Objective FP7-ICT-2009-5-257448/D-2.8

Future Networks

Project 257448

"SAIL – Scalable and Adaptable Internet Solutions"

D-2.8
(D-A.8) Evaluation of Business Models

Date of preparation: **12-10-31**
Start date of Project: **10-08-01**
Project Coordinator: **Thomas Edwall**
Ericsson AB

Revision: **1.0**
Duration: **13-01-31**

Document Properties:

Document Number:	FP7-ICT-2009-5-257448-SAIL/D2.8
Document Title:	D.A.8. Evaluation of the business models
Document responsible:	Nan Zhang
Author(s)/editor(s):	Luís M. Correia, Ricardo J. Ferreira, João P. Gonçalves, Tapio Levä, Johan Myrberger, Börje Ohlman, Jukka Salo, Daniel Sebastião, João Soares, Nan Zhang
Target Dissemination Level:	PU
Status of the Document:	Final
Version	1.0

Production Properties:

Reviewed by:	Holger Karl, Benoit Tremblay

Revision History:

Revision	Date	Issued by	Description
1.0	2012-10-31	N Zhang	Final version

This document has been produced in the context of the SAIL Project. The research leading to these results has received funding from the European Community's Seventh Framework Programme ([FP7/2010-2013] [FP7/2010-2013]) under grant agreement n° 257448

Abstract:

Due to the growing traffic volume in the Internet, new technical solutions are being developed. The three SAIL technologies, i.e. Network of Information (NetInf), Open Connectivity Services (OConS) and Cloud Networking (CloNe), aim at improving the scalability and performance of the Internet, as well as to increase the quality of experience for end users. The changing technical structure also changes the industry and market structure. This document aims at discussing the business and regulatory potential of the three SAIL technologies. After the market and ecosystem overview and the stakeholder analysis, potential business models for each of the technologies are proposed. The value of this work is the set of recommendations for technical development of each technology, which were based on the analysis reported in this work.

Keywords:

NetInf, OConS, CloNe, Business model, Ecosystem, Content, Recommendations, Interconnection, Privacy

Executive summary

Due to the growing traffic volume in the Internet, new technical solutions are being developed. The three SAIL technologies, i.e. Network of Information (NetInf), Open Connectivity Services (OConS) and Cloud Networking (CloNe), aim at improving the scalability and performance of the Internet, as well as to increase the quality of experience for end users.

However, changing technologies affect the market and industry structures as well as the stakeholders involved. For a new technology to be widely deployed and welcomed by the market, each of the stakeholder's benefits and incentives has to be ensured. Thus, this document continues the socio-economic work of Work Package A (WPA) and the previous deliverables, D.A.1 [1] and D.A.7 [2], proposing feasible and viable business opportunities for the three technical solutions. This document also links the technical work packages and socio-economics.

This document uses scenario planning to survey the ecosystem for each of the technologies and briefly presents the technical and business architectures. In addition, the different stakeholders' benefits and value networks are analysed and possible business models proposed. Additionally, a regulatory perspective is taken on issues concerning interconnection charging, privacy, security, and content.

The main results of this document include the business models presented in Sections 3.5, 4.5 and 5.5. For NetInf (Section 3.5), a six-step business model evolution path is suggested, from which three are evolutionary and the last two include the entrance of new actors and business agreements into the market. Similarly, for OConS, four cost/benefit scenarios were proposed where the revenue and cost flows of the different stakeholders were shown. On the other hand, CloNe's usage includes a wide variety of applications, thus no single business model could be suggested.

Another important finding is the business recommendations, which arose from the business and regulative analysis done in both D.A.7 and this document. The recommendations help the technical work packages in meeting the demand set by end users, stakeholders in the market, and regulators when developing the new technologies.

Contents

1 Introduction

1.1 Motivation of document and objective of document

Due to the growing traffic volume in the Internet, new technical solutions are being developed. In SAIL, three technical solutions are proposed in three work packages, i.e. Network of Information (NetInf), Open Connectivity Services (OConS) and Cloud Networking (CloNe). The three technologies aim at improving the scalability and performance of the Internet, as well as to increase the quality of experience (QoE) for end users.

However, changing technologies affect the market and industry structures as well as the stakeholders involved. For a new technology to be widely deployed and welcomed by the market, each of the stakeholder's benefits and incentives has to be ensured. Thus, this document continues the socio-economic work of Work Package A (WPA) and the previous deliverables, D.A.1 [1] and D.A.7 [2], proposing feasible and viable business opportunities for the three technical solutions. This document also links the technical work packages and socio-economics.

This document surveys the ecosystem for each of the technologies and briefly presents the technical and business architectures. In addition, the different stakeholders' benefits and value networks are analysed and possible business models proposed. Additionally, a regulatory perspective is taken on issues concerning interconnection charging, privacy, security, and content. Lastly, based on the business analysis, several business recommendations for the technical work and development are suggested.

1.2 Structure of document

The document is divided according to the three technical work packages, i.e. NetInf, OConS and CloNe. The research results from the above-mentioned topics are reported for each of the technologies. In addition, a SAIL overall view, which aims at discussing the socio-economic effect of all three technologies combined, is given in the beginning.

Thus, the socio-economic analysis starts with Section 2, which gives the SAIL overall perspective as well as motivates the rest of the work. Sections 3, 4 and 5 focus on NetInf, OConS, and CloNe, respectively. The recommendations for the technical development arising from the business analysis are given in Section 6. Finally, Section 7 concludes this document.

2 SAIL overall analysis

2.1 The evolution of the Internet

The Internet is today a crucial backbone for almost every aspect of business and other human interactions across the world. The amount of traffic carried across this backbone is increasing at an exponential rate, and is forecasted to continue to grow with a similar rate.

According to Cisco [3], "*Globally, peak Internet traffic will grow 4.5-fold from 2011 to 2016, a compound annual growth rate of 35%.*"

Furthermore, according to Ericsson [4] the amount of data traffic that is carried across mobile networks is forecasted to grow at an even higher rate (see Figure 1).

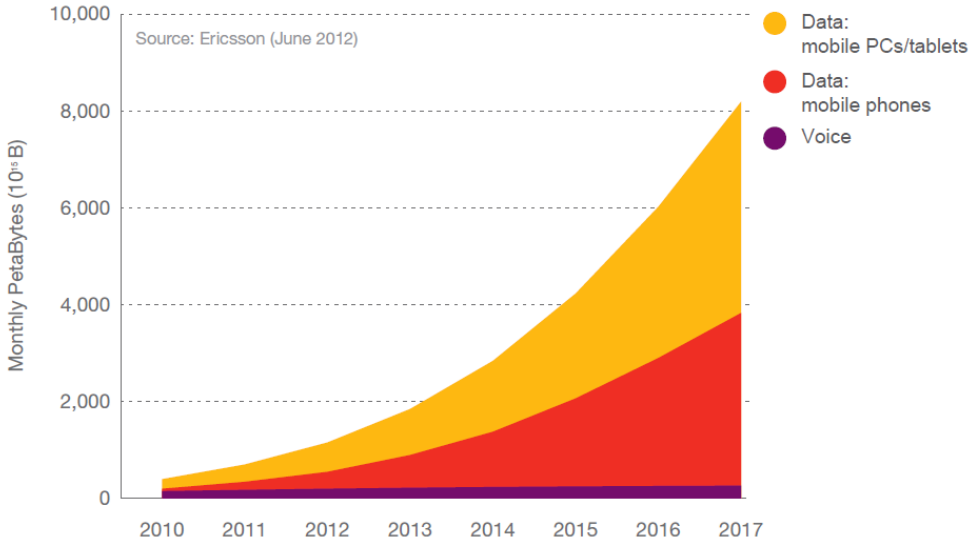


Figure 1. Mobile traffic mix forecast according to Ericsson [4]

This increased share of mobile traffic is also stated by Cisco [5]: "*Globally, mobile data traffic will grow 18-fold from 2011 to 2016, a compound annual growth rate of 78%*".

The growth in data traffic, especially in the mobile area, is caused by a combination of an increasing number of users and the growth in usage per user.

Starting by looking at the global number of mobile users, the number of mobile subscriptions is continuously increasing both developed and developing nations, although the growth is faster in the latter. As Figure 2 shows, the number of subscriptions just passed 6 billion [6], almost a billion higher than last year. This means double digit growths, even if the overall growth is steadily decreasing, Figure 3 [6]. These are very large numbers, and operators need to upgrade their networks to keep up with the demand.

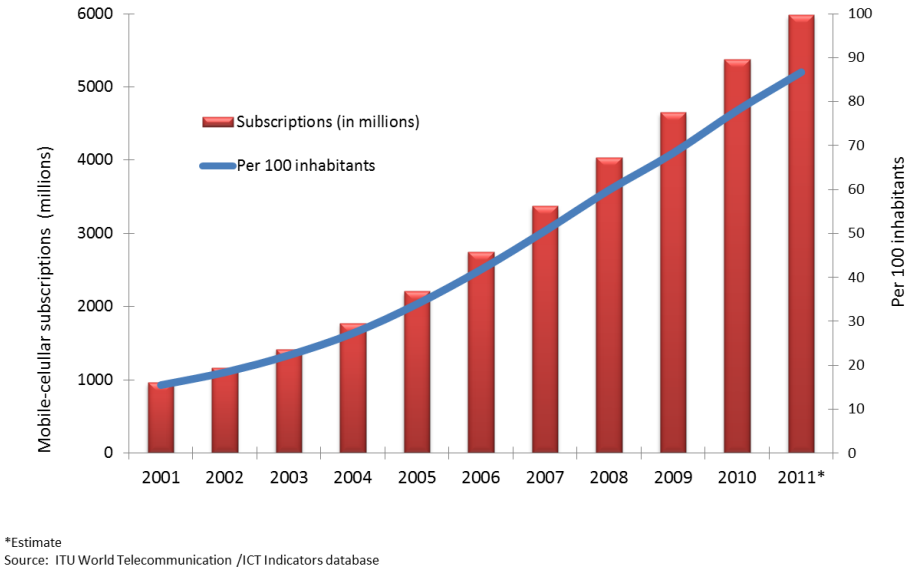


Figure 2. Evolution on the global number of mobile phone subscriptions (total and per 100 inhabitants) in 2001-2011 (extracted from [6]).

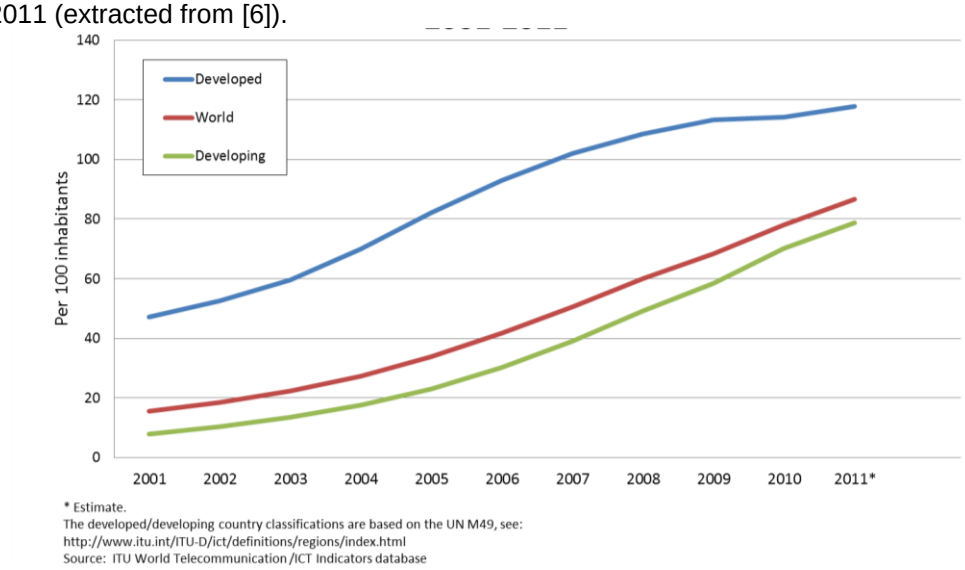


Figure 3. Mobile cellular subscriptions per 100 inhabitants in 2001-2011 (extracted from [6]).

However, the major challenge for operators does not come from the evolution of the number of users but from the huge growth in the traffic generated by each one. The average monthly traffic by a single mobile user is still quite moderate, but with the explosion of the number of smartphones, tablets, and laptops, these numbers are growing very fast.
In 2011, a regular mobile phone generated about 4.3 MB/month (up from 1.9 MB in 2010), but a smartphone generated almost 150 MB/month (35 times more) [7]. By comparison, in 2010, smartphones generated 24 times more traffic than the regular feature phones, even though the regular phones more than doubling the data generated in 2010. As of 2010, smartphones represented just 12% of the number of terminals, but account for 88% of the traffic; both these figures are expected to increase even more as the importance of video grows and the number of tablets increases sharply in the coming years [7], [8], and [9]. Mobile video is, and it is expected to continue to be, one of the major drivers of this growth [2].

The expected growth rate and shift towards mobile data are on their own reasons to research and explore alternative and complementing ways for the the Internet backbone to cope with the Internet traffic.

On top of the pure traffic forecasts, there is also a change in the traffic patterns and utilization of the Internet. These changes are driven by a combination of a growing number of devices connected to the Internet and by services that utilize the Internet in ways that was not previously foreseen. The growth of eg video traffic and social network traffic are only two such examples from a consumer perspective, and the current CDN approaches and general Cloud Computing evolution are two examples from a more deployment perspective.

The Cloud Computing evolution provides new opportunities from a network perspective. Many of the current deployments bring a dynamic cloud resource of computing power and storage to the user, while the current offerings in many cases do not solve the access part – how to dynamically access the cloud-based resources. The cloud market are further discussed in section 5.2.1.

The combined picture of the forecasted growth and evolution of Internet provides the motivation for research and development around the Future Internet. In a document [10] the FIArch Group lists a number of the current limitations and weaknesses are identified. It can be noted that the document includes statements like:

- "*Lack of efficient caching & mirroring:* There is no inherited method for on-path caching and mirroring of data/content (compared to off-path caching) that could deal with issues like flash crowding, as the onset of the phenomenon will still cause thousands of cache servers to request the same documents from the original site of publication"
- "*Lack of efficient transmission of content-oriented traffic:* Multimedia content-oriented traffic comprises much larger amounts of data as compared to any other information flow, while its inefficient handling results in retransmission of the same data multiple times and possibly from sub-optimal sources/paths"
- "*Scaling to deal with flash crowding.* The huge number of (mobile) terminals combined with a sudden peak in demand for a particular piece of data may result in phenomena which can't be handled"

2.2 The SAIL approach

The research work carried out within the SAIL project aims to bring "*Scalable and Adaptive Internet Solutions*" to cater for the evolution and challenges outlined above.

In SAIL, three research areas are explored. Network of Information (NetInf), Open Connectivity Services (OConS) and Cloud Networking (CloNe). Each of these three areas addresses the combined scenario of a Future Internet, both on their own, and more notably with the combination of two or more of the research areas.

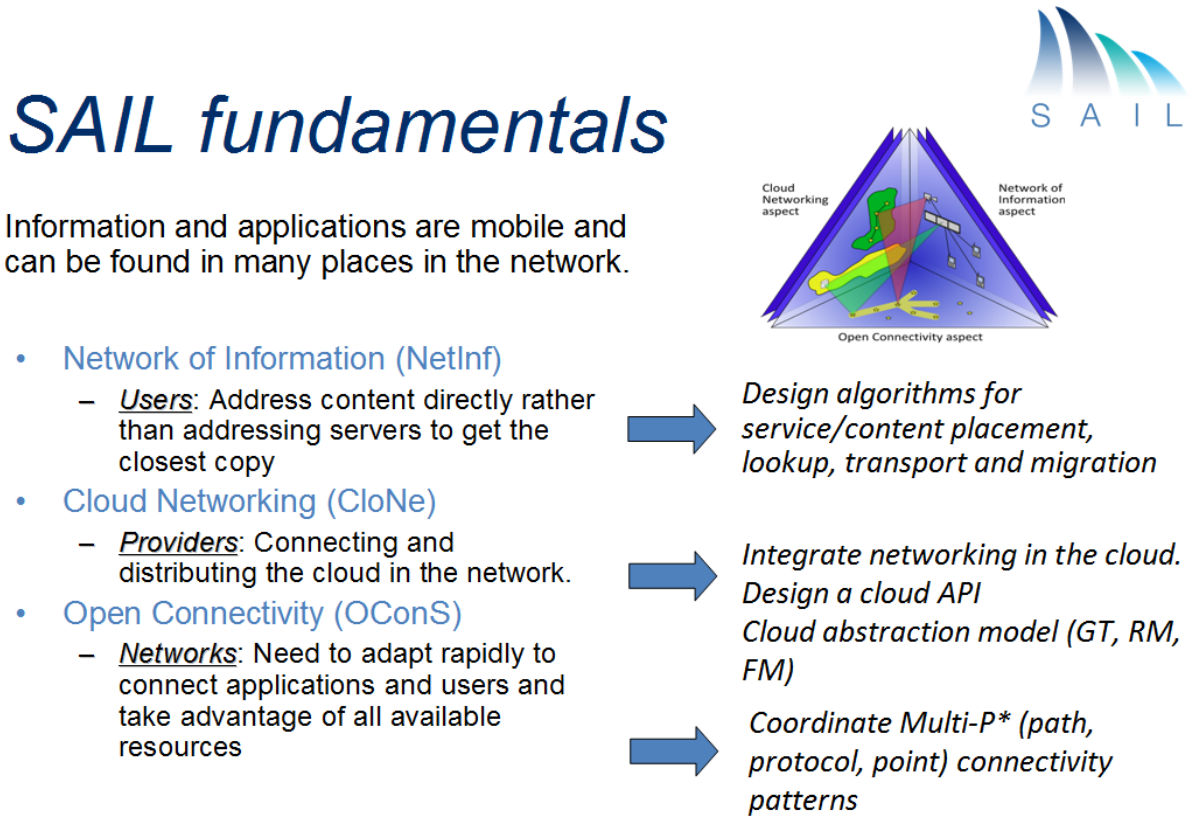


Figure 4: Three concepts within SAIL

The technical achievements and description of each of these areas are available in other deliverables from the SAIL project.

A common set of scenarios and use cases was identified early in the project and have guided the work throughout the project [1]. These scenarios represent some of the foreseen challenges from a traffic perspective and provide a common ground across SAIL. Further more, the scenarios and use cases are described form a user perspective and are a tool to explain both the challenges and the technical areas to a wider audience.

However, a sound and validated technical solution will not solve the issues on its own. Any technical solution must also make sense from a business perspective in order to be deployed live by an actor on the market.

A set of business recommendations are listed in chapter 6. These have been discussed within the SAIL project, during the technical work. These recommendations are also valid for any player that considers launching a solution based on SAIL.

Also, new technology and the overall market evolution are likely to make new type of players enter the market, and to introduce new business models and value chains. These new entrants come with new opportunities, and are at the same time a threat to current market actors.

In later chapters within this document, the socio-economic aspects for each of the core research areas within SAIL are explored. The analysis includes new and existing business models, regulatory considerations and other aspects. All in all, these chapters will provide stakeholders looking into deployment and development of SAIL technologies with a good overview, as well as details, which will support the commercial considerations.

2.3 Overall SAIL deployment considerations

When deploying new technologies like SAIL the overall deployment scenario, including migration aspects, need to be considered. These cover both the technical as well as more business-oriented views.

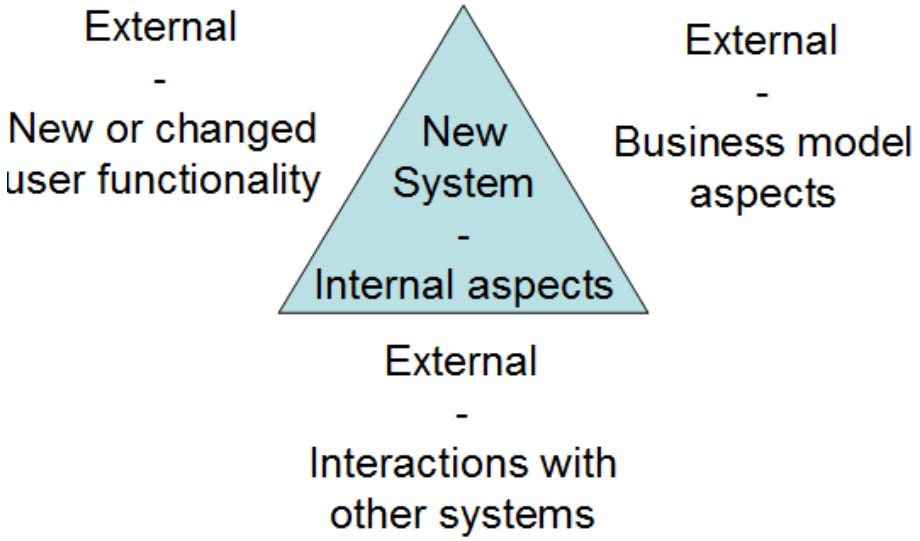


Figure 5: External vs internal migration aspects

In Figure 5 we broadly divide these aspects into an Internal and an External domain. The borderline between internal and external is very much set by the deploying actor – the border is not necessarily inside or outside the deploying actor, but can also be within the context of the deploying actor. Two such examples from within a single actor include:

- When a New System is connected with another system at the same actor ("Interactions with other systems")
- When a New System interacts with the business aspects of the actor, eg by putting new requirements on the sales force ("Business model aspects")

In these two examples the internal/external borderline is within the same actor. In many, but far from all, cases the internal/external borderlines are also found outside a single actor.

The internal aspects are here meant to be very much how the actual deployment is carried out – is the system introduced as a "new, separate box", deployed either as a replacement of an existing system or as a parallel deployment, or is the system introduced more as a (software) upgrade of an existing system.

We are from a SAIL perspective more focusing on the external dependencies, and more specifically – the nature of these. To what extent are they changing the status quo?

- New or changed user functionality:
  To what extent does the new system imply new or changed user behaviour? For SAIL, most of the enhancements are a few steps away from the end-user, and this aspect is not covered in detail within the scope of SAIL
- Business model aspects:
  To what extent does the deployment of the new system change the existing dynamics and setup around business models and B2B (business-to-business) interaction? This is the main topic of this document.
- Interactions with other systems:
  To what extent does the new system require new types of interfaces and interworking

with other systems, and to what extent can these changes not be catered for with pure remapping? This is the main topic for the upcoming deliverable on Migration, which is due at the end of the SAIL project (ie Q113).

2.3.1 Is SAIL a sustaining or disruptive innovation?

The overall approach for SAIL has been to ensure that SAIL technologies can migrate from existing infrastructure, and can co-exist with the current Internet architecture. In other words, SAIL does not impose a “clean slate” approach from a technology perspective.

However, SAIL technologies may still be perceived as disruptive by the market or by current actors in the market. For all of the external aspects visible in Figure 5 we can discuss in terms of sustainable vs disruptive change.

By *disruptive*, we apply the definition by Clayton M. Christensen [11]. Disruptive relates to the business model dimension, to what extent current business models are challenged by a new technology or innovation.

The opposite of a disruptive innovation is a *sustaining* innovation, a technology or innovation that preserves existing business models.

As can be seen in the business model analysis further down in this document, as well as in the earlier deliverable *New business models and business dynamics of future networks (DA.7)* [2], the SAIL concepts can both be brought to market based on existing business models (sustaining) or introduce new actors and new business models (disruptive).

Furthermore, even if SAIL technologies are implemented and brought to market by existing actors, and to a large degree aligned with existing business models, they can impose a new (and disruptive) service model towards the users of the system. An example of this is video telephony, which was one of the new mobile services made possible with the roll-out of UMTS/3G, but still has not been widely used among consumers.

2.3.2 To deploy a disruptive innovation

SAIL technologies can be deployed in both sustaining and disruptive ways. Eg a new solution can be deployed within the borders of a single actor, in order to increase efficiency. In many cases such scenarios are sustaining. However, the same new solution can be deployed outside a single actor, in which case the new solution can bring a disruptive scenario.

The potential duality of the situation motivates a brief discussion on the implications and considerations when deploying a disruptive innovation.

- For potential new actors (service providers and operators) that want to leverage the new technology, it is important to understand how to go-to-market with a disruptive innovation.
- For legacy service providers and operators, this is important for two reasons:
    - Most likely they want to protect their current business from new entrants to the market.
    - In the case where the new technology does imply a disruptive service model towards existing customers it is important to understand how to bring that new service model to the market in an efficient way, in order to ensure acceptance and usage among the existing customer base.
- And lastly – for vendors, a similar situation exists. If the innovation is disruptive in its nature, the go-to-market model towards existing and new customers (i.e. service providers and operators) potentially needs to be adjusted.

The business strategy literature has covered this in many books and publications. Perhaps most known are *Crossing the chasm* and *Inside the tornado* by Geoffrey Moore [12][13]. Both

of these publications identify niche markets as a crucial component in the business strategy related to disruptive innovations.

The importance of niche markets comes mainly from the fact that new and disruptive innovations in many aspects still might be inferior to existing technology.

1. Even though the evolution of the innovation might contain superior performance from a technology viewpoint, initial versions might only be superior from a few aspects.
2. The business maturity of the new innovation might be low in the beginning, leaving several aspects which are important for mainstream adaptation un-addressed.

Still, despite such potential short-comings, the new innovation might be suitable for one or more niche markets and it is within these markets the initial deployment are most likely to succeed.

The identification and selection of potential niche markets is a business development activity by each potential commercial player. The selection must not only be guided by a analysis of the solution that is sought to be deployed, but is as much dependent of the current position of the business actor. This deliverable will provide an initial analysis and will, together with other deliverables from the SAIL project, provide some insights of where to look.

And lastly – SAIL technology can in many cases still be deployed as a sustaining and evolutionary innovation.

2.4 Regulative analysis

Internet raises different regulatory issues compared to earlier network architectures. One example is network interconnection, which involves large economic network externalities and may favor large operators too much. However, this potentially large regulatory problem seems to not materialize in the Internet backbone because competition works. That is, operators can easily by-pass any monopolistically behaving operators via alternative peering and transit contracts. Regulator's attention is mainly needed in Internet access where the technology, e.g. copper, limits competition or in mobile Internet where GRX-based interconnection and roaming arrangements limit competition. Further, the 3GPP/GRX-based mobile architecture does not allow easy creation of virtual mobile network operators.

Another important regulatory topic today is Security and Privacy. Several Security and Privacy issues related to the Clouds have been identified both on the Cloud Service Provider side and on the Cloud Service User side. These issues may be quite complicated arising from the inherently global nature of the Clouds. However, Security and Privacy in Cloud computing is essential if there is to be significant take-up and adoption by end users, especially when private or commercially sensitive data may be stored, accessed and processed in remote locations, including for example different countries.

In this study of the SAIL Work Package A, the regulatory issues in Interconnections have been studied in the context of the NetInf and OConS concepts (sections 3.6 and 4.6, respectively), and the Security and Privacy issues have been studied in the context of the CloNe concept (section 5.6).

2.4.1 Interconnection charging

According to surveys from ITU [14], interconnection-related issues are ranked in many countries as the most important problem in the development of a competitive marketplace for telecommunications services. For that reason Interconnection has been in focus when investigating the NetInf concept from regulatory perspectives.

The potential Interconnection issues in the context of the SAIL concepts were studied in Deliverable D.A.7 [2]. That study resulted in the identification of several technical and administrative interfaces, where Interconnection is needed. All scenarios introduced several new technical interfaces, new actors for running the business (a part of a value chain), and

new roles for the existing and new actors. A prerequisite for the deployment of the new technologies and for running the business is that the interoperability across the technical interfaces and fair Service Level Agreements (SLAs) across the involved parties are ensured. Also, running the business across countries and regions requires that the rules are harmonised among them. This, in turn, requires that the regulatory authorities in different countries and regions have to cooperate.

Interconnection charges are payments between operators to compensate each other for the traffic exchanged between their networks. According to [14], there are various reasons for specifying that interconnection charges should approximate costs. Serious problems can result from a dominant firm charging competitors interconnection prices that are significantly above cost. First, it prevents market entry and the development of competition. Second, customers of the competitors will ultimately have to pay for these excessive charges. Third, the excessive prices can provide a pool of revenues that the dominant firm can use to subsidise losses, e.g., losses incurred as a result of predatory pricing action taken by the dominant firm to drive competitors out of a market.

There are number of costs that are associated with setting up and maintaining an interconnection agreement and these differ depending on whether it is a peering or transit agreement [15]. The set up costs include both capital costs of the requisite equipment, as well as the transaction costs associated with negotiating the agreement. In addition, all interconnection services increase operational cost somewhat. Every time a network adds a link, it increases complexity, and therefore the cost of operating the network.

2.4.2 Regulatory approaches for interconnection charging

A number of different procedures might be used to establish Interconnection charges. These include [16]:

- the regulator in advance determines the charges, together with other essential elements of interconnection, using different approaches to price regulation;
- the regulator sets guidelines which should be used for establishing the rates through (bilateral or multilateral) negotiations among the operators;
- operators set the rates through negotiation and commercial agreements, without the involvement of the regulators (the regulator intervenes only if parties fail to agree).

To set the interconnection prices regulators might use several possible approaches to the wholesale **price regulation**. The most common ones include [16]:

- **Rate of Return regulation (RoR)** – Rate of return regulation is a way of regulating the prices charged by a firm. It restricts the amount of profit (return) that the regulated firm can earn. The regulated price can be adjusted upward if the utility starts making a lower rate of return, and it will be adjusted downward if the utility makes a higher rate. The Rate of return regulation has been used extensively to regulate utilities in many countries.
- **Price-cap regulation** – This is a process for establishing rates or prices that will be charged for a service, which are adjusted each year by an index that reflects the overall rate of inflation in the economy, the ability of the operator to gain efficiencies if compared to the average firm in the economy, and the inflation in the operator's input prices if compared to the average firm in the economy. Sometimes a **price ceiling** approach might be used for the same purpose. Under this approach a regulator imposes a limit on how high a price can be charged on a service, without making periodical adjustments.
- **Cost-orientated or cost-based pricing** means that prices should reflect their costs plus reasonable rate of return which operators are allowed to earn. Operators or regulators might use different cost bases (current cost, historical cost, forward-looking cost) and different methodologies (Fully distributed cost (FDC), LRIC) to determine the prices.

2.4.3 Security and Privacy

It is clear that ensuring Security and Privacy will be one of the key objectives when designing the new information-sharing concepts of the Future Internet. The definitions of the key concepts related to Security and Privacy are given in Annex 1.

With respect to Clouds, the clarification of the applicable law governing the flow, processing, and protection of data is desirable, so that both Cloud users and Cloud providers have a clear understanding of which rules apply where and how. On 25 January 2012, the European Commission proposed a comprehensive reform of the EU data protection rules. The reform of the outdated privacy rules reflects that technological progress and globalization have profoundly changed the way data are collected, accessed and used. To ensure the growth and adoption of cloud computing, it will be necessary to find technological and policy solutions for ensuring privacy and assuring information security.

There are several levels at which Security and Privacy could be regulated. Their applicability for ensuring Security and Privacy in Clouds has been studied in this work.

3 Business Analysis of NetInf

The technical work of NetInf is progressing with good speed and the technical motivation for such a new technology is clear [17][18]. On the other hand, the socio-economic motivation for NetInf is less widely studied. Thus, this section aims at raising the awareness of the non-technical drivers for NetInf by first studying the ecosystem and constructing possible future scenarios for Internet content delivery. In addition, as one of the building blocks of NetInf is in-network caching, its potential is also studied. Based on the overview of the ecosystem, the different ways to monetise the NetInf investments are evaluated by first making a stakeholder analysis and finally suggesting a six-step business model evolution. Lastly, the regulatory issues of interconnection charging are discussed as well as the existing content regulations examined.

3.1 Business Drivers

This section presents motivation for the research reported in Sections 3.2-3.5. The amount of Internet traffic, especially video traffic, is growing significantly. Not only is the IP traffic growing but the nature of traffic traversing the Internet is also witnessing strong consolidation towards certain types of traffic. For example, the share of Real-time Entertainment traffic such as movies, video clips and music is rising constantly from year to year [19].

As a consequence, new technologies, such as NetInf, are being developed to cope with the changing traffic structure. However, adopting new technologies also causes industry and market to change. Thus, economic analysis is needed to understand how the market might change and how the relevant stakeholders can prepare for the future.

3.2 Ecosystem Analysis

This section surveys the ecosystem that NetInf will compete in, namely the Internet content delivery market. The section begins by proposing possible future scenarios of the Internet content delivery market in terms of which stakeholder controls the content delivery process and which stakeholder can decide on which content delivery architecture to use. The second topic discussed in this section relates to the potential of caching, a fundamental component of NetInf.

3.2.1 Scenarios of Internet Content Delivery

As a consequence of the growing Internet traffic, the Internet ecosystem is changing, and new business opportunities are emerging. Predicting the future is difficult, but formulating possible alternative scenarios can be done instead, for example with Schoemaker's Scenario Planning [20] method. Thus, the question to be answered in this section is as follows: *What are the alternative scenarios of heavy commercial content delivery over Internet for the next 10 years?*

In addition, the following supporting strategic questions are discussed, as the operators play a major role in the development of the Internet and NetInf: 1) *What is the role of mobile operators in Internet content delivery?* 2) *Which scenarios drive the adoption of NetInf?*

Two brainstorming sessions were organised to generate 94 forces that affect the evolution of the Internet content delivery market in the next ten years. After grouping and prioritising, ten basic trends and eight key uncertainties were singled out. Two of the uncertainties were singled out to form four possible scenarios for Internet content delivery's future. This section briefly discusses these two uncertainties and the scenarios. For more detailed results and analysis, see [21].

U1. Mobile ISP bundling: strong ISP bundling or no ISP bundling?

The cost of building the network is now borne by the ISPs and the costs are passed onto the end users and content providers through charging for network access. However, due to the increasing traffic volume and the competitive consumer prices, network access and connectivity is becoming less profitable for ISPs. In addition, the network is becoming more

content-centred. Bundling mobile devices together with network subscription has become common practice, because service providers wish to lock-in end users. Furthermore, end users may perceive the cost of a bundle to be lower than using the services separately and thus may consume more. Will the situation stay the same in the future or will ISPs attempt to increase revenue by playing a bigger role in the Internet content delivery process and offer also content? For example, Orange [22] in Europe and Comcast [23] in the U.S.A offer triple-play bundles that include certain amounts of films or TV channels, Internet broadband and mobile access.

Although the main issue in this uncertainty is whether content is bundled to the mobile ISP's service offer, device bundling is also important. For example, big content providers are offering their content together with devices with which to access their content in order to bypass the ISPs, e.g. [24]. Thus, it is important for the ISPs to also control the devices in addition to controlling access and content.

U2. Content provider revenue model: advertiser revenue or consumer revenue?

In the past, Internet content providers have mainly earned revenue from advertisers. However, several payment-based content providers have emerged into the market recently, e.g., Spotify [25], Sony Music Unlimited [26] and Voddler [27]. Thus, how will the dynamics evolve: will paid content, i.e. consumer revenue model, become more popular than the advertiser revenue model?

3.2.1.1 Scenarios

The final scenarios are illustrated in Figure 6. The resulting scenarios present the dominant end user type, whose decisions will lead to each of the scenarios. The dominant end user types include the comfort buyers, the quality buyers, the indifferent savers and the demanding savers. In addition, each of the scenarios show which actor will rule the Internet content delivery market and make the decision on the used caching system. The dominant actors in each of the scenarios are the local ISP, the global ISP, the advertisement content provider and the payment-based content provider. This section explains briefly the different scenarios. In addition, the differences between each scenario in terms of the key parameters are summarised in Table 1. For more detailed descriptions of each scenario and the differences, please refer to [21].

In the ***Comfort Buyer*** scenario, the end users are willing to pay for their comfort and thus prefer bundled services and to pay for the content. Therefore, the local ISPs are dominating the Internet content delivery process by providing service bundles to end users. This scenario is ideal for a local ISP because the ISP controls the content delivery platform as well as the content itself. In other words, the local ISP takes control of the content provision role. In addition, unlike the advertiser revenue model, the consumer revenue model does not require a large customer base.

In the ***Indifferent Saver*** scenario, the end users are relatively indifferent about the service quality and prefer to have bundled services but are not willing to pay for the content. This means that the access, device and content are still provided by the ISP, but the ISPs receive content revenue from advertisers. Because advertisers attempt to reach a wide audience, the ISP in this scenario should have a large subscriber base and thus the global ISP dominates the content delivery process. In this scenario, the global ISP among its other roles also acts as a content provider.

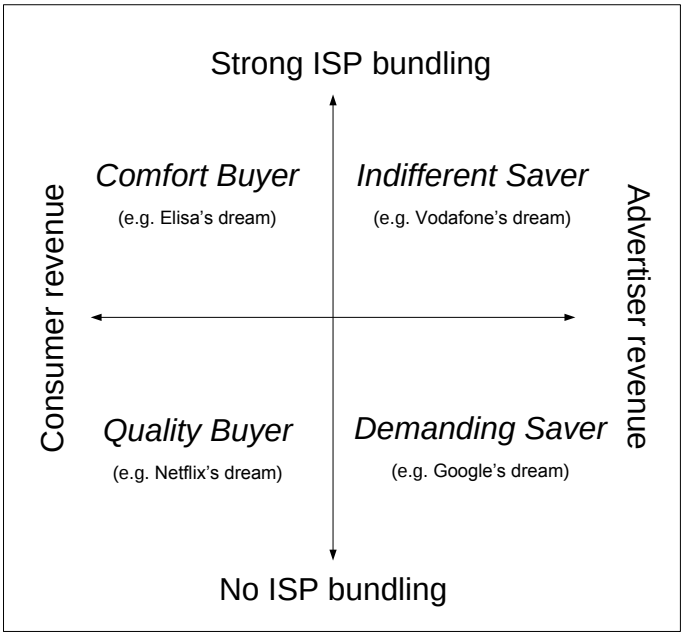


Figure 6. Scenario matrix.

Table 1. Comparison of scenarios.

Parameter\Scenario	Comfort Buyer	Indifferent Saver	Quality Buyer	Demanding Saver
Economies of scale	Low	High	Medium	High
Network effect	Low	High	Medium	High
Probability of own billing mechanism	Medium	High	Low	High
Ease of paying for end users	Medium	Medium	Low	High
Bank's role	Medium	Low	High	Low
Content provider control	Medium	Low	High	High
Amount of content usage statistics	Low	Medium	Medium	High
Importance of standardisation	Medium	High	Low	Medium
Winning actor	Local ISP	Global ISP	Payment-based content provider	Advertising content provider

In the ***Quality Buyer*** scenario, the end users know exactly what they want and thus choose to take the services separately and pay for the content. Therefore, the content provider, who employs the consumer revenue model (i.e. payment-based content provider), has the power to decide which Internet content delivery system to use in this scenario.

Content providers that use advertising as their revenue model (i.e. advertising content providers) are dominating the Internet content delivery market in the ***Demanding Saver*** scenario, because the end users know what they want and choose each service separately

but are not willing to pay for the content. Due to economies of scale and strong network effects, globally, only a few advertising content providers dominate the market.

3.2.1.2 Conclusions

Four future scenarios were constructed: *Comfort Buyer*, *Indifferent Saver*, *Quality Buyer* and Demanding Saver. Each scenario identifies the corresponding winning business role and the related winning actors that get control over the Internet content delivery market and can decide which caching architecture to use. The alternative winning actors are a) (small) local access ISPs, b) (large) global access ISPs, c) (small) payment-based content providers and the banking system, and d) (large) advertising content providers.

Based on the winning actors of each scenario, an overview of the possible dominating caching architectures can be reached. In-network caching, whether Information-centric networking or web proxy caching, are strong candidates for the Comfort Buyer and Indifferent Saver scenarios. On the other hand, content delivery networks (CDNs) – either pure play CDNs or content provider built CDNs – and clouds are possible outcomes in the Quality Buyer and Demanding Saver scenarios.

3.2.2 Factors influencing caching potential

In this section we identify the factors that affect caching potential, i.e., what share of content and traffic it is feasible to serve from locations other than the origin server. We limit our analysis by focusing on in-network caching. With this limitation, client-side caching is excluded and the total traffic volume in the Internet is the aggregate traffic volume traversing the access links towards end users (outbound from origin servers, inbound to end users). In-network caching includes all the intermediate caches between clients and the origin server, for example, proxy caches and P2P caches owned by ISPs or CPs, surrogate servers owned by CDNs, peers in P2P architectures and future ICN caches.

The potential of caching can be analysed either based on the number of objects or the volume of traffic. For our purposes, analysis on the traffic level is more interesting because most of the benefits come through reduced traffic volumes between the origin server and in-network caches. The content level analysis is relevant when caching is seen as a local phenomenon, where the main challenges relate to choosing the optimal cache size and eviction algorithms. From this perspective, the two main questions are: 1) which share of the objects is cacheable (i.e. the content owner and regulator allow it to be cached), and 2) which part of the cacheable objects is truly cached considering the economic and strategic limitations.

The caching potential depends on the properties of Internet traffic. In the following sections, the typical motives and needs for caching are identified for the three most relevant stakeholders: end users, CPs and ISPs. Then the parameters related both to the traffic in the Internet and to the properties of caching architectures are identified. Figure 7 shows a summary of these factors.

3.2.2.1 Incentives for caching

Caching has clear benefits for the different stakeholders, but also negative impact. Thus caching is discussed from the perspective of different stakeholders.

3.2.2.1.1 Content providers' incentives

Caching has a cost impact as it reduces load on origin servers and on the CPs' access links to the Internet. The main motives, however, relate rather to revenues. Due to the reduced load, the CP can scale more easily and the reduced latency improves the service quality experienced by end users. The improved QoE can translate into revenues by attracting increased usage or more end users, and it also helps in coping with the fierce competition among CPs.

Especially for the commercial CPs, the content is the source of revenues, so they want to control their content and its delivery in the Internet. Caching can have both negative and positive impact on this, depending on how the caching architectures enable CPs' control. On

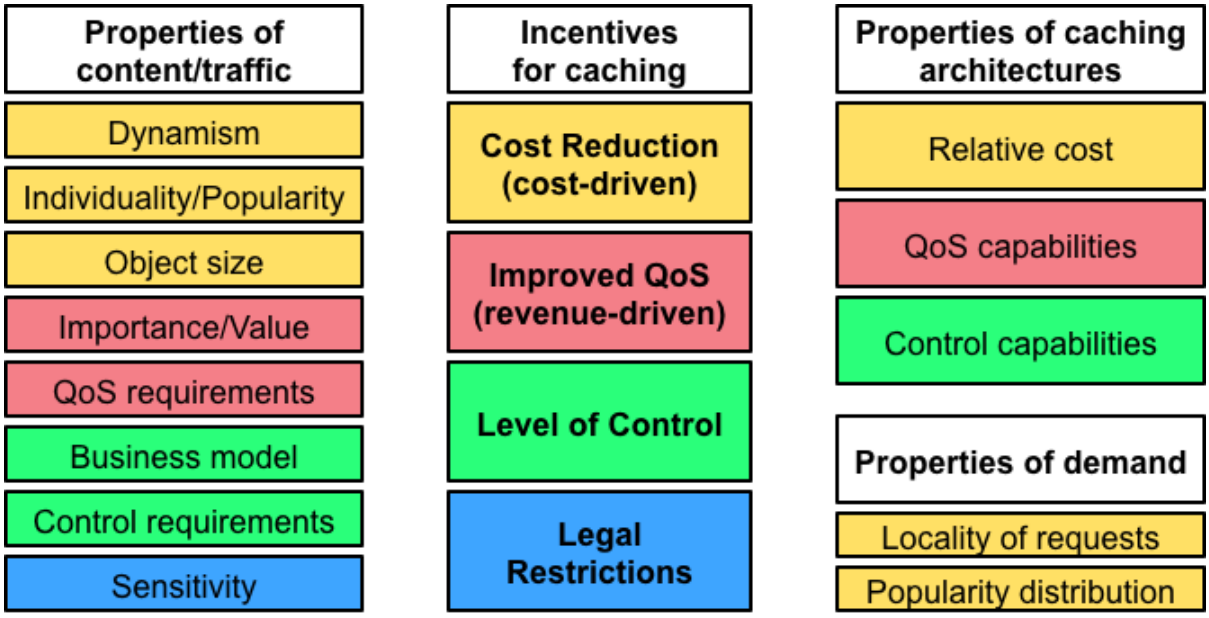


Figure 7. Factors affecting potential of in-network caching.

the positive side, the CPs may have more control over the content delivery and the service quality, which is the case especially with CDN caching and CPs' own caches. On the negative side, CPs may lose knowledge of the popularity of their content, the content may end up at unauthorized end users, or the caching party, for example ISPs, may not conform to the CPs' instructions for validity time or other parameters.

3.2.2.1.2 ISPs' incentives

ISPs have typically seen caching primarily as a cost-saving method because transport can be partly substituted by storage. Thus, ISPs can save transit costs. The improved QoE is a positive side effect that helps competing with other ISPs. However, ISPs are increasingly seeing caching also as a revenue possibility. Many ISPs are building their own CDNs, hoping to sell the CDN service to CPs while still saving transit costs.

3.2.2.1.3 End-users' and regulators' incentives

End-users are not interested from where their content requests are served as long as they get what they requested, QoE is good, and the cost is not too high. Thus, for the most part, end users interests are aligned with CPs' interest. The conflict of interest may arise when the content is personal or otherwise sensitive, which limits the locations where they want it to be stored. As end users rarely can themselves enforce their wishes, the legislator may take this role and limit caching of certain content.

3.2.2.2 Properties of content

Caching potential is also determined by the different content or traffic properties, such as the rate at which content changes, the popularity of content and object size. The most important content properties are shown in Figure 7 and this section briefly discusses the most important ones.

Content freshness and validity formulates an important constraint for caching. Content dynamics affect the feasibility of caching since constantly changing objects can be served from the cache only for a short period of time before an updated version has to be requested from the origin server. By the conventional definition, dynamic objects are generated at the time the user requests them, whereas a static object is an object which is delivered to the end user exactly as it was stored originally [28]. Here dynamism is defined in as a continuous variable, which changes based on the update rate of the content. If the object changes very often, especially compared to the rate of content requests, the efficiency of caching remains limited. In an extreme case, the rate of content changes is higher than the rate of requests,

which makes it unattractive to serve it from a cache. This condition can be presented by the following formula (Equation 1):

$$\textit{Rate of content change} > \textit{Rate of content requests} \quad (1)$$

An example of a static content is a static HTML document on a website, which experiences no or slow change over time. A weather update, on the other hand, represents a type of dynamic information that changes slower than the speed of caching.

The economic feasibility of caching of content is constrained by the number of subsequent requests after the initial request, i.e. **popularity**. This parameter influences the cacheability of information objects heavily because the main objective of caching is to serve subsequent requests of the same content, and hence it only makes sense to cache when actual subsequent requests exist. For example, a news article represents an information object that would be requested several times; hence, caching it would introduce efficiency in the delivery process. On the contrary, if the content is personal by nature, such as emails, the potential for storing it in in-network caches is limited as the number of subsequent requests remains typically low compared to the content that is of interest for a wider audience.

Quality of service requirements differ between different content and traffic types. For example, live communications, such as VoIP or gaming, have strict requirements for latency and jitter due to their interactive nature. Also, end users' quality expectations affect significantly their tolerance towards latency and jitter. For example, when paying for premium content, end users expect better service level, higher availability and have lower tolerance towards any kind of delays and jitters compared to free content.

The **level of control needed** by content providers due to the need for usage analysis and preventing illegal copies from spreading out significantly affects the feasibility of caching in the first place (are they willing to lose part of the control to other stakeholders); it also affects the decision between different caching architectures. Two main types of content control can be exercised:

- Access: control related to end user authorization and content consumption statistics.
- Distribution: control related to the right to hold and distribute the content.

Limiting the content access to paying customers and data on the characteristics of requesters and content consumption statistics is critical to most commercial content providers. Therefore, authorizing or at least recognizing customers is often required. Distribution control sets higher constraints on caching location, as only those in contractual agreement with the content provider can hold or distribute the content.

In addition, the content's value, its business model and sensitivity are important in determining the caching potential. For example, if the **value of the content** is high (i.e., it generates high revenues), the generated revenues cover more easily the costs of caching. The related **business model** impacts the level of control & quality needed. Lastly, if the content is somehow **sensitive**, the regulators may wish to limit caching of such content or the locations at which the content can be cached.

3.2.2.3 Properties of demand

Properties of demand affect mainly the economic feasibility of caching. Caching in its basic form is about local optimisation and the achievable efficiency in caching depends on the demand in each part of the network. For example, **popularity distribution** among objects affects the efficiency of caching, i.e., the size of the cache needed to serve some proportion of traffic from the cache.

In addition, the **locality of requests** affects local popularity. Caching is more efficient if the same amount of requests is concentrated in a small geographic area and thus can be served by a single cache compared to a distributed cache. This affects mostly revenue-driven caching.

3.2.2.4 Properties of caching architectures

Finally, the properties of caching architectures play an important part in the equation. The better caching satisfies stakeholders' incentives, the better its potential. These properties include the **cost level of caching** compared to the cost of transport and revenue gains, the **ability to satisfy the stakeholders' needs** for improved and/or controlled QoS, and the **ability to satisfy the stakeholders' needs for control**.

3.3 Technical and Industry Architecture

Sections 3.3-3.5 form a coherent whole that continues the value network configuration analysis started in earlier socio-economic deliverables, D.A.1 [1] and D.A.7 [2]. D.A.1 scratched the surface by identifying and briefly analysing a wide range of scenarios and use cases for NetInf. D.A.7 focused on the global, commercial content delivery scenario (NetInfTV) where the widest-scale deployment is expected. The key contribution was to identify twelve key roles that are needed to implement information-centric content delivery and to analyse eight possible value network configurations that either exist or could exist on the market. Both of these earlier deliverables avoided taking the perspective of a single stakeholder but tried to look at the opportunities and threats that NetInf brings to each stakeholder in the Internet content delivery ecosystem.

This final deliverable continues on the same path as D.A.7 by looking into using NetInf in commercial content delivery from content providers to content consumers but focuses now on the ISP perspective. From the perspective of ***technical architecture***, NetInf is seen as a standardized alternative to proprietary information-centric approaches, such as CDNs and P2Ps. Ubiquitous caching is the key feature that brings large share of the benefits. Naming of data is a key feature but its impact on the content delivery business is more difficult to understand and thus has a smaller role in our analysis. From the perspective of ***industry architecture*** (i.e., the way in which roles are distributed among interacting firms, see D.A.1 [1] for more detailed terminology definition), NetInf aims to bring more control to ISPs. However, from a purely technical perspective, also other stakeholders, for example CDN providers, could use NetInf as a part of their proprietary solutions.

The overarching goal is to analyse the success chances of NetInf by identifying the business opportunities it brings to ISPs and presenting strategies that can be used to gain acceptance among other stakeholders, especially among content providers that ultimately choose their content delivery method. To achieve this, the following topics are covered here. The remainder of Section 3.3 briefly summarizes the technical and industry architecture of NetInf and basics of the role analysis conducted in D.A.7. Then, Section 0 analyses the tussles that could emerge if ISPs take a larger set of roles in the content delivery than they currently do. Finally, Section 3.5 suggests an evolutionary business model adoption strategy to ISPs, which allows ISPs first to experiment in a small scale with immediate benefits of cost saving business models, and later to extend stepwise towards larger scale and revenue gaining business models.

3.3.1 Technical architecture

The studied use case is illustrated in Figure 8. It considers two Access Network Providers (ANPs) that employ NetInf to offer content delivery services to their customers. The two ANPs are connected through transit links to an Inter-Connectivity Provider (ICP). Both ANPs employing NetInf have deployed their own networks of caches. Within the ANPs' premises, local Name Resolution Systems (NRSs) are also provided, which are connected to a global NRS. The NRSs could be controlled by either the respective network infrastructure provider (ANP or interconnectivity provider) itself or by a third-party. Potential requestors (i.e., content consumers) of a named data object (NDO) exist in both ANPs; however, only a single publisher P_1 (i.e., content provider) of that specific content exists initially, in ANP_1.

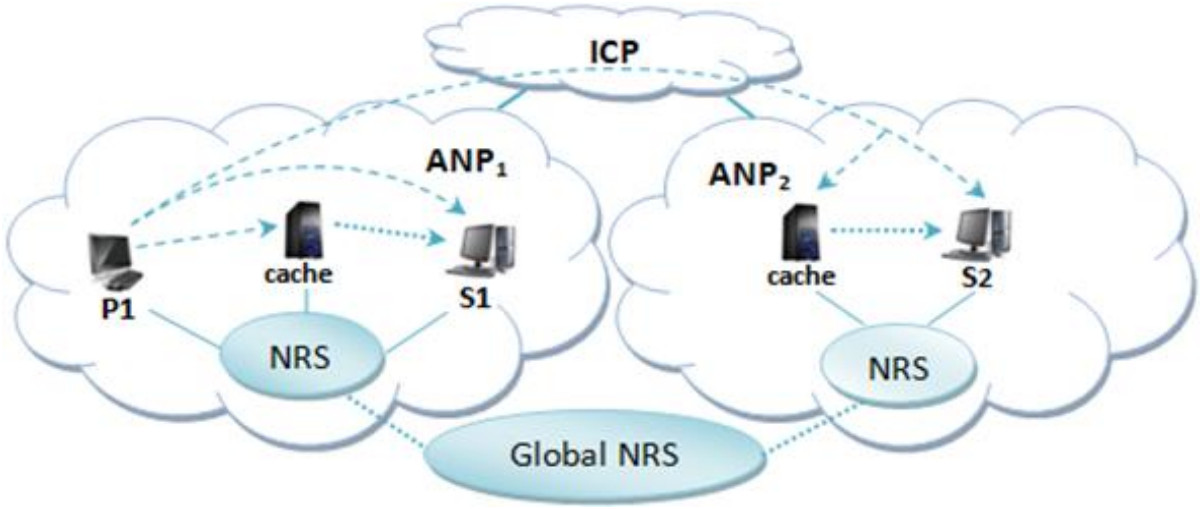


Figure 8. Content delivery in NetInf architecture.

- **Intra-domain scenario.** We assume that P_1 in ANP_1 publishes an NDO to its local NRS, and the local NRS advertises the publication to the global NRS. Then, S_1 in ANP_1 requests an NDO from the local NRS of its ANP. The local NRS identifies that the requested NDO is available within the ANP and forwards the request to P_1. If more requests for the same NDO occur, the ANP may also decide to cache the content to another location in order to achieve load balancing and to provide higher QoS to its customers (=content consumers).
- **Inter-domain scenario.** Let us now assume that S_2 in ANP_2 also requests the same NDO from its local NRS. Since the NDO is not published within ANP_2, the local NRS forwards the request to global NRS. The global NRS, which is aware of P_1, forwards the request to P_1. ANP_2 may cache the NDO in its caches in order to serve potential future requests.

The technical architecture of NetInf is described in more detail in WP-B deliverables D.B.1 [17] and D.B.2 [18].

3.3.2 Industry architecture

Industry architecture defines the ways in which roles are distributed among interacting firms [29]. As this is typically understood as an industry-level, quite stable setting, we use the term value network configuration (VNC) in this deliverable similarly to earlier deliverables to discuss about the different value networks (and business models) a technology enables.

The key functionalities and roles in information-centric content delivery were identified in D.A.7 [2] and are summarized in Table 2. Based on the selected ANP-centric use case, we focus on the role allocation (VNC) visualized in Figure 9. In this setup, the content access management (i.e. AAA) role can be taken by either the Content Provider (CP) or the ANP; the name resolution role is taken by either the ANP or a third-party provider; and the other four roles are assigned to the ANP. The chosen role allocation differs from the typical situation in the market today where other stakeholders than ANPs, such as CDN providers or CPs, control the name resolution, caches and content network.

Table 2. Key roles and functionalities in information-centric content delivery.

Role	***Functionalities***
Name Resolution	Controlling content directory and resolving content names to locations.
Content access management	Authentication, Authorization, and Accounting (AAA) related to content usage.
Cache management	Controlling (and owning) cache servers, including content selection and cache updating.
Cache location ownership	Controlling the locations where cache servers are to be installed.
Content network management	Routing, managing QoS, accounting of content delivery.

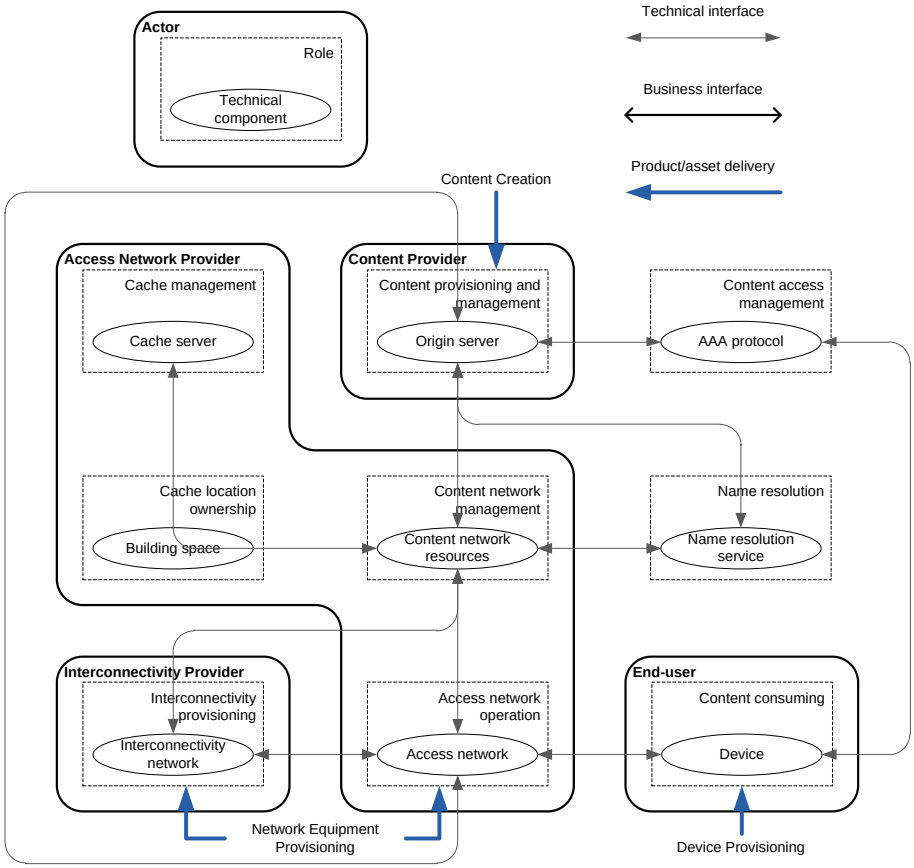


Figure 9. Value Network Configuration for ANP-centric NetInf architecture.

3.4 Stakeholder Analysis

The stakeholder analysis explores and analyses the tussles that may arise between different stakeholders due to the selected role division. The term '*tussle'*, introduced by Clark et al. [30], is defined as an *'on-going contention among parties with conflicting interests'*. The analysis presented in this section is a collaborative effort of SAIL and SESERV projects, which resulted in a paper published in FIA Book 2012 [31]. The aim of the work was to combine the value network configuration method used by SAIL with the tussle analysis method [32] developed by the SESERV project. The value network configuration part of this analysis is presented already in Section 3.3, so here we focus on summarizing the tussle analysis part. First, though, we introduce briefly the tussle analysis methodology.

3.4.1 Tussle analysis method

The tussle analysis method [32] consists of the following steps:

1. Identify all primary stakeholder roles and their characteristics for the functionality under investigation.
2. Identify tussles among identified stakeholders.
3. For each tussle:
    a. Translate knowledge into models by assessing the mid-term and long-term impact on each stakeholder;
    b. Identify potential ways for stakeholders to circumvent negative impacts and the resulting spill-overs.
4. For each circumvention technique, apply steps 1-4 again.

3.4.2 Tussles

ICN brings new challenges in the Internet market since different stakeholders, including ANPs and CPs, may offer name resolution services. Control of name resolution is important because the stakeholders are often interested in optimizing different things. Additionally, the content access management is a role with many possible tussles related to access control and content usage statistics. Even though these are control plane issues not directly linked to technical realization of content delivery, they should be considered important also by engineers designing NetInf architecture so that NetInf would be accepted both by ANPs and CPs. These and other identified tussles are summarized in Table 2 per each key role. For more detailed description of each tussle, please read the FIA Book paper by Kostopoulos et al. [31].

Table 3. Potential tussles in information-centric networking

Role	***Tussle***	***Stakeholders***	***Description***
Name resolution	Spam requests tussle	CP – End-user	End-users receive content they have not requested.
	Net neutrality tussle	CP – ANP	The content of some CPs gets preferential treatment.
	Conflicting optimization criteria tussle	ANP – CP; ANP – ICP	The location from where the content is served may differ based on the optimization criteria, which may be different for different stakeholders.
Content access management	Access control tussle	ANP – CP	ANP may provide content to unauthorized users from its local caches without consulting CP.
	Content usage statistics tussle	ANP – CP	ANP may not provide accurate content usage information to CPs, whose business depends on that information.
	Privacy tussle	CP – End-user	CP may use end-users' private information without permission.
Cache management	Content freshness tussle	ANP – CP	ANP may return stale content from its caches to save in transit costs.
Cache location ownership	Cache placement for revisiting interconnection agreements tussle	ANP – ANP; ANP – ICP	Current interconnection agreements may not be justified in the existence of NetInf caches.

Content network management	Network information tussle	ANP – ANP	ANPs may not be willing to provide accurate information about their network topology and utilization, which reduces both QoE and efficiency of NetInf.

3.5 Business Models

In this section we suggest an evolutionary NetInf business model adoption strategy to ISPs. We focus on analysing how access ISPs (ANPs) can benefit from NetInf caches installed in their networks. The suggested strategy allows ANPs to extend step-by-step the scope and scale of NetInf cache usage from the cost-driven optimization of their own network to revenue-driven CDN services. Extending the scope means that the ANPs use their NetInf caches for more content types and content of larger number of CPs, whereas extending the scale means larger content volume and extending the footprint of the services based on NetInf caches.

The core idea is that an ANP can first implement NetInf caches on their own network independent of other ANPs and gain immediate benefit by saving transport costs and by providing better quality of experience (QoE) to their own access customers. Later, after the NetInf technology has been tested internally, the ANP can gradually extend the usage of NetInf caches to also cover commercial, revenue-creating CDN services requiring business agreements with CPs. As identified already in D.A.7 [2], these multi-stakeholder CDN business models have more challenges related to business agreements but also potential for larger gains.

Figure 10 illustrates the suggested business model adoption strategy with six steps introduced in more detail in the following subsections:

1) **Internal network optimization:** Using NetInf to optimize the content delivery of ANP-provided services (e.g. an IPTV service) inside the ANP's own network.
2) **Transparent caching:** Building a transparent caching system for cacheable content originating from sources external to ANP.
3) **Telco CDN:** Providing commercial CDN services to content providers, i.e., monetizing the transparent caching.
4) **Telco CDN with CDNi:** Extending the footprint of the Telco CDN by interconnecting with other (Telco) CDNs.
5) **Virtual CDN:** Outsourcing the customer relationships with CPs to a virtual CDN provider.
6) **Elastic NetInf deployment:** Extending the footprint of the Telco CDN by deploying NetInf caches in virtual machines in the cloud operated by a Cloud Network (CloNe) Provider.

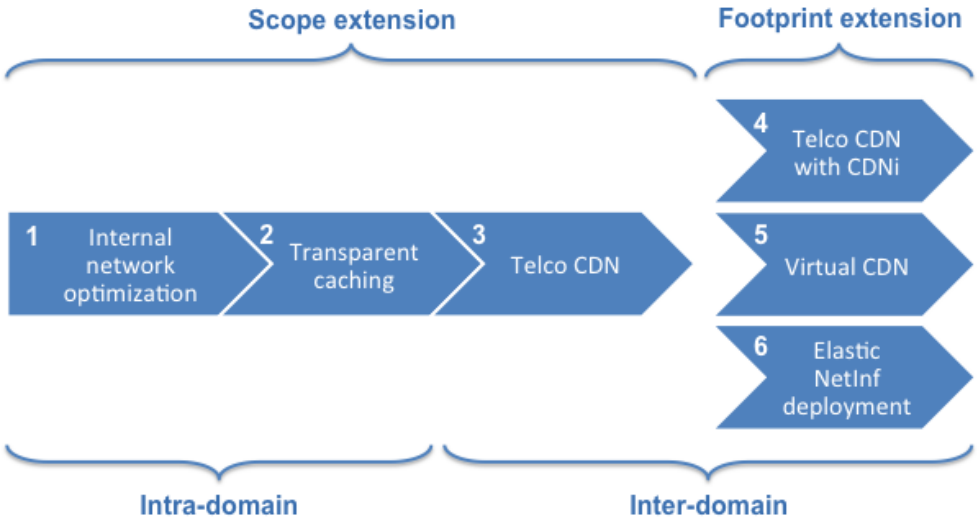


Figure 10. An evolutionary NetInf business model adoption strategy to ANPs.

The suggested business models have been described partly in the D.A.7 deliverable. Thus, our analysis focuses on the evolutionary perspective and explains the opportunities and challenges in taking each step. However, we do not aim justifying the usage of NetInf compared to other technical alternatives, such as the technologies currently used by commercial CDN providers (Akamai, Limelight, etc.), which have been discussed in the earlier deliverables by WP-A and WP-B, as well as in the forthcoming WP-B deliverable D.B.3.

We also identify the technical components that are needed in each phase and the extent to which SAIL specifies these. Please note that some of these technical components are not developed in SAIL due to the limited scope of the work. This applies especially to control plane technologies on inter-domain level because the technical work in NetInf has mostly focused on data plane issues with intra-domain scope. Therefore, we also refer to research conducted outside SAIL and suggest some topics for future research.

3.5.1 Step 1: Internal network optimization

A recommendable use case to begin NetInf adoption is using NetInf caches to optimize the delivery of operator-provided content services, such as a video rental service. In these services, an ANP operates the origin server and the whole content delivery process remains local, i.e., inside the ANP's own network. This use case has already been described in Section 3.2.2 of D.A.7 deliverable (ANP ICN). We do not repeat the description here but focus on justifying the benefits of starting the adoption of NetInf from this particular use case. The value network configuration of this use case is illustrated in Figure 11.

Adopting new technology such as NetInf first at intra-domain provides significant benefits. Most importantly, the deployment does not require costly coordination with other stakeholders. For example, the ANP knows beforehand the content that is travelling the network and it can take care that the content is properly named and contains the necessary metadata to make the system work. Additionally, the ANP often controls the customer premises equipment (CPE), such as internet-capable set-top boxes, that are bundled with the broadband access or IPTV service subscription. Thus, they can also take care that these devices support the NetInf naming scheme.

Furthermore, the benefits that the ANP receives, such as cost savings from more efficient network resource usage and better customer satisfaction due to improved QoE, realize immediately independent of other stakeholders' adoption decision. Existence of these kinds of "standalone" benefits helps the ANP to mitigate the risks related to the later steps where the additional "network" benefits depend on other stakeholders' adoption decisions. This is also in

line with the adoption strategy to *"facilitate sub-network adoption"* suggested by Ozment and Schecter [33].

As a novel technology the reliability and performance of NetInf may not reach its full potential immediate after it leaves the labs. The suggested small-scale deployment fully controlled by the ANP allows experimenting and tweaking the technology so that the reliability and performance can be improved to a desired level. Since this service is in practice a CDN for ANP-internal services that, the same technology can be used to provide commercial CDN services to external content providers (analysed further in step 3) when the NetInf technology has matured. A good thing from the perspective of SAIL is that the use case can be implemented with technologies provided by the project.

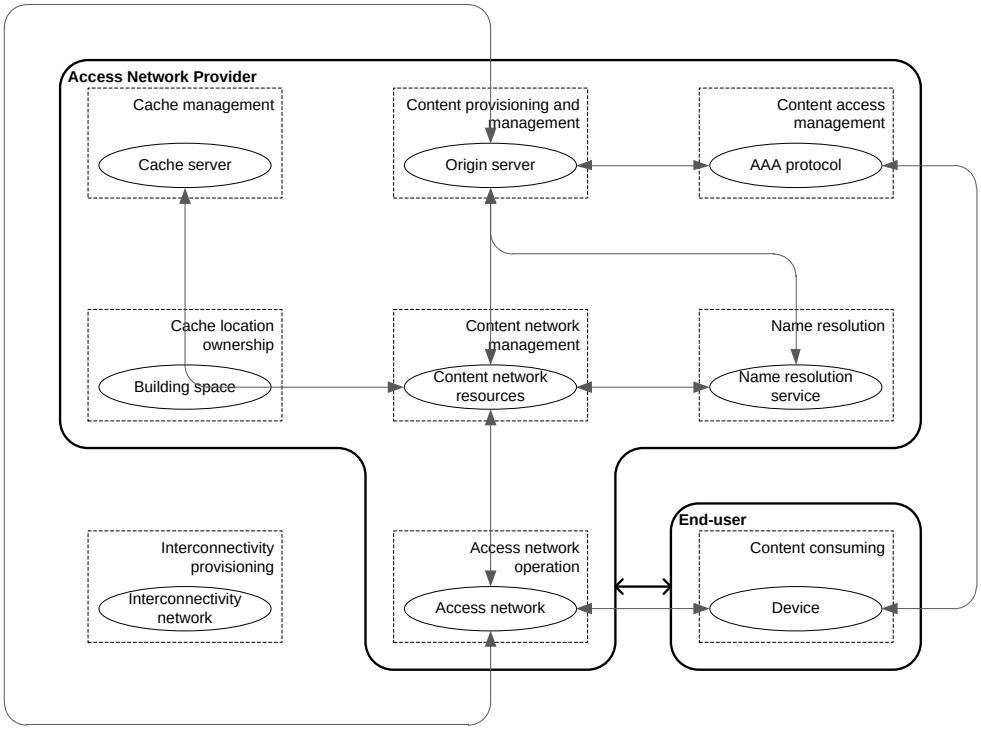


Figure 11. Step 1: Internal network optimization.

3.5.2 Step 2: Transparent caching

The logical extension of step 1 is to use the same NetInf caches for transparent caching of content originating outside of the ANP's network. The term "transparency" means here that there are no business agreements concerning content caching between the ANP and CPs. The business case is significantly more attractive here than in step 1, because a major share of consumed content comes from the content giants, such as Google or Facebook. Thus, in addition to the benefits of step 1, the ANP can substantially save transit costs when the off-net traffic decreases. This use case is illustrated in Figure 12 and described in more detail in D.A.7 (Pure ICN without business agreements).

The lack of business agreements with CPs makes step 2 straightforward because additional stakeholders are not needed to deploy transparent caching. NetInf can be used internally by the ANP hidden from the network, and potentially also from the communication endpoints allowing legacy applications to work with it [34]. Thus, the ANP only needs to extend the capacity of its NetInf architecture from that used in step 1 to scale to the increasing traffic and content volumes.

The lack of CP adoption is also the major drawback as the content naming does not conform to NetInf naming and the ANP needs to name the content again. The ANP also depends on incomplete information of content cacheability, which may limit the efficiency of transparent caching, or lead to problems with CPs if the ANP caches content without CPs' permission.

This problem is not so prevalent with HTTP content as HTTP contains a mechanism for defining cacheability, which is used by traditional web caching mechanisms. However, the main benefit of using NetInf instead of traditional web caches is that NetInf is not limited to HTTP content but the same infrastructure can be used for all kinds of traffic, including for example P2P traffic for which separate caches are implemented nowadays.

This use case can be implemented fully with technologies developed in the SAIL project. WP-B is developing a prototype of this use case under the name “Localized CDN” to demonstrate the feasibility of the use case. The prototype uses a rendezvous-based ICN control plane that operates on a legacy (non-ICN) data plane. In other words, the prototype creates an ICN domain where (not necessarily on-path) local caches/storages are created in the operator/ISP networks and managed and operated through the ICN control plane. The prototype is described in more detail in deliverable D.A.9 [34].

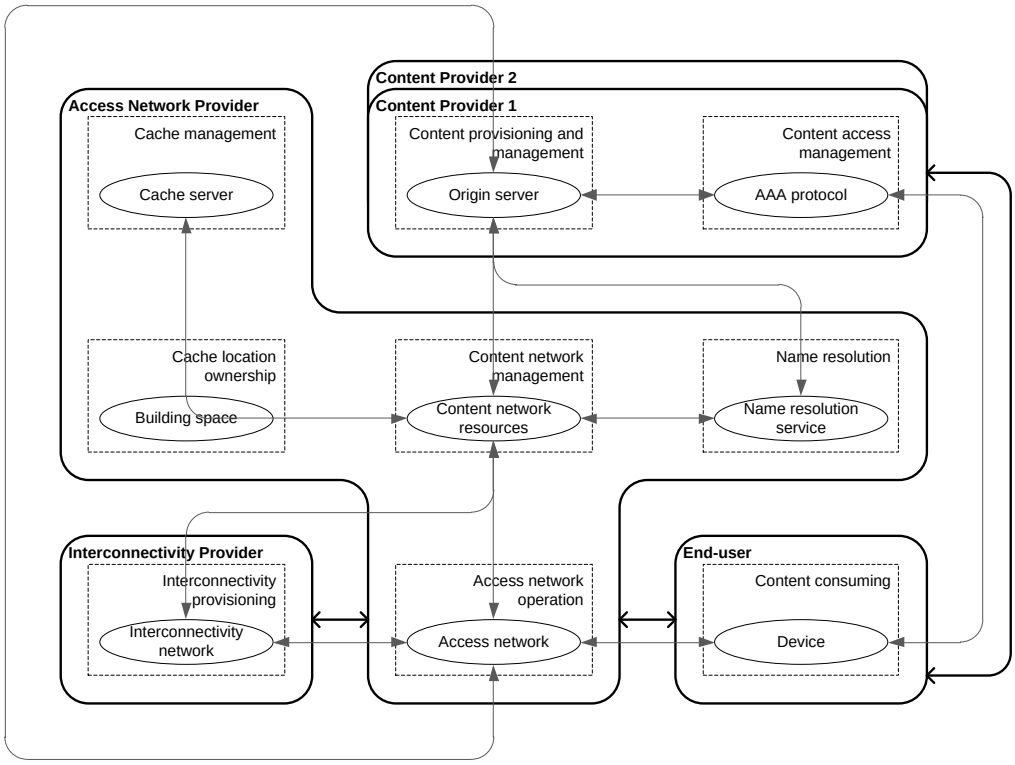


Figure 12. Step 2: Transparent caching.

3.5.3 Step 3: Telco CDN

The transparent caching architecture can be extended to a commercial CDN service by negotiating content delivery agreements with CPs. This would give the ANP the same benefits as step 2 but the ANP could also collect revenue from CPs. Compared to mostly proprietary technologies used in current commercial CDNs representing a technical alternative to NetInf, standardized NetInf naming enables better caching efficiency and scale advantages. This use case is illustrated in Figure 13 and described in more detail in D.A.7 (Pure ICN with business agreements).

Currently ANPs are deploying Telco CDNs separately from their transparent caching systems. In some cases there may be business reasons for doing that but typically this separation wastes resources due to unnecessary redundancies. NetInf as a standardized solution allows providing both services with one infrastructure. We note that the Telco CDN could serve either content requests originating from the ANP’s own network only or extend to content requests originating from other ANPs’ networks in the same geographic area. In the further discussion we limit to the former case as it can be built directly upon step 2.

A big advantage of the Telco CDN model is that it does not require the CPs to deploy NetInf. The transparent caching system can be used similarly as in step 2 – the only difference being that the content of the contracted CPs gets preferential treatment. To achieve this, the caching algorithms need to be updated to also reflect CP preferences, which may differ from those of the ANP as described in Section 3.4.2. A simple solution would be to first follow the preferences of the paying customer (i.e., the CPs), and then use remaining cache space for maximizing transit cost savings or other criteria important to the ANP. On the other hand, if already the CPs would follow NetInf naming system in their origin server, the performance of the NetInf system could be improved.

Extending to the Telco CDN also requires some additional investment to components related to the CP-ANP interaction. Most importantly, an accounting system for charging CPs for content delivery services needs to be deployed. The need for these kinds of business-related control plane components has been expressed already in the earlier deliverables [1][2] but SAIL has scoped them out from its research topics. This is reasonable as existing accounting systems used by current CDN solutions can be utilized also with NetInf.

The biggest challenge of the Telco CDN is its small footprint limited to the customers of a single ANP, which decreases its attractiveness compared to global commercial CDNs (Akamai, Limelight, etc.) with significantly larger footprint. Therefore, the Telco CDN model may not be feasible for small ANPs or their customer base limits to CPs that deliver content mostly to end-users accessing the Internet through this ANP. To overcome this problem, steps 4 and 5 introduce business models for extending the footprint of the Telco CDN. These business models are more disruptive than those presented in steps 1-3, so entering to those requires more careful investigation.

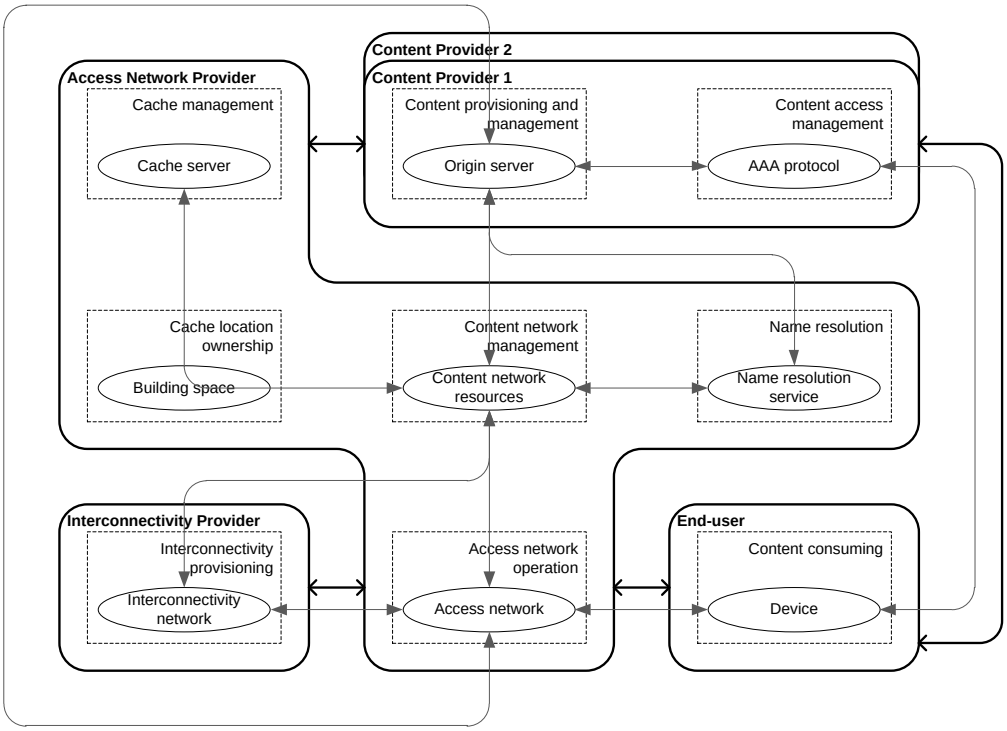


Figure 13. Step 3: Telco CDN.

3.5.4 Step 4: Telco CDN with CDNi

In the first three steps NetInf has been implemented only by a single ANP. To extend the footprint of NetInf beyond the footprint of single ANP, NetInf needs to go inter-domain. Interconnecting multiple Telco CDNs is one way to achieve this; it does not necessitate updates to applications and communication end-points. This would help a single ANP to interconnect their possibly separated CDNs (e.g., an ANP operating in multiple geographic

regions may have many separate CDNs) or allow interconnection of Telco CDNs provided by multiple ANPs. In this deliverable we focus on the latter case concerning multiple ANPs. As this use case has not been studied in the earlier deliverables, and inter-domain issues have not been defined extensively by the SAIL project, we refer mainly to the work of the CDNi WG [35] in the IETF. The VNC of the CDNi business model has been illustrated in Figure 14.

The idea behind CDN interconnection is to find technical as well as contractual solutions for interconnecting disparate CDN systems. In case of CDNi being implemented, CPs could agree on content delivery with only one Telco CDN but achieve global distribution for their content as well as allow off-net delivery of content across multiple operators in a fashion similar to roaming services offered by mobile operators. Moreover, having such interconnection gives the ANPs the possibility to offload some of their traffic to other Telco CDNs during the peak hours and hence provide a better QoS as well as reduce capital costs. In general, extending the scale allows improved efficiency through economies of scale.

Network equipment vendors such as Cisco have been driving the efforts for standardizing CDN interconnections. This can be a viable future solution for their customers, namely the ISPs, especially if no pure-play CDN will have been able to provide a de facto interconnection standard. The CDNi working group [35] and the Open ContEnt Aware Networks (OCEAN) project [36] are prominent examples of such standardization efforts. The CDNi WG is preparing multiple internet-drafts describing the problem [37], use cases [38] and requirements [39] for CDNi. The work focused on defining the control plane interfaces related to control, logging, request routing and CDNi metadata, whereas the data plane interfaces are out of scope of their work. Moreover, the CDNi WG does not study the commercial, business and legal aspects of CDN interconnection. Those questions are highly relevant and provide an interesting topic for future research. The only business model topic that the current Internet-drafts discuss relates to the value network configuration, which is also reflected in Figure 14. The idea with CDNi is that the coverage the CP receives depends on the (Telco) CDN it makes an agreement with. This CDN is called as an authoritative CDN, and other CDNs that the authoritative CDN connects to are non-authoritative CDNs. So coverage may differ depending on which Telco CDN the CP chooses to contract with. Therefore, the CDN providers would still compete over CPs and the interconnection model would actually be a co-operative model, such as the ANP business in general is.

The CDN interconnection has some challenges. Firstly, standardization takes a lot of time and many ISPs are looking for quick solutions in order to deal with the rapid increase in video traffic on their networks. This has resulted in business pilots, such as the CDN federation effort lead by Cisco [40], where ISPs try out CDN interconnection. Secondly, CDN interconnection faces business challenges. No solutions exist yet to ensure a reliable cascading of payments and SLAs between the interconnecting CDNs, so conflicts may arise due to the different interests of different telecom operators. There are generally two ways of approaching the agreements between interconnecting CDNs, one is that each operator goes into bilateral agreements with the operators they want to interconnect with, the other way is to have an interconnection hub that can manage the interconnections and the settlement fees based on the volume of exchanged traffic [41]. This latter model is discussed in more detail in step 5.

From the SAIL perspective, the CDNi work provides an interesting possibility for enabling interconnectivity not only among multiple NetInf domains but also between NetInf and non-NetInf domains. Especially the possibility to interconnect NetInf-based Telco CDNs with CDNs using other technologies is very attractive from a migration perspective because this would remove barriers to adopt NetInf decreasing competition between CDN technologies. To interconnect with non-NetInf CDNs, SAIL should guarantee that NetInf could support the CDNi interfaces specified by the CDNi WG, when they have been defined. Additionally, as the CDNi WG is specifying only the control-plane interfaces, SAIL should consider data plane interoperability with non-NetInf CDNs, i.e., how the acquisition and distribution of actual

objects with non-NetInf CDNs takes place. Here the ideas used in the Localised CDN prototype are useful.

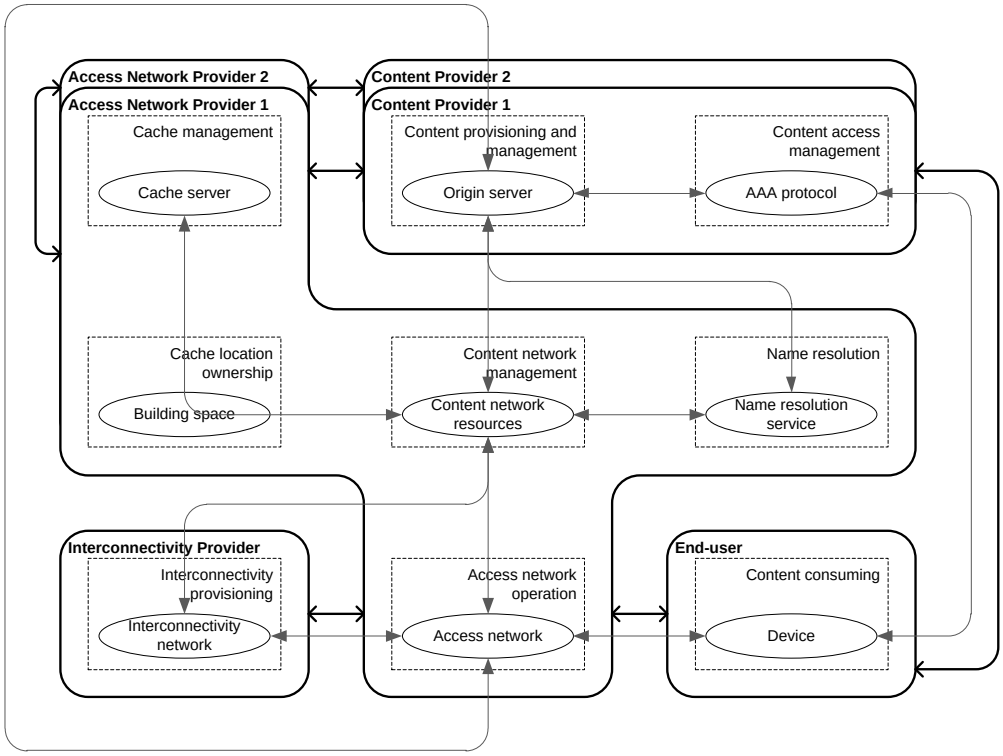


Figure 14. Step 4: Telco CDN with CDNi.

3.5.5 Step 5: Virtual CDN

Virtual CDN represents another business model for extending the footprint of the Telco CDN. This business model can be built directly on step 3, even though it is possible to extend to Virtual CDN also from step 4. The core idea of the virtual CDN model is that the resources of separate Telco CDNs are combined and controlled by a single stakeholder, a virtual CDN provider, that acts also as a single contact point towards CPs. The VNC of this business model is presented in Figure 15 and the model is described in more detail in D.A.7 (Virtual CDN).

The main advantage of the virtual CDN model for the ANP compared to the CDNi model is the decreased transaction costs, because the ANP needs to negotiate only with the virtual CDN provider instead of multiple ANPs. This is analogous to the case of IXP peering vs. private peering. Additionally, the virtual CDN model provides a clearer offering and a stronger brand in the eyes of CPs as the service is marketed under one name and sold by a single company. This benefits the participating ANPs, since the service looks more attractive to CPs and thus provides a stronger competitor to pure-play CDNs. Additionally; the specialization of the virtual CDN provider to the business agreements frees ANPs from the customer management costs.

On the other hand, the lost control over customer relationships with CPs as well as the emergence of additional player (Virtual CDN provider) may decrease the ANP's revenue. The attractiveness of the virtual CDN model to ANPs depends on the balance between the cost and revenue reductions compared to CDNi model. One solution for ANPs to keep the Virtual CDN Provider on leash is that ANPs establish the virtual CDN provider as a non-profit joint venture. In this solution, the ANPs would in practice form a forum where they can negotiate about the business issues related to the CDNi operation.

The virtual CDN model represents just a value network and business model change to the CDNi model and does not require any new technical components. The development of this model is therefore out of SAIL's scope.

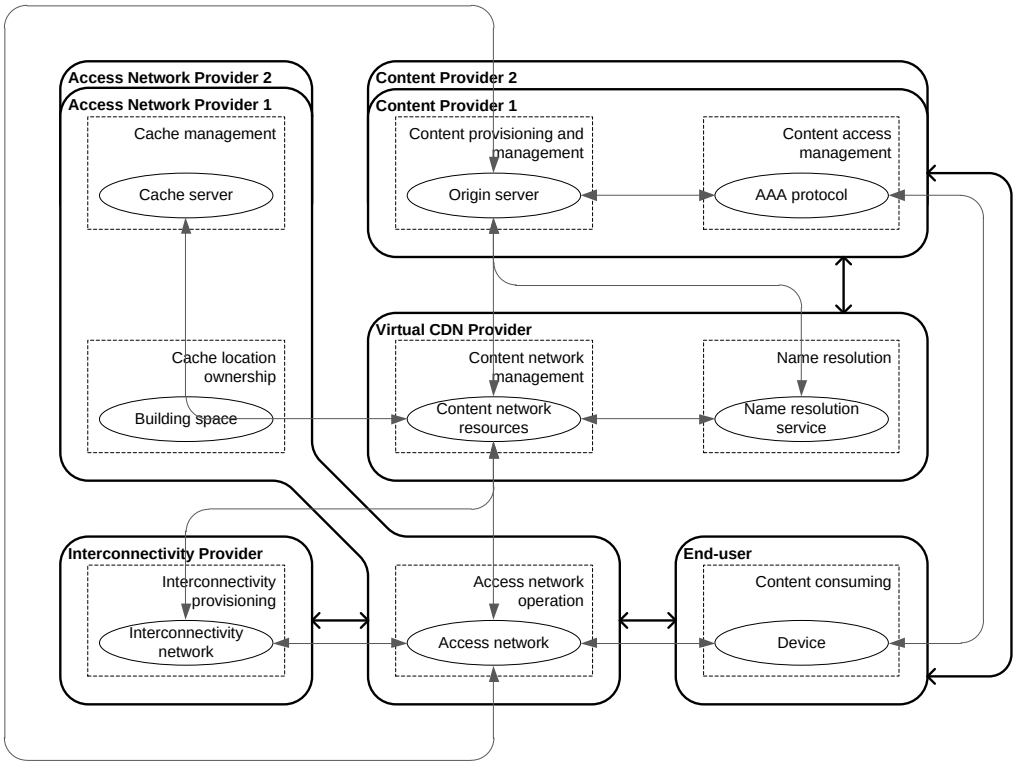


Figure 15. Step 5: Virtual CDN.

3.5.6 Step 6: Elastic NetInf Deployment

Elastic NetInf deployment prototype introduced in more detail in D.A.9 [34] represents an additional architectural model for extending the scale of a NetInf deployment. In this case, NetInf is provided over cloud networking (CloNe) that is another technical concept introduced by SAIL (see Section 5). Elastic NetInf deployment does not affect the business model towards CPs, because it only changes the way the NetInf resources are provided. As a result, elastic NetInf deployment can be used together with any of the business models 1-3 (and even with business models 4 and 5). For example, if a mobile operator (ANP) wants to provide a good QoE (and save in transit costs) for the customers of its IPTV service (step 1) also when they are roaming in the network of another ANP, it could add NetInf caches operated by CloNe close to the network of that another ANP. However, we envision that the need for footprint extension may be most relevant for increasing the CPs' interest towards CDN services. Thus, we demonstrate the impact of elastic NetInf deployment in extending the scope of the Telco CDN service (step 3).

Elastic NetInf deployment business model differs from all the other models in the way the NetInf caches (and other resources) are provided. In steps 1-5, NetInf caches were deployed "in-house" by the ANPs whereas here the NetInf resources are outsourced to CloNe provider. In other words, the NetInf caches are not located inside the ANP's own network but the ANP uses virtual resources of a CloNe provider to dynamically add and remove NetInf caches in different geographic locations based on the demand. In the VNC (Figure 16), CloNe provider controls only the caches but also name resolution system could be deployed in the cloud. Additionally, the overloaded role of content network management would in practise we divided between the CloNe provider and the ANP. As explained in D.A.9 [34], CloNe provider operates a management component through which the ANP (i.e., a NetInf provider) manages the NetInf caches. This management component reports the resource usage to the ANP for the purposes of content network management and billing between the CloNe provider and the ANP, and between the ANP and CPs. In the future work, the division of content network management role into multiple roles may be required.

Elastic NetInf deployment has advantages over the other two footprint extension business models of the Telco CDN service. In general, the model scales more dynamically to the

changes in the demand patterns. Compared to the CDNi model (step 4), elastic NetInf deployment does not require collaboration (i.e. bilateral agreements) with other ANPs. Instead, the ANP becomes a customer of a CloNe provider operating data centres and providing virtual machines around the globe. The service provided by the CloNe provider resembles the existing cloud computing services, such as Amazon Elastic Computing Cloud (Amazon EC2). Compared to the Virtual CDN model (step 5), the ANP can keep the very valuable customer relationship with CPs because the CloNe provider is invisible to CPs. This enables larger autonomy and profit margin than the Virtual CDN model.

The model has also drawbacks, as the ANP loses some of the control to the CloNe provider. Additionally, the ANP is not in any special position to provide a CDN service using virtualized resources but also other stakeholders can provide the service, including the CloNe provider itself that would effectively become a CDN provider. Actually, extending the virtual CDN model (step 5) to cover also the cache management role would result exactly the same VNC as the commercial pure-play CDN model (Pure-play CDN VNC in D.A.7 [2]) exemplified by Akamai, Limelight, etc.

The feasibility of the elastic NetInf deployment for the ANP depends on the relation between the revenues from the CPs (for the CDN service) and the payments to the CloNe provider (for NetInf cache deployment and related traffic). Consequently, this business model may prove to be attractive only if the ANP already operates a profitable Telco CDN service including an extensive set of own caches and the CloNe resources are only used for extending to locations where providing own caches is impossible or economically unprofitable.

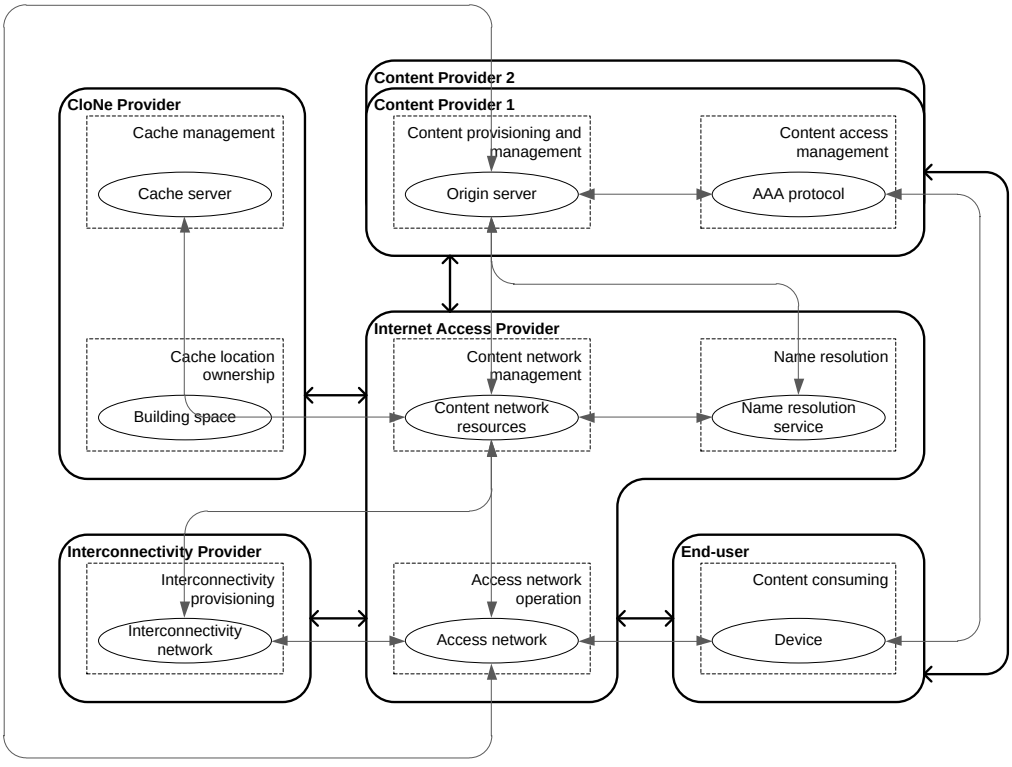


Figure 16. Step 6: Elastic NetInf deployment

3.5.7 Conclusion

NetInf is a technology that enables a variety of business models ranging from simple optimization of a network (intra-domain) to large-scale content delivery network operation (inter-domain). As NetInf is developed mostly by ISPs, we focused in this section into access network provider's business models. Six introduced business models build on top of each other allowing ANPs to start from small scale and gradually extend the scope and the footprint of their services. Consequently, the evolutionary business model adoption strategy suggests

also a feasible migration path. The migration issues will be studied from a more technical perspective in an upcoming SAIL deliverable D.A.4.

The presented business models are not unique for NetInf but they can be used with any (information-centric) content delivery technology, including the technologies used by commercial CDN providers (e.g., Akamai) and large content players (e.g., Google Global Cache, Voddler). Therefore, the selection to use NetInf as the technology will be based on the technological performance benefits introduced by content naming, such as larger reduction in redundant traffic due to more efficient caching than the existing technologies. The standardization of NetInf should also bring economic benefits due to support for larger number of traffic types, scale advantages and more open competition among content delivery service providers than the current proprietary CDN technologies that focus mostly on HTTP traffic.

Still it is valuable to recognise the business models and the challenges of NetInf as a technology to support them, because in its current form it is uncertain if NetInf truly has all the technical components needed to support all the presented business models. Consequently, the control (or management) plane issues need to be taken seriously in the prototyping activities. The elastic NetInf deployment over CloNe is a significant effort to this direction. Besides this prototype, the management planes of CloNe (and also OConS) might actually be used even more extensively with NetInf. Finally, also the existing network management technologies can potentially be used with the NetInf data plane.

3.6 Regulative analysis of interconnection charging in the NetInf context

The potential Interconnection issues in the context of the SAIL concepts were studied in Deliverable D.A.7 [2]. That study resulted in the identification of several technical and administrative interfaces where Interconnection is needed. Key prerequisites for the deployment of the new technologies and for running the business is interoperability across the technical interfaces and fair Service Level Agreements (SLAs) across the involved parties.

The regulatory backgrounds and targets for interconnection charging were presented in Section 2.4. The key statements from that section can be summarised as follows:

- Interconnection-related issues are ranked in many countries as the most important problem in the development of a competitive marketplace for telecommunications services.
- There are various reasons for specifying that interconnection charges should approximate costs.
- There are a number of costs that are associated with setting up and maintaining an interconnection agreement. The set up costs include both capital costs of the requisite equipment as well as the transaction costs associated with negotiating the agreement. In addition, all interconnection services increase operational cost somewhat.

3.6.1 Netinf and Interconnections

With respect to the SAIL's NetInf concept, our areas of interest are the potential changes in the Interconnection charging arrangements due to the deployment of NetInf and what models the Regulator should promote there.

3.6.1.1 Key actors

Large-scale content delivery is a huge business nowadays with multiple existing actors and business models. The NetInf concept can possibly be used in multiple existing information-centric content delivery models.

The key actors in Interconnections in the different delivery systems were listed in [1]:

- **End-user**, who does not care which content delivery model is used, as long as the quality of end user experience is good and the cost level low.

- **Content Provider (CP)**, who is interested in NetInf capabilities if they can get quality of service comparable to or better than other content delivery network models.
- **Access Network Provider (ANP)**, who may be interested in installing NetInf facilities because the in-network caching can enable savings in the transit costs. Purchasing the NetInf facilities, however, is a big investment that may turn out to unprofitable if the NetInf concept does not fly in the market.
- **Interconnectivity Provider (ICP)**, whose transit revenues may be decreased because of local caching, direct peering between content providers and ANPs as well as traditional CDNs. Thus ICPs may oppose the deployment of NetInf, even though they are also in an excellent position to move into the NetInf business.
- **NetInf Provider** is a new actor taking the content management role. The NetInf provider resembles the virtual mobile network operator, because also there the actor's main responsibility is to handle customer relationships, and the actual technical resources are owned by other actors. Thus, entering the market can be fast and does not require heavy upfront investments but the service quality can be controlled only indirectly through service level agreements.

Caching is a fundamental property of the NetInf concept. An entity controlling and managing the cache servers has its word to say about content selection and lifetime in the cache. Due to cost considerations, content freshness may be questioned which may lead to a tussle between those who manage caches and those who provide content (the Cache owner may not want to update content often in order to save Interconnection costs). Additionally, the location of cache servers is crucial for both performance and cost reasons, and their proximity to content consumers is often desirable.

Several possible value network configurations (VNCs) for information-centric content delivery were identified [1]. The ANP-driven VNC and the Virtual Content Delivery Network VNC give good views also on the interconnections and have been studied in the following from the perspectives of Interconnection charging.

3.6.1.2 Interconnections in ANP-driven Value Network Configuration (ANP-driven VNC)

In this VNC the Access Network Provider with the NetInf capability (ANPNetInf) plays a major role as it controls the content network apart from the content access management role, which is controlled by the Content Provider (CP) [2]. In this VNC the CP has to sign the contract, potentially with several providers of NetInf capability.

The ANPNetInf itself also benefits from this VNC as less inter-domain traffic is generated. In addition, as the ANP takes both the cache location ownership and cache management roles, no conflict of interest between these roles can arise.

For this concept the data flows and interconnection costs have been illustrated in Figure 17. In the illustrated network topology the interconnections are not necessarily new, but the deployment of the NetInf concept has an impact on the needed interconnection capacity and on the end-user perceived QoS.

The impacts on the interconnection costs (low/medium/high) for different players from setting up and operating the NetInf-based content delivery networks and the potential savings in the interconnection fees are presented in Table 4.

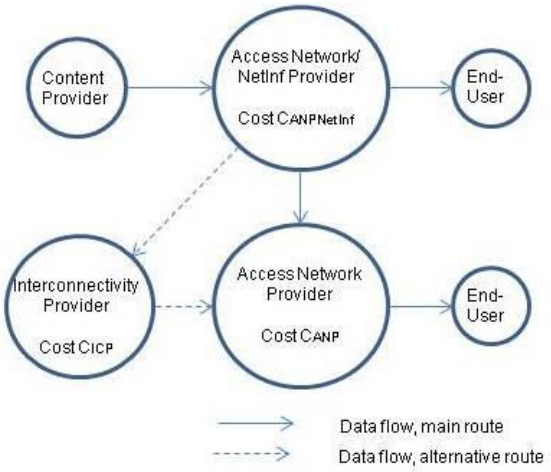


Figure 17. Data flows in the ANP-driven VNC.

Table 4. Interconnection costs and benefits in ANP-driven VNC.

Costs		Content Provider Cost C_{CP}	Access Network / NetInf Provider Cost $C_{ANPNetInf}$	Access Network Provider Cost C_{ANP}	Interconnec-tivity Provider Cost C_{ICP}
Set Up	*Capital Costs*	low	high[1]	n/a	n/a
	Transaction Costs	medium[2]	medium	low	low
Operational	*Operating Costs*	low	medium	low	low
Savings in interconnection fees		high[3]	high[4]	n/a	n/a[5]

n/a = no costs nor savings

The **following remarks** on the costs can be made:

- The level of investment in NetInf by the Access Network Provider is high. However, that investment has no direct impact on the actual cost of setting up an interconnection link.
- The investment in NetInf by the Access Network Provider will dramatically reduce the needed interconnection capacity between the Content Provider and the network.
- The investment in NetInf by the Access Network Provider will dramatically reduce the interconnection fees paid by them.
- Less interconnection capacity is needed from the Interconnectivity Provider due to the content caching by the Access Network Provider.

[1] The investment level has been assessed in the deliverable D.A.1. It is not directly related to interconnections, however.
[2] CP needs to negotiate the contract possibly with several ANPs. Per ANP the costs are on the medium level, however.
[3] Less interconnection capacity is needed from CP to network compared to the situation where NetInf has not been deployed.
[4] Less interconnection capacity is needed towards ICP and CP.
[5] ICP will lose a lot of its business because less interconnection capacity is needed, however.

Flow of Interconnection fees

The flow of Interconnection fees, between 1) the Content Provider (CP) and Access Network/NetInf Provider (ANPNetInf), 2) ANPNetInf and ANP, and 3) Interconnectivity Provider (ICP) and ANPNetInf is discussed in the following. Here we are interested especially in the changes to the interconnection fees due to the deployment of NetInf.

1) With respect to **the flow of interconnection fees between CP and ANPNetInf** the following options are available to cover the costs of interconnection:
   - No interconnection fees. In this option each party recovers all its interconnection costs from its own customers.
   - ANPNetInf imposes a fee on the interconnected CP, where the payment helps to cover some of the set up and operating costs. Even though those costs are not directly related to the interconnection between these two players, the payment could be justified by the higher QoS that ANPNetInf can now provide to the end-users of content. On the other hand, both players have savings due to the reduced need for interconnection capacity. Presumably, CP will pass the difference of the interconnection cost to the content producers, who pay more to CP and thus indirectly cover the cost of transporting their content across ANPNetInf. In the end, the end-users see the net value of these payments as higher content fees.
   - Payment from ANPNetInf to CP. This makes sense only in the case where ANPNetInf is a small, rural ISP. If there is no direct connection between ANPNetInf and CP, all of the content from the producers will come into ANPNetInf over a potentially expensive transit link. Having CP make a direct connection to ANPNetInf may greatly reduce ANPNetInf's costs, but if ANPNetInf is small, it may not be cost-effective for CP to connect to ANPNetInf. The connection might actually increase CP's cost, not reduce it. In this case, it might make sense for ANPNetInf to pay. ANPNetInf could then cover the cost from its own customers, which could be very hard to sell in a competitive market.
2) With respect to **the flow of interconnection fees between ANPNetInf and ANP,** the following options are available to cover the costs of interconnection:
   - No change to interconnection fees. This is normally a revenue-neutral peering arrangement where each network covers all its interconnection costs from its own customers.
   - Payment from ANP to ANPNetInf. Setting up and operating the NetInf system by ANPNetInf does not have any impact on the needed interconnection capacity between these two players. But ANPNetInf can now provide better QoS (faster content delivery), which may justify the payment to cover some of its costs due to setting up and operating the NetInf systems. ANP may also have an option to connect via Interconnectivity Provider (ICP), but in that case both players should pay more transit fees.
   - Payment from ANPNetInf to ANP. This makes little sense. The price of transit for both ISPs should be used as a reference price. However, the deployment of NetInf does not mean any change to the interconnection needs.
3) With respect to **the flow of interconnection fees between ANPNetInf and ICP,** the following options are available to cover the costs of interconnection:
   - No change to the interconnection fees due to the deployment of NetInf. ANPNetInf has to cover the costs from deploying NetInf from its own customers.
   - Due to the deployment of the NetInf concept less interconnection capacity is needed and that causes damage to the business of INP. Because of the reduced need for the interconnection capacity ICP may need to increase the interconnection fee per capacity unit in order to cover their operating costs. This would be applied for all interconnections provided by INP.

3.6.1.3 Interconnections and their costs in Virtual CDN Value Network Configuration (Virtual CDN VNC)

One potential use case for NetInf is a distributed CDN [2]. Here**,** a Virtual NetInf Provider (VNetInfP) controls customer relations with Content Providers (CP). The cache servers are managed by the multiple Access Network Providers with cache servers (ANPCache) instead of a VNetInfP, and, thus, the VNetInfP has a business relationship with each ANPCache. In this VNC, the content network management (cache selection) and name resolution (cache vs. server selection) roles are controlled by the VNetInfP, who as a consequence has the strategic position to offer content delivery services to CPs with guaranteed QoS.

The VNetInfP solves the ANP-driven VNC's inconvenience of CPs having to sign, potentially, contracts with several ANPs. Instead, only one contract with the VNetInfP is enough. Thus, the revenue logic lies in the VNetInfP charging CPs for the guaranteed QoS [2].

In the pure CDN case, the ANP owns the cache location and the CDN owns the cache servers. However, as the cache location owner controls who can place cache servers in its premises, the ANP may not wish to enter into agreements with the CDN if the ANP considers the CDN as a competitor for its own content. Thus, the virtual CDN configuration has an advantage compared to the Pure-play CDN VNC because ANPCache owns both the cache management and cache location ownership roles.

For this concept the data flows and interconnection costs have been illustrated in Figure 18. In the illustrated network topology all interconnections are not necessarily new, but the deployment of the NetInf concept has an impact on the needed interconnection capacity and on the end-user perceived QoS.

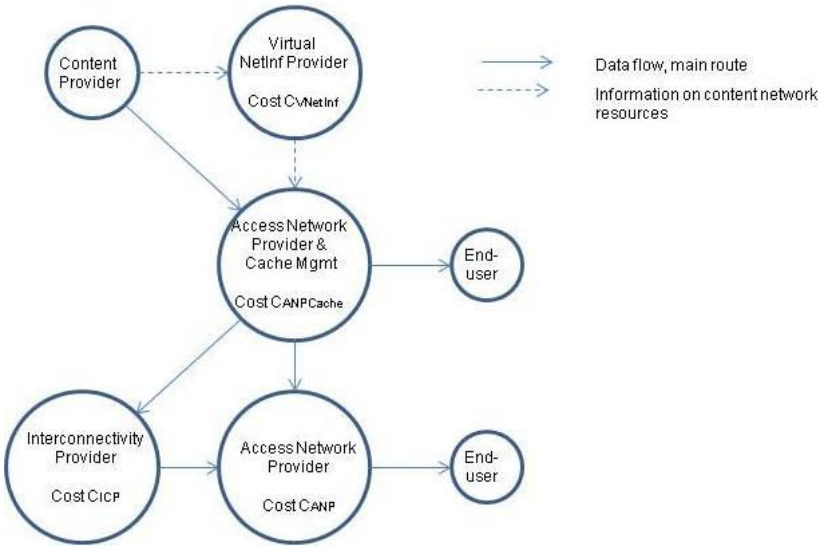


Figure 18. Data flows in the Virtual CDN VNC.

The impacts on the interconnection cost levels (low/medium/high) for different players from setting up and operating the NetInf-based content delivery networks and savings in the interconnection fees are presented in Table 5 below.

The table is helpful in understanding the level of costs in setting up and operating the NetInf, in the context of the Virtual CDN VNC, and the level of savings in interconnections because of those investments.

Table 5. Interconnection costs and benefits in Virtual CDN VNC.

Costs		Content Provider	Virtual NetInf Provider $C_{VNetInf}$	Access Network Provider & Cache Mgmt $C_{ANPCache}$	Access Network Provider C_{ANP}	Interconnectivity Provider C_{ICP}
Set Up	*Capital Costs*	low	medium[6]	medium[7]	n/a	n/a
	Transaction Costs	medium[8]	high[9]	medium	n/a	n/a
Operational	*Operating Costs*	low	high[10]	medium	n/a	n/a
Savings in inter-connection fees		high[11]	n/a[12]	high[13]	n/a	n/a[14]

n/a = no additional costs nor savings

The **following remarks** on the costs can be made:

- The level of investment in NetInf by the Access Network Provider is on the medium level, because of no investment in the content management system. That investment has no direct impact on the actual cost of setting up an interconnection link, however.
- The Virtual NetInf Provider has medium level set up and high operating costs for running the content network management and name resolution service, especially because of the multiple Access Network Providers it has to negotiate with. Only a part of those costs can be considered as interconnection costs, however.
- The investments in NetInf by the Virtual NetInf Provider and Access Network Provider will dramatically reduce needed interconnection capacity between the Content Provider and the network, which leads to lower interconnection fees.
- The interconnection capacity needed by the Access Network Provider is not affected by the investments made by other parties.
- Less interconnection capacity is needed from the Interconnectivity Provider due to content caching. Downsizing capacity investment does not directly reduce the operational costs; the operational costs per interconnection link may increase.
- The investment in NetInf will dramatically reduce the interconnection fees paid by the Access Network Provider who is running the cache servers.

Flow of Interconnection fees

The flow of interconnection fees, between 1) the Content Provider (CP) and Virtual NetInf Provider (VNetInfP), 2) VNetInfP and ANPNetInf, 3) ANPNetInf and Interconnectivity Provider (ICP), and 4) ANPNetInf and Access Network Provider (ANP) have been discussed in the following. Here we are interested especially in the changes to the interconnection fees due to the deployment of the NetInf concept.

[6] The total costs of setting up NetInf are divided between VNetInfP and ANPCache.
[7] See Footnote 5 above. No investment in content management.
[8] CP has to negotiate the contract only with VNetInfP, not with several ANPs.
[9] VNetInfP has to negotiate the contracts with CPs and ANPs, which are responsible for the cache location and management. The transaction costs are on the medium level per ANP, however.
[10] VNetInfP is reponsible for the QoS of the service delivery. That has to be monitored together with ANPCaches.
[11] Less interconnection capacity is needed from CP to network
[12] VNetInfP is a new player who needs interconnection capacity for content network management and name resolution. VNetInfP does not need interconnection capacity for delivering content.
[13] Less interconnection capacity is needed from INP
[14] Less interconnection capacity is needed from the INP and for that reason it will lose a lot of its fees from interconnection

1) With respect to the **interconnection between CP and VNetInfP,** this is a new interconnection, but only a small amount of interconnection capacity is needed because the actual content will be mainly downloaded from the cache servers. The costs of interconnection are about equal for both players. Because VNetInfP is the service provider for CP, it is important that the interconnection fee is clearly separated from the rest of the service fee. If VNetInfP would have significant market power, they could try to get a high interconnection fee for accessing the service, but also in this case the limit to the interconnection part of the fee would be set by the fee required by the Interconnection Network Provider. With respect to the flow of interconnection fees between CP and VNetInfP, the following options are available:
   - No interconnection fees. In this option each party covers all its internal costs from its own customers. For VNetInfP, the other (than CP) customers are the ANPCaches.
   - VNetInfP imposes a fee to CP for the delivery of their content with the required level of QoS. The payment helps to cover some of the set up and operating costs of the NetInf concept, but those costs are not directly related to the interconnection between these two players. It is important that the interconnection fee and the service fee have been separated, and the reference fee to the interconnection fee can be received from the interconnection via ICP if such is available. If there are several competing VNetInfPs, they may want to keep the interconnection fee as well as other service fees as competitive as possible, and that should be supported by the Regulator. The End-user perceived QoS, provided together with ANPCaces, could be a means to differentiate between the competing VNetInfPs.
   - Payment from VNetInfP to CP. If CP has very interesting content to deliver, VNetInf may want to pay a part of the interconnection fee in order to extend its own service portfolio. However, it may be difficult to separate the interconnection fee from the rest of the service fee.

The discrimination of the CPs by the VNetInfP may be an issue and should be prevented by the Regulator.

2) With respect to **interconnection between VNetInfP and ANPCache**, this is also a new Interconnection, but only a low interconnection capacity is needed because the actual content will be mainly downloaded from the cache servers. The costs of interconnection are about equal for both players and are not high because of the low capacity needs. The separation of the Interconnection fee from the service fees is important. With respect to the flow of interconnection fees between VNetInfP and ANPCache, the following options are available:
   - No interconnection fees. In this option each party recovers all interconnection costs from its own customers.
   - Payment from VNetInfP to ANPCache. VNetInfP is a new player and the successful entry to the market requires the agreements and interconnections with ANPCaches. Without interconnections a VNetInfP could not provide the content delivery service to the CPs. The fee could be justified if the costs of setting up and operating the cache servers are high compared to the costs of setting up and operating the content network management and name resolution functions; or, there should be separate SLAs between the parties. Since there may be several competing VNetInfPs using the capacity of cache servers it is important to understand how much of their capacity is used by each VNetInfP and clearly separate the pricing of that capacity from the interconnection pricing. The price of transit via an ICP sets a kind of reference price for the direct peering between the parties.
   - Payment from ANPCache to VNetInfP. This could make sense, if ANPCache is a small, rural ISP, who wants to provide a high quality service offering to its customers and if the investment to the cache server(s) is at a reasonable level. Also, it may be too costly for a VNetInfP to interconnect directly with a rural ISP. The Regulator should

support the low interconnection fee for ensuring the equal access to services for all End-users.

If VNetInfP can provide a unique service (some exclusive deal with an interesting CP), there would be pressure also for the big ANPs to pay VNetInfP for the higher service fees.

With respect to **interconnections between** 3) ANPNetInf and Interconnectivity Provider (ICP), and 4) ANPNetInf and Access Network Provider (ANP), there is no change to the respective interconnections in the ANP-driven VNC.

Because of the investment in the cache servers an ANPCache cannot justify the raise to the interconnection fees with other ANPs. That investment has not an impact on the interconnection costs between those parties.

3.6.2 Regulatory analysis of charging options in NetInf Interconnections

The regulatory approaches for Interconnection charging presented in section 2.4 have been applied for the NetInf Interconnections in the following sections. The **criteria for assessing the importance** of Interconnections were presented in [2], section 6.4. They included: 1) Investments, 2) Competition, 3) Market entry, 4) Innovation, 5) Efficiency, 6) Security, 7) Universal Access, 8) Justice w.r.t. scarce resources and 9) National competitiveness. Of these criteria, the items 1) – 5) are most relevant when analysing the interconnection charging schemes in the NetInf context.

3.6.2.1 Regulatory analysis of charging options in ANP-driven Value Network Configuration

The regulatory approaches presented in section 2.4.2 have been applied to the ANP-driven VNC in Table 6.

Table 6 Regulatory approaches in the ANP-driven VNC.

Criteria	RoR	Price ceiling	Cost orientation
Prevents exercise of market power	Yes. It restricts the amount of profit (return) that a regulated party can earn.	Yes. It restricts the amount of profit that a regulated party can earn.	Yes. The price of a service, or of the improved quality of interconnection service will consist of its cost + reasonable rate of return. The investment in NetInf would benefit both operator's own customers and the customers behind the interconnection link
Promotes competition	No. This does not permit pricing flexibility for a party to set prices to reflect forward-looking costs in response to competition. However, if a party does not care of the level of costs, it will be eaten by the competition.	Yes. The party has sufficient pricing flexibility to respond to competitive pressures by setting prices that reflect underlying costs and demand conditions.	Yes. The party has to set prices that reflect underlying costs. No cross-subsidization is allowed.
Ensures productive efficiency	No. The party will not reap the benefit from reducing costs. However, the overall efficiency of providing services will increase by deploying the NetInf facilities. Less interconnection capacity is needed.	Yes. The parties are rewarded with higher earnings when they reduce costs (and penalized when costs increase).	Yes. In the case of forward-looking cost accounting. No. In the case of backward-looking cost accounting.

Ensures allocative efficiency	No. The prices for individual services need not equal the cost of the service. There is no incentive for an Access Network Provider to invest in and run the interconnection service, and NetInf in an efficient way.	Yes. The parties have flexibility to set prices for individual services. If NetInf is seen to reduce the cost of interconnection and improve the quality of service, it will be invested on.	Yes. Prices for individual services equal the costs of a service. There is an incentive for an operator to invest in and run the interconnection service, and NetInf in an efficient way.
Ensures dynamic efficiency	No. No big incentive to invest in new technologies or services which would improve the efficiency of a certain service. E.g. investment in NetInf would improve the quality of interconnection service	Yes. The parties have incentives to improve efficiency. The NetInf will reduce the interconnection fees paid by the operator.	Yes. The operator has incentives to invest efficiently, service by service.
Minimizes regulatory costs	No. The rate determination proceedings would be lengthy, because the value of the NetInf facilities for the interconnection service would be difficult to define	Yes. The price ceiling setting procedures are not frequent.	No. The control proceedings are resource intensive. The control of profits service by service implies that the setting up and operating costs can be monitored service by service.

Productive efficiency requires that goods and services should be produced at the lowest possible cost.

Allocative efficiency requires that the prices one observes in a market are based upon and equal to the underlying costs that a society incurs to produce those services (generally the long-run incremental cost of producing the service).

Dynamic efficiency requires that firms should have the proper incentives to invest in new technologies and deploy new services.

The table above summarizes how the different regulatory targets would materialize with the different regulatory approaches to interconnection charging. The following remarks can be made:

- **Rate of Return** approach would have positive impact by preventing a party, especially the Access Network Provider with the NetInf facilities, to exercise its potential market power, but this approach would not contribute to the other regulatory targets. I.e., this approach would not promote competition because of inflexibility to base pricing on the forward-looking costs; productive efficiency would not be ensured because of no benefits from reducing costs; allocative efficiency would not be ensured because the service would not need to equal the costs; dynamic efficiency would not be ensured because of no incentive to invest in new technologies; and regulatory costs would be high.
- **Price ceiling** approach would have positive impacts on all regulatory targets. The interconnection fees would be based on the interconnection costs and the operator would seek opportunities to reduce the costs. The investment in the NetInf facilities would reduce the costs of interconnection and would improve the quality of service perceived by the End-users. Less interconnection fees would be paid.
- **Cost orientation** approach would mainly have positive impacts on all regulatory targets. The competition and efficiency would be supported because the interconnection fees should be based on the underlying interconnection costs plus a reasonable rate of return. The productive efficiency would be supported but only if the forward-looking cost accounting would be applied. The regulatory costs would not be

minimized, however, because the control of profits implies the monitoring of costs service by service.

3.6.2.2 *Regulatory analysis of charging options in Virtual CDN Value Network Configuration*

The regulatory approaches presented in section 2.4.2 have been applied to the ANP-driven VNC in Table 7 below. The focus of this analysis is on the Virtual NetInf Provider and Access Network Provider managing cache servers. They together are called here 'concerned parties'.

Table 7 Regulatory approaches in the Virtual CDN VNC.

Criteria	RoR	Price ceiling	Cost orientation
Prevents exercise of market power	Yes. It restricts the amount of profits that the concerned parties can earn.	Yes. It restricts the amount of profit that the concerned parties can earn.	Yes. The price of a service, or of the improved quality of interconnection service, will consist of its cost + reasonable rate of return.
Promotes competition	No. This does not permit pricing flexibility for a party to set prices to reflect forward-looking costs in response to competition.	Yes. The concerned parties have sufficient pricing flexibility to respond to competitive pressures by setting prices that reflect underlying costs and demand conditions. Virtual NetInf Providers and Access Network Providers with cache servers are competing with the respective players in their segments.	Yes. The party has to set prices that reflect underlying costs. No cross-subsidization is allowed. A challenge here is, however, how much of the costs of the NetInf facilities can be allocated to the interconnection costs.
Ensures productive efficiency	No. A party will not reap the benefit from reducing costs. However, the overall efficiency of providing services will increase by the deployment of the NetInf facilities and by the establishment of the Virtual NetInf Provider.	Yes. The parties are rewarded with higher earnings when they reduce costs (and penalized when costs increase).	Yes. In the case of forward-looking cost accounting. No. In the case of backward-looking cost accounting.
Ensures allocative efficiency	No. The prices for individual services need not equal the cost of the service. There is no incentive for the concerned parties to invest in and run the interconnection service, and NetInf in an efficient way. However, the competition from other players will push the parties to keep the NetInf facilities and interconnection costs down.	Yes. The parties have flexibility to set prices for individual services. If NetInf is seen to reduce the cost of interconnection and improve the quality of service, it will be invested on.	Yes. The prices for the individual services equal the costs of a service. There is an incentive for a party to invest in and run the interconnection service, and NetInf in an efficient way.
Ensures dynamic efficiency	No. No big incentive to invest in new technologies or services which would improve the efficiency of a certain service.	Yes. The parties have incentives to improve efficiency and invest in new technologies. The NetInf facilities will	Yes. The parties have incentives to invest efficiently, service by service (including interconnection).

	However, the investment in the NetInf facilities would improve the quality of the service delivery.	reduce the interconnection fees paid by the Access Network Provider. The interconnection fees paid by the Virtual NetInf Provider may be quite low.	
Minimizes regulatory costs	No. The rate determination proceedings would be lengthy, because the value of NetInf for interconnection would be difficult to define	Yes. The price ceiling setting procedures are not frequent.	No. The control proceedings are resource intensive. The control of profits service by service implies that the setting up and operating costs can be monitored service by service.

Productive efficiency requires that goods and services should be produced at the lowest possible cost.

Allocative efficiency requires that the prices one observes in a market are based upon and equal to the underlying costs that a society incurs to produce those services (generally the long run incremental cost of producing the service).

Dynamic efficiency requires that firms should have the proper incentives to invest in new technologies and deploy new services.

Table 7 above summarizes how the different regulatory targets would materialize with the different regulatory approaches to interconnection charging. The remarks are mainly the same as in the case of the ANP-driven VNC:

- **Rate of Return** approach would have positive impact by preventing a party, especially the Virtual NetInf Provider and the Access Network Provider with the cache server, to exercise its potential market power, but this approach would not contribute to the other regulatory targets. However, the overall efficiency of providing services would be increased by the deployment of the NetInf facilities and by the entries of the new Virtual NetInf Providers. Also, the competition from other players in the same market segment will push the parties to keep the interconnection costs down.
- **Price ceiling** approach would have positive impacts on all regulatory targets.
- **Cost orientation** approach would mainly have positive impacts on all regulatory targets. The regulatory costs would not be minimized, however, because the control of profits implies the monitoring of costs service by service.

3.6.3 Available Regulations on Internet Content Delivery

This section discusses the current legislatives on Internet content in Finland. The focus areas include privacy, copyright, content control and consumer protection related regulations. In addition, for each focus area, the available court case examples will be examined briefly.

3.6.3.1 Privacy

User privacy and data protection are important issues in the Internet, where users' privacy is violated frequently both intentionally and unintentionally. For example, a research done by Mayer [42] indicates that when visiting certain website, your private information such as age, gender and e-mail address, is sent to several other sites. These sites include several large news agencies', e.g. CNBC, Reuters and Wall Street Journal, as well as social networks. In the following, a brief explanation on the privacy related EU legislations is given.

User privacy can be divided into two sub-categories: the publisher's privacy and the content consumer's privacy. On the publisher side, privacy means the ability to publish anonymously. Whereas content consumer's privacy deals with what is commonly perceived as user privacy, e.g. protecting user's private data, such as usernames, e-mail addresses, phone numbers, etc, and usage statistics.

On the EU level, no clear legislation that grants anonymous publishing to content providers exists. From the Finnish legislation, a requirement for the content provider's identity is found [43] where the content provider's name, contact information, trade register and VAT identification should be always available to the content consumers and authorities. However, whether this applies to mini-content providers, such as home video publishers, is not clear.

DIRECTIVE 2002/58/EC [44] requires the content providers to process users' personal data with confidentiality and protect the security of its services and states that private communications and information should not be stored without the consent of the users. In addition, this legislation mandates that the traffic and location data should be erased when they are no longer needed for billing or communication purposes. The Finnish implementation of the legislation can be obtained from Ministry of Justice [45].

3.6.3.2 Copyright

As the popularity of accessing electronic versions of content increases, also the amount of copyright infringements has increased. With the emergence of peer-to-peer networks, piracy of music, video, applications and other content have been on the rise. The trend has, however, shifted towards video traffic between consumers and servers in the recent year [18] due to better quality of service. This to some extent has reduced copyright issues of video traffic, but even the legal service providers, such as TVKaista in Finland [46][47], have had legal disputes regarding copyrights.

Several legislations on the protection of intellectual rights and copyright exist on the EU level, such as the DIRECTIVE 2001/29/EC [48] and COM(2009) 532 [49]. In the latter, different stakeholders' perspectives are examined and the issues related to orphan works are raised. In addition, the increased amount of user-generated content has been identified as a regulative challenge and investigations on how to protect their rights are planned.

3.6.3.3 Content Control

Content control in this work includes the division of liabilities and the control over the actual content in terms of distribution and processing. No specific regulation exists on who controls the content once it leaves the origin server as it depends on the agreements between the content provider and the possible CDN or service provider. On the other hand, the Act on the Provision of Information Society Services – Electronic commerce [50] states that the service provider is not liable for illegal content if the service provider simply provides a technical solution and is not involved in producing the illegal content.

3.6.3.4 Consumer protection

Consumer protection includes ensuring content access and filtering of illegal or harmful content or marketing. In addition, consumer's privacy is part of consumer protection. Regulation on consumer protection of Internet content is almost non-existent. However, consumer protection on physical goods and services as well as audiovisual and media services to some extent can be applied to Internet content.

3.6.3.5 Impact on NetInf

The findings suggest that content related legislation is inadequate. This can be positive for NetInf's deployment, as no regulation will limit or guide the development. On the other hand, some of NetInf's limitations such as CP's control could be solved by regulatory means.

3.7 Conclusions

Section 3 discussed several issues related to NetInf deployment from both economic and regulatory perspectives. The key findings are summarised in this section. Section 3 started with an overview of the existing ecosystem by identifying the key trends and uncertainties of the Internet content delivery market as well as the current caching technologies. Based on the understanding of the current situation, six steps for NetInf deployment are proposed.

The identified uncertainties helped in forming four future scenarios, which represent the end user's preferences and choices in the Internet content delivery market with regard to content bundling and payments. The four scenarios thus formed are named according to the end user' preferences: *Comfort Buyer*, *Indifferent Saver*, *Quality Buyer* and *Demanding Saver*. Each scenario identifies the corresponding winning business role and the related winning actors that get control over the Internet content delivery market and can decide which caching architecture to use. Based on the winning actors of each scenario, an overview of the possible dominating caching architectures can be reached. In-network caching, whether Information-centric networking or web proxy caching, are strong candidates for the *Comfort Buyer* and *Indifferent Saver* scenarios. On the other hand, content delivery networks (CDNs) – either pure-play CDNs or content provider-built CDNs – and clouds are possible outcomes in the *Quality Buyer* and *Demanding Saver* scenarios.

A key finding from the caching study include the current situation of CDN providers, who are looking for further business opportunities by improving their interoperability and interconnectivity as well as by licensing their CDN technologies. In addition, the caching study together with the VNC analysis of D.A.7 identified four key control points: the user access, request routing, cache management and delivery choice decision. The management of the control points differs in caching architectures and keeping each of the actors satisfied in NetInf will be a key success factor for NetInf deployment.

With the understanding of the current market situation, a six step evolutionary NetInf business model adoption strategy is proposed for ISPs. The first step is internal network optimization, which uses NetInf to optimize the content delivery of ANP-provided services inside an ANP's network. After this, the ANP can build a transparent caching system for cacheable content originating from sources external to the ANP, i.e. a localized CDN system. The next step commercialises the localised CDN system by providing CDN services to content providers, which is followed by interconnecting the commercialised CDN with other commercialised CDNs offered by other ANPs. Lastly, a virtual CDN provider can enter the market to handle the customer relationship with CPs.

Lastly, three potential approaches for the interconnection charging, which could be promoted by the regulators, are explained and analysed: Price ceiling, Cost orientation and Rate of return. The analysis shows that the Price ceiling -approach seems to have positive impacts on all regulatory targets. In this approach the interconnection fees are based on the interconnection costs and the operator should seek opportunities to reduce those costs.

The Cost orientation -approach would have positive impacts on most of the regulatory targets, but would not minimize the regulatory costs, because the control procedures are resource intensive. The Rate of return -approach would prevent the parties to exercise their potential market power, but would not contribute to other regulatory targets; for instance, this approach would not promote competition because of inflexibility to base pricing on the forward-looking costs.

Even if the accurate information on the interconnection and NetInf costs was not available in the analysis, the Price ceiling and Cost orientation based regulatory approaches seem to have about equal impacts on the regulatory targets and should be promoted by the regulator. Investments in the NetInf facilities would be a good means to reduce the costs of interconnections and would also improve the quality of service perceived by the end-users. Then, the competition on the end-user perceived quality of service would stimulate new innovations. The clear separation of the interconnection costs and fees from the other service costs fees would be necessary for ensuring the fair pricing and competition, and for fulfilling the principle of 'Net neutrality'.

4 Business Analysis of OConS

This chapter addresses OConS business aspects. Business drivers are identified in the beginning, identifying the scenarios under analysis and related traffic aspects, after which an ecosystem analysis is performed by listing both challenges and requirements. Then, the network analysis is shown, identifying the stakeholders, followed by an analysis of the pros and cons in the roles they play in this architecture. Afterwards, business models are discussed, concerning several scenarios on who bears the deployment costs, with an identification of the revenue flow. Before the conclusions, regulation aspects are addressed.

In the scenario defined for WP-C supporting Flash Crowd connectivity needs, four use cases were initially defined and already presented in D.A.1 [1] and D.C.1 [62]:

- *Use Case 1*: Creating and sustaining the connectivity in wireless challenged networks;
- *Use Case 2*: Using multiple path/protocol transport for optimised service delivery of heterogeneous content;
- *Use Case 3*: Optimising the QoE for end users with adequate management of the cloud/network services;
- *Use Case 4*: Autonomous interoperation and connectivity of cloud and NetInf data centres.

After the refocusing of WP-C, the use cases around the Flash Crowd scenario were redefined, aiming at the integration of WP-B (NetInf) and WP-D (CloNe) topics, as presented in D.C.1 Addendum [63]:

- *OConS for CloNe*: Mobile Access and Data-Centre Interconnection Use Case;
- *OConS for NetInf*: Mobile and Multi-P for Information Centric Networks Use Case.

Still, these two new use cases include the topics addressed by the former ones, i.e., *OConS for CloNe* is associated to Use Cases 3 and 4, while *OConS for NetInf* is linked to Use Cases 1 and 2.

OConS aims at improving connectivity, providing a flexible approach by means of orchestration [64]. In the previous report in WP-A regarding OConS aspects, i.e., D.A.7 [2], the focus was devoted to Use Case 1. An economic analysis was performed, and regulatory aspects were addressed concerning interconnection. In what follows, an economic analysis for another use case, Use Case 3, is performed, and the regulatory aspects for the previously identified use case, Use Case 1, within OConS for NetInf continue to be addressed.

4.1 Business Drivers

Business drivers start by identifying the scenarios under analysis, bridging with the work developed in WP-C. The actual drivers are discussed and identified, being followed by an analysis of a possible idea of how OConS can be implemented.

The purpose of this analysis is to identify the key valuation drivers for the OConS flexible approach and to consider its impact in several scenarios. OConS business drivers were taken into account, nevertheless, other aspects besides business drivers need also to be addressed and some questions are posed and tried to be explained:

- How do investors measure and value growth?
- What are the criteria used by investors in an initial valuation of targets?
- How does the traffic estimate affect the network value?

The first business driver for a new investment is capital. OConS incurs a high level of CAPEX in the process; however, overall network efficiency (one of the main capabilities of the network) will reduce OPEX costs in medium to long-term perspectives.

The innovation driver must also be taken into account. OConS enables to manage networks that already exist. Through a more flexible approach being delivered by OConS, some new running processes are presented, delivering a more optimised way to work.

With a more simplified organisation structure, a quick flow of information over the network can provide another key driver for the overall OConS business success. In OConS, this is achieved with, e.g., the multi-path attribute, which is a characteristic of this technology. OConS also creates a possible consolidation of business operations, meaning that one can operate all available networks from a single OConS platform centre, hence, decreasing management costs.

Another business driver is the improvement of economies of scale. Upon OConS implementation, an increasing number of connected devices will correspond to a decrease on the operation cost per unit, from the common operating process for all units, enabling a better coordination throughout the whole business. One will be capable of rapidly shift sourcing, path, and distribution functions in response to changing patterns of supply and demand.

In conclusion, the main business drivers that OconS follows are:

- High level of CAPEX
- Lower OPEX in a medium/long term;
- Network efficiency increasing in medium- to long-term;
- Innovative Processes
- Simplified organisation structure and a consolidation of business operations;
- Economies of scale (concerning operating costs);
- Traffic-management efficiency.

4.2 Ecosystem Analysis

Following the ideas presented in the use-cases and scenarios of OConS [1], several ad-hoc networks can be created, which facilitate Internet connection for multiple end users. A proposed mesh solution has been taken as a first step, and a more global solution was presented in Use Case 3 within OConS for CloNe, combining all the existing technologies [1].

Regarding a global and more extensive solution, OConS connectivity services are created from specific mechanisms that are requested on demand, and use a certain policy. OConS connectivity services are grouped into three classes:

- Link Connectivity Services
- Network Connectivity Services
- Flow Connectivity Services

Surrounded by all the devices that compose the Flash Crowd, several services can be created, offered, and provided by end users to end users. This can be done through some available networks (which can range from mobile cellular networks to Wireless Local Area Networks (WLANs)), all combined in one single network provided by all these infrastructure providers. The scenario under analysis is one where Base Stations / Access Points may dynamically become available and disappear. This has been developed in D.A.7 [2], where the idea of a Wireless Mesh Network can be complemented with the applications and services that Use Case 3 intends to support [62].

The general idea is the creation of ad-hoc networks that deal specifically with decision-making mechanisms that "optimally" choose the interfaces, the access networks, and the paths (and hence, schedule/map/route traffic flows accordingly) to achieve the highest possible QoE for an end user. QoE is a key element for this business model. The implicit added value is to create an appropriate management of connectivity and optimisation between all the players

present in the developed model. A win-win situation can be created with this new service, which can reward end users, and augment the quality and capacity of ad hoc networks to the levels of involvement of each player. All actors have key characteristics in the return of investment policy, and the provision of different scenarios for each player to support this new technology can help to establish a decision to invest.

In what follows, some challenges to the implementation of OConS were identified, and then, some requirements are put forward. The challenges to be faced from the OconS approach are from various perspectives, e.g., collection of network information, network capacity, liability of information, decision making procedures in the network, and application to different levels of the network.

- **Challenge 1**: **Collection of Information**
  From the viewpoint of gathering information, one must consider several available sources that are at the disposal of the network, e.g., end-users, access networks, and core networks, and how they can deliver that information to the relevant element in the network infrastructure. Each one of these players will have a significant benefit by adopting this new technology from an economic viewpoint. The end-user will reduce the time to collect network information by having a constant “on the fly” connection, and network players can reduce costs with the constant information collection by optimising the network according to this aspect. The capacity of choosing which node of the network is available to transmit to another the information to be shared, if optimised, will also reduce infrastructure costs and maximise profits. The storage of large volumes of information, and then to deliver the contents in a dynamic and efficient way, from one network node to another, is one of the challenges that is identified.

- **Challenge 2: Information Credibility**
  The trustfulness of the information that is being gathered on Challenge 1 is another challenge that one must take into account; from a business viewpoint, this is crucial for the success of the operation. If a client does not trust the information from the network, he/she will restrict him/herself from using it, and the service, which becomes more successful as more clients use it, will suffer a severe setback. One needs to make the most out of end-users’ behaviour and their contextual information, e.g., the routes that the users usually take and the services they usually request. Privacy, and several types of security for the collected information, need to be ensured, in order to have a proper performance and quality of the network. In terms of quality, once again, the measure of QoE should be taken into account, for an adequate assessment of the network. Also, the required capacity of information that is needed to store and receive/transmit in a node has to be considered. Given a requested service, the network needs to have procedures to decide on which is the best path to route the information.

- **Challenge 3: How to decide the path to use over the network?**
  The capability to take decisions and apply them in the network is another challenge. Which player can control a given ad-hoc network? Which path to use if the demand is high? Each decision mechanism must consider all the characteristics of the players, in order to make the best use of them from a business performance viewpoint. Another matter is the development of cooperation strategies between players. They should be efficient, updated in real time, and allow other players to be a part of infrastructure; the profit that each player can receive (not only in terms of money, but also in other terms, e.g., access advantages) will contribute to the success of the development of network services.

- **Challenge 4: Who takes control of the network path decision?**
  A player will have more added value if it has more control over the network, namely on the routing of information. The network must control the load that goes through a node, which path to take to route it at a certain point in time and to change this when required, and to

be able to take these decisions accounting for economic parameters as well. The heterogeneity of the network must be constantly exploited in order to take advantage of all available paths. So, the role that players will have in the various networks nodes, management, and so on, will be crucial.

So, for the success in applying OconS, some economic and business requirements are presented below, identifying in each one, if they are Business (B), or Social (S) related.

- **OConS-R1: Increasing Network Performance (B, S)**
  Service operators are interested in increasing the network performance. For a successful implementation, all the technologies that are being combined in this new approach must have good quality of service. It is critical that the overall quality of service is maintained in most cases dealing with multi-path routing for ad-hoc networks.

- **OConS-R2: Proper work of the Network and Network Conditions (B)**
  This means that the available types of technology offered by the network are interworking well. One should also assume that the network has conditions of being operated efficiently, and that integrity is being preserved (the latter by means of suitable security solutions).

- **OConS-R3: Need of Information (B, S)**
  This requirement is usual for all new technologies, and a demand research must be put in place. The constant changing environment calls for frequent research, to make sure that the requirements coming from the information users need are met, and that information acquires the required speed to survive with the effective management of the information resources and plans for the future. In order to guarantee this, there is a critical need to understand the process of “identifying information needs”, which is a vital link in the chain of the network operations.

- **OConS-R4: Better Network Management (B, S).**
  There is a need to reduce the current time spent running and maintaining the network. In this requirement, one should take into account the need to reduce the cost of the network infrastructure and maintenance, the emerging need to reduce server spaces, and the increase of several features and capabilities.

4.3 Technical and Industry Architecture

More and more, the Internet traffic escalation is creating an uneven situation, as network capacity is struggling in some areas and in others is superfluous; each player has its own type of reward, but this is not being equally shared. The market has not yet undergone an adjustment. One can identify the following advantages of taking OConS solutions into the market, with a great potential for success:

- Resiliency: Due to distributed and autonomous approaches used in OConS, one recognises that the OConS framework offers higher resiliency (multi-path) compared to other approaches.
- Manageability: By using appropriate management models (e.g., domain-based), and by abstracting and filtering the information exposed by a given OConS mechanism, OConS framework is well suited to handle the management aspects in a better way than others technologies, more particularly with 3GPP EPS and with IETF MIF.
- Complexity: The rich set of connectivity services come with some complexity, however, one intends to keep this internally and to expose only what is really necessary; likewise, having the orchestration functionality in place will help one to cope with this complexity, because all the mechanisms and services need to follow a certain blueprint/interfaces as imposed by the OConS framework. In this specific attribute, the 3GPP EPS has a higher level of complexity when implemented.

- Energy Efficiency: This is achieved by using appropriate connectivity services depending on a given networking context, by configuring, deploying, and instantiating only the needed functionalities, and by re-using existing modules for several services (e.g., mutualising the Information Management Entities).
- Performance: OConS aims to achieve at least the degree of performance that the current networking mechanisms are providing; moreover, one is also proposing approaches that seek to jointly optimise the performances across multiple mechanisms and multiple layers from the networking protocol stack.
- Flexibility: Among the important aspects in OConS, one identifies its ability to stay open and flexible, accommodating a large number of mechanisms, spanning from data-link, network, transport to flow/session layers; depending on the context and on the application needs, OConS is able to combine and offer the most appropriate connectivity services.
- Scalability (signalling): OConS mechanisms are built with this in mind; the example of the mobility framework where the mobility decision and execution functions are distributed to a large extent is appropriate to work.
- Scalability (data): Due to inherent distributed approach, that the scalability of OConS data plane will stay high.

The revenue that is generated by service providers at the edge of the network, the value of the network specifically from online content and services viewpoint, and the growth in costs (and investments) that are being incurred by network operators, will necessarily imply that the costs associated to the new types of network architectures have to decrease.

Other aspects concerning the use of other technologies, competitors to OconS, have also to be taken into account. Technologies as 3GPP EPS, IETF MIF, and OpenFlow, have specifications that can be also relevant when implementing OconS.

The proposed network architecture is shown in Figure 19.

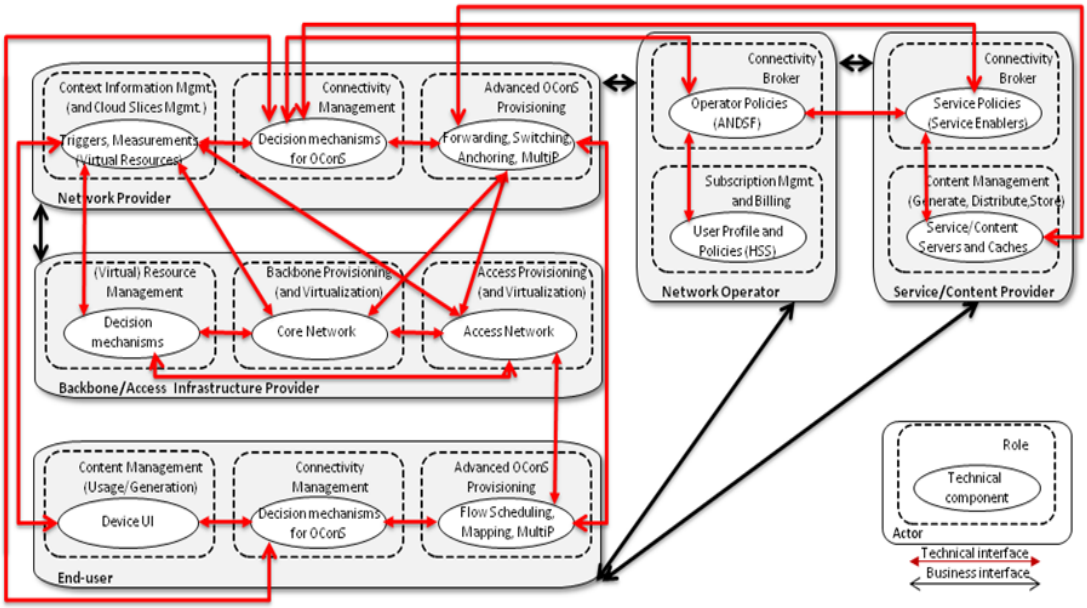


Figure 19. Network Architecture for OConS Use-Case 3 within OConS for CloNe [62].

This architecture will be the starting point for the development of the possible market scenarios that can be designed for the OconS entrance in the market. One can see that all players will interact among themselves, creating a network that an end-user can use, combining all the available technologies. The quality and performance of this new network are

some of the key successful ingredients for it to prevail in the market. Also, the relationship between cost and benefit needs to be taken into the analysis of the several implementation scenarios. Concerning the roles of each player, even if they can be well known from the current approaches, one proposes clearer relationships among them, so as to keep a high degree of flexibility for the business models as well.

4.4 Stakeholder Analysis

With the business development that one intends to create, and with the architecture previously presented (Figure 19), one has several key actors playing a role in the business model. Pros and cons are identified; concerning the role they play in the model and compared with the ecosystem that exists today.

- **End-user -** The End-user can be a human, a machine, a business user (such as cloud and/or service provider), an abstract "higher-layer application", or an information object (content). The End-user can be the source, the destination, or both for the communication services and/or the content. The End-user is one of the main actors within the use case 3, since the decision to be made will likely have impact on his/her/its QoE [73].
  Pros:
  - Transparent and access-agnostic connectivity to services and content and better/personalised end-to-end QoE.
  - It is always served with the most appropriate network access alternative; depending on the factors used to take the decision on network access, the goodness is perceived by means of several parameters, e.g., better performance, lower price, and/or lower power consumption.
  - If Multi-P is allowed, reliability and performance enhancements might be brought up by using (in parallel) various interfaces.

  Cons:
  - The required terminal complexity, in order to handle all the available features.
  - The dependence on the availability of specific technologies/techniques/procedures.
  - The increase of energy consumption (if using various interfaces at the same time).
  - Privacy considerations (information flow between providers, with which the end-user may not have agreements).

- **Infrastructure/Resource Provider -** The Infrastructure/Resource Provider is the stakeholder that provides the physical means for communication, thus, it owns and manages the physical and virtualised resources of the infrastructure, and it offers them to Network Providers. Examples are Hotels, Municipalities, Transportation Companies, current Telecom Operators, among others.
  Pros:
  - The efficient use of the available resources, e.g., via load balancing.
  - The increase of the overall available capacity.
  - The improvement of user (client) satisfaction.

  Cons:
  - The need to cooperate with other providers (leading to potential privacy concerns, and other conflicts).
  - The increase complexity of the network.
  - Depending on the particular conditions of networks, some providers may get their traffic reduced (by more aggressive counterparts) or exploding (causing their clients to be unsatisfied).
  - The need for a tight interoperability between heterogeneous technologies.

- **Network Provider -** The Network Provider uses the infrastructure and resources to build and provide networking services, i.e., those foreseen by OConS. They usually maintain a business relationship with the Network Operators, to get paid for the right-of-use/leasing

and for the maintenance of their networks. A Network Provider can be also seen as Cloud/Virtual Network Provider where it requests, uses and consumes shared network services and resources provided by Network Providers; thus, the Cloud/Virtual Network Provider combines several service and resource offerings of various Network and Infrastructure Providers (both horizontally and vertically), and offers them to a third party. Examples are OConS Network Provider, Access Provider, Backbone Provider, Community Infrastructure Provider, Network Infrastructure Provider, Internet Backbone Provider, Internet Service/Access Provider, OConS Business User, and Virtual (or Cloud) Network Provider.

Pros:

- Provision of optimal application-aware connectivity services.
- Lower OPEX by using the shared infrastructure from Infrastructure Providers, and/or the capabilities of other Network Providers.
- Optimisation of network resources for the delivery of content (e.g., connectivity management/intelligence distributed in the right places within the network).

Cons:

- The need for the availability of cooperation schemes between peer entities.
- The increased complexity of the network.

- **Network Operator -** The Network Operator provides Connectivity Services to end-users, it maintains the adequate level for these services, and it performs overall operation/management of these communication services. The Network Operator may, or may not, own the underlying infrastructure or other networking assets (e.g., radio spectrum). Likewise, the Network Operator benefits from the OConS capabilities to offer better services to end-users (who will be more satisfied), and to cope with the traffic increase from Service/Content Providers (who will be able to expand their services). The Network Operator has a business relationship with the End-users (e.g., billing), Network Providers, and with the Service/Content Providers. Examples are current Telecom operators, both infra-structured and virtual mobile ones.

  Pros:

  - The increase of customers' satisfaction, and the prevention of churn.
  - Greater productivity for business users.
  - Generation of more revenue per-user by enabling customised/personalised offerings.
  - The enabling of closer partnerships with Content/Service Providers.

  Cons:

  - The need to establish cooperation mechanisms with other operators.
  - The increased complexity in the required procedures.
  - Privacy issues (in terms of the information that should be made available).

- **Service/Content Provider -** This actor will benefit from the optimum connectivity of End-users, e.g., being able to adapt the QoS; it does not have a direct role on the whole process, rather than the specific parameters that must be considered when taking the decision. They can be called has Over-the-top (OTT) provider, examples being current Internet content providers (e.g., Google, Facebook, and Apple).

  Pros:

  - The possibility to increase the quality of the offered service (as a consequence of the optimum connectivity).
  - New business opportunities from open APIs with the network side.

  Cons:

  - The need for new interfaces (business and technical ones) towards Network Operators.

4.5 Business Models

For the implementation of the technologies under development, one should explore several scenarios, analysing the role that each actor plays in the network, concerning not only the application incurred costs, but also the retrieved benefits and revenues. When analysing the problem, one needs also to answer three questions:

- How do we introduce this technology in the market?
- Which player(s) will support implementation costs?
- How will they take profit out of the investment?

These questions are addressed while developing the four scenarios that are described below.

One starts by presenting the service delivery model in between the various players identified in the network architecture (Figure 19), Figure 20. The services that are being delivered from a player to another are presented, the model being the same for all scenarios that are presented afterwards. There is a unique structure and plan for the delivery of services and that is explained as follows:

- Arrow 1: Network Provider - End-User relationship: The Network Provider controls the service offer and delivers the service/product to the End-User. This is not a money flow transaction; however, it is important to be represented, because it is the visible return of the payment made by the End-user.
- Arrow 2: Network Provider – Network Operator relationship: It represents the technology package that is being supplied, and it is delivered to the operator so that it can put it in the market for selling purposes.
- Arrow 3: Infrastructure Provider – Network Provider relationship: This service delivery is the infrastructure usage and maintenance that it is used by the Network Provider, to be then offered to the End-user.

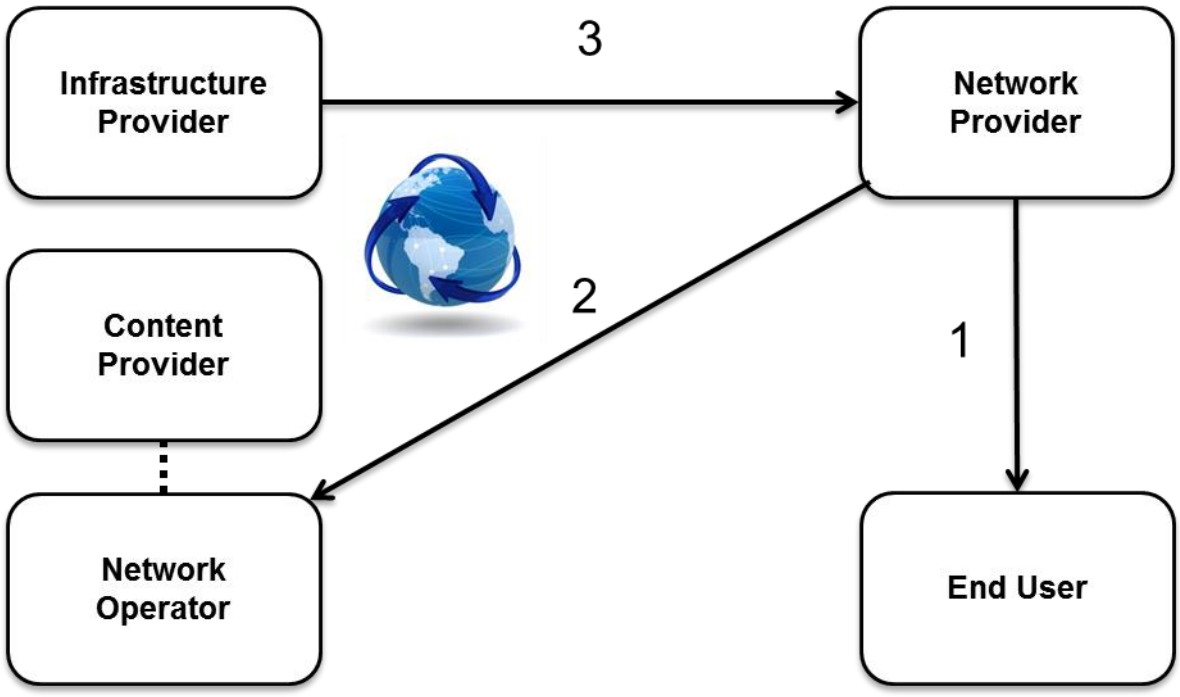


Figure 20. Services Delivered Scenario Model.

Having this common service delivery model as a background, four different scenarios concerning the entrance of OConS in the market were developed:

- End-user Cost-Benefit Scenario
- Network Operator Cost-Benefit Scenario

- Infrastructure/Network Provider Cost-Benefit Scenario
- Multi-player Cost-Benefit Scenario

In what follows, an analysis of these scenarios is presented.

1. End-user Cost-Benefit Scenario

In the “End-user Cost-Benefit” scenario, the payment for using the service appears in the End-user bill, as a new service that combines all the available networks that an End-user has contracted, and which are available to him/her. This player can benefit from an increase in the perceived quality, and a decrease in the more expensive connections.

The End-user is the only player that pays for the implementation of the developed technology. From an End-user viewpoint, this will become as a high level of costs, implying a low level of costs for the provider that sells the technology. In these conditions, there will be some barriers to enter the market, as the End-user will have to be convinced of the benefit to take the option to adopt the service. Performance will be also at a medium level, meaning that not everybody will use this innovative way of connectivity and interconnection. The scenario complexity in terms of business is assumed low, because the money flow is only a simple buy-sell issue.

Figure 21 represents the money flow for this scenario. The Content Provider is a player (Figure 19), but it does not influence the connectivity process; there is in fact a money flow with this player, but it is not within the scope of this analysis, as it is beyond OConS, hence the analysis of these scenarios. An explanation of the cash-flow follows:

- Arrow 1: End-User - Network Operator relationship: The End-user pays a certain amount of money in a fixed and flat rate, which is determined by the Network Operator. The idea is that the End-user stops using the conventional packages of Internet (i.e., ADSL+3G+WiFi+Mesh-Network+4G) and starts using OConS as an aggregator of them all with a combined price. The system controls all network accesses (traffic flow), adapting to the user needs and to the location where the need for connectivity exists.
- Arrow 2: Network Operator – Network Provider relationship: The Network Operator acts as a broker, by collecting the fee that the technology sale provides. The Network Operator is the agent and the interface to the End-user of the technology service, receiving a percentage, and paying to the Network Provider for the service.
- Arrow 3: Network Provider – Infrastructure Provider relationship: This is a simple client/supplier transaction, representing the payment for the usage of the network infrastructure that is being provided.

This architecture will be the starting point for the development of the possible market scenarios that can be designed or the OConS entrance in the market. One can see that all players will interact among themselves, creating a complex network that an end-user can use, combining all the available technologies. The quality and performance of this new network are some of the key successful ingredients for it to prevail in the market. Also, the relationship between cost and benefit needs to be taken into the analysis of the several implementation scenarios. Concerning the roles of each player, even if they can be well known from the current approaches, one proposes clearer relationships among them, so as to keep a high degree of flexibility for the business models as well.

The euro coins shown in Figure 21 are a symbolic representation of the payments, in two colours (yellow and blue): the three yellow coins (Arrow 1) represent the visible transaction that is made, while the blue coins (Arrows 2 and 3) represent the costs of the process. The number of coins decreasing from the Arrow 1 to Arrow 3 is also a symbolic representation of the margin left by each payment to each player.

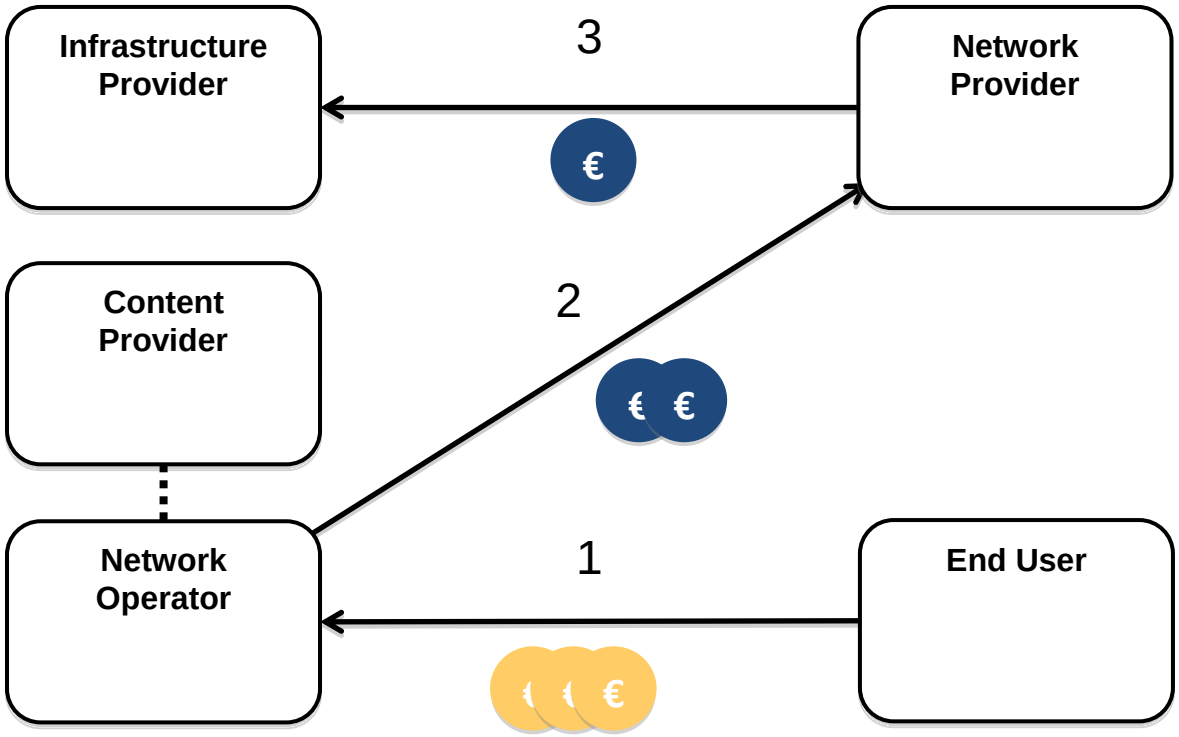


Figure 21. End-user Cost-Benefit Cash Flow Scenario Model.

The benefits of a scenario like this are that, as a first approach, it is quite simple to implement a pay-per-service model in the market nowadays; however, the price practiced by the service should be competitive in order to be successfully implemented. Another player that benefits from this scenario is the Infrastructure Provider, which has this new technology service implemented and sold almost in the first instance without having selling problems, as it is a service that benefits all provider players concerning network costs that can be reduced while operating the network.

One example of the good usage of this scenario is the recent implementation of LTE (4G) in Europeans markets. This new technology is being commercialised as an upgrade of UMTS (3G), better performances and services being delivered to the End-user. For this new technology, the End-user pays an additional premium fee.

2. Network Operator Cost-Benefit Scenario

Concerning a "Network Operator Cost-Benefit" scenario, Figure 22, it will have the cost process "at home", and can benefit from a reduction of constrain in several points of the network. There will be more available network for its clients, and it will also benefit from a more balanced traffic over the networks.

This scenario assumes that costs are incurred by the Network Operator in the beginning, but after achieving a mature point, it will start dividing the costs among the players: they take the operation costs, and the Network Operator will work only as a broker in this interaction. This scenario is more complex than the previous one, because the network operator will become the owner of the technology, and the other players will have no control over it. It is seen as an innovation of the operator that offers it to the market and then explores it.

- Arrow 1: Network Operator – Network Provider relationship: It represents the cost for the usage of a new technology that the operator intends to incur in order to upgrade its offers to the End-User.
- Arrow 2: Network Provider – Infrastructure Provider relationship: The Network Provider pays to the Infrastructure Provider the handling of the network infrastructure.

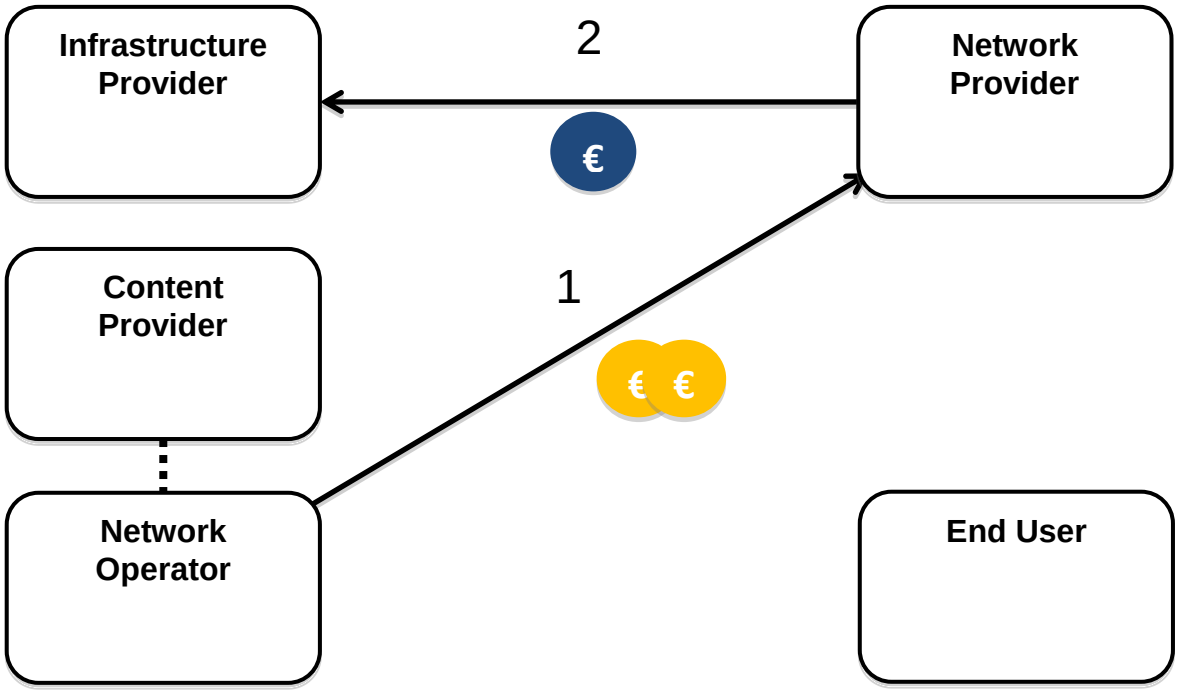


Figure 22. Network Operator Cost-Benefit Cash Flow Scenario Model.

One example of this implementation scenario is the increase of Internet speed delivered to the End-user, without increasing the Internet package price, but delivering more down- and upload speeds from time to time.

3. Infrastructure/Network Provider Cost-Benefit Scenario

In the "Infrastructure/Network Provider Cost-Benefit" scenario, Figure 23, this technology is just seen as an upgrade to the infrastructure, decreasing interconnection costs and creating a more sustainable network, with more capacity to aggregate all interested End-users. There is no cash-flow process, since it only results on CAPEX investment and decrease of associated costs:

- Arrow 1: Network Provider – Infrastructure Provider relationship: It represents the shared costs from the players for the implementation of the technology delivered to the market.

Regarding the scenario where the Infrastructure/Network Provider takes the most important role, one assumes that it is the simplest scenario to be implemented, and that it has high levels of performance and low levels of barriers to enter the market. This is because it is the developer of the technology that introduces OConS into the market, meaning that it will have 100% of usage, and the entry barriers to be faced will only have constrains in the CAPEX needed for the implementation.

When the 2G and the 2.5G became obsolete, a new technology (3G) entered the market, in a way similar to the process described above.

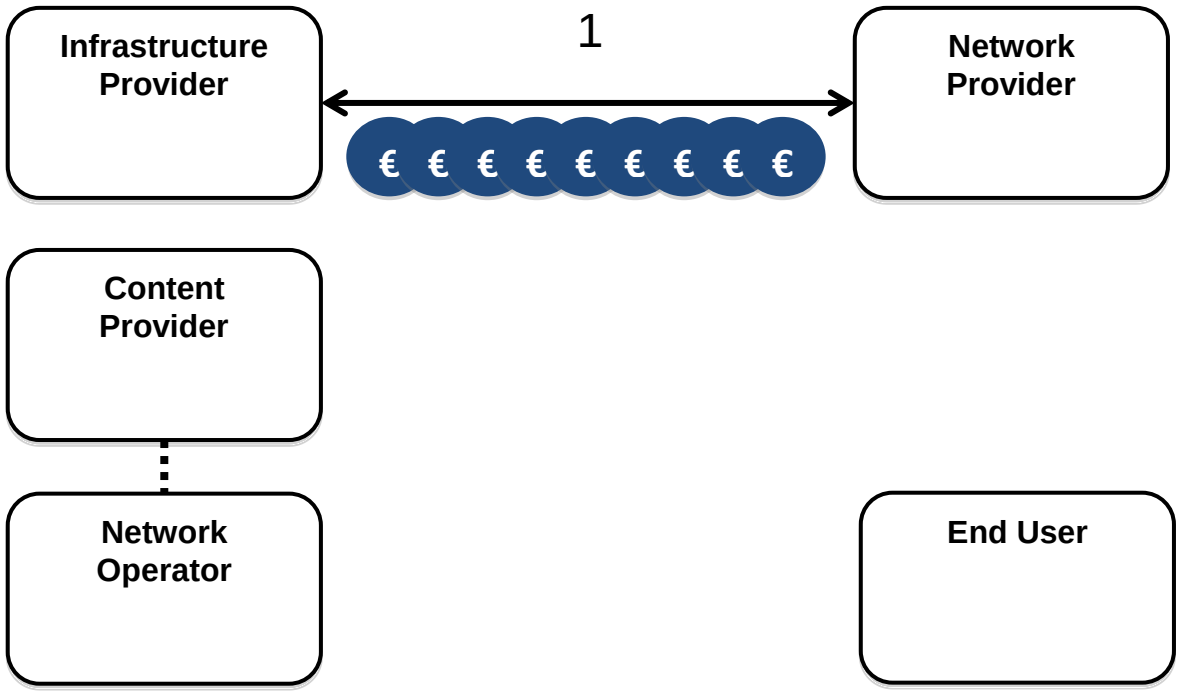


Figure 23. Infrastructure/Network Provider Cost-Benefit Cash Flow**.**

4. Multi-player Cost-Benefit Scenario

The last scenario taken in the analysis, the "Multi-player Cost Benefit Scenario", Figure 24, has a high level of complexity and also of barriers to enter the market. The single reason for this to happen is that the bill for the implementation will go to all the players in a variable form: all players will have an associated cost and benefit, which is divided by all. It will be a complex scenario, because the rewarding and delivery process will be completely divided among all.

This scenario consists of an upgrade process of the network, by delivering a new way of work flow with more efficient procedures. For this to happen, a regulatory norm must take place, because all players must agree on this, which is very rare to occur. They will be dividing the costs, for which they will pay, but they will also benefit from it by augmenting network speed and capacity. In Figure 24, it appears that the End-user is the one who pays the technology, however, the Network Operator and the Provider will stop receiving former payments for the ending technologies that they are still paying; this will be the hidden costs that they will have if they adopt this scenario:

- Arrow 1, 2, 3: The same amount of money flows in all players and ends in the Infrastructure Provider, but even this last one will incur in installation investments.

The optical fibre technology has started to be delivered at the edge of the networks (i.e., directly to end-users), meaning closer to user terminals, after the conduction of hard negotiations by regulatory authorities with all players. This is a good example of the complexity of a business scenario like this. Network Operators "delivered" a new way of Internet access, managing to have the End-user paying a small portion of the changes, and the Network and the Infrastructure Providers pay another part of the investment, reducing network backbones. With this approach, a new technology was implemented and delivered to end-users.

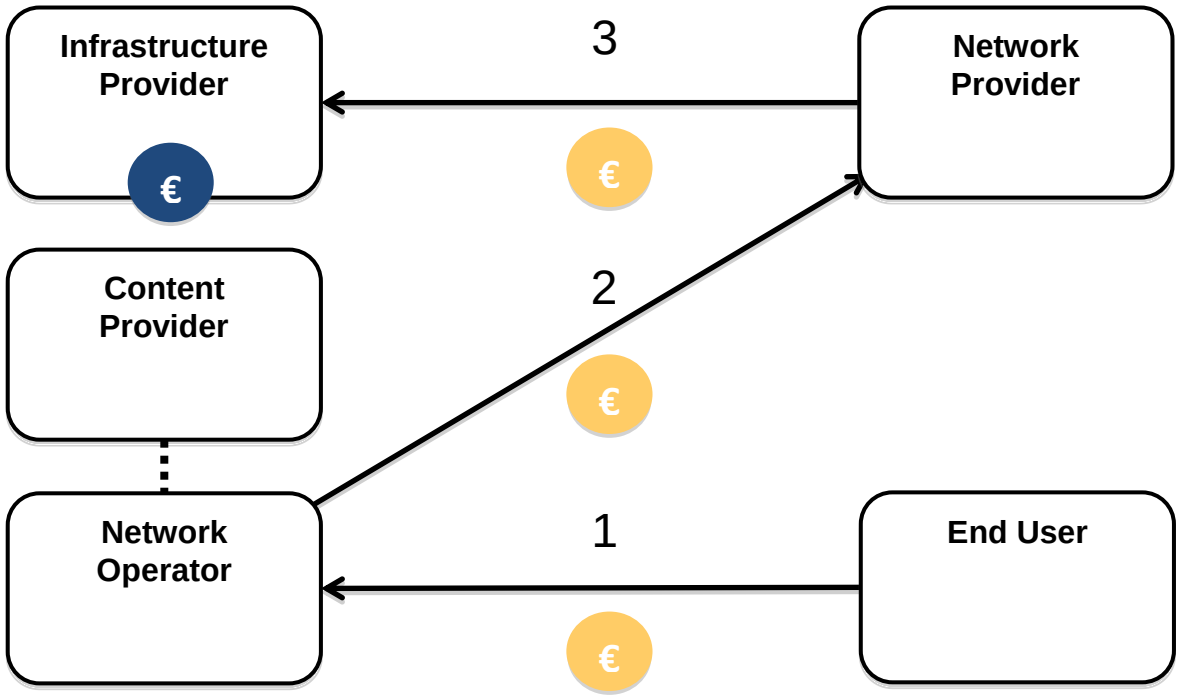


Figure 24. Multi-player Cost-Benefit Cash Flow Scenario Model.

In Table 8, a comparison among these scenarios is done, grading the effort that each player has on each scenario.

Table 8. Comparison of scenarios characteristics and their advantages.

Scenario		Costs		Barriers to Enter the Market	Scenario Complexity	Performance
		End-User	Provider			
1)	End-user	High	Low	Medium	Low	Medium
2)	Infrastructure/Network Provider	Low	High	Low	Low	High
3)	Network Operator	Medium	Medium	Low	Medium	High
4)	Multi-player	Medium	Medium	High	High	High

When analysing these four scenarios from an End-user viewpoint, the best scenario approach is the Infrastructure/Network Provider one, since it is the one with lower costs and good performance. Concerning the Multi-player scenario, a first analysis may seem that it is the one with lower chances to be successful, however, in terms of reasonability; it can be presented as a good entrance alternative. The presentation of four possible scenarios is specific to give the overall chances of entrance into the market of the OConS technology. By giving an example, one tried to explain that a new scenario possibility is not likely to be produced, but rather reproducing one that already has been put into action, and is most likely to be successful.

Another issue that must be taken into account is that OConS can be sustainable and a pro-active new technology. OConS has attributes and valuable drivers that must be explored, and as a result costs to the End-user, as well, to the “producer”, will decrease significantly.

4.6 Regulative analysis of interconnection charging in the OConS context

With respect to the SAIL concept OConS, our area of interest is the interconnection charging in the Wireless Mesh Networks (WMN) and what type of models the Regulator should promote there. The Wireless Mesh Networks concept was presented in the deliverable DA7 “New Business Models and Business Dynamics of the Future Networks [2].

The regulatory backgrounds and targets for the interconnection charging were presented in section 2.4. The key statements from that section can be summarised as follows:

- Interconnection related issues are ranked in many countries as the most important problem in the development of a competitive marketplace for telecommunications services
- There are various reasons for specifying that interconnection charges should approximate costs.
- There are number of costs that are associated with setting up and maintaining an interconnection agreement. The set up costs include both capital costs of the requisite equipment, as well as the transaction costs associated with negotiating the agreement. In addition, all interconnection services increase operational cost somewhat.

4.6.1 Key actors in the Wireless Mesh Networks

With respect to the business aspects of the SAIL concept Open Connectivity Services (OConS), the use case “Creating and Sustaining the Connectivity in Wireless Challenged Networks” was discussed in deliverable D.A.7 [2]. It analyses a very challenging concept of the Wireless Mesh Networks (WMNs), which is very interesting from the business perspective. WMNs have the ability to provide connection to the Internet in the areas with difficult or limited access to the network, via the ability to connect several devices together. The total availability of wireless connections will also promote the full use of Internet services in rural areas, and end the digital divide, which still exists in regions with low purchasing power. This infrastructure can be easily implemented on college campuses, community neighbourhoods, enterprise environments, or isolated villages without new network infrastructures.

The OConS architecture benefits from the efficiency with which it transports the subscriber traffic from a certain point over a number of hops to either the destination within the mesh or to a point that interconnects to the backhaul. With more efficient mesh networks fewer backhaul connections are needed, which reduces costs.

The relevant actors in the Mesh Networking have been listed in the following:

- **Community Operator (CO)** – This player authorizes and manages the community’s infrastructural resources. It defines a set of policies, based on which the community builds a spontaneous and self-organized network. It encourages End-users to share their resources and cooperate by giving incentives, rewards or even a cash payment. T
- **Community Infrastructure Provider (CIP)** (neighbours, old buildings, universities, hospitals, sports arenas, hotels and airports) – The CIPs are responsible for building the spontaneous and self-organized wireless network communities of cooperating nodes. In these cases, the ad-hoc network will be created, enabling a reduction in CAPEX, provided that the infrastructure already exists. A community infrastructure provider is basically composed of End-user nodes with the traffic forwarding capabilities.
- **End-user** – The End-user has multiple alternatives to access Internet. In order to choose a WMN as the preferred access there has to be a possibility for some kind of incentive. This incentive is delivered to the end-user in two ways: First, the usage of a WMN must be cheaper than any other private connection. Second, he/she must receive some compensation for routing traffic of other users. With these two options, a dramatic cost reduction to access the Internet must occur. An End-user may have the following roles in the community:

- End-user and member
- End-user but not member
- End-user and Community Infrastructure Provider
- End-user and Community Infrastructure Provider with connection to the Network Infrastructure Provider

- **Access Network Provider (ANP)** – The ANP owns and uses the access and core infrastructure resources to provide global network connectivity. It exchanges traffic with the WMN through gateway mesh nodes. Note: The Network Infrastructure Provider and Network Operator in [2] have been combined here to the Access Network Provider.
- **Content/Service Provider** – Provides services, applications and content.

In the value flows between actors an End-user of the community must pay to the Community Operator, in order to become a member of the community. The Community Infrastructure Provider (CIP), in turn, must pay to the Network Operator for the Physical access to the network. It should be noted that, any given user can play all of the above roles at once, thus, he/she can be an End-user and a Provider at the same time.

The player for whom the WMN brings more advantages is when an End-user becomes a CIP: the benefits come from the resource sharing and cost reduction of his direct connection to the network operator.

4.6.2 Interconnections and their costs in Wireless Mesh Networks

For the Wireless Mesh Networks scenario of the Open Connectivity Services the model of data flows and costs has been illustrated in Figure 25 below. Data from the Content Provider to the Community Network flows via the Access Network Provider's network to different types of members of the WMS. Since the WMN may have several gateways to the Internet, it is possible that data flows to a Member, for instance, via two gateways and via a Member & Community Infrastructure Provider.

The options for the Community Infrastructure Providers (CIP) to recover their costs, $C_{CIP/M}$ or $C_{CIP/GW}$, are to get incentives from the Community Operator (CO). The CIP with the Gateway needs higher incentives since they have to pay to the Access Network Provider for the Internet connection. The Members and Non-members have to pay to the Community Operator for the Internet Access.

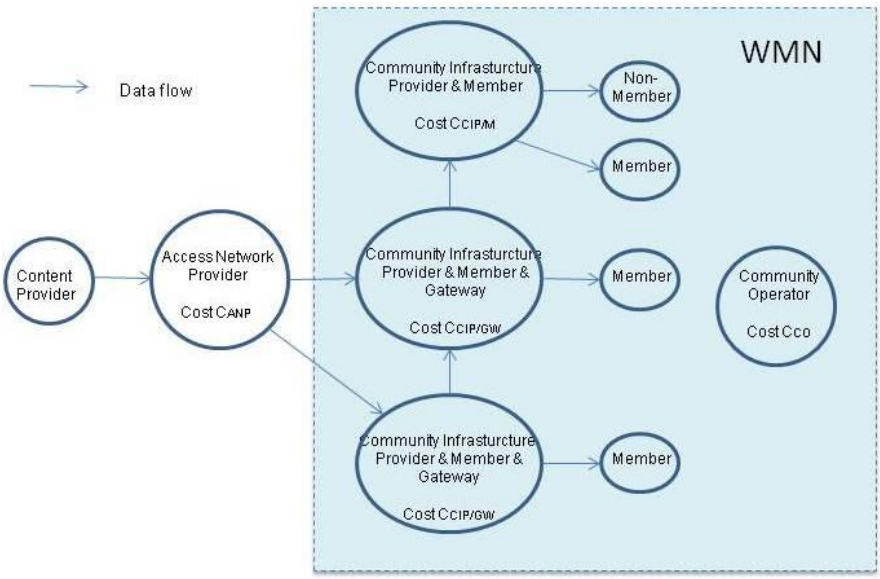


Figure 25. Data flows in Wireless Mesh Networks

The impacts on the interconnection cost levels (low / medium / high) for different players from setting up and operating the Wireless Mesh Networks (OConS), and savings in the interconnection fees have been presented in Table 9 below. In addition to the interconnections between the new players within a WMN, the analysis covers also the access to the Internet because of its important role in this concept. Within a WMN the Community Operator has the role of running the business, and the interconnection payments are paid via them.

Table 9. Interconnection costs and benefits in Wireless Mesh Networks (OConS).

Costs		Community Infrastructure Provider & Member CCIP/M	Community Infrastructure Provider & Member & Gateway CCIP/GW	Access Network Provider CANP
Set Up	*Capital Costs*	low	medium[15]	high[16]
	Transaction Costs[17]	low[18]	medium	high
Operational	*Operating Costs*	low[19]	medium[20]	high[21]
Savings in interconnection fees		n/a[22]	n/a	n/a

n/a = no savings

The following **remarks** on the costs can be made:

- The level of investment in the access network by the Access Network Provider is high. However, this is not an additional investment due to the setting up a Wireless Mesh Network
- The level of investment and operating costs for the Community Infrastructure Provider are low if he is not also providing a Gateway. In that case the level of investment would be medium.
- The Community Infrastructure Provider & Member would pay for the Internet access via the Provider with the Gateway, and not directly to the Access Network Provider.

Flow of interconnection fees

The flow of interconnection fees between 1) the Access Network Provider (ANP) and Community Infrastructure Provider with a Gateway (CIP/GW), 2) two CIP/GWs, and 3) CIP/GW and Community Infrastructure Provider & Member (CIP/M) have been discussed in the following.

1) With respect to **Interconnection between ANP and CIP/GW**, this is the **access to Internet** and can be implemented either via the fixed access or mobile access

[15] CIP with a Gateway has to pay also for the access to Internet and that cost has to be covered by the interconnection fees from other CIPs. It also has to be prepared for the interconnections with, possibly, several CIPs without a Gateway, and the cost per interconnection depends on the number of the CIPs to connect with.
[16] Access network connection can be implemented by cable or by mobile access. The Mobile Broadband Access is normally more expensive than the Fixed Broadband Access.
[17] The level of Transaction costs is lower than that of Capital costs.
[18] Manual actions on the site are needed irrespective of the number of Interconnections to set up.
[19] Once Interconnection has been agreed with the Community Operator, further operational actions are limited.
[20] Every time a new Interconnection is needed, it increases the complexity of the configuration, and therefore the cost of operating the network.
[21] Due to the increased traffic in the access network line, the ANP needs to pay more for the transit traffic to the Interconnectivity Provider. The increased traffic is on the line from the Gateway to network, but the overall traffic and transit volume may not increase, however.
[22] The Community Infrastructure Provider & Member doesn't need to pay for the Internet Access to the Access Network Provider, directly, but via the Provider with the Gateway.

technologies. Very often a flat rate is applied on this access and is dependent on the maximum bit rate available on it. Because several End-users can now use the same access line, the available capacity will now be more effectively used and will load the backhaul connections more than a single user would load. For this reason ANP may want to apply a different charging approach for CIP/GW customers than for other customers, e.g. normal residential users.

2) With respect to **Interconnection between two CIP/GWs**, this interconnection capacity is needed only when the access to Internet from another Gateway is not available for some reason; traffic between the members (End-users) of these CIPs is not exchanged directly within the WMN. This interconnection benefits more the CIP which has more members and the CIP with fewer members may want to have a compensation for Interconnection. If the charging on the access line to Internet is dependent on the volumes of transferred data, then that compensation fee becomes even more justified.

3) With respect to **Interconnection between two Community Infrastructure Providers**, one **with the Gateway** and the other **without the Gateway**, this is the path to Internet for the members of the CIP without the Gateway. Interconnection between these two players may cost more to the one with the Gateway because of the additional complexity from operating several Interconnections. The CIP with the Gateway has to cover also the cost of the access line to Internet. For these reasons the payment to the CIP with the Gateway can be justified.

4.6.3 Regulatory analysis of charging options in Wireless Mesh Networks

In the Wireless Mesh Network (WMN) concept, a key business player is the Community Operator (CO). Different COs compete against each other by trying to extend the coverage of their WMNs and get as many members and Community Infrastructure Providers (CIP) connected to their networks as possible. Another key business player is the Access Network Provider (ANP), who provides the access to Internet for the members of a WMN.

The CIPs with Gateways are interconnected with other CIPs. The different WMNs are not directly interconnected, however.

Within a WMN there is no competition between the CIPs. The Access Network Providers compete to get as many CIPs with Gateways connected to their networks as possible. Also, a WMN may be connected to Internet via several ANPs.

The procedures to establish the interconnection charges have been discussed in section 2.4. The same criteria [2] as used in the regulatory analysis of the NetInf concept have been used in the following analysis in Table 10.

Table 10. Regulatory approaches in Wireless Mesh Networks (OConS).

Criteria	RoR	Price ceiling	Cost orientation
Prevents exercise of market power	Yes, w.r.t. ANPs. It restricts the amount of profit (return) that the regulated operator can earn. Yes. w.r.t. CIPs within a WMN. It restricts the amount of profits that a CIP, especially a CIP/GW, can earn from other CIPs. Yes, w.r.t. the CO operating a WMN, where the CO is responsible for negotiating the interconnection fees between the CIPs. This approach would restrict the amount of profit	Yes. It restricts the amount of profit that CIP/GWs can earn by providing an access to Internet for other CIPs within a WMN. Yes. It restricts the amount of profit that an ANP can earn from providing access to Internet. Yes, w.r.t. the CO operating a WMN, where the CO is responsible for negotiating the interconnection fees between the CIPs. This	Yes, w.r.t. interconnect-tions between CIPs and towards Internet. Price of a service, or of the improved quality of interconnection service will consist of its cost + reasonable rate of return. Yes, w.r.t. the CO operating a WMN, where the CO is responsible for negotiating the interconnection fees between the CIPs. In this approach the interconnection fees

	that they and the CIPs could earn. N/A, w.r.t. COs operating different WMNs. WMNs are interconnected only via access networks and they are not seen responsible for negotiating the access prices to Internet.	approach would restrict the amount of profit that they and the CIPs could earn. N/A, w.r.t. COs operating different WMNs. WMNs are interconnected only via access networks.	should be based on the costs. N/A, w.r.t. COs operating different WMNs. WMNs are interconnected only via access networks.
Promotes competition	No, w.r.t. ANPs. This does not permit pricing flexibility for the operator to set prices to reflect costs in response to competition. New entries are anyway difficult when the fixed line technologies are used for accessing Internet. Mobile technologies are easier for new entrants to the market. No, w.r.t. CIPs within a WMN. This does not permit pricing flexibility. N/A, w.r.t. COs operating different WMNs and competing for new members. WMNs are interconnected only via access networks and they are not seen responsible for negotiating the access prices to Internet.	Yes, w.r.t. CIP/GWs and ANPs. They have sufficient pricing flexibility to respond to competition by setting prices that reflect costs and demand conditions. N/A, w.r.t. COs operating different WMNs. WMNs are interconnected only via access networks.	Yes. The ANPs and CIPs have to set prices that reflect underlying costs. No cross-subsidization is allowed.
Ensures productive efficiency	No. The different players will not reap the benefit from reducing costs.	Yes. All players, i.e. the ANPs and CIPs within a WMN, are rewarded with higher earnings when they reduce costs (and penalized when costs increase). If WMN is seen to reduce the cost of accessing Internet, it will be invested on by all parties.	Yes. In the case of forward-looking cost accounting. No. In the case of backward-looking cost accounting. If WMN is seen to reduce the cost of accessing Internet, it will be invested on by all parties.
Ensures allocative efficiency	No. Prices for individual services, like interconnect-ivity, need not to equal the cost of the service. There is no incentive for an ANP to invest in and run the access line, or for a player in a WMN, to run the interconnectivity in an efficient way.	Yes. All players, i.e. the ANP and CIPs within a WMN, have flexibility to set prices for individual services like interconnection.	Yes. The prices for the interconnection service equal the costs of the service. There are incentives for all players, i.e. the ANPs and CIPs within a WMN, to invest in and run the interconnection service in an efficient way. Competition keeps the interconnection costs and prices as low as possible.
Ensures dynamic	No. There are no big incentives for players in an	Yes. All players, i.e. the ANPs and CIPs within a	Yes. Yes. All players, i.e. the ANPs and CIPs within

efficiency	access network or in a WMN to invest in new technologies or services, which would improve the efficiency of the connectivity.	WMN, have incentives to improve efficiency. A WMN can be seen as a new technology to reduce the costs of connecting to Internet.	a WMN, have incentives to improve efficiency, service by service.
Minimizes regulatory costs	No. The rate determination proceedings are often lengthy and resource intensive.	Yes. Price ceiling setting procedures are not frequent.	No. Control proceedings are resource intensive. The control of profits, service by service (interconnection) implies that the setting up and operating costs can be monitored service by service.

Productive efficiency requires that goods should be produced at the lowest possible cost.

Allocative efficiency requires that the prices one observes in a market are based upon and equal to the underlying costs that a society incurs to produce those services (generally the long run incremental cost of producing the service).

Dynamic efficiency requires that firms should have the proper incentives to invest in new technologies and deploy new services.

Table 10 summarizes how the different regulatory targets would materialize with the different regulatory approaches to the interconnection charging:

- **Rate of Return** -approach would prevent execution of market power by any player, but would have a negative impact on all other regulatory targets.
- **Price ceiling** –approach would have positive impacts on all regulatory targets: it would restrict the profits for all players in the Value Network Configuration and would also promote competition between them; the players would also have incentives to improve their efficiency; by reducing their costs all players would be rewarded with higher earnings; and there would be more flexibility of setting prices for individual services.
- **Cost orientation** –approach would mainly have positive impacts on all regulatory targets. The regulatory costs would not be minimized, however, because the control of profits implies the monitoring of costs service by service. It would not contribute to the productive efficiency in the case of backward-looking cost accounting. Also, the control of regulatory proceedings is resource intensive.

4.7 Conclusions

OConS aims at creating a new technology that can interconnect all available devices. In OConS, four Use Cases have initially been defined in order to highlight the new ideas being developed later having being merged into two evolved ones. In this chapter, an economic analysis for OConS for CloNe is provided, and then it addresses the regulatory aspects for OConS for NetInf (continuing previous work).

The business model starts by the identification of the business drivers, such as innovation, economies of scale, and traffic aspects. Then, the technical aspects of the proposed solution are briefly analysed, followed by a description of all the stakeholders involved. Finally, some business models were identified, analysing the different Cost-Benefit Scenario that can be implemented in order to have a commercial solution: End-user, Network Operator, Infrastructure/Network Provider, Multi-player. For each one, the money flows and the pros and cons are identified.

Three potential approaches for the interconnection charging, which could be promoted by the regulators, are explained: the Price ceiling, Cost orientation and Rate of return. The Price ceiling -approach would have positive impacts on all regulatory targets, and the Cost

orientation -approach on most of them. The Cost orientation scheme, however, would not minimize the regulatory costs, because the control procedures are resource intensive. The Rate of return -approach would prevent the parties to exercise their potential market power, but would not contribute to other regulatory targets.

Even if the accurate information on the interconnection and WMN costs was not available in the analysis, the main conclusion here is the same as for the interconnection charging in the NetInf concept: the Price ceiling and Cost orientation approaches seem to have about equal impacts on the regulatory targets and should be promoted by the regulators. Especially, the pricing of the access link to Internet via the access Networks Provider shall be paid attention to.

5 Business Analysis of CloNe

This chapter addresses the future CloNe services from a socio-economic perspective. We start in Section 5.1 by pointing out some of the drivers that support the analysis performed in the chapter. Section 5.2 provides an overview of the ecosystem, where CloNe's uniqueness is enhanced in a market with a huge momentum but no real solutions (so far). In Section 5.3, our view of the value network configuration (VNC) is described in line with the previous work carried out in the project preceded by an overview of CloNe's technical architecture. Section 5.4 provides a brief description of the market players and scenarios are discussed. Section 5.5 tackles the business models topic. Security is a widely discussed topic and from what we have concluded a decisive factor in the cloud business adoption decision; therefore, in Section 0 we look at security focusing on the regulatory viewpoint. Finally, a number of conclusions are drawn in section 5.7.

5.1 Business Drivers

Current best-effort support for Cloud services is not enough as an increasingly large number of services cannot be handled in this way. Furthermore, looking to the enterprise market sector the network reliability is a "must have", not only from a performance perspective but also from a security one. In some cases, when typical best effort Internet model is not enough, an independent network service that fulfils the Cloud service requirements can be purchased, backed up by a Service Level Agreement (SLA), connecting the user and the Cloud hosting the service. This typically happens in the enterprise sector, namely through operator-managed Virtual Private Network (VPN) service. There is no reason to believe that future cloud services will require a lesser degree of reliability and performance guarantees from the network. However, network services are not integrated nor compliant with cloud services as their current configuration is not on-demand and reconfigurations are supposed to be relatively infrequent and usually involve a significant amount of manual effort.

In line with the abovementioned factors and with CloNe's dynamic enterprise scenario this chapter looks at a deployment of CloNe more oriented to the enterprise market.

5.2 Ecosystem Analysis

CloNe business spaces focus around the integrated offering of dynamic and self-managed network capabilities in conjunction with traditional cloud computing resources and services. Target customers are Corporate, Small and Medium Enterprises (SMEs), Small office/Home office (SoHo) and the end-user market segments. Additionally, CloNe technology can also address the business space of network operators' internal efficiency tools by implementing flexible network resource allocation capabilities and network management within the network operator Business and Operational Support System (B/OSS) ecosystem. Note that CloNe does not restrict these latter capabilities only to the network operators' domain but extends it also to the cloud provider domains.

SAIL CloNe architecture manages physical and logical resources distributed through several administrative domains[23] with self-managed dynamic connectivity service capabilities. This enhances QoE, performance and reliability for end-users compared with pre-SAIL scenarios. In addition, it provides new business opportunities to non-traditional actors, such as cloud-based service providers and content producers: they can easily and quickly distribute and migrate cloud services to/between data centers; traffic peaks between data centers are handled as well.

By offering an integrated view of network and computing resources, in a cloud-like business model (with dynamic and adaptable properties such as resource elasticity, resource mobility,

[23] An administrative domain is the underlying virtual or physical equipment managed by a single administrator.

self-managed on-demand allocation and de-allocation of resources, including network resources, and a pay-as-you-go business model), CloNe technology brings about many possible application scenarios, each of which could be mapped onto a commercial service or commercial application.

The idea of merging cloud and network services, by some called *cloud networking*, is not entirely new. In fact, the concept is reflected in pretty much all cloud computing definitions (e.g. "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)...*" [94]. However, today's cloud computing offers/solutions/services do not reflect these definitions in their entirety.

The network component within cloud computing has been pretty much neglected until the last couple of years due to its traditional IT business origin (e.g. Google, Amazon, Microsoft). Nowadays, there is a huge momentum that is closing this gap, due to Telco and IT convergence and network operators trying to vertically integrate in order to avoid being a mere bit pipe. Standardization bodies and enterprise efforts have highlighted the need for cloud and network resources to be handled together [95] [96] [97]. For example, IBM offers enterprises a cloud data backup supported by Verizon's VPN services, and Cisco has recently presented CloudVerse [98]. The Open Grid Forum (OGF), with the pyOCNI [99] is one of the standardization bodies actively involved in the subject. Also the Metro Ethernet Forum (MEF) and the International Telecommunication Union (ITU) have put efforts in this field, with the former launching its first official document specifically targeting the topic in February 2012 [100] while the latter has, for some time, a working group addressing the subject (FG Cloud).

Despite the momentum around cloud networking there is no commercial solution that tackles the reality of this ecosystem where several actors (such as communications service providers, cloud providers, content producers, and customers from all segments) playing different roles exist and need to interact. Thus, it is not vanity to say that today, the CloNe service has no real competitor (so far).

The remainder of this section is organized as follows: Section 5.2.1 provides an overview on how the cloud computing market is dealing to date with the Wide Area Network (WAN) connectivity, Section 5.2.2 gives an insight on the near future market, and Section 5.2.3 presents the service adoption determinants.

5.2.1 The Market Today

The majority of today's cloud computing market offers were developed considering just the data center side of the cloud. This does not mean that providers were unaware of the fundamental role of the network (i.e. WAN), we can just say that there was neither significant market demand nor business driver to bring the network into the picture. However, it seems that the demand and the driver exists today – some providers already reflect that in their market offers. Take Amazon and AT&T for example.

Amazon, one of the first and biggest cloud service providers in the market, launched in mid 2009 the service Amazon Virtual Private Cloud (VPC) [101]. The VPC service allows companies to connect a set of Amazon compute (EC2 service) and storage (S3 service) resources with a corporate data centre using a virtual private network (VPN) connection over the IPsec protocol. This was, as far as we know, the first cloud service that looked at the connectivity aspect of the cloud.

Although the VPC service tackles some important network issues, it does not tackle several others that require actual interaction with the network (e.g. performance-related issues). Bearing this in mind, and due to market demand, in August 2011 the Direct Connect service [102] was released. This service allows Amazon Web Services (AWS) costumers to establish dedicated network connections to an AWS data centre, e.g. from an enterprise or data centre site. In practice the service is nothing more than a way for costumers to ask for a letter of authorization to connect to Amazon's facilities. With this letter, a costumer can hire a

connectivity service (e.g. BGP/MPLS VPN) from a network operator, or extend an already existing one, to one of Amazon's data centres. Currently, Amazon has several partnerships with network operators to provide connectivity services to their costumers [103] (without obligation to use these operators). One of the major limitations, not from the Direct Connect service itself but from connectivity services, is the fact that the management of this type of services is still done manually with face-to-face, telephone or e-mail interaction.

The Direct Connect service is the connector of two worlds, cloud and WAN. However, the service is far from fulfilling the expectations. After a long process (to obtain a letter of authorization can take days and to have a connectivity service up and running can take weeks) the costumer ends up with a patchwork set of services (network and cloud), with the usual self-managed control over the cloud service but with no control over the network/connectivity service. This is probably one of the biggest gaps between cloud and network services that needs to be closed so that cloud and network can be integrated.

Similarly, AT&T introduced its Virtual Private Cloud service [104] in February 2012. The service combines virtual private networking services with cloud infrastructure services. Compared to Amazon's offer, AT&T has the advantage of providing a composed service with a single point of contact. In other words, the costumer can purchase both cloud and network services directly from AT&T. However, it also lacks an adequate management of the network part of the service.

Although current market solutions are still far from what SAIL envisions, they are a step forward and a clear indicator that CloNe is one step ahead of what the market needs in the near future.

It is also important to highlight that the business convergence at the moment seems to have two distinct paths: one followed by well settled cloud providers who opt for strategic partnerships with some network operators (e.g. Amazon); and another followed by big network operators who see the network as a differentiating factor, enabling them to conquer their share in the cloud business by providing **both** typical cloud services **and** connectivity services (e.g. AT&T).

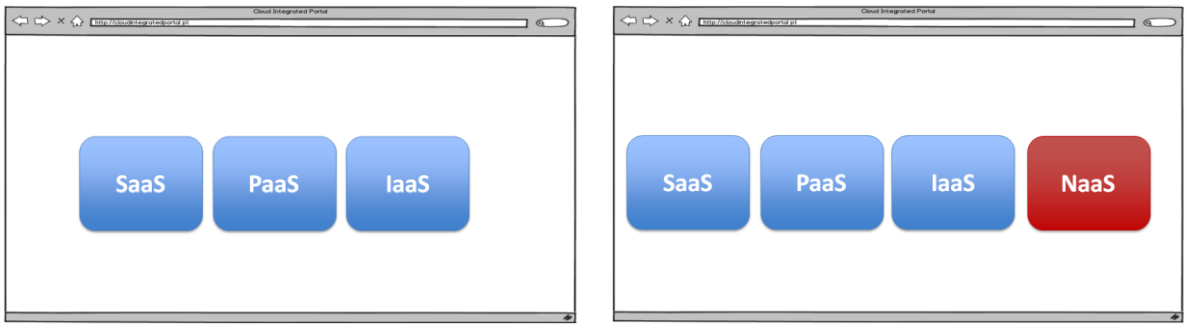
5.2.2 The Market Tomorrow

After an overview on how the market is dealing with the network/connectivity side of the cloud, we now elaborate on how we believe the market will look like in a near future.

Today, cloud offers are of three types: IaaS, PaaS and SaaS. There are providers in the market that dedicate themselves to a single category (e.g. Terramark, CloudBees, and SAP); others that have more complete offers (e.g. Amazon and Google). Services such as Amazon VPC or Direct Connect do not actually fit in any of the above service categories, as they can be considered as another type of service, complementary to the typical ones, i.e. connectivity/network services. However, as stated in the previous section these connectivity services are far from fulfilling what are becoming the needs today.

Following the trend in offering services, we believe that sooner or later operator networking services (e.g. BGP/MPLS VPNs) will be provided in a way that will allow them to actually complement services like Direct Connect. We believe that a next generation of operator networking services will come up, which will differ from the current one by its on-demand features, allowing the self-management of connectivity through a self-service portal. In other words, certain operator network services will embrace some of the fundamental cloud features.

As an example, Figure 26 tries to illustrate in a very simple way the homepage of a future integrated cloud service portal. In this portal, the user will also – apart from the traditional SaaS, PaaS and IaaS services – have some control over networking services (NaaS tab), e.g. VPN endpoint configuration like bandwidth. The combination of NaaS services with the traditional cloud offers is what CloNe is tackling. Thus, CloNe fundamental blocks are the foundation for this future generation of cloud services.



Today Tomorrow

Figure 26. Cloud Service Integrated Portal

With respect to the business convergence it is expected that the two paths mentioned in the former section will remain, with the big cloud providers opting for strategic partnerships in the NaaS offer, and with big network operators taking advantage from the network to gaining ground in the remaining sectors (IaaS, PaaS, SaaS).

5.2.3 Service Adoption Determinants

In order to evaluate the proposed CloNe service design and business adoption determinants, in a broad sense, and also to consolidate the identified service business requirements, we chose to inquire a small number of people after a CloNe service demonstration to, on one hand, validate our previous work and, on the other hand, to test and validate our investigation model. The goal was for a revised inquiry to be sent to a wider population group. Focusing on CloNe services in an abstract sense and not on one or two specific commercial services supported by CloNe technology seems more adequate for the purpose of the experimental work being carried out, because it will not confine the respondent view to one specific scenario or service, thus allowing for several dimensions relating to CloNe to emerge.

The SAIL general meeting in Lisbon, which took place on month 18 of the project, provided the opportunity for such an inquiry because it was the first time that a public CloNe service demonstration was put forward (Figure 27).

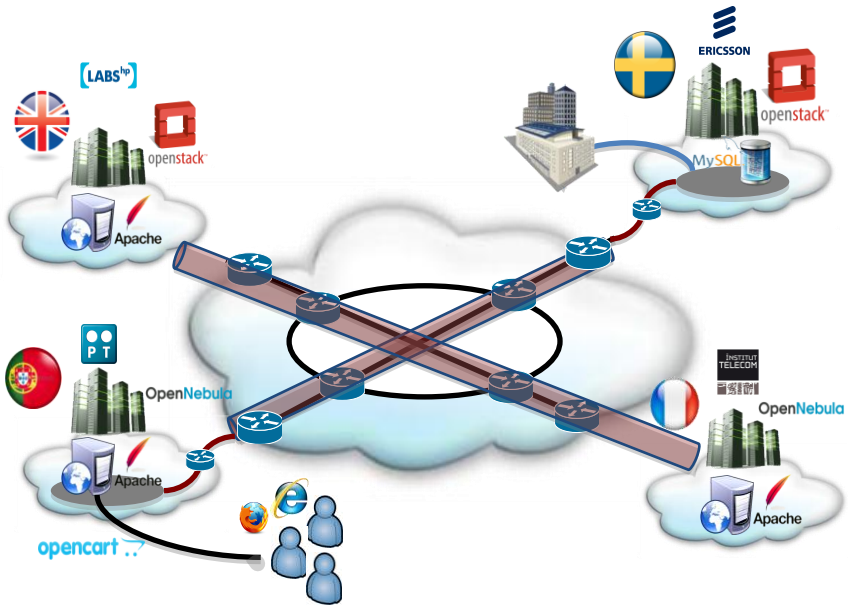


Figure 27. Dynamic Enterprise scenario – demo set-up at SAIL Lisbon meeting.

Immediately after the Clone Service demo, a questionnaire was delivered to the audience in order to capture their perceived dimensions regarding the CloNe Service.

The investigation model that supported the questionnaire modelled the effective CloNe adoption as a function of the adoption intention. The latter is modelled as a function of attitude towards the adoption behaviour. Attitude is determined by several dimensions and factors identified in previous work and tested for their influence in this investigation work.

This type of investigation models can be traced back to the theory of reasoned action (TRA) from Fishbein and Ajzen or the theory of planned behaviour (TPB) [105] that supported the technology adoption model (TAM) as discussed in D.A.7 [2], and also to the parallel work of Rogers with its Innovation Adoption Model [106].

In the recent past this type of model has been used to validate technological innovation adoption determinants by the end-users and abundant literature exists on this topic related to information systems adoption, telecommunication services adoption and technological artefacts adoption (e.g., triple play services, mobile phones or advanced computer systems).
The model used in this investigation is depicted in Figure 28. Six influential factors (independent variables) were considered as hypotheses to understand the CloNe adoption intention. The adoption intention itself is a function towards the effective CloNe adoption. Note that both the adoption intention and the effective adoption depend on the influential factors and thus are considered dependent variables.

We tried to assess the opinion of the people how saw the Clone demo on the following points: (a) does the CloNe service bring to the market an advantage over current services, (b) is it compatible with the way people work with cloud services today, (c) is it easy to use, useful and secure.

From the work developed in DA7, namely from the interviews with industry experts and potential clients, mobility emerged as a new dimension. Therefore, we introduced this dimension in the model to test the degree to which it is perceived as important by the respondents.

CloNe Adoption Determinants

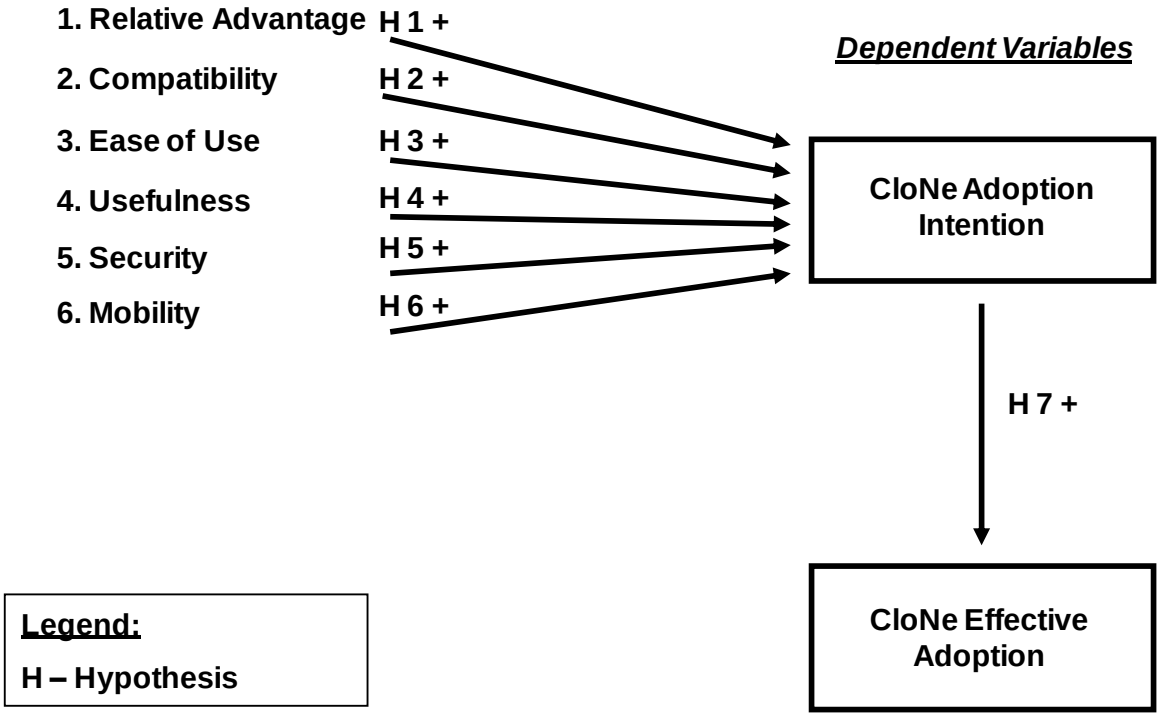


Figure 28. CloNe adoption model.

The questionnaire used for the study, supported on the model above, is depicted in Annex 2.

The questionnaire had a very good receptivity amongst the present audience and the results seem encouraging due to the high level of discussion that it generated.

From the questionnaire results we concluded that CloNe Service is viewed as (a) compatible with the current mind set of potential users, thus favoring adoption, (b) a useful service at enterprise usage level, with added usefulness to support temporary events/projects, (c) not useful at a personal/individual level.

Some perceived expected relative advantages and benefits of the CloNe service emerged, such as:

- single supplier of network & IT/IS services;
- increased end-user autonomy via self-service portals;
- increased mobility with inclusion of 3G/LTE connection options on the service;
- an expected cost optimization and connection savings for end-users;

Moreover, the end-users perceive the CloNe Service as easy-to-use, globally available through internet portals and acting as a driver for faster adoption of Cloud Services.

From the questionnaire emerged also some concerns regarding the service, namely:

- security and privacy are at the top concerns when regarding short term service adoption;
- peak traffic network availability assurance is a fundamental condition for service adoption;
- experimentation will favor service adoption because adequate QoS & QoE concerns were rated of high importance;

- technology maturity (or lack of maturity) to date is perceived as an issue to be solved over time;
- adequate SLAs and business models for the corporate segment were considered very important, and are related to the expected cost benefit advantage of the service;

Finally the business case for network operators or cloud providers was perceived as very complex, correlated with other businesses, and requiring additional reflection.

5.3 Technical and Industry Architecture

In the first architecture deliverable D.D.1 [107], a three-layer model of CloNe was defined, a framework for characterising virtual infrastructure relative to three different viewpoints: resource, single domain infrastructure, and cross-domain infrastructure. Figure 29 illustrates the model.

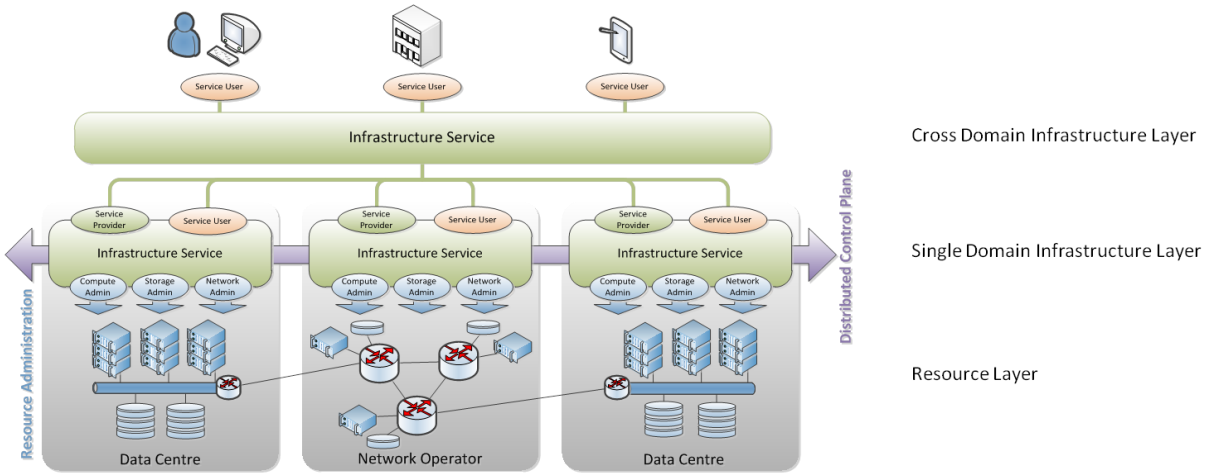


Figure 29. CloNe's Three-Layer Model.

From CloNe's three-layer model, roles, interfaces and managements functions were defined. We will focus on the three generic roles identified by the architecture, due to its importance to this analysis. The three roles are transcribed bellow:

- **Administrator** – *has administrative authority over underlying virtual or physical equipment (the administrative domain) used to implement resources. The administrator uses management systems to configure and manage resources within the administrative domain.*
- **Infrastructure Service Provider** – *offers an infrastructure service that may be used by an infrastructure service user to obtain, examine, modify and destroy resources.*

(An Infrastructure Service Provider can be: a CloNe provider; a Cloud provider; or a Network provider.)

- **Infrastructure Service User** – *accesses an infrastructure service in order to obtain, examine, modify and destroy resources.*

(An Infrastructure Service User can be: a CloNe end-user when interacting with a CloNe provider; a CloNe provider when interacting with another CloNe Provider, a Cloud Provider, or a Network Provider.)

The business model that supported the Lisbon demo tried to be as generic as possible in order to capture the different perceptions regarding the CloNe Service and not the perceptions towards any specific service supported on the CloNe framework.

The VNC for this business model, presented in Figure 30 and Figure 31, is based not only on the demo scenario but also on CloNe's architecture and prototyping details. In Deliverable D.A.7 [2] a first VNC for CloNe was presented. However, this VNC was done without considering the first technical architecture description of CloNe, which was made available in D.D.1 by the same due date as DA.7. Thus, it is prudent to perform a reformulation of the VNC, according to the technical information depicted in D.D.1 and also the demonstration scenario.

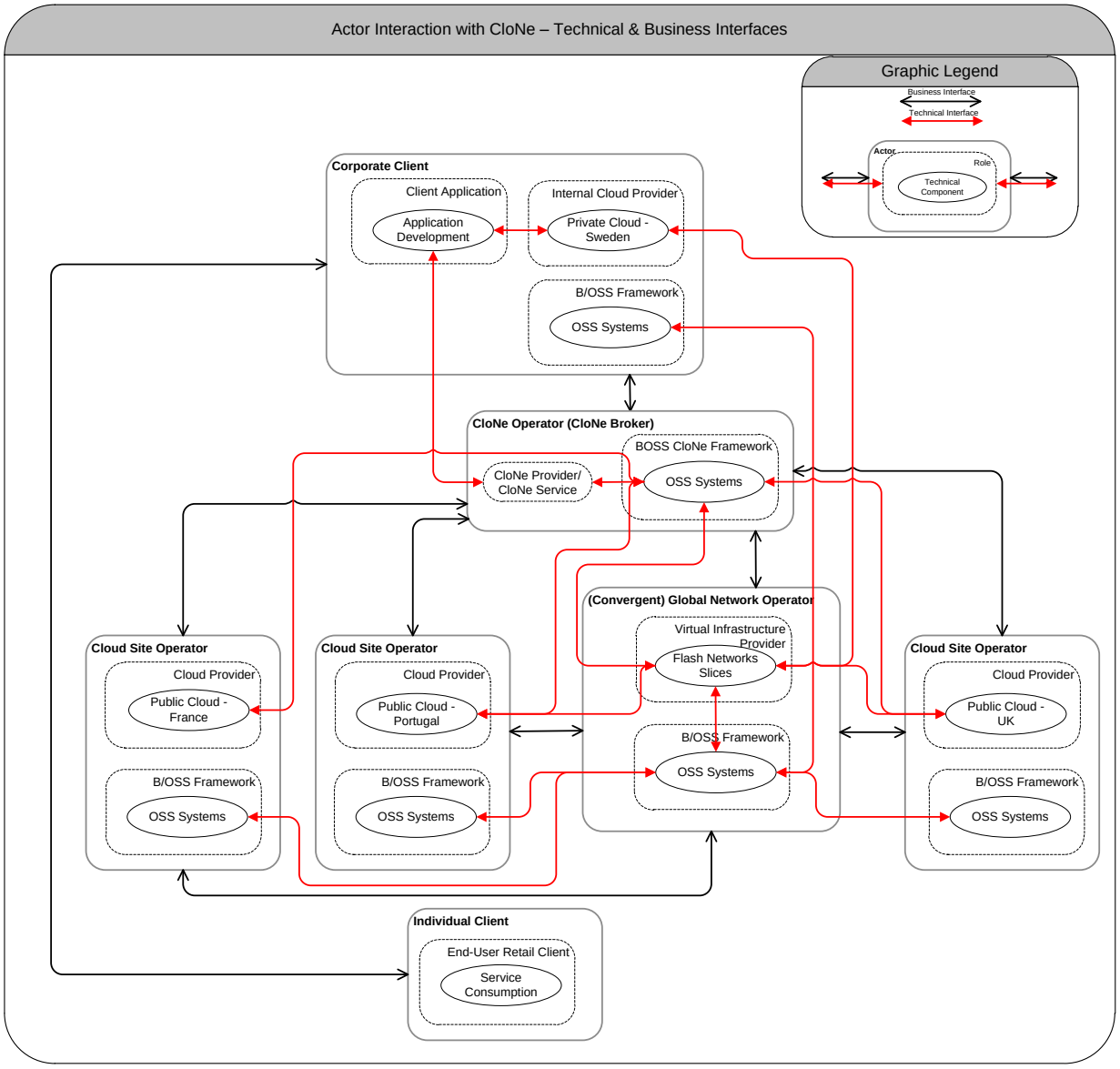


Figure 30. Lisbon demo VNC – technical and business interfaces.

It is important to emphasize that in this analysis, delegations from Cloud Providers and Network Providers are not considered; however, we do consider the CloNe Provider to act as a broker, i.e., a virtual provider that splits the requests and delegates it to the different Cloud Operators and the (Global) Network Operator. The scenario only considers one hop delegation (D.D.1 [107]), where in a worst-case scenario we can assume that business relations not only exist between the broker and the underlying domains but also among the underlying domains (to allow DCP interaction between the Cloud Operators and the Network Operator – see CloNe-R12 and D.D1 for more information).

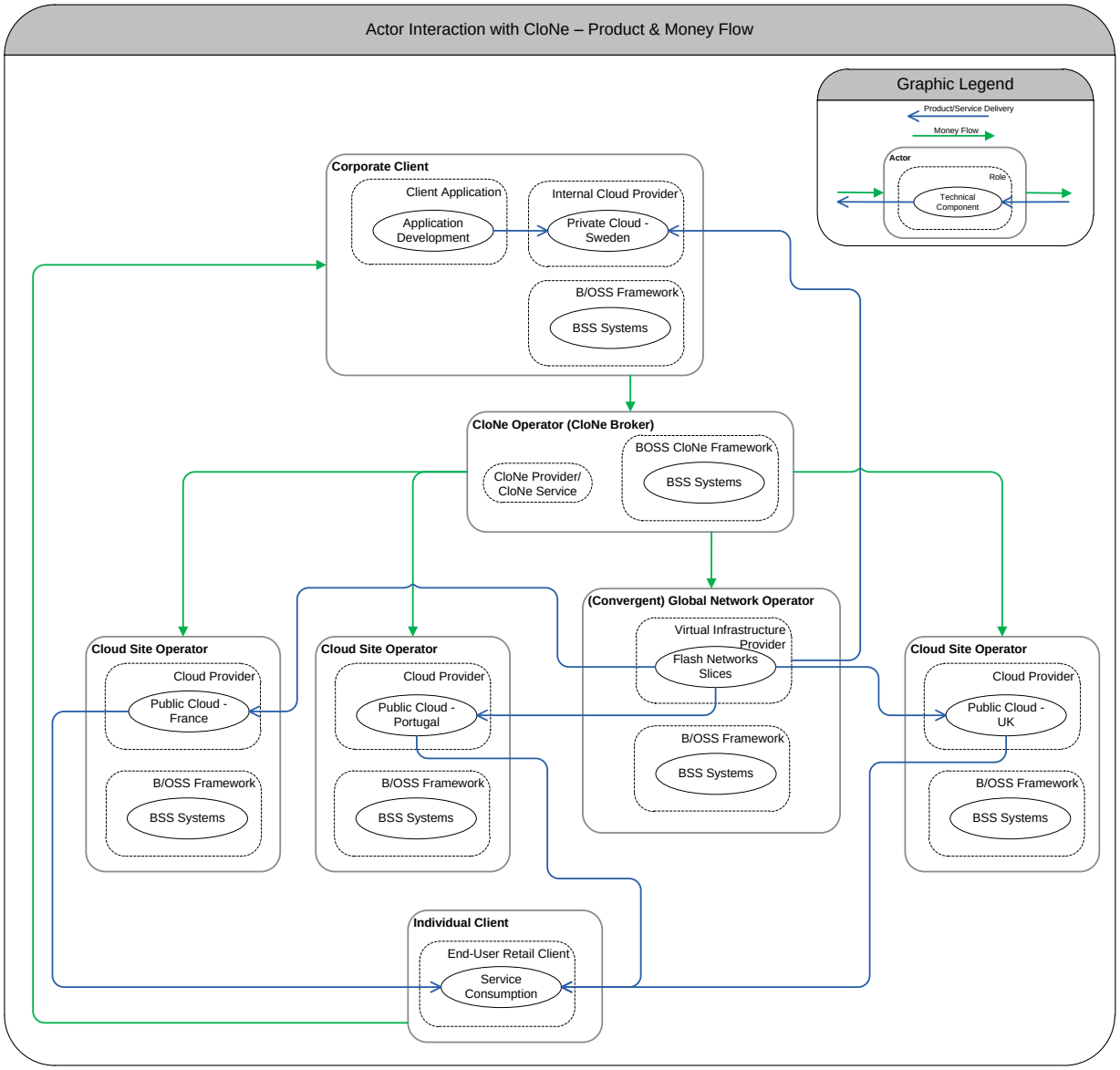


Figure 31. Lisbon Demo VNC – product & money flows。

5.4 Stakeholder Analysis

The business analysis done so far has been close to the ongoing technical WP developments. That is why we have decided to create a business model around the CloNe Lisbon demo. By doing this, there was the inherent risk of getting into a particular case that would divert us from CloNe's overall framework. However, with the interaction with the WP and its prototyping team we made sure that the opposite happened. We did enter into a specific market scenario, but one that could realize CloNe's overall architecture and ease the perception of other possible scenarios that can arise from it.

In this market scenario all the roles and possible actors (players) were identified. We considered one actor per role to ensure the generalized perception of CloNe's framework, thus when describing one we are implicitly describing the other. Five actors were identified:

- **Corporate/Enterprise Client** – The user of the CloNe service. The client asks the CloNe Operator to deploy its (the client's) application in a CloNe infrastructure. With respect to the CloNe service itself, the client only knows about the existence of the CloNe Operator.

- **CloNe Operator –** The provider of the CloNe service. In the presented VNC, this player is a broker that relies on other players to implement the actual service, namely on Cloud and Network Operators. However, its role (CloNe Provider) can be taken by either the Cloud Operator or the Network Operator. The CloNe Operator is responsible for splitting the request and sending it to the players that have indeed the infrastructure that will deploy and support the service. Despite the service being held by different players, towards the Corporate Client the CloNe Operator is the one responsible for service.
- **Cloud Operator –** The provider of Cloud resources.
- **(Convergent) Global Network Operator –** The provider of a Flash Network Slice (FNS) in the WAN.
- **Individual Client –** The end-user retail client. It is the one consuming the application that the Corporate Client deployed over a CloNe infrastructure. However, it is not aware of the deployment details and only knows about the existence of the Corporate Client.

5.5 Business Models

CloNe service business model investigation is a complex task due to the disruptiveness that the service introduces into the current market landscape.

On one hand, current market actors, like Cloud Providers and Network Providers, can position themselves to offer CloNe Services and thus vertically integrate the service into their current business value chain – an evolutionary approach from a business model perspective. On the other hand, they can opt for partnerships that will turn out to be a more disruptive approach.

Moreover, CloNe service capabilities will increase competition on both the connectivity market and the Cloud Computing market. Therefore, the overall market value sustainability and expansion will require new entrants to broaden the offers leveraged on CloNe at the value-added services top layers.

The resolution tentative for elaborating concrete business models is a complex equation that seems to be grounded on a few simple and obvious premises, such as (1) CloNe technology must be adopted and implemented by Network Operators, (2) CloNe Service must be leveraged on Cloud Computing offerings and value-added services hosted on the Cloud, (3) the overall (CloNe + Cloud) offering must bring benefits (tangible and/or intangible) to both service providers and end-users, in comparison to current market landscape, and finally (4) regulation must evolve to enclose the normally accepted regulative principles applied to CloNe Service and simultaneously protect end-user and business actors interests whenever possible.

With this much degrees of freedom and uncertainty regarding the CloNe future business landscape it seems advisable not to put forward any future business model evaluation at this time, apart from the previous qualitative analysis performed above.

5.6 Security and Privacy in Clouds – Regulatory Analysis

5.6.1 Background

The **Cloud Computing** technologies can be classified into four different types: **public Clouds, private external Clouds, private internal Clouds and hybrid Clouds** [87]. In a public Cloud, organizations use Cloud Computing technologies through a Cloud Service Provider (CSP).

In the private external Clouds, Cloud Computing is still offered by a CSP. The difference between public Clouds and private external Clouds is in the hardware: in public Clouds the hardware is shared among different Cloud customers; in private external Clouds, the hardware

hosts the Cloud of only one customer. In private internal Clouds, organizations use Cloud Computing technologies within the organization's data centre.

The aim of the SAIL **cloud networking** (CloNe) concept is to complete the Cloud Computing picture by addressing the network aspects; the computing and storage resources are distributed in the network to allow for better end-user experience and lower the dependency on network capacity. An administrative domain in this concept is a collection of physical or virtual equipment that is under the management of an administrative authority. The Wide Area Networks and data centres are examples of the administrative domains in the CloNe context.

Since the Cloud Computing and CloNe concept are complementary to each other, the Security and Privacy issues of the Cloud Computing are relevant also in the CloNe concept. Trust in these complementary concepts is essential if there is to be significant take-up and adoption by end-users; especially when private or commercially sensitive data may be stored, accessed and processed in remote locations, including for example different countries.

The key concepts of Security and Privacy have been presented in Annex 1 of this document.

5.6.2 Generic Security and Privacy issues in Clouds

Users expect to be able to access and use the cloud services where and when they wish. They expect that the cloud provider will prevent unauthorized access to both data and code, and that sensitive data will remain private. Also, the cloud provider and governments are expected not to monitor their activities.

In cloud computing, the roles of customers and providers can vary or overlap. Cloud computing service providers may be unaware that the data they process or store on behalf of a customer is classified as 'personal data'. However, under the present Directive, a lack of knowledge is not a legitimate excuse, and they could still be considered 'processors' under the Directive [84].

ITU focus group on Cloud Computing[24] has identified the following **security issues with respect to the cloud service users** [89]:

- **Responsibility Ambiguity**. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Also, the problem of which entity is the data controller stays open at an international scale.
- **Loss of Governance**. For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers.
- **Loss of Trust**. It is sometimes difficult for a cloud service user to recognize his Provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the Provider's security level in a formalized manner. Furthermore, the cloud service users have no abilities to evaluate security implementation level achieved by the Provider.
- **Service Provider Lock-in**. A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another.
- **Unsecure Cloud Service User Access**. As most of the resource deliveries are through a remote connection, i.e. non-protected APIs, services is one of the easiest attack vector. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results.
- **Lack of Information/Asset Management**. When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of

[24] ITU-T Focus Group on Cloud Computing (FG Cloud) was established further to ITU-T TSAG agreement at its meeting in Geneva, 8-11 February 2010 followed by ITU-T study groups and membership consultation. It was successfully concluded in December 2011.

information/asset management by Cloud Service Providers such as location of sensitive asset/information, lack of physical control for data storage, and reliability of data backup.

- **Data loss and leakage**. The loss of encryption key or privileged access code will bring serious problems to the cloud service users.

With respect to the **Cloud Service Providers (CSP),** the following security issues were identified by the Focus Group identified [89]:

- **Responsibility Ambiguity**. Different user roles, such as cloud service provider, cloud service user, client IT admin and data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention.
- **Protection Inconsistency**. Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistent among distributed security modules.
- **Bylaw Conflict**. Depending on the bylaw of the hosting country, data may be protected by different applicable jurisdiction. An international Cloud Service Provider may commit bylaws of its local data-centres which is a legal threat to be taken into account.
- **Shared Environment**. Cloud resources are virtualized and different cloud service users (possibly competitors) share the same infrastructure. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.
- **Abuse Right of Cloud Service Provider**. For a cloud service user, migrating a part of its own IT to a cloud infrastructure implies to partially give control to the Provider. This may lead to a mis-configuration or malicious insider attack.

The specific Security and Privacy issues in the CloNe concept have been explained in Annex 3.

5.6.3 Legal framework

The networks today are in general more open than in the past and one weak link affects the integrity of the whole system. The growth of spam, viruses, spyware and other forms of malware, which is undermining users' confidence in electronic communications, is partly due to that openness. To ensure the security of these critical infrastructures and to protect the citizens' privacy The European Union has taken several measures for ensuring the security of these critical infrastructures and to protect the privacy of its citizens.

In the EU's Privacy Directive (EC Directive 2002/58/EC) [44] and Data Protection Directive (Directive 95/46/EC) [80] privacy in the processing of personal data and the confidentiality of communications are recognised as fundamental rights that should be protected.

The Privacy Directive requires the Member States to harmonise and ensure an equivalent level of protection of the right to privacy with respect to personal data in the electronic communication sector. Regarding confidentiality of communications, the Privacy Directive says that EU member states shall ensure the confidentiality of communications and the related data traffic through the national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned.

The Data Protection Directive prohibits the transfer of personal information to any country that does not have adequate privacy laws. As a result, EU member states have implemented legislation that prohibits the transfer of personal information from

the EU to third countries unless such countries have adequate privacy protection in their laws [77].

For comparison, the United States do not provide adequate privacy protection from the European point of view [87]. To address this problem, the European Commission and the United States Department of Commerce negotiated the Safe Harbor agreement, which is only applicable to transfers between the United States and the European Union. Organizations outside the United States that have business operations within the European Union, have to rely on different mechanisms to adhere to the Transborder Transfer principle from Directive 95/46/EC. This principle requires that personal identifiable information can only be transferred to those countries that are deemed to provide adequate security.

5.6.4 Status of Security and Privacy regulation in Clouds

In Europe, processing of personal data is mainly regulated by the Data Protection Directive 95/46/EC, which is currently under revision. The Directive imposes quite stringent duties and obligations on the actors of such processing, mainly on the '**Controller**'[25] but also on the '**Processor**'[26]. The facts that personal data can be rapidly transferred by the Cloud Service Providers (CSPs) from one data-centre to another and that the customer has usually no control or knowledge over the exact location of the provided resources (the 'location independence' concept described in the article *Cloud Computing Legal Issues: An Overview (Part 1/2)*), stimulate customers' concerns on data protection and data security compliance [86].

On 25 January 2012, the European Commission proposed a comprehensive reform of the EU data protection rules. The draft European Data Protection Regulation is meant to supersede the EU Data Protection Directive from 1995. According to the EC, the new rules will strengthen online privacy rights and boost Europe's digital economy. The reform of the outdated privacy rules reflects that technological progress and globalization have profoundly changed the way data are collected, accessed and used [81].

Article 4 of the Data Protection Directive [80] requires the Member States to apply data protection rules to controllers who process personal data in the 'context of the activities' of their EEA (European Economic Area) 'establishment', or who are not 'established' in the EEA but, for purposes of processing personal data, 'makes use of' equipment (or 'means') situated in the EEA [83]. However, the **application of article 4 to Cloud Computing is complicated** by the fact that many cloud computing service providers don't own the data centres or equipment they use, and may well use the resources of other clouds. Those other Cloud Service Providers in turn may ultimately use data centres and servers rented by third parties. This means that the cloud users don't necessarily know in which data centres, or even countries, their data are stored or where their processing operations are run.

In addition, the data protection laws may differ between EU member states. There are also practical issues relating to whether the Directive can be enforced in non-EU countries. Clarification is therefore needed in the updated Directive on which country's security requirements and other rules apply to a Cloud Computing user or provider [84].

The **Governance models** and processes need also to take into account the specific issues arising from the inherently global nature of the Clouds. Data is subject to specific legislative

[25] *Controller* means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. *Processing of personal data* (*Processing*) means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

[26] *Processor* means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

requirements that may depend on the location where they are hosted, and for what purposes they are processed. Different countries have different laws regarding which kind of data may be hosted where and how it is to be protected. Within the Cloud, data/code may be hosted anywhere within the distributed infrastructure, i.e. potentially anywhere in the world [85].

Clarification of applicable law governing the flow, processing and protection of data is desirable, so that both Cloud customers and Cloud Service Providers have a clear understanding of which rules apply where and how. While there is no question that the Privacy Directive, like other EU Directives, applies to Cloud services, questions do arise as to how and to what extent they apply (geographic and potential subject-matter limits), as well as how they *should* apply to maximise the potential benefits of those services, while still providing the appropriate level of personal data protection [85].

The Cloud Computing Providers hold massive aggregations of customer data. Release of these data, whether accidentally or through the action of a malicious third party, can harm customers particularly if those customers are unaware of the breach. The loss of service continuity and network integrity may be part of breaches, in general, as well. The current European breach notification regime (introduced recently under the Telecommunication Framework Directive (Article 13a) and e-Privacy Directive (2002/58/EC)) only applies to providers of electronic communication services, thus excluding most Cloud Service Providers and other businesses, which does not help to build trust with Cloud customers [85].

To ensure the growth and adoption of cloud computing, it will be necessary to find technological and policy solutions for ensuring privacy and assuring information security.

As a summary, the key regulatory targets for Security and Privacy in Cloud Computing are listed in the following [85], [92], [93]:

- **Promote the Digital Single Market** to encourage efficient cross border cloud services; harmonised implementation of all relevant Directives and legislative instruments are needed in the EU and in the global context.
- **Balance of interests** in protecting privacy and in fostering the EU-wide and global use of cloud computing services; Europe to become not only cloud-friendly but cloud-active to fully realise the benefits of cloud computing; Note: the current laws may discourage non-European users from using EU-based cloud computing providers or making use of European data centres.
- Privacy legislation is looked at in a **global context** and its compatibility with Cloud Computing has to be ensured; Cloud Computing has to be facilitated in Europe and at a global level; Different jurisdictions / regions shall cooperate to develop interoperable requirements that facilitated information flows with appropriate security and privacy protection.
- **Foster interoperability and data portability in the Cloud**; Endorse technology neutrality and promote competition; Avoid mandated standards or preferences that could frustrate, rather than promote, on-going interoperability efforts of the industry at large and among the vendors providing Cloud services and solutions.
- **The applicable law must be easy to define**; A single set of rules on data protection, valid across EU, shall be set up; A legal framework is needed that can be applied across borders, which gives users the means to exercise their rights across borders, which is based on the concept of accountability and draws on technological controls and self regulatory codes and mechanisms as supported by Articles 17 and 27 of the Directive 95/46/EC.
- **The right to be forgotten**, i.e., the right for the individual to request deletion of his/her personal data.
- **Increased responsibility and accountability** for those processing personal data.

5.6.5 Analysis of issues and regulatory approaches

There are at least three levels at which Security and Privacy could be regulated, each with benefits and drawbacks [91]:

- **Government regulation**
- **Industry self-regulation**
- **Consumer or market regulation**

The most obvious place to regulate privacy is at the governmental level. Governments are responsible for writing laws and regulations, and people look to governments to lay down clear rules that prevent harms to the public.

Another level at which to regulate privacy is at the industry level. Industries can develop principles and practices that reflect consensus on the best approach to privacy. In "industry self-regulation," a network of leading companies may require their business partners to meet industry standards on privacy.

Finally, there is consumer or market regulation. Consumers are in the best position to know their desires with respect to privacy, and they are in the best position to enforce the terms of their desires through their choices in the marketplace.

The different approaches have been analysed from the regulatory goals' perspective in Table 11. The goals were introduced in section 5.6.4.

Table 11. Regulatory approaches in Clouds for Security and Privacy.

Criteria (Regulatory targets)	**Government regulation**	**Industry self-regulation**	**Consumer or market regulation**
Promote the Digital Single Market	Yes. Agreements between governments are needed. Yes. Citizens expect that governments lay down rules that prevent harms to the public.	Yes. Industrial players can reach the consensus e.g. on the standards for the interoperability of the cloud systems. Yes. Industries can develop principles and practices that reflect consensus on the best approach to security and privacy. No. Industrial players cannot agree e.g. on the single set of rules for managing security and privacy across different regions.	No. Different standards and rules for managing security and privacy may exist depending on the service provider.
Balance of interests	Yes. Balancing the interests in protecting security and privacy, on one hand, and fostering EU-wide of cloud computing services, on the other hand, can be agreed at least on the EU level. No. Balancing the interests across regions (Europe, America, Asia) is almost impossible. No (all approaches). How to control many types and	Yes/No. Industrial players try to realise the benefits of the cloud computing. However, the success will depend on whether the consumers or corporate users trust in the security and privacy levels. That depends on the service in question. No. There will be variations of balance in different regions and countries. No. Commercial interests	Yes. Consumers and corporate users can choose whether to deal with businesses who promise them a given level of security and privacy. CPSs who offer security and privacy that pleases consumers and corporate users succeed. No. Where some consumers may have very strict senses of privacy, others have fewer reservations about revealing personal

	uses of information in balance with encouraging the commercial exploitation of cloud services.	may lead to breaches in using information.	information and receiving benefits of participation on commercial life.
Security and privacy legislation is looked at in a global context and its compatibility with Cloud Computing has to be ensured	Yes. Security and privacy legislation and its compatibility with Cloud Computing can be agreed at the European level or in any other region. No. The compatibility of the security and privacy legislation with the Cloud Computing is difficult to reach across regions. No. The different levels of privacy are difficult to regulate. Consumers may have • strict senses of privacy • less reservations about revealing personal information No. New uses of information could be cut off.	Yes, but only at the regional levels.	No. Market regulation is not allowed in some regions.
The applicable law must be easy to define	Yes. The governments (EU Commission) can agree on the applicable law. Responsibility and accountability of those storing and processing data can be defined. The agreement on the applicable law across regions would be difficult to reach.	No. The Industrial players have no mandate to agree on the applicable law. No. Depending on the bylaw of the hosting country, data may be protected by different applicable jurisdiction. This may lead to reduced use of cloud services.	No. Consumers have no mandate to agree on the applicable law.
The right to be forgotten	Yes. The governments can enforce the rule 'to be forgotten'.	Yes. The consensus on the right 'to be forgotten' can be reached between the companies of good reputation. No. Rogue companies, that do not want to follow industry standards, may take the opportunity to charge	No. Consumers cannot enforce to be forgotten by the Cloud Service Provider.
Increased responsibility and accountability	Yes. Governments and define and enforce the responsibility and accountability for Cloud Service Providers. This is challenging, however, because the data may be located anywhere.	No. Definition of responsibility and accountability across regions and countries is challenging for the industrial players. Lack of clear definition of responsibility among	No. Consumers have no power to define nor to enforce responsibility and accountability within and across regions and countries.

		cloud service providers and users may evoke conflicts.	

The table above summarizes how the different regulatory approaches would contribute to the different regulatory targets. The Government regulation would promote most of those targets and the Industry self-regulation also many of them. Clearly, the Consumer or market regulation would have most difficulties to promote any of the targets; in this approach the CPSs, which offer the Security and Privacy that pleases consumers and corporate users, would succeed, but most of the issues of the Security and Privacy would remain unresolved.

5.6.6 Summary

Several Security and Privacy issues related to the Clouds have been identified both on the Cloud Service Provider side and on the Cloud Service customer side. These issues may be quite complicated arising from the inherently global nature of the Clouds. The wide scale of deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed or sub-processed.

Data is subject to specific legislative requirements that may depend on the location where they are hosted, and for what purposes they are processed. Different countries have different laws regarding which kind of data may be hosted where, and how it is to be protected. Clarification of applicable law governing the flow, processing and protection of data is desirable, so that both Cloud Users and Cloud Service Providers have a clear understanding of which rules apply where and how.

In the beginning of this year (2012) the European Commission proposed a comprehensive reform of the EU data protection rules. It is meant to supersede the EU Data Protection Directive from 1995. The reform of the outdated rules reflects that the technological progress and globalization have profoundly changed the way the data are collected, accessed and used. In this context the industry recommendations to EU Commissioner Neelie Kroes on the orientation of a European Cloud Computing strategy has stated that "*The EU needs to become not only Cloud-friendly, but Cloud-active to fully realise the benefits of Cloud computing. Besides allowing for the provision of Cloud computing in its various forms, the relevant environment in the EU has to address the needs of end users and protect the rights of citizens*. *At the same time, it should allow for the development of a strong industry in this sector in Europe*" [85].

5.7 Conclusions

In this chapter a business analysis of CloNe was performed more focused on the enterprise market sector. In this analysis we highlighted some of the business drivers behind CloNe, provided an overview on CloNe's ecosystem with special focus on the current state of the market and on what we believe to be the market in a near future, showing that CloNe is on the right path to serve the market of tomorrow. Moreover, we evaluated on the service adoption determinants. The technical and industry architecture as well as stakeholders were also studied. The business model issue was brought up, were the uncertainty regarding the CloNe future business landscape was highlighted, which makes it risky to put forward any detailed future business model evaluation now. Finally, a regulatory analysis was performed on the security and privacy aspects of cloud computing.

In this study, three different approaches for regulating Security and Privacy in Clouds were analysed and compared and the results are seen to be relevant also in the CloNe context. None of the three approaches promotes all regulatory targets, but Government regulation would do that the most. However, balancing the interests and agreeing on the applicable law across regions would be very difficult also in this approach. It would also be difficult to control

many types and uses of information in balance with encouraging the commercial exploitation of Cloud Services.

Industry self-regulation does also support many of the regulatory targets, but it would be difficult to agree on the single set of rules across different regions. Also, the industrial players would not have a mandate to agree on the applicable law, anywhere. The definition of responsibility and accountability would be challenging for the industrial players, and the lack of them would evoke conflicts. Regarding Consumer or Market regulation, consumers and corporate customers can choose whether to deal with businesses who promise them a given level of Security and Privacy. However, where some consumers may have very strict senses of Privacy, others have fewer reservations about revealing personal information. In the end, those Cloud Service Providers, who offer Security and Privacy that pleases most consumers and corporate customers, will succeed.

In the end, achieving Trust in Clouds needs the European and global level actions. The European Commission proposed on 25 January 2012 a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. And as Vice-President Neelie Kroes said in the press-release (Brusses, 27 September 2012): *"Cloud computing is a game-changer for our economy. Without EU action, we will stay stuck in national fortresses and miss out on billions in economic gains. We must achieve critical mass and a single set of rules across Europe. We must tackle the perceived risks of cloud computing head-on."*

6 Business Recommendations

Based on the business analysis earlier in this document and in D.A.7, several business recommendations for the technical development of each technology are proposed in this section. Though the recommendations are all meant for supporting the technical development, they arise from three different aspects: business, social and regulation, and are marked with B, S and R, respectively.

6.1 Business Recommendations for NetInf

This section presents requirements for NetInf in general, identified during the socio-economic analysis conducted for earlier SAIL Deliverables D.A.1 [1] and D.A.7 [2]. The requirements are relevant to all types of communication (content distribution, interactive web services, person-to-person, and machine-to-machine), but they originate from the NetInf TV scenario, which focuses on commercial content distribution from providers to consumers. Interestingly, many of the identified requirements are discussed in the security section of Deliverable D.B.1 [17]. Actually, security threats are often more interesting from the business than security perspectives, since security is rarely a good selling point itself. Thus, emphasising the business relevance of the identified security threats is a recommended strategy.

The requirements are identified and explained below, each being identified with the letters B, S, or R, highlighting if the requirement is related to Business, Social or Regulation aspects, respectively.

NetInf-R1: NetInf should be able to accommodate conflicting stakeholder interests (B, S, R)

Stakeholders may have conflicting interests and objectives when it comes to content delivery. End-users and their content service providers are interested in improving end-user experience, e.g., by minimising the latency or maximising content freshness, whereas Internet Service Providers may be more interested in minimising network traffic. One objective, transport cost minimisation, is common to all stakeholders, but often the cost reduction for one stakeholder leads to cost increase (or other negative impact) for another. Balancing stakeholder objectives, so that every stakeholder would be satisfied, may not be possible, but the successful deployment of NetInf requires that, at least, all stakeholders that can affect (either positively or negatively) the deployment are satisfied.

This requirement covers many of the other requirements and can therefore be taken as a general guideline.

NetInf-R2: NetInf should allow flexible and versatile control over request routing (B)

If the content is available in multiple locations, where to serve content requests is the most interesting business question. In an optimal case, end-user, content provider and all the ISPs on the path between them should be able to signal their preferences. However, it is not certain which of the stakeholders should make the final decision, even though the most successful of the early ICN architectures (CDN, CP-controlled P2P) allow content providers to make that decision. From the perspective of this requirement, the name resolution-based operation of NetInf seems more feasible than the name-based routing one because NRS provides a natural control and management point, which seems to be missing from the name-based routing mode.

NetInf-R3: NetInf should to be able to deliver guaranteed and differentiated QoS without questioning net neutrality (B, R)

Neither is every piece of content equally important nor does it have the same QoS requirements. The emergence and success of CDNs suggests that a need and willingness to pay for “better than best effort” quality exists in the market. Therefore, NetInf should allow different stakeholders, most notably content providers who seem to have largest interest for paying for quality [108], to flexibly control content caching. This comes back to cache management algorithms, methods to signal preferences, and mechanisms to charge for differentiated QoS. One concern that may emerge relates to net neutrality, especially if an actor that serves also its own content through the same system controls caching. NetInf as a technology may have difficulties in solving this problem, but the more transparent the ICN is, the more difficult it is to violate net neutrality.

NetInf-R4: NetInf should have space for a platform that controls content distribution (B)

The success of the proprietary CDN model (Akamai style) suggests that a platform can more easily solve the coordination challenges of content distribution (e.g., related to cost allocation, contracting, QoS guarantees and content usage statistics) than distributed, end-to-end solutions. On the other hand, platforms being able to internalize the positive network effects, such as platforms on two-sided markets [108], have a tendency to become monopolistic or oligopolistic, which may not be desired. Therefore, encouraging platform owners to collaborate by devising open standards, interfaces and information structures may be recommendable to increase competition.

NetInf-R5: NetInf should be able to limit the content access to authorised users (B)

This requirement has been identified in the security section of Deliverable D.B.1 [17], but the used terminology (e.g., bad user) refers more to a security threat involving an attacker rather than to plain business incentives of content owners or providers to limit the usage to those who have registered (and possibly paid) for the content. The solution should scale to large number of users and constant changes in authorisations.

NetInf-R6: NetInf should be able to collect content usage and delivery information (B)

Content usage parameters, such as number and timing of content requests or information about content requestors, and content delivery parameters, such as cache server load, end-to-end delays, or cache hit ratio, are important information for the content providers whose business depends on their availability. For example, the payments to content makers and from advertisers may depend on the number of requests. Also, tracking the end-user experience is vital for content providers to survive in competition for end-users’ attention.

NetInf-R7: NetInf should have a mechanism to control where the content is cached (B, R)

Even though for NetInf content is just bits, the bits may contain some information that should not be stored everywhere. For example, a government may require that health care data are stored only on domestic servers, which would limit the cache locations. Additionally, cache owners are not interested in being responsible for the content they cache. Thus, NetInf caching needs to fit to the legislative framework so that cache owners are not held responsible for the cached content.

NetInf-R8: NetInf should share information about network state between stakeholders as transparently as possible without revealing business secrets (B)

Cache owners may decide to hide critical information, or provide inaccurate information about the state (load, congestion, etc.) of cache servers or other network elements, in order to affect the content delivery, fearing that such sensitive information could be used for espionage. For instance, a cache owner may want to promote the content delivery by an overloaded server due to lower cost although this would imply degraded QoE for end-users. Therefore, to avoid misuse and conflicts related to asymmetric information between different stakeholders, NetInf should promote transparent operation at an acceptable level (i.e., reveals enough, but not too much).

NetInf-R9: NetInf should ensure that the end-users get the IOs they wanted (S)

Current P2P networks suffer from the pollution problem [109] where end-users often do not get the content they want but rather some spam with the same name. Globally unique names may solve this problem only partially because often the problem relates more to choosing the right object from a set of available candidates based on their metadata including, for example, content name or description. The source/content owner identification available in the meta-data may help here but also trust and reputation systems [110] used, for example, in P2P networks could be helpful to differentiate real content from spam.

NetInf-R10: NetInf deployment should extend stepwise from small-scale intra-domain deployments towards wide-scale and inter-domain deployment (B)

A new technology faces challenges when trying to get the acceptance from the market with incumbent solutions. This holds true especially for technologies with substantial network effects, such as NetInf. Facilitating sub-network adoption, i.e., adopting networking technology first in intra-domain scope, has been identified as a strategy to avoid the bootstrapping problem where the benefits of technology adoption realize only after a certain number of potential end-users (known as critical mass) has adopted the technology [33]. Consequently as Section 3.5 suggests, for example ISPs should start using NetInf first inside their own network and only later extend to inter-domain business models including transactions with other stakeholders.

6.2 Business Recommendations for OConS

As already stated before, the Open Connectivity Services (OConS) scenario has several use-cases to highlight different aspects of the work being developed. Use-Cases 1 and 3 have been considered the most important ones for a business analysis perspective.

The business recommendations for the use-case 3 have been already presented in Section 4.2. Below, the business requirements for the Use-Case 1 are presented. This Use-Case has already been analysed in Deliverable D.A.7 [2]. It focuses on the development of Wireless Mesh Networks (WMNs), which have the ability to provide connection to the Internet in areas with difficult or limited access to the network by connecting several devices together. This can revolutionise mobile network technology and network architectures. Regarding requirements for technical work, WMN solutions require a service infrastructure that ensures the following, as presented in D.A.7. Some of these requirements are very much generic for any similar solution, but nonetheless, they must be taken into account when developing a business model

OConS-UC1-R1: Need for regulatory concerns (B, R)

The technology that is being created, as any new technology, will need new regulation prospects. A down to business approach can facilitate and prevent the call for

regulation in the initial situation, and reduce the interference caused by new regulation where it appears.

OConS-UC1-R2: Back-office transaction operations (B)

Back-office transactions should include billing for different user groups, subscriber management, and pre- and post-paid billing systems, as well as credit card paying options (predominantly to support expatriate subscribers), one-time password, scratch cards, and e-voucher solutions.

OConS-UC1-R3: Security (B, S)

Sufficient security with authentication and authorisation steps to prevent misuse and achieve accountability of resources usage is needed. Also a combination of factors that describe the integrity of a system and its users must be taken into action. This requirement should also be applied for including the security of users over the network, as well as the secure transport of information.

OConS-UC1-R4: Efficiency (B)

The network management must be efficient. In this requirement, the following topics and actions must be evaluated: Operational costs – one can expect a maximum of efficiency in areas such as Business processes, work performance and levels of capital costs; Flexibility – a high capacity is required to deal with the market needs, in order to provide a good level of service; Collaboration – all the areas that this new technology combine must have high levels of joint performance; Information Flow – this is a key area for efficiency, since without a good information flow, all the technology approach and implementation can be questioned.

OConS-UC1-R5: New transport paradigms and a new application protocol design (B)

A new way of implementing a service was created and, in order to succeed, it must be supported by all players.

OConS-UC1-R6: Capabilities (B, S)

The new service presented to the market must contain and have developed roaming. This new technology should also enable nodes to constantly take benefit of intelligent network services, in order to improve QoE and reduce the cost of deployment and network operations. These new capabilities must reduce the costs and the complexity of deploying a new network, and accelerate the troubleshooting and the capability to analyse the impact of data on the network.

OConS-UC1-R7: Adaptive Network Architectures (B)

The infrastructure for self-service and service lifecycle management, roaming, clearing house and settlement functions must be created for a good performance of the mesh networks. In this case, the technology developed in Use-Case 1 must have adaptive network protocols for a proper use of the service that will be implemented.

6.3 Business Recommendations for CloNe

For commercial CloNe services to have a general market acceptance, some business requirements must be identified and considered during service design and prototyping; therefore, a minimum set of business requirements for this service are put forward below.

These requirements intend to draw the attention to factors that may impact a successful commercial deployment of CloNe in the future. Some of these requirements have more and others less impact at the technical level, but either way CloNe's development on WPD must have in mind these requirements, stating in the end of the project to what extent the developed work complies with them.

Note that, in Deliverable D.A.7 [2], the adoption determinants of the CloNe service were analysed in the light of the perceived service perspective from the enterprise client and the network operator actors towards the Dynamic Enterprise scenario. Some of the requirements pointed out below came from that analysis, again being identified as being Business (B), Social (S), or Regulation (R) related.

CloNe-R1: CloNe should be able to support end-user mobility (B, R)

It emerged clearly from D.A.7 [2] that mobility is today a fundamental requirement for service adoption in the corporate context. Clients of the enterprise sector expressed large interest in the service concept if it could be applied also to their 3rd Generation (3G)/Long Term Evolution (LTE) wireless access solutions. Recurring questions on the interviews from clients were: "How does this cloud networking service concept relate to the access network, namely to mobility scenarios?", or "Can we use the CloNe service to access my service while on the move?". When combining mobility needs and technological trends of high bandwidth wireless solutions, such as LTE, most of the interviewed clients asked if they could use the cloud networking service to access their Information Technology (IT) / Information System (IS) resources when they are on the move.

Even if CloNe's technical WP does not directly address mobility scenarios, it should not neglect to emphasize CloNe's ability to support such scenarios. In line with this thought comes the next requirement, CloNe-R2.

We believe that despite this requirement coming from the enterprise segment, it also applies to other market segments.

Regulatory issues also arise in relation to this requirement, because the mobility concept extends to international mobility if the service is to have broad success.

CloNe-R2: CloNe technical and business requirements on the Access and Edge Networks (B, R, S)

CloNe's architecture description (Deliverable D.D.1 [107]) defines a FNS as an abstraction of the basic network resource that can be instantiated on different types of networks, focusing on existing or near-term protocols and systems. This description focuses on the core network segment of the network operators, but strongly relies on edge and access network capabilities, namely availability, reliability, broadband throughput capacity, geographical coverage, access and edge technology used, roaming capabilities, etc. At the same time, nothing in the architecture prevents an FNS from being instantiated over a 3G/LTE network. Therefore, CloNe minimum technical requirements on edge and access network segments should be described by WP-D. The ability for CloNe to rely on OConS in such scenarios should also be considered. This requirement also relates to CloNe-R1. Also a business model impact analysis should be performed, in order to account for the impact of the access network business model in the overall CloNe one, from the end-users as well as the network operator perspectives.

CloNe-R3: CloNe should be able to support resource mobility/migration (B, R)

Mobility is a requirement for CloNe, not only at the end-user level (CloNe-R1) but also at the resource level (the former naturally implies the latter). Resources must be able to migrate whether to respond to a user's request or to optimise resource allocation, which sometimes helps preventing SLA violation.

The migration of computing resources (virtual machines) is a reality within data centres and also between data centres, thus CloNe cannot aim for less. From computing resources to

network resources, CloNe must be able to support (to some extent) the mobility of its resources. One of the biggest challenges of CloNe lies in the operator's network, where such functionalities do not exist today, neither at the Operations Support System (OSS) level nor at the Business Support System (BSS) level.

In an ideal approach, CloNe should embrace live migration as a natural function, however as stated in D.D.1 [107] this is not a simple task.

CloNe-R4: CloNe should have a mechanism to control and audit where resources are located (B, R)

Resource and information location are a major concern (constrain/restriction) in Cloud environments, from either a business, regulatory or end-user perspective. CloNe should have the means to be aware of the location of the virtual resources for a given moment in time and also be able to provide such information to external entities (e.g., end-users, regulatory entities).

CloNe-R5: CloNe should possess end-to-end information regarding the state of resources in use (B, R)

Service-Level Agreements (SLAs), especially those in the Cloud and Telco business, rely on probability information (e.g., availability of a service). In order to support such SLAs, end-to-end information from the support infrastructure is required (e.g. deterministic, statistical or probabilistic information). Information flowing between different administrative domains (different actors) will naturally have a smaller degree of detail to prevent the disclosure of relevant actor-specific business information.

CloNe-R6: CloNe must emphasize in which way it improves the reliability of today cloud computing solutions (B)

Knowing that every now and then cloud services get interrupted, CloNe should promote itself in the market by pointing out its key advantages and reliability improvements over today's cloud computing solutions. Cloud Computing keeps on conquering the market at a high rate and CloNe must highlight the "plus" that it adds to it.

CloNe-R7: CloNe must highlight how it will handle applications (B)

Deploying and managing (virtual or physical) infrastructure for supporting complex applications is not a simple task. Which management tools will be available with CloNe to facilitate that? How do CloNe management tools compare to other management tools available in other cloud computing solutions?

Moreover, who should manage the elasticity of the application, the application or CloNe If it is CloNe what are the interactions/interfaces between the application and CloNe which allow CloNe to know how to extend/reduce resources? Is there a specific programming model/architecture that should be respected to use the elastic feature of CloNe? If the application is the one that will manage the elasticity, then what are the management tools available to monitor and adjust the resources used by my application?

CloNe-R8: CloNe must provide a single commercial focal contact point to the end-users (B, R)

Again, from D.A.7 [2] emerged the need for a single commercial focal contact point to the end-users in order to favour service adoption. In DA.7, respondents stated that it is easier to hold a single entity than several entities responsible for any occurrence in the IT/IS solution; and that it is preferable to manage a single invoice for IT/IS systems than several ones. In other words, there should not be any delegation of responsibilities from the end-users perspective.

End-users do not need to have full visibility to all of the managed domains that support their solutions, as long as they have a single entity accountable for the service and the Service Level Agreement (SLA), thus, regulation and clear responsibility assignment to the entire supply chain must be established.

CloNe-R9: CloNe should provide IT/IS systems that can evolve and be customised for end-users specific needs (B)

Clients expected that the administration of IT/IS systems can be done effortlessly by the enterprise (either directly on a self-service tool or API or via HelpDesk in Software as a Service (SaaS) model). CloNe should provide an easy to use Web Service Interface or a standard API for IT/IS systems, in order for end-users to be able to take advantage of the CloNe service offerings with ease of use and evident relative advantage when facing other solutions.

CloNe-R10: CloNe should exhibit a two flavour service – autonomous & on-demand self-service (B)

Scalability is a fundamental feature of CloNe, thus, it must have (B/OSS) systems to constantly monitor resources and scale them automatically. Moreover, it should also have an on-demand self-service portal for management with human interaction. Additionally, enterprise end-users expect that these systems can evolve and be customised for the specific needs of each enterprise.

CloNe-R11: CloNe should provide self-service portals to manage services based on a use-case choice (B)

In order to expedite the service adoption and remove complexity from the service usage, service interfaces should be self-explanatory and very much focused on end-users business context, e.g., “If you want to interconnect two High Definition (HD) video-conference points chose this option”. This suggests an interface able to hide the complexity from the end-user as much as possible, which also may avoid the reservation of unnecessary resources. Naturally, it is difficult to tackle all possible situations. Nevertheless, CloNe should be able to, at least, provide some possibilities, mainly those related to the scenarios and use-cases defined in Deliverable D.A.1 [1]. Moreover, it should provide the ability to add more usage use-case choices as the service evolves over time.

CloNe-R12: SAIL and Traffic Prioritisation, Net-Neutrality and Service Assurance (B, R)

The CloNe architecture offers the capability to manage physical and virtual resources, distributed through several network domains with self-managed dynamic connectivity service capabilities, thus, enabling enhanced QoE, performance, and reliability for end-users compared with pre-SAIL scenarios. This concept will implicitly require non-net-neutrality scenarios and traffic prioritisation rules across all of the managed domains, in order to guarantee the final QoE promised to the end-users. In addition, service assurance capabilities across the entire managed domains must be guaranteed to end-users, which imply network element troubleshooting capabilities across the entire managed domains, in an integrated end-to-end view.

CloNe-R13: CloNe’s cost element estimates in the operator network (B)

Additionally, if CloNe is to ever see the light of day in commercial implementations, a network operators’ cost-benefit analysis must be sufficiently attractive for them to deploy the CloNe technology in their networks. Cost element estimates should be put forward from the technical group in WP-D, in order for WP-A to be able to build a cost structure for CloNe deployment in a network (CAPEX + OPEX estimates should be put forward).

CloNe-R14: CloNe should make sure that its proposed architecture can be supported by at least one business model

The CloNe architecture allows different possible (implementation) scenarios. However, CloNe cannot forget that these scenarios must be held by a business model, i.e., for CloNe technical WP to specify technical interactions a business model must be taken into account. Multiple business models can be considered, depending on the scenario.

We call attention, for example, to the situation in which a CloNe provider relies on other domains to respond to a request. The CloNe provider in this case can be seen as a virtual provider, a broker. The way business relations are established in such scenario is intimately related on how the technical components (Distributed Control Plane (DCP) and Infrastructure Service Interface) will work among the different domains. This issue must also be taken into account in scenarios in which more than one hop delegation present.

We believe this to be a critical issue, where business and technical issues intersect, and therefore it cannot be neglected.

From our point of view the above business requirements are themselves technical challenges that must be addressed by the technical WPs of the project to support commercial CloNe service adoption.

7 Conclusion and future work

This document linked the technical work done in SAIL to the socio-economic perspectives and possible business potentials. For each of the technologies, an overview of the ecosystem is given, which is followed by the technical and industry architectures. In addition, the different stakeholders' benefits and value networks were analysed and possible business models proposed. Additionally, a regulatory perspective was taken on issues concerning interconnection charging, privacy, security and content. Lastly, based on analysis, several business recommendations for the technical work and development were suggested.

The main results of this document include the business models presented in Sections 3.5, 4.5 and 5.5. For NetInf (Section 3.5), a six-step business model evolution path is suggested, from which three are evolutionary and the last two include the entrance of new actors and business agreements into the market. Similarly, for OConS, four cost/benefit scenarios were proposed where the revenue and cost flows of the different stakeholders were shown. On the other hand, CloNe's usage includes a wide variety of applications, thus no single business model could be suggested.

Another important finding is the business recommendations, which arose from the business and regulative analysis done in both D.A.7 and this document. The recommendations help the technical work packages in meeting the demand set by end users, stakeholders in the market, and regulators when developing the new technologies.

Both the business models and the business recommendations aim at a smooth transition from the existing technology and market to the new technologies. Thus, future work includes defining the possible technical migration paths but also taking into consideration the socio-economic factors. The result of the migration work should be visible in the SAIL delivery D.A.4. From the business aspects, future work could include, for example, quantification of the caching potential presented in Section 3.2.2.

List of Abbreviations, Acronyms, and Definitions

3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
AAA	Authentication, Authority, Accounting
ADSL	Asymmetric Digital Subscriber Line
ANP	Access Network Provider
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CDNi	CDN Interconnect
CIP	Community Infrastructure Provider
CloNe	Cloud Networking
CO	Community Operator
CP	Content Provider
CPE	Customer premises equipment
ICN	Information-Centric Networking
ICP	Inter-Connectivity Provider (aka Transit Provider)
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
IP	Internet Protocol
IPTV	IP Television
IXP	Internet Exchange Point
LTE	Long Term Evolution
NDO	Named Data Object
NetInf	Networking of Information
NRS	Name Resolution Service
OConS	Open Connectivity Services
OPEX	Operational Expenditure
OTT	Over-the-top
QoE	Quality of Experience
QoS	Quality of Service
RoR	Rate of Return
SAIL	Scalable and Adaptive Internet Solution
VNC	Value Network Configuration
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

List of Tables

List of Figures

References

All references used in the document must be defined in the References chapter in the following format:

[1] B. Tremblay (ed.), *Deliverable D.A.1 - Description of project wide scenarios and use cases*, SAIL Project, Apr. 2011 (http://www.sail-project.eu/wp-content/uploads/2011/09/SAIL_DA1_v1_2_final.pdf)

[2] J. Salo (ed.), *Deliverable D.A.7 - New Business Models and business dynamics of the future networks*, SAIL Project, July 2011 (http://www.sail-project.eu/wp-content/uploads/2011/08/SAIL_DA7-Final-Version_public.pdf).

[3] Cisco, *VNI Forecast Highlights*, http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html Accessed 120920

[4] Ericsson, *Traffic and Market Report, June 2012* (http://www.ericsson.com/res/docs/2012/traffic_and_market_report_june_2012.pdf)

[5] Cisco, VNI Mobile Forecast Highlights, 2011-2016 http://www.cisco.com/web/solutions/sp/vni/vni_mobile_forecast_highlights/index.html Accessed 120920

[6] ITU, ITU-D: ICT Data and Statistics (IDS): Mobile Cellular Telephony, June. 2012 (http://www.itu.int/ITU-D/ict/statistics/).

[7] Cisco, Cisco Visual Networking Index: Global Mobile Data. Traffic Forecast Update, 2011–2016, June 2012 (http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html).

[8] CNN, Smartphone traffic is up 193% in a year, June 2012 (http://tech.fortune.cnn.com/2010/03/25/smartphone-traffic-is-up-193-in-a-year).

[9] Telecoms.com, Smartphone traffic to grow 700% in five years, June 2012 (http://www.telecoms.com/23187/smartphone-traffic-to-grow-700-in-five-years).

[10] EC FIArch Group, Fundamental Limitations of current Internet and the path to Future Internet (http://www.future-internet.eu/uploads/media/FIArch_Current_Internet_Limitations_March_2011__FINAL_.pdf)

[11] Wikipedia, *Disruptive Innovation* http://en.wikipedia.org/wiki/Disruptive_innovation Accessed 120920

[12] G.A. Moore; *Crossing the chasm*, ISBN 0-06-051712-3

[13] G.A. Moore; *Inside the tornado*, ISBN 0-88730-824-4

[14] Telecommunications Regulation Handbook, Hank Intven, McCarthy Tétrault [infoDev, ISBN 0-9697178-7-3], 2000, http://www.infodev.org/en/publication.22.html

[15] P Farating et al: Complexity of interconnections, http://people.csail.mit.edu/wlehr/Lehr-Papers_files/Clark%20Lehr%20Faratin%20Complexity%20Interconnection%20TPRC%202007.pdf

[16] GSR 2009 Discussion Paper, http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Lazauskaite_MTRs.pdf

[17] P. Pöyhönen and O. Strandberg (eds.), *Deliverable D.B.1 - The Network of Information: Architecture and Applications*, SAIL Project, July 2011 (http://www.sail-project.eu/wp-content/uploads/2011/08/SAIL_DB1_v1_0_final-Public.pdf).

[18] G. Kunzmann, D. Staehle (eds.). *Deliverable D.B.2: NetInf Content delivery and operations*, SAIL Project, May 2012 (http://www.sail-project.eu/wp-content/uploads/2012/06/SAIL_DB2_v1_0_final-Public.pdf).

[19] Sandvine Inc., *Global Internet Phenomena Report: 1H 2012,* 2012. [online] Available at: < http://www.sandvine.com/news/global_broadband_trends.asp> [Accessed 10 June 2012]

[20] P.J. Schoemaker, "Scenario Planning : A Tool for Strategic Thinking", *Sloan Management Review*, Vol. 36, No. 2, Winter 1995, pp.25-40.

[21] N. Zhang, H. Hämmäinen, T. Levä, *Future Scenarios of Commercial Internet Content Delivery.* In Proceedings of 23rd European Regional ITS Conference, 1-4 July 2012, Vienna, Austria.

[22] Orange, *Press release: Orange France updates its triple play range, introducing Livebox star and Livebox zen*. 8 Apr 2011. [online] [Accessed on 14 Jun 2012] at: http://www.orange.com/en_EN/press/press_releases/cp110408en.jsp.

[23] XFINITY, *Comcast Triple Play,* 2012. [online] [Accessed on 14 Jun 2012] at: http://www.comcast.com/Corporate/Learn/Bundles/bundles.html.

[24] Sanoma, *Press Release: Helsingin Sanomat is the first Finnish media company to provide a combo deal for an iPad and newspaper,* 23 Apr 2012 [online] [Accessed on 19 Jun 2012] at: http://www.sanoma.com/about-us/sanoma-news/news/helsingin-sanomat-is-the-first-finnish-media-company-to-provide-a-combo-deal-for-an-ipad-and-newspaper.

[25] Spotify, *What is spotify,* 2012. [online] [Accessed on 24 May 2012] at: http://www.spotify.com/fi/about/what/.

[26] Sony, *Music unlimited,* 2012. [online] [Accessed on 24 May 2012] at: https://music.sonyentertainmentnetwork.com/.

[27] Voddler, *About voddler,* 2012. [online] [Accessed on 24 May 2012] at: http://voddlertalk.voddler.com/om/.

[28] K. Yagoub, D. Florescu, V. Issarny, P. Valduriez, *Caching Strategies for Data-Intensive Web Sites*. VLDB 2000, pp. 188-199, 2000.

[29] Jacobides M., Knudsen T., Augier M. (2006), Benefiting from innovation: Value creation, value appropriation and the role of industry architectures, Research Policy, vol. 35, pp. 1200–1221. doi:10.1016/j.respol.2006.09.005

[30] D.D. Clark, J. Wroclawski, K.R. Sollins, R. Braden, *Tussle in Cyberspace: Defining Tomorrow's Internet*. IEEE/ ACM Trans. Networking 13, 3, pp. 462-475, June 2005.

[31] A.Kostopoulos, I.Papafili, C. Kalogiros, T. Levä, N. Zhang, D. Trossen, *A Tussle Analysis for Information-centric Networking architectures*, FIA Book 2012.

[32] C. Kalogiros, C. Courcoubetis, G.D. Stamoulis, M. Boniface, E.T. Meyer, M. Waldburger, D. Field, B. Stiller, *An Approach to Investigating Socio-economic Tussles Arising from Building the Future Internet*. FIA Book 2011, LNCS, vol. 6656, pp. 145-159, May 2011.

[33] A. Ozment, S. Schechter. *Bootstrapping the adoption of internet security protocols*. Proc. Fifth Workshop on the Economics of Information Security, 2006

[34] B. Tremblay, M. Soellner (eds.). *Deliverable D.A.9: Description of overall prototyping use cases, scenarios and integration points*, SAIL Project, June 2012 (http://www.sail-project.eu/wp-content/uploads/2012/08/SAIL_DA9v1_0_final-public.pdf).

[35] Content Delivery Networks Interconnection (cdni) - Working Group Charter. [online] Available at: http://datatracker.ietf.org/wg/cdni/charter/ [Accessed 13 Sep 2012]

[36] OCEAN. Open ContEnt Aware Networks (OCEAN). EU FP7 project. [online] Available at: http://www.ict-ocean.eu/ [Accessed 13 Sep 2012]

[37] Niven-Jenkins, B., Le Faucher, F., Bitar, N. Content Distribution Network Interconnection (CDNI) Problem Statement, draft-ietf-cdni-problem-statement-08, Internet-draft (Work in Progress) [online] Available at (http://datatracker.ietf.org/doc/draft-ietf-cdni-problem-statement/) [Accessed 13 Sep 2012]

[38] Bertrand, G. , Stephan, E., Burbridge, T., Eardley, P., Ma, K., Watson, G. Use Cases for Content Delivery Network Interconnection, draft-ietf-cdni-use-cases-10, Internet-draft (Work in Progress) [online] Available at (http://datatracker.ietf.org/doc/draft-ietf-cdni-use-cases/) [Accessed 13 Sep 2012]

[39] Leung, K., Lee, Y. Content Distribution Network Interconnection (CDNI) Requirements, draft-ietf-cdni-requirements-03, Internet-draft (Work in Progress) [online] Available at (http://datatracker.ietf.org/doc/draft-ietf-cdni-requirements/) [Accessed 13 Sep 2012]

[40] S. Puopolo, M. Latouche, F. Le Faucheur, J Defour. *Content Delivery Network (CDN) Federations - How SPs Can Win the Battle for Content-Hungry Consumers.* [online] Available at http://www.cisco.com/web/about/ac79/docs/sp/CDN-PoV_IBSG.pdf [Accessed 13 Sep 2012]

[41] Skytide. *7 Online Video Trends to Watch in 2012*. White paper. 2012 [online] Available at: http://www.skytide.com/blog/7-online-video-trends-to-watch-in-2012.html [Accessed 13 Sep 2012]

[42] Mayers, J., Tracking the trackers: where everybody knows your username. Blog post on Stanford University Law School's Center for Information and Society, 11 Oct 2011. [online] [Accessed on 12 Dec 2011] at: http://cyberlaw.stanford.edu/node/6740.

[43] Ministry of Justice, *458/2002: Act on on provision of information society services*. FINLEX, 2002. [online] [Accessed 12 Dec 2011] at: http://www.finlex.fi/fi/laki/kaannokset/2002/en20020458.pdf.

[44] EU, L 201/37: DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002. *Official Journal of the European Communities*. [online][Accessed on 12 Dec 2011] at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

[45] Ministry of Justice, *516/2004: Act on the Protection of Privacy in Electronic Communications* (amendments up to 365/2011 included), 2004. [online] [Accessed on 12 Dec 2011] at: http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf.

[46] Lehto, T., Tekijänoikeuskiista jaruuttaa netti-tv kehitystä. *Tietokone*, 9 Mar 2010. [online] [Accessed on 12 Dec 2011] at: http://blogit.tietokone.fi/tietojakoneesta/2010/03/tekijanoikeuskiista-jarruttaa-netti-tv-kehitysta/.

[47] HS, Poliisi epäilee TVKaistaa tekijänoikeusrikoksesta. *Helsingin Sanomat*, 5 May 2011. [online] [Accessed on 12 Dec 2011] at: http://www.hs.fi/kulttuuri/artikkeli/Poliisi+ep%C3%A4ilee+TVkaistaa+tekij%C3%A4noikeusrikoksesta/1135265903220.

[48] EU, L 167/10: DIRECTIVE 2001/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001. *Official Journal of the European Communities.* [online][Accessed on 11 Sep 2012] at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF.

[49] EU, COM(2009) 532 final: COMMUNICATION FROM THE COMMISSION, Copyright in the Knowledge Economy. 19 Oct 2009. [online] [Accessed on 11 Sep 2012] at: http://ec.europa.eu/internal_market/copyright/docs/copyright-infso/20091019_532_en.pdf.

[50] FICORA, *Act on the Provision of Information Society Services - Electronic commerce,* 2011. [online] [Accessed 13 Dec 2011] at: http://www.ficora.fi/en/index/saadokset/lait/tietoyhteiskunta.html.

[51] Project-wide evaluation of Business Use Cases, 4WARD deliverable D1.2

[52] Final Assessment on the Non-technical Drivers, 4WARD deliverable D1.4

[53] CITEL Guidelines and Practices for Interconnection Regulation, draft June 1999, Inter-American Telecommunications Commission, http://www.citel.oas.org/ccp1-tel/guidelines/guidelines%20on%20Interconnection.pdf

[54] ICT Regulation Toolkit, Designing Next Generation Telecom Regulation: ICT Convergence or Multisector Utility? By Anders Henten, Rohan Samarajiva, William H. Melody,. Published May 2006, http://www.ictregulationtoolkit.org/en/index.html

[55] Wikipedia, Internet Transit, http://en.wikipedia.org/wiki/Internet_transit

[56] Gilbert Tobin Lawyers: Economic study on IP interworking, http://www.gsmworld.com/documents/ip_intercon_sum.pdf

[57] D Clark, W Lehr, S Bauer: Interconnetion in the Internet: the policy channel, prepared for the 39th Research Conference on Communication, Information and Internet Policy, George Mason University, Arlington, VA, September 23-25, 2011; http://www.tprcweb.com/images/stories/2011%20papers/Clark-Lehr-Bauer_2011.pdf

[58] DrPeering International, http://drpeering.net/white-papers/Peering-Policies/A-Study-of-28-Peering-Policies.html

[59] EU Commission: Cloud Computing, Digital Europe's perspective – version 5, Final Draft

[60] Graeme A. Guthrie (Victoria University of Wellington), John P. Small (University of Auckland) Pricing Access: Forward-looking versus Backward looking cost rules http://profile.nus.edu.sg/fass/ecsjkdw/forward%20looking%20costs%20revised.pdf

[61] William P. Rogerson (Northwestern University) October 3, 2005: ON THE RELATIONSHIP BETWEEN HISTORIC COST, FORWARD-LOOKING COST AND LONG RUN MARGINAL COST, http://www.chicagobooth.edu/research/workshops/archives/accounting/marginalcost35.pdf

[62] L. Suciu (ed.), Deliverable D.C.1 - Architectural Concepts of Connectivity Services, SAIL Project, July 2011 (http://www.sail-project.eu/wp-content/uploads/2011/08/SAIL_D.C.1_v1.0_Final_PUBLIC.pdf).

[63] L. Suciu and A. Timm-Geil (eds.), Deliverable D.C.1 - Architectural Concepts of Connectivity Services – Addendum, SAIL Project, Jan. 2012.

[64] L. Suciu and A. Timm-Geil (eds.), Deliverable D.C.2 - Architecture and Mechanisms for Connectivity Services, SAIL Project, Sep. 2012.

[65] G. Zibi, Low-cost Mobile Business Models - Strategies for Profits at the Bottom of the Pyramid, Pyramid Research, 2006 (http://www.pyramidresearch.com).

[66] Financial Times, AT&T turns to femtocells to offload surging smartphone traffic, June 2012 (http://blogs.ft.com/fttechhub/2010/03/att-turn-to-femtocells-to-offload-surging-smartphone-traffic).

[67] Motorola, Wide Area Mesh Networks, June 2012 (http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Wireless+Broadband+Networks/Mesh+Networks).

[68] UTMS Forum, Spectrum for future development of IMT-2000 and IMT-Advanced, Jan. 2012 (http://www.umts-forum.org/content/view/3846/315/).

[69] 3GPP, Policy and charging control architecture, TS 23.203 (http://www.3gpp.org/ftp/Specs/html-info/23203.htm).

[70] 3GPP, Access Network Discovery and Selection Function (ANDSF) Management Object (MO), TS 24.312 (http://www.3gpp.org/ftp/Specs/html-info/24312.htm).

[71] P. Seite, G. Feige, T. Melia and J.C. Zuniga, Connection Manager Requirements, Work in Progress, Oct. 2010 (http://www.ietf.org/id/draft-seite-mif-connection-manager-02.txt).

[72] OpenFlow, Switch Specification, V1.0.0, Dec. 2009 (http://www.openflowswitch.org/wp/documents).

[73] C. Blachier and M. Jadoul, Increasing Competitiveness through Ongoing Operational Excellence, Alcatel-Lucent, 2010

[74] EU Commission: Cloud Computing, Digital Europe's perspective – version 5, Final Draft

[75] Graeme A. Guthrie (Victoria University of Wellington), John P. Small (University of Auckland) Pricing Access: Forward-looking versus Backward looking cost rules http://profile.nus.edu.sg/fass/ecsjkdw/forward%20looking%20costs%20revised.pdf

[76] William P. Rogerson (Northwestern University) October 3, 2005: ON THE RELATIONSHIP BETWEEN HISTORIC COST, FORWARD-LOOKING COST AND LONG RUN MARGINAL COST, http://www.chicagobooth.edu/research/workshops/archives/accounting/marginalcost35.pdf

[77] Security in Telecommunications and Information Technology, 2003, ITU-T, http://www.itu.int/itudoc/itu-t/85097.pdf

[78] ITU-T Recommendation X.805 "Security architecture for systems providing end-to-end communications, http://www.itu.int/rec/T-REC-X.805-200310-I/en

[79] European Council Resolution on a Strategy for a Secure Information Society in Europe, 22 March 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:068:0001:0004:EN:PDF http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:068:0001:0004:EN:PDF/

[80] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995, http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[81] Eurescom mess@ge, The magazine for telecom insiders, 1/2012

[82] Paul T Jaeger: Cloud Computing and Information Policy: Computing in a Policy Cloud? Forthcoming in the Journal of Information Technology and Politics, 5(3), http://www.umiacs.umd.edu/~jimmylin/publications/Jaeger_etal_2008.pdf

[83] Computer World UK, Blog: Cloud computing and EU data protection law, 28 September 2011, http://blogs.computerworlduk.com/cloud-vision/2011/09/cloud-computing-and-eu-data-protection-law/index.htm

[84] University of London, Centre for Commercial Law Studies, News: Data protection law creates cloud of uncertainty for cloud computing, 21 November 2011, Cloud of Unknowing papers, http://www.ccls.qmul.ac.uk/news/2011/59982.html

[85] Industry Recommendations to Vice President Neelie Kroes on the Orientation of a European Cloud Computing Strategy, November 2011, http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendations-ccstrategy-nov2011.pdf

[86] Cloud Computing Legal Issues: When does Directive 95/46/EC Apply? http://common-assurance.com/blog/files/2cf981cc32595f347ba14371ea17643f-11.html

[87] Joep Ruiter, Martijn Warnier: Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice. http://www.iids.org/aigaion/indexempty.php?page=actionattachment&action=open&pub_id=316&location=spcc10.pdf-9869f6a896824ba29d27ad19e6da5585.pdf

[88] Volker Fusenig, Ayush Sharma, Paul Perie, Houssem Medhioub: Initial security framework for virtualised resources. SAIL Milestone Document M.D.8

[89] ITU Focus Group on Cloud Computing. http://www.itu.int/en/ITUT/focusgroups/cloud/Pages/default.aspx

[90] Carmine Rizzo for Gerald McQuaid (Vodafone Group) and Carmine Rizzo (ETSI). ETSI Security Workshop 2011. http://docbox.etsi.org/workshop/2011/201109_CLOUD/03_SERVICESandAPPLICATIONS/ETSI_TCLI_RIZZO.pdf

[91] Privacilla.org. http://www.privacilla.org/business/howtoregulate.html

[92] Industry joint paper on the review of the EU Legal Framework for data protection. http://www.orange.com/en_EN/group/european_policy/privacy/att00022388/1010_Industry_Joint_Paper_on_Data_Protection.pdf

[93] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing (Adopted July 1st 2012)

[94] P.Mell and T. Grance, “The NIST Definition of Cloud Computing (Draft)”, National Institute of Standards and Technology, January 2011.

[95] Akamai, “Can Cloud and High Performance Co-Exist?”, Whitepaper, May 2011.

[96] Cisco, IP Next-Generation Network [Online]. Available: http://www.cisco.com/en/US/netsol/ns537/networking_solutions_solution_category.html [Mar. 8, 2012].

[97] Cisco, “The Cisco Powered Network Cloud: An Exciting Managed Services Opportunity”, 2009.

[98] Cisco, CloudVerse [Online]. Available: www.cisco.com [Mar. 8, 2012].

[99] Institut Télécom, pyOCNI [Online]. Available: http://occi-wg.org/2012/02/20/occi-pyocni/ [Mar. 8, 2012].

[100] Metro Ethernet Forum, “Carrier Ethernet for Delivery of Private Cloud Services”, February 2012.

[101] AWS VPC [Online]: http://aws.amazon.com/vpc/ [Set. 4, 2012]

[102] AWS Direct Connect [Online]: http://aws.amazon.com/directconnect/ [Set. 4, 2012]

[103] APN Partners supporting AWS Direct Connect [Online]: http://aws.amazon.com/directconnect/partners/ [Set. 4, 2012]

[104] Introducing AT&T's "Virtual Private Cloud" [Online]: http://www.att.com/gen/press-room?pid=22362&cdvn=news&newsarticleid=33844 [Set. 4, 2012]

[105] Icek Aizen [Online]: http://people.umass.edu/aizen/ [Set. 4, 2012]

[106] Rogers, Everett M. *Diffusion of Innovations* Free Press New York 5ft Edition 2003.

[107] Paul Murray et al. *Cloud Networking Architecture Description*. Deliverable FP7-ICT-2009-5-257448-SAIL/D.D.1, SAIL project, July 2011. Available online from http://www.sailproject.eu.

[108] Zhang N., Levä T., Hämmäinen H. Two-Sidedness of Internet Content Delivery. Proc. of the 10th Conference of Telecommunication, Media and Internet Techno-Economics (CTTE), May 16-18, 2011, Berlin, Germany.

[109] Liang, J.; Kumar, R.; Xi, Y.; Ross, K.W.; , "Pollution in P2P file sharing systems," INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE , vol.2, no., pp. 1174- 1185 vol. 2, 13-17 March 2005. doi: 10.1109/INFCOM.2005.1498344

[110] Audun Jøsang, Roslan Ismail, Colin Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems, Volume 43, Issue 2, March 2007, Pages 618-644, ISSN 0167-9236, 10.1016/j.dss.2005.05.019.

ANNEX 1: Key concepts of Security and Privacy

According to [77], the concept of **privacy** is a fundamental motivation for security. Privacy is commonly understood as the right of individuals to control what information related to them may be collected and stored and by whom and to whom that information may be disclosed. By extension, privacy is also associated with certain technical means (e.g., cryptography) to ensure that this information is not disclosed to any other than the intended parties, so that only the explicitly authorised parties can interpret the content exchanged among them.

Most commonly, privacy and **confidentiality** are used as the same term, but in [78] the privacy and data confidentiality are differentiated, the former relating to the protection of the association of the identity of users and the activities performed by them (such as online purchase habits), and the latter relating to the protection against unauthorised access to data content. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.

Information security is related with the requirement that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information on this (e.g., in accordance with EC Directive 95/46/EC), inter alia about the purposes of the processing and the subscriber is offered the right to refuse such processing by the data controller.

Network security is related with the requirement to protect sensitive data from unauthorised access or accidental disclosure. The network security problem is typically divided into integrity and confidentiality. The integrity problem affects public information (e.g., stock information) and can be addressed by signatures and checksums *that need to be verified*, while confidentiality requires encryption. The more problematic aspect of trust in a network is related to authentication, access control and authorisation, when the first question to be checked is whether you are connected to the entity you intended, with no malicious middlemen.

The **communication security** dimension is a new dimension defined in [78] that ensures that information flows only between authorised end points. This dimension deals with measures to control network traffic flows to prevent traffic diversion and interception.

Data integrity is the property that data have not been altered in a unauthorised manner. By extension, data integrity also ensures that information is protected against unauthorised modification, deletion, creation, and replication and provides an indication of these unauthorised activities.

The **availability security** dimension ensures that there is no denial of authorised access to network elements, stored information, information flows, services and applications due to network interruption. Network restoration and disaster recovery solutions are included in this category.

ANNEX 2: Questionnaire used in the Business Analysis of CloNe

CloNe Questionnaire
Lisbon Workshop
01/2012

SAIL - Scalable and Adaptive Internet Solutions
CloNe - Cloud Networking

The following questions refer to the usage of CloNe services for corporative/work use, not personal /individual use. Some of the questions are somewhat abstract, therefore we recommend you to consider them in a wide sense.

	Absolutely Disagree	Partially Disagree	Neither Agree nor Disagree	Partially Agree	Completely Agree
	1	2	3	4	5
Using Corporative CloNe services will provide my organization more reliable Cloud services.	☐	☐	☐	☐	☐
Using Corporative CloNe services would be compatible with all aspects of my organization workflow.	☐	☐	☐	☐	☐
My interaction with Corporative CloNe services will be clear and understandable.	☐	☐	☐	☐	☐
Overall, I believe Corporative CloNe services would be easy to use.	☐	☐	☐	☐	☐
I intend to use Corporative CloNe services in the future when they become available.	☐	☐	☐	☐	☐
Using Corporative CloNe services will provide me more convenient Corporative Cloud services.	☐	☐	☐	☐	☐
Using Corporative Clone services would fit well with the way I like to work.	☐	☐	☐	☐	☐
Compared to the effort I need to put in, I expect the use of Corporative CloNe services to be beneficial to me.	☐	☐	☐	☐	☐
Using Corporative CloNe services will not pose my organization additional security threats.	☐	☐	☐	☐	☐
Using Corporative CloNe services in my mobile phone would be an advantage.	☐	☐	☐	☐	☐
Using Corporative CloNe services would fit well into my work style habits.	☐	☐	☐	☐	☐
Compared to the time I need to spend, I expect the use of Corporative CloNe services to be worthwhile to me.	☐	☐	☐	☐	☐
Overall, I expect the use of Corporative CloNe services to deliver me good value for money.	☐	☐	☐	☐	☐
Using Corporative CloNe services in a pay-as-you-go model would be an advantage.	☐	☐	☐	☐	☐
I will recommend to others Corporative CloNe services as soon as they become available.	☐	☐	☐	☐	☐
If Corporative CloNe services were offered to you today, you would adopt them immediately.	☐	☐	☐	☐	☐

Page 1 de 3

SAIL - Scalable and Adaptive Internet Solutions
CloNe - Cloud Networking

The following questions refer to the usage of CloNe services for personal/individual use, not corporative/work use. Some of the questions are somewhat abstract, therefore we recommend you to consider them in a wide sense.

	Absolutely Disagree	Partially Disagree	Neither Agree nor Disagree	Partially Agree	Completely Agree
	1	2	3	4	5
Using CloNe services for personal use will provide me more reliable Cloud services.	☐	☐	☐	☐	☐
Using CloNe services for personal use would be compatible with all aspects of my usage habits.	☐	☐	☐	☐	☐
My interaction with CloNe services for personal use will be clear and understandable.	☐	☐	☐	☐	☐
Overall, I believe CloNe services for personal use would be easy to use.	☐	☐	☐	☐	☐
I intend to use CloNe services for personal use in the future when they become available.	☐	☐	☐	☐	☐
Using CloNe services for personal use will provide me more convenient Cloud services.	☐	☐	☐	☐	☐
Using Clone services for personal use would fit well with the way I like to work.	☐	☐	☐	☐	☐
Compared to the effort I need to put in, I expect the use of CloNe services for personal use to be beneficial to me.	☐	☐	☐	☐	☐
Using CloNe services for personal use will not pose me additional security threats.	☐	☐	☐	☐	☐
Using CloNe services for personal use in my mobile phone would be an advantage.	☐	☐	☐	☐	☐
Using CloNe services for personal use would fit well into my work style habits.	☐	☐	☐	☐	☐
Compared to the time I need to spend, I expect the use of CloNe services for personal use to be worthwhile to me.	☐	☐	☐	☐	☐
Overall, I expect the use of CloNe services for personal use to deliver me good value for money.	☐	☐	☐	☐	☐
Using CloNe services for personal use in a pay-as-you-go model would be an advantage.	☐	☐	☐	☐	☐
I will recommend to others CloNe services for personal use as soon as they become available.	☐	☐	☐	☐	☐
If CloNe services for personal use were offered to me today, you would adopt them immediately.	☐	☐	☐	☐	☐

Page 2 de 3

SAIL - Scalable and Adaptive Internet Solutions
CloNe - Cloud Networking

The following questions refer to the usage of CloNe Services in a wide sense.

Considering what I know and saw about CloNe Services:

	Very Hardly				With Much Certainty
	1	2	3	4	5
I would for sure adopt CloNe services for personal/individual use.	☐	☐	☐	☐	☐

Considering what I know and saw about CloNe Services:

	Very Hardly				With Much Certainty
	1	2	3	4	5
I would for sure adopt CloNe services for corporative/work use.	☐	☐	☐	☐	☐

Please list some of your perceived usefulness of CloNe Services:

Please list some of your perceived disadvantages of CloNe Services:

Demographics:

Gender	
Male	☐
Female	☐

Age		Company Business Area	
Literacy		Function within Company	

Country of Residence	

Page 3 de 3

ANNEX 3: Specific Security and Privacy issues in the CloNe concept

The CloNe architecture introduces similar Security and Privacy issues as listed in the previous section. The specific issues from this architecture and which are relevant from the regulatory perspective are listed in the following

- **Information security** relies on the classical three pillars, confidentiality (information should not be disclosed to unauthorised third parties), integrity (information should not be transformed without evidence of the transformation), and availability (information should not be withheld from rightful access). The cloud scope adds a significant dimension in the mixing of code and data. Cloud users will need to ship code for execution on their data to cloud providers. Cloud providers will in turn ship code to users to easily manipulate the data. This mixture of code and data is one of the major causes of malware infection, as it becomes extremely challenging to distinguish code from data and qualify the acceptability of both.
- **Trust in an adversarial environment** Cloud environments are by their very nature adversarial. Cloud providers balance the needs of their multiple users, and attempt to monetise by-products of their activity. Cloud users strive to obtain the cheapest possible services, while requesting services of high quality and respecting their privacy. Attackers, who have become very skilled at operating huge botnets (which can be seen as the first large scale clouds), will attempt to either access the information available in clouds or avail themselves to this processing power free of charge.
- **Confidentiality of information and processes** Encrypting data can be used to maintain integrity and confidentiality of stored or transmitted data. However, processing encrypted data is still under research (Homomorphic Cryptography and cannot yet be applied in practice. As implementing technical solutions that ensure integrity and confidentiality is not possible we need to rely on audit traces to assert “after the fact” usage control demonstrating that data and code have not been misused by service providers and cloud users. Furthermore, attacks on the confidentiality of data can also have impact on the privacy of a user. In this case not only the data itself reveals information on a user also the usage itself reveals personal information.
- **Secure key distribution** The key distribution in cloud networking is also a challenge as the CloNe infrastructure changes dynamically. When indicated a new trust model needs to be developed in order to build up a dynamic key distribution infrastructure.
- **Policy models and policy enforcement** The currently available security policy models are not sufficiently flexible. For example, the OrBAC model introduces organisations and contexts in addition to the classic notion of roles. Both concepts are extremely useful to define security policies that span organisational boundaries. However, the combination of organisations and contexts with negotiation remains largely an unsolved problem. The complexity of these policies has not been resolved either. Furthermore, Security policies need to be enforced. However, there is no such clear picture for the cloud computing world. First, it is not known if the policy enforcement technology can be ported into the cloud world and how. Second, it is unclear if cloud computing enabling technologies, such as virtualisation, will bring new policy enforcement points.
- **Provider policy change** During the lifetime of a CloNe infrastructure there might be changes in the security policies by the provider. In this case the provider has to implement and enforce the new security policy. From the customer’s perspective these new security policies might violate its own policies.

1. **Virtualisation management** Virtualisation management entails management of virtual resources which are implemented by an infrastructure service provider and are

provisioned to a cloud user. The cloud networking infrastructure requires an access control policy model, which enables control and delegation of access to virtual resources.

- **Secure management of cloud networking** For the management of CloNe, access to the physical infrastructure and to the network properties is needed. This access should be implemented as a single interface, where a user can specify several parameters on-demand. By the combined access to the physical virtualisation infrastructure and the network infrastructure new attacks arise. One challenge is to define rules for accessing the management interface and how to implement these rules.

2. **Communication security and isolation of virtual machines** In the CloNe infrastructure, the underlying physical infrastructure is shared by different tenants. Besides the separation of communication and the separation done by a hypervisor, the CloNe management has to take care of complying to SLAs of all customers. Furthermore, the data that is sent to, from, or inside the cloud networking infrastructure should be secured from information leakage.
   - **Secure virtual networking** In addition to cloud computing, virtual networking introduces new security challenges by enabling communication between different virtual components. From a virtual network user's perspective the network might be private while in reality the communication itself occurs via a public infrastructure. Therefore, mechanisms to secure this communication (e.g., by encryption) have to be established.
   - **Hypervisor VM separation** Virtual machines in different flash network slices should be isolated from each other when sharing the same physical host. The level of separation in the hypervisor must be sufficiently strong so that the presence of one compromised machine does not affect other machines (potentially from other customers) in the same physical host.
   - **SLA enforcement** The resources that are committed to one cloud network should be protected from other cloud networks. A SLA for cloud networking will include the guaranteed computing, storage and networking resources of a customer. One challenge is the management of virtual and physical resources so that the SLAs of all customers can be fulfilled. Another challenge is to verify as a customer that your SLAs are fulfilled.
3. **Misuse protection** Mechanisms for detecting misuse of the CloNe infrastructure need to be devised and integrated into the overall security framework.
   - **Misuse of CloNe capabilities** The ability of cloud computing and cloud networking to allocate computational resources on demand can also be misused, e.g., for DoS attacks, spamming, and providing illegal content. Attacks that use cloud infrastructures are already known today. One example is Zeus ``in-the-cloud'' where the command and control of a botnet was located at the Amazon EC2.
4. **Protection against denial of service** The cloud network integrated with computing and storage can suffer denial of service (DoS) attacks from external and internal sources. Such attacks prevent legitimate users from accessing services they should be able to. The DoS attacks may occur in different parts of the system. The first part of the system that is susceptible to attacks is the virtual machines where the applications are hosted. Another part of the system that may be targeted is the administrative or management interface that allows the cloud system to scale up/down the provisioning of resources.