FLAMINGO

European Seventh Framework Network of Excellence

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

WP7 — Economic, Legal and Regulative Constraints

Deliverable D7.1 — Basics, Requirements, Scenarios, and Architecture

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
E-mail:	garg@ifi.uzh.ch
Doc ID:	D7.1
Delivery Date:	31.10. 2013
Authors:	Anthea Mayzaud, Anuj Sehgal, Björn Stelte, Burkhard Stiller, Christos Tsiaras, Corinna Schmitt, Daniel Dönni, Daphne Tuncer, Joan Serrat, Juan Luis, Marinos Charalambides, Mario Flores, Mario Golling, Maxim Claeys, Niels Bouten, Nikolay Melnikov, Peter Hillmann, Radhika Garg, Rashid Mijumbi, Ricardo Schmidt, Rick Hofstede, Sebastian Seeber, Sofie Verbrugge, Steven Latre

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

The objectives of WP7 concentrate on the integration of network and service management research with economic, legal, and regulative constraints. Methodology and approaches for understanding the economic dependency of technology, and stakeholders interrelation form the prime focus of this work package. Therefore, the purpose of this document is to analyze and discuss key scenarios (in close collaboration and conjunction with WP5 and WP6) in terms of methodology, requirements, and functionality to propose a joint architecture. The goal of this proposed joint architecture is to enable the formalization of major techno-economic inter-dependencies in a first step and later legal-regulative inter-dependencies followed within the second step.

WP7 is driven by the underlying understanding that technology proves more beneficial when it is developed with economic, legal, and regulative perspectives, as well as constraints it is effected by. In detail, analysis of business indicators (*e.g.,* resource utilization efficiency, performance) for network and application optimization helps in identifying the dependency of underlying technology on economic and initial regulative needs. Therefore, assisting technologists in comprehending limiting factors from the above mentioned perspective is the prime focus of this deliverable. To this end, and with the experience and engagement in the first year of FLAMINGO with those studying technologies under the umbrella of the Future Internet (FI), this deliverable D7.1 follows a methodology of identifiying major facets of the answers to three major questions:

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

2. Who are the major stakeholders and what is the value exchange between them in networks and telecommunication systems?

3. What are business indicators, which can be listed based on the hence identified constraints for each management technology and solution under consideration?

In reply to these questions, WP7 defined a dedicated FLAMINGO management architecture, which forms the basis for the analysis of the set of scenarios from the business policy management, value networks, and initial regulative point of view. The major findings for all the scenarios include four major aspects: First, each stakeholder in such a setting has varied interest and stake. This makes analysis in terms of incentives, and tussles, as well as legal and regulative constraints a crucial part of holistic approach of successfully operating such services. To this end, value networks are identified so that interrelations between the identified stakeholders (*e.g.,* service provider, operator) are clearly visible. Second, establishing an appropriate price-performance ratio is not only important for the service provider but also from the end-user's point of view. Thus, this factor is the major reason of tussle amongst stakeholders. Third, attempt of stakeholders to improve the performance of network and/or service is considerably impacted by legal laws, regulations and policies. Fourth, it is important to include management decision as part of functionality of services. In this context, business indicators are identified. This will help in measuring the progress of achieving organizations goals.

Those above mentioned findings from various scenarios investigated follow from the application of a pre-defined methodology, which at first identified major constraints it is effected by. Thus, the economic analysis comprises relevant facets, like stakeholder identification, an incentives discussion, a tussle analysis, and, where applicable, pricing models and regulative demands discussions. Major legal and regulative constraints depend on those facets and lead to partially measurable parameters, such as contractual relations, performance guarantees, privacy, and data protection and

security. Secondly, those identified constraints act as a guide for business indicators, which allow for the measurement or the quantification of economic performance. Thirdly, the preliminary stakeholders analysis reveals the importance of following regulative demands, which may vary over time.

Therefore, the analysis and discussion of scenarios within the scope of WP7 verifies the initial assumption of a general inter-dependency of technological requirements and economic, legal, and regulative constraints. In order to reduce the gap between operations and management decisions cross-disciplinary methods and approaches have been selected and have been applied on technology in terms of those scenarios. In the same line of initial steps undertaken within WP7, those business indicators identified for each scenario can be monitored based on those business policies defined. This will help 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 years of FLAMINGO to come.

2 Introduction

The Future Internet will see many management decisions to be taken as the commercial deployments and operations of networks and services will be driven by economic optimization. While the technological dimension covers the network and service monitoring as well as automatic configuration and repair, the integrated economic dimension addresses incentives, cost benefit analysis, Value Networks (VN), and Business Indicators (BI). The integrated legal dimension will address major stakeholders imperatives in a certain country or region, and the integrated regulative dimension will/does address impacts and effects of country- or region-specific regulations. The complement of technology and economics with legal and regulative constraints has and will be evaluated in order to ensure that the mechanisms are legally compliant with regulations and respective economic and cost models are legally valid.

2.1 Goals of WP7

Therefore, the goal of this deliverable D7.1 is to identify the methodology for understanding the mechanism of such a cross-disciplinary approach. To this end, a management architecture is proposed, which evaluates selected scenarios in terms of relevant and interesting economic, legal, and regulative constraints. Also BIs are identified in order to analyze and monitor the progress of business objectives for internet-based communication systems.

This deliverable D7.1 contains for all three WP7 tasks the current state, especially the documentation of basics required in methodology, key requirements, an assessment of relevant scenarios, and a proposed management architecture for relevant mechanisms. This resulting architecture helps to discuss and analyze in a homogeneous and comparable manner techno-economic and will support the legal and regulative inter-dependencies. Thus, this section recalls the three tasks of WP7, introduces the methodology developed and to be applied for all investigations, and finally outlines the full deliverable structure.

2.2 Tasks of WP7

The three tasks for this work package are executed for each of the scenarios that are being studied in WP5 and WP6. The methodology, models, and architecture for economic and legal analysis for these scenarios are identified completely. These scenarios have their key backdrop in network and service monitoring (WP5) and automated configuration and repair (WP6) in order to show an integrated effort in FLAMINGO and to study them in the view of economic, legal, and regulative constraints following three tasks are defined and followed. Thus, the three WP7 tasks are defined as follows.

- **Task T7.1: Economic Analysis**
  This task identifies detailed insights into economic analysis in the area of network and service management. This deliverable D7.1 concentrates on identifying major and re-appearing stakeholders involved in different scenarios, their incentives, interrelation, and VNs. Also, BIs are identified as a basis of management decision of operations, which is driven by economic optimization guidelines. The set of current and detailed outcomes of T7.1 is summarized in Table 1.

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

No.	Task Activities	Status as of Y1	Description	Section	To be Addressed in Y2-Y4
1.1	Muti-actor cost-benefit analysis	IN PROGRESS	Stakeholders and their incentives are identified	4.1 to 4.9	To be refined and cost-benefit analysis to be done
1.2	Trade-offs between cost of operations and obtained Quality-of-Experience (QoE)	FUTURE	-	-	To be done in scenario Value of Service (VoS)
1.3	Incentives-based interface of users/providers	IN PROGRESS	Value Networks discussing incentives between stakeholders are identified	4.1 to 4.9	To be refined and studied in depth
1.4	Charging approach for inter-domain Cloud Computing	FUTURE	-	-	To be discussed as charging, cost and revenue models of various stakeholders
1.5	Validation of economic management approaches by using trace-based behavior information	FUTURE	-	-	To be discussed in future as validation approach

- **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. T7.2 focuses on evaluating possible achievements of business objectives by monitoring BIs. 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 areas of Service Level Agreements (SLA), applicable law and jurisdiction, Quality-of-Service (QoS) fulfillment aspects, which are guided by legal or regulative limitations. This will demonstrate the strength, importance, and impacts of business models and network neutrally aspects for economic management. The set of current and detailed outcomes of T7.3 is summarized in Table 3.

Table 2: Task T7.2: SLA and Policy Management

No.	Task Activities	Status as of Y1	Description	Section	To be Addressed in Y2-Y4
2.1	Presentation of monitoring information of the managed system	FUTURE	-	-	To be defined and analyzed
2.2	Manipulation of managed system to maintain expected service performance	IN PROGRESS	As the first step, BIs are identified	4.1 to 4.9	To be refined, monitored, analyzed based on performance or business level objectives
2.3	Policy refinement and analysis	FUTURE	-	-	To be studied by identifying business policies and its impact on BIs
2.4	Economic traffic management techniques	FUTURE	-	-	To be discussed as negotiation process, tussle analysis between stakeholders
2.5	Interoperability functionalities and management tasks based on Service Level Agreements (SLA)	FUTURE	-	-	To be discussed in future as SLA driven task

Table 3: Task T7.3: Legal and Regulative Constraints

No.	Task Activities	Status as of Y1	Description	Section	To be Addressed in Y2-Y4
3.1	Approach to determine and negotiate SLA parameters, such as applicable law and jurisdiction	FUTURE	-	-	To be defined and analyzed
3.2	Determining SLA fulfillment aspects	IN PROGRESS	Undertaken in scenario SLA Fulfillment scenario	4.1 to 4.9	To be refined and analyzed in depth for legal and regulative limitation
3.3	Policy-based aspects in view of legal or regulative limitations	FUTURE	-	-	To be studied in terms of impact of legal and regulative constraints on business policies
3.4	Cost and accounting models in view of legal or regulative limitations	FUTURE	-	-	To be discussed as prerequisite in legal/regulatory domain for such models
3. 5	Business models and Network neutrality aspects	IN PROGRESS	Studied as business models of various scenarios	4.1 to 4.9	To be discussed further, specially in terms of network neutrality

2.3 Methodology

By addressing the overall goal as defined in Sec 2.1 the following three targets are addressed by the methodology chosen: First, to understand the basic requirements of economic, legal, and regulative constraints and methodology for the identification of interdependencies. Second, to establish guidelines for suitable models for techno-economic relations, legal, and regulative recommendations. Third, to perform detailed analysis of scenarios and use-cases that are part of FLAMINGO's technical scope, especially from WP5 and WP6.

In order to deliver appropriate scenarios, which in terms of their technical content are based on the objectives of WP5/WP6, the area of research concentrates on network and service monitoring approaches, which also addresses Internet mobility, virtualization and backward compatibility strategies, and automated configuration and repair for managed objects. To this end, nine major scenarios are identified and analyzed. As developed and shown in Figure 1, these scenarios form the basis of the economic, legal, and regulative analysis. For project year Y1 the focus has been laid on the scenario to Business Indicators and Value Networks derivation, which may already by now indicate some legal and regulative constraints, which, however, will be deepened in project Y2 and Y3. Each scenario due to its scope and field of research mainly selects one or more of the following four major areas of analysis:

- **Business Indicators:** SLA Fulfillment Mechanism, Virtual Network Embedding (VNE), Business-oriented Service Management
- **Value Networks:** Value-of-Service (VoS), Virtual Network Embedding, Quality Improvement, Protocol for Low-Power and Lossy Networks
- **Legal Constraints:** SLA Fulfillment Mechanism, Cache Management
- **Regulative Constraints:** Intrusion Detection Systems, Traffic Aggregates

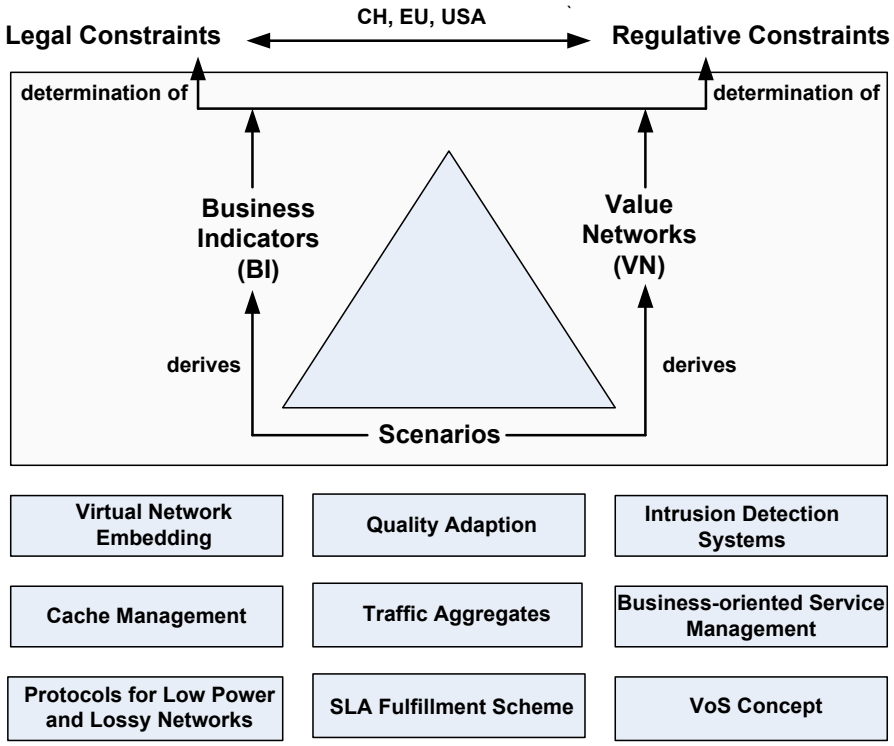

Figure 1: Methodology for WP7

The aforementioned defined four areas define or complement the existing “body of practices, procedures, and rules used by those who work in a discipline or engage in an inquiry; a set of working methods” [6]. These act as four pillars of methodology of identifying the various techno-economic dependencies within the envelope of legal, and regulative restrictions.

BIs and VNs form the basis for identifying the techno-economic interrelation. BIs are more focused on economical aspects, but this does not mean that only monetary BIs (*e.g.,* Losses due to QoS violation) will be the measure of a scenario’s goals, as also non-monetary BIs (*e.g.,* User Satisfaction) have an impact on economical issues. VNs concentrate on identifying multi-actor value analysis. Identification of roles and incentives form directions for understanding economical dependencies of the scenarios. Therefore, this deliverable identify the stakeholders, their incentives, tussles, and value exchange. In order to monitor and understand the business aspect of each scenario BIs, its relevance and measurement method is identified. Even though the results obtained so far are preliminary and may see variations in future, they form a strong basis for the future work within FLAMINGO. These results will have an impact on the way accounting, charging, cost, revenue, and other economic models are framed and identified in the next years of the project.

The investigation of legal and regulative constraints help to identify boundaries, which each stakeholder is bounded by, in order to implement the technical scenario in real world. Such requirements differ based on geographical region(s) under consideration (*e.g.,* Switzerland (CH), the European Union (EU), or the United States of America (USA)). For example, in case of monitoring traffic flows the operator might be restricted to monitor certain type of flows owing to legal and regulative mandates. This causes considerable impact on the flexibility and efficiency of an operators business and, thus, the right steps to improve the performance of the network.

2.4 Document Structure

The rest of this document for Deliverable D7.1, entitled “Basics, Requirements, Scenarios, and Architecture”, is structured in the following manner. Section 3 defines the FLAMINGO management architecture used by WP7. It explains the reason and relevance of using such an architecture for analyzing various technical scenarios from the economical, legal, and regulative perspective. Section 3 gives a brief overview about progress of various scenarios, which are studied in this deliverable D7.1. Towards the end of this section major concepts and terms, which are used and applied throughout the deliverable, are introduced.

Section 4 focuses on applying the integrated methodology, models and architecture to scenarios identified within the scope of WP7. This section is divided for each scenario into three major parts: (1) Introduction of the area and scope of each scenario, (2) identification of economic, legal, and regulative constraints, and (3) identification of business indicators and its measurement method. In other words, this section includes the major results obtained after applying the methodology and FLAMINGO management architecture, which is identified as the roadmap of WP7.

Section 5 contains preliminary conclusions and summarizes fundamental aspects of the work. This section also presents a brief outlook to the work of next years within FLAMINGO. Section 6 lists and documents progress of WP7 with respect to the WP7 and S.M.A.R.T objectives.

Finally, Section 7 and Section 8 complements the documents with a list of abbreviations and bibliographic references.

3 Definition of a Management Architecture

Based on the research work in WP5 and WP6, several scenarios have been identified and selected. In order to analyze those scenarios, in a structured and comprehensive manner a basic FLAMINGO management architecture is used. In this section thematic areas of such an architecture are introduced and explained. These thematic areas form basis of work for WP7. Future Internet and services will change the communication environment. The end-users will become more transparent owing to be being continuously monitored, tracked, and profiled. Also, an end-user will increasingly depend on the availability and performance of network-services, and billions of devices needs to be operated, controlled, and managed. Therefore, it is essential that management decisions become part of the process of operating such services/resources.

3.1 Basic FLAMINGO Management Architecture

Many requirements towards management of the FI have strong basis in the economic, legal, and regulative sphere. Therefore, the FLAMINGO management architecture proposed here serves as an integrated and holistic approach of (a) value-awareness, (b) incentives and tussles for service provisioning, (c) business policies, and (d) legal/regulative aspects. The completeness of such an analysis will be defined and evaluated in the next FLAMINGO years. As shown in Figure 2, the basic FLAMINGO management architecture covers three major thematic areas:

- **Economic, Legal, and Regulative Constraints:** Each scenario is analyzed to identify the set of key constraints in two broad categories: (i) economic constraints, (ii) legal and regulative constraints. The first category of economic constraints studies all the scenarios to list the constraints in the area of (1) incentives and tussles between the identified stakeholders, (2) cost, pricing and charging models, (3) safety and risk management. From the legal and regulative perspective, the constraints are categorized in terms of (1) contractual relations, (2) SLAs, (3) performance guarantees, (4) privacy, data protection, profiling, and (5) Net Neutrality. These constraints form the envelope within which business objectives and decisions can be taken. This is because these constraints serve as the boundary, which most of the times can restrict stakeholders from achieving the goals defined.
- **Business Indicators:** BIs can be understood as quantitative parameters that are specified on various levels of abstractions for the scenario under consideration (*e.g.,* network, resources, processes). By defining indicators expected target values can be evaluated. In addition, by continuously monitoring them, resources can be appropriately configured or manipulated so that the desired level of performance or quality of service is achieved. BIs are a way of reducing the complexity of all data generated from the operations of the company, so this data can be presented in a more digested or understandable form so people can evaluate the progress towards a goal more easily. These parameters serve as the starting point of evaluating various scenarios within the boundaries of economic, legal, and regulative constraints. For example, assuming a scenario where a stakeholder wants to temporarily cache some content in the network, but is restricted to do so, due to the privacy and copyright laws of some geographical region. This leads to making a boundary for the level of performance that can be targeted and achieved. The constraints from economic, legal, and regulative point of view define the business indicator (one-to-one mapping), or at least have an impact on their relevance. The completeness and evaluation of such an impact will be part of analysis for the next FLAMINGO years.

- **Business Policies:** Business Policies (BP) are the guidelines developed for a scenario in order to govern its target goals. They define the limits within which decisions must be made. A BP is a statement describing strategies for each scenario to successfully manage and handle the resources. This part of work is the next step towards the analysis of each scenario under WP7, and will be investigated within the next years of FLAMINGO.

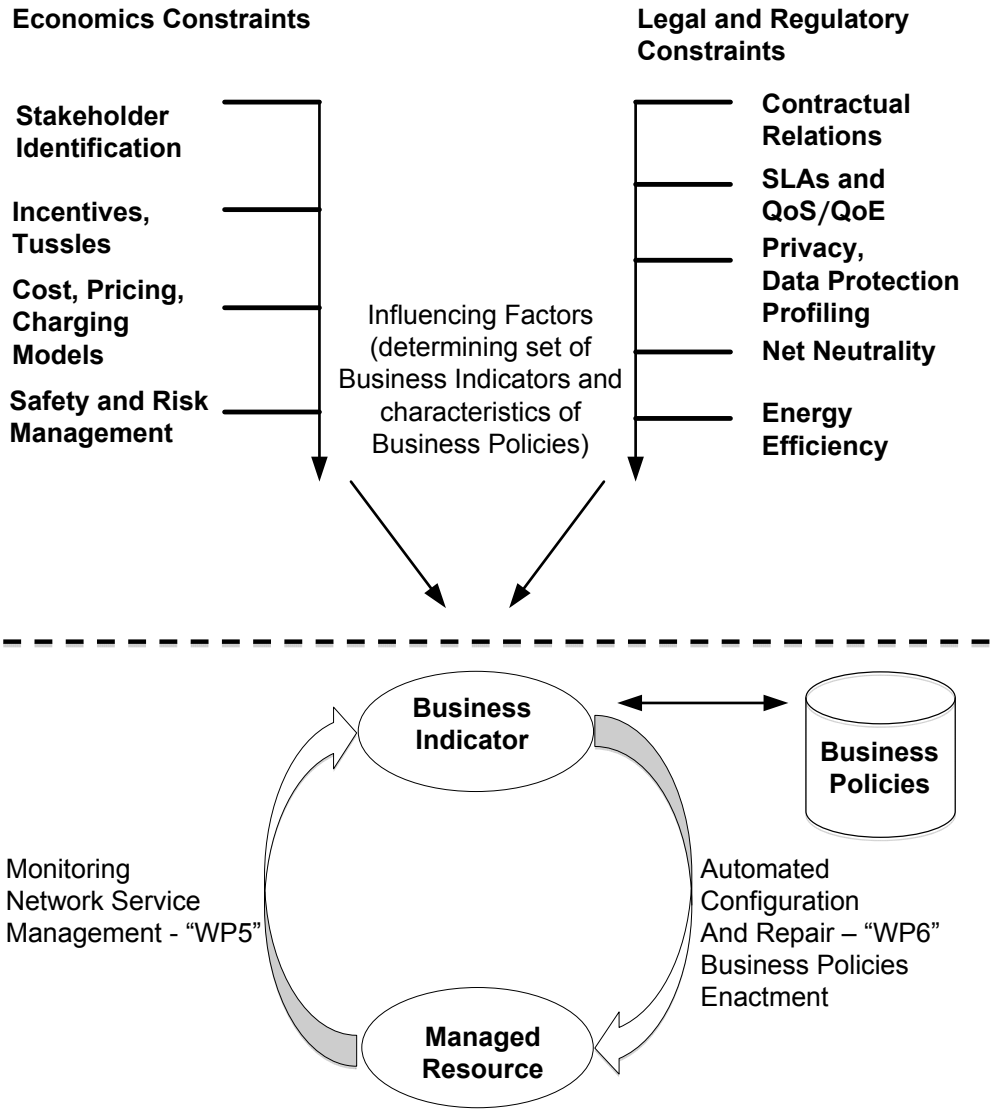

Figure 2: FLAMINGO Management Architecture

As shown in Figure 2, the FLAMINGO management architecture follows the methodology identified for WP7. The architecture based on the goals of WP7 is divided in two major tasks: (1) economic, legal, and regulative constraints identification, and (2) monitoring and configuring managed resources based on business policies. The integrated economic evaluation of dramatically changing underlying technologies and services of the FI, include the following major aspects of (a) price-performance trade-offs, (b) cost, revenue, pricing models, and (c) stakeholder identification along with their value interrelation. These are complemented with legal and regulative constraints, which have to be evaluated to ensure that contracts concluded will be legally valid, user's privacy and security is not compromised, and provider-dependent cost models as well as accounting models

are legally compliant with regulations. As the first step such factors, which enable, limit, or undermine the feasibility of operating and deploying the technical scenarios, are identified. The next task is to monitor, configure, and adapt the managed resources or services based on the business objectives. This is done by first determining business indicators, which in turn are influenced by the mentioned constraints. Adaptation and (re-)configuration of the managed resource is based on the business policies, which are identified within the boundaries of constraints. The loop shown in Figure 2 follows these above mentioned steps for all the scenarios identified within the scope of WP5 and WP6. Therefore, based on identified business indicators and policies, the resources (for each of the scenarios) are configured to achieve the desired business objectives.

The global vision of a FI is that taking a purely technical and service oriented viewpoint while defining the FI runs the risk to optimize that will be very difficult to deploy on a global scale. This approach, thus, fulfills the aim of FLAMINGO to diminish the gap between the control, operations, and management aspect of FI services and resources.

3.2 Overview and Status of Scenarios

Various scenarios encompassing the area of network and service management monitoring as well as automatic configuration and repair are analyzed in accordance with the aforementioned FLAMINGO management architecture in Section 3.1. However, these scenarios, as shown in Table 4, vary in depth of the analysis, which can be performed in the areas of constraints and BIs. The analysis done in the first year of FLAMINGO is based on current status of technical work of WP5 and WP6. In Table 4 "✓" signifies that a scenario has started to analyze the work with respect to the column heading. The completeness and evaluation of such analysis would only be achieved in next FLAMINGO years. The symbol "x" shows that this part of analysis is not done so far. This is mainly due to the progress and scope of the technical work under consideration in the first year of the FLAMINGO project.

Table 4: Scenario-specific Progress

Scenarios	**Economic Constraints**	**Legal and Regulative Constraints**	**Business Indicators**
Virtual Network Embedding	✓	✓	✓
Quality Improvement	✓	✓	✓
Intrusion Detection Systems	✓	x	x
Cache Management	✓	✓	x
Traffic Aggregates	x	x	x
Business Oriented Service Management	✓	✓	✓
SLA Fulfillment Mechanism	✓	✓	✓
Protocol for Low-Power and Lossy Networks	✓	x	x
VoS Concept	✓	✓	✓

3.3 Major Concepts Used and Methodology Applied

Major concepts harmonized for WP7 include the terminology applied in terms of stakeholders and BI. This is complemented by the concepts of VN, Business Models (BM), and Business Policies (BP), all being applied to describe primary facets of each scenario in a comparable manner.

3.3.1 Stakeholder

Stakeholders include individuals, group of people or organizations with an interest in the entity (here: scenario) under consideration. The interest can have economic stakes - monetary and non-monetary - and/ or are affected by the actions taken within the scope of the entity. The stakeholders are the potential beneficiaries or risk bearers of the entity being analyzed. For example, end-user (or referred to as user), service provider are some of the stakeholders.

The scenarios mentioned in Table 4 have some common stakeholders. Thus, those are defined below. Major scenario-specific details of stakeholder are available in Section 4.

- **End-user** is the consumer of the service/ resource. In most cases end-user are dependent on other stakeholders for the service he requires and in exchange provides monetary benefits to the provider of the service.
- **Infrastructure Provider (IFP)** provides infrastructure for fulfilling the requirements of deploying the service. Caching space, connectivity infrastructure, and physical resources can be counted as some of the infrastructure such a stockholder can provide.
- **Operator** is a stakeholder who is responsible for operating the service, managing infrastructure, and successfully achieving the set of business objectives.
- **Legal and Regulative Bodies** are responsible for regulating any illegal activities and stating legal requirements for any monitoring/profiling methodology. In general, these bodies create, limit, and allocate responsibility for another stakeholders. The policies, the acts, and the mandates generated by these bodies can have considerable impact on the economic and business evaluation of the scenario.

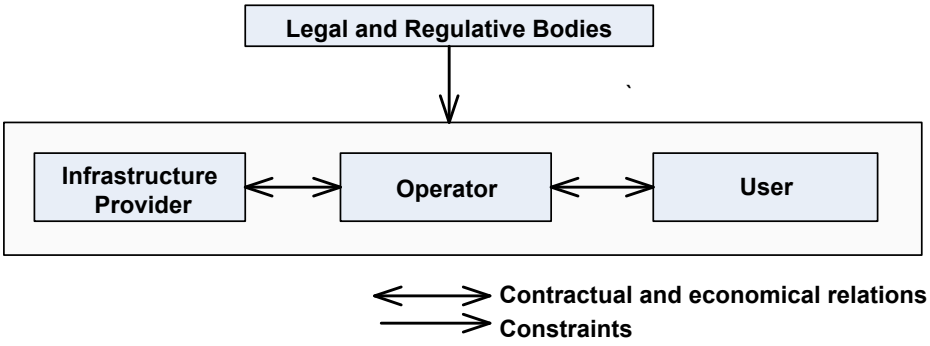

Figure 3: Blueprint for Stakeholder Identification and Relations

Stakeholders have contractual and economical interrelations, are bounded by the factors imposed, and governed by legal as well as regulative bodies (cf. Figure 3). These common stakeholders can be instantiated to identify scenario-specific stakeholders along with their specific interrelations. In order to identify the interrelations a VN is used as explained in Section 3.3.4.

3.3.2 Service Level Agreement

An important facet for IT services is the set of QoS guarantees a service provider gives. This is a part of Service Level Agreement (SLA). The aim is to make the control options transparent to user by including performance guarantees such as latency, reaction time, and speed. SLAs also include penalties in case of non-fulfillment of the promises/guarantees from the device providers.

3.3.3 Business Model

A Business Model (BM) indicates the way value (monetary and non-monetary benefits) is being generated in the market. 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 4 [19]. 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.

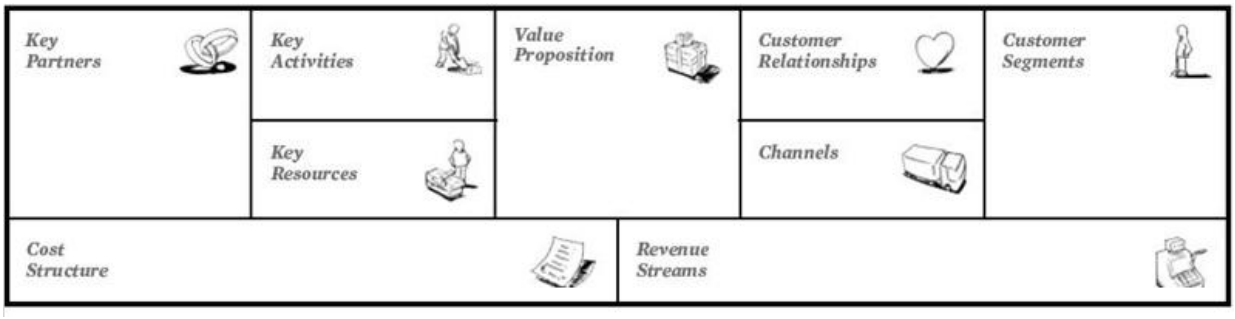

Figure 4: Business Model Canvas [19]

3.3.4 Value Network

A Value Network (VN) indicates how a value is exchanged between involved business actors. 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 VN is shown in Figure 5. Those VNs developed for each of the scenarios concentrate on streams of legal implications, tussles, and incentives of the players.

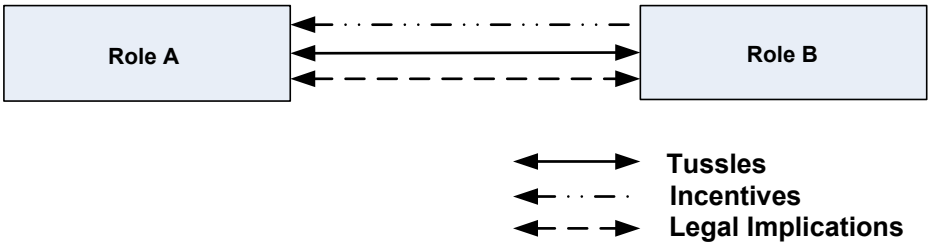

Figure 5: Template for Value Network

3.3.5 Business Indicators

Business Indicators (BI) are the prime instruments for measuring or quantifying the progress or how well a scenario is meeting its goals. It may include monetary and non-monetary aspects.

The goal behind identifying BIs for each scenario is to describe each scenario from the business perspective. This will help to model each scenario in a context where a service provider is delivering services to customers. In this context, clear goals must be set for each scenario that reflect what they are addressing to achieve, improve, and optimize. Every scenario identifies parameters and data, which can be collected from operations or behavior of their scenario. This data will define input for formulas that will be used to compute the magnitude of BIs. Each formula will link BIs with scenario operation data that have direct impact on them.

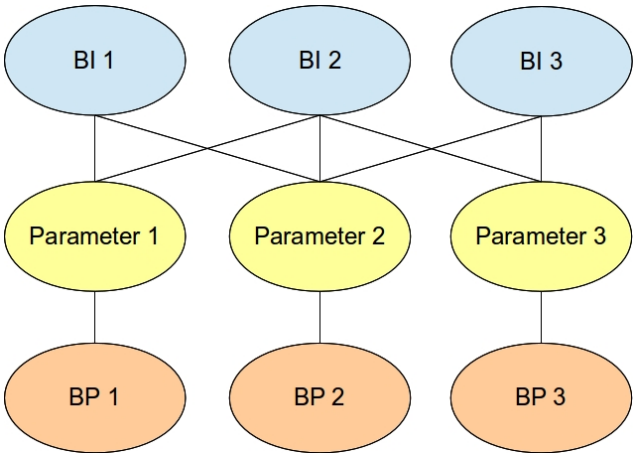

Figure 6: Relation BIs-Parameters-BPs

3.3.6 Business Policies

The process of identifying BPs will follow a refinement process proposed in reference [22] that first associates high level goals to high level policies and based on these policies hierarchy for policy are defined. Once business goals have been defined for the purpose of identifying BIs, high level policies can be linked to these goals. After these high level policies are identified, these can be refined defining policies for each function the system performs. Each function of the system may have a set of software modules corresponding to it, for whose a policy will be created in the policy hierarchy. Each sub-function of a module will also show a policy corresponding to it. This process will continue until only single parameters are handled by one policy. These lowest level policies have to be unambiguous, need to being capable of being executed automatically, and must be enforceable in the implementation of system.

The relation between BIs, parameters, and BPs can be seen in Figure 6. Each BI is related to some parameters that serve as input for their formulas so that BIs can be computed. These parameters are affected by BPs that control the behavior of each scenario so target values of BIs can be obtained. One example of this relations can be taken from reference [20], where a service provider is trying to provide QoS to its users, so it is necessary to implement some kind of access control to services. Losses due to invocation rejection BI is identified that would measure the losses that the operator will suffer every time a user cannot access services. The data collected from the network operation that have direct impact on this BI is the number of accepted and rejected users into the network. This data would then become parameters in the BI formula. The number of accepted and rejected users is affected by a policy that decides to reject new users into the network when a threshold is crossed, that indicates the ”safe” amount of used network resources that guarantees a certain level of QoS to users.

4 Scenarios

As discussed in Section 2.3 the set of nine WP7 scenarios form the basis for the detailed analysis of those under the economic, legal, and regulatory constraints by applying the concepts and methodology as defined in Section 3. These scenarios map specifically to the constraints mentioned in FLAMINGO architecture and as shown in Table 5. These scenarios as per the methodology (cf. Section 2.3) also identify business indicators and value networks. This following section will discuss all nine introduced scenarios.

Table 5: Mapping of Scenarios to FLAMINGO Management Architecture

Scenarios	**Acronym**	**Economic Constraints**	**Legal and Regulative Constraints**
Virtual Network Embedding	iMinds-UPC-NetVirt	Incentives and tussles	Contractual Relations
Quality Improvement	iMinds-UT-QoS	Incentives and tussles	SLAs and QoS/QoE
Intrusion Detection Systems	UT-UniBwM-IDS	Incentives and tussles	SLAs and QoS/QoE Privacy, data protection
Cache Management	UCL-iMinds-Cache	Incentives and tussles	Privacy, copyright, data protection SLAs and QoS/QoE
Traffic Aggregates	JUB-UT-Pattern	x	x
Business Oriented Service Management	UCL-UPC-BoSM	Incentives and tussles	SLAs and QoS/QoE
SLA Fulfillment Mechanism	UZH-UniBwM-SLA	Incentives and tussles	SLAs and QoS/QoE
Protocol for Low-Power and Lossy Networks	UniBwM-JUB-RPL	x	x
VoS Concept	UZH-VoS	Incentives and tussles	SLAs and QoS/QoE Privacy, data protection

4.1 Virtual Network Embedding

This joint research activity, is a collaboration between iMinds and Universitat Politècnica de Catalunya (UPC). The work focuses on virtual network embedding. In virtual network embedding a Virtual Network Provider (VNP) acts as a mediator between Service Providers (SP) and IFP. Virtual network requests are launched by the service providers and requests containing requirements on node and link capacities. SPs target to receive a virtual network, fulfilling the request that minimizes the embedding costs. The VNP reserves substrate resources from the IFP to be able to embed the virtual networks.

FLAMINGO considers two stages of the problem, namely VNE and dynamic resource allocation. The first stage - VNE - involves embedding of virtual networks onto a substrate network (SN) and is initiated by a SP specifying resource requirements for both nodes and links to the VNP, who forwards them to the IFP. The specification of virtual network resource requirements can be represented by a weighted undirected graph denoted by $\hat{G}_v = (\hat{N}_v, \hat{L}_v)$, where $\hat{N}_v$ and $\hat{L}_v$ represent the sets of virtual nodes and links respectively. Each virtual link $\hat{l}_{ij} \in \hat{L}_v$ connecting the virtual nodes i and j has a maximum delay $\hat{D}_{ij}$ and bandwidth (data rate) $\hat{B}_{uv}$, while each virtual node $i \in \hat{N}_v$ has a queue size[1] $\hat{Q}_i$ and a location $\hat{L}_i(x, y)$ as well a constraint on its location $\Delta\hat{L}_i(\Delta x, \Delta y)$, which specifies the maximum allowed deviation for each of its x and y coordinates. In the same way, a SN can be modeled as an undirected graph denoted by $G_s = (N_s, L_s)$, where N_s and L_s represent the sets of substrate nodes and links, respectively. Each substrate link $l_{uv} \in L_s$ connecting the substrate nodes u and v has a delay D_{uv} and a bandwidth B_{uv}, while each substrate node $u \in N_s$ has queue size Q_u and a location $L_u(x, y)$.

The VNE problem involves the mapping of each virtual node $i \in \hat{N}_v$ to one of the possible substrate nodes with in the set $\Theta(i)$. $\Theta(i)$ is defined as a set of all substrate nodes $u \in N_s$ that have enough *available queue size* and are *located* within the maximum allowed deviation $\Delta\hat{L}_i(\Delta x, \Delta y)$ of the virtual node i. For a successful mapping, each virtual node must be mapped and any given substrate node can map at most one virtual node from the same request. Similarly, all the virtual links have to be mapped to one or more substrate links connecting the nodes to which the virtual nodes at its ends have been mapped. Each of the substrate links must have a sufficient data rate to support the virtual link. In addition, the total delay of all the substrate links used to map a given virtual link must not exceed the maximum delay specified by the virtual link.

The second stage follows a successful embedding of each virtual network, in which case the resources allocated/reserved for an embedded virtual network should be managed to ensure optimal utilization of overall SN resources. User traffic could take the form of packets being transmitted over the network. By monitoring actual use the resources allocated to a virtual network are then dynamically managed. However, this is performed carefully to ensure that quality of service parameters such as packet drop rate and delay for the virtual networks are not affected.

The contributions of this research are two-fold: First, it is noted that most current virtual network embedding algorithms are centralized [9]. Due to the hardness of the embedding problem, heuristics had to be developed to be able to achieve an embedding solution in a scalable way. Even for the available distributed solutions, there are strong constraints on the complexity of the problem that can be solved. Therefore, the goal is to develop a hybrid solution that would take advantage of both a centralized as well as distributed approach. The aim is to be able to scalably establish virtual networks with a high complexity, which is induced by a high number of considered resource characteristics.

In addition, current embedding solutions are based on the resource capacities requested by the service providers. Actual load will however vary over time, leading to situations where a lot of substrate resources remain unused [9]. Thus, the second target is to design and evaluate a learning-based dynamic embedding algorithm, able to dynamically adapt the embedding solution to the actual demands, and perceived by network monitoring. This will optimize substrate resource usage and increase the acceptance rate of virtual network requests.

[1] The queue size is a measure of the maximum number of packets (or Bytes) a given node can have in its buffer before dropping packets.

4.1.1 Economic and Legal Constraints

Figure 7 illustrates the BM for the VNP as described in Section 3.3.3. Three main stakeholders can be identified in this case:

- **SP** offers service to the end-user. They request virtual networks with performance guarantees to be able to optimize the quality of the delivered service.
- **VNP** embeds the virtual network requests in the substrate network. They try to find embedding solutions that minimize the embedding costs.
- **IFP** leases physical resources of the substrate network infrastructure to the network virtualization provider.
- **Regulator** monitors the privacy breach, which can be caused due monitoring of user traffic by other stakeholders.

Goals	
Service Providers request virtual networks to the Network Virtualization Provider. These requests are embedded at Substrate resources while minimizing costs	
Methods to Achieve Goal(s)	**Customers**
Find an optimal network embedding solution in a distributed way. Dynamically adapt the solution to the actual demands, perceived by network monitoring	Service providers requesting virtual networks. The service providers are charged on a pay-by-use basis
Costs	**Revenue**
Substrate network resource reservation cost. Management costs.	Pay-by-use charges by the service providers, who are interested in getting the cheapest virtual network embedding, while fulfilling the demanded performance.

Figure 7: BM for the Virtual Network Provider.

Figure 8 illustrates the VN that shows economic and legal constraints. Economic tussles are identified amongst the above mentioned stakeholders. The service providers will target the cheapest embedding solution, while the infrastructure provider will prefer an embedding, which balances the load on the substrate network. The VNP will act as a mediator, trying to maximize its own revenue.

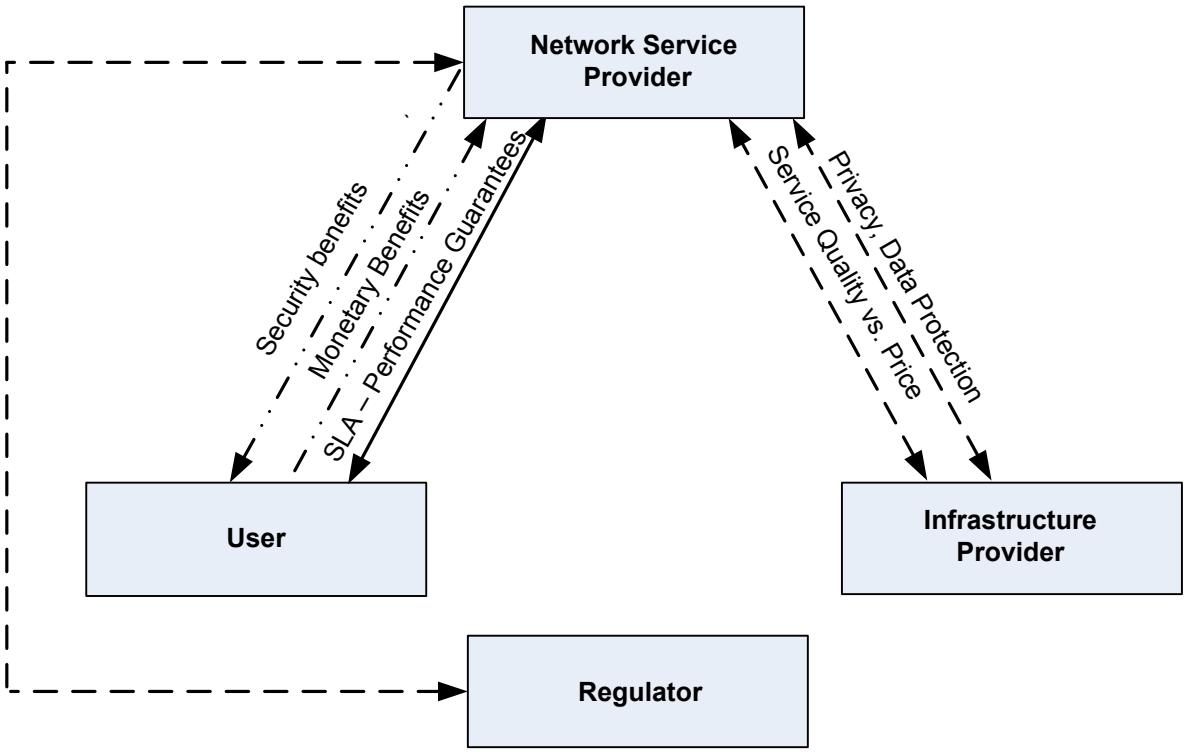

Figure 8: VN for the Network Virtualization Provider.

From a legal perspective, two relationships can be identified for the NVE use-case: First, SLA is required to guarantee the performance of the virtual networks. Penalties should be regulated in the case the VNP cannot provide the level of quality requested by the service provider. Second, since the VNP reserves substrate network resources from the infrastructure provider in order to embed the virtual networks, a SLA at this side is also needed to guarantee the availability of the requested substrate resources.

4.1.2 Business Indicators

The following section explains the BIs, which a stakeholder can measure and monitor in order to evaluate the achievement of business goals.

Infrastructure Provider BIs
The following paragraph lists the BIs from perspective of Infrastructure Provider.

Embedding Efficiency, E_{eff}
Embedding Efficiency is a measurement of how well the embedding algorithm performs. It is important since it determines how much substrate resources are used for a given embedding; and hence the resources that remain available for accepting other requests. One factor to consider for monitoring embedding efficiency is the length of a substrate path (measured in terms of number of hops) used to map a given virtual link. A substrate network that always uses the shortest paths for embedding virtual links with high bandwidth requirements results in better embedding efficiency,

and hence embeds more virtual networks, which directly results into better profitability. E_{eff} can be measured with the following formula:

$$E_{\text{eff}} = \frac{\sum_{\hat{l}_{ij} \in \hat{L}_v} \sum_{l_{uv} \in L_s} f_{l_{uv}}^{l_{ij}}}{\sum_{\hat{l}_v \in \hat{L}_v} 1}, \tag{1}$$

where $f_{l_{uv}}^{l_{ij}}$ is a binary variable which is 1 when the virtual link l_{ij} uses the substrate link l_{uv}. All the information needed to determine E_{eff} would be available from the VNE result.

Resource Utilisation Efficiency, U_{eff}

This BI measures proportion of total substrate node and link resources that are occupied at any time. A substrate network whose resource utilization is almost to full capacity would be more profitable. For defining formula of U_{eff} link and node resource utilization are first defined as:

$$\text{Link utilisation efficiency}, L_U = \frac{\text{Utilized substrate link resources}}{\text{Total substrate link resources}} = \frac{\sum_{l_{uv} \in L_s} B_{l_{uv}} - A_{uv}^B}{\sum_{l_{uv} \in L_s} B_{l_{uv}}} \tag{2}$$

$$\text{Node Utilisation efficiency}, N_U = \frac{\text{Utilized substrate node resources}}{\text{Total substrate node resources}} = \frac{\sum_{u \in N_s} Q_u - A_u^Q}{\sum_{u \in N_s} Q_u} \tag{3}$$

For equations (2) and (3), A_{uv}^B and A_u^Q are the available capacities of a substrate link and substrate node respectively:

$$A_{uv}^B = B_{uv} - \sum_{\hat{l}_{ij} \in L_{uv}^{ij}} B_{l_{ij}}^*, \tag{4}$$

where $B_{l_{ij}}^*$ is the bandwidth allocated to virtual link $\hat{l}_{ij}$ and L_{uv}^{ij} is the set of all virtual links embedded onto the substrate link l_{uv}.

$$A_u^Q = Q_u - \sum_{\hat{i} \in N_u^i} Q_i^*, \tag{5}$$

where Q_i^* is the queue size allocated to virtual node $\hat{i}$ and N_u^i is the set of all virtual nodes embedded onto the substrate node u. Hence, U_{eff} can be defined as:

$$U_{\text{eff}} = \frac{\lambda \times L_U + \mu \times N_U}{2}, \tag{6}$$

where λ and μ are constants that can be used to make one of the resources more important than the other.

Losses due to VNR Blocking, L_B

L_B signifies the number of virtual network requests that are rejected by the substrate network due to substrate resource constraints. It is a measurement of the revenue that the infrastructure provider loses by failing to embed virtual network requests. This factor is important in two ways: First, it directly affects the income of the infrastructure provider, and second, continuously rejecting

virtual network requests could have a negative impact on the good will of the resource provider. The measurement formula is given by:

$$L_B = \Upsilon \times \Big(\text{Total Requests} - \text{Accepted Requests}\Big), \tag{7}$$

where Υ is the average income earned from a successfully embedded virtual network.

Losses due to QoS violation

This BI signifies deviation of quality of service parameters (data rate and link delay) with respect to the values specified in the virtual network request. It is also important in two ways: First, it directly affects the income of the infrastructure provider, and second, continuously violating the QoS parameters in a SLA could have a negative impact on the good will of the resource provider. In order to determine this BI, the networks are monitored, recording the link delays, packet drops, and virtual and substrate network resource utilization. Specifically, the losses due to QoS violation is dependent on the percentage resource allocation R_a, the percentage resource utilization R_u, the link delay $\hat{D}_{ij}$ in case of $l_{ij} \in L_v$ and the number of dropped packets $\hat{P}_i$ in the case of $i \in N_v$. the losses into two parts: one representing the loss due to a violation of a threshold node packet loss, QoS_N and the loss due to a violation of a threshold link delay, QoS_L. The measurement formula is given by:

$$QoS_N = \begin{cases} \sigma_1 & \text{if } R_a \leq 0.25 \\ \nu_1 R_u - \kappa_1 \hat{P}_i & otherwise \end{cases} \tag{8}$$

$$QoS_L = \begin{cases} \sigma_2 & \text{if } R_a \leq 0.25 \\ \nu_2 R_u - \kappa_2 \hat{D}_{ij} & otherwise \end{cases} \tag{9}$$

Where ν_1, ν_2, κ_1, κ_2, σ_1, and σ_2 are constants. The values these constants take depends completely on the goals of the infrastructure provider and do not have a defined range.

Service Provider BIs

The following paragraph lists the BIs from perspective of Service Provider.

Embedding Cost, E_c

E_c is the total amount of money that a virtual network pays to the substrate network after a successful embedding. It directly affects the profitability of a service provider as a high embedding cost would negatively affect its bottom line. This depends on the size of the virtual network, i.e. number of links and nodes. The measurement formula is given by:

$$E_c = \sum_{\hat{i} \in N_v} \alpha Q_i + \sum_{\hat{l}_{ij} \in L_v} \beta B_{ij}, \tag{10}$$

where α and β are the unit costs of substrate node and link resources. High embedding costs for a virtual network would negatively impact on profitability.

4.2 Quality Improvement

For quality improvement following scenario is investigated.

Flow-Based Traffic Measurement for In-Network Video Quality Adaptation is a joint research activity, between University of Twente (UT) and iMinds. It combines the expertise of UT on flow-based network management with the efforts of iMinds concerning in-network quality adaptation. Flow-based network measurement allows classifying and quantifying the different cross traffic flows in a scalable way in comparison with packet-based techniques [24, 25]. Hyper-text Transfer Protocol Adaptive Streaming (HAS) services allow the quality of streaming video to be automatically adapted by the client application in face of network and device dynamics. A major obstacle for deploying HAS in managed networks, is the purely client-driven design of current HAS approaches, which leads to excessive quality oscillations, globally suboptimal behavior, and the inability to enforce management policies. Therefore, this research aims to tackle these challenges and facilitate the adoption of HAS in managed networks by combining flow-based measurements and in-network quality control for HAS. Figure 9 shows how the in-network quality decision works: First, the available bandwidth for HAS on each link is estimated by using flow-based traffic measurement classifying the different cross-traffic flows and quantifying their bandwidth consumption. Second, each HAS session is assigned a quality level based on the number of sessions crossing each links and the residual bandwidth for that link. Third, the quality selection is enforced at the clients. This leads to more stable quality selections at the clients, since oscillations due to changed network environments are avoided.

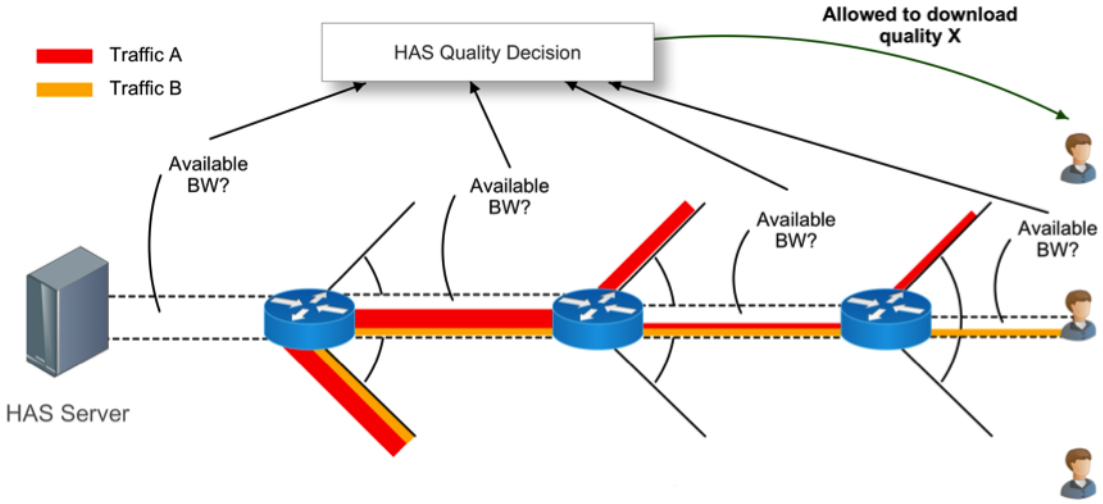

Figure 9: Flow-based Measurement for HTTP-based Adaptive Streaming.

4.2.1 Economic and Legal Constraints

Figure 10 illustrates the BM for the In-Network Quality Adaptation for HAS, as described in Section 3.3.3. Depending on the scenario setup, several stakeholders can be identified for the In-Network Quality Adaptation for HAS:

- **Network providers** offering the network/server infrastructure to be leased by a service provider or even offering the service as well.

- **Service providers** leasing network/server infrastructure and offering the service to the end-users.
- **HAS users** are the stakeholders, who use the service and benefit from the improved quality of service.

The goal of managed HAS is to optimize and assure the quality delivery on a per user basis from within the network. This allows the network/service provider to gain revenues in two ways: (1) By adapting the pricing scheme based on the service level of the users and (2) by reducing the costs by optimizing network usage. The costs consist out of several resources: Computational resources to compute the optimal quality allocations, per flow states that should be kept in memory, and content caching in intermediary proxies.

Goals	
Allow Network and Service Provider to control the delivered quality and provide more reliable service	
Methods to Achieve Goal(s)	**Customers**
Via managed HTTP Adaptive streaming Via in-network quality decision 1) Available Bandwidth for HAS estimated 2) Each HAS client is assigned quality level 3) Quality level is enforced	HAS streaming users, *e.g.,* streaming video
Costs	**Revenue**
Required computational resources, per flow state in memory, content caching in intermediary proxies add to cost	Pricing scheme based on service level of users. Internet Service Provider can reduce losses by optimizing network resource usage

Figure 10: BM for the In-Network Quality Adaptation for HAS

Figure 11 illustrates the VN modeling the constraints from both a legal and economic perspective as described in Section 3.3.4. From a legal point of view, multiple relationships can be identified. First, a SLA is required to capture the performance guarantees of the service. Second, privacy issues and time to live constraints should be dealt with, when caching the adaptive video streaming segments in the network as the law states that service providers should merely transfer the data and, therefore, is not allowed to process the data [7, 8]. Furthermore, copyright issues can arise when the network/service provider obtains content from a data owner without taking proper measures.

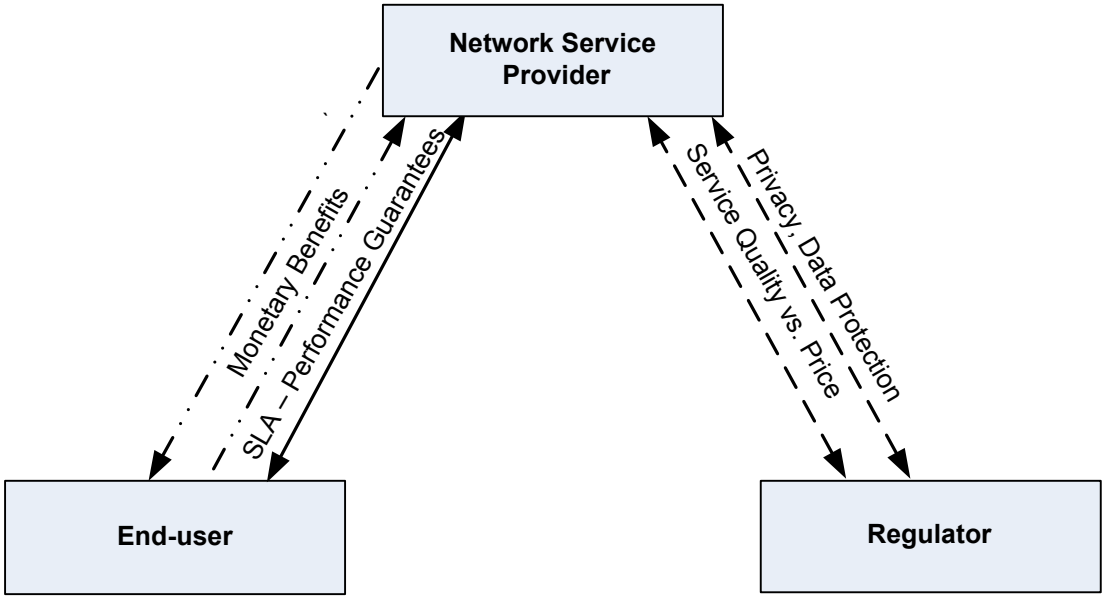

Figure 11: VN for the In-Network Quality Adaptation for HAS

At the economic side price negotiations between the network/service providers are needed to handle dynamic needs towards the infrastructure. Second, an equilibrium needs to be established between the offered quality and the price the user is willing to pay for this level of service.

4.2.2 Business Indicators

The following business indicators and measurements apply to the scenarios described in 4.2. The overall goal is to improve the user satisfaction and minimize the service provider losses due to service degradation/rejection.

User satisfaction
User satisfaction provides an indication of the streaming quality observed by active streaming sessions. The user satisfaction provides valuable information to the service provider concerning the offered service. This information can be used to improve customer retention when linking user satisfaction to customer churn. For HAS this quality is mainly impacted by:

- **Startup delay** in case of a channel switch or service startup, how long does it take before the video starts playing out?
- **Quality rate** since there are a number of quality levels between which the clients can switch, what is the average quality rate?
- **Buffer starvations** if switching to a lower quality is not sufficient to assure video delivery, the buffer can deplete, causing frame freezes, what is the average length of them and how frequent do they occur?
- **Quality switches** switching quality has a negative impact on observed quality by the end-user, what is the switching frequency?

Optimizing each of these impact factors, allows optimizing the overall streaming quality. The overall user satisfaction can objectively be measured using a combination of the aforementioned components:

$$\begin{aligned} UserSatisfaction =& a * \overline{QualityRate} - b * \overline{BufferStarvations} \\ & - c * \frac{1}{|BufferStarvations|} - d * \delta_{QualityRate} \\ & - e * \frac{1}{|QualitySwitches|} - f * \overline{StartupDelay} + g \end{aligned} \tag{11}$$

Where a, b, c, d, e, f, and g are tuneable parameters and $QualityRate \in [0, rate_{max}]$, $BufferStarvations \in [0, length_{video}]$, $QualitySwitches \in [0, |segments_{video}|]$ and $StartupDelay \in [0, ...]$.[2]

Service Provider losses due to service degradation
It provides an indication of the projected losses due to the degradation experienced by active connections during congestion situations, in terms of offered quality rate with respect to the ones specified in the SLA's. If s_i is the quality specified in the SLA for client i and a_i is the quality that is actually achieved for client i, the following formula is used:

$$loss_{PerfDegrad} = \sum_i f(s_i, a_i), \tag{12}$$

where f is a function modeling the impact of SLA-violation on a per client basis.

Service Provider losses due to service rejection
When too many users are using the video streaming service and the framework can no longer guarantee the delivery of the lowest quality to each user, the network will need to reject a number of service requests. This will result into operator losses and possible increased customer churn, which can be calculated by

$$loss_{InvRejct} = \frac{|rejctUsr|}{|rejctUsr| + |accptUsr|} \tag{13}$$

If $BottlneckBW$ is the maximum achievable throuhgput through the bottleneck and $Qlowest$ is the bit rate of the lowest quality representation, the number of $accptUsr$ is at most $BottlneckBW/Qlowest$, where

$$loss_{InvRejct} = 1 - \frac{BottlneckBW}{Qlowest * TotalUsr} \tag{14}$$

4.3 Intrusion Detection Systems

This joint research activity, is a collaboration between UT and UniBwM. Intrusion detection is nowadays commonly performed in an automated fashion by IDS [23]. Several classifications for IDSs are common. One of these classifications focuses on the kind of data that is used for performing intrusion detection. The first class of IDSs mainly uses packet headers (flows) for intrusion detection. While these flow-based IDSs have a high-performance and are usually little privacy-intrusive, they are typically affected by a high number of undetected attacks (false negatives; see Figure 12).

[2] Recently, these functions have been specified by some authors, but the application of them is sometimes limited to a particular scenario/setting. Therefore, we have not included the specific values, but rather indicated how they impact user satisfaction.

In contrast to flow-based IDSs, payload-based IDSs are capable of performing extensive layer-7-detection (and, therefore, have a lower false negative rate), but to the prize of a much higher system requirements as well as a violation of privacy issues [12].

Given these observations, performing intrusion detection in high-speed networks is a challenging task. While many payload-based IDSs are working well at the backend of service provider networks, the backbone is often characterized by communication links with high-speed connections and thus requires well equipped IDS in order to be capable of handling 100 Gbps or more, for example [11]. Within this collaboration it is planned to create a framework for distributed intrusion detection in high-speed networks by combining especially flow-based and payload-based intrusion detection. As already stated, in addition to monetary aspects, legal issues in general, and privacy issues in particular are also important reasons, why payload-based IDS are rarely deployed in high-speed networks today [12].

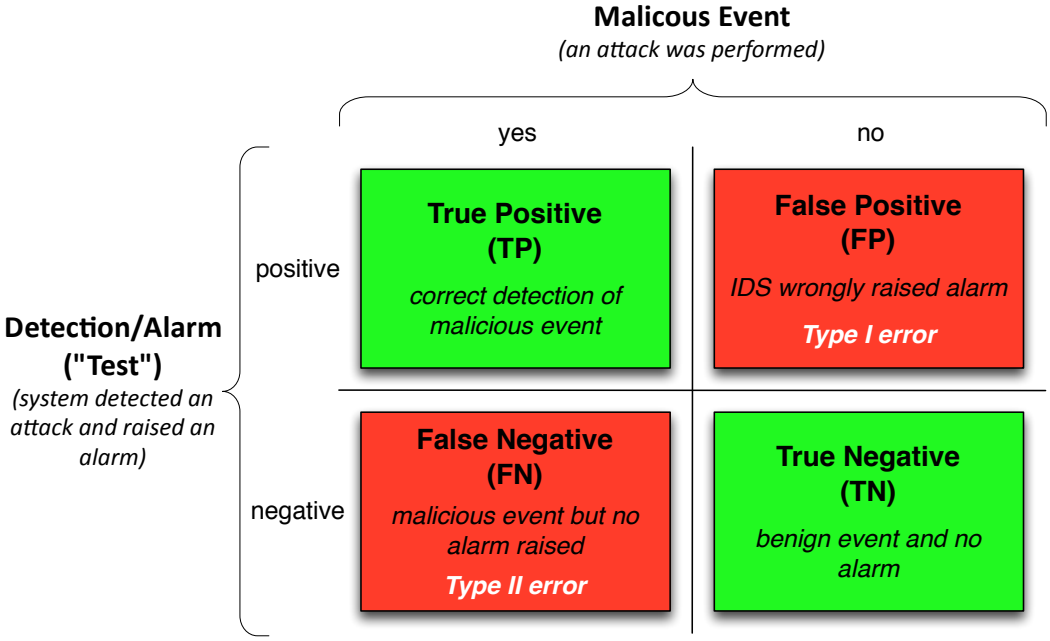

Figure 12: Categories of Alarms “Confusion Matrix”)

In order to overcome the mentioned disadvantages, this collaboration tries to make use of both approaches (both flow-based and payload-based intrusion detection) in a multi-layered approach. As depicted in Figure 13, the approach is centered around the ideas that (i) the first layer comprises flow-based intrusion detection, which performs detection based on the entire packet stream (100%) and that (ii) depending on the result of the flow-based detection, the payload-based IDS is activated for a certain period of time to investigate the anomaly of the flow-based IDS in more detail (1%) - in order to verify or falsify the result of the flow-based IDS. As network attacks can last shortly and a switch has to be made from flow-based to packet-based detection, detection has to be performed in real-time.

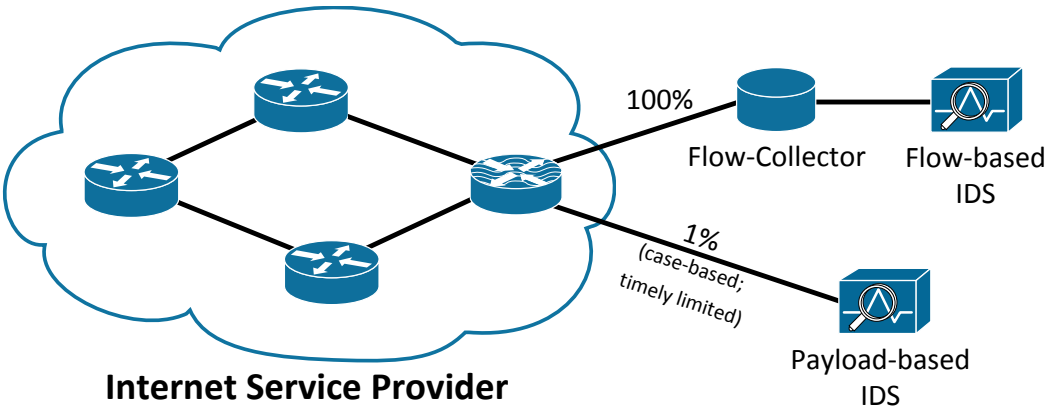

Figure 13: Simplified Scenario

4.3.1 Economic and Legal Constraints

Figure 14 illustrates the BM for the Infrastructure Provider, whereas Figure 15 illustrates the corresponding VN. The following roles can be identified for the involved stakeholders:

- **Network Service Provider** are owner and operator of the high speed network, the corresponding sensors, and the IDSs.
- **End-user** uses network of a service provider.
- **Regulator** is the body that provides legal requirements and mandates to restrict the monitoring of flow-based or packet based traffic in order to detect intrusions.

The goal of performing intrusion detection in high-speed networks is to increase the security level of a service provider network and as a result to optimize and assure the overall service level provided to end-users. This allows the network/service provider to gain revenues in two ways: (1) By adapting the pricing scheme based on the service level, and (2) by reducing the costs by a decreased network usage.

On the economic side, security improvements will be the main driver. Together with performance improvements of the network, this allows for better SLAs and, therefore, generates higher monetary benefits for the service provider. In addition, the service provider's costs are reduced since less expensive hardware is needed for performing intrusion detection based on our approach. Also the legal situation is considered in a better way.

The legal and the regulative constraints in terms of how and which parameters within the packet can be monitored in order to detect attacks restricts the efficiency of IDS. Therefore, the laws that are country specific, and/or partially region specific have to be studied and analyzed in future, to answer such questions.

Goals	
Allow High-Speed Network Operators/Providers to perform an Intrusion Detection at lower costs and without a violation of privacy and legal issues	
Methods to Achieve Goal(s)	**Customers**
Via a multilayered combination of flow-based and packet-based IDSs	Big national and international Service Providers
Costs	**Revenue**
Marginal/significantly lower than the current state of the art, since a high speed packet-based intrusion detection is relatively cost intensive	Internet Service Provider can: - increase the security level of the network -> advertisement - reduce losses by optimizing network resource usage

Figure 14: BM for the operator of a high-speed network implementing the multilayered IDS.

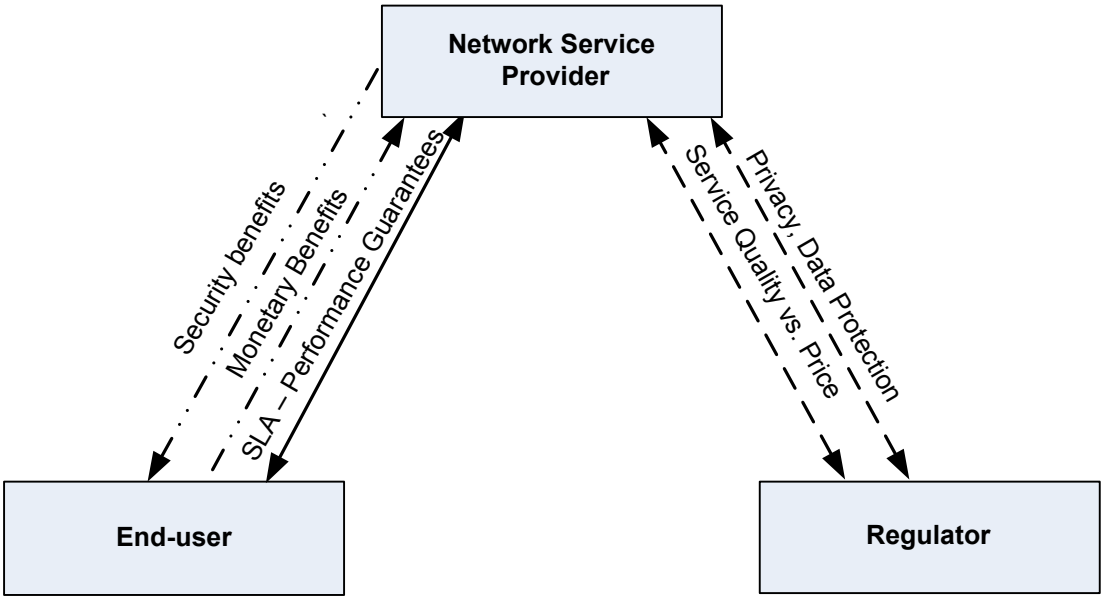

Figure 15: VN for the operator of a high-speed network implementing the multilayered IDS.

4.3.2 Business Indicators

Following three business indicators have been identified:

Network uptime: How much time has the service provider network been online? In situations where anomalies are not detected timely, the service provider network may suffer from downtime due to overload by an attack, for example.

QoS: Service provider networks may suffer from QoS degradations in case of an anomaly. This may be the case when an anomaly is causing the service provider's access link to be overloaded, for example. QoS provides an indication of the network quality observed by customers (QoE).

Quality vs. price: A higher network uptime and QoS may improve user satisfaction in case the SLAs and monetary agreements remain the same.

For metrics on how to measure QoS, QoE and Quality vs. price see Section 4.9.

4.4 Cache Management

In this joint research activity, University College of London (UCL) and iMinds are investigating a scenario where ISPs operate a small-scale content delivery network service by maintaining their own caching points in the network [16]. The work focuses on a dynamic cache management approach where ISPs, by controlling the placement of content items in the network, can have more control over their resources. Current content delivery services operated by large Content Distribution Network (CDN) providers can exert enormous strain on ISP networks [15]. This is mainly attributed to the fact that CDN providers control both 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) [10]. These decisions are taken without knowledge of the precise network topology and state in terms of traffic load and may result in network performance degradation.

This joint activity focuses on two goals: First, identification of dynamic cache management decisions methods, which adapt to changing content popularity and geographic location of content requests. Second, investigation of mechanisms by which the cache capacity can be dynamically adjusted so that memory resources can be flexibly allocated to multiple service providers.

4.4.1 Economic and Legal Constraints

Figure 16 illustrates the BM for the IFP, whereas Figure 17 illustrates the VN for the main stakeholders involved - Infrastructure Provider (*e.g.,* ISP), Service Provider (*e.g.,* YouTube), Content Producer (*e.g.,* WarnerBros), and Regulator. The following roles can be identified for the involved stakeholders:

- **IFP** provides caching space and connectivity infrastructure for the distribution of content to end users.
- **SPs** are players in the current content delivery chain (*e.g.,* Akamai, YouTube) which act as the original sources of content.

Goals	
Cache management to improve service provider performance and optimize infrastructure resource management	
Methods to Achieve Goal(s)	**Customers**
Considering variable cache sizes to be reserved for a service. Dynamically adjust cache sizes to perceived traffic patterns and content popularity. Dynamically move content to best location.	Service providers who gain performance and are able to increase QoS. Infrastructure providers have better management of their resources.
Costs	**Revenue**
Reservation of storage capacity. Management costs.	Pay-by-use charges by the service provider.

Figure 16: BM for the Cache Management Provider.

- **Content Producers** are the producers and legal owners of digital content.
- **Regulator** is responsible for monitoring the violation of privacy and copyrights in the distribution of protected content.

From a legal perspective SLAs between the IFP and SP need to be established to regulate the reservation of caching capacity and to guarantee relevant performance metrics. Furthermore, copyright infringements need to be regulated in cases where cached content items are protected by the Content Producer. Copyrights are regulated so that content is only consumed by customers registered for specific services associated with that content (as opposed to illegal p2p content distribution). These copyright issues are unchanged with respect to the current single provider use case.

On the economic side, price negotiations will be required between the IFP and the SP. Both storage reservation costs and the cost for providing a specified level of performance have to be agreed between these two actors.

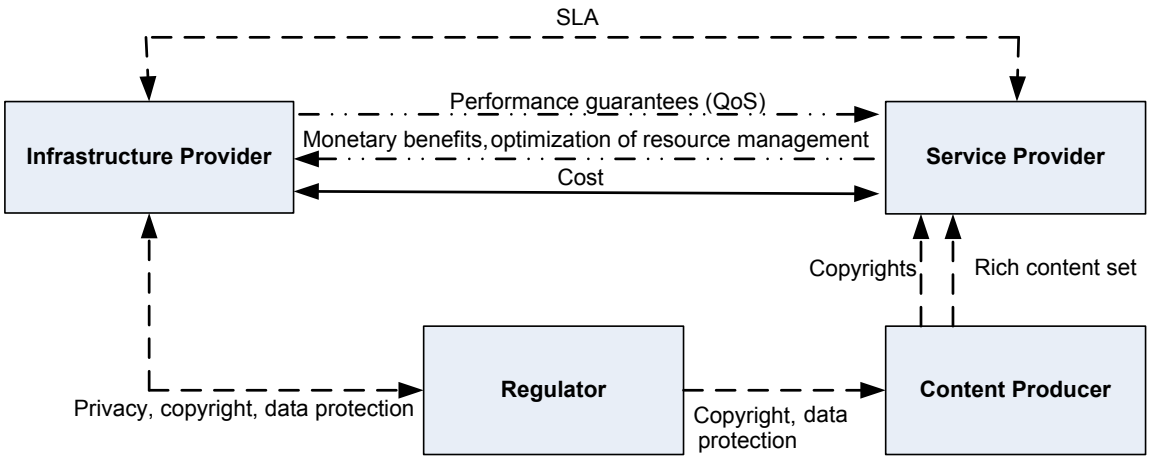

Figure 17: VN for the Cache Management Provider.

4.4.2 Business Indicators

The BI considered in the cache management scenario is the QoE with respect to the delay between requesting a content and consuming it. Due to resource constraints only a subset of all available contents can be accommodated in the caching infrastructure operated by the Internet Service Provider (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 and, as such, the QoE as perceived by the user.

In practice, it may be difficult to measure the delay in serving a content request. The value of the BI can be computed based on the volume of redirections at the network level. More specifically, in the scenario considered in this study, it is assumed that the configuration of each caching point is known by every other caching node in the network. As such, the cache manager associated with each network cache can monitor locally the number of user requests that need to be redirected to the origin servers. Upon receiving a content request, the cache manager can determine whether this can be served from within the network or not. In case the requested content is not stored in any of the network caches, the request is redirected to the origin server and a cache miss counter is incremented. In order to determine the total volume of redirections at the network level, the cache managers can collectively exchange and aggregate the values of their local counters. The total number of redirections can be used by the ISP to decide when to reconfigure its resources, i.e. when to update the placement of contents in the network. As content popularity evolves over time, interests for previously less popular contents not cached in the network may increase, and as such, it may be judicious for the ISP to cache these contents locally. In order to determine when reconfigurations are required, certain thresholds can be defined. If the volume of redirections exceeds these thresholds, then the reconfiguration process can be triggered by the ISP.

4.5 Traffic Aggregates

This joint research activity is a collaboration between UT and Jacobs University Bremen (JUB). The collaborative work investigates the extent of impact of individual Internet hosts as well as the influence of their application usage on the properties of the traffic aggregate.

It is often assumed that Internet traffic exhibits Gaussian characteristics, and this assumption has been validated in various studies of real Internet traffic. However, less is known about the aggregation requirements in order for traffic to be Gaussian. This work is based on the flow-level traffic measurements of individual hosts. The results from the investigation of individual hosts or their clusters are used to determine their impact on the aggregate traffic properties.

4.5.1 Economic and Legal Constraints

This work on the impact of individual Internet hosts as well as the influence of their application usage on the properties of the traffic aggregate has no legal or economic constraints per se. However, the work involves sensitive traffic traces that may reflect the behavior and browsing preferences of individual hosts. Despite the fact that no information about the "host-to-person" match in our traffic traces is known, it is nonetheless needed to make sure that all of the studied data resides on secure servers and that only the involved parties have access to it.

4.5.2 Business Indicators

A network flow trace contains information about data activity (*e.g.,* data packet transfers) that occurred in the monitored network. Instead of storing information about individual packets, trace data contains information about network flows. Network flow represents a sequence of packets from a source computer to a destination. It can also be viewed as an artificial logical equivalent to a call or connection. A number of characteristic properties of network traces were established over the last decade. These properties may vary, and depend on the origin environment of the trace. The goal of this activity was to get a thorough understanding of one such property - Traffic Gaussianity [17]. The outcome of the study estabished a relation of certain network trace parameters to the Gaussanity level of a traffic aggregate. No business indicators could be associated with the outcome of the study. Gained results can instead be used to further the undestanding of the aggregate traffic properties.

4.6 Business Oriented Service Management

This joint research activity, is a collaboration between UCL and UPC. There has been substantial work on mechanisms for providing some level of quality to offered services in Internet Protocol (IP) networks. However, these mostly focus on optimizing individual network-level objectives, such as resource utilization [28], in isolation. As a result, network configurations that accurately reflect multiple business-level objectives cannot be generated automatically. Motivated by the lack of such solutions, UCL and UPC collaborate in this research activity with the goal to bridge the gap between business value and configuration management in IP networks.

Previous joint work between UCL and UPC had proposed an approach to automate the generation of service management policies, based on a set of high-level business indicators (BIs) and their relationships with lower-level service management objectives and policies [21]. The focus was on static and dynamic Admission Control (AC) of service subscriptions for which the influence of BIs when generating appropriate configuration policies has been considered. This was realized by a set of mapping functions that take into account the impact of BIs over service management policies. Administrator assigned weights of importance are given to each BI and are then used to derive appropriate policy parameters.

The simple linear mapping functions between BIs and AC policies used previously [21] may not necessarily result to optimal policy parameter values. As such, the objective of this research activity is to improve the accuracy of derived configuration parameters in the face of contradictory

business objectives. This can be viewed as an optimization problem with preferences, with the latter being represented by BI weights. This work has been investigating evolutionary algorithms that are able to determine trade-offs in multi-objective environments. These will take as input the range of possible parameter values, their relationships with BIs, and BI weights - appropriate feedback will fine-tune configurable parameters. This research activity will be developing a mechanism that determines policy parameter values that best reflect business-oriented service management preferences.

4.6.1 Economic and Legal Constraints

Figure 19 illustrates the BM for the Network Provider, whereas Figure 18 illustrates the VN for the main stakeholders involved:

- **Network Provider** provides connectivity infrastructure
- **Users** are private/corporate consumers that buy connectivity services
- **Regulator** regulates the performance of offered services

  From a legal perspective SLAs between the Network Provider and Users need to be established to control the allocation of network resources and to guarantee relevant performance metrics. The Regulator monitors the performance of connectivity services and reports misalignment with respect to service pricing. On the economic side, users pay for the services they receive, but they can also receive service credits in case of SLA violations. The deployment of business-oriented admission control logic can improve the service satisfaction, thus providing incentives to new users to subscribe and existing ones to maintain their contracts.

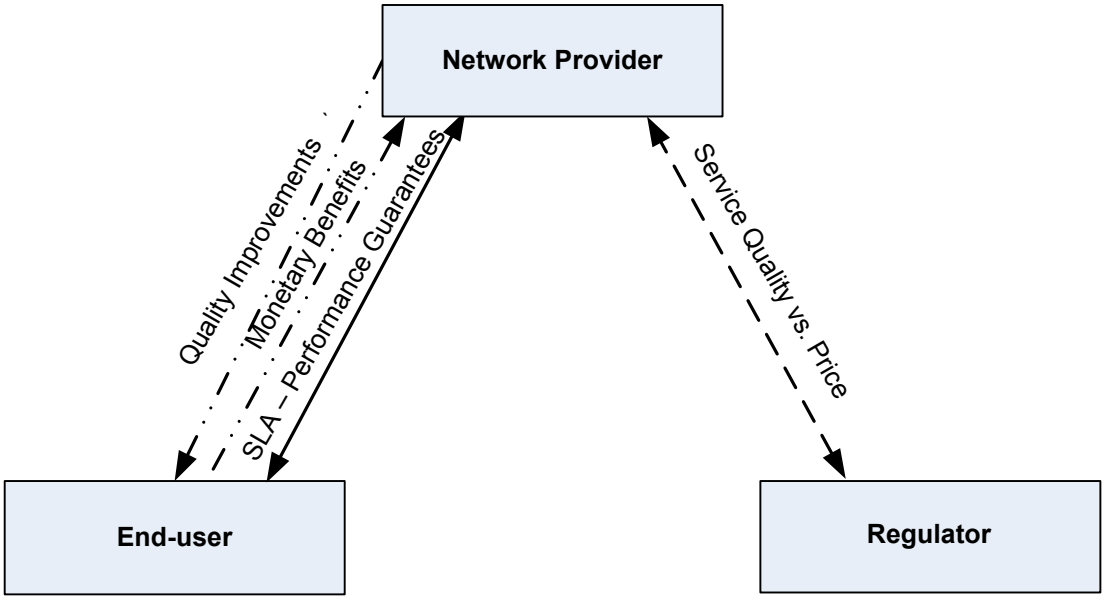

Figure 18: VN for Business Oriented Service Management.

Goals	
Mechanisms that allow Network Providers to realize their high-level objectives while satifsying contracted SLA requirements	
Methods to Achieve Goal(s)	**Customers**
Logic to enable joint optimization of multiple business/level objectives and translate those to network'	Private/corporate users of connectivity services with guarantees
Costs	**Revenue**
Admission control logic Installation on network Devices Management costs	Improved service satisfaction (can increase number of subscribed users). Less penalties imposed (reduced SLA violations)

Figure 19: BM for the Network Provider.

4.6.2 Business Indicators

BIs that are considered in this study are as follows: Potential losses due to invocation rejections, service satisfaction (SES), and potential losses due to service degradation. A description of each is provided hereafter.

Potential losses due to invocation rejections
This indicator correlates the losses of an operator with the rejections of service invocations and is linked with the access control procedure. When services are rejected the operator suffers economic penalties. Assigning the highest importance to this BI over the other indicators would imply that the operator prioritizes the acceptance of all service invocations irrespective of the network state. This could eventually result in network congestion due to an excess of active services injecting traffic to the network. Congestion would adversely affect the other two BIs described below due to the degradation of active services (poor service quality).

In order to measure this BI it should be noted that it is associated with the number of rejected services, and it is influenced by an admission control-specific threshold. When the injected traffic crosses this threshold the corrective action of rejecting new service invocations is triggered. In order to quantify the business indicator, the number of rejected services needs to be measured across all network ingress points and expressed as a fraction of the total number of services.

Potential losses due to service degradation
This indicator is correlated with the impact over the business objectives of the quality offered to services when network congestion occur. In other words, this is representative of how well the

network can cope with network congestion with regards to the quality offered to active services. Prioritizing this BI over the other two can result in scenarios where the network never gets congested. This could adversely affect the potential losses due to invocation rejections due to high service invocation rejection rates, i.e. only few active services in the network. In contrast, the SES would be favored since the few active services are more likely to be fully satisfied for most of their duration. In order to measure this BI, in should be noted that service degradation occurs when active users do not enjoy the contracted service rates and it occurs when the injected traffic exceeds the capacity for which the network was dimensioned. In such a case, corrective actions to adjust the service rates are triggered to prevent network congestion. As a result, users may experience lower service rates than the contractual ones, i.e. service degradation. This BI can be measured by computing the ratio of experienced service rates (as an average) with respect to the contracted rates.

Service satisfaction
This indicator relates to the impact over the business objectives of the quality offered to services during the life cycle of service provisioning. Prioritizing this BI over the others would imply that users enjoy their services with the highest quality during most of the time. However, this is at the expense of the number of accepted users and thus adversely affecting the potential losses due to invocation rejections. In contrast, there is a positive impact on the potential losses due to service degradation as service degradation will not likely occur.

This BI is computed in the same way as the potential losses due to service degradation, i.e. ratio of experienced service rates with respect to contracted ones, but it is measured at different timescales. In contrast to the potential losses due to service degradation, which is measured during times of potential network congestion, this indicator is measured periodically during the service lifecycle.

4.7 SLA Fulfillment Mechanism

This joint research activity, is a collaboration between University of Zurich (UZH) and UniBwM. It defines a mechanism that detects SLA violations for voice services over mobile networks. The motivation of such mechanism is the demand for an SLA violation detection solution for QoS-guaranteed voice services, as described in reference [27]. Furthermore, this joint research activity aims to determine suited actions in respect to charging when a violation is detected. Facilitating the first goal on the level of traditional circuit-switched mobile phone calls would demand insight in a Mobile Network Operator's (MNO) infrastructure. Since this is currently not possible, the decision to focus on Voice-over-IP (VoIP) services over mobile networks has been taken. To author's knowledge, nowadays there is not a QoS related metric for VoIP services over mobile networks. Thus, this work of SLA Fulfillment Mechanism aims to provide the respective metric as well as a prototype of the evaluation mechanism.

The potential of integrating with other research such as NETRADAR, which is developed at Aalto University in Finland, was examined [18]. NETRADAR focus on the QoS for data over mobile networks in general, while in this joint research activity the specific requirements of voice services are taken into consideration. There is an ongoing discussion with the NETRADAR team to define if and under which terms there is room for collaboration. In parallel with external liaisons, a VoIP server was deployed in the testbed at UZH. The server is reachable at `sip.abacusproject.eu` and is used as a VoIP infrastructure test environment. The respective Asterisk platform study period determines ongoing work to become familiar with it [3].

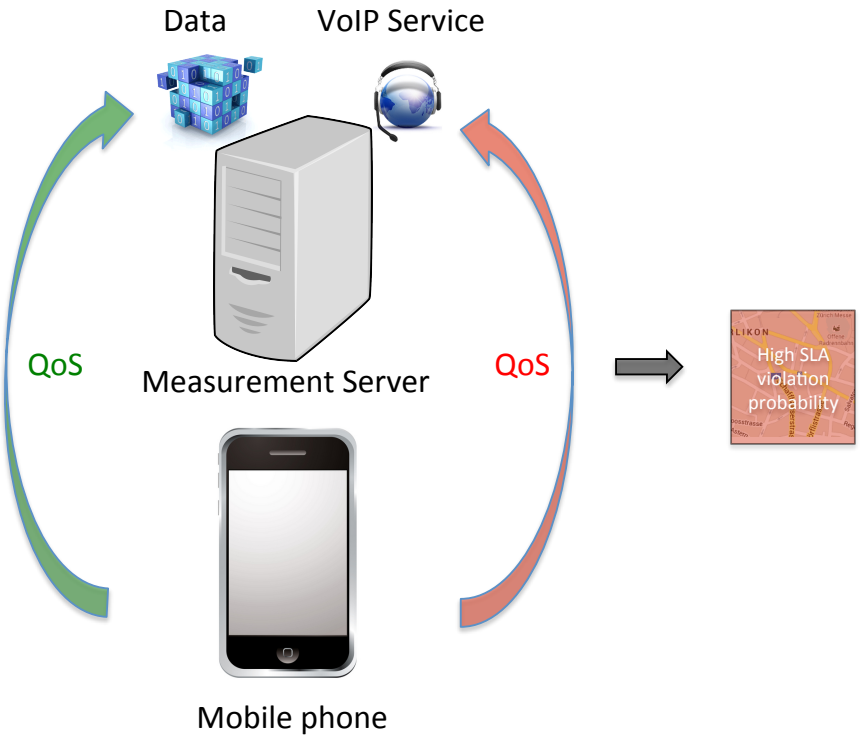

Figure 20: High SLA Violation Probability Scenario.

The formalization of the suited metric for defining the QoS of a VoIP call over a mobile network is currently an on-going work. An initial approach is to capture and analyze RTCP XR packages during a VoIP session [1]. RTCP XR packets contain useful information concerning the QoS of a VoIP call such as jitter information and the Mean Opinion Score (MOS) value [13]. However, on a mobile environment other parameters, such as the signal strength, the battery level, etc. might influence the jitter and MOS value. Thus, such parameters need to be taken in to account as well.

In case that the VoIP traffic is facing lower performance than the data traffic as shown in Figure 20, a potential SLA violation flag will be raised. The high level idea is to interpolate the results of measurements concerning generic data traffic and VoIP related traffic over mobile networks. As a final step, the visualization of real time obtained data on a map will follow. The latest will facilitate a real time overview of the MNOs SLAs violation probabilities in respect to VoIP services at a given area. An example of how the representation will look like is illustrated in Figure 21. The red color represents high probability of SLA violation while the green and the rest colors respectively lowest probabilities.

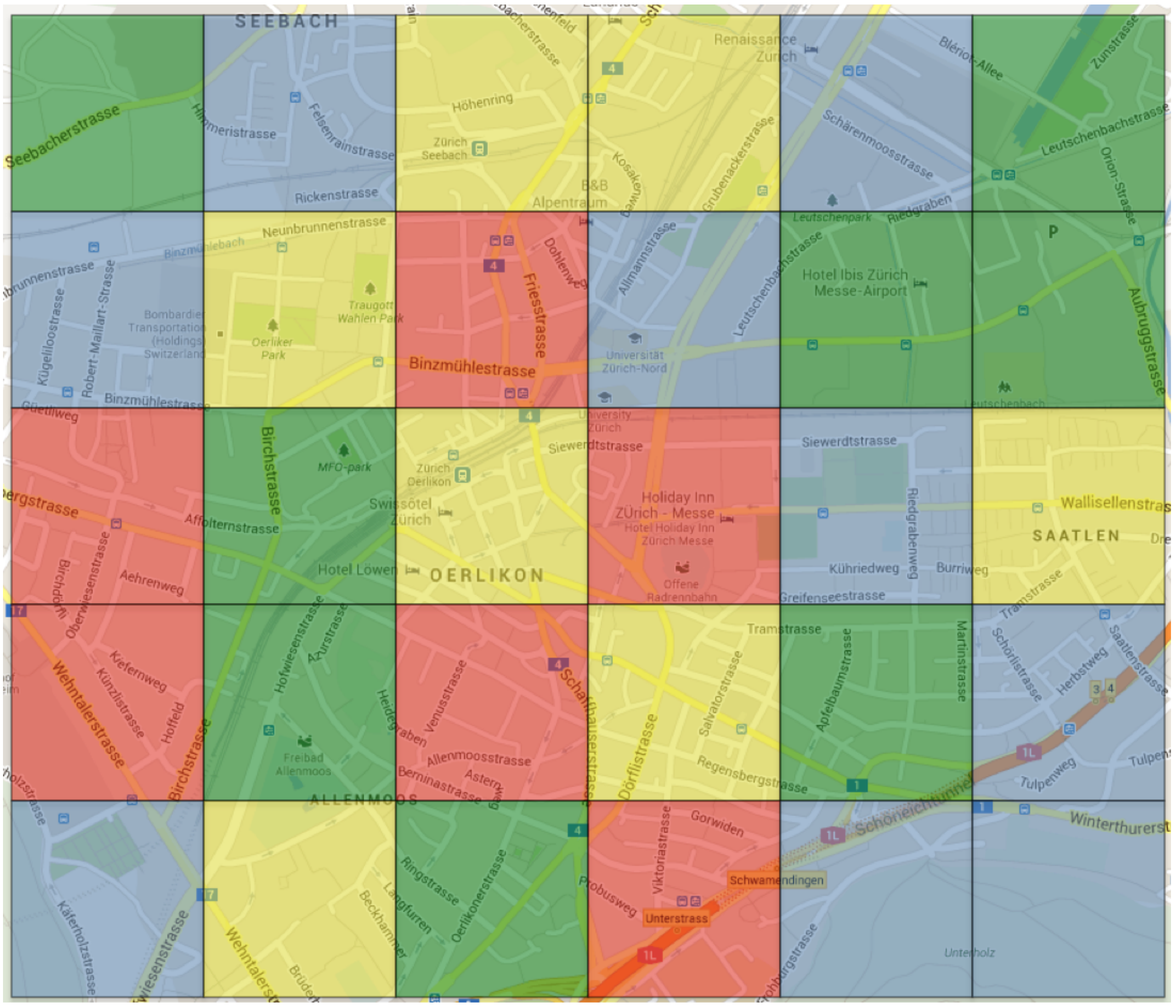

Figure 21: VoIP QoS probability on a MNO's Network.

4.7.1 Economic and Legal Constraints

Relevant stakeholders concerning the legal and economic perspective are the MNOs and the end-users. The mobile operator is responsible for the correct fulfillment of the proposed service class, which was chosen by the customer. For this reason the operator could take into account the input from the customers. For example, this mechanism provides a map with the possible service classes, which is based on the user input, the MNO can adapt his network settings to reach a better quality and therefore earn, if requested from a customer, more money. In contrast the customers could unite themselves to manipulate the provided services. If the customers from one region report low quality the MNO will reconfigure the network to ensure that all the proposed SLAs will be fulfilled and the customers can now use a lower services class, which is cheaper but with a better quality. The MNO can get a more clearly evidence about their provided service to the customer. So the operator can minimize the costs until the quality, which he proposes to the customer is served correctly. The customer instead hopes to get a better performance or a cheaper price if he reports a lower quality as proposed to the MNO. So a legal constraint in this relationship is the trustworthiness between the MNOs and the customers.

Goals	
Mechanism to identify SLA violations in MNO's voice services (offered by a third party)	
Methods to Achieve Goal(s)	**Customers**
Measure whether the quality prescribed by the SLA was reached indeed. Also take into account input from consumers	End consumer Other involved actor: Auction authority (could be regulator)
Costs	**Revenue**
- Development Cost of mechanism - Computer power at MNO environment and mobile device of customer - Additional infrastructure for hosting database with measurement data	Revenues from auction => Auction Environment: different MNO publish their prices for certain service class, auction authority chooses on behalf of the customer (this is assuming willingness to pay for premium offers)

Figure 22: BM for the SLA Fulfillment Mechanism.

The legal constraints of the SLA Fulfillment Mechanism read as follows: (1) Penalties that are applied in case of an SLA violation detection. In more detail the MNO that violates an SLA should either provide a monetary reimbursement or a discount for future demands, or being penalized by temporary exclusion in future auctions. (2) An Auction Authority (Au^2) should be responsible for the penalization in case of SLA violation detection. Thus, such authority should be trusted by the regulator of the market, MNOs and the MNO's customers. The economic constraints of the SLA Fulfillment Mechanism read as follows. (1) The MNO's customers should be aware of price discrimination according to the QoS of a service, such as additional costs for premium services. (2) MNOs should obey to any cost-related decisions of the Au^2, concerning SLA fulfillment tussles between them and their customers.

Figure 22 and Figure 23 illustrate the BM and VN as it has been described in Section 3.3.3 and 3.3.4 respectively. The value model shows that the users have to be supported to use the application, because they get an revenue only via the costs for a service in conjunction with their selected quality level and the associated quality guarantees via SLAs. The user has to be involved in the SLA fulfillment process because otherwise user would not recognize why to use and why to spend energy for the application. The revenues for the MNO could only be fulfilled if he invests in the development of the application and the additional infrastructure, which is needed for the measurement database and presentation environment.

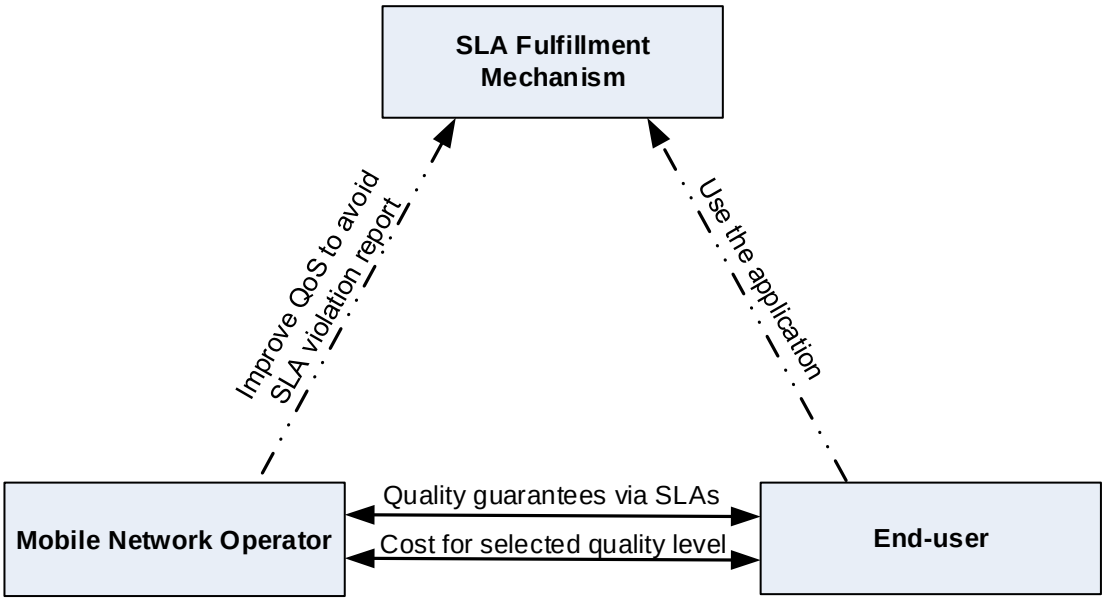

Figure 23: VN for the SLA Fulfillment Mechanism.

4.7.2 Business Indicators

Several BIs exist and are categorized based on their usage. Thus, there exist (a) visualization and localization related BIs, (b) general QoS mobile data related BIs, and (c) VoIP over mobile networks related BIs. Table 6 summarizes the set of BIs according to its category.

Visualization and Localization BI
This BI will be used to identify the location of a potential SLA violation incident for a given MNO. Such information can be used either for accounting, visualization purposes (cf. Figure 21), or by the regulator that might need to take an action in case of persistent SLA violation status of a specific MNO in a specific area.

In order to measure this BI the mobile client that will be developed during this work will collect the location of the mobile user either from the Global Positioning System (GPS) module, the network, or the Wireless Local Area Network (WLAN). The Mobile Network Operator (MNO) will also be captured.

Table 6: SLA Fulfillment Mechanism BIs List

Visualization and Localization BI	**General QoS Mobile Data BI**	**VoIP Over Mobile Networks BI**
Location •GPS •Network •WLAN MNO	**Attributes not influenced by the MNO** Speed **MNO infrastructure attributes** Signal strength **Data QoS attributes** Mobile technology •UMTS, HSPA, LTE Download speed Upload speed Latency	**MOS score** MOS-LQ MOS-CQ **Jitter information** Mean jitter Deviation of the jitter

General QoS Mobile Data BI

The general QoS mobile data BI will be used to calculate Mean Opinion Score (MOS) normalized value that represents the QoE of the mobile data service of a MNO in a given location, irrespective of the Type of Service (ToS).

For measuring this BI there are three subcategories that identify (i) parameters that the MNO cannot influence, (ii) parameters that are primarily related to the Base Station (BS) infrastructure, and (iii) parameters that have to do with general QoS in data services. In (i) the instance of the accelerometer of the device, or periodic location coordinates will identify if the user is stable. In case he is moving his average speed will be calculated if possible with the use of the location data. The mobility state of the mobile user might influence the result of his QoE since users that move with a high speed are expected to have lower QoE than a stable user, due to handover [4]. In (ii) the signal strength will be captured since this also affect the QoE in mobile data services due to the fact that when the signal is weak, several retransmission that increase the delay are required [5]. In (iii) the mobile technology that is used will be captured *e.g.,* Universal Mobile Telecommunications System (UMTS), High Speed Packet Access (HSPA), and Long Term Evolution (LTE) etc. This will define the maximum expected download and upload speed. Thus, the real download and upload speed will be captured and compared with the theoretical values. However, any restriction in bandwidth that is related with the data plan of the mobile subscriber has to be considered. This information can only be retrieved manually from the subscriber while starting the application for the first time. Last but not least the latency will be measured. The lowest the lately is the best the score will also be.

VoIP Over Mobile Networks BI

The VoIP over mobile networks BI will be used to calculate MOS-normalized value that represents the QoE of VoIP services of a MNO in a given location.

For measurement reasons the information from the RTCP XR packets will be extracted and the MOS values concerning the Listening Quality (MOS-LQ) and the Conversational Quality (MOS-CQ) will be captured [13]. The values of this parameters is between 1 and 5 with 5 to be excellent and 1 to be poor [1]. Those values will be compared with the maximum theoretical value according

to the codec that is used when the test call is performed. Finally, the last two attributes that will be considered while generating the score that will define if an SLA might be violated are the mean jitter and the standard deviation of it. The lower those values are the better a VoIP quality is [26].

There is no concrete decision yet of how each parameter will affect the final BIs. Thus, measurements in a controlled environment will be done once the BIs will be modeled in a mathematical model. During this procedure the BIs model ”calibration” will take place.

4.8 Protocol for Low-Power and Lossy Networks

Trust Computing Architecture in Routing Protocol for Low power and Lossy Networks This joint research activity, is a collaboration between the JUB and the UniBwM. Cyber Physical Systems (CPSs) are widely expected to be formed of networked resource constrained devices. In order to suit the constraints of such networks, the Internet Engineering Task Force (IETF) developed the Routing Protocol for Low power and Lossy Networks (RPL) and Low-power and Lossy Networks (LLNs) [29]. Security in CPSs is important for maintaining the integrity and privacy of data, while also improving network resiliency to attacks. Even though RPL provides support for integrity and confidentiality of messages, details regarding key management and signatures are not covered. Since complexity and size is a core concern in LLNs, off-loading the security features to a Trusted Platform Module (TPM) can make it possible to include sophisticated security provisions in an RPL implementation. This collaboration develop a mechanism to use the security mechanisms of a TPM in order to secure the communication in an RPL network.

The design of a trust establishment and key exchange mechanism around the implied trust of a TPM to provide keys for secure RPL nodes, is a main task of this research. With this approach the usage of a TPM on resource constrained devices reduces the processing load on the main processor. The goal of this examination is the prevention of the dissemination of misleading routing information, which can affect the availability of the whole network. As a next step the previous developed idea should be deployed on real hardware devices to evaluate the solution in comparison to other approaches. This is necessary to proof the existing simulation results.

Detecting and Countering RPL Destination Oriented Directed Acyclic Graph Inconsistency Attacks This joint research, is a collaboration between JUB and INRIA. The growing interest for the Internet of Things (IoT) has resulted in the large-scale deployment of LLNs, such as wireless sensor networks and home automation systems. These networks have strong constraints in terms of resources (energy, memory, power) and their communication links are currently characterized by a high loss rate and low throughput. A new routing protocol called RPL for IPv6 over Low Power, Wireless Networks (6LoWPAN) based IPv6 networks has been specifically designed by the IETF ROLL (Routing Over Low Power Lossy Networks) working group to deal with these requirements [29]. However, this protocol may be exposed to multiple security attacks that can lead to resource exhaustion or denial of service. A malicious node can also simply refuse to route messages or provide incorrect routing information data.

RPL forms a tree like topology for routing packets, which is more specifically referred to as a Destination Oriented Directed Acyclic Graph (DODAG). Loop free topologies are formed by using objective functions to optimize the rank of nodes in the network. Each node joining the network picks a parent and calculates its rank using a specified objective function. Essentially, RPL ensures that children never have ranks lower than their parents.

In order to detect any possible loops, also referred to as DODAG inconsistencies, RPL uses IPv6 header options to track the direction of the packet and any rank errors. Specifically, the O-Bit option

is used to track direction of the packet, i.e. upwards or downwards in a tree. If an upwards packet is received from a node with a rank lower than the current node, an inconsistency is detected. As such, the node will set the R-bit option, used to track rank errors, and forward the packet. If the next receiving node also detects an inconsistency in the direction of the packet, and the R-bit option is also set, this node will drop the packet and reset the trickle timers of RPL.

Such a reset of trickle timers leads to an increase in the number and frequency of control packets being sent and received in the DODAG. An attacker can create artificial DODAG inconsistencies by manipulating these IPv6 header options, thereby leading to increased overhead, denial of service and even blackhole attacks that are hard to detect.

The objective of this joint scenario is (1) to establish a state-of-the-art about security attacks against RPL networks, (2) to identify the key parameters that are required to detect these attacks, (3) develop a mitigation strategy to reduce the effect of such attacks, (4) develop a trustworthiness establishment approach for children to detect when a parent might be malicious, and (5) to experiment and evaluate the developed solutions.

4.8.1 Economic and Legal Constraints

The focus of the research on the RPL routing protocol for LLNs leads to a very general definition of possible stakeholders, which are identified in this step as the operators of the sensor network.

Trust Computing Architecture in RPL networks In the current state, the mechanisms of trust establishment and key exchange around the implied trust of a TPM do not store or monitor any data. Based on this fact there are no legal constraints to be analyzed. If in further research the monitoring and storing of data is required these constraints have to be investigated as fast as possible.

An economic contraint in this environment could be the usefulness of the security and trust mechanisms from the perspective of the customer. If he is not willing to pay more for an security aware device then it would not be produced by the manufacturers. Only in security aware environments it is conceivable that an revenue can produced by offering a trust computing architecture in an RPL network. In this case also the decrease of the energy consumption could play a role.

Detecting and Countering RPL DODAG Inconsistency Attacks Detecting DODAG inconsistency attacks does not require monitoring or storing any data that is not already part of the state maintained by the routing protocol. As such, there are no legal constraints that need to be analyzed. If the development of mitigation strategies requires monitoring or storing data, then any legal constriants posed by that situation will need to be analyzed.

Similarly, no additional economic constraints are added by the detection and mitigation approaches, since they do not utilize any new services that lead to additional costs. There are also no additional resources being utilized on the devices or within the network that may lead to an increased cost. If the further development of the mitigation strategy results in storage or transmission of extra information, then that may increase the energy consumption by a small factor. In that case, an analysis of the economic constraints will be necessary. Interestingly, mitigating DODAG inconsistency attacks can also alleviate economic constraints since the packet overhead and energy consumption during an attack can reduce as a result.

4.8.2 Business Indicators

Trust Computing Architecture in RPL networks The scenario "Trust Computing Architecture in RPL networks" has no business indicators that could be identified because there does not exist a service that can be used by others, which is the perspective of a scenario where Business Indicators make more sense.

Security in cyber-physical systems is important for maintaining the integrity and privacy of data, while also improving network resiliency to attacks. Even though RPL provides support for integrity and confidentiality of messages, details regarding key management and signatures are not covered. Since complexity and size is a core concern in LLNs, off-loading the security features to a TPM can make it possible to include sophisticated security provisions in an RPL implementation.

In this scenario we design a trust establishment and key exchange mechanism around the implied trust a TPM offers, to provide keys for secure RPL modes. Unlike other approaches, this ensures that nodes only provide keys to and use those supplied by trustworthy nodes. The only thing that comes to mind could be the 'security' which can be established, but that is not provided as a service. Also the research is at an early state where no data is monitored or stored to be able to relate this data to a BI.

Detecting and Countering RPL DODAG Inconsistency Attacks Mitigating DODAG inconsistency attacks can improve the performance of a network since it counters denial of service, packet losses, energy consumption, and overheads. However, the goal of this research is not to design a tool or system that can be used to provide a service to customers, but rather to improve the already built-in mechanisms of RPL, so as to better perform in scenarios when attacks may occur; and also to augment the protocol such that it is able to identify malicious nodes in itself.

Furthermore, it is in the interest of an operator to optimize their network and protect it against attacks that can critically bring down their network, rather than delivering this as a service to a customer. Not being a service that can be provided to clients, no specific Business Indicators can be identified.

4.9 Value-of-Service

QoS and QoE are used to describe the objective and subjective performance of an IP network. However, neither approach takes the price which has to be paid for some particular level of QoS or QoE into consideration. The VoS concept, which has been developed by UZH, fills this gap by relating metrics of the QoS and the QoE space to the price paid by the customer. It consists of a generic VoS definition and a series of VoS metrics capturing the price-performance ratio of an IP network with respect to specific QoS and QoE metrics. Thus, VoS provide a means to allow for a price-performance ratio, which enables the assessment and comparison of service delivery in IP networks.

Generic VoS Definition determines the price-performance ratio of an IP network. It consists of a set of well-defined VoS metrics capturing distinct price-performance aspects of an IP network. Each VoS metric relates a specific QoS or QoE performance aspect to a normalized price.

The above definition explains in an abstract manner what the VoS concept does and how this is accomplished. Two metric definitions are provided in the subsequent paragraph.

VoS Metrics relate metrics of the QoS or the QoE space to a price. Subsequently, the one-way delay VoS and the listening-quality MOS VoS are presented to explain how the VoS concept is applied to QoS and QoE metrics. It is conceivable though to define additional metrics for connectivity, loss, delay variation, reordering, or duplication.

One-way Delay VoS metric is based on the one-way delay metric defined by the IETF's IP Performance Metric (IPPM) working group. The working group defines the *one-way delay* metric as the time ΔT_{ow} that elapses from the point in time T when the source IP address sends the first bit of a packet and the point in time $T + \Delta T_{ow}$ when destination IP address receives the final bit of the packet. ΔT_{ow} is undefined if the packet is lost [2]. This definition can be used to define the *one-way delay VoS* as follows.

Let $\Delta T_{ow_{max}}$ be the maximum waiting time after which a packet is considered lost. The one-way delay VoS is then defined as

$$VoS_{owd} = \max(\frac{\Delta T_{ow_{max}} - \Delta T_{ow}}{p_{n_X}}, 0), \quad where \quad p_{n_X} > 0 \tag{15}$$

Due to the expression $\Delta T_{ow_{max}} - \Delta T_{ow}$, a smaller delay results in a greater VoS_{owd} value. A metric value of $\frac{\Delta T_{ow_{max}} - \Delta T_{ow}}{p_{n_X}}$ means that the packet was received and the customer is billed p_{n_X}. A metric value of zero means that the packet was lost or not received in time but the costomer is billed p_{n_X} nevertheless.

The VoS concept cannot only be applied to QoS metrics but also to QoE metrics. A frequently used means to capture the subjective performance of is the **listening-quality MOS** defined by the International Telecommunications Union - Telecommunications (ITU-T). The listening-quality MOS is determined by having test subjects rate the quality of an audio source on a scale from 1 = bad to 5 = excellent and by calculating the mean of their scores [13]. This definition can be used to define the listening-quality MOS VoS.

Let MOS_{lq} be the result of a test procedure conducted to determine the listening-quality MOS of an audio stream transferred using an IP network. The listening-quality MOS VoS is then defined as

$$VoS_{MOS_{lq}} = \frac{MOS_{lq} - 1}{p_{n_X}}, \quad where \quad p_{n_X} > 0 \tag{16}$$

$VoS_{MOS_{lq}}$ values range from 0 to $\frac{4}{p_{n_X}}$ in the worst and the best case respectively. A value of 0 means that the quality was bad, a value of $\frac{4}{p_{n_X}}$ states that the quality was excellent. The customer is billed p_{n_X} in either case.

4.9.1 Economic and Legal Constraints

The BM for the VoS concept is depicted in Figure 24. Four stakeholders can be identified for this scenario: The network provider, end-user, the measurement platform operator and the regulator.

- **Regulator** defines the framework within which network operators can provide their services.
- **Network Provider** offers network services such as DSL (Digital Subscriber Line)-, Cable-, FTTH (Fiber to the Home)-based, or mobile Internet access. It may operate its own infrastructure or use an existing infrastructure.

- **Measurement Platform Operator** runs the measurement infrastructure, collecting VoS data.
- **End-user** uses network services and the VoS data made available by the measurement platform operator.

Goals	
A mechanism to capture the price-performance ratio of an IP network.	
Methods to Achieve Goal(s)	**Customers**
1) Implement a measurement application that allows to capture the QoS of an IP Network 2) Define a scenario to capture the QoE of an IP network 3) Set up a database containing up-to-date price Information 4) Determine the VoS values	Consumers profit because they are given the opportunity to compare the price-performance ratio of IP networks and choose the best one
Costs	**Revenue**
1) Development and maintenance costs for the measurement application and price database 2) Potential fees for human test subjects	Revenue streams may appear from customers paying for data access providers marketing their offers

Figure 24: BM for the VoS Concept.

The network provider and measurement platform operator have a legal relationship with the regulator. The network provider must run its infrastructure within the constraints defined by the regulator, *e.g.,* with respect to pricing or customer data that needs to be collected. The measurement platform operator must collect VoS data in a way that respects the privacy laws defined by the regulator.

The legal and economic constraints with respect to the VoS concept are illustrated in Figure 25.

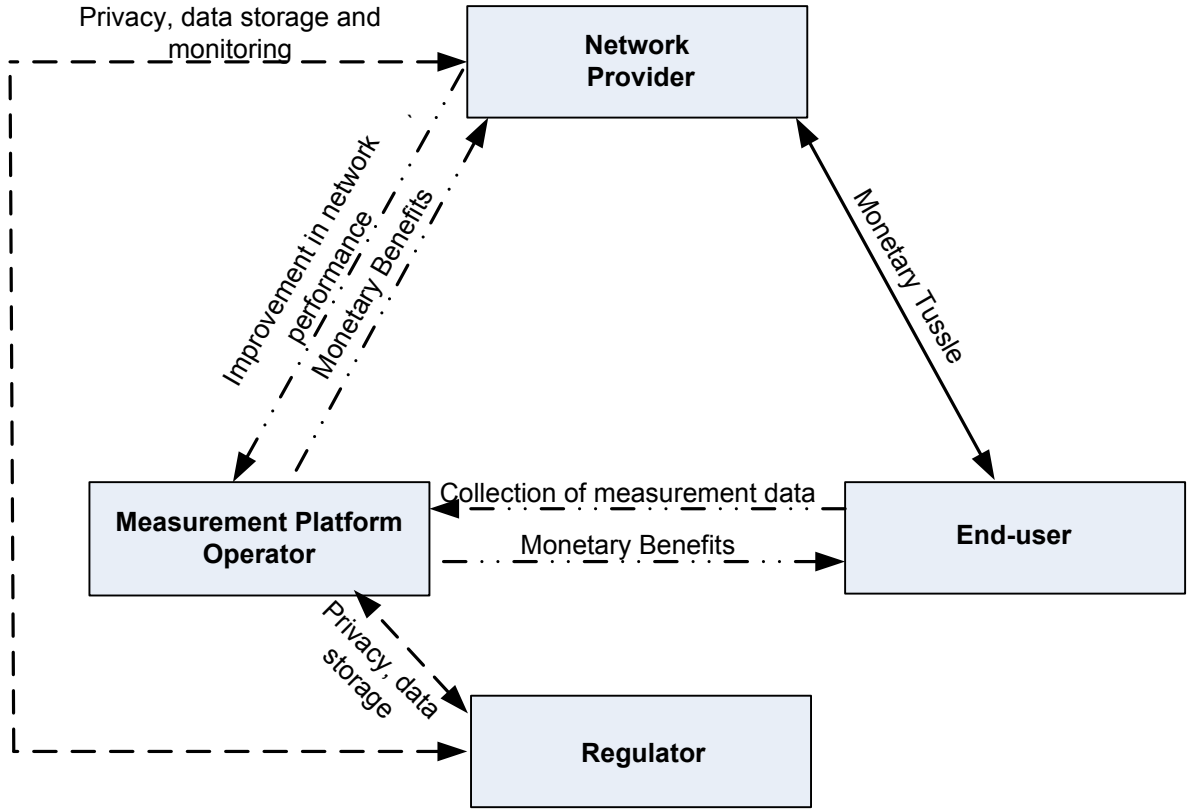

Figure 25: VN for the VoS Concept.

The measurement platform operator has a monetary incentive with respect to the network provider as well as the end-user. This is because they constitute the two conceivable revenue sources. The network operator may use the measurement platform operator to market its services while the customer might be ready to pay a fee for accessing the VoS data. On the other hand, the network provider has an incentive to run its infrastructure efficiently such that the VoS values obtained by the measurement platform operator are favorable. Further, the end-user has an incentive to access the VoS data, because it allows to select the network provider offering the price-performance ratio.

Finally, there is a monetary tussle between the end-user and the network provider. The end-user wants to pay the lowest possible price and the network provider wants to maximize its revenue.

4.9.2 Business Indicators

Individual metrics of the VoS concept can be considered as good BIs as they describe the price-performance ratio of an IP network with respect to specific aspects.

One-way Delay VoS
The one-way delay VoS describes the price-performance ratio of an IP network with respect to the one-way delay metric defined by the IPPM [2]. Because Internet users are sensitive to network delay [14], network operators have an incentive to minimize the network delay experienced by their customers. The one-way delay VoS measures how well the network operator meets this goal at a given price level and how its offer relates to the offers of other network operators. The one-way

delay VoS is defined as follows:

$$VoS_{owd} = \max(\frac{\Delta T_{ow_{max}} - \Delta T_{ow}}{p_{n_X}}, 0), \quad where \quad p_{n_X} > 0. \tag{17}$$

In the above equation $\Delta T_{ow_{max}}$ represents the maximum time after which a packet is considered lost. It is not measured but defined by the person performing the measurement. ΔT_{ow} represents the measured delay.

A measurement application for Android which allows to measure the one-way delay is currently in the early stages of development. Its architectural components will consist of a mobile measurement application running on Android, a measurement server which acts as the counterpart to the mobile measurement application, and a measurement database which stores the collected data. Further architectural details are not known yet due to the early state of development. The normalized price p_{n_X} is collected manually for different network operators and stored in the measurement database. The term *normalized* means that the prices offered by different network operators are brought in a comparable form.

Listening-quality MOS VoS

The listening-quality MOS VoS describes the price-performance ratio of an IP network with respect to the listening-quality MOS defined by the ITU-T [13]. The listening-quality MOS VoS is relevant for the scenario because it tells the network operator how an audio stream delivered over an IP network at a given price level is perceived by customers. Based on this information, network operators can see whether their customers are satisfied or not and how their service offer relates to the one by other network operators.

The listening-quality MOS VoS is defined as follows:

$$VoS_{MOS_{lq}} = \frac{MOS_{lq} - 1}{p_{n_X}}, \quad where \quad p_{n_X} > 0. \tag{18}$$

In the above equation, MOS_{lq} represents the listening-quality MOS. It is determined by letting test subjects rate the listening-quality of an audio source on a scale from 1 to 5 where 1 is bad and 5 is excellent. Because VoS metric capture the price-performance ratio of IP networks, the audio file must be delivered over an IP network. The normalized price p_{n_X} is the same as the one described in the previous section.

How to measure the MOS VoS is a question of ongoing research. The current idea is to develop an Android application playing an audio stream that can eventually be rated by the users of that application.

For the moment being, only the one-way delay VoS and the listening-quality MOS VoS have been considered as business indicators. The one-way delay and the listening-quality MOS have been chosen, because they are frequently used metrics from the QoS and the QoE space respectively. It is conceivable to define additional VoS metrics though, such as connectivity VoS or conversational-quality MOS VoS. However, these are areas of future work.

5 Summary, Conclusions, and Future Work

The work performed in project year Y1 within FLAMINGO's WP7 has lead to a number of relevant observations, results, and preliminary conclusions, which will be followed by next steps in Y2-Y4 as identified in the future work subsection.

5.1 Summary

The overall approach taken by FLAMINGO's WP7 on "Economic, Legal, and Regulative Constraints", covers areas addressing both (1) a cross-disciplinary approach to technology as well as (2) economic, legal, and regulative aspects. Several areas in terms of selected and specified use cases have been discussed in terms of (a) incentives and tussles of stakeholders involved in communications, (b) legal and regulative boundaries for various telecommunication based systems, (c) business policy driven specifications, (d) constraints for various scenarios in terms of performance, and (e) quality and cost. Thus, the major findings of this deliverable D7.1 are summarized as follows:

- A basic FLAMINGO management architecture and methodology for understanding the techno-economic, legal, and regulative interdependencies is identified. This serves as an underlying mechanism to analyze the dynamics of areas above on various scenarios.
- Major stakeholders involved in network and service management scenarios are determined uniquely, and they include network provider, operator, infrastructure provider, service provider, regulator, and end-user.
- Tussles between stakeholders in general include establishing a trade-off between performance and cost, and agreeing on conditions and penalties in SLAs.
- Incentives identified are majorly on the end-user side, as they achieve a transparent view and an opportunity to compare the price-performance ratio.
- The attempt of 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 privacy, data protection as well as on cost/pricing restrictions.
- In order to identify the feasibility of a deployment of respective network and service management scenarios, business indicators are identified. They serve those parameters, which are influenced by economic dependencies of the technology. Monitoring business indicators and configuring resources according to predefined goals can serve as an approach to ensure respective targets to be achieved. These business indicators are influenced, as identified with the help of joint management architecture for WP7 by various economic, legal, and regulative constraints, thus, presenting an integrated approach of important areas within the scope of WP7.

5.2 Preliminary Conclusions

The preliminary conclusions drawn after the first project year Y1 identifies three major facets. First, those constraints and business indicators identified serve as the initial step towards ensuring that the Future Internet will be manageable in an operational setting. Second, bridging the gap between technologists and the economic, legal, and regulative areas reveals important insights in

key stakeholders and, thus, determines a basis for a successful technology introduction. Third, the approach identified within this deliverable combines all relevant areas - technical, economical, legal, and regulative - to start the definition of a future vision on a holistic and homogeneous methodology for network and service management tasks and related research.

Therefore, investigating and analyzing the set of aforementioned major facets has helped to identify key techno-economic dependencies, especially embedded within the envelope of legal and regulative boundaries (cf. Figure 1, p. 6). Note, the set of scenarios selected for a closer investigation as described above do cover the full range of necessary areas and their interrelation. These scenarios include various network and service monitoring approaches, virtualization methods, and automated configuration and repair of managed resources. In order to optimize management decisions these scenarios are studied within the scope of economic methodology, legal and, regulative aspects to enable the refinement of detailed steps in the following project years.

Therefore work of WP7 in FLAMINGO and its related documentation within this deliverable D7.1 forms the key basis of network and service management decisions, the stakeholder-based analysis, country-specific, partially region-specific legal and regulative settings and frameworks, and business policy-driven mechanisms, all of which will be refined in the Network of Excellence due to very close combination of technology, networking, economic expertise with and applied legal and regulative know-how.

5.3 Future Work

In the next years of FLAMINGO, WP7 will see a deeper analysis in terms of constraints both in the economic as well as the legal and regulative dimension. Appropriate charging, revenue, and cost models will be identified for a selected set of scenarios. The key interrelation between value networks and business indications will be identified, which will help to identify stakeholder-specific business indicators. The identification of limits and boundaries, which are specific to laws and regulations being country-specific, and/or partially region-specific have to be studied and analyzed under a set of to be determined acts and regulations of the EU and Switzerland. Also, the identification of business policies - signifying business objectives - so that business indicators can be monitored and resources can be manipulated/reconfigured to achieve or maintain the expected level of performance. From the legal and regulative point of view constraints in terms of SLA fulfillment aspects, policy refinement, cost, accounting, and models will be studied and analyzed.

6 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 following manner.

6.1 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 7.

6.2 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 first project year in total reads as follows:

1. **Writing of joint scientific papers:** This work will be taken up in next FLAMINGO years, since Y1 had to concentrate on the identification of basic scenarios, their requirements, their stakeholders, and the respective analysis. Thus, the next years of FLAMINGO will continue with a joint description of concrete results, forming joint papers, and it will follow on with an implementation of the identified cross-disciplinary methodology, providing again the basis for joint papers.
2. **Integration of Ph.D. students:** WP7 works in close collaboration with Ph.D. students. Those scenarios identified describe various research activities within the scope of network and service management. This technical perspective (seeing typically the expertise of one person) is the technical perspective is complemented with the economical, legal, and regulative views (seeing typically the expertise of a second person). D7.1 indicates the first outcomes of those steps, thus, forming the basis for writing joint integrated Ph.D. works. Those steps prepared outline the foundation for successfully integrating expertise and know-how for joint Ph.D. work, which are made explicit in the WP2 reporting.

Table 7: WP7 Objectives

No.	Objective	Status as of Y1	Description	Section	To be Addressed in Y2-Y4
1.	Integrating network and service management research regarding economic, legal, and regulative constraints	IN PROGRESS	Analyzing various scenarios in these dimensions	3.1, 4	To be refined and studied in further depth
2.	Maintaining Online Informative Systems	FUTURE	-	-	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	4	To be refined and studied in depth
4.	Methods and approaches for economic-legal analysis	DONE	Joint architecture defined	3.1	Can be adapted, if required
5.	Models, architecture for stakeholders (operator, application provider, end-user)	DONE	Refined and studied in value networks	3.3, 4	-
6.	Integration of cost, incentive, business policies and legal/regulative frameworks	IN PROGRESS	Refined and studied in constraint analysis and BIs identification	3.1, 4	To be adapted with progressing work
7.	Operational costs for Internet Service Provider and telecommunication system providers	FUTURE	-	-	Cost models to be investigated for stakeholders
8.	Evaluate mechanisms under scenarios determined and derive guidelines for stakeholder defined.	FUTURE	-	-	To study constraints and business requirements in details and derive guidelines

7 Abbreviations

$6LoWPAN$	IPv6 over Low Power, Wireless Networks
AC	Admission Control
BI	Business Indicator
BM	Business Model
BP	Business Policy
CDN	Content Distribution Network
CPS	Cyber Physical Systems
CH	Switzerland
$DODAG$	Destination Oriented Directed Acyclic Graph
DoW	Description of Work
DSL	Digital Subscriber Line
EU	European Union
FI	Future Internet
FN	False Negative
FP	False Positive
$FTTH$	Fiber to the Home
GPS	Global Positioning System
HAS	HTTP Adaptive Streaming
$HSPA$	High Speed Packet Access
$HTTP$	Hyper-text Transfer Protocol
IDS	Intrusion Detection System
$IETF$	Internet Engineering Task Force
IFP	Infrastructure Providers
$INRIA$	Institut National de Recherche en Informatique et Automatique
IoT	Internet of Things
IP	Internet Protocol
$IPPM$	Internet Protocol Performance Metric
ISP	Internet Service Provider
$ITU-T$	International Telecommunications Union - Telecommunications Standardization Sector
JUB	Jacobs University Bremen
LLN	Low-power and Lossy Networks
LTE	Long Term Evolution
MNO	Mobile Network Operator
MOS	Mean Opinion Score
QoE	Quality-of-Experience
QoS	Quality-of-Service
$ROLL$	Routing Over Low Power Lossy networks
RPL	Routing Protocol for Low power and Lossy Networks
SLA	Service Level Agreement
SN	Substrate Network
SP	Service Provider
SES	Service Satisfaction
$S.M.A.R.T$	Specific Measurable Achievable Relevant Timely
TN	True Negative
TP	True Positive
TPM	Trusted Platform Module

ToS	Type of Service
$UniBwM$	Universität der Bundeswehr München
UCL	University College London
$UMTS$	Universal Mobile Telecommunications System
UPC	Universitat Politecnica de Catalunya
USA	United States of America
UT	University of Twente
UZH	University of Zürich
VN	Value Network
VNE	Virtual Network Embedding
VNP	Virtual Network Provider
$VoIP$	Voice-over-IP
VoS	Value-of-Service
$WLAN$	Wireless Local Area Network
WP	Work Package

8 References

[1] K. Almeroth, R. Caceres, A. Clark, R. G. Cole, N. Duffield, T. Friedman, K. Hedayat, K. Sarac, and M. Westerlund. RFC3611 - RTCP XR. `http://www.ietf.org/rfc/rfc3611.txt`. June 2013.

[2] G. Almes, S. Kalidindi, and M. Zekauskas. A One-way Delay Metric for IPPM. RFC 2679 (Proposed Standard), Sept. 1999.

[3] Asterisk. `http://www.asterisk.org/`, June 2013.

[4] B. Ciubotaru and G. Muntean. SASHA—A Quality-Oriented Handover Algorithm for Multimedia Content Delivery to Mobile Users. *IEEE Transactions on Broadcasting*, 55(2):437–450, June 2009.

[5] R. Comroe and D. J. Costello. ARQ Schemes for Data Transmission in Mobile Radio Systems. *Selected Areas in Communications, IEEE Journal*, 2(4):472–481, July 1984.

[6] Definition of Methodology. http://www.thefreedictionary.com/methodology, October 2013.

[7] DMCA Digital Millennium Copyright Act - 105th United States Congress. . `http://www.gpo.gov/fdsys/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf`. October 28, 1998.

[8] European Parliament and of the Council- Directive 2000/31/EC. . `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML`. June 8, 2000.

[9] A. Fischer, J. Botero, M. Beck, H. De Meer, and X. Hesselbach. Virtual network embedding: A survey. *Communications Surveys Tutorials, IEEE*, PP(99):1–19, 2013.

[10] B. Frank, I. Poese, G. Smaragdakis, S. Uhlig, and A. Feldmann. Content-aware Traffic Engineering. *SIGMETRICS Performance Evaluation Review*, 40(1):413–414, June 2012.

[11] Géant. Breakthrough GÉANT Network Marks Ten Years of Success: High Bandwidth pan-European Research Network Continues Advances with 100 Gbps Plans . `TenYearsOfSuccess`, November 2010.

[12] M. Golling and B. Stelte. Requirements for a Future EWS-Cyber Defence in the Internet of the Future. In *3rd International Conference on Cyber Conflict*, pages 1–16. ICCC, IEEE, 2011.

[13] ITU. ITU-T, P.800, Methods for Subjective Determination of Transmission Quality. `http://www.itu.int/rec/T-REC-P.800-199608-I/en`. June 2013.

[14] J. Jacko, A. Sears, and M. Borella. The Effect of Network Delay and Media on User Perceptions of Web Resources. *Behaviour & Information Technology*, 19(6):427–439, 2000.

[15] W. Jiang, R. Zhang-Shen, J. Rexford, and M. Chiang. Cooperative Content Distribution and traffic engineering in an ISP network. In *Proceedings of the 11th International Joint Conference on Measurement and Modeling of Computer Systemsoint conference on Measurement and modeling of computer systems*, pages 239–250. ACM, 2009.

[16] N. Kamiyama, T. Mori, R. Kawahara, S. Harada, and H. Hasegawa. ISP-operated CDN. In *Proceedings of 28th International Conference on Computer Communications*, pages 1 –6. INFOCOM, IEEE, April 2009.

[17] J. Kilpi and I. Norros. Testing the gaussian approximation of aggregate traffic. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, IMW '02, pages 49–61, New York, NY, USA, 2002. ACM.

[18] NETRADAR. `http://www.netradar.org/en`, June 2013.

[19] A. Osterwalder. Business model canvas. `http://www.businessmodelgeneration.com/downloads/business_model_canvas_poster.pdf`.

[20] 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*, pages 240–247. NOMS, IEEE, 2010.

[21] J. Rubio-Loyola, M. Charalambides, I. Aib, J. Serrat, G. Pavlou, and R. Boutaba. Business-driven Management of Differentiated Services. In *Proceedings of 10th IEEE/IFIP Network Operations and Management Symposium '12*, pages 240–247. NOMS, IEEE, April Osaka, Japan, 2010.

[22] J. Rubio-Loyola, J. Serrat, M. Charalambides, P. Flegkas, and G. Pavlou. A Methodological Approach toward the Refinement Problem in Policy-based Management Systems. *Communications Magazine*, 44(10):60–68, 2006.

[23] K. Scarfone and P. Mell. Guide to Intrusion Detection and Prevention Systems (IDPS). *NIST Special Publication*, 800(2007):94, 2007.

[24] R. d. O. Schmidt and A. Pras. Estimating Bandwidth Requirements using Flow-level Measurements. In *Managing the Dynamics of Networks and Services*, pages 169–172. Springer, 2011.

[25] R. d. O. Schmidt, A. Sperotto, R. Sadre, and A. Pras. Towards Bandwidth Estimation using Flow-level Measurements. In *Dependable Networks and Services*, pages 127–138. Springer, 2012.

[26] S. Tao, K. Xu, A. Estepa, T. Gao, R. Guerin, J. Kurose, D. Towsley, and Z.-L. Zhang. Improving VoIP Quality Through Path Switching. In *Proceedings of the 24th IEEE International Conference on Computer Communications*, pages 2268–2278. INFOCOM, IEEE, March 2005.

[27] C. Tsiaras and B. Stiller. Challenging the Monopoly of Mobile Termination Charges with an Auction-based Charging and User-centric System (AbaCUS). *NetSys 2013 - Networked Systems*, GERMANY, March 11-15, 2013.

[28] D. Tuncer, M. Charalambides, G. Pavlou, and N. Wang. DACoRM: A Coordinated, Decentralized and Adaptive Network Resource Management Scheme. In *Proceedings of 12th IEEE/IFIP Network Operations and Management Symposium '12*, pages 417–425. NOMS, IEEE, April Hawaii, USA, 2012.

[29] T. Winter and P. Thubert. RPL: IPv6 Routing Protocol for Low power and Lossy Networks. *IETF RFC 6550*, Mar 2012.

9 Acknowledgement

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.