (Telefónica I+D)

Interviewer's Name: Joan Serrat (UPC) and Juan-Luis Gorricho (UPC)

1. **General Questions:**
   a. **Does the scenario under consideration expose a relevant problem?**
   In general it does. Because resources are scarce, optimization of their use is always needed. But optimization of resource utilization that an InP like Telefonica is sharing with other SPs is not of primary importance. The reason is that this resource sharing is done following specific regulations that are subject of audits. Modifying the amount of resources initially granted to a SP is not seen as feasible in the current contexts. Keep in mind that this sharing of resources is also done by means of ad-hoc (traditional) techniques and not making use of resource virtualization.

   b. **Do the scenarios' stakeholders form a complete approach?**
   As the scenario is presented, yes. The necessary stakeholders are the InPs and the SPs

   c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**
   Understanding the core problem as the lack of optimization of resources, then the answer is yes. But if we understand the core problem as the need to share resources among incumbent operators and emerging ones, then this is a problem of complete different nature.

   d. **Which areas impact this scenario?**

   ☑ Economic constraints
   ☐ Legal constraints
   ☑ Regulative constraints

e. Are the key assumptions made for this scenario realistic?

In part only. The assumption of traffic variability and the need of resource reallocation is a valid one. Nevertheless, the assumption that this comes from an initial virtual network embedding due to a dynamic demand of VNs by several SPs is not realistic nowadays. As mentioned before, when a SP needs resources from an InP, this is negotiated in a conventional way and the allocation of resources is rather static and done by means of technologies nothing to do with network virtualization. While we agree that in niche application domains these assumptions could be realistic, this is not the general trend.

2. Scenario Specific Questions:

a. Opportunistic use of resources contracted to SPs

Q. Assuming that the SPs are paying for total contracted resources, would it require specific agreements to allow that "their resources" are taken back by the InP? Or is it in the powers of the InP to determine resource allocation for as long as these resources are given back to the SPs when needed?
A. InPs are able to charge SPs according to their real use of resources. Therefore there is no need to establish specific agreements. The SLA, OLA or UC between stakeholders would include such a “pay per use” attribute.

b. Resource status monitoring

Q. Do you (the InP) currently have capacity to support the monitoring of network resource utilisation/allocation as required by our proposal? If not, would you easily accept to deploy a system that does so? In terms of frequency of monitoring/resource adjustments, how often is practical? Would this frequency have any impact on network load and performance or on user quality of service?
A. Resource status monitoring is perfectly possible in the current infrastructures at least to the extent of the attributes to be monitored in this scenario. On the other hand, it would be more difficult to measure the latency because it would require active end to end measurements. The monitoring of resources and the QoS would not impact the users’ QoS.

c. Practical implementation

Q. Is it possible to implement the proposed algorithms in state of the art communication systems i.e. to embed learning agents in real network nodes and links? If not, what would be the limiting factor?
A. Proposed learning algorithms are simple enough to be embedded in the network elements where they should be running.

3. General recommendations to the scenario owner

The InP consulted is very much interested in NFV and not specifically interested in virtualization of resources as understood in the current scenario. Nevertheless they see important connections between the two problem domains, namely resource virtualization with usage optimization and NFV. Particularly in what is related to the optimization techniques. In NFV there are important optimization problems to solve and they recommend us to see how our know-how could be reoriented to solve these problems.

4. Applicability of scenario in the real world

a. Please tick the relevant box based on relevance

☐ irrelevant
☐ partially irrelevant
☐ neither
☑ partially relevant
☐ relevant

b. List of limitations (if any) with their reasons

The main assumption about the need to partition network nodes and links is not currently realistic. Resources from an InP are assigned much more ad-hoc and statically, as opposed to the demand-based approach assumed in this scenario. In other words, from an economical perspective the mechanisms actually in place are good enough and don't need to be changed.

12.2 ISP-oriented Content Delivery

FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: **ISP-oriented Content Delivery**

Scenario Owner: **UCL, iMinds**

Expert's Name: **Raul Landa, Sky UK**

Interviewer's Name: **Marinos Charalambides, Daphne Tuncer**

1. **General Questions:**
   a. **Does the scenario under consideration expose a relevant problem?**
   The research you are conducting is quite relevant to the current and future plans/developments at Sky. We have already deployed a caching infrastructure to improve the VoD services we provide to our customers. Our network is heavily biased towards content distribution, and at the moment about half of all the traffic served to our customers is provided by CDN. This is forecasted to grow over the next year to about 75%.

   b. **Do the scenarios' stakeholders form a complete approach?**
   I believe you have successfully identified all the necessary stakeholders for providing the proposed service. However, the relationship between the ISP and large CDNs is a bit sensitive since they can be considered as competitors under the proposed scheme. Care must be taken so that the business relationship is not compromised.

   c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**
   Both content placement and the selection of the caching location to serve requests from are part of the problem core (and relevant to Sky) since the associated intelligence can largely impact the utilisation of the resources to support VoD services.

   d. **Which areas impact this scenario?**

   ☑ Economic constraints

☐ Legal constraints
☑ Regulative constraints

e. Are the key assumptions made for this scenario realistic?

From a technical point of view your assumptions seem to be realistic. From a business perspective other factors come into play, such as the investment required to support the service. It would be wise to investigate the cost associated with installing and maintaining the caching infrastructure.

2. Scenario Specific Questions:

a. What are typical values for cache size (few large or many small)?

For managed content (e.g. Sky's own library of media assets) or very popular content moving closer to the subscriber is extremely useful. For the long tail, off-net storage and peering agreements for best. For the stuff in the middle, a strategy mixing CDN surrogates in the core of the network and closer to the users is required. Smaller caches can lead to low hit ratios, so there is a tendency for caches to grow to a minimum size. On the other hand, large caches become single points of failure, require large network footprint and are may involve multiple buildings and machine rooms, increasing complexity. The really important thing, rather than having many small caches or a few smaller ones, is to have efficient and intelligent mechanisms to offload demand between caches without generating excessive signalling or network traffic footprint.

b. What is a typical cost for inter domain traffic?

I do not think I can share this freely but it is not a small amount. Finance is definitely interested in reducing this cost. On the other hand, the cost in terms of power and space required in order to host multi-terabits of caching capacity mean that peering can be cheaper in many cases. It is not a simple problem nor dominated by a single side of the argument.

3. General recommendations to the scenario owner

Experimentation with a set of real VoD request traces would be beneficial to your work so that you can validate the model you have developed and investigate the behaviour of the management intelligence under various settings. Furthermore, it is vital for your work to flee out the underlying mechanisms of the protocol (DNS extensions, HTTP redirection, BGP announcements for prefix locality, etc). This way it can be placed in context

alongside traditional CDNs. A modular architecture where a CDN node has decoupled computation and storage, so that many computation units can share a common storage library would be fundamental too.

4. Applicability of scenario in the real world

a. Please tick the relevant box based on relevance

☐ irrelevant
☐ partially irrelevant
☐ neither
☐ partially relevant
☑ relevant

b. List of limitations (if any) with their reasons

none

12.3 Mobile Measurements

FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: Mobile Measurements

Scenario Owner: University of Zürich

Expert's Name: Leo Lehmann, BAKOM, Biel, Switzerland

(BAKOM: Bundesamt für Kommunikation, the Swiss Federal Communications Commission, speaking as a private person)

Interviewer's Name: Christos Tsiaras, Burkhard Stiller, Radhika Garg

1. **General Questions:**
   a. **Does the scenario under consideration expose a relevant problem?**
   It does cover an important problem of transition from QoS to QoE. The relevant aspects to consider cover the telecommunications law, the data privacy aspects, and the data protection laws. Swiss law may differ from European law.

   b. **Do the scenarios' stakeholders form a complete approach?**
   The set of stakeholders determined address the user, the provider, and the regulator and the legislation, respectively. This does determine to the best of our knowledge the complete view on such a scenario.

   c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**
   The mapping of the networks services onto a measurement approach for users, who measure their dedicated view of a service quality in cooperation with a measurement server, does enable the determination of quality aspects of service delivery. The problem to identify the real cause, behind not getting as service as expected, still remains and cannot be solved in such a set-up. However, the set of potential reasons for such a case may have been measured and documented as well. Thus, there remain chances of false claims in case of such an event due to the one-time

measurement. The consequences of legal effects and impacts for the user and the provider need to be discussed.

d. Which areas impact this scenario? (tick all being relevant)

- ☐ Economic constraints
- ☑ Legal constraints
- ☑ Regulative constraints

e. Are key assumptions made for this scenario realistic?

- ☑ Yes
- ☐ No
- ☐ Concerns: _____

2. Scenario-specific Questions:

a. Is it legal to present data concerning the QoE/Type-of-Service of a Mobile Network Operator (MNO) to the public or users, since in case of "bad" results a different Autonomous System on the communication path might be responsible? Do respective regulations on opening-up "performance" data of MNOs exist in Switzerland?

The telecommunications act for Switzerland does not handle this issue. If this case shall be considered as a problem or no problem can only be answered by legal experts. A legal problem may also exist in terms of the interpretation of data measured: Who can be hold responsible for this measurement? How was the data produced? Which explicit influence does a provider has on such a measurement? What effect an interpretation will have on an operator or user? In case of false claims, what are the related (legal, economic, reputation) consequences?

b. If the answer to Q2.a is "No", would it be legal to do so, if such an information is stated explicitly in the End-user License Agreement (EULA) of the Application?

The Telecommunication act for Switzerland does not handle this issue there may remain problems in terms of ownership of those data collected.

c. If again the answer to Q2.b is "No" again, how should such a measurement result be presented to the end-user? Which terminology, data should be used? What kind of disclaimer?

Under the same assumptions made above, the way the data is interpreted and the way the information that is collected is more important. In case of an actual reason for a low quality of service, it must be carefully identified and stated with respective analysis methods, algorithms, and interpretation schemes. Any possible false claim can lead to unwanted consequences.

d. Is it possible as an end-user to use such measurement data to claim that his SLA was not fulfilled or that network neutrality is violated? If yes, how may that be done and to which extend can details be revealed?

QoS measurements for the fixed network are done in Switzerland. Thus, there is the basis to run the respective technology. The clear view on the legal relevance, importance, or effect, however, has not been studied for the fixed network.

3. General recommendations to the scenario owner

While the mobile measurement scenario reads very well and interesting the technology applied for the experience measurements in a mobile setting is new and may be further considered. The main recommendation provided is that the data collected – under written consent or otherwise – should lead to a discussion with the Swiss "Datenschutzbeauftragten" (Representative for Data Protection), which may shed light in those areas the Swiss regulator by definition is not the responsible stakeholder for.

4. Applicability of scenario in the real world

a. Please tick the relevant box based on relevance

☐ irrelevant
☐ partially irrelevant
☐ neither
☐ partially relevant
☑ relevant

b. List of limitations (if any) with their reasons

As the Swiss Telecommunication Law there does not include a legal framework to enforce options for accessing or implementing such a measurement scenario for mobile services, the value of such voluntary measurements may be questioned. However, the QoS and the related QoE is highly relevant for service improvements intended by providers. Note that objective QoS measurements do find a technical basis in ITU recommendations for telecommunication provider.

12.4 Legal and Ethical Facets of Data Sharing

FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: Ethics in Data Sharing

Scenario Owner: University of Twente

Expert's Name: Roland van Rijswijk-Deij, SURFnet bv, NL

Interviewer's Name: Anna Sperotto

1. **General Questions:**
   a. **Does the scenario under consideration expose a relevant problem?**
   Yes; as a National Research and Education Network SURFnet regular has to deal with requests from researchers that perform research on networks and research on network security for access to all sorts of operational data. Although SURFnet has a workable *ad hoc* policy for dealing with such requests using a target non-disclosure agreement, it is highly desirable to have a more comprehensive policy that takes into account the relevant legal (e.g. privacy law) context and is based on a solid ethics framework.

   b. **Do the scenarios' stakeholders form a complete approach?**
   Yes; all perspectives that are relevant to the problem are represented in the form of:

   - A data supplier (SURFnet, NREN)
   - Data consumers (researchers from the University of Twente and University of Amsterdam)
   - Legal expertise (University of Tilburg)
   - Ethics expertise (University of Twente)

   c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**
   Yes, we have a shared goal of coming to a concise and workable policy by the end of 2014 to apply to data sharing requests that we aim to put to the test over the course of the coming years.

d. Which areas impact this scenario?

- ☐ Economic constraints
- ☑ Legal constraints
- ☑ Regulative constraints

e. Are the key assumptions made for this scenario realistic?
Yes, all parties involved have real world experience in the subject matter and herald a practical approach towards creating a policy that is on the one hand well-founded in theory and law and on the other hand flexible enough not to hinder data sharing requests. Both the legal as well as the ethics experts have a constructive approach in the sense that they do not seek to limit behaviour based on rules but rather strive to best facilitate all parties' wishes in a data sharing relationship within the constraints allowed by the law and taking into account ethics best practices.

2. Scenario Specific Questions:
none

3. General recommendations to the scenario owner
The Dagstuhl Seminar at which all parties collaborating in this scenario met was key in forming the team and the opinions of the team; a follow-up seminar where progress in this area is revisited within the time frame of about one year is highly desirable.

4. Applicability of scenario in the real world

a. Please tick the relevant box based on relevance

- ☐ irrelevant
- ☐ partially irrelevant
- ☐ neither
- ☐ partially relevant
- ☑ relevant

b. List of limitations (if any) with their reasons
none

12.5 Auction-based Charging User-centric System

FLAMINGO WP7 — Scenario Validation wrt Economic, Legal, and Regulative Constraints

Scenario Name: AbaCUS _____

Scenario Owner: University of Zürich _____

Expert's Name: Leo Lehmann, BAKOM, Biel, Switzerland _____

(BAKOM: Bundesamt für Kommunikation, the Swiss Federal Communications Commission, speaking as a private person)

Interviewer's Name: Christos Tsiaras, Burkhard Stiller, Radhika Garg

1. **General Questions:**
   a. **Does the scenario under consideration expose a relevant problem?**
   Precondition: The Swiss national Roaming had been emulated by utilizing international SIM cards, such as from Germany and Greece.
   The regulation of Mobile Termination Rates (MTR) in Switzerland differs from the one in the EU, since in Switzerland a respective request is needed from the side of market players (ex-ante vs. ex-post). Thus, the regulation itself would be possible, if such a request would be addressed to the BAKOM. However, by legislation, the BAKOM cannot make that first step.
   The role of legal interception and the payment schemes of call-by-call as well as flat rate would need to be considered, too, if such an approach of auctioning off the receiver's provider would be in place. Besides voice traffic the consideration of data traffic under a similar perspective would be needed.
   Note that the Swiss case and possible EU case may look very different.

   b. **Do the scenarios' stakeholders form a complete approach?**
   No, the given scenario does not form a complete approach when related to Switzerland. The prerequisite of such an approach is to have national roaming in place, which would need to include Mobile Network Operators (MNO), users, legal acts, and the regulator. Currently there is no agreement between Swiss operators in respect to a national roaming approach. There is also no legal or regulative framework included in the

Swiss Telecommunication law, which can force operators to have such an agreement being established. Such a framework has to be decided by the government.
For the legal surveillance of such a service commercially being offered an extra hop seems to be required, because even if the callee is changed dynamically, traces for legal interception reasons still need to be collected.

c. **Does the scenario's major mechanism in solving this problem approach the core of the problem?**
Yes, the core of the problem is being covered at the respective technical level and under an economic optimization view, which balances the providers' and users' perspectives at eye level. However, the legal basis to apply such a mechanism mandatorily within Switzerland is not in place currently. In order to bring in any of this change into the current Swiss market, especially under the assumption that all MNOs have to participate, a new legal framework, which forces operators to enable competition, is needed.

d. **Which areas impact this scenario? (tick all being relevant)**

☑ Economic constraints
☑ Legal constraints
☑ Regulative constraints

e. **Are key assumptions made for this scenario realistic?**

☑ Yes
☐ No
☑ Concerns: Operators might not have interest in reducing the mobile termination rates.

2. **Scenario-specific Questions:**
   a. **Which are the actions that a regulator needs to take to enforce a competitive environment, such as the one proposed in AbaCUS? How long such a process demands?**
   The key prerequisite to enable a competitive environment for such an approach is to have national roaming in place. Furthermore, the legal basis to enforce all participants from the MNO's side would be required, if an enforcement of AbaCUS would be intended.

b. Under which circumstances a regulator would enforce AbaCUS? Due to (1) economic benefit for stakeholders, (2) social welfare increment, or (3) an MNO's infrastructure utilization maximization?

Social welfare is a clear goal of a regulator, which is not different for the Swiss regulator compared to other FCCs worldwide. It is, however, difficult to say, if the approach proposed will reach such an optimum, since the obligation of national roaming and the collaboration of operators is needed for AbaCUS. What are the counter-intuitive aspects to be considered?

And from an economic point of view a respective law has to be in place, which can enable the implementation of such approach in the given market. When respective legal instruments are in place and a market analysis has been performed, the problem may become obvious. Once the problem is identified and theoretically analyzed, only then the right efficient instrument can be developed, and AbaCUS is one of those solutions foreseen.

c. Is it more efficient to regulate Mobile Termination Rates (MTRs) or to enforce competition between MNOs?

The regulation of Mobile Termination Rates (MTRs) as well as the enforcement of the competition between MNOs is means that serve the same purpose related to the economic benefits of a society. They are not considered as alternatives as stated by the question.

3. General recommendations to the scenario owner

The virtualization of services and operators has progressed, thus, a respective Virtual Mobile Network Operator (VMNO) view may be considered, too. In general, the technology neutrality is very important to be respected, meaning that no specialized technology may be required to solve a problem, which a regulator considers relevant.

4. Applicability of scenario in the real world

a. Please tick the relevant box based on relevance

☐ irrelevant
☐ partially irrelevant
☐ neither
☐ partially relevant
☑ relevant

b. List of limitations (if any) with their reasons

For the Voice-over-IP services within LTE, the AbaCUS approach would work, as this is packet-based. However, the accounting problem may still remain to be solved.