SPARC

Deliverable 2.2

Revised definition of use cases and carrier requirements

Editor:	*Fritz-Joachim Westphal, Mario Kind, Deutsche Telekom AG*
Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	M24
Actual delivery date:	M27
Version:	1.0
Total number of pages:	80
Keywords:	Use cases, carrier requirements, techno-economic analysis, business developments

Abstract

This document reviews the use case access/aggregation and the related defined use cases on Seamless MPLS or SDN approaches to MPLS transport, multi-service/-provider environments (service creation), mobile backhaul, Software Defined Networking application in context of IEEE 802.11 compliant devices and dynamic control composition. It compromises the feedback from the work packages 3, 4 and 5 about development of concepts, prototypical implementation and validations. In addition it contains a review of the selected carrier requirements and groups of requirements accordingly.

Moreover the deliverable provides a comprehensive overview of the results of task 2.3, a techno-economic evaluation of a mobile backhaul network scenario with detailed analysis of capital as well as operational expenditures. In addition uncertainties based on the estimated assumptions are covered by a sensitivity analysis.

Beside techno-economic analysis, the evaluation of the business environment was continued and scenarios about future directions developed, verified and evaluated.

Disclaimer

This document contains material, which is the copyright of certain SPARC consortium parties, and may not be reproduced or copied without permission.

In case of Public (PU):
All SPARC consortium parties have agreed to full publication of this document.

In case of Restricted to Programme (PP):
All SPARC consortium parties have agreed to make this document available on request to other framework programme participants.

In case of Restricted to Group (RE):
All SPARC consortium parties have agreed to full publication of this document. However this document is written for being used by <organisation / other project / company etc.> as <a contribution to standardisation / material for consideration in product development etc.>.

In case of Consortium confidential (CO):
The information contained in this document is the proprietary confidential information of the SPARC consortium and may not be disclosed except in accordance with the consortium agreement.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the SPARC consortium as a whole, nor a certain party of the SPARC consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using this information.

Imprint

[Project title]	*Split Architecture*
[short title]	*SPARC*
[Number and title of work package]	*WP2 – Use cases / Business scenarios*
[Document title]	*D2.2 Revised definition of use cases and carrier requirements*
[Editor]	*Mario Kind, Deutsche Telekom AG*
[Work package leader]	*Fritz-Joachim Westphal, Deutsche Telekom AG*
[Task leader]	*Fritz-Joachim Westphal, Deutsche Telekom AG*

Executive summary

Besides analysing new business opportunities of a Split Architecture, the objective of work package 2 is the description of use-cases and the definition of carrier-grade requirements, derived from these use cases. Both will be provided as input to the development of the technical aspects of a SplitArchitecture in work package 3. The second and final contribution to fulfil the objective is covered in this deliverable.

The deliverable gives an overview of the work on the use case access/aggregation, which was selected from three use-cases covering all important aspects of a carrier environment as defined for next-generation-networks by ITU-T. The use case was subdivided into six sub-use cases representing service areas as well:

- General architecture

- Seamless MPLS or SDN approaches to MPLS transport

- Multi-service and multi-provider environments (service creation)

- Mobile backhaul

- Software Defined Networking application in context of IEEE 802.11 compliant devices

- Dynamic control composition

Each use case was covered by work streams, starting with a set of requirements (WP2), followed by the development of concepts (WP3) and prototypical implementations (WP4) and finally testing of functional and performance aspects (WP5). Overall it is guaranteed that each use case is sufficiently covered by the developments of SPARC.

The work was based on 67 requirements detailed in D2.1. They were prioritized with respect to overall importance, fulfillment in existing architecture concepts and/or existing implementations and their relevance for one or more use cases. In the SPARC context four requirement groups were identified. During the course of the project, these groups required further refinement. In total, twelve requirement groups have been identified:

(a) Recursive control plane

(b) Network management

(c) Openness and extensibility

(d) Virtualization and isolation

(e) OAM (technology-specific MPLS OAM / technology-agnostic Flow OAM)

(f) Network resiliency

(g) Control channel bootstrapping and topology discovery

(h) Service creation

(i) Energy-efficient networking

(j) Quality of service

(k) Multilayer aspects

(l) Scalability

These twelve groups of requirements cover the majority of high priority requirements identified in D2.1.

The mobile backhaul use-case was further analysed with a first attempt of a techno-economic cost study. Given the immaturity of SDN in the mobile backhaul context several assumptions have to be made, often based on expert opinions or results from previous preliminary studies. To cope with the uncertainty related to the gathered input a sensitivity analysis was performed to examine the effects of modifications of the critical parameters on the overall results. Two different scenarios were defined, one scenario covering state of the art design principles ("classical scenario") and the other scenario to reflect advanced SDN developments ("SDN scenario").

For the considered parameters, the SDN scenario provides a capital expenditure advantage at 12%. The majority of capital expenditures savings is based on modifications in the pre-aggregation stages which is explained by the high number of sites at this partition of the network. A second contribution is based on the lower cost of first time installation. The savings in the pre-aggregation sites amount to up to 13% which is a bit higher than the total reduction of 12%. Introducing SDN however also involves introducing of centralized controllers to the network architecture which accounts for an extra 3% of the total cost.

Within the OpenFlow community the focus is often on the promised capital expenditures reductions. Little attention is however given towards operational expenditures. The analysis shows an 11% reduction in OpEx in the SDN based scenario. The main benefits can be located in the network operations center where the cost of operational processes such as service provisioning and service management is reduced by 3% and 6% respectively. The environmental cost (energy consumption) has not been increased nor reduced. It could be however argued that the energy consumption of the router is reduced because part of the control plane functionality is now taken over by the SDN controller. This is open for further research.

The performed sensitivity analysis introduces an overview on the level of uncertainty on the following parameters:

- Cost of a SDN controller has a rather low impact on the capital expenditures

- Number of OpenFlow enabled network elements one SDN controller is able to steer has a rather low impact as well on the overall cost basis

- Effect of wholesale price discounts by vendor on SDN advantage has a contradictory effect

  o The benefits of SDN on capital expenditures are reduced when higher discounts are applied

  o The benefits of software defined networking on operational expenditures increase when higher discounts are applied

  o The overall delta between the scenarios varies from 12% without discount to 9% for capital expenditures and from 10.7% to 12.3% for operational expenditures with 50% discount

- Effect of cost reduction in cost of operating system of router increases the delta between the scenarios by 50% for capital expenditures

- The highest effect of change has the effect of extra reductions in hardware cost because of specialization and interoperability of devices with potential reduction of price points for the SDN scenario by 50% and a delta of up to 47% (CapEx) and 25% (OpEx) respectively.

Again one has to mention that there exist a number of uncertainties in the techno-economic analysis and this has to be taken into account when viewing the results.

Up to date, the impact of SDN on the existing telecommunication business environment is unclear. Therefore experts from the project tried to outline today's market roles, their functions and possible future market roles. Based on this analysis, a questionnaire was developed, trying to answer the key questions: Which markets will be strongly affected by OpenFlow and what will change and which impact will OpenFlow have on different market roles? Finally, these expert views and the OpenFlow market description were substantiated with an evaluation of key financial data of ONF and ATCA member organizations regarding head office as well as revenues and employees in 2011.

The analysis came to the conclusion that in the year 2020, OpenFlow is expected to be widely supported in the mass market. This will strongly affect several markets, especially carrier-grade fixed and mobile telecommunication networks, data centres as well as enterprise networks. Additionally, OpenFlow is expected to offer new market potentials for nearly every involved player. Broadcom Corporation, Cisco Systems, Juniper Networks and VMware are spotted as the potential dominant players in the market. In addition wide OpenFlow support might imply some general changes. First, the software market will be split up due to emerging network applications. Secondly, hardware vendor and system integrator will lose their dominance and, thirdly, interfaces and software solutions will become increasingly standardized. The introduction of OpenFlow is likely to make business model changes necessary for hardware vendors and system integrators. New market opportunities open up for software vendors, especially network application vendors will benefit from OpenFlow. Vendors of network management solutions, on the other hand, will be exposed to increased competition. Network operators can expect simplified operations, but possibly at the cost of major changes to the traditional network design. The analysis of the participation of companies in the three different standardisation organisations ONF, ATCA and OpenStack shows only a loose connection. Overall only six from more than 150 organisations are participating in all three organisations and this imposes new questions on how the market will evolve and how SDN or more precisely OpenFlow will be supported in the telecommunication market.

List of authors

Organisation/Company	Author
DTAG	Fritz-Joachim Westphal, Mario Kind, Steffen Topp
EICT	Maximilian Schlesinger
IBBT	Bram Naudts

Table of Contents

List of figures and list of tables

Abbreviations

ANDSF	Access Network Discovery Selection Function	IpoE	Internet Protocol over Ethernet
API	Application Programming Interface	IS-IS	Intermediate System – Intermediate System; Link State Routing Protocol from OSI (IGP)
ARP	Address Resolution Protocol		
ARP	Allocation and Retention Priority	ISO	International Organization for Standardization
ARPU	Average revenue per user	ITIL	IT Infrastructure Library
ATCA	Advanced Telecommunications Computing Architecture	ITU	International Telecommunication Union
		LDP	Label Distribution Protocol
ATM	Asynchronous Transfer Mode	LTE	Long Term Evolution
BFD	Bidirectional Forwarding Detection	mLDP	Multicast Label Distribution Protocol
BRAS	Broadband Remote Access Server / Service	MME	Mobility Management Entity
BSC	Base Station Controller	MMF	Multi Mode Fiber
CapEx	Capital Expenditures	MPLS	Multi-Protocol Label Switching
CRUD	Create, Read, Update and Delete	NMF	Network Management Function
DHCP	Dynamic Host Configuration Protocol	NMS	Network Management System
DSCP	Diff Serve Code Point	NNI	Network-to-Network Interface
DSL	Digital Subscriber Line	NOX	
DSLAM	Digital Subscriber Line Access Multiplexer (network side of ADSL line)	OAM	"Operation, Administration and Maintenance" or "Operations and Maintenance"
EGP	Exterior Gateway Protocol	OF	OpenFlow
ePDG	Evolved Packet Data Network Gateway	ONF	Open Networking Foundation
EPS	Evolved Packet System	OpEex	Operational Expenditures
ERPS	Ethernet Ring Protection Switching	OS	Operating System
FMC	Fixed Mobile Convergence	OSI	Open Systems Interconnection
ForCES	Forwarding and Control Element Separation	OSPF	Open Shortest Path First; Link State Routing Protocol from IETF (IGP)
GbE	Gigabit Ethernet		
GGSN	Gateway GPRS Support Node	PBB	Provider Backbone Bridge
GMPLS	Generalized Multi-Protocol Label Switching	PCE	Path Computation Element
GRE	Generic Route Encapsulation	PCEF	Policy and charging enforcement function
GTP	GPRS Tunneling Protocol	PDG	Packet Data Gateway
HLR	Home Location Register	PMIP	Proxy Mobile IP
HSDPA	High Speed Downlink Packet Access	PPP	Point-to-Point Protocol
HSPA	High-Speed Packet Access	PPPoE	PPP over Ethernet
HSS	Home Subscriber Server	PSC	Packet Service Card
ICT	Information and Communication Technology	QCI	QoS Class Identifier
IEEE	Institute of Electrical and Electronics Engineers	QoS	Quality of Service; general for differentiated quality of services or absolute quality of services.
IETF	Internet Engineering Task Force		
IGP	Interior Gateway Protocol	RFC	Request for Comment (in IETF)
IMS	IP Multimedia Subsystem	RNC	Radio Network Controller
IP	Internet Protocol	SDH	Synchronous Digital Hierarchy
		SDN	Software Defined Networking

SFP	Small Form Factor Pluggable	TE	Traffic Engineering
SGSN	Serving GPRS Support Node	TEID	Tunnel Endpoint Identifier
SGW	Serving Gateway	TFT	Traffic Flow template
SIPTO	Selective IP Traffic Offload	TLS	Transport Layer Security
SLA	Service Level Agreement	UDP	User Datagram Protocol
SMF	Single Mode Fiber	UMTS	Universal Mobile telecommunication Service
SONET	Synchronous Optical Network	VPLS	Virtual Private LAN Service
SSID	Service Set Identifier	VPN	Virtual Private Network
SSL	Secure Sockets Layer	VRF	Virtual Routing Function
TCP	Transmission Control Protocol	W-CDMA	Wide Code Division Multiple Access
TDM	Time Division Multiplexing	XPP	eXtensible Port Parameter

1   Introduction

1.1   Project context

The SPARC project ("Split Architecture for carrier-grade networks") is aimed at implementing a new split in the architecture of Internet components. In order to better support network design and operation in large-scale networks for millions of customers, with high automation and high reliability, the project will investigate splitting the traditionally monolithic IP router architecture into separable forwarding and control elements. The project will implement a prototype of this architecture based on the OpenFlow concept and demonstrate the functionality at selected international events with high industry awareness, e.g., the MPLS Congress.

The project, if successful, will open the field for new business opportunities by lowering the entry barriers present in current components. It will build on OpenFlow and GMPLS technology as starting points, investigating if and how the combination of the two can be extended, and study how to integrate IP capabilities into operator networks emerging from the data center with simpler and standardized technologies.

1.2   Relation to other work packages
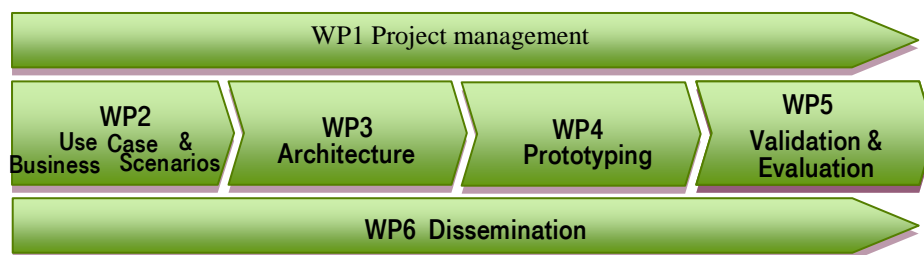
Figure 1: Relation of SPARC work packages

In the "workflow" of the work packages, WP3 is embedded between WP2 (Use Cases / Business Scenarios) and WP4 (Prototyping). WP3 will define the SplitArchitecture taking use cases and requirements of WP2 into account and will analyse technical issues with the SplitArchitecture. Moreover, this architecture will be evaluated against certain architectural trade-offs. WP4 will implement a selected subset of the resulting architecture, and feasibility will be validated in WP5. WP6 disseminates the result at international conferences and publications.

1.3   Scope of the deliverable

SplitArchitecture defines a paradigm shift in network architectures, offering more freedom to deploy and operate carrier-grade networks. However, carrier-grade networks are characterized by some specific challenges including provisioning of a large coverage area, providing broadband access in urban and rural areas, QoS-enhanced transport of (triple-play) services towards (residential) customers. D2.2 revisits the analysis of access/aggregation use case and the derived requirement group defined in D2.1. In addition, the techno-economic analysis of SDN applied on a mobile backhaul is presented. Finally, the results of the value chain analysis with an overview of involved players are shown.

2　　　　Use cases and requirements

2.1　　　Review use case access/aggregation

2.1.1　　　General aspects of the use case access/aggregation

This use case is targeting a certain network domain of carriers, the access/aggregation domain. Currently, the transformation to Ethernet/IP technologies in this domain is still on-going and a plethora of possibilities for the technical implementation exist (see D2.1 section 2.2.1 and D3.2 section 4.1). Apart from this fact, the requirements are many, depending on the services to be supported (in SPARC covered as use cases on multi-service in general, mobile backhaul, MPLS transport (Pseudowire) and IEEE802.11). In addition, it is essential that the network supports different business models (in SPARC covered as use case on multi-provider). Another problem space is the support for legacy technologies and the transformation of existing capabilities to more future proof solutions (in SPARC covered as use case on dynamic control composition, dealing with the question on how the network can be more flexible).

As a starting point there are two different aspects. The first aspect is the acknowledgement of the generic idea of SplitArchitecture as baseline for the project which is not limited to the access/aggregation domain. This leads to a set of requirements for the modification of the generic architecture of control plane, data path and the SplitArchitecture itself. In the following paragraphs, the results for the use case on access/aggregation network domain are detailed. The report on dynamic control composition is covered in a separate use case report (see section 2.1.6). The second aspect is a description of the state of the networks and their network design, the requirements resulting from the use cases and the functional analysis. This results in a list of requirements dealing with different functions and areas like, authentication, authorization and auto configuration, OAM, and network management, security and control. During the analysis, important aspects have been added with Quality of Service (QoS), resiliency, energy-efficient networking, control channel bootstrapping and topology discovery, network virtualisation, multilayer and scalability.

The development of the generic architecture started with a gap analysis of the existing OpenFlow protocol (which was OpenFlow 1.0 at the time of the start of the project – see also D3.1 section 4.3). Important results of the analysis was the missing support for IP network domain interaction (results of related developments are covered in section 2.1.2), support for a number of protocols required from a carrier perspective (e.g. Pseudowire), standardisation of integration of processing capabilities and scalability. That also includes balancing the interaction between the OpenFlow data path elements and controller entities.

In a second step, the different existing SDN approaches have been reviewed and the SplitArchitecture defined by SPARC was developed (see Figure 2). A central aspect is the hierarchical or recursive controller concept (see section 2.1.6 and D3.3 section 4.1.5 for further details) providing a flexible way for abstraction in the control plane. In OpenFlow context the result of the control plane is the generation of appropriate match-action-rule sets. In addition, network management is integrated as an overarching function, managing the control plane and the data path elements (see D3.3 section 4.2).
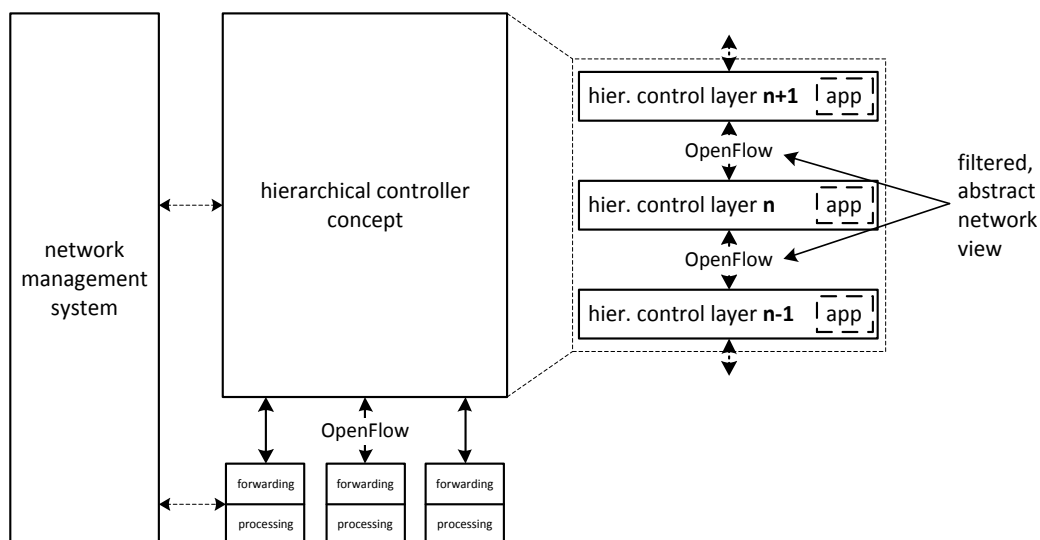
Figure 2: SplitArchitecture defined by SPARC

Support for network management is one of the key requirements in carrier networks. With SDN (based on OpenFlow) and its central control entities, the boundaries between network management and control blurs and a new approach was developed. This approach splits the function between integration into controller and data path element (as Network Management Function (NMF)) taking the current OF-Config specification of the ONF and a separate element (Network Management System (NMS)) into account. For verification 27 element, network and service management functions have been analysed to understand if they should be integrated in either the integrated entity (i.e. the controller) or in a separate element (i.e. the NMS). A final and general conclusion is not possible and really depends on the particular use case. However, one conclusion is that time critical aspects should be integrated into the controller or data path element and functions that accept loose reaction times may remain in the classical NMS. Finally, an integration proposal with the hierarchical, recursive controller architecture and network management was developed.

The third step is the application of the general concept on the use case access/aggregation network. The first question deals with the level of integration of OpenFlow in the network and which devices are controlled by means of the OpenFlow protocol. Different options have been developed (see D3.3 section 6.1) applied on service creation, but a final decision is left open with respect to the real-network deployments (see D3.3 section 6.2). The second question deals with the scalability of such access/aggregation domains (see D3.3 section 6.4). With respect to scalability a static and a dynamic regime have been investigated. The static regime deals with the setup of the network, including establishment of links, etc. Depending on the evolution of the network, such a domain requires handling between 1 and 10 million flow entries if all devices and links are to be covered. Therefore different optimisations have been developed, which reduce the requirements about an order of magnitude to a level that could be provided by already existing controllers and switches. The dynamic part deals with unexpected behaviour like link failures, which would require a reconfiguration and installation of flow entries in a relative small time period. Again, there are some scalability concerns, but they have been relaxed by the development of alternative solutions.

Moreover, the aspect of messaging performance between switch and controller was investigated in order to analyse the need for Quality of Service in the control network (see D5.2 section 7). It was concluded that the existing OpenFlow control channel mechanism using TCP/SSL as a transport layer already provide sufficient congestion control. In addition, it was shown that a separated transport stream implemented with UDP could reduce the configuration delay in a network heavily loaded by "packet-in" traffic.

The general aspects of the SplitArchitecture and the access/aggregation use case have been analysed, extended, developed and implemented in order to cover carrier-grade support. But details of network functions had to be investigated in detail as well.

Already mentioned is the fact that the different requirements were grouped into four groups (see D2.1 section 3) and groups and aspects were added to represent the required network functions (more details are presented in section 2.2):

- Modification of the generic architecture of control plane, data path and SplitArchitecture (covered in section 2.1.6 and D3.3 section 4.1.5)

- Authentication, authorization and auto configuration (covered in use case on Service Creation (see section 2.1.3) , Pseudowire (see section 2.1.2) and in D3.3 section 5.6 and 6.2)

- OAM (see details in the following paragraphs)

- Network management, security and control (for network management see previous paragraphs) including Quality of Service (QoS), Energy-efficient networking, control channel bootstrapping and topology discovery (also see details in the following paragraphs)

- Network virtualisation (covered in section 2.1.3 on multi-service/-provider environments)

- Resiliency (see details in the following paragraphs)

- Multilayer (see details in the following paragraphs)

- Scalability (see details in previous paragraphs)

OAM is linked with the ability to discover loss of connectivity or violation of delay and loss constraints. Different OAM toolsets exist, but they are technology dependent and to a large extent not compatible to the SplitArchitecture approach. In addition, OpenFlow in the current design has only limited OAM capabilities and needs extensions. The developments in SPARC concentrated on two things. First, the focus on MPLS as transport technology (see section 2.1.2) required adoptions and implementations for

- BFD based continuity check / connection verification

- Protection switching

- Updates to OpenFlow 1.1.

All three aspects have been developed (see D3.3 section 5.3), implemented (see D4.3 section 4.2) and the BFD implementation for different OpenFlow versions tested (see D5.2 sections 4 and 5). The second focus is on the question how to overcome the technology specific solutions for OAM and to develop a generic flow-based OAM. So an independent Flow OAM architecture was developed. In addition, a concept for meta-data encapsulation was developed allowing a more fine granular indication of packet and protection class.

Quality of Service is already broadly defined, but requires some adoptions in the different OpenFlow versions. In detail the required and analysed functions are classification, metering and colouring, policing, shaping, scheduling and rewriting (see D3.3 section 5.8). The improvements required are an extension to the per-packet context data with a colour field and advanced scheduling algorithms like the hierarchical QoS model. With this in place virtualization requirements can be easily met.

A network could be broken into essentially two parts: the data plane between two devices and the connection between data and control plane (see D3.1 section 10). For OpenFlow, the latter is becoming more important as it requires an additional data plane part compared to traditional scenarios. Therefore different concepts have been developed (see D3.3 section 5.4). For data plane resiliency, it is required that a failure is first detected by e.g. BFD (see previous paragraph on BFD for MPLS). This mechanism could be used in OpenFlow scenarios, too. Once a failure has been detected there are two different mechanisms to deal with it, restoration (reactive reconfiguration of the network with alternate paths after the failure) and protection (proactive installation of alternate paths before the failure). Both mechanisms have been analysed, adapted for OpenFlow and developed as well as verified in experiments (see D3.3 section 5.4 and D5.2 section 5). It was concluded that both mechanisms work in an OpenFlow network setup but protection is superior in terms of response time to restoration schemes. For the control channel resiliency (the link between data and control plane or in OpenFlow context controller), numerous options are discussed and verified in test (see D5.2 section 6 for details).

Increasing awareness of carbon emission has raised demand for energy-efficient networking optimisation in Internet technologies. From an OpenFlow and SPARC perspective, there are a number of optimisation possibilities (see D3.3 section 5.7). First, the centralization of control plane features could reduce the energy consumption of dedicated parts (in the order of 11%). Second, a number of features and control interfaces could be established related to enabling ports to be switched on/of and enabling functions like Adaptive Line Rate or Burst Mode. The third aspect concerning energy efficiency is the configuration and monitoring of components of the switch itself. For all three aspects, a set of OpenFlow extensions has been developed (see D4.2 section 3.7).

Before an OpenFlow enabled network is up and running, a bootstrapping process starts in order to establish a logical connection between the data path element and the controller and in order to configure required parameters for establishment of the OpenFlow connection (see D3.3 section 5.5.1). In practice, this includes steps such as DHCP-based network layer configuration, controller address exchange and TCP/TLS connection setup. This works well in cases where a direct connection between data path element and controller is available, but lacks a number of features in in-band scenarios where the control channel has to traverse multiple OpenFlow enabled switches. For the latter scenario a number of modifications have been developed for data path element behaviour to for example to connect a DSLAM located at a remote area with a controller attached to a central core network element. The prototypical implementations have been verified in various experiments:

- The OpenFlow control channel negotiation mechanism (see D5.2 section 6.1)

- Functional validation of in-band OpenFlow (see D5.2 section 6.4)

- Performance validation of in-band OpenFlow (see D5.2 section 6.5)

Another important aspect of network design and optimisation is the flexibility to steer traffic according to the actual situation of the network. One of the requirements to enable this flexibility is the knowledge about the available topology. Again, in several SDN controllers there was support for topology discovery, however, they lack support for legacy switches that are not taking part in the topology discovery triggered by the controller (see D3.3 section 5.5.2). This extensions has been implemented for MPLS (see D4.3 section 5.4) and verified (see D5.2 section 6.2 for functional and section 6.3 for performance validation).

Today's networks feature more layers than the canonical OSI/ISO model. It is concluded that OpenFlow can support in unifying the control plane, traffic engineering and recovery mechanisms (see D3.1 section 9 for details). Essentially the concept of Virtual Ports needs extensions to support dynamic behaviour. Three different approaches to overcome the issues have been identified: interworking, abstracted optical layer and impairment-aware OpenFlow. In addition, two existing solutions from Stanford and Ericsson are introduced.

The required network functions have been analysed and specified in detail where appropriate solutions could be found. They have been developed, implemented and tested. Overall, all aspects required in the access/aggregation use case access/aggregation are covered above or in the sections below.

With the focus on access/aggregation, it was been possible to develop a comprehensive set of solutions covering all requirements.

2.1.2   Seamless MPLS or SDN approaches to MPLS Transport

The trend towards MPLS based transport networks increased continuously in the recent years, with different flavours being developed and standardised. In D2.1 section 2.2.1.2, a number of advantages have been presented for extending the reach of MPLS from its classic placement within the core network towards the access/aggregation network. Among the advantages is the ability to provide VPN-like services which could be used to isolate users, services or operators from each other including numerous built-in network services and functions providing for example advanced QoS support, resilience features, etc. The addition of MPLS into the access/aggregation domain is also known as "seamless MPLS", an illustrative example is given with Figure 5 of D2.1.

The starting point for the analysis and developments are description of the business customer service (see D3.3 section 6.2.2), the Ericsson OpenFlow Extensions (see D3.1 section 4.2) and the standardised GMPLS with its split of data and control plane (see D3.1 section 6). The latter one is important in the discussion of packet-optical integration (which is part of the multi-layer use case to some extent), but access/aggregation networks also depend heavily on the optical networks and certain aspects have been covered also in this use case.

The versatility of MPLS has grown to a complex mix of numerous network integration options (see D3.3 Section 6.3.2). In the core network, IP/MPLS is typically used, but in the access/aggregation network more lightweight mechanisms could be used. Unfortunately, a number of protocols and mechanisms are required to provide interworking within and between these network domains, like link-state IGP protocols (OSPF or ISIS), Traffic Engineering (TE) extensions to share resource information, LDP to distribute MPLS tunnels between the domains, mLDP for multicast support, etc. As a result, the controller architecture and the OpenFlow MPLS extensions had to be further extended in order to cover all the different mechanisms. This includes (see D4.3 section 4 for details):

- BFD based OAM with continuity check, connection verification and protection switching (see section 2.1.1 for details)

- Pseudowire emulation

- Updates concerning adoption to OpenFlow 1.0

- Updates concerning adoption to OpenFlow 1.1

In addition, the MPLS/Pseudowire controller required numerous extensions (see D4.3 section 5 for details). It should be noted that some of the components already existed or have been extended based on existing components (see D4.1 for details):

- NOX kernel update for support of protocol messages (NOX event handling subsystem, I/O system)

- Topology discovery module

- Transport connection manager for provisioning of the flows

- NNI protocol proxy for interaction with other domains

- Graphical User Interface proxy collecting and presenting information about the network state

The prototype works on an Open Source software implementation. This solution has been heavily disseminated with demonstrations at key international events (see D6.1 and D6.2 for details). In addition, integration with the service creation controller was shown.

Another important aspect is the integration of optics. The fundamental different representation and handling between the packets and optics/circuits causes some difficulties. Nonetheless, there already exist some ideas how both could be integrated into an OpenFlow network and some implementation ideas as well (see D3.3 section 5.9). In addition, the ONF has recently started a working group on new transport technologies which is dedicated to deal with optical transport.

Overall, it can be concluded that the support for a Seamless MPLS or an SDN approach for MPLS Transport is possible. The developed components, the MPLS/Pseudowire controller and the general prototype provide a solid basis for future developments even with integration of optical transport.

2.1.3   Multi-service/-provider environments (Service Creation)

The use case on multi-service/multi-provider operation is motivated by the need to share physical or virtual infrastructures in access/aggregation domains due to financial or regulatory constraints or new business opportunities (details are covered in D2.1 section 2.2.1.3).

A technical solution has to cover different network functions detailed in section 2.1.1 above. Nonetheless, two essential concepts are detailed here: service creation covering the aspect of establishment of carrier-grade network services and virtualisation providing a mechanism to isolate either services or administrative domains (providers) against each other.

Service creation in the telecommunications industry describes the concept of service creation points, the points for configuration of network functions with customer- or product-specific parameters. Due to the lack of simplicity in today's networks and technologies it is essential to take this into account in the development of new architectures. Among the different requirements is the support for legacy, which imposes high migration cost and is typically neglected in the design and development today.

Two different types of services were identified, for residential and business customers. The business customer part is already covered in the section on MPLS transport. For residential customers, two basic scenarios are identified and combined with OpenFlow (see D3.3 section 6.2.1):

- SPARC BRAS based on PPPoE

- SPARC DHCP++ based on a combination of DHCP and additional mechanisms required for authentication and for gathering additional information required by the operator

For each scenario several different options are identified based on the capabilities of OpenFlow and potential integration in carrier networks. In addition, a prototype implementation was developed for both scenarios. In general, the implementations use MPLS as transport service in contrast to the suggested models of the Broadband Forum. On top of the MPLS architecture, different applications have been developed like DHCP and BRAS as well as interworking functions between the network services and the transport services (details see D4.3 section 6 and 7).

This includes the following components:

- BRAS
    o BRAS component organised in BRAS groups
        ▪ BRAS control plane
        ▪ BRAS data path element
        ▪ Logical Ethernet controller
        ▪ Logical IPv4 controller
        ▪ PPPoE module with termination and adaptation functions
        ▪ IPoE module with termination and adaptation functions
    o BRAS descriptor organising port descriptions for configuration of PPPoE
    o Interworking with MPLS
- SPARC DHCP++
    o UNI signalling module for DHCP and ARP
    o Service instance module taking care of configuration
    o IPoE-IPoMPLS interworking function
    o Transport connection request handler

The SPARC BRAS implementation has been tested and we verified to works as expected (see D5.2 section 3.1).

For virtualisation, design goals could be identified on a more detailed level than described in D2.1 (see D3.1 section 7). Different virtualisation approaches with different levels of abstraction for nodes, links or even complete networks are identified. Existing technologies (multi split instances like Virtual Routing Function (VRF)) and OpenFlow provides some but not complete support of network virtualisation. The important aspects providing virtualisation in the SPARC context are:

- Customer traffic mapping

- Existing OpenFlow techniques for network virtualisation

- Control channel isolation

- Out-of-band and in-band control networks

- OpenFlow state isolation

- Isolation in forwarding plane

Altogether results on the improvement proposal are detailed in D3.1 section 3.2.5 / D3.2 section 5.2.5. This system proposal of complete virtualisation provides a high degree of isolation in data and control path with a very limited

demand of interaction between operators and could achieve a solution for the multi-provider as well as multi-operator use case.

Unfortunately, the proof-of-concept implementation differs in certain details from the proposal combining OpenFlow capable switches with a virtual network translation unit, vendor extensions for data path modifications and an extended NOX (details in D4.2 section 3.4). One major question on the cost of different data plane virtualisation approaches was answered in the experiments performed within the project (details in D5.2 section 4). The results confirm the assumption that more complex technologies require higher penalties. These first indications of the potential impact of virtualisation need to be proofed in real production networks of operators.

In addition to network functions detailed in section 2.1.1, service creation and virtualisation provide a complete set of technology options to cover the use cases on multi-service/-provider operation (detailed in D2.1 section 2.2.1.3). The developments of the SPARC project show the potential of SDN, that it is possible to support numerous business models (cf. D2.1 Figure 6), have the freedom of choice for the desired network technology, to reduce the number of required technologies in the access/aggregation network domain, to use a network wide technology based on MPLS, to enable migration by decoupling service centric from transport centric functions and to enable desired levels of quality for different service demands.

2.1.4   Mobile backhaul

The analysis of mobile backhaul is increasingly important as costs for providing the service are increasing faster than costs per bit shrink and revenues increase. Several options are imaginable and detailed in D2.1 section 2.2.1.4. The analysis is split into a technical one for the use cases and a techno-economic one for an exemplary network deployment in order to show potential benefits of SDN.

An important aspect of the technical analysis is that the transport network is not in scope of the analysis of the different use cases. Therefore it was required to first analyse the architecture and its possibilities before analysing the concrete use cases. It required more steps in the analysis and conclusions are documented in Annex A of this document.

In summary, the analysis shows that the mobile world is using two different approaches. The first approach uses reference interfaces and specifies in detail how these interfaces should be integrated. Here the interfaces S1/5 using DiffServ approaches would be sufficient. The second approach uses some tunnelling mechanism for the transport of data. More specifically, the protocol tunnelling over the transport stack is GTP (GPRS Tunnelling Protocol) over UDP/IP/L2/L1 and GTP encapsulates another application/(TCP/UDP)/IP stack. Therefore an analysis of GTP and its capabilities is a prerequisite in order to improve mobile backhaul use cases. The solution is a rather simple idea and a straightforward approach of the OpenFlow development with the integration of another tunnel endpoint identifier (TEID) in OpenFlow matching rules and appropriate actions (see section A.3 for details). In addition, an external interface is required which transfers the information about the TEID and the desired action to the SDN controller (representing a system which takes care of the information and performs appropriate traffic engineering).

Based on this idea, the first five use cases have been analysed and it was concluded that the support by OpenFlow could provide some substantial support (see section A.4 for details). Unfortunately the analysis stopped at this still very general level and further activities will be needed to elaborate on a more detailed level on the potential integration into the architecture, development of prototypes and proof of concept evaluation.

The second major activity on mobile backhaul, the techno-economic analysis is documented in section 3 of this document. Given the newness of SDN in the context of mobile backhauling several assumptions had to be made which are often based on expert opinions or results from previous preliminary studies. To cope with the uncertainty related to the gathered input a sensitivity analysis was performed which examines the effects of change in the critical parameters on the overall results. Two different scenarios were defined, one covering state of the art design principles (classical scenario) and one advanced with SDN developments (SDN scenario).

For the considered parameters, the SDN scenario provides a capital expenditure advantage at 12%. The majority of capital expenditures savings is attributed to the savings at the pre-aggregation stages which is explained by the high number of sites at this level. A second contributor is the lower cost of first time installation. The savings in the pre-aggregation sites amount to up to 13% which is a bit higher than the total reduction of 12%. Introducing SDN however also involves introducing of centralized controllers to the network architecture which accounts for an extra 3% of the total cost.

Within the OpenFlow community the focus is often not on the promised capital expenditures reductions. Little attention is however given towards operational expenditures. The analysis shows a 10.7% OpEx reduction in case of the introduction of SDN. The main benefits can be found at the network operations center where the cost of operational processes such as service provisioning and service management is reduced by 3% and 6% respectively. The environmental cost (energy consumption) has not been increased nor reduced. It could be however argued that the energy consumption of the router is reduced because part of the control plane functionality is now taken over by the SDN controller. This is open for further research.

The performed sensitivity analysis introduces an overview on the level of uncertainty on the following parameters:

- Cost of a SDN controller has a rather low impact on the capital expenditures

- Number of OpenFlow enabled network elements one SDN controller is able to steer has a rather low impact as well on the overall cost basis

- Effect of wholesale price discounts by vendor on SDN advantage has a contradictory effect

    o The benefits of SDN on capital expenditures are reduced when higher discounts are applied

    o The benefits of software defined networking on operational expenditures increase when higher discounts are applied

    o The overall delta between the scenarios varies from 12% without discount to 9% for capital expenditures and from 10.7% to 12.3% for operational expenditures with 50% discount

- Effect of cost reduction in cost of operating system of router increases the delta between the scenarios by 50% for capital expenditures

- The highest effect of change has the effect of extra reductions in hardware cost because of specialization and interoperability of devices with potential reduction of price points for the SDN scenario by 50% and a delta of up to 47% (CapEx) and 25% (OpEx) respectively.

Again one has to mention that there exist a number of uncertainties in the techno-economic analysis and results have to be taken into account carefully. More details can be found in section 3.

2.1.5   Software Defined Networking application in context of IEEE 802.11 compliant devices

The use case of application of SDN in IEEE 802.11 compliant devices reflects another area of carrier environment and aspects in the access/aggregation network. The problem is the tight integration of 802.11 features in hardware, suspending improvements or enhancements and demanding physical exchange of the devices. Application areas are encryption schemes, mobility or more specifically handover, modifications at run time and virtualisation of the network as such.

There has been no explicit research or development in the context of this use case, but aspects have been taken into account in the development of the other use cases. For example the flexibility and modifications at run time are covered in the section 2.1.6. Therefore, the use case is not covered directly through the developments of the SPARC project, but numerous aspects are covered and can be supported like virtualisation, network management or quality of service.

2.1.6   Dynamic control composition

A major drawback of the today's network design principles is inflexibility. Almost anytime something changes, network elements have to be modified as well. In the best case this could be done with a firmware update in worst case, the device needs to be replaced. In conjunction, control and management functions needs to be adopted, too. Long innovation cycles are one result of this. In order to overcome this issue, network design principles must change in a way that it is possible to dynamically adapt the composition of control functions. This is the desired target of the analysis of dynamic control composition. In D2.1 several options of already existing approaches are described, like the best practices of ITIL (see D2.1 section 2.2.1.6 for details). In addition, it is briefly discussed which capabilities elements should have to enable dynamicity in control composition as such.

Within the project, again a multistep approach was carried out in order to come to conclusions. First, an analysis of ForCES and a comparison with OpenFlow has been done (see D3.1 section 5). In consequence it was concluded that ForCES defines a model which is both more generic and more comprehensive than OpenFlow:

- It defines a network element and describes how the ForCES components are integrated. An interaction with legacy is part of the discussion per se.

- ForCES is more generically defined

- ForCES defines management interfaces

In particular, OpenFlow should borrow concepts and should be extended with abstract architecture, information model, transport layer mapping, failure recovery mechanisms and management interface or system. In addition, hierarchical controller architectures have been identified as a solution for split of functions and therefore complexity.

In the second step, the hierarchical controller concept was detailed and numerous extensions were defined (see D3.3 section 4.1.5 and section 5.1). Basically, the concept describes a container providing an interface to underlying controllers as controller and upwards as data path element (cf. see Figure 2). It has network management interfaces and certain logic (app) which performs the analysis of packet-in events.

The OpenFlow port definition was extended and may support additional or different configuration parameters. This is done by definition of the Transport-Endpoint control message supporting CRUD lifecycle (Create, Read, Update, and Delete) and the definition of the eXtensible Port Parameter set (XPP) for these endpoints. In addition, the fixed C-structure was extended to type-length-value fields, enabling another degree of openness and extensibility. Based on the analysis of state full or less, history of preceding packets and timing requirements, four additional concepts are developed:

- Extension of processing entities for persistence and providing history of flows

- OpenFlow action ActionProcess bundles an action in the OpenFlow action set with a processing instance

- Pre-/post filters enabling the testing of the data path in between them (e.g. deploying OAM capabilities with the help of Virtual Ports)

- Split state machines provide possibilities to synchronize between protocol components deployed close to the data path (e.g. for meeting delay constraints) and protocol components deployed in the control plane

Another identified concept is the programmable data path at run time. This is beyond the scope of SPARC and will be subject of study in the ICT ALIEN project [21].

The third step was the implementation of the concept of dynamic configuration of Virtual Ports and flow space registration (see D4.2 section 3.2 and 3.3). For the Virtual Ports, vendor extensions are defined which provide control for creation, deletion and updating as well as the attachment and detachment to other Virtual Ports or processing interfaces. The second implementation deals with the organisation of flow space between controllers through flow space registration. Each controller could request a part of the flow space, the controller wants to be responsible. So a split of functions and dynamicity is enabled.

In total, it is a bit difficult to conclude whether this use case is covered by the developments described here and somehow is left open for the specific target of more concrete use cases (like service creation). Nonetheless, the concepts as well as prototypical implementations provide an increased level of flexibility enhancing OpenFlow as such. Dynamicity of the control plane could be enabled by the hierarchical or recursive controller architecture with accompanying concepts like flow space registrations. In addition the processing part is enhanced so that different types of protocols or other functional extensions could be added easily.

2.2   Review of requirements

2.2.1   Summary of D2.1 conclusions

In D2.1, 67 requirements have been identified. The study and analysis of the requirements came to the conclusion that, with respect to importance in the context of SPARC, the set of requirements can be subdivided in different clusters. So the total of 67 requirements had to be reduced in order to concentrate only on those requirements that are not already fulfilled with respect to existing architecture concepts and available implementations. The selection process was based on

- the opinion of the technical experts of the project

- the use of the key words "must", "should" and "may" as specified in IETF RFC 2119

- the relationship to the different use cases (D2.1 had three major use cases)

- prioritisation with respect to overall importance, fulfilment in existing architecture concepts and/or existing implementations

Overall, four groups of general, important requirements were identified. The first group covers all required "Modifications and extensions for the data path element" or the SplitArchitecture itself. The other three groups deal with needed extensions of carrier-grade operation of ICT networks. The aspects related to the operation of an ICT network "authentication, authorization and auto configuration" (not to be mixed up with "AAA", as accounting is use-case-specific) are covered in a second group; "OAM" in the sense of facilitating network operation and troubleshooting in the third group, "network management, security and control" of the behaviour of the network and protocols in the fourth group. Within network management, the aspects for the use of policies in network environments are included.

2.2.2   Summary of WP3

In D3.1 the assessment of existing SplitArchitecture approaches, such as ForCES, GMPLS/PCE and most importantly OpenFlow revealed a number of issues and open questions that need to be considered for future carrier-grade Split Architectures. The following topics have been identified that require special attention in the current architecture study:

- Requirement group "Network virtualization", e.g. to ensure strict virtual network isolation and integrity and handling of overlapping address spaces should be handled

- Requirement group "Recovery and redundancy" including open question not only with respect to the data plane of the network, but also with respect to controller and control plane failures

- Requirement group "Multilayer control" include integration of circuit switching and multilayer coordination for optimization or resiliency purposes

- Requirement group "OAM" functionalities for service management

- Requirement group "Scalability" to be considered for the data plane and proposing controller architecture

In the following architectural deliverable D3.2, the specific functions have been investigated and additional refinement of the different groups has been required (each requirement group now effectively represents a general network function or feature):

- Requirement group "Modifications and extensions to the data path elements" has been broken down into two detailed groups identified as particularly relevant in a carrier-grade networking context:

  o Requirement group "Openness and Extensibility" developing ways of how to extend OpenFlow to support a more complete, stateful processing on data path elements in order to enable OpenFlow support for further technologies with high relevance to carrier networks, such as PBB, VPLS, PPPoE, GRE, etc. [R28, R30-33 in D2.1]

  o Requirement group "Multilayer" aspects is on the extension of OpenFlow in order to control non-Ethernet-based layer 1 technologies (as specified by IEEE 802.3 study group), especially the integration of circuit switched optical layers into OpenFlow (packet-optical integration).

- Requirement group "Authentication, authorization and auto configuration," is covered by the broader topic of "Service Creation" [R6-7, R10, R23 in D2.1].

- Requirement group "OAM" has also been identified as important matter in D3.1. Both a technology-dependent OAM solution (i.e., MPLS BFD) and a novel technology-agnostic Flow OAM solution was identified, the latter targeting a generalized OAM Split Architecture. [R25-27, R67 in D2.1]

- Requirement group "Network management" was divided into several subgroups:

  o Requirement group "Network Management" as such is a relevant separate group, but covered in D3.3. However, the general framework required for implementation of network management functions in a SplitArchitecture environment are fault and performance management covered by "OAM" [R22-24, R27, R60, R67 in D2.1]; configuration management [R17-19, R21, R34-36, R38-40, R51-56, R61-62 in D2.1]

  o Requirement group "Quality of Service" is discussed separately [R11-14, R37, R48 in D2.1]

  o Requirement group "Resiliency" is commonly seen as one key attribute of carrier-grade networks, i.e., the ability to detect and recover from incidents within a 50ms interval without impacting users. In D3.1 recovery and redundancy mechanisms were identified as important issues regarding a (partly) centralized SplitArchitecture. [R42, R47 in D2.1]

  o OpenFlow enables Split Architectures by providing an open management interface to the forwarding plane of data path devices, which allows centralized control of multiple OpenFlow data path elements by a single control element. In order to facilitate this centralized network management operation, we identified automatic (Requirement group) "Control Channel Bootstrapping and Topology Discovery" as an important feature for carrier-grade Split Architecture networks. [R27, R51 in D2.1]

  o Requirement group "Energy-Efficient Networking" provides functionalities to increase the energy efficiency of modern and future networks. [R59-60 in D2.1]

- Requirement group of D3.1 "Virtualization and Isolation" enabling multiservice (within the responsibility of one operator) and multi-operator scenarios on a single set of a physical network infrastructure [R1-4, R41-45 in D2.1]

- Requirement group "Scalability" is another key feature of the SPARC controller architecture [not covered in D2.1].

In the final architecture deliverable D3.3 harmonized the different concepts covering the requirement groups outlined before and defined the "Recursive Control Plane" architecture (referred to as hierarchical controller concept as well), an extension and further detailing of requirement group "Modifications and extensions for the data path element" of D2.1 [R5, R35, R40, R64]. In addition, the requirement group of "Network management" was finally detailed as a separate main group (not to be confused with the other requirement groups on QoS, resiliency, etc.).

2.2.3   Conclusions on review of requirements

The groups of requirements listed in D2.1 were not sufficiently well grouped in order to be dealt with in the development of the SplitArchitecture. Therefore, the groups have been further refined during the course of the project. It should be noted that the requirement groups were detailed with focus on the access/aggregation use case only. The resulting groups are:

(m) Recursive Control Plane [R5, R35, R40, R64 in D2.1]

(n) Network Management [R17-19, R21-24, R27, R34-36, R51-56, R60-62 in D2.1]

(o) Openness and Extensibility [R28, R30-33 in D2.1]

(p) Virtualization and Isolation [R1-4, R41-45 in D2.1]

(q) OAM (technology-specific MPLS OAM [R25-27 in D2.1] / technology-agnostic Flow OAM [R25-26, R67 in D2.1])

(r) Network Resiliency [R42, R47 in D2.1]

(s) Control Channel Bootstrapping and Topology Discovery [R27, R51 in D2.1]

(t) Service Creation [R6-7, R10, R23 in D2.1]

(u) Energy-Efficient Networking [R59-60 in D2.1]

(v) Quality of Service [R11-14, R37, R48 in D2.1]

(w) Multilayer Aspects [R65-66]

(x) Scalability

For group (l), no firm requirements have been formulated in D2.1. However D2.1 section 2.2.3, numbers for access/aggregation networks are given, but scalability in data path elements and controllers as well as API depend on the concrete implementation scenarios in carrier networks.

In the Annex B the mapping between requirements of D2.1 and the requirement groups of this document has been documented. Overall, the list with the requirements can be grouped in five segments:

- Very important (**) and missing (**) in OpenFlow and SplitArchitecture (Score 4)

- Very important (**) and partly missing (*) in OpenFlow and SplitArchitecture (Score 3)

- Important (*) and missing (**) in OpenFlow and SplitArchitecture (Score 2)

- Important (*) and partly missing (*) in OpenFlow and SplitArchitecture (Score 1)

- All other groups are not important and/or not integrated (Score 0)

It can be concluded that the most important requirements with a score 4 are covered in the development of the SplitArchitecture and its supporting features. Two requirements are missing. R-38 (A data path element classifier should be constructed in a protocol agnostic manner or should be at least flexible enough to load new classifier functionality as a firmware upgrade with identical performance.) is revised during the beginning of the project as being covered in OpenFlow 1.1 with the introduction of Virtual Ports. The second one is R-39 (The Split Architecture should introduce a clean split between processing and forwarding functionality.) which is a basic working assumption for SPARC and covered in scenarios for implementation of service creation. Nonetheless, it was decided to keep it as not covered as no architectural split is detailed enough and is subject of future work on hardware abstraction layer like ICT ALIEN project [21]. For the next lower level of important requirements, score 3, two requirements have not been covered, but these two are dedicated to the use case area of data centres, which is out of the scope of the analysis. In the score 2 group, two requirements have been left open. The first one, R-9 (The Split Architecture should support TDM emulation and/or mobile backhaul.) has been left open for further studies, because TDM emulation has not been in focus in the analysis of the use case on mobile backhaul in access/aggregation network domain. The second requirement, R-15 (The Split Architecture must control the access to the network and specific services on an individual service provider basis.) has been discussed in different details. Multi-provider was discussed within requirement group virtualisation and isolation. Access control was not in focus and left open. The group with a score 1 was not used in the analysis of the requirements.

Overall, it can be concluded that the work on the technical aspects covers the majority and all important requirements as detailed in D2.1. So, the requirements of access/aggregation use case are covered and the use case as such with the developments fulfilled.

3 Techno-Economic analysis of use case mobile backhaul transport

3.1 Scope of the analysis

The goal of this study is to make a comparison between the capital- and operational costs of a traditional IP/MPLS network and a Software Defined Network.

The explosion in the data traffic for mobile users is a challenge for mobile operators. Mobile wireless subscribers are demanding content at any place at any time. Data sessions over mobile networks are increasing sharply and more bandwidth per subscriber is required. Further increasing the need for bandwidth is a technology evolution which includes an increase of bandwidth capacity in the access network.

With increasing bandwidth demand and the average revenue per user (ARPU) which is not expected to grow as fast as the rate of data traffic, mobile operators need to keep capital expenditures lower to eventually gain a lower cost per bit. In addition, the monthly recurring charges for existing backhaul technologies

- Asynchronous Transfer Mode over Synchronous Digital Hierarchy (ATM over SDH) and

- Synchronous Optical Networking/ ITU-T Synchrone Digital Hierarchy (SONET/SDH)

increase linearly with the capacity.

At the demand side for a backhaul network low latency, higher bandwidth, network intelligence, resiliency, security, quality of service and service differentiation are expected.

These challenges are directing mobile operators to:

- newer radio access technologies such as Long Term Evolution (LTE),

- Packet-based, non circuit switched technologies and backhaul architectures based on Ethernet and IP Multiprotocol Label Switching (IP/MPLS)-based packet backhaul architectures

Investigating the potential of future mechanisms that can decrease the capital expenditures (capex) and operational expenditures (opex) of a mobile network is essential to eventually reduce the cost per bit. Reducing the cost of network equipment and network operations is such a mechanism.

One of the main contributors to the cost structure of network operators are the network devices. Much of today's network equipment is highly specialized and monolithic (there is no separation between the control and the forwarding, that could be used in a modular manner). In today's dynamic environment network operators need to be able to rapidly deploy new capabilities and services in response to changing user demands in order to stay competitive. However, because of the lack of an open interface between the control logic and forwarding logic the ability to innovate is hindered. The operator must wait for the vendor of network infrastructure equipment to implement it which can take in some cases up to years.

This mismatch between market requirements and network capabilities has led to a rethinking of network architecture. By separating the control and forwarding logic it is possible for the operator to reduce vendor dependence, increase the speed of innovation and potentially reduce the total cost of ownership. This might result in operators using standard networking hardware and custom control and management software in standard network controllers.

Software defined networks can overcome this problem and a solution based on exploring OpenFlow (OF) has been proposed. We investigate two network scenarios based on this OF solution in a techno-economic analysis: (scenario 2) software-defined networks and compare it against the current situation (scenario 1). By doing so, we want to provide insights on the relative cost savings that a mobile network operator can reach through the use of Software Defined Networking (SDN) in a state-of-the-art backhauling network infrastructure.

3.2 Scenario analysis

We consider the aggregation- and core parts of a separate network for mobile backhaul as potential targets for software defined networking. The network under consideration will be analysed over a time period of 5 years starting in 2012 and ending in 2017.

The network under consideration is ready for LTE and provides support for legacy access technologies. A state-of-the-art network design is considered with IP/MPLS based technology and mobile backhaul using Ethernet as the main technology. The network element part of the infrastructure (routers, transceivers, software, etc.) is considered while the cost of the fibre interconnections is out of scope of this analysis. Significant parts of the analysis are based upon input from the SPARC consortium partners.

The two scenarios under consideration are:

Classical scenario: the network architecture consists of monolithic network devices in which forwarding and network control is unified in the network elements.

Software Defined Networking (SDN) scenario: SDN is a network architecture where forwarding is (1) decoupled from network control and (2) there is more freedom of choice in programming the forwarding logic. Network intelligence is (logically) centralized in software-based SDN controllers, which maintain a global view of the network [1]. The SDN controller typically has knowledge about the physical topology of the network either by discovery mechanisms or appropriate databases and can based upon this topology create paths that are programmed into the forwarding engines of network devices. In essence, SDN abstracts the network like an operating system abstracts the applications from the hardware. SDN is different from the current network architecture because current (virtual) networks combine the control and forwarding logic in the virtual and physical switches. A second difference is the programmability of forwarding paths. OpenFlow [2] is considered as the enabler of SDN. It is a standard communications interface defined between the control and forwarding layers of an SDN architecture. OpenFlow allows direct access to and manipulation of the forwarding plane of network devices such as switches and routers, both physical and virtual (hypervisor-based) [1]. The path of packets through the network of OpenFlow enabled switches is determined by software running on a separate SDN controller. OpenFlow is, as an enabler of SDN, a solution to the mismatch between market requirements and network capabilities as it provides an open communication interface between the control and forwarding layer allowing network operators to be less vendor dependent.

3.3   Methodology

We follow the methodology described in [23] to evaluate the costs of a network scenario for a telecom operator. Figure 3 gives a schematically representation of the sub categories. We will use this visualization to illustrate the categories considered and their impact on total costs.
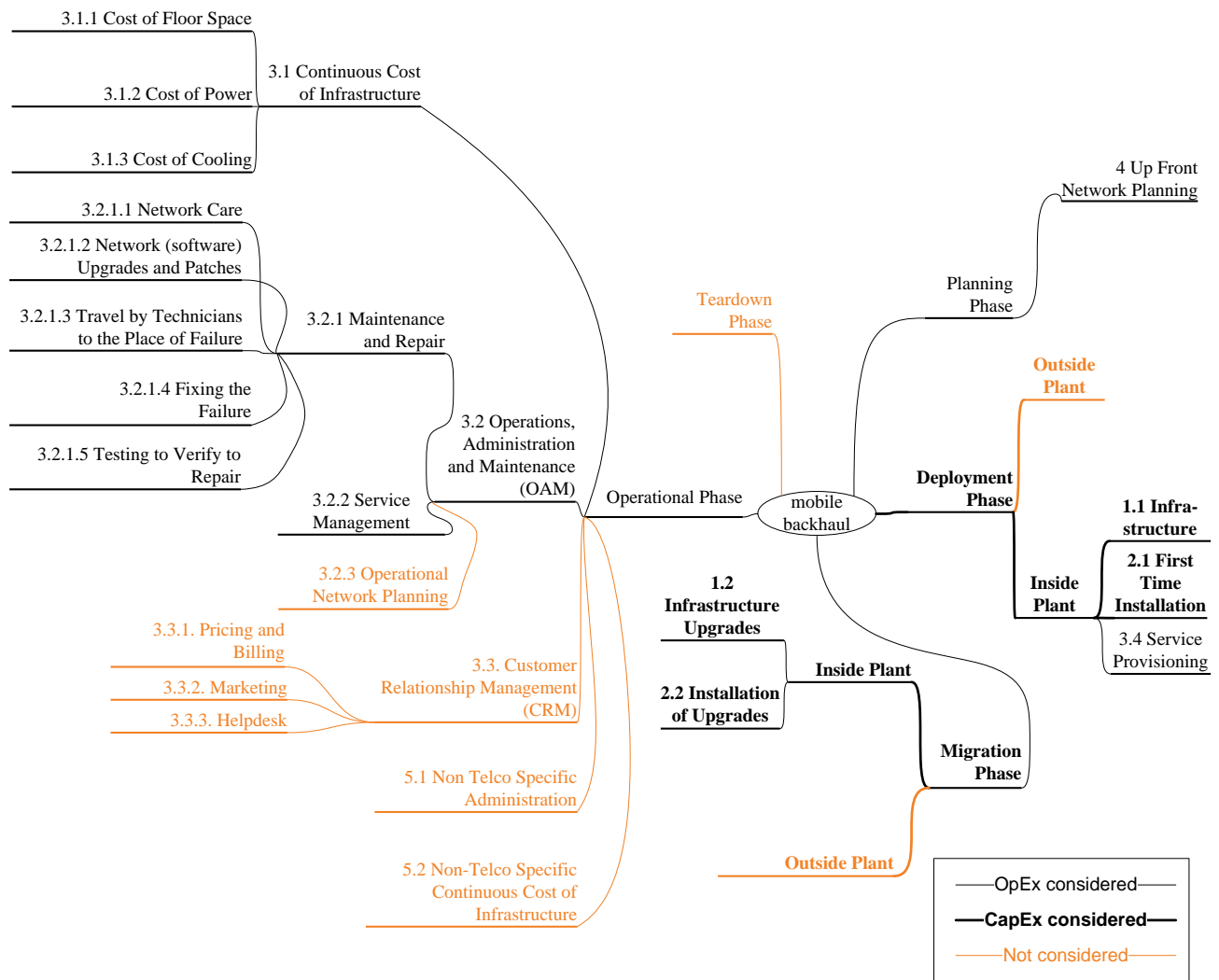
Figure 3: Cost breakdown of processes for a telekom operator

Capital Expenditures or CapEx contribute to the fixed infrastructure and they are depreciated over time. For a network operator, they include the purchase of land and buildings (e.g. to house the personnel), network infrastructure (e.g. optical fiber and IP routers), and software (e.g. network management system).

The major contributors to CapEx can be defined in two subcategories:

Category 1: Infrastructure

All costs related to buying the equipment are counted here. In this study we only consider the cost of network elements (e.g. routers and switches) at the aggregation and core sites. The consideration fiber costs are out of scope.

Category 2: First time installation

All costs related to installing the equipment (after buying it) are counted here. The cost of first-time installation includes the actual connecting and installation of the new component into the network, as well as the necessary testing of the component and its installation. This first-time installation is usually carried out by the equipment vendor. In this case, the costs for the operator are included in the contract with the vendor.

Operational Expenditures or OpEx do not contribute to the infrastructure; they represent the cost of keeping the company operational and include cost of technical and commercial operations, administration, etc. For a network operator, OpEx are mainly constituted of rented and leased infrastructure (land, building, network equipment, fiber,…) and personnel wages.

The major contributors to OpEx can be classified into three subcategories. A detailed overview of what is understood for each of the categories is given below.

Category 3: The telco specific OpEx for a network which is up and running groups expenditures for operating an existing, up and running network:

> Subcategory 3.1: Continuous cost of infrastructure

The cost of keeping the network operational in a failure-free situation. It includes the cost for floor space, power and cooling energy, leasing network equipment and right-of-ways.

> Subcategory 3.2: Operations, Administration and Management

> Subcategory 3.2.1: Maintenance and repair cost

The costs of preventative measures such as monitoring and maintaining the network against possible failures. The main actions performed here aim at monitoring the network and its services. Therefore, the actions involved include direct as well as indirect (requested by an alarm) polling of a component, logging status information, etc. Also stock management (keeping track of the available resources and ordering equipment if needed), software management (tracking software versions and install updates), security management (tracking people who try to violate the system, and blocking resources if needed), change management (tracking changes in the network, e.g., whether a certain component goes down), and preventive replacement are included. Furthermore, cleaning of equipment can be taken into account as well.

Repairing the failure in the network, if this cannot happen in routine operation. Repair may lead to actual service interruptions, depending on what protection scheme is used. The repair process includes diagnosis and analysis, travel by technicians to the place of the failure, fixing the failure, and testing to verify the repair.

> Subcategory 3.2.2: Service provisioning

This begins with a service request from a potential customer and includes the entire process from order entry by the administration to performing the needed tests, service provisioning, service move or change, and service cessation.

> Subcategory 3.2.3: Service management

Service management is concerned with the process of keeping a service up and running once it has been set up. It includes configuration of new services after the initial rollout and the reconfiguration of existing services.

> Subcategory 3.2.4: Operational network planning

It includes all planning performed in an existing network that is up and running, including day-to-day planning, optimization, and planning upgrades.

> Subcategory 3.3: Customer Relationship management

> Subcategory 3.3.1: The cost of pricing and billing

This means sending bills to customers and ensuring payment. In addition, it includes actions such as collecting information on service usage per customer and calculating cost per customer. Calculating penalties to be paid by the operator for not fulfilling the service level agreement (SLA) is another task here.

Subcategory 3.3.2: Marketing

The acquisition of new customers for a specific service of the telco. Marketing involves promoting a new service, providing information concerning pricing, etc. Possibly, new technologies enable new services.

Category 4: Opex for planning

This category of OpEx that we distinguish is associated with equipment installation and groups two expenditures. This represents all the costs to be made before connecting the first customer in case of a green field scenario, or the migration costs before the network becomes operational again in case of a major network extension.

Subcategory 4.1: Up-front planning

All planning done before the decision "let's go for this approach" is taken: planning studies to evaluate the building of a new network, changing the network topology, introducing a new technology or a new service platform, etc.

Category 5: General OpEx (overhead)

Subcategory 5.1: Non-telco specific cost of infrastructure

This includes OpEx subparts that are present in every company; they are not specific for a telecom operator.

Subcategory 5.2: Non-telco specific administration

This includes the administration every company has, such as employee payroll administration, office support staff, the human resources department, etc.

Not all cost categories were relevant for further consideration in the analysis, an example is subcategory 5. General OpEx which will not be affected by the introduction of SDN and subcategory 3.3. Customer Relationship Management which has no connection with the introduction of SDN. An overview of the considered processes and the expected impact of SDN on OpEx is given in Figure 4.

ID	Planning Phase 4	Deployment Phase 1.1	2.1	3.4	Migration Phase 1.2	2.2	Operational Phase 3.1	3.2			3.3			5.1	5.2	Tear-down Phase
								Operations, Administration and Management			Customer Relationship Management					
	up-front planning	Infrastructure	first time installation	service provisioning	Infrastructure upgrades	intsallation upgrades	Continuous Cost of Infrastructure	maintenance and repair	service management	operational network planning	pricing and billing	marketing	helpdesk	non telco specific administration	non telco specific cost of infrastructure	
Classical Scenario	0	0	0	0	0	0	0	0	0							
SDN Scenario	-1	-1	-1	-1	-1	-1	-1	-1	-1							

0	no effect on costs		-1	cost saving
■	not considerd			

Figure 4: Overview of capital expenditures and operational expenditures and potential savings with the classical scenario as reference point

3.4   Qualitative Cost Evaluation

Capital expenditures (categories 1.1., 1.2., 2.1. and 2.2.) can be reduced in the SDN scenario compared to the classical scenario because the control logic is removed from the router and shifted to a SDN controller. With SDN, operators might be able to improve utilization of physical resources and prevent vendor lock in. SDN allows the use of simpler and cheaper devices in the network. The extra cost for SDN controllers will however increase the capital expenditures. The overall balance is expected to shift to a cost reduction because one SDN controller can control multiple OpenFlow switches.

Main parameters that will influence the potential for cost reductions by applying Software Defined Networking are: (1) cost savings that can be reached by using simpler network devices, (2) cost of extra components such as an extra SDN controller and the extra line cards and (3) the ratio of the number of switches that a SDN controller can manage and (4) the possibility to better align network capacity with actual demand.

The continuous cost of infrastructure (3.1) for the SDN scenario will be slightly lower because the cost for power and cooling energy is reduced as there is no more energy consumption by the control plane in the network switches. Further, SDN allows for better traffic-steering, potentially reducing the number of network devices and their power consumption. The additional SDN controller(s) will, if not embedded, consume more energy compared to a classical scenario without SDN controllers.

Maintenance- and repair cost (3.2.1) will be lower in the SDN scenario. SDN creates a single cohesive system where in old architectures it was required to manage and maintain a bunch of independent autonomous devices. An example is the maintenance cost of software. Software management will be easier because the number of running software versions is reduced to a minimum of one. Similar effects come into play for security management and stock management.

Costs for repair can be reduced in the SDN scenario because of the better testing possibilities ahead of rollout which will reduce the number of bugs that can reach actual production traffic. Spare parts for broken down infrastructure are less expensive because due to the trend to use apply commodity systems, hardware in general is less expensive. A large drawback of SDN is the creation of a single point of failure: the SDN controller. Failures in these network elements can destabilize the entire network. This short come can be resolved by a redundant controller architecture which offers robustness, but also adds complexity and cost.

Cost of service provisioning (3.4) can be lowered because SDN enables automated configuration of the network. Today experienced networking personnel are required to set up, administrator, change and maintain the network. These personnel can be hard to find, expensive and difficult to retain. SDN reduces the amount of manual configuration required in the network which will also result in fewer errors and less network downtime.

The cost for up-front planning (4) and first time installation of network equipment (2.1) will alter. SDN creates a higher level of innovation which will lead to faster iteration times and a higher frequency of testing. SDN however has robust testing abilities ahead of rollout and reduces the number of devices that need to be updated. The network environment can be simulated to create a test environment before the transition to the new system and production flows can be mirrored into this test environment allowing for early identification and fixing of bugs. The created test environment also offers the opportunity to train staff working at the network operating center on a real-world simulated network before they need to operate the network while they are in production.

3.5 Network design for a German reference network

We have found one previous study that quantifies the operational expenditures, capital expenditures and total cost of ownership [22] for carrier grade SDN. We've chose a network design which is very similar to this study to be able to benchmark our results with those form the ACG Research study.

The results from the ACG Research study show a large cost saving potential for SDN:

- 79% lower total cost of ownership,

- 80% lower capital expenditures and

- 79% lower operational expenditures

The analysis of network dimensioning has been started with a generic network layout that reflects the topology, the amount of customers and the customer distribution within Germany. The generic network layout exists of a logical IP network with 25,000 radio base stations or access nodes. The network has two aggregation stages. A pre-aggregation stage with 1,000 sites and next an aggregation stage with 80 sites.

The access network is connected with the pre-aggregation stages via a ring topology containing 5 radio base stations per ring and 5 rings per pre-aggregation site summing up to a total of 25 radio base stations per pre-aggregation site.

The connection between the pre-aggregation sites and aggregation sites is also established through a ring topology. Each ring contains 4 pre-aggregation stages and there are 4 rings per aggregation site summing up to a total of 16 pre-aggregation sites per aggregation site.

This ring network provides shared protection with extra traffic (1:N protection). The ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) mechanism is used to provide sub-50ms protection and recovery switching for Ethernet traffic in this ring topology. We chose this particular network design and ring protection switching mechanism to be able to benchmark our analysis against a total cost of ownership analysis for SDN done by ACG Research [22].

An overview of the network design up to the aggregation sites is given in Figure 5.

25,000 radio base
stations   1,000 pre-aggregation sites   80 aggregation sites   12 core sites

5 radio base stations per access ring
5 access rings per
pre-aggregation site

4 pre-aggregation sites
per aggregation ring
4 aggregation rings per aggregation site

Each aggregation
device is connected to
2 distinct core sites
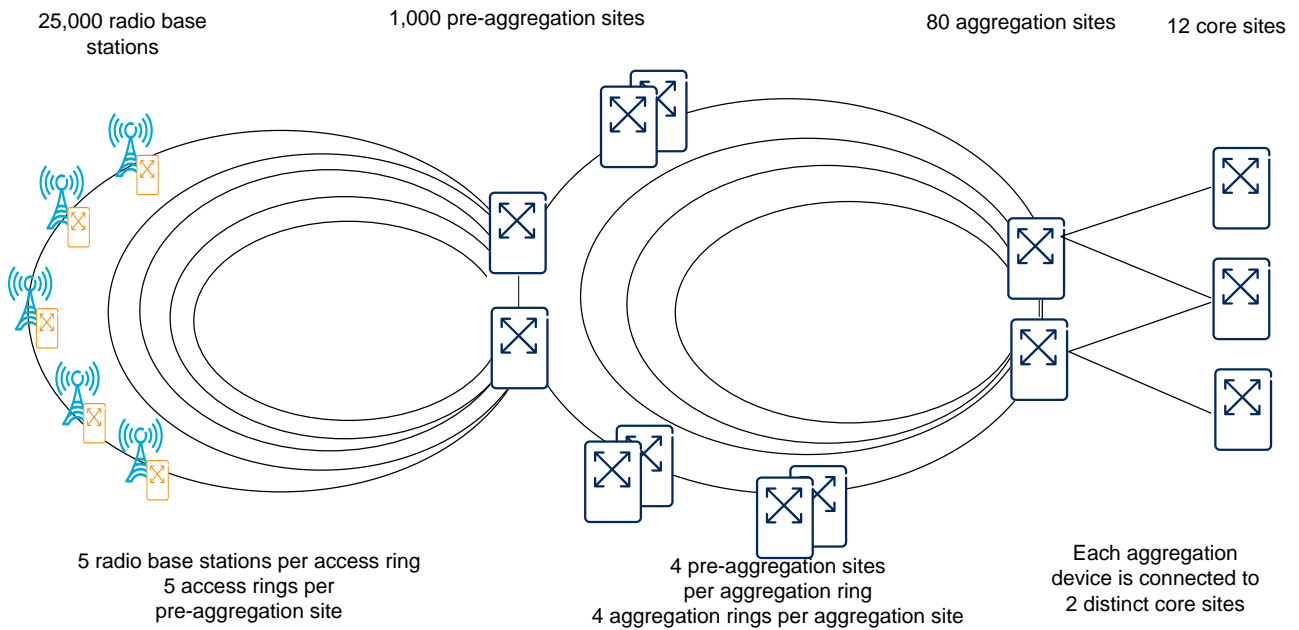
Figure 5: Schematic overview of the metro network design

Seven aggregation sites are concentrated at 1 of the 12 core locations with a redundant path to another 1 of the 12 core locations. This is illustrated in Figure 6.
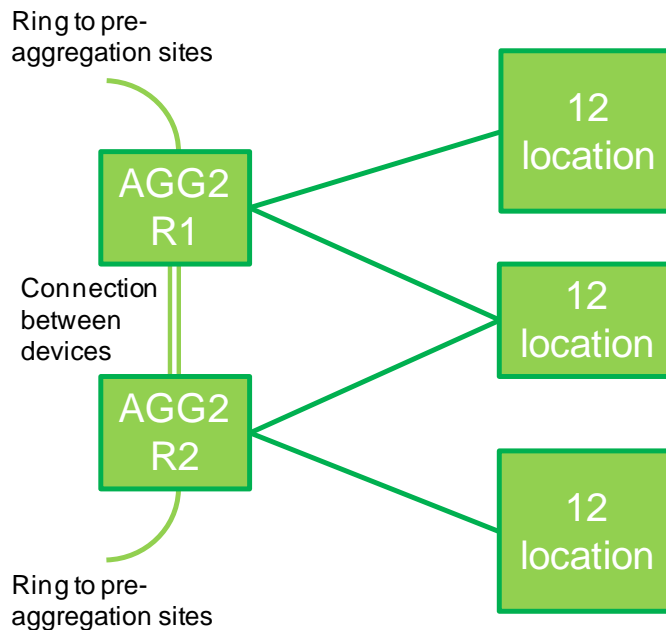
Figure 6: Link connection for aggregation sites

Of these 12 core locations, 6 locations are used as inner core in parallel. A combination of mesh and direct connections links the core locations. Each of the 12 core locations is attached redundant to 1 of the 6 inner core locations. An overview of the core network design is given in Figure 7. By doubling the available capacity at disjunctive locations and appropriate connections a complete redundant network is provided. The inner core (6 locations) has connection to the "internet".
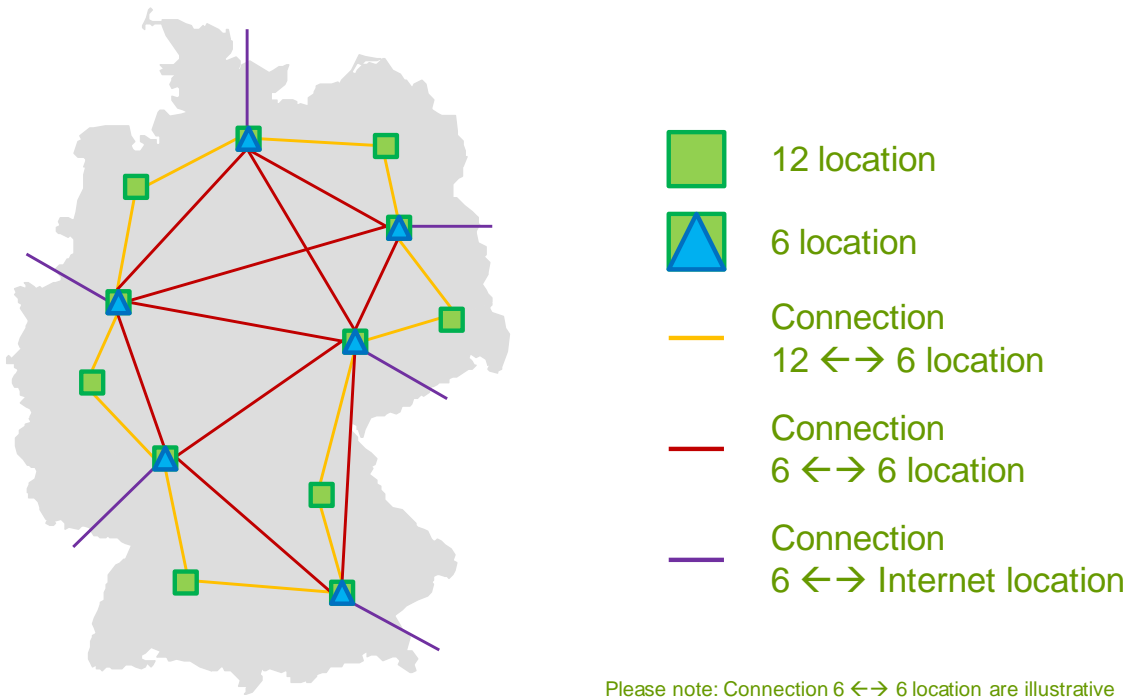
Figure 7: Schematic overview of core network design

An overview of the modified general network design is given in Figure 8. All required mobile core network elements are connected to the core- and inner core locations. Each of the 6 core locations is connected to the Serving GateWay (SGW), Serving GPRS Support Node (SGSN), Mobility Management Entity (MME), etc. Each of the 6 inner core locations is also connected to the Packet Data Gateway (PDG), Gateway GPRS Support Node (GGSN), etc. and the internet.

The colour legend for the location interconnections used in Figure 7 is also used in Figure 6 and Figure 8.
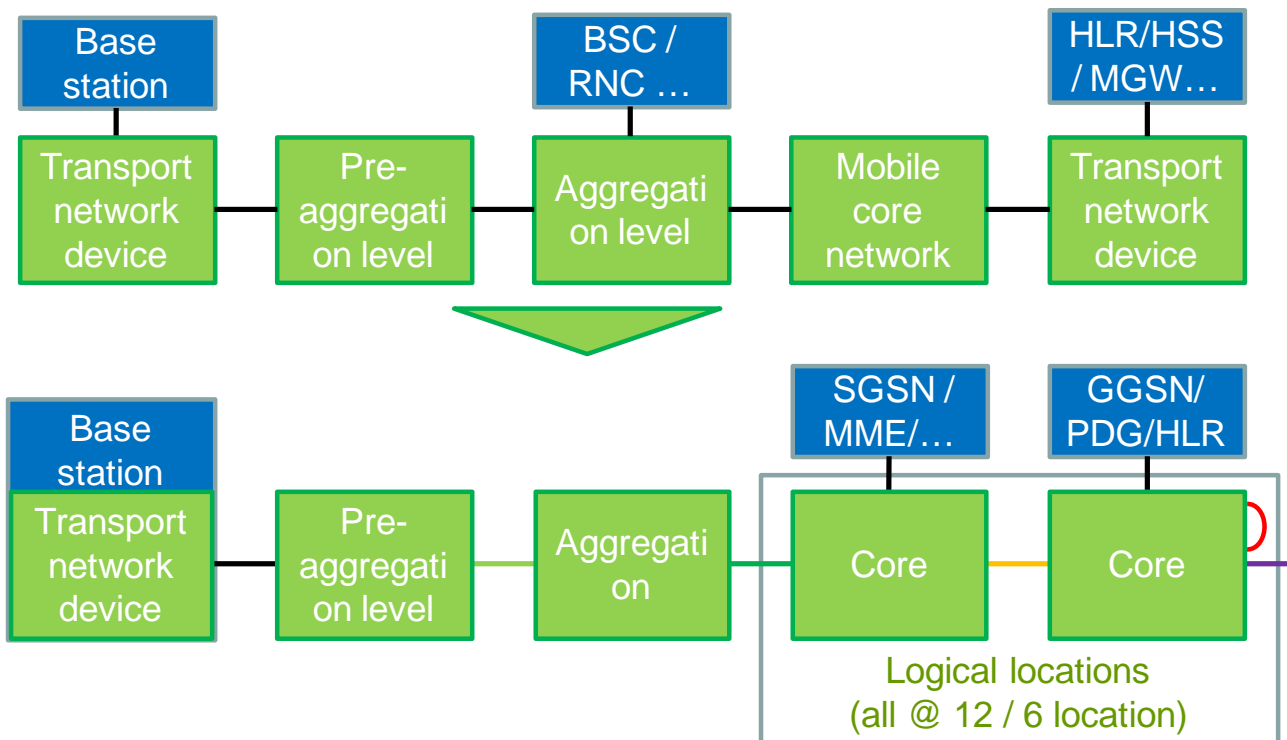
Figure 8: Modification in general network design

3.6 Traffic sources for Germany

A bottom-up approach has been used to analyze the traffic sources, which should reflect the situation given in Germany. The analysis of traffic profiles of customers is based on, but not necessarily identical with, Ericsson input values. The actual number of customers using a mobile broadband device for 2011 and the expected number of customers for the period 2012-2017 are shown in Figure 9. From Figure 9 it's clear that HSDPA will overtake W-CDMA and that the adoption rate of LTE will steadily increase.
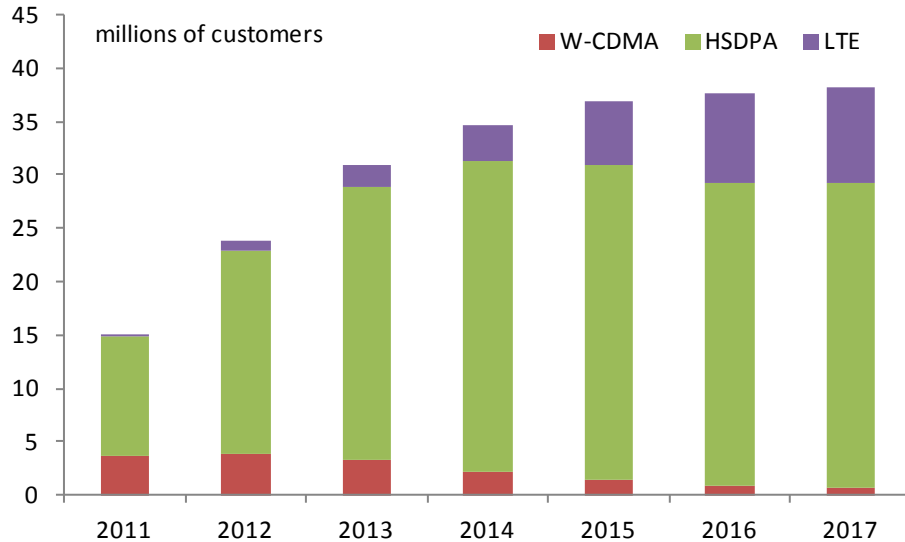
Figure 9: Evolution of the amount of customers for each wireless data communication standard

The traffic per customer per month is split up in two categories: (1) mobile pc or tablet and (2) handheld devices such as smartphones. The evolution of the share of mobile pc or tablet to all mobile broadband devices is illustrated in Figure 10. The absolute number of customers increases for each broadband device category. The number of customers with mobile pc or tablet is expected to stabilise around 5 million from 2013 on.

Evolution of traffic per device category is given in Figure 11. The amount of traffic generated by each category of devices is given in MB/month. It is clear from this graph that mobile pc and tablet generate more data than mobile handheld devices.
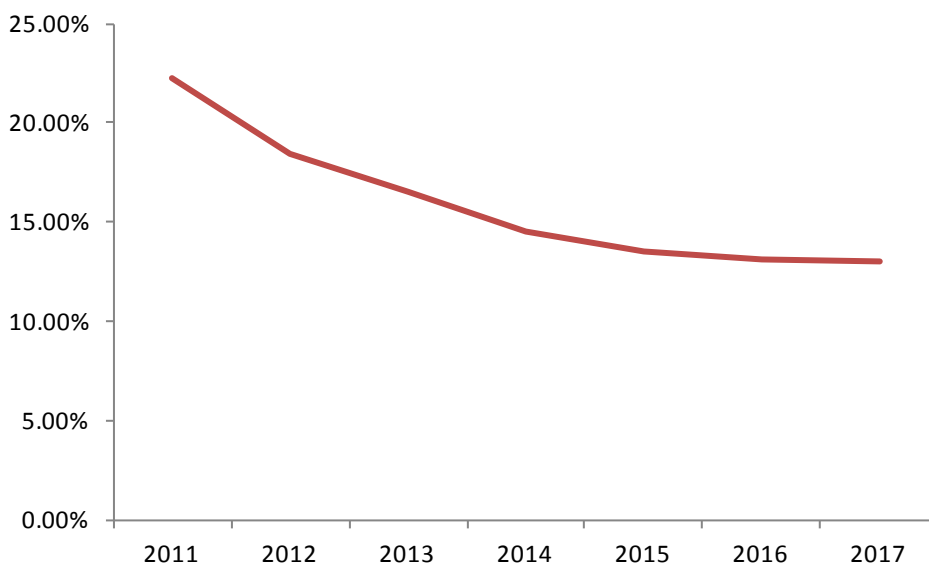
Figure 10: Share of mobile pc and tablet to all mobile broadband

In order to be useful for link dimensioning, the peak traffic demand needs to be derived from this data. The data was therefore rescaled to kbit/s. Because of the distribution of demand for traffic throughout the day a 7% share during busy hour was taken into account. We assumed an even distribution of customers per radio base station and an extra heavy tailing factor of 3 times of the "normal" demand. This heavy tailing factor was used to take into account the specifics of the distribution of traffic between access sites (radio base stations). This approach includes the risk of potential overdimensioning in parts of the aggregation stages.

To overcome the issue of potential overdimensioning, real data concerning the traffic per radio base station were analysed. A large difference in traffic load between individual radio base stations was discovered. The radio base stations with the highest traffic (top 5% and top 10%) have around 20 times and 10 times more traffic than an average radio base station. There is also a large difference in between the distribution of radio base stations to pre-aggregation sites. To take this into account, the following distribution between types of radio base stations in one access ring connecting the base stations to the pre-aggregation site was taken into account: 15% top 5 + 15% top 10 + 70% normal traffic of respective radio base station types (Mix 70/15/15).

The evolution of the total traffic during busy hour per radio base station is given in Mbit/s in Figure 11. It takes into account an average growth rate of 25% per year over the period 2012-2017. The dotted line is used to illustrate the evolution of traffic per radio base station. This traffic estimation per radio base station will be used in the further analysis.
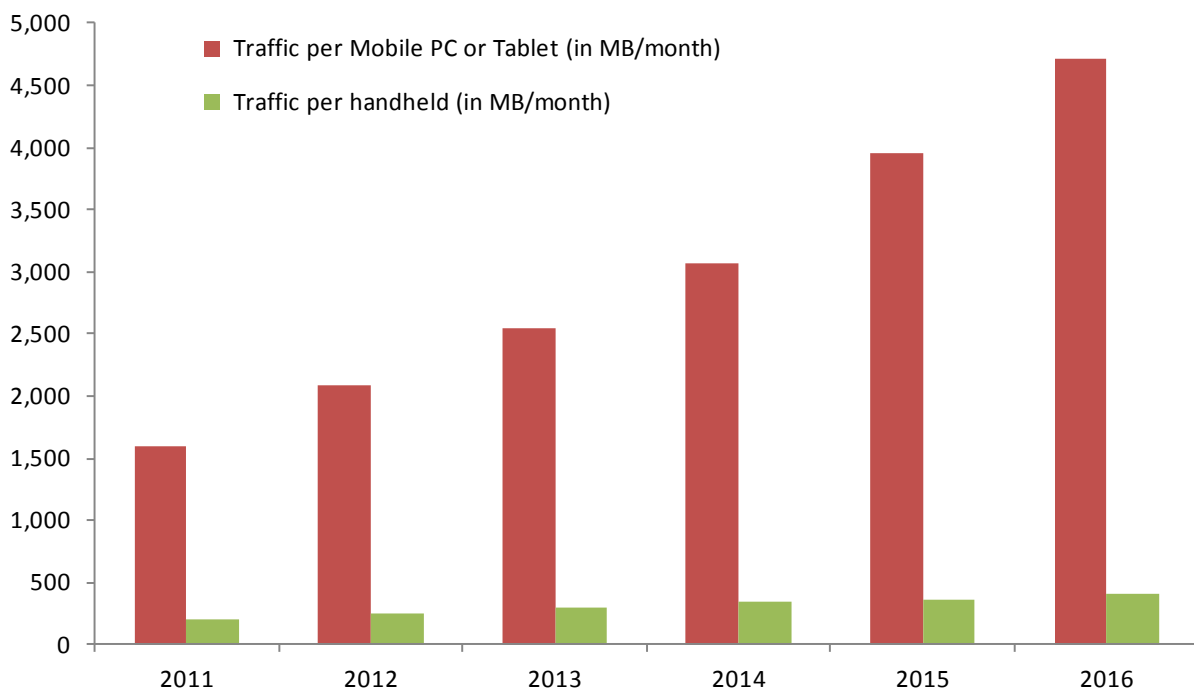
Figure 11: Traffic per mobile broadband category (in MB/month)

Each of the 5 access rings has to support traffic from 5 radio base stations. Each of the pair of switches at the pre-aggregation site has to support traffic from 5 access rings which sums up to 25 radio base stations. Each of the 4 aggregation rings has to support traffic from 4 pre-aggregation sites which is equivalent to 100 radio base stations and each of the pair of switches at the aggregation site has to support traffic from 16 pre-aggregation sites which is equivalent to 400 radio base stations.
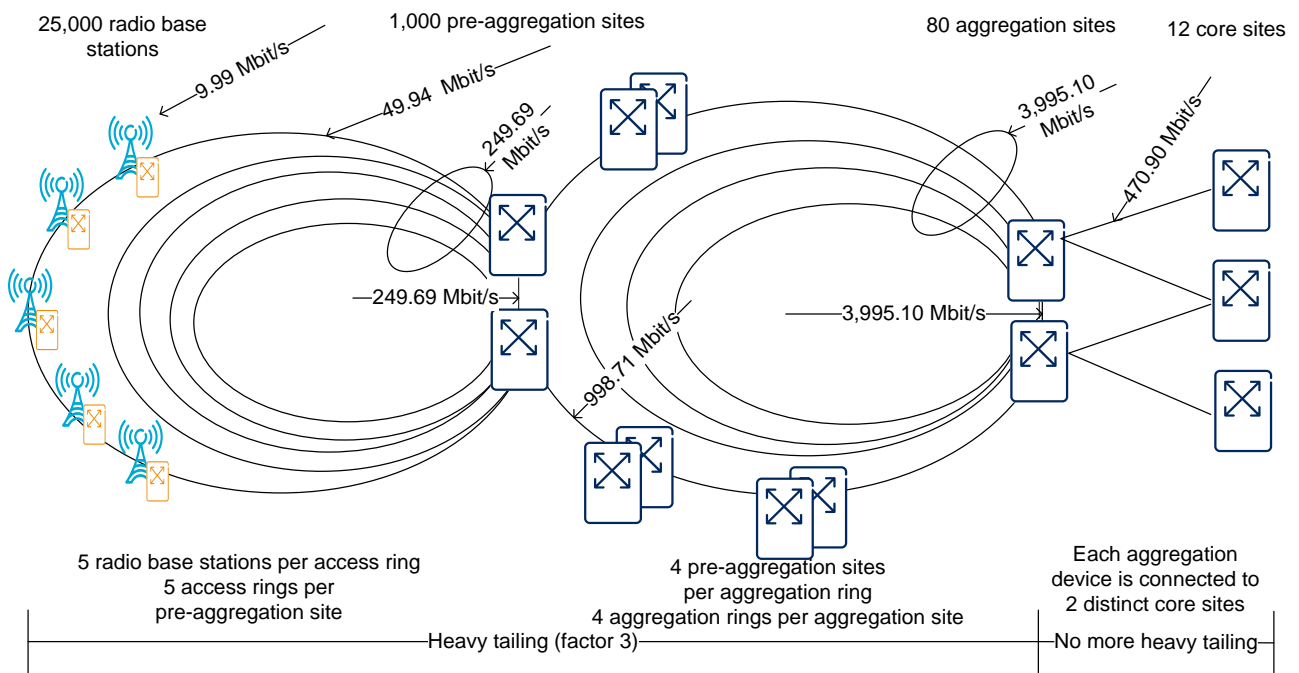
Figure 12: Schematic overview of traffic sources and traffic aggregation for 2011

More interesting for the dimensioning of the devices and links is the expected traffic for the last period (2017). Each of the devices is required to be able to handle the traffic as illustrated in Figure 13.
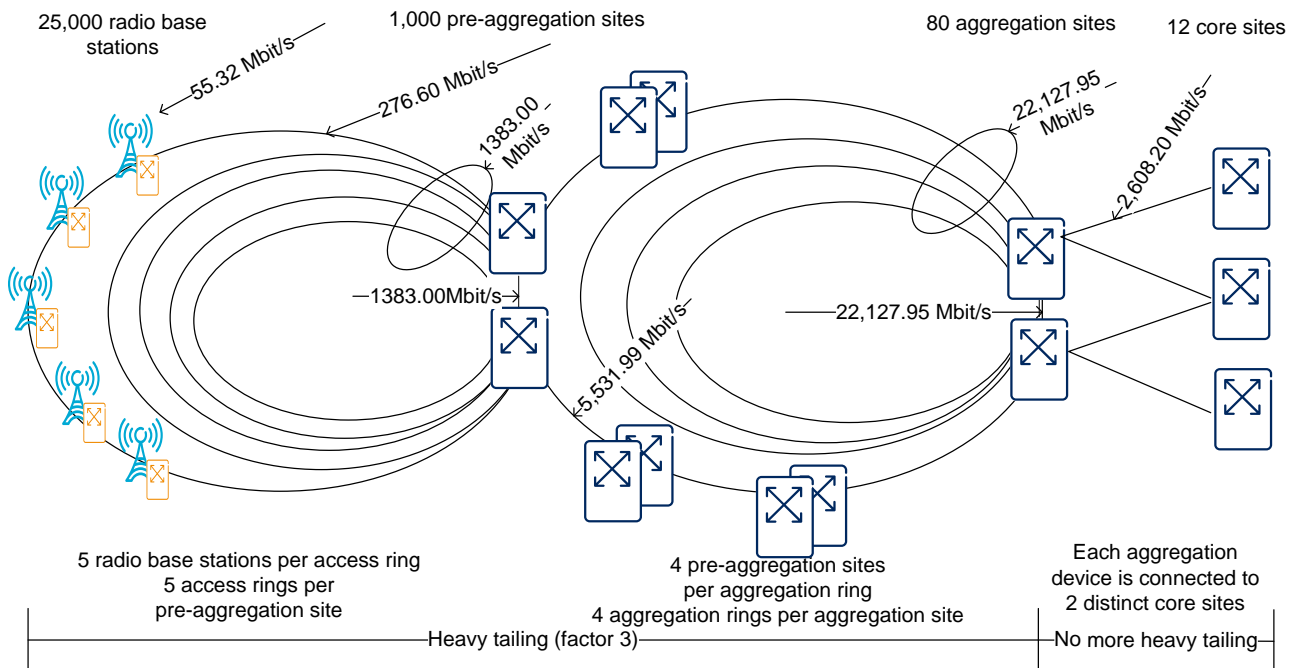
Figure 13: Overview of traffic sources and traffic aggregation for 2017

The effect of an unequal distribution of traffic between radio base stations is no longer relevant when traffic from over 400 radio base stations is aggregated. Therefore neither additional "heavy tailing factors", nor specifics of the distribution of radio base stations are considered northbound the aggregation sites.

3.7   **Capital expenditures for a German reference case**

3.7.1   **Pre-aggregation and aggregation locations**

This analysis considers the pre-aggregation and aggregation stages of the mobile network as a potential target for software defined networking. The wholesale price list of a network equipment vendor without any discounts has been used to complete the shopping list. All prices have been randomized but are never more than 25% different from the list price. The same randomization factor has been applied to similar components (e.g. all interfaces were altered by the same factor). These steps were required because the data used is considered confidential.

For the design of the pre-aggregation locations and the aggregation locations we have selected network devices for a device platform that gives ITU-T G.8032 support and synchronization with IEEE 1588 v2. Next to the operating system, IEEE 1588 license and a Virtual Private Network (VPN) license are required in the classical scenario. The IEEE 1588 license enables the IEEE 1588-2008 protocol to distribute precision time and frequency across the network (synchronisation). The VPN license enables full-scale VPN routing and forwarding (VRF) instances per line card.

3.7.2   **Classical scenario**

For the classical scenario a small size router is deployed in both the pre-aggregation and aggregation locations. The small size router has a basic chassis with an integrated route processer. It delivers 120Gbps of non-blocking, full-duplex fabric capacity. It takes 2 rack units to store. The small size router can support two 1GbE or 10 GbE line cards. The base chassis has four integrated 10GbE Small Form-Factor Pluggable (SFP) ports.

Each location has two routers for redundancy reasons in case of a single node failure.

In the pre-aggregation network devices one 20-port Gigabit Ethernet line card with 1000BASE-SX MMF interface for connection between the network devices and 1000BASE-EX SMF interface for the connection with both access- and aggregation rings is selected.

A shopping list for interfaces per device of the pre-aggregation is given in the table below. Note that the capacity is increased each time traffic demand exceeds the available capacity.

Table 1: Interfaces required for pre-aggregation site router

Pre-aggregation shopping list for interfaces		2012	2013	2014	2015	2016	2017
Interfaces for access rings	1GbE	5	5	5	5	5	5
Interfaces between devices	1 GbE	1	1	2	2	2	2
Interfaces for aggregation rings	1 GbE	2	3	4	5	5	6
Total	**1 GbE**	**8**	**9**	**11**	**12**	**12**	**13**

A bill of material for one of the devices at a pre-aggregation sites for the classical scenario can be found in the table below. Costs are based on internally available reference price lists from different vendors and suppliers. An average was calculated. Remember that each of the pre-aggregation sites has a pair of devices for redundancy purposes and that there are a total of 1,000 pre-aggregation sites.

Table 2: Shopping list for router at pre-aggregation site (classical scenario)

pre-aggregation sites classical scenario

	2012	2013	2014	2015	2016	2017
Small size router (compact design)	1	1	1	1	1	1
Power Supply	1	1	1	1	1	1
Cable Management Tray	1	1	1	1	1	1
Power Cord 25Vac Europe	1	1	1	1	1	1
Fan Tray	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support	1	1	1	1	1	1
VPN license (system)	1	1	1	1	1	1
Line Card 20x1GbE	1	1	1	1	1	1
1000BASE-SX MMF (550m)	1	1	2	2	2	2
1000BASE-EX SMF (40km)	7	8	9	10	10	11
Total	€ 105,992	€ 107,775	€ 110,047	€ 111,829	€ 111,829	€ 113,612

In the aggregation network devices, integrated ports with 10GBASE-SR MMF interfaces are used for the connection between devices in each location and two 20-port Gigabit Ethernet line cards with 1000BASE-EX SMF are used for all other connections. A shopping list for interfaces per device of the pre-aggregation is given in the table below. Note that the capacity is increased each time traffic demand exceeds the available capacity. The choice for 10 GbE interfaces between the devices was logic given the availability of four integrated 10 GbE ports in the chosen small size router.

Table 3: Interfaces required for aggregation site router

Aggregation shopping list for interfaces		2012	2013	2014	2015	2016	2017
Interfaces for aggregation rings	1GbE	8	12	16	20	20	24
Interfaces between devices	10 GbE	1	2	2	2	2	3
Interfaces for core mesh	1 GbE	1	2	2	2	3	3
Interfaces for core mesh (redundancy)	1 GbE	1	2	2	2	3	3
Total	**1GbE**	**10**	**16**	**20**	**24**	**26**	**30**
	10 GbE	**1**	**2**	**2**	**2**	**2**	**3**

A bill of material for one of the devices at an aggregation site for the classical scenario can be found in the table below. Remember that each of the aggregation sites has a pair of devices for redundancy purposes and that there are 80 aggregation sites.

Table 4: Shopping list for router at aggregation site (classical scenario)

aggregation sites classical scenario

	2012	2013	2014	2015	2016	2017
Small size router (compact design ʋ	1	1	1	1	1	1
Power Supply	1	1	1	1	1	1
Cable Management Tray	1	1	1	1	1	1
Power Cord 25Vac Europe	1	1	1	1	1	1
Fan Tray	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support	1	1	1	1	1	1
VPN license (system)	1	1	1	1	1	1
Line Card 20x1GbE	1	1	1	2	2	2
1000BASE-ZX-SMF (70km)	10	16	20	24	26	30
1000BASE-SX MMF (550m)	0	0	0	0	0	0
10GBASE-ZX SMF (70km)	0	0	0	0	0	0
10GBASE-SR-MMF (550m)	1	2	2	2	2	3
	€ 130,000	€ 152,713	€ 166,977	€ 189,767	€ 196,899	€ 212,481

3.7.3   Software defined networking effects at the aggregation sites

Capital expenditures can be reduced in the SDN scenario compared to the classical scenario because the control logic is removed from the switch and shifted to a SDN controller. This allows the use of simpler and cheaper devices in the network. The routers in the SDN scenario function as OpenFlow enabled switches.

Even though the support from vendors for OpenFlow is increasing we could not find any OpenFlow enabled switches with complete specifications that could meet the requirements for the network under consideration. Therefore we had to model the routers as if they were OpenFlow enabled (which we assumed can be done by the vendor via a firmware upgrade, but is open for further analysis).

Once the network devices are OpenFlow enabled the SDN controller will take over the control plane functionality like maintaining routing databases from the routers. By removing the control functionality from the routers they turn into no more than a switch that handles forwarding decisions. This is modelled by removing the cost for software licenses responsible for the functioning of the control logic from the shopping list for network devices. The networking devices require three types of software: an Operating System (OS) for the router, a license for synchronisation support (IEEE 1588 support) and a VPN license. The license for synchronisation is a hardware feature and is required. VPN licenses can be replaced by custom written software. The software development cost is modelled, assuming good open source software exists, as a fixed fee per year for 10 full time software designers. We expect the OS to be simpler as it requires less capabilities, fewer updates and modifications. This was modelled by reducing the cost of the OS with 25 per cent. These assumptions and their effect on total cost are further investigated using sensitivity analysis in section 3.9.3.

The proposed bill of material and shopping list for a SDN enabled small sized router at a pre-aggregation site and an aggregation site can be found in the tables below. The changes relative to the classical scenario are highlighted. Not that there are only cost reductions in the pre-aggregation and aggregation sites. The SDN controllers are located at the core locations. The core components will therefore have both cost reductions as well as extra costs related to SDN.

Table 5: Shopping list for router at pre-aggregation site (SDN scenario)

pre-aggregation sites SDN scenario

	2012	2013	2014	2015	2016	2017
Small size router (compact design v	1	1	1	1	1	1
Power Supply	1	1	1	1	1	1
Cable Management Tray	1	1	1	1	1	1
Power Cord 25Vac Europe	1	1	1	1	1	1
Fan Tray	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support	1	1	1	1	1	1
VPN license (system)	0	0	0	0	0	0
Line Card 20x1GbE	1	1	1	1	1	1
1000BASE-SX MMF (550m)	1	1	2	2	2	2
1000BASE-EX SMF (40km)	7	8	9	10	10	11
	€ 85,837	€ 87,620	€ 89,891	€ 91,674	€ 91,674	€ 93,457

Table 6: Shopping list for router at aggregation site (SDN scenario)

aggregation sites SDN scenario

	2012	2013	2014	2015	2016	2017
Small size router (compact design v	1	1	1	1	1	1
Power Supply	1	1	1	1	1	1
Cable Management Tray	1	1	1	1	1	1
Power Cord 25Vac Europe	1	1	1	1	1	1
Fan Tray	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support	1	1	1	1	1	1
VPN license (system)	0	0	0	0	0	0
Line Card 20x1GbE	1	1	1	2	2	2
1000BASE-ZX-SMF (70km)	10	16	20	24	26	30
1000BASE-SX MMF (550m)	0	0	0	0	0	0
10GBASE-ZX SMF (70km)	0	0	0	0	0	0
10GBASE-SR-MMF (550m)	1	2	2	2	2	3
	€ 109,845	€ 132,558	€ 146,822	€ 169,612	€ 176,744	€ 192,326

3.7.4   Mobile core components

For the mobile core components a multimedia core platform of the same vendor is assumed. The platform could cover with the following functions:

- Long Term Evolution (LTE) Evolved Packet Core (EPC)
    - Mobility Management Entity (MME)
    - Serving Gateway (SGW)
    - Packet Data Network Gateway (PGW)
        - For policy and charging enforcement function (PCEF)
        - Manages quality of service (QoS)
        - Provides deep-packet inspection and lawful intercept
    - Evolved Packet Data Gateway (ePDG)
- Universal Mobile Telecommunications Service (UMTS) with High-Speed Packet Access (HSPA)
    - Serving GPRS Support Node (SGSN)
    - Gateway GPRS Support Node (GGSN)

The multimedia platform combines the network functions such as the voice and packet gateway function for 3G and Long Term Evolution (LTE) in a single specialized hardware platform. A performance test for a comparable, but not

necessarily the same multimedia platform is available by EANTC and Light Reading [5][6]. The test emulated 16 large base stations each of which emulated 62,500 subscribers to emulate a total of over 1 million mobile handsets for voice and data traffic with 20Gbit/s of throughput. Our assumptions are based on this analysis:

- One device supports up to one million subscribers

- One device is capable of 20 Gbit/s throughput (bi-directional)

Each multimedia platform has 14 Packet Service Cards (PSC) which is important for packet and call processing. One or two line cards can be attached to a PSC. A 1:1 and M:N redundancy environment is created at the card level. This complete 1:1 redundancy limits the capacity per device to 10 Gbit/s or 0.7 Gbit/s per PSC (requires two independent 1GbE interfaces).

In 2017, the total number of customers is at around 38 million (Figure 9). This is an average of around 3.5 million subscribers for each of the 12 core locations. The following design rules were kept in mind:

- Each inner core location is a mobile core location

- Each inner core location requires the multimedia platform as mobile core elements 2nd level (GGSN/PDG/etc.)

- Each inner core location must provide redundant capacity for mobile core elements 2nd level for one other inner core location

- Each inner core location provides capacity to all 5 other inner core locations for 5/6 of total traffic

- Each inner core location must be able to carry all traffic to the internet

3.7.5   Design of core locations

Each of the 12 core locations is connected to 14 aggregation sites (7 normal operating and 7 for redundancy). In addition each of the core locations is connected to two inner core locations (at disjoint location or at same location as core location) and to the mobile core elements (1st level). This is illustrated in Figure 13. Relative to the classical scenario (left part of Figure 14), a SDN controller is located at each core location in the SDN scenario (right part of Figure 14). The SDN controllers are located at the core 12 and 6 inner core locations. The OpenFlow enabled switches are able to talk to the controller through in-band control. The ratio of SDN controllers to OpenFlow switches was estimated at 1 to 100. This estimate is based on the rather simple and static network design under consideration. This will limit the networking dynamics and decreases performance requirements for a SDN controller. For the SDN scenario two SDN controllers are added to each of the 12 mobile core locations. These can serve a total of 2400 switches (2160 for the network design under consideration). The price for a SDN controller is estimated to be in line with the price of the NEC Univerge PF 6800 ProgrammableFlow controller. Each SDN controller is duplicated to eliminate a single point of failure. The effect of this assumption on total cost has been tested in section 3.9.3.

12 location in classical scenario   12 location in SDN scenario
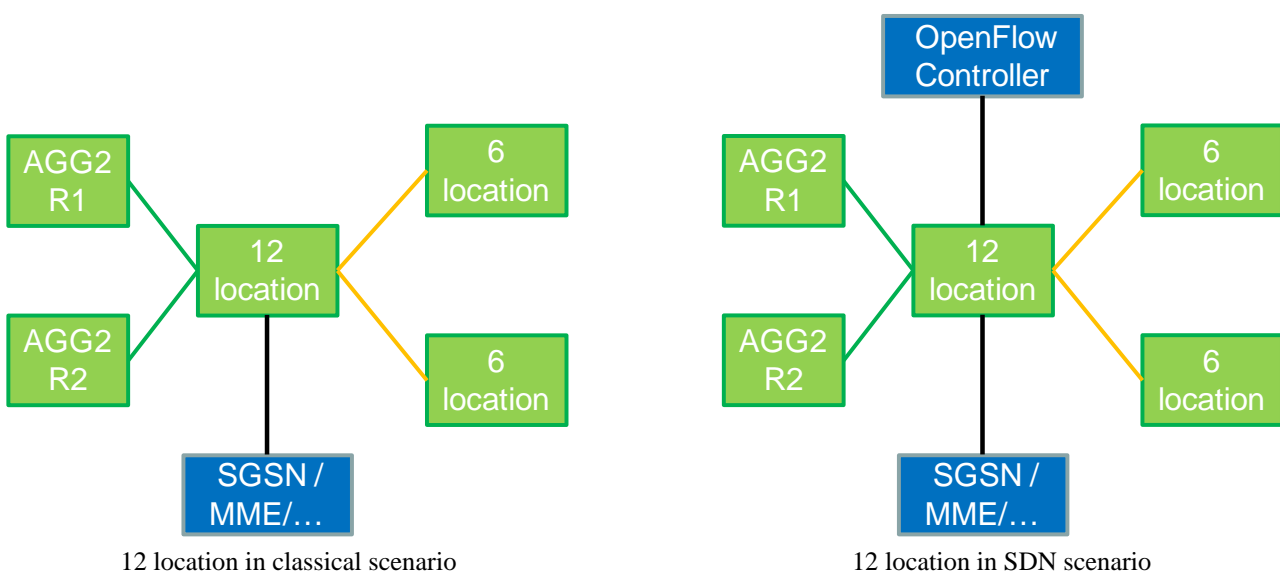
Figure 14: Design of core location in classical- and SDN scenario

The number of multimedia platform devices per core location is dependent on:

- The number of subscribers per core location → max 1 million per multimedia platform device (no redundancy)

Table 7: Number of multimedia platform devices required for subscriber handling (including redundancy)

	2012	2013	2014	2015	2016	2017
Number of subscribers (including redundancy) (see Figure 9 in million)	3.98	5.15	5.79	6.16	6.29	6.36
Number of subscribers per multimedia platform device (in million)	1.00	1.00	1.00	1.00	1.00	1.00
Number of multimedia platform devices required for subscriber handling (including redundancy)	**4**	**6**	**6**	**7**	**7**	**7**

- The traffic volume per core location → max 10 Gbit/s per multimedia platform device (redundancy included)

Table 8: Number of multimedia platform devices for traffic per core location

	2012	2013	2014	2015	2016	2017
Traffic per core location (uplink to inner core location, in Gbit/s)*	6.13	9.01	11.02	13.61	15.85	18.26
Capacity per multimedia platform device (including spare capacity for redundancy, in Gbit/s)	10.00	10.00	10.00	10.00	10.00	10.00
Number of multimedia platform devices for traffic per core location	**1**	**1**	**2**	**2**	**2**	**2**

* Total traffic in backhaul/12, no heavy tailing, no mix 70/15/15

Number of PSC per core location → max 14 PSC per multimedia platform device

Table 9: Number of multimedia platform devices required for PSC

	2012	2013	2014	2015	2016	2017
Traffic per core location (uplink to inner core location, in Gbit/s) *	6.13	9.01	11.02	13.61	15.85	18.26
Capacity per PSC from multimedia platform device (in Gbit/s)	1.40	1.40	1.40	1.40	1.40	1.40
Number of PSC for traffic at core location	4.38	6.44	7.87	9.72	11.32	13.04
Number of PSC for traffic at core location (redundancy)	4.38	6.44	7.87	9.72	11.32	13.04
Total number of PSC	8.75	12.87	15.74	19.44	22.65	26.08
Number of PSC per multimedia platform device	14	14	14	14	14	14
Number of multimedia platform devices required for PSC	**1**	**1**	**2**	**2**	**2**	**2**

The highest value of these 3 factors is determining the number of required multimedia platform devices.

Table 10: Determination of required multimedia plaform devices

	2012	2013	2014	2015	2016	2017
Number of multimedia platform devices required for subscriber handling (inclusive redundancy)	**4**	**6**	**6**	**7**	**7**	**7**
Number of multimedia platform devices for traffic per core location	1	1	2	2	2	2
Number of multimedia platform devices required for PSC	1	1	2	2	2	2

The choice of routers for the core locations is dependent on the selection of the interfaces (1 GbE or 10 GbE). After considering different options a medium size router with 40 x 1 GbE Ethernet line card was chosen. The table below gives an overview of the chosen interfaces per core location.

Table 11: Number of interfaces for routers at 12 core location

Number of interfaces		2012	2013	2014	2015	2016	2017
From aggregation sites	1 GbE	7	14	14	14	21	21
From aggregation sites (redundant)	1 GbE	7	14	14	14	21	21
For PSC	1GbE	13	19	23	28	33	38
For inner core location	1 GbE	7	10	12	14	16	19
For inner core location (redundant)	1 GbE	7	10	12	14	16	19
Total	**1GbE**	**45**	**71**	**79**	**88**	**111**	**122**

The resulting shopping list for a core location site router in the classical scenario is given in the table below. Please keep in mind that each inner core location is also a core location. Of the 12 core locations only 6 are therefore pure core locations while the other 6 locations are modelled as inner core locations.

Table 12: Shopping list for router at 12 core location (classical scenario)

core 12 sites classical scenario

	2012	2013	2014	2015	2016	2017
Medium size router	1	1	1	1	1	1
Power Supply	1	1	1	1	1	1
Fan Tray	2	2	2	2	2	2
Fan Filter	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support (system)	1	1	1	1	1	1
VPN license (line card)	2	2	2	3	3	3
Route Switch Processor	1	1	1	1	1	1
Line Card 40x1GbE	2	2	2	3	3	3
1000BASE-SX MMF (550m)	13	19	23	28	33	38
Line Card 24x1GbE	0	0	0	0	0	0
10GBASE-ZX SMF (70km)	0	0	0	0	0	0
1000BASE-ZX-SMF (70km)	28	48	52	56	74	80
	€ 233,147	€ 307,395	€ 323,612	€ 369,775	€ 436,403	€ 460,240

3.7.6   Software defined networking effects at the core sites

The core routers are modelled as OpenFlow enabled switches by deleting the unnecessary software licenses from the bill of material. Further, extra transceivers are required for the connections with the SDN controllers.

The ratio of SDN controllers to OpenFlow switches was estimated at 1 to 100. This estimate is based on the rather simple and static network design under consideration. This will limit the networking dynamics and decreases performance requirements for a SDN controller. For the SDN scenario two SDN controllers are added to each of the 12 mobile core locations (6 core locations and 6 inner core locations). These can serve a total of 2400 switches (2160 for

the network design under consideration). The SDN controllers are located at the core locations. The OpenFlow enabled switches are able to talk to the controller through in-band control.

The adapted bill of material for the SDN scenario can be found in the table below. The changes related to the classical scenario are highlighted. Note the requirement for 4 extra transceivers for the extra connections with the SDN controllers.

Table 13: Shopping list for router at 12 core location (SDN scenario)

core 12 sites SDN scenario

	2012	2013	2014	2015	2016	2017
Medium size router	1	1	1	1	1	1
Power Supply	1	1	1	1	1	1
Fan Tray	2	2	2	2	2	2
Fan Filter	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support (system)	1	1	1	1	1	1
VPN license (line card)	0	0	0	0	0	0
Route Switch Processor	1	1	1	1	1	1
Line Card 40x1GbE	2	2	2	3	3	3
1000BASE-SX MMF (550m)	17	23	27	32	37	42
Line Card 24x1GbE	0	0	0	0	0	0
10GBASE-ZX SMF (70km)	0	0	0	0	0	0
1000BASE-ZX-SMF (70km)	28	48	52	56	74	80
	€ 207,969	€ 282,217	€ 298,434	€ 336,070	€ 402,698	€ 426,535

3.7.7 Design of inner core locations

Each of the inner core locations is connected to several core locations (at a disjoint location or at the same location). In addition each of the inner core locations is connected to another inner core location and to the mobile core elements (1st level) and the internet. This is illustrated in Figure 15. Relative to the classical scenario (left), a SDN controller is located at each (inner) core location in the SDN scenario (right). An extra SDN controller is added in the SDN scenario for redundancy.

6 location in classical scenario   6 location in SDN scenario
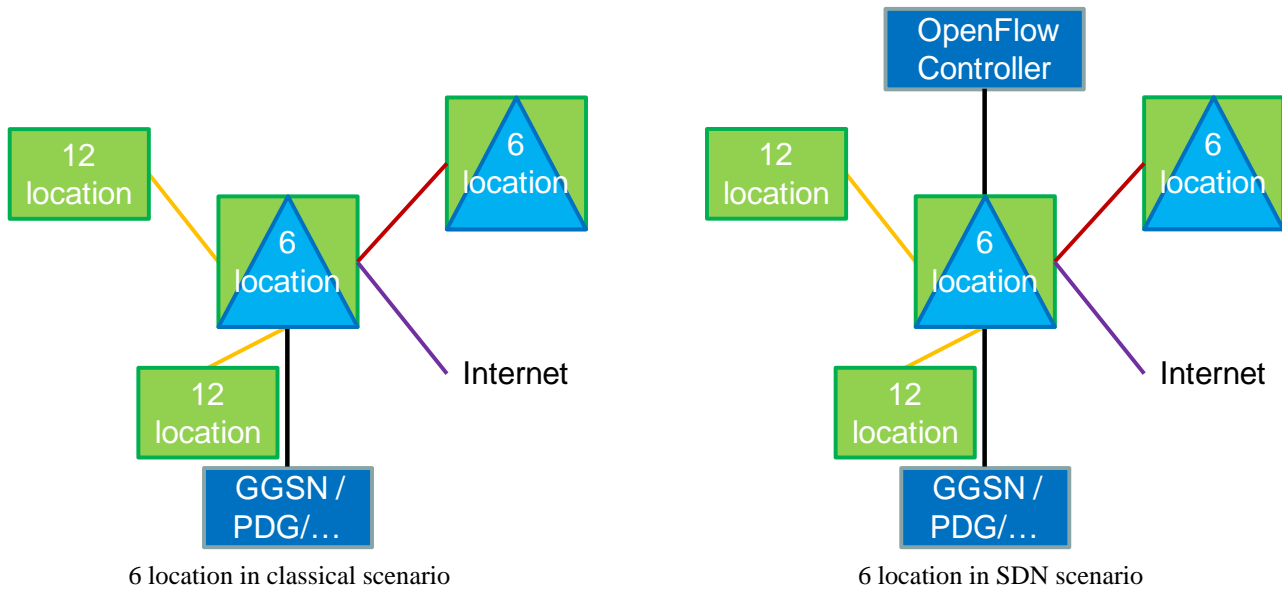
Figure 15: Design of inner core location in classical- and SDN scenario

The number of multimedia platform devices per inner core location is depending on:

1. The number of subscribers per inner core location → max. 1 million per multimedia platform device (no redundancy)

Table 14: Number of multimedia platform devices required for subscriber handling (inclusive redundancy)

	2012	2013	2014	2015	2016	2017
Number of subscribers (including redundancy) (see Figure 9, in million)	7.96	10.34	11.57	12.32	12.57	12.72
Number of subscribers per multimedia platform device (in million)	1.00	1.00	1.00	1.00	1.00	1.00
Number of multimedia platform devices required for subscriber handling (inclusive redundancy)	**8**	**11**	**12**	**13**	**13**	**13**

2. The amount of traffic per inner core location → max 10 Gbit/s per multimedia platform device (redundancy included)

Table 15: Number of multimedia platform devices for traffic per core location

	2012	2013	2014	2015	2016	2017
Required throughput of core location (in Gbit/s)	6.13	9.01	11.02	13.61	15.85	18.26
Required throughput of inner core location for mobile core functions* (inclusive redundancy, in Gbit/s)	36.77	54.06	66.12	81.66	95.13	109.54
Capacity per multimedia platform device (including spare capacity for redundancy, in Gbit/s)	10.00	10.00	10.00	10.00	10.00	10.00
Number of multimedia platform devices for traffic per core location	**4**	**6**	**7**	**9**	**10**	**11**

* requires bandwidth of core location for mobile core network 1st level + 2 times bandwidth of core location for mobile core network 2nd level

3. The number of PSC per inner core location → max 14 PSC per multimedia platform device

Table 16: Number of multimedia platform devices required for PSC

	2012	2013	2014	2015	2016	2017
Traffic per inner core location (in Gbit/s)	36.77	54.06	66.12	81.66	95.13	109.54
Capacity per PSC from multimedia platform device (in Gbit/s)	1.40	1.40	1.40	1.40	1.40	1.40
Number of PSC for traffic at core location	52.53	77.22	94.46	116.65	135.90	156.49
Number of PSC for traffic at core location (redundancy)	52.53	77.22	94.46	116.65	135.90	156.49
Total number of PSC	106	155	189	234	272	313
Number of PSC per multimedia platform	14	14	14	14	14	14
Number of multimedia platform devices required for PSC	**8**	**12**	**14**	**17**	**20**	**23**

The maximum of these 3 factors defines the required number of multimedia platform devices.

Table 17: Number of multimedia platform devices required for PSC

	2012	2013	2014	2015	2016	2017
Number of multimedia platform devices required for subscriber handling (inclusive redundancy)	8	11	12	13	13	13
Number of multimedia platform devices for traffic per core location	4	6	7	9	10	11
Number of multimedia platform devices required for PSC	**8**	**12**	**14**	**17**	**20**	**23**

The choice of routers for the inner core locations is dependent on the selected of interfaces (1 GbE or 10 GbE). After considering different options a pair of large size router devices was chosen for each inner core location. The table below gives an overview of the selected interfaces per inner core location.

Table 18: Number of interfaces for routers at inner core location

Number of interfaces		2012	2013	2014	2015	2016	2017
For core location part							
From aggregation sites	10 GbE	7	7	7	7	7	7
From aggregation sites (redundant)	10 GbE	0	0	0	0	0	0
For inner core location part							
For PSC	1GbE	75	109	133	164	191	220
For core location	10 GbE	1	1	2	2	2	2
For core location (redundant)	10 GbE	0	0	0	0	0	0
For inner core location mesh connectivity	10 GbE	5	5	6	7	8	10
For internet connectivity	10 GbE	5	6	7	9	10	11
Sum	**1GbE**	**75**	**109**	**133**	**164**	**191**	**220**
	10 GbE	**18**	**19**	**22**	**25**	**27**	**30**

The resulting bill of material for an inner core location site router is listed in the table below. Keep in mind that each inner core location has a pair of these devices. So the cost has to be doubled.

Table 19: Shopping list for router at inner core location (classical scenario)

core 6 sites classical scenario

	2012	2013	2014	2015	2016	2017
Large size router	1	1	1	1	1	1
Power Supply	2	2	2	2	2	2
Fan Tray	2	2	2	2	2	2
Fan Filter	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support (system)	1	1	1	1	1	1
VPN license (line card)	3	4	5	7	7	8
Route Switch Processor	1	1	1	1	1	1
Line Card 40x1GbE	2	3	4	5	5	6
1000BASE-SX MMF (550m)	75	109	133	164	191	220
Line Card 24x1GbE	1	1	1	2	2	2
10GBASE-ZX SMF (70km)	5	6	7	9	10	11
1000BASE-ZX-SMF (70km)	13	13	15	16	17	19
	€ 491,178	€ 538,558	€ 605,860	€ 821,310	€ 848,217	€ 917,961

3.7.8 Software defined networking effects at the inner core sites

The inner core routers are modelled as OpenFlow enabled switches by deleting unnecessary software licenses from the bill of material. Further, extra transceivers are required for the connections with the SDN controllers.

Table 20: Shopping list for router at inner core location (SDN scenario)

core 6 sites SDN scenario

	2012	2013	2014	2015	2016	2017
Large size router	1	1	1	1	1	1
Power Supply	2	2	2	2	2	2
Fan Tray	2	2	2	2	2	2
Fan Filter	1	1	1	1	1	1
Router OS	1	1	1	1	1	1
IEEE 1588 Support (system)	1	1	1	1	1	1
VPN license (line card)	0	0	0	0	0	0
Route Switch Processor	1	1	1	1	1	1
Line Card 40x1GbE	2	3	4	5	5	6
1000BASE-SX MMF (550m)	77	111	135	166	193	222
Line Card 24x1GbE	1	1	1	2	2	2
10GBASE-SX MMF (550m)	5	6	7	9	10	11
10GBASE-ZX-SMF (70km)	13	13	15	16	17	19
	€ 463,473	€ 502,326	€ 561,101	€ 759,496	€ 786,403	€ 847,620

The Software Defined Networking scenario also requires the introduction of the SDN controllers and the development of customized software. The software development cost model it is assumed that high quality open source software exists and would be available for a fixed fee per year, equivalent to the cost of 10 full time software designers. A total of 48 SDN controllers are located at the core locations.

The price point for a SDN controller is estimated to be in line with the price of the NEC Univerge PF 6800 ProgrammableFlow controller and the IBM Programmable Network Controller. The average of both price points is assumed. Each SDN controller is duplicated to eliminate a single point of failure.

Table 21: Shopping list for SDN controller at inner core location

SDN components

	2012	2013	2014	2015	2016	2017
Core Location OpenFlow Controller	1	1	1	1	1	1
Core Location Transceiver	1	1	1	1	1	1
Inner Core Location OpenFlow Controller	1	1	1	1	1	1
Inner Core Location Transceiver	1	1	1	1	1	1
Total	€ 74,558	€ 74,558	€ 74,558	€ 74,558	€ 74,558	€ 74,558
Fixed fee for software development*	1	2	3	4	5	6
Total	€ 1,500,000	€ 3,000,000	€ 4,500,000	€ 6,000,000	€ 7,500,000	€ 9,000,000

* the software development cost is capitalized each year

3.8 Operational expenditures for a German reference case

In order to come up with a meaningful estimate for operational expenditures a large set of parameters had to be collected. The input values are based on expert knowledge and input from different partners of the SPARC consortium. Each of the operational processes is hereafter explained in more detail and the relevant parameters are quantified.

The set of parameters consists out of the following topics:

- General parameters
  - Cost of floor space
  - Cost of power
  - Cost of cooling
- Maintenance and repair
  - Network care

  - o   Network software upgrades and patches

  - o   Travel by technicians to the place of failure, fixing the failure and testing to verify repair

  - o   Service provisioning

  - o   Service management

- Up-front network planning

And will be described in detail in the following section.

General parameters

Inflation is accounted for a yearly cost of 3%. Cost of hardware and human capital are both corrected for inflation with the same rate.

General parameters	
inflation (per year in percent)	3
hourly wage of employee in customer service (in euro)	45.00
hourly wage of employee in network operations center (in euro)	58.00
hourly wage of field technician (in euro)	52.00

Operational process continuous cost of infrastructure is subdivided in three subcategories:

Cost of floor space

The cost of floor space is subdivided in several categories. A category per type of site (pre-aggregation, aggregation, core and inner core) has been used to take into the different geographic situation across sites. Typically most of pre-aggregation- and aggregation sites are located in dense urban geographic locations and small parts are located in urban locations with lower rent prices. All core- and inner core locations are typically located at dense urban areas with higher rent prices.

Cost of floor space = number of devices x rack space in m2 x correction factor x yearly rent per m²

Number of devices to calculate floor space	
number of devices pre-aggregation	2000
number of devices aggregation	160
number of devices core	12
number of devices inner core	24
number of SDN controllers	48
ratio urban/dense urban pre-aggregation sites and aggregation sites (in %)	15/85
ratio urban/dense urban core sites (in %)	0/100
yearly rent urban (in euro)	170.00
yearly rent dense urban (in euro)	220.00
correction factor	2.65
rack space (in m^2)	0.78

Cost of power and cost of cooling

The cost of power and the cost of cooling are taken together. The cost of power does include the cost of backup power supply. The cost of power per device is based on the power required by the router, line cards and the route switch processor. Because of periodic upgrades of hardware (with extra line cards) the cost of power will also increase.

Cost of power and cooling = number of devices x yearly consumption per device (in kW) x cost per kW per year

Parameters to calculate cost of power and of cooling	
consumption of devices pre-aggregation	
Router, compact design with integrated route switch processor, backplane, power supply, fan tray, etc. (in kW)	335
Line card 20x1 GbE (in kW per line card)	420
consumption of devices aggregation	
Router, 6 slot, incl. basic components (in kW)	375
Route Switch Processor (in kW)	235
Line card 40x1 GbE (in kW per line card)	350
consumption of devices core and inner core	
Router, 10 slot, incl. basic components (in kW)	600
Route Switch Processor (in kW)	235
Line card 40x1 GbE (in kW per line card)	350
Line card 24x10 GbE (in kW per line card)	895
consumption of SDN controllers (in kW)	660
yearly price per kW (in euro)	2700.00

Maintenance and repair

This subcategory is again split up in 5 categories:

Network care

Network care is considered as a process done by the network operations center which is active 24/7. This is typically done by having 5 shifts with an adequate number of full time employees (which is here estimated at 10).

Network care = number of shifts x hours per year per shift x employees per shift x wage per hour for employee at network operations center

Parameters to calculate network care	
number of shifts	5
hours per year per shift (in hour)	1,976
employees per shift (in full time employees)	10

Network software upgrades and patches

A yearly inventory of software components has to be maintained and on a regular basis upgrades and patches need to be installed. This is supposed to be an extra task of the network operations center for which extra employees are hired and trained. This process is expected to be considerably easier with SDN because of the centralization of certain software components (within the SDN controller) which are now distributed such as the VPN license.

Network software upgrades and patches = number of licenses x number of devices x time per license per year (in h) x wage per hour for employee at network operations center

Parameters to calculate software upgrades and patches		
	classical	SDN
number of licenses per pre-aggregation device		
Router OS	1	1
IEEE 1588 Support (for the system)	1	1
VPN license (for the system)	1	0
number of licenses per aggregation device		
Router OS	1	1
IEEE 1588 Support (for the system)	1	1
VPN license (for the system)	1	0
number of licenses core and inner core		
Router OS	1	1
IEEE 1588 Support (for the system)	1	1
VPN license (per line card)	1	0
number of licenses SDN controllers	0	2
time per license per year (in hour)	1.75	

Travel by technicians to the place of failure, fixing the failure and testing to verify repair

Even with careful maintenance occasional failures cannot be avoided. Failures are categorized in two categories: hardware failures and software failures. In case of a hardware failure, broken equipment has to be replaced and the technician needs to go to the location of failure. In case of software failure, the failure is supposed to be solvable by a software upgrade, patch or a reboot. In most cases it will not be required to go down to the actual location because the equipment is remotely available.

Travel by technicians to the place of failure = number of hardware failures x [average distance to the failure (in km) x cost per km + average time to reach the failure location (in hour) x hourly wage]

Fixing the failure = number of hardware failures x (average time to fix the failure x hourly wage of technician + average hardware replacement cost) + number of software failures x average time to fix a software failure x hourly wage of employee at network operations center

Parameters to calculate repair	
Mean Time Between Failures	
Chassis (in hour)	175,200
Ethernet line card (in hour)	110,000
SFP interface (in hour)	300,000
Software (in hour)	110,000
average distance to the failure (in km)	100
cost per km (in euro)	0.40
average time to reach the failure location (in hour)	1
average time to fix the failure (in hour)	3
average hardware replacement cost (in euro)	cost of component that failed
average time to fix a software failure (in hour)	1.75

Service provisioning and service management

Given the mobile backhaul scenario there is no direct contact with customers. A service is here defined as sending a request for configuration between two locations to the entity that is responsible for setting up a single fiber connection between a base station and one of the different locations or between different locations. Service management includes the configuration of the connection and the documentation.

Service provisioning = number of connections to be configured (per year) x configuration time per connection (in hour) x wage per hour for employee at network operations center + number of connections to be configured (per year) x documentation time per connection (in hour) x wage per hour for employee at customer service center

Service management = number of connections to be reconfigured (per year) x configuration time per connection (in hour) x wage per hour for employee at network operations center + number of connections to be reconfigured (per year) x documentation time per connection (in hour) x wage per hour for employee at customer service center.

parameters to calculate service provisioning		
number of connections per pre-aggregation device	classical	SDN
towards radio base station	50,000	50,000
in between pre-aggregation devices	1,000 x number of interfaces between device*	1,000 x number of 1000BASE-SX-MMF (550m)*
to aggregation sites	2,000 x number of interfaces for aggregation rings*	2,000 x number of interfaces for aggregation rings*
number of connections per aggregation device		
in between aggregation devices	80 x number of interfaces between devices*	80 x number of interfaces between devices*
to core sites	160 x number of interfaces for core mesh*	160 x number of interfaces for core mesh*
number of connections per core site		
to local devices	6 x # of interfaces to PSC*	6 x # of interfaces to PSC
to inner core sites	12 x number of interfaces to inner core*	12 x number of interfaces to inner core*
to OF controller	0	24
number of connections per inner core site		
in between inner core devices	6 x number of interfaces between devices*	6 x number of interfaces between devices*
to other 6 locations	15 x number of interfaces for inner core mesh*	15 x number of interfaces for inner core mesh*
to local devices	# of interfaces to PSC *	# of interfaces to PSC*
to OF controller	0	24
to the internet	6 x number of interfaces for internet connectivity*	6 x number of interfaces for internet connectivity*
service planning and management	0.8	0.5
network planning	2.25	1
service accounting and administration	0.8	0.8
number of existing connections that need to be reconfigured (per year)	1 of every 3	1 of every 3

* the number of interfaces can be found in Section 3.7.

Up-front network planning

Up-front network planning is considered as a percentage of capital expenditures and estimated at 7%. Equipment is typically installed by the vendor for a fee.

3.9   **Results**

This section summarizes the advantages of the SDN-scenario for mobile backhauling concerning capital - and operational expenditures. Given the newness of SDN in the context of mobile backhauling we had to make several assumptions which are often based on expert opinions or results from previous preliminary studies. To cope with the uncertainty related to the gathered input we have extended the section with a sensitivity analysis which examines the effects of change in a critical parameter on the overall results.

The results from this study show a clear advantage in both capital expenditures and operational expenditures. It must be noted that the results related to cost savings from this study are highly diverging (a lower level of potential savings) from the results of the previous ACG research study. We traced this divergence to three main reasons:

1. Oversimplified devices in the SDN scenario from the ACG research study in contrast to the classical scenario in which state-of-the art IP/MPLS routers are dimensioned. This enlarges the gap between both scenarios and in particular for capital expenditures.

2. Operational expenditures in the ACG research study are highly correlated with capital expenditures, therefore for both categories of expenditures the same, high level of savings has been found in the ACG research study.

3. This study did not take into account the possibility of cheaper hardware prices because of a higher level of specialisation and the possibility to make interoperability possible. It is however unclear if the ACG research study took these effects into account.

We would like to point out that this study provides a first, by far not complete benchmark to estimate the benefit of a software defined networking based architecture in a specific use case / scenario. The study however has limitations and is not meant to be a total cost of ownership analysis. The main limitations for the capital expenditures study are the availability of price points. We had access to the wholesale price list of one major vendor but given that we required ITU-T G.8032 Ethernet Ring Protection Switching, the set of available devices was limited. A second limitation, influencing at least the relative difference in-between the scenarios is the lack of fibre costs and outside infrastructure in general. The main limitations for the operational expenditures are the driver based estimation methods. These are in general less precise than process based methods but were required given the limited set of information that was available.

3.9.1   **Classical scenario versus SDN scenario for capital expenditure**

For the use case considered and the parameters as detailed in section 3.7 the SDN scenario capital expenditure advantage is quantified at 12%. The majority of capital expenditures savings is attributed to the savings at the pre-aggregation stages which is explained by the high number of sites at this level. A second contributor is the lower cost of first time installation. The savings in the pre-aggregation sites amount to up to 13% which is a bit higher than the total reduction of 12%. Introducing SDN however also involves introducing of centralized controllers to the network architecture which accounts for an extra 3% of the total cost. Further details are provided in Figure 16 and Figure 17.

Classical scenario total cost

	# routers		2012		2013		2014		2015		2016		2017
Pre-aggregation site routers	2000	€	105,992	€	1,783	€	2,271	€	1,783	€	-	€	1,783
Aggregation site routers	160	€	130,000	€	22,713	€	14,264	€	22,791	€	7,132	€	15,581
Core site routers	12	€	233,147	€	74,248	€	16,217	€	46,163	€	66,628	€	23,837
Inner core site routers	24	€	491,178	€	47,380	€	67,302	€	215,450	€	26,907	€	69,744
Subtotal		€	247,370,543	€	9,228,093	€	8,634,667	€	12,937,147	€	2,586,388	€	8,018,822
first time installation	13%	€	32,158,171	€	1,199,652	€	1,122,507	€	1,681,829	€	336,230	€	1,042,447
Total Capital Expenditures		€	279,528,713	€	10,427,745	€	9,757,173	€	14,618,976	€	2,922,618	€	9,061,269

SDN scenario total cost

	# routers		2012		2013		2014		2015		2016		2017
Pre-aggregation site routers	2000	€	85,837	€	1,783	€	2,271	€	1,783	€	-	€	1,783
Aggregation site routers	160	€	109,845	€	22,713	€	14,264	€	22,791	€	7,132	€	15,581
Core site routers	12	€	207,969	€	74,248	€	16,217	€	37,636	€	66,628	€	23,837
Inner core site routers	24	€	463,473	€	38,853	€	58,775	€	198,395	€	26,907	€	61,217
Total without SDN components		€	202,868,589	€	9,023,442	€	8,430,016	€	12,425,519	€	2,586,388	€	7,814,171
OpenFlow controller	48	€	74,558	€	-	€	-	€	-	€	-	€	-
Software development cost	1.5 mio/year	€	1,500,000	€	1,500,000	€	1,500,000	€	1,500,000	€	1,500,000	€	1,500,000
Subtotal		€	207,947,380	€	10,523,442	€	9,930,016	€	13,925,519	€	4,086,388	€	9,314,171
first time installation	13%	€	27,033,159	€	1,368,047	€	1,290,902	€	1,810,318	€	531,230	€	1,210,842
Total Capital Expenditures		€	234,980,539	€	11,891,489	€	11,220,918	€	15,735,837	€	4,617,618	€	10,525,013

Figure 16: Comparison of CapEx between classical scenario and SDN scenario
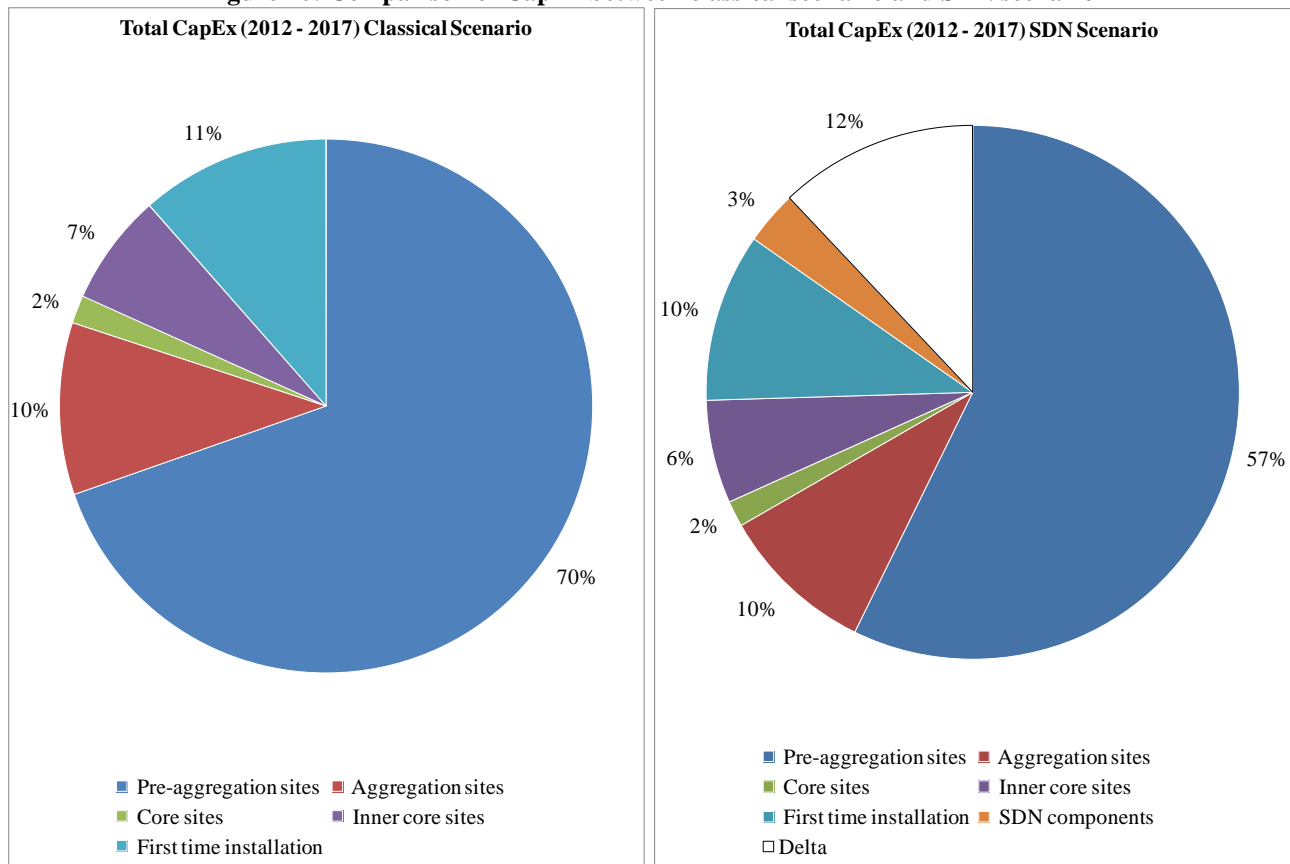
Figure 17: CapEx categories as part of total CapEx in the classical scenario

3.9.2   Classical scenario versus SDN scenario for operational expenditures

Within the OpenFlow community the focus is often not on the promised capital expenditures reductions. Little attention is however given towards operational expenditures. For the use case considered and the parameters detailed in section 3.2 our analysis shows a 10.7% OpEx reduction in case of the introduction of SDN. The main benefits can be found at the network operations center where the cost of operational processes such as service provisioning and service management is reduced by 3% and 6% respectively. The environmental cost (energy consumption) has not been increased nor reduced. It could be however argued that the energy consumption of the router is reduced because part of the control plane functionality is now taken over by the SDN controller. This is open for further research.

Classical scenario total cost

	2012	2013	2014	2015	2016	2017
Continuous cost of infrastructure	€ 5,787,798	€ 5,985,493	€ 6,189,841	€ 6,683,314	€ 6,883,813	€ 7,117,409
Maintenance and repair cost	€ 13,748,205	€ 14,215,672	€ 14,698,260	€ 15,662,169	€ 16,121,302	€ 16,241,978
Service management	€ 4,025,726	€ 4,209,317	€ 4,498,435	€ 4,646,613	€ 4,675,213	€ 4,835,456
Service provisioning	€ 12,077,178	€ 550,772	€ 867,355	€ 444,535	€ 85,799	€ 480,728
Up-front planning	€ 17,315,938	€ 645,967	€ 604,427	€ 905,600	€ 181,047	€ 561,318
Total Operational Expenditures	€ 52,954,846	€ 25,607,221	€ 26,858,318	€ 28,342,232	€ 27,947,174	€ 29,236,888

SDN scenario total cost

	2012	2013	2014	2015	2016	2017
Continuous cost of infrastructure	€ 5,813,484	€ 6,011,950	€ 6,217,092	€ 6,711,382	€ 6,912,723	€ 7,147,186
Maintenance and repair cost	€ 13,635,673	€ 14,103,699	€ 14,586,930	€ 15,547,587	€ 16,010,188	€ 16,131,769
Service management	€ 2,328,759	€ 2,434,826	€ 2,601,860	€ 2,687,468	€ 2,703,991	€ 2,796,569
Service provisioning	€ 6,986,277	€ 318,201	€ 501,102	€ 256,824	€ 49,569	€ 277,734
Up-front planning	€ 14,534,535	€ 713,036	€ 671,496	€ 951,182	€ 262,442	€ 628,387
Total Operational Expenditures	€ 43,298,729	€ 23,581,712	€ 24,578,480	€ 26,154,442	€ 25,938,914	€ 26,981,645

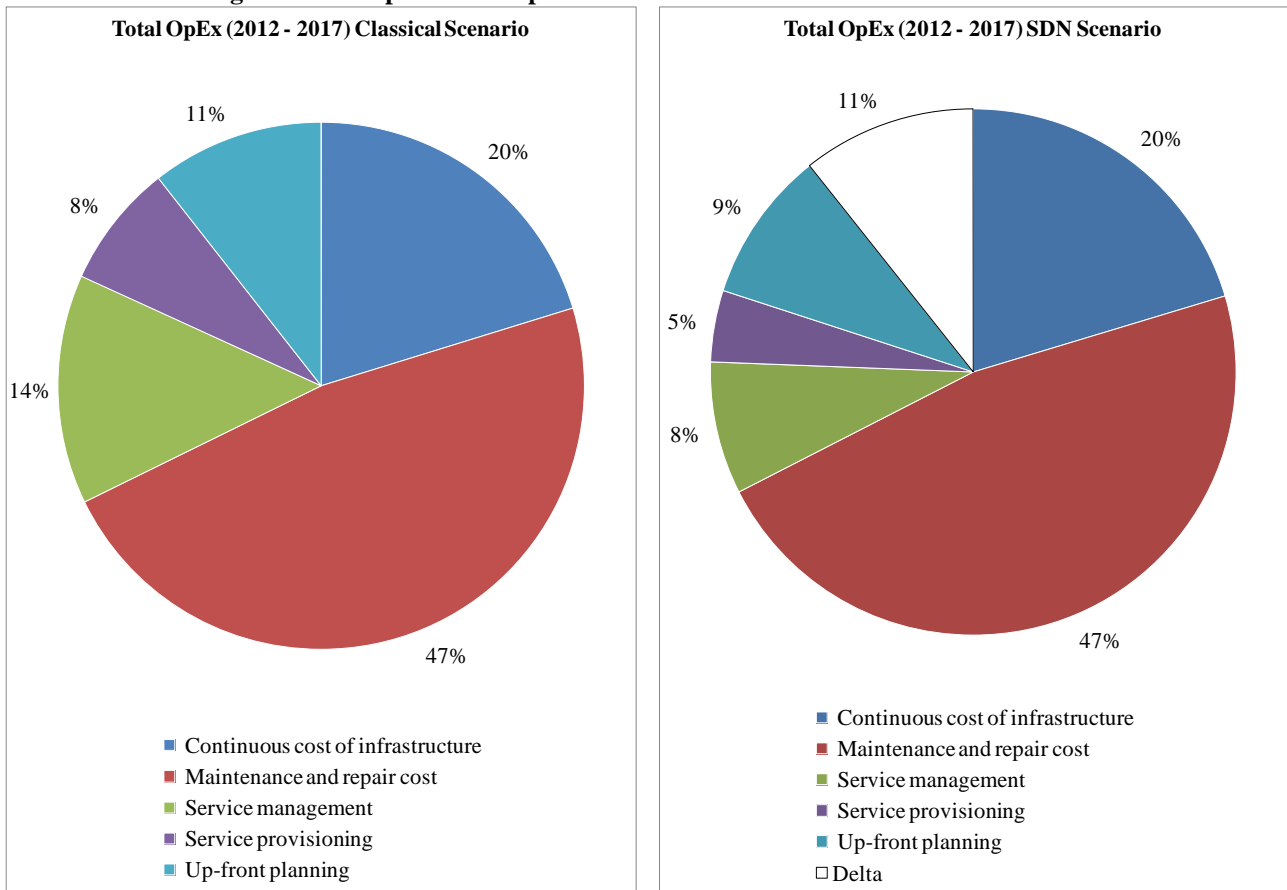**Figure 18: Comparison of OpEx between classical scenario and SDN scenario**

Figure 19: OpEx categories as part of total OpEx in the classical scenario

3.9.3 Sensitivity Analysis

We've performed sensitivity analysis on the following parameters:

- Cost of a SDN controller

- Number of OpenFlow enabled network elements one SDN controller is able to steer

- Effect of wholesale price discounts by vendor on SDN advantage

- Effect of cost reduction in cost of operating system of router

- Effect of extra reductions in hardware cost because of specialization and interoperability of devices

The main reason to analyze these parameters in a bit more detail is the uncertainty that surrounds them. The application of SDN in a carrier grade environment is still rather novel. Carriers have no experience at all with this technology and very limited input is available on these parameters.

Cost of a SDN controller

At the moment no carrier grade SDN controller is available. Therefore the price point was estimated as the average of the available SDN controllers from NEC and IBM.

The original price point was estimated at 65,000 dollar or around 50,388 euro. The price of a SDN controller was varied with intervals of 25%. The data is presented in Figure 16. An increase of the price by 25% corresponds with a small decrease (-0.21%) in capital expenditures cost savings for the network operator. We therefore conclude that the price of the SDN controller has a rather low effect on the overall analysis.

OpenFlow Controller' Price	€ 25,194	€ 37,791	€ 50,388	€ 62,984	€ 75,581	€ 88,178	€ 100,775
Total Capital Expenditures (2012-2017) for Classical Scenario	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495
Total Capital Expenditures (2012-2017) for SDN Scenario	€ 285,677,461	€ 286,360,717	€ 287,043,973	€ 287,727,229	€ 288,410,484	€ 289,093,740	€ 289,776,996
Delta	-12.45%	-12.24%	-12.04%	-11.83%	-11.62%	-11.41%	-11.20%

Figure 20: Data for different price points of OF controller

**Number of OpenFlow enabled network elements one SDN controller is able to steer**

The original ratio was estimated at one SDN controller which is able to control 100 OpenFlow enabled network devices. Very little information is known on this ration in a carrier environment. To incorporate this uncertainty, we varied the ratio with steps of 25%. Capital – and operational expenditures for the SDN scenario change stepwise. The more OpenFlow enabled network devices one SDN controller can control, the lower total CapEx and OpEx. The data is presented in Figure 18 and Figure 19 presents the delta between both scenarios. Note that the axis intercept is not at 0%. The delta for capital expenditures- and operational expenditures savings between 50 and 200 controllers is no more than respectively 1.30% and 1.0%.

Ratio OF controller to OF enabled network devices	50	75	100	125	150	175	200
Total Capital Expenditures (2012-2017) for Classical Scenario	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495
Total Capital Expenditures (2012-2017) for SDN Scenario	€ 289,856,464	€ 287,747,096	€ 287,043,973	€ 286,340,850	€ 286,340,850	€ 286,340,850	€ 285,637,727
Delta on Total Capex	-11.17%	-11.82%	-12.04%	-12.25%	-12.25%	-12.25%	-12.47%

Ratio OF controller to OF enabled network devices	50	75	100	125	150	175	200
Total Operational Expenditures (2012-2017) for classical scenario	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678
Total Operational Expenditures (2012-2017) for SDN scenario	€ 171,794,782	€ 170,845,251	€ 170,533,922	€ 170,225,183	€ 170,225,183	€ 170,225,183	€ 169,919,034
Delta on Total OpEx	-10.03%	-10.53%	-10.69%	-10.85%	-10.85%	-10.85%	-11.01%

Figure 21: Data for different ratio's of OF controllers to OF enabled network devices
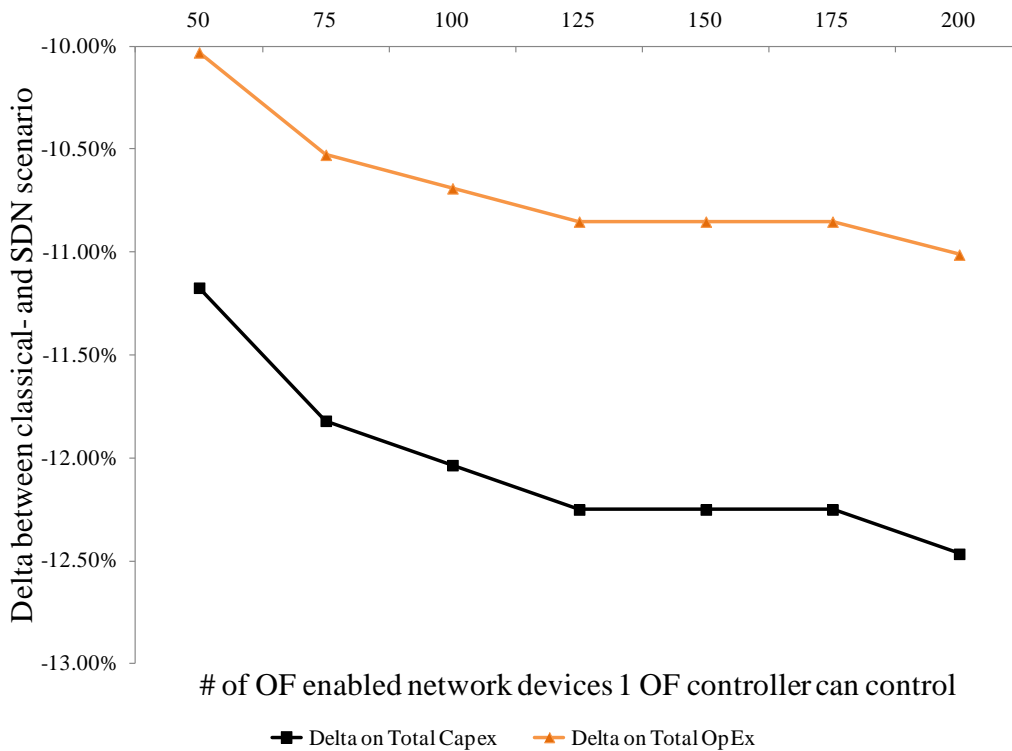
Figure 22: Data for delta between both scenario's for different ratio's of OF controllers to OF enabled network devices

Effect of wholesale price discounts by vendor on SDN advantage

In the study we've taken wholesale prices as reference values. It is however common practice to give large discounts to large buyers such as a network operator. We therefore take into account discounts up to 50% in steps of 10%. Discounts are applied to both classical network elements and SDN network elements but not the development cost of customized software.

The benefits of software defined networking on capital expenditures are reduced when higher discounts are applied. This is due to:

-    SDN lowers the cost of software, this advantage is reduced in absolute terms,

-    SND requires the development of customized software for which the development cost cannot be expected to be lowered by the same discount rate.

The benefits of software defined networking on operational expenditures are higher when higher discounts are applied. This is due to:

-    The effect of hardware related operational processes such as repair and up-front planning (which is here calculated as a percent of total hardware cost) is lower because of the general lower prices of hardware components,

-    The cost saving effect of processes which are not hardware related such as service provisioning and service management is more pronounced due to relative lower values of the hardware related operational processes.

The data is presented in Figure 20 and Figure 21 presents the delta between both scenarios graphically. Note that the axis intercept is not at 0%.

Discount rate	0%	10%	20%	30%	40%	50%
Total Capital Expenditures (2012-2017) for Classical Scenario	€ 326,316,495	€ 293,684,845	€ 261,053,196	€ 228,421,546	€ 195,789,897	€ 163,158,247
Total Capital Expenditures (2012-2017) for SDN Scenario	€ 287,043,973	€ 259,263,727	€ 231,483,481	€ 203,703,234	€ 175,922,988	€ 148,142,742
Delta on Total Capex	-12.04%	-11.72%	-11.33%	-10.82%	-10.15%	-9.20%

Discount rate	0%	10%	20%	30%	40%	50%
Total Operational Expenditures (2012-2017) for classical scenario	€ 190,946,678	€ 184,184,428	€ 177,422,178	€ 170,659,929	€ 163,897,679	€ 157,135,429
Total Operational Expenditures (2012-2017) for SDN scenario	€ 170,533,922	€ 163,993,264	€ 157,452,607	€ 150,911,949	€ 144,371,292	€ 137,830,634
Delta on Total OpEx	-10.69%	-10.96%	-11.26%	-11.57%	-11.91%	-12.29%

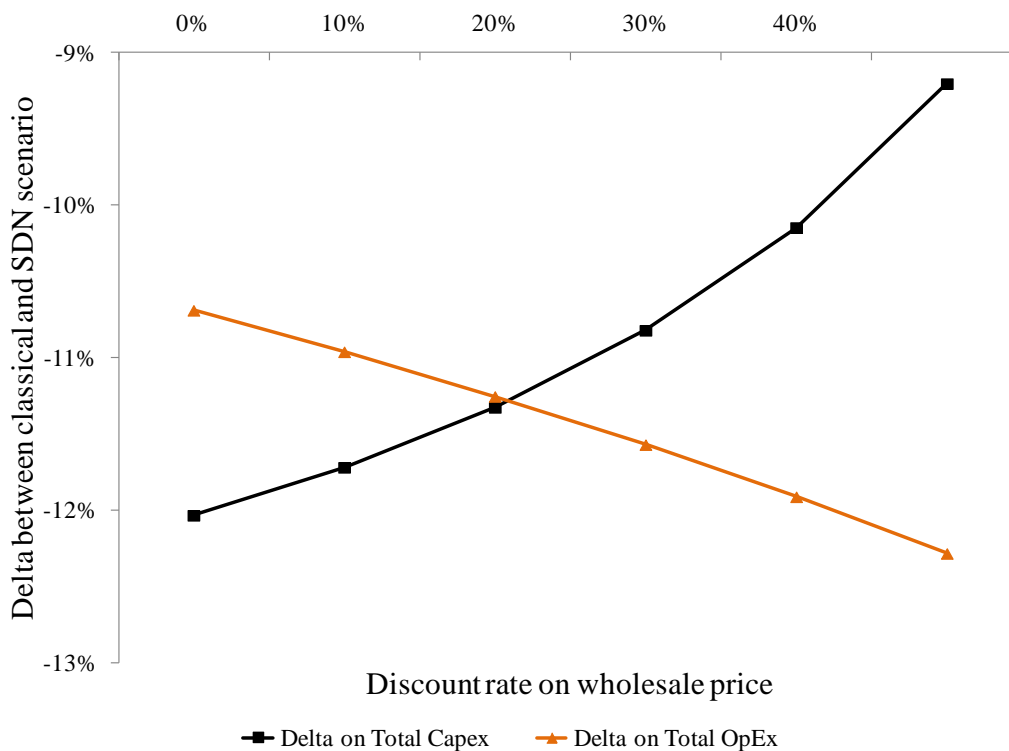**Figure 23: Data for different discount rates of wholesale price**

Figure 24: Data for delta between both scenario's for different discount rates of wholesale price

Effect of cost reduction in cost of operating system of router

In this scenario we test the influence of our assumption of the cost reduction of the operating system. We therefore take into account discounts up to 50% in steps of 12.5%. It can be seen that in the case of no cost reduction there still is a 10.7% SDN advantage. This is due to the lower VPN licensing costs which are taken over by the software development cost.

The data is presented Figure 22 and

Figure 23 presents the delta between both scenarios graphically. Note that the axis intercept is not located at 0%.

Expected lower cost of Operating System		0.00%		12.50%		25.00%		37.50%		50.00%
Total Capital Expenditures (2012-2017) for Classical Scenario	€	326,316,495	€	326,316,495	€	326,316,495	€	326,316,495	€	326,316,495
Total Capital Expenditures (2012-2017) for SDN Scenario	€	294,738,484	€	290,891,229	€	287,043,973	€	282,234,903	€	278,195,284
Delta on Total Capex		-9.68%		-10.86%		-12.04%		-13.51%		-14.75%

Figure 25: Data for expected lower cost op router'operating system
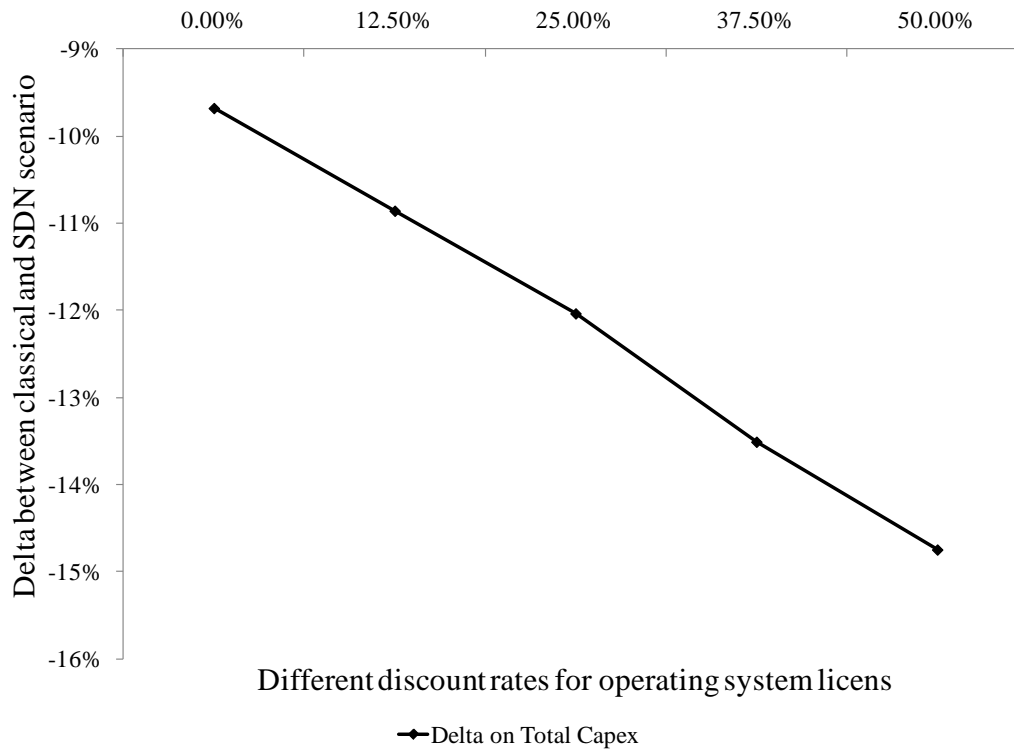
Figure 26: Data for delta between both scenario's for different discount rates of operating system

Effect of extra reductions in hardware cost because of specialization and interoperability of devices

Up to now we did not take into account two other advantages of SDN, the ability to allow for (1) interoperability between vendors and (2) specialization in one aspect of the current monolithic design. This will put margin pressure on the prices of commodity hardware and therefore the effects of this should be taken into account.

The data is presented Figure 24 and

Figure 25 presents the delta between both scenarios graphically.

Expected reductin in cost of hardware components	0.00%	10.00%	20.00%	30.00%	40.00%	50.00%
Total Capital Expenditures (2012-2017) for Classical Scenario	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495	€ 326,316,495
Total Capital Expenditures (2012-2017) for SDN Scenario	€ 287,043,973	€ 264,557,382	€ 242,070,792	€ 219,584,202	€ 197,097,612	€ 174,611,021
Delta on Total Capex	-12.04%	-18.93%	-25.82%	-32.71%	-39.60%	-46.49%

Expected reductin in cost of hardware components	0.00%	10.00%	20.00%	30.00%	40.00%	50.00%
Total Operational Expenditures (2012-2017) for classical scenario	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678	€ 190,946,678
Total Operational Expenditures (2012-2017) for SDN scenario	€ 170,533,922	€ 164,844,863	€ 159,155,803	€ 153,466,744	€ 147,777,685	€ 142,088,625
Delta on Total OpEx	-10.69%	-13.67%	-16.65%	-19.63%	-22.61%	-25.59%

Figure 27: Data for expected reduction in cost of hardware components
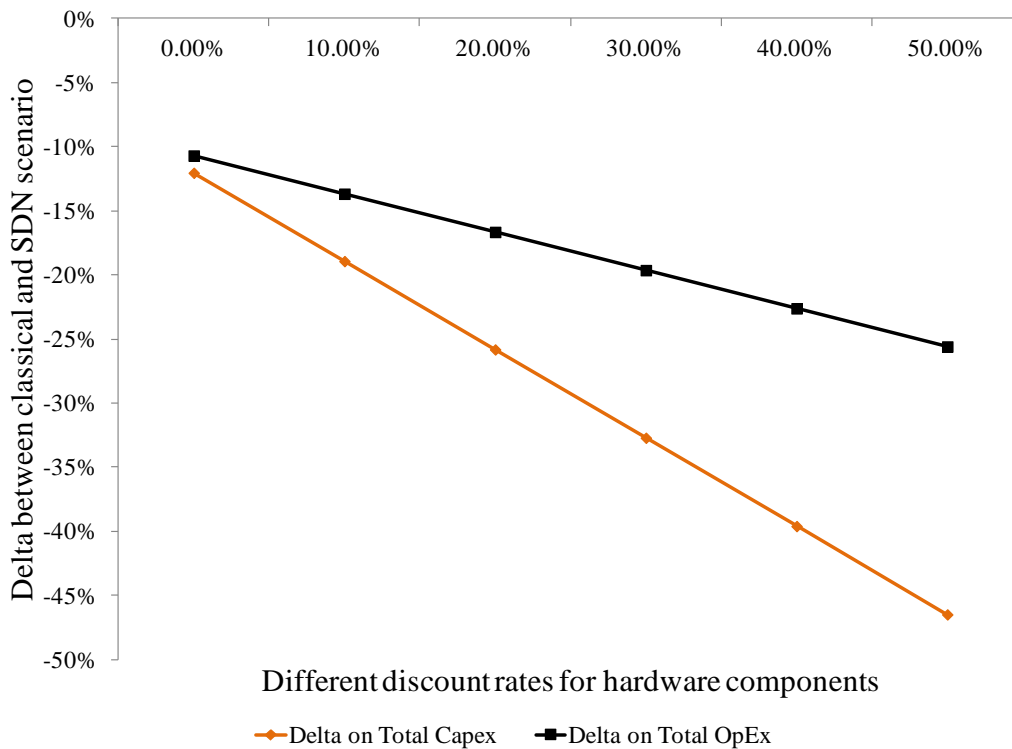

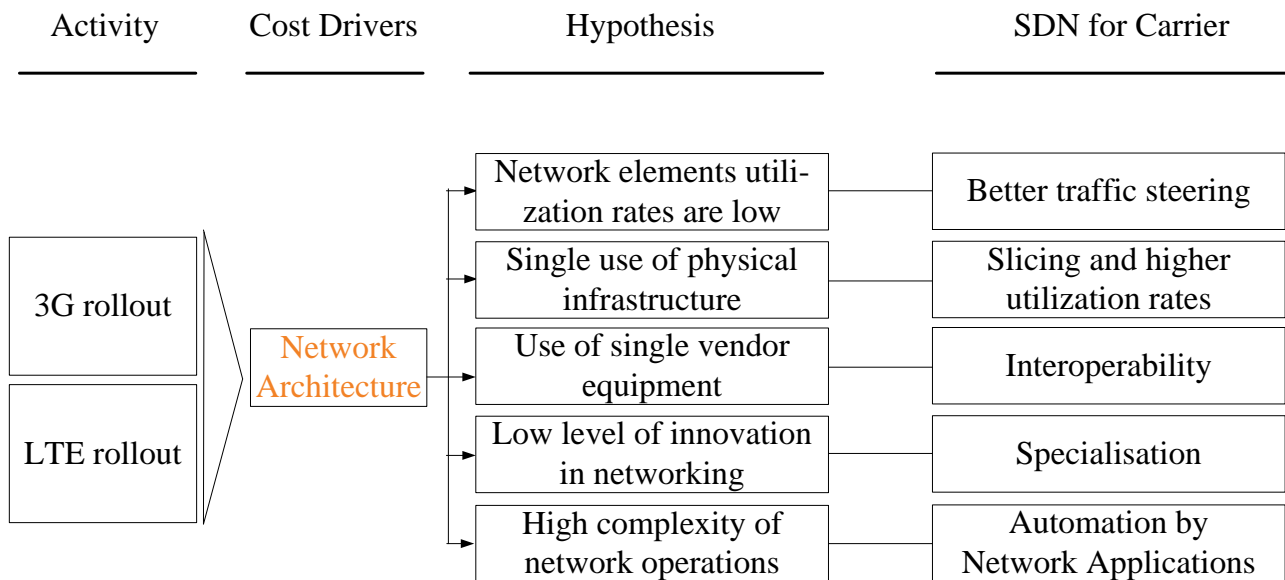**Figure 28: Data for delta between both scenario's for different discount rates of hardware components**

3.10   Conclusion and open topics

Carriers experience a rapid increase in demand for data traffic which requires substantial investments in the rollout of new radio access technologies such as LTE. Costs for the mobile carriers, including the cost for the backhauling network infrastructure are therefore rising while revenue growth is nearly flat. The main cost driver for a mobile carrier is the network architecture and in this domain software defined networking promises considerable innovation which is summarized in Figure 29.

The lack of information regarding the economic benefits of SDN in a carrier environment is however one of the factors that delay the actual application of SDN. This study therefore is a first attempt to quantify the SDN benefit for a particular use case: LTE mobile backhauling.

The OpenFlow community is at the moment mainly focusing at the capital expenditures that can be gained by switching to software defined networking. Our analysis does give a first indication of the possible gains that can be reached in

capital expenditures. We have identified four factors that will influence the potential for CapEx reductions (1) the use of simpler network devices, (2) cost of extra components such as SDN controllers, line cards and transceivers, (3) the ratio of the number of switches that a SDN controller can manage and (4) the possibility to better align network capacity with actual demand. The analysis shows that the main benefit of software defined networking is due to the lower cost of software licenses. In many cases large discounts are given on the cost of software or the software may even be offered for free. The benefit of SDN may therefore be limited regarding capital expenditures. However, this might not be anticipating the trend toward commodity hardware sub-systems and the related cost benefits. From our analysis it is also clear that further research and real experience with the deployment of software defined networking is required to give a more detailed estimate of the capital expenditures. Examples are the cost of customized software development taking into account the availability of open source software and possible reductions in hardware costs because of specialisation and interoperability. These are however at the moment hard to quantify because of the lack of experience with the SDN architecture.

Activity	Cost Drivers	Hypothesis		SDN for Carrier
3G rollout	Network Architecture	Network elements utilization rates are low		Better traffic steering
		Single use of physical infrastructure		Slicing and higher utilization rates
		Use of single vendor equipment		Interoperability
LTE rollout		Low level of innovation in networking		Specialisation
		High complexity of network operations		Automation by Network Applications

Figure 29: root cause diagram for margin pressure of mobile carrier and potential of SDN

Although the focus of the OpenFlow community is at the moment mainly on CapEx, carriers equally struggle with keeping operational expenditures low. We've done a detailed cost break down in this study and the results show that the main benefits can be found in operational processes that are conducted by the network operations centre such as service provisioning and service management.

Software defined networking can provide further benefits when more network based applications become available.

4 Analysis of the OpenFlow ecosystem

4.1 Methodology of analysis

Experts from DTAG and EICT participated in an internal workshop in October 2011 that was held to outline today's market roles, their functions and possible new market roles in future.

In a second step, a questionnaire was answered by experts from Acreo, DTAG, EICT and Ericsson. The key questions were: Which markets will be strongly affected by OpenFlow and what will change? Which impact will OpenFlow have on different market roles?

Finally, these expert views and the OpenFlow market description were substantiated with an evaluation of key financial data of ONF and ATCA member organizations regarding head office as well as revenues and employees in 2011.

4.2 Value network analysis – Open Flow market

4.2.1 General

All experts were convinced that most switches in the mass market will support OpenFlow by no later than 2025, while the majority expects it to happen already by 2020 (see Figure 30).

The introduction of OpenFlow is likely to strongly affect several markets: carrier-grade fixed line telecommunication networks, carrier-grade mobile telecommunication networks, data centers and enterprise networks (see Figure 31).
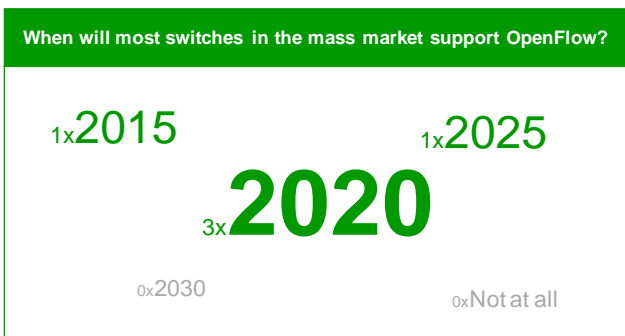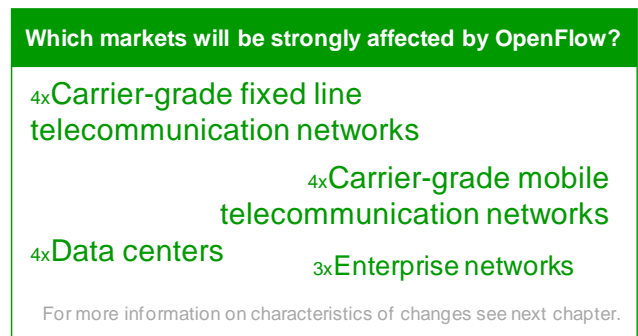

Figure 30: Availability of OpenFlow

Figure 31: Affected markets

Within these markets some players are affected more significantly than others, since their products are likely to be superseded by the OpenFlow technology (see Figure 32, Figure 33, and Figure 34). In the telecommunication networks market, today's vendors of AGS1 and AGS2 are probably hit most by the introduction of OpenFlow (e.g. ALU, Ericsson, Cisco, Huawei, Juniper, Cienna, NSN, and others). In the datacenter market, OpenFlow has presumably most impact on today's vendors of top-of-rack and DC switches (among others NEC, HP, IBM, Cisco, Force10 (Dell), LG Ericsson, BIG Switch, Juniper and component vendors). In the enterprise market, today's vendors of 48 port switches and enterprise switches and routers are likely to be affected.
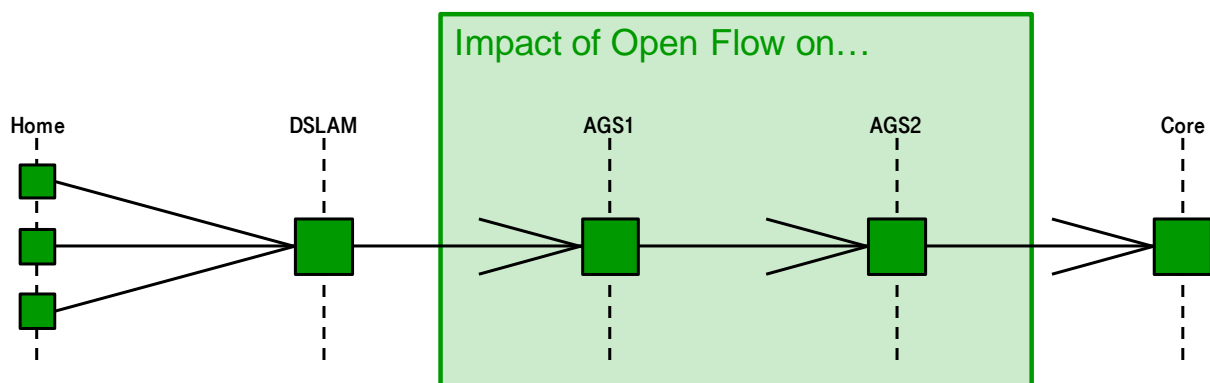
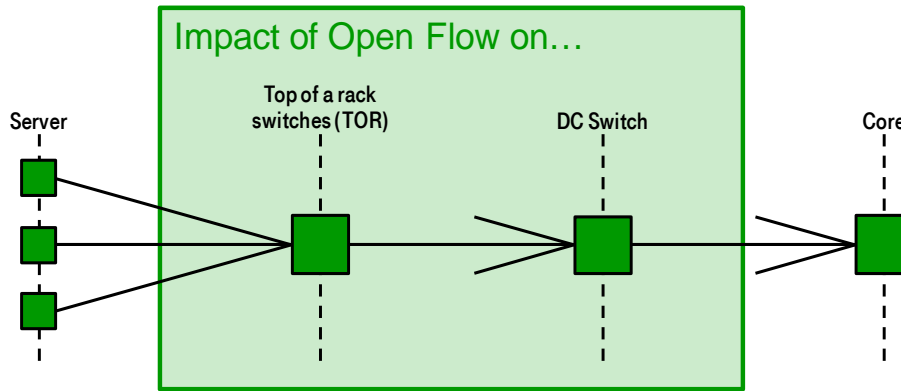*Market definition I – Telecommunication Networks*

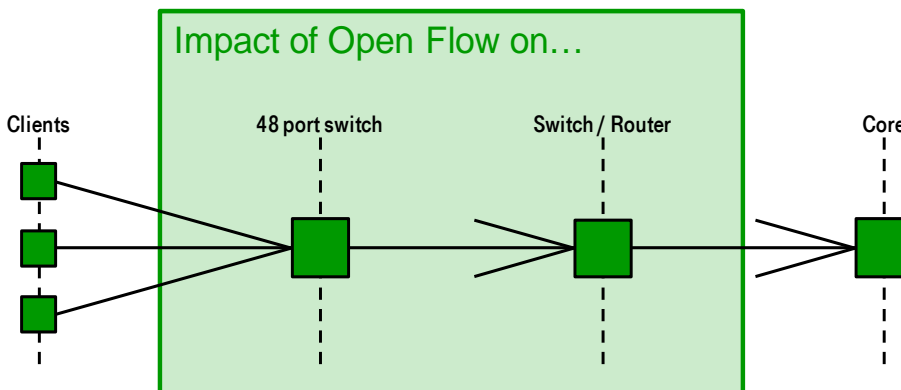**Figure 32: Market definition I: Telecommunication networks**
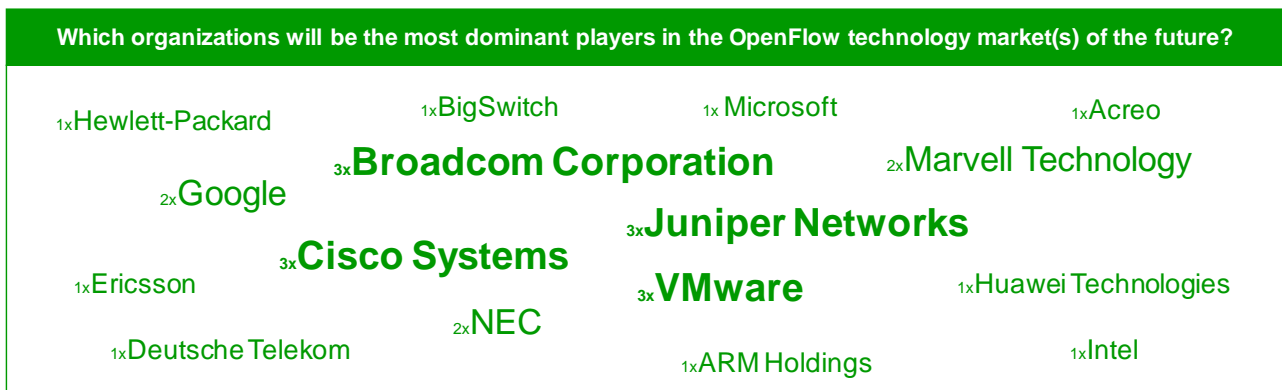
Market definition II – Datacenter

Figure 33: Market definition II: Datacenter

Market definition III – Enterprise

Figure 34: Market definition III: Enterprise

In the OpenFlow technology markets, Broadcom Corporation, Cisco Systems, Juniper Networks and VMware are spotted as the potential most dominant players (see Figure 35).

Figure 35: Dominant market players in future

4.2.2   Main changes in today's markets

In carrier-grade fixed line telecommunication networks, OpenFlow will be used to share and virtualize infrastructure, enabling virtual operators, the migration to "new" access protocols (e.g. DHCP, HIP), and the fixed-mobile convergence. Not only simpler TE routing and operations in general add to the benefits of OpenFlow, but also more flexible services, network virtualization and enhancements in the cost structure.

For carrier-grade mobile telecommunication networks, OpenFlow allows to merge fixed and mobile data networks. This step reduces costs in the aggregation and backhaul networks. The merge also increases the throughput in mobile networks and offloads mobile traffic making use of WiFi access rates.

In addition to the above-mentioned benefits of fixed line networks, OpenFlow also helps to apply QoS in a better way and allows for SDN in mobile networks.

In data centres, a tighter integration between VM, storage and network simplifies the operations. Both resources within the data center and data center interconnects can be utilized in an optimized way. OpenFlow will also alter the data center flow control and improve the migration of VMs and their data flows in the network due to new protocols (e.g. for tunnelling traffic).

Introducing OpenFlow also simplifies the operations of enterprise networks. In particular, it becomes possible to forward more efficiently on L2/L3 and to control access more strictly. In addition, it supersedes highly dedicated devices.

4.2.3   Situation today

Today, system integrators have a dominant market presence (see Figure 36). They obtain chips, aerials, line cards and other hardware from a hardware vendor who is specialized in their development and production. Software vendors develop proprietary software solutions, network stacks and handle the adaption to different hardware platforms. They are linked to vendors of network management solutions who develop dedicated solutions. All these hardware and software components are assembled by system integrators in their own proprietary solutions. Network operators focus on the operation of various networks, e.g. telecommunication networks and purchase network solutions from the system integrators.

4.2.4   Situation tomorrow

OpenFlow impacts the ecosystem for a carrier-grade network set-up in several ways (see Figure 37). On the one hand, more standardized interfaces and software solutions emerge. Software vendors take on new business, e.g. operating systems for different hardware as well as OpenFlow-controllers. The software market splits up and a separate market for network applications arises ("Network application vendors"). On the other hand, hardware vendors and system integrators lose ground as network operators can assembly their own solutions directly with commodity hardware and network applications.
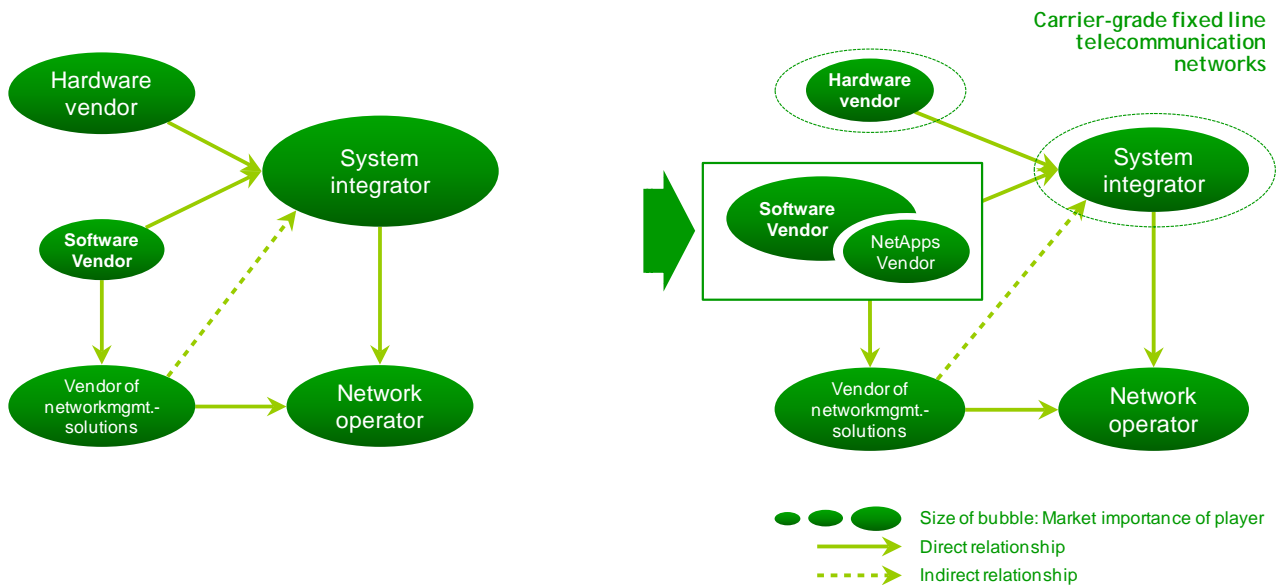
Figure 36: Situation today   **Figure 37: Situation tomorrow**

4.3   Value network analysis – Impact on market roles

The following subsections outline trends, risks and chances for the different market roles.

4.3.1   Hardware vendors

Limited impacts are expected for chip manufacturers as just another protocol is to be supported. Hardware vendors of switches etc. are likely to face higher impact, as a convergence of the industry seems possible due to OpenFlow. The

trend is towards commodity hardware assembled from basic building blocks, therefore hardware vendors have to apprehend increased competition and less profitability.

The main opportunities lie in chips with easier-to-use interfaces that will lead to increasing revenues and, for some big companies, to capture a dominant market role.

OpenFlow makes the adaption of a new business model necessary, imposing a major risk to hardware vendors. They have to shift their focus from hardware more towards software solutions running on generic hardware. Especially smaller companies might fail to survive, while more resources and costs must be dedicated to the competition between the big companies.

Figure 38: Trends for hardware vendors

4.3.2 Software vendors

New market opportunities arise for software vendors and which lead to higher profitability (the addressable market increases), but also to higher competition and increased pressure to innovate. Overall, the technological complexity of solutions is reduced.

New market opportunities open up for controller middleware solutions. Software for SDN controllers has a single focus, rather than dealing with the whole network. A new market could develop where network features are sold as netapps. A further business potential lies in offering support for advanced protocols, e.g. firmware or vendor extensions.

Theses chances are accompanied by new risks, however. The business model needs to be adapted to include controller software, netapps and more. Two more risks arise because neither the northbound interface has been specified so far nor has OpenFlow been accepted as an industry standard yet.

Figure 39: Trends for software vendors

4.3.3 Network application vendors

Today's market for network applications is limited and rather small. It consists of mostly startups. Hitherto, network applications are often proprietary solutions.

OpenFlow offers good prospects in terms of a shorter time to market, more innovative applications in a diversity of application areas such as data centre, enterprises, carrier networks and many more.

It harbours the risk of an uncharted market with undefined actors: The development of the market remains unforeseeable; in particular the OpenFlow standard diversity is hard to predict.
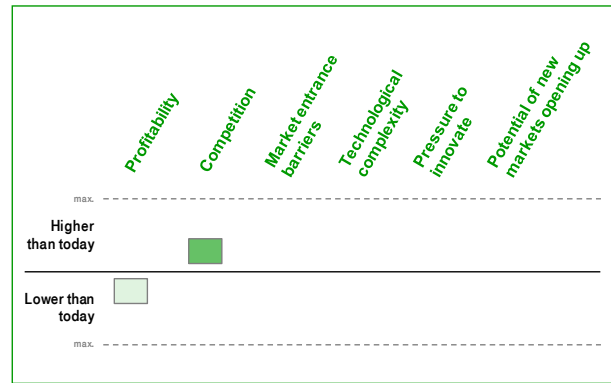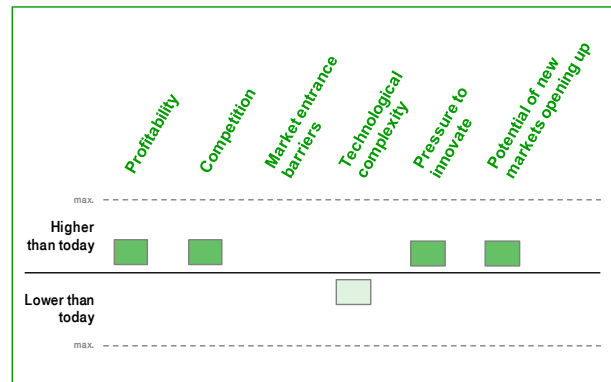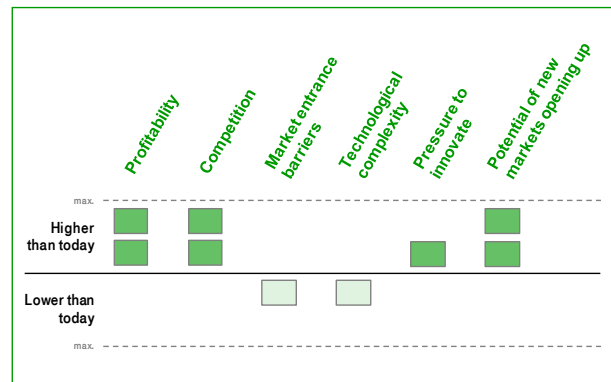

Figure 40: Trends for network application vendors

4.3.4 System integrators

System integrators are likely to face a multitude of changes. The introduction of switches simplifies the hardware side (routers/switches) and requires fewer features in the future. Despite of the OpenFlow technology, proprietary solutions are still possible due to OF vendor extensions.

However, it is expected that the system integrators' market power decreases and the impact of closed proprietary complex systems is reduced. Eventually, this will result in a consolidation of actors and possibly a merging of the telecommunication and data centre market.

Against all odds, OpenFlow harbours a number of opportunities for system integrators, too. First, it becomes easier to compete with custom-built solutions for different markets, e.g. data centre solutions. Secondly, less integration of hardware and software is needed. Finally, they can sell their "optimized" version of complete SDN solutions, including hardware (with specific extra features, e.g. specific processing actions, OAM etc.), control layer middleware, use-case specific network applications as well as management systems.

Risks are identified in a potential business model shift to either added-value services like replacement services or additional software like network management. While there are a lot of benefits from a simplified integration of software on hardware, it leads to increased competitive pressure, too.

Figure 41: Trends for system integrators

4.3.5 Network management solutions vendors

For network management solutions vendors, no major differences in business models could be discerned, as OpenFlow and OF-Config will probably be just another interface to support. Probably, they must act in an increasingly competitive market. Most likely, however, the leading position of established companies will not alter. Large networks will still require mature NMS/OSS/BSS solutions, a segment where current NMS market leaders have a head-start and will remain in the lead.

The opportunities of OpenFlow for this group lie mainly in a better utilization of the network due to improved algorithms and in increased hardware coverage using a single protocol. It might also entail risks, especially from increased competition for smaller or niche customers, a lack of control of vendor extended parts and decreasing revenues as today's management software is possibly not needed anymore.

Figure 42: Trends for networkmanagement solutions vendors

4.3.6 Network operators

Network operators can look forward to OpenFlow, as it has several positive features: Operations and network management could be organized in a simplified manner. The introduction of innovations in the network is eased by reduced complexity, simplified and unified processes and simplified migration, so that new or differentiating features in the network may be introduced faster.

Interoperability between different suppliers is increased and dependencies on single players are reduced. The higher vendor independence should result in increased competition among system integrators and have favourable impacts on network operators' purchase conditions. Further opportunities can be seen in possible CAPEX and OPEX savings, increasing network utilization, a split of transport from services and improved control of data centre networks.
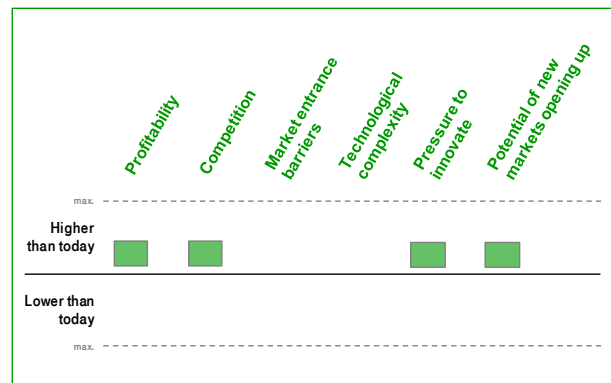
Figure 43: Trends for network operators
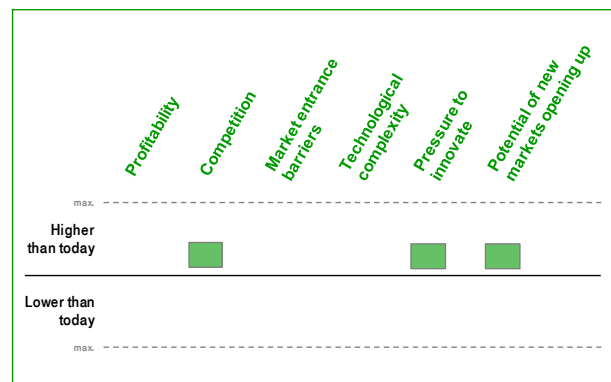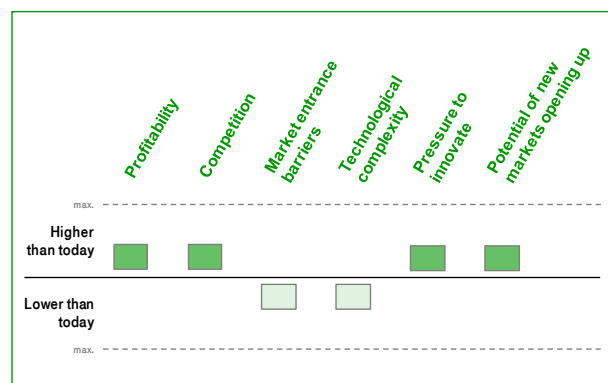
In addition, new business models may become possible, e.g. virtual operators. The other side of the coin is increased competition in form of these virtual network operators, however. A second possible risk of OpenFlow is that proprietary vendor extensions bring back vendor dependence.

4.4   Analysis of key data of ONF and ATCA member organizations

For the analysis of key data of ONF and ATCA member organizations, a total of 127 organizations were taken into consideration (see Figure 44). The geographic distribution shows that 61% are situated in the USA. Their membership is equally divided between ONF and ATCA executives; only a minor percentage is member of both groups. Only 18% are located in Europe, with a majority of organizations being ATCA executive members, closely followed by ONF members. Only a minor percentage is member of both groups. With its share of 16.5%, the group of organizations headquartered in Asia and China is only slightly smaller than the European group, while its membership is, similarly to the US, equally divided between ONF and ATCA executives, only a minor percentage is member of both groups. The rest is divided among Australia, Middle East, Russia and South America, where the majority of considered organizations are ONF members.
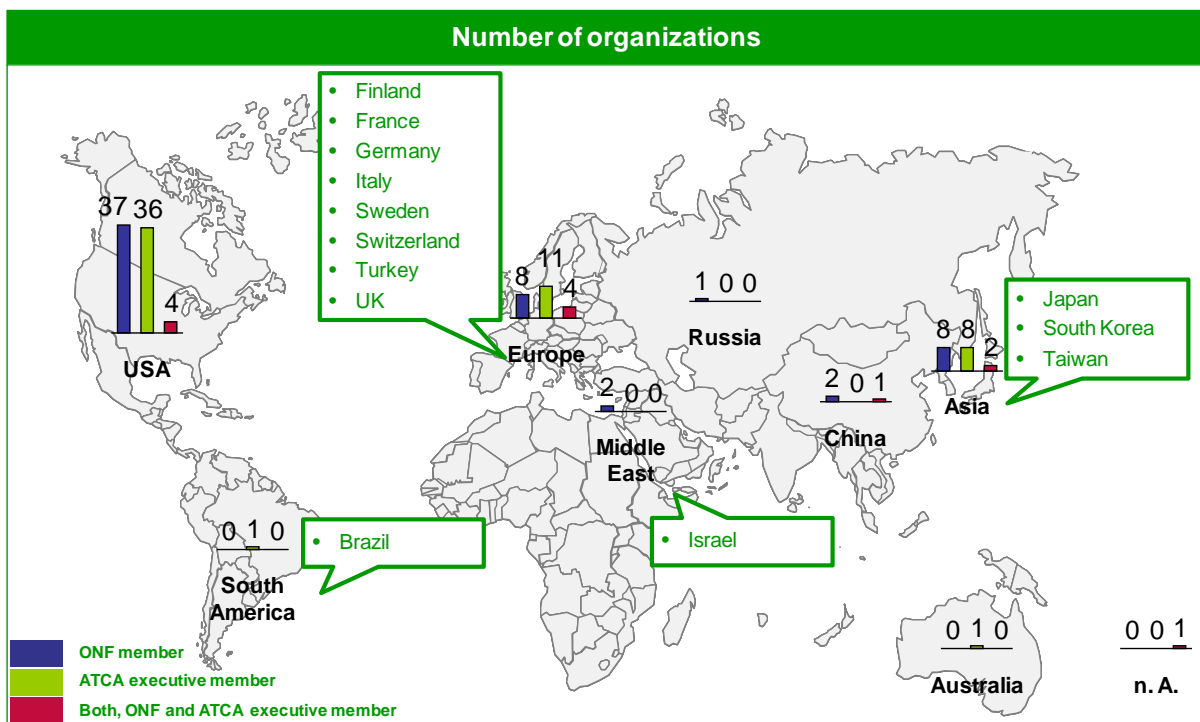
Figure 44: Number of considered organizations

The total revenues of all organizations are $ 1'453 billion (see Figure 45). Analysed in geographic terms, nearly 50% of the revenues originate in the USA, followed by Asia, Europe, China and Middle East. Sorted by membership, ONF member organizations have far higher revenues than ATCA organizations.
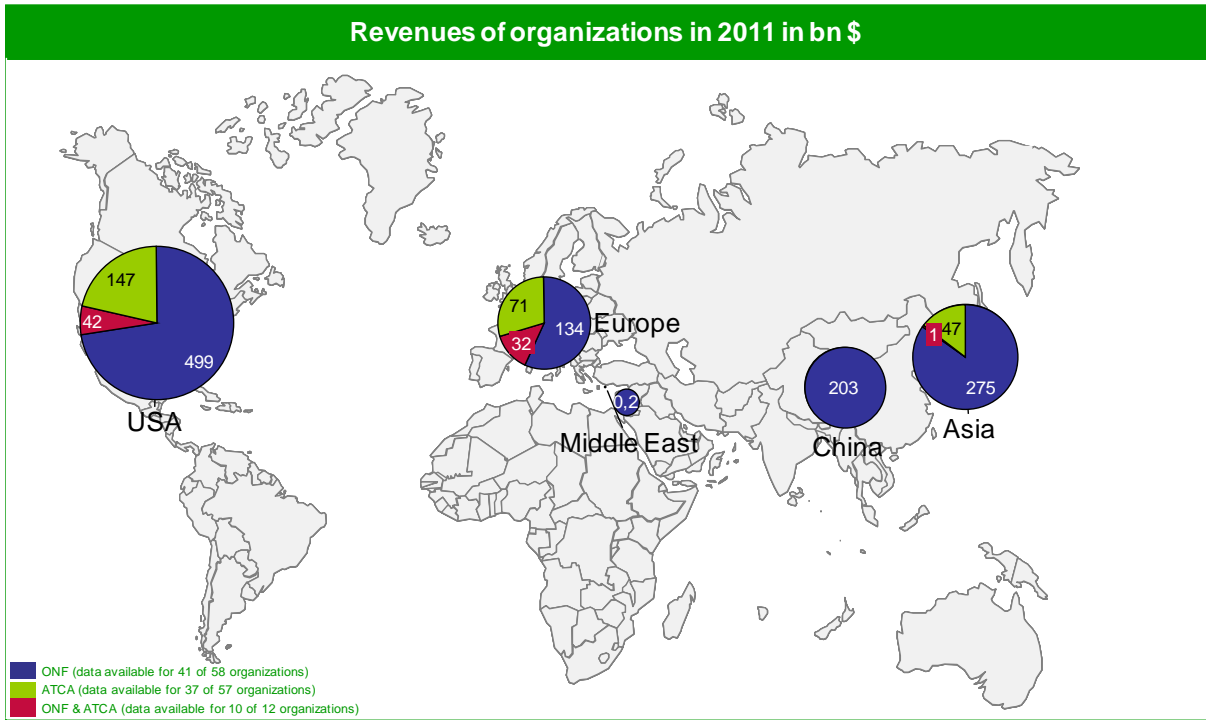
Figure 45: Revenues of considered organizations in 2011 in $

The total number of employees is 3.8 million (see Figure 46), with the USA again dominant, followed by Asia, China, Europe and the Middle East. In terms of membership, two thirds of total employees are working for ONF member organizations, one quarter for ATCA member organizations and nearly 10% for organizations which are member in both groups.
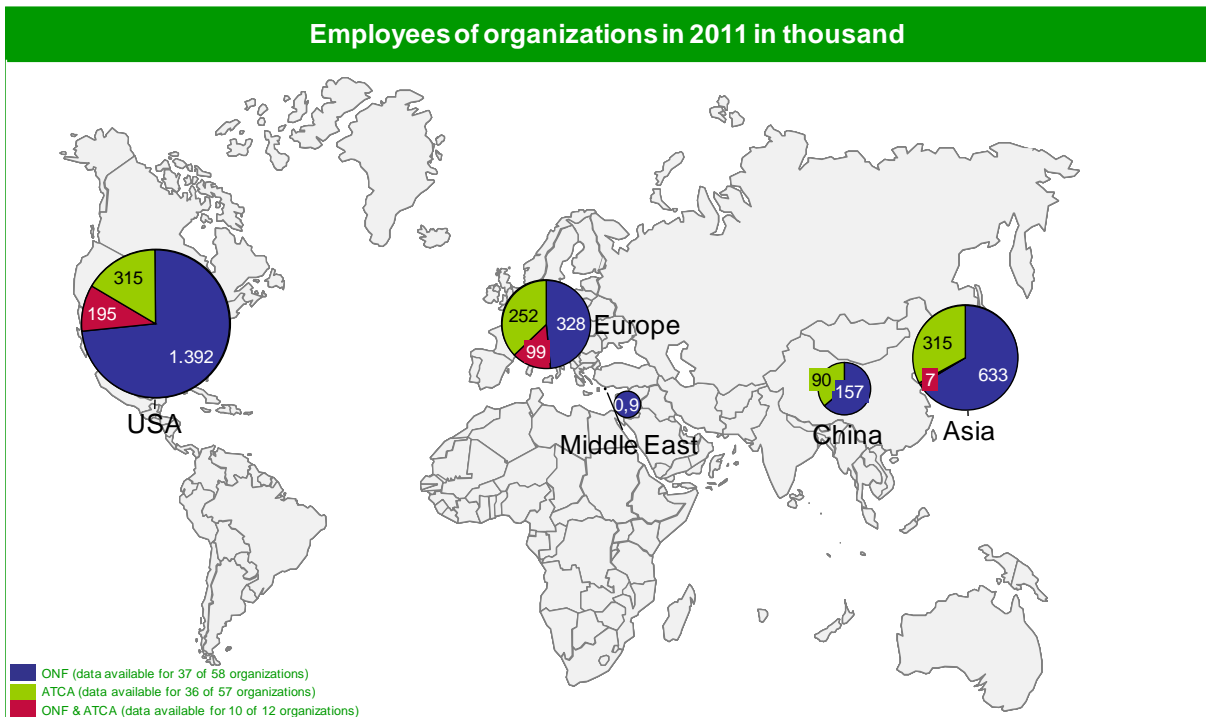
Figure 46: Employees of considered organizations in 2011 in thousands

4.5   ONF, ATCA and OpenStack

The analysis of participation of ONF members in ATCA executive members as well as OpenStack show that only six out of 59 ONF members or respective 75 ATCA executive members are represented in all three organizations.

4.6   Summary

4.6.1   Open flow market

In 2020, OpenFlow is expected to be widely supported in the mass market. This will strongly affect several markets, especially carrier-grade fixed and mobile telecommunication networks, data centres as well as enterprises. Additionally, OpenFlow is expected to offer new market potentials for nearly every involved player. Broadcom Corporation, Cisco Systems, Juniper Networks and VMware are spotted as the potential dominant players in this market.

4.6.2   General changes through OpenFlow

OpenFlow might imply some general changes. First, the software market will be split up due to emerging network applications. Secondly, hardware vendor and system integrator will lose their dominance and, thirdly, interfaces and software solutions will become increasingly standardized.

4.6.3   Changes for different market roles

The introduction of OpenFlow is likely to make business model changes necessary for hardware vendors and system integrators. New market opportunities open up for software vendors, especially network application vendors will benefit from OpenFlow. Vendors of network management solutions, on the other hand, will be exposed to increased competition. Network operators can expect simplified operations, but possibly major changes to the traditional network design are required.

4.6.4   Analysis of three standardisation organisations ONF, ATCA and OpenStack

The analysis of the participation of companies in the three different standardisation organisations ONF, ATCA and OpenStack shows only a loose connection. Overall only six from more than 150 organisations are participating in all three organisations.

Annex A   Analysis of SplitArchitecture for LTE backhaul

The initial use cases of the Split Architecture for mobile backhaul in the Long Term Evolution (LTE) mobile system has been described in Section 2.2.1.4 of SPARC Deliverable 2.1 "Initial definition of use cases and carrier requirements" [1] and defined a high-level approach where the OpenFlow can potentially be deployed:

1. High capacity packet transport service between mobile base station and SGW (S1 interface).

2. Shared network where typically more than one provider utilizes the same mobile base station and same backhaul, but still uses separate mobile core networks (MME/SGW).

3. Distributed mobile service to enable local cashing and selective traffic off-load, e.g., supported by the 3GPP SIPTO (Selective IP Traffic Offload) approach [8]

4. Inter-base station connectivity (X2), supporting simple configuration of connectivity between neighbouring base stations.

5. Fixed-Mobile Convergence (FMC) to support, the increasing capacity demand by utilizing fixed-line access / aggregation between other access points (e.g., WiFi) to PGW (S2 interface).

6. 3GPP ANDSF (Access Network Discovery Selection Function) [10], where the operator can steer mobility between access types, e.g., based on SSID.

7. FMC supporting common network functions (like QoS, policy control, AAA, etc.).

The first five use cases have been further analysed and are documented in the following. Before details of potential implementation options for the use case are presented, details about the LTE data plane and Evolved Packet System (EPS) incorporating both E-UTRAN (radio) and Evolved Packet Core parts of the EPS are presented. In addition, a proposal for extension of OpenFlow for interworking with the LTE data plane is presented.

A.1   EPS architecture

The LTE architecture and functionality described in the present document is based on 3GPP Releases 8 and higher available at [4] and reflects the features only relevant for use of OpenFlow in the context. The EPS network elements are illustrated in [5] an overview is shown in the Figure 47 below.
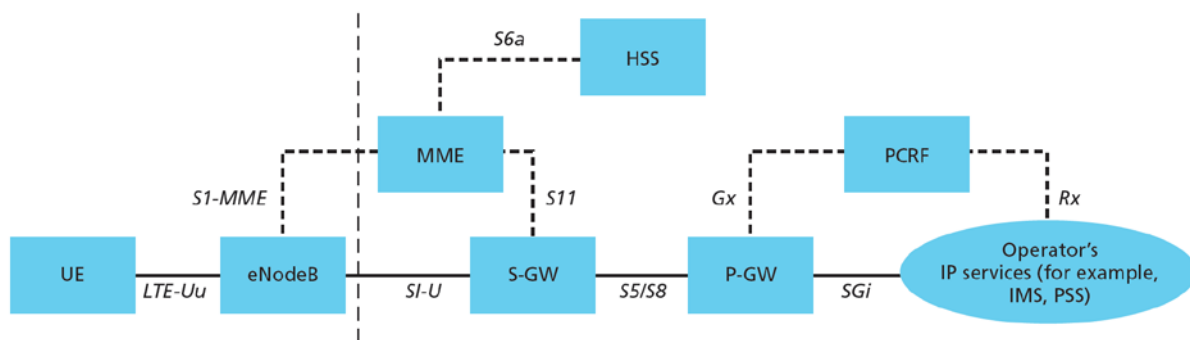
Figure 47: Evolved Packet System network elements and interfaces

In Figure 47, the E-UTRAN part of the EPS compromise of User Equipment (UE) and base station (eNodeB), whereas SGW (Serving SAE Serving Gateway or simply Serving Gateway), MME (Mobile Management Entity), HSS (Home Subscriber Server), PGW (Packet Data Network Gateway) and PCRF (Policy Control and Charging Function) comprise the EPC part of the EPS. Each of the network elements is interconnected by means of standardised interfaces (such as S1, X2 etc) to allow multi-vendor compatibility. This implies that modifying the interface (i.e. its protocol stack and procedures) is not possible without disrupting the interoperability and should be avoided (unless the change of the interface will greatly benefit the use of OpenFlow).

A.2   Transport across EPS interfaces

The following figure illustrates how the IP packets from the UE are delivered to the PGW. The figure represents the end-to-end user (data) plane protocol stack from the UE via the eNodeB and SGW to PGW as shown in [5].
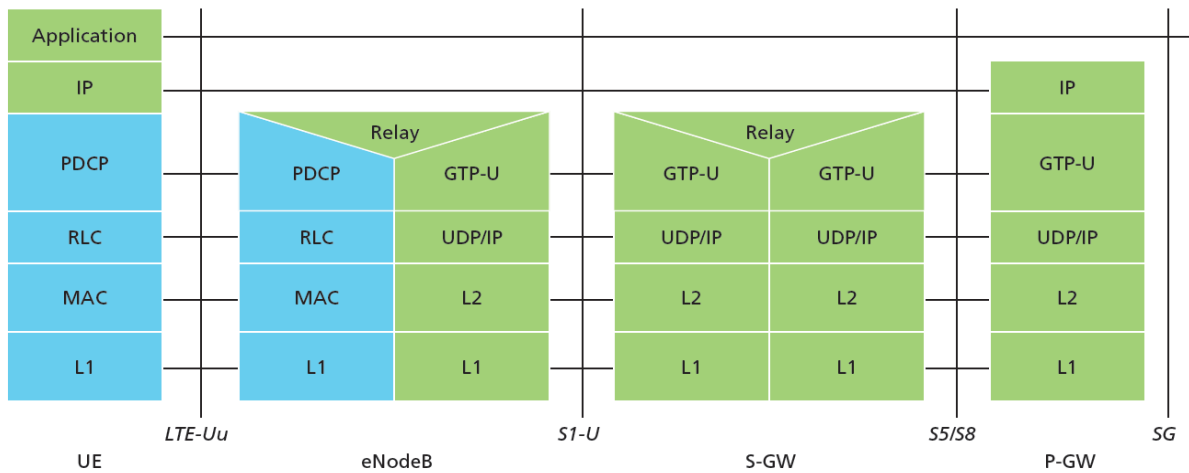
Figure 48: EPS data plane protocol stack

The IP packets from the UE are encapsulated and transported in the GTP-U (user-plane GPRS transport protocol) layer across the radio interface (LTE-Uu), the user-plane interface S1-U between the eNodeB and SWG [6] and between the S5/S8 interface between the SGW and PGW [6]. Note that other protocols, like Proxy Mobile IP PMIP protocol, can be used instead of GTP in other implementations.

The encapsulation in GTP-U is required to support multiple bearers (switched paths with a specified QoS) carrying different services across the interfaces.

The GTP-U is the user-plane 3GPP GPRS tunnelling protocol, which in particular facilitate intra-3GPP mobility and interoperability with legacy UMTS and GPRS technologies. The GTP-U packets are transported by UDP on the top of UDP/IP/L2/L1 stack [7]. Note that additional layer of IPSec can be used (and formally mandated, but not always implemented) in the stack, but omitted here for simplicity. The GTP-U is used at two interfaces: S1 and S5/S8. The bear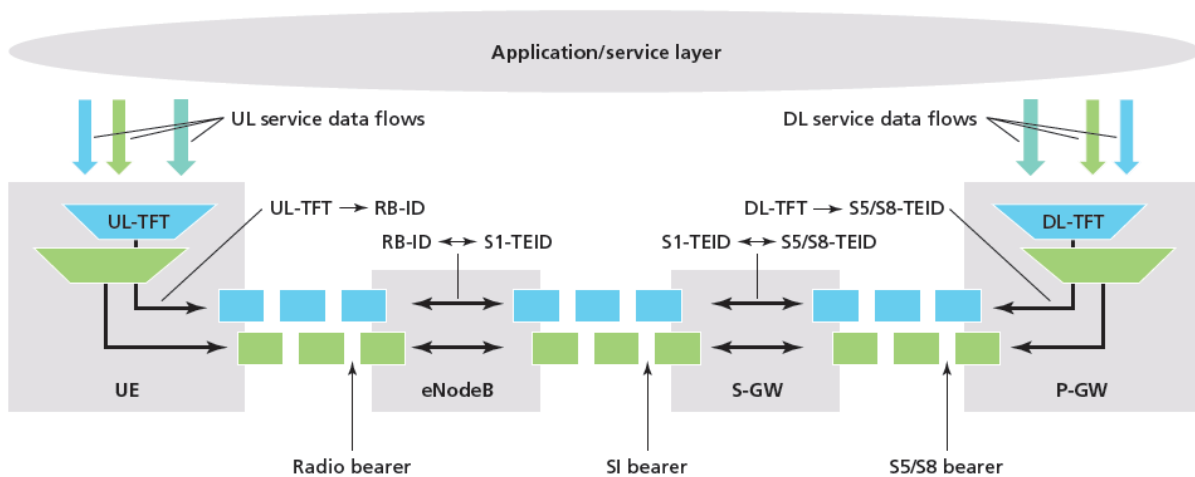er is identified by the source TEID (Tunnel Endpoint ID), destination TEID, source IP address and destination IP address. The bearer concept and identification is illustrated in Figure 49 [5].

Figure 49: LTE bearers across the difference interfaces

Outside IP packets (uplink at UE and downlink at PGW) are mapped at UE and PGW to the respective bearers using the Traffic Flow Templates (TFT). The TFT uses the source and destination IP addresses and TCP port numbers to filter packets (such as VoIP or web-browsing) into respective bearers.

The bearers are established at command from PCRF (Policy Control and Charging Rules Function, see [5]) by communicating to PGW, which in turn send the QoS and TFT parameters to SGW and are further forwarded to MMS which manages the Bearer Setup Request to eNodeB. The QoS information is used by eNodeB to ensure appropriate treatment of packets according to this QoS in particular at the radio interface. The bearer setup can also be triggered by the UE (as it is done for the initial default bearer) and triggered by the external IMS platform.

Each bearer corresponds to a certain Quality-of-Service (QoS), which is characterised by a corresponding QoS Class Identifier (QCI) which have a number of standardised values as illustrated in [5].

QCI	RESOURCE TYPE	PRIORITY	PACKET DELAY BUDGET (MS)	PACKET ERROR LOSS RATE	EXAMPLE SERVICES
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real-time gaming
5	Non-GBR	1	100	10^{-6}	IMS signaling
6	Non-GBR	7	100	10^{-3}	Voice, video (live streaming), interactive gaming
7	Non-GBR	6	300	10^{-6}	Video (buffered streaming)
8	Non-GBR	8	300	10^{-6}	TCP-based (for example, WWW, e-mail), chat, FTP, p2p file sharing, progressive video and others
9	Non-GBR	9	300	10^{-6}	

Figure 50: Standardized QCI for LTE

The bearers are broadly divided in minimum Guaranteed Bit-Rate (GBR) and non-GBR. Each bearer is also associated with a value of Allocation and Retention Priority (ARP), a number between 0 and 15, which is used for bearer admission control, i.e. affects the decision whether the bearer can or cannot be established in the case of radio congestion and also governs priorities in the potential bearer pre-emption (in case a new high-priority bearer needs to be established). Ten classes of ARP are reserved for commercial use and the others for other services (emergency, public, security, administration). ARP values are stored at HSS.

A.3   General approach for introducing OpenFlow in LTE

In the general case, it is assumed that the elements of EPS (eNodeB, SGW and PGW) are not connected directly to each other, but have other network elements (say switches and routes) interconnecting them, as shown in Figure 52. The number of devices between the different elements could differ in practice. For example, the Figure 4 in D2.1 shows an fixed mobile integrated network layout with four or five different network elements in between eNodeB and S-GW (interface SI-U). In the techno-economic assessment study of mobile backhaul presented in section 3, a separate network with three devices has been assumed.
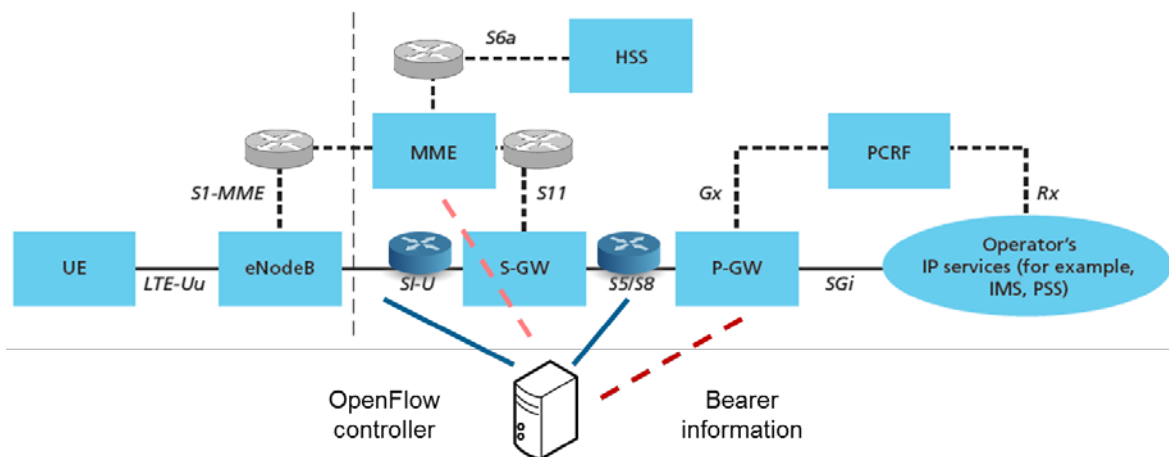
Figure 51: LTE elements as part of a general network and integration of OpenFlow

eNodeB, SGW and PGW have the ability to read the GTP-U packets, identify the bearers and handle the bearer packets according to its QoS (via policing/shaping, queuing, and scheduling). 3GPP TS 36.414 version 10.1.0 Release 10 [6] specifies that "IP Differentiated Services code point marking (IETF RFC 2474) shall be supported. The mapping between traffic categories and DiffServ code points shall be configurable by O&M based on QoS Class Identifier (QCI) Characteristics and others E-UTRAN traffic parameters". We have not found a similar 3GPP spec on DiffServ for s5/s8, but assume that if SGW supports it on one interface, it should be able to support it on the other.

Using OpenFlow in this environment requires that one is able to perform normal IP routing, which OpenFlow supports, as well as support for DSCP based QoS treatment, which is not explicitly supported in the standards. However, this

would be something very simple to add by making sure that the port queues prioritizes based on the DSCP markings, see the section on Quality of Service (Section 5.2) in Deliverable 3.3 for more details. Another possibility might be to have an interworking function between the different QoS classes of the mobile and fixed network. Here OpenFlow matching could be a viable solution.

Integration into an OpenFlow-enabled mobile backhaul transport network could be provided by adding bearer information to the OpenFlow system (already indicated as SDN controller in Figure 52). This bearer information is forwarded to the SDN controller, which uses the information and modifies scheduler and QoS policier accordingly. How this information is transferred to or retrieved by the SDN controller (or an network application representing the traffic engineering) is out of scope of this study.

A.4   Elaboration of use-case

A.4.1   High-capacity packet transport service between mobile base station and SGW (S1 interface)

The LTE mobile base station – eNodeB – is connected to the Serving Gateway (SGW) via the S1-U interface where "U" stands for user (data) plane. The protocol stack for this interface is shown below [5].
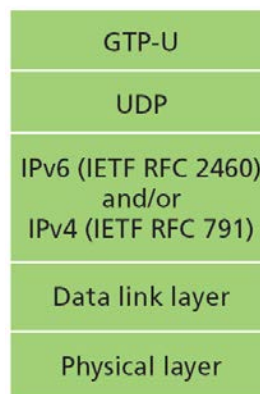
Figure 52: S1-U user plane protocol stack

The OpenFlow solution for the S1-U interface is a partial case of the solution covered in Section A.3 "General approach for introducing OpenFlow in LTE".

A.4.2   Shared network where typically more than one provider utilizes the same mobile base station and same backhaul but still uses separate mobile core networks (SGW/MME)

This use-case can be further generalized to running multiple LTE mobile operators on the same OpenFlow-supported infrastructure. The case is illustrated in the picture below.
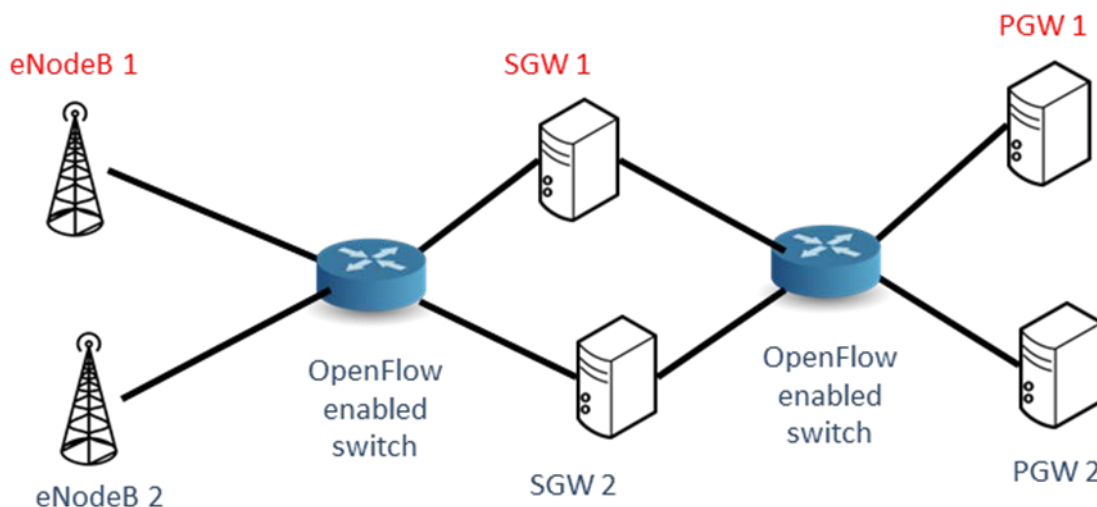
Figure 53: Multiple LTE operators on the single OpenFlow-enabled infrastructure

This subject is dealt with in Section 5.8 of Deliverable 3.3, "Virtualization and Isolation", which presents a solution able to provide virtual networks that supports common SLA requirements.

A.4.3 Distributed mobile service to enable local cashing and selective traffic offload e.g. supported by the 3GPP SIPTO approach

The selective IP traffic off-load (SIPTO) specified in 3GPP TS 23829 [8] assumes the offload of mobile unit traffic to e.g. Internet when connected to a Home eNodeB (femto node) directly to the Internet without traversing the operator mobile network as generally illustrated in the Figure below. Such functionality offload can be implemented in a number of ways for various scenarios as described in [8].
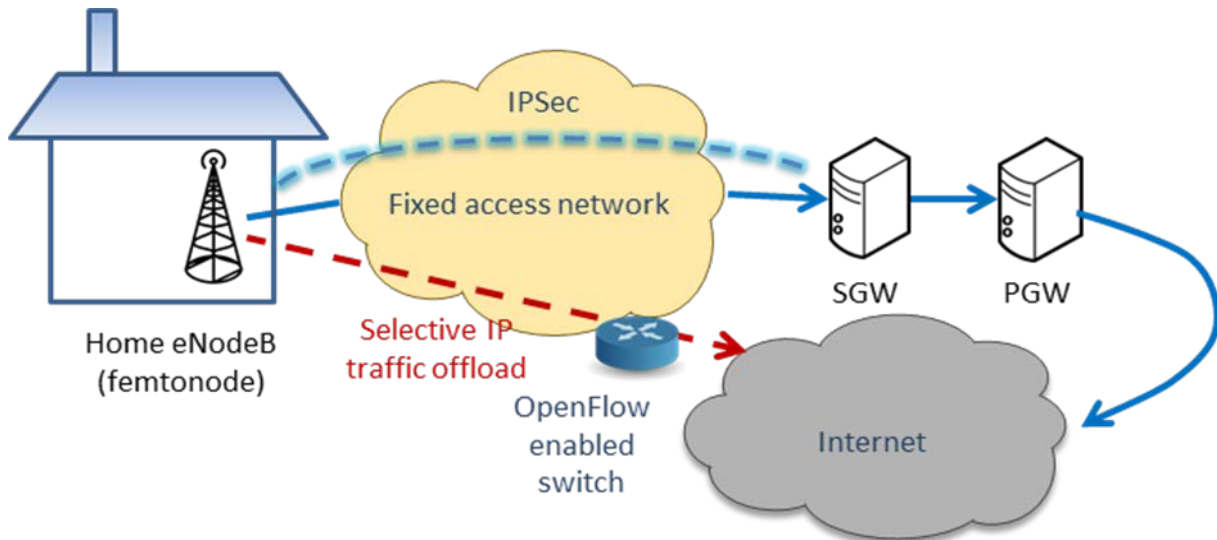
Figure 54: Selective IP traffic offload for Home eNodeB (femtonode)

In this case, the possibility to use the current OpenFlow solution will depend on whether Home eNodeB supports the mapping of QCI classes to DSCP markings and whether the access (and also residential/enterprise) networks being traversed by the offload traffic are OpenFlow-enabled. If both conditions are satisfied, then the general approach described in Section A.3 applies here as well.

A.4.4 Inter-base station connectivity (X2) supporting connectivity between neighbouring base stations.

The X2 interface is used to interconnect eNodeBs and the X2 data plane interface (for inter-base station connectivity) uses the same protocol stack as the S1 interface between eNodeB and SGW as illustrated in Figure 55 below.
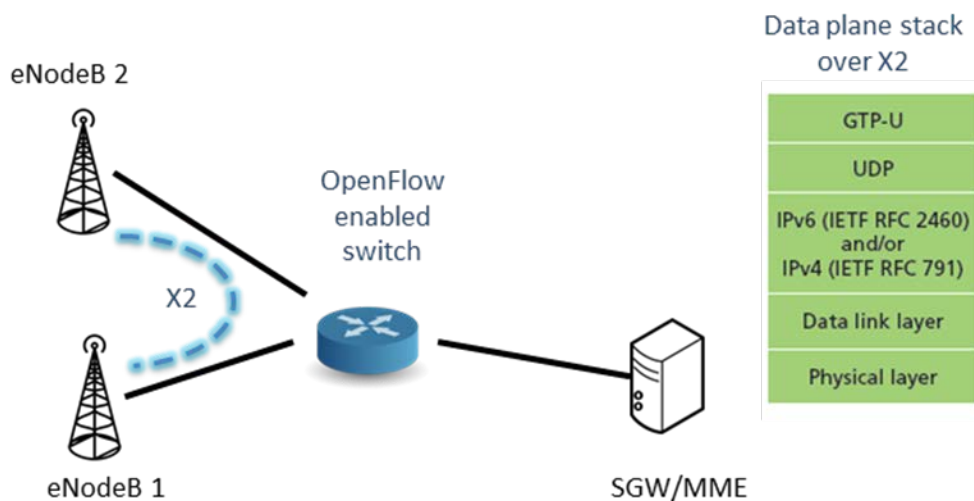
Figure 55: X2 interface between two base stations and its data plane stack

Furthermore, 3GPP TS 36.424 version 10.1.0 Release 10 [9][10] mandates the same support for DiffServ code points (IETF RFC 2474) based on QoS Class Identifier as for S1 interface. This makes possible to use the same approach for using OpenFlow on this interface as it has been done for S1 interface in Section A.4.1.

A.4.5   Fixed-mobile convergence (FMC) to support the increasing capacity demand by utilizing fixed-line access aggregation between other access points (e.g. WiFi) to PGW (S2 interface).

Non-3GPP access to the EPS is specified in 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses" [10] and illustrated for the case on untrusted access (using the evolved Packet Data Gateway – ePDG, and its interface s2b) in the Figure below:
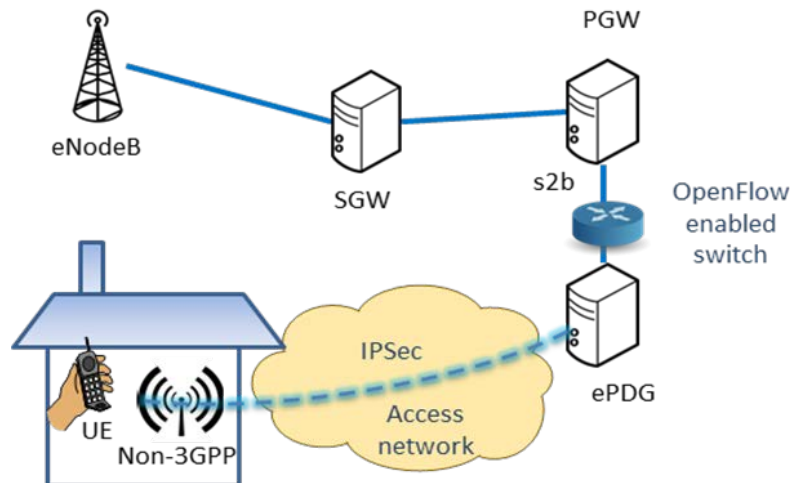
Figure 56: Untrusted non-3GPP access using s2b interface

The s2b interface between ePDG and PGW can be GTP or Proxy Mobile IPv6 (PMIPv6) based in the similar way as the s5/s8 interface between PGW and SGW. If the GTP-based interface s2b is used, the establishment of bearers (default and dedicated) is similar to that over the GTP-based S5/S8 interface. Furthermore, the uplink TFT template at the ePDG maps the uplink traffic to the corresponding bearers (as established by the TFT) towards the PGW in the same way as done by the TFT at the UE in the 3GPP access case. The use of DSCP is not explicitly mandated for ePDG and PGW by [10], but if supported the approach for using OpenFlow with DSCP markings described in Section A.3 applies.

The data between ePDG and UE are transported using IPSec, which carries the packets of all s2b bearers. In this case, it is not possible in a straightforward way to provide OpenFlow support to separate bearers. However, for the aggregate stream (e.g. to prioritise it over the other traffic in the access network) the use of OpenFlow for this interface can be considered similarly as for use–case 3 (SIPTO offload).

Annex B   Updated list of requirements

In order to give an overview, all requirements derived from the three different use case areas are summarized in the following Table 4. The definition of the use cases results in a mix of general and use case specific requirements. However, not all requirements are meaningful and specific with respect to a Split Architecture or different implementations of OpenFlow. Therefore an evaluation of all requirements with respect to the potential impact on a Split Architecture and/or OpenFlow extensions is given. A high degree of impact is indicated by "**", some potential impact is indicate by "*".

So the most important requirements to be considered in the future discussion about the blue-print of a Split Architecture are those indicated with one or more "*".

No.	Requirement	Importance of Requirement	Missing in OpenFlow / SplitArchi.	Covered by Requirement group of D2.2
R-1	A wide variety of services / service bundles should be supported.	**	-	(d)
R-2	The Split Architecture should support multiple providers.	**	-	(d)
R-3	The Split Architecture should allow sharing of a common infrastructure, to enable multi-service or multi-provider operation.	**	-	(d)
R-4	The Split Architecture should avoid interdependencies of administrative domains in a multi-provider scenario.		**	(d)
R-5	The Split Architecture should support operation of different protocols / protocol variations at the same OSI layer in case of shared networks.	**	**	(a)
R-6	The Split Architecture should support policy based network control of network characteristics.	**	**	(h)
R-7	The Split Architecture shall enforce requested policies.	**	**	(h)
R-8	The Split Architecture should support automatic transfer methods for distribution of customer profiles and policies in network devices.		**	
R-9	The Split Architecture should support TDM emulation and/or mobile backhaul.	*	**	
R-10	The Split Architecture should provide sufficient customer identification.	**	**	(h)
R-11	The Split Architecture should support best practices for QoS with differentiated, four classes according to the definition documented by the Metro Ethernet Forum.	**	*	(j)
R-12	The Split Architecture should handle data not carrying QoS class identifier as default class.	**	**	(j)
R-13	The Split Architecture should map data carrying invalid QoS class identifier to a valid QoS class.	**	**	(j)
R-14	The Split Architecture must handle control data as highest priority class.	**		(j)
R-15	The Split Architecture should support Source-Specific Multicast.			
R-16	The Split Architecture must control the access to the network and specific services on an individual service provider basis.	*	**	
R-17	The Split Architecture should provide mechanisms to control broadcast domains.			(b)
R-18	The Split Architecture should support enforcement of traffic directions.			(b)
R-19	The Split Architecture should support control mechanisms for identifier. This should include any		**	(b)

	kind of identifiers like addresses or protocols as well as limitation for send rate.			
R-20	The Split Architecture should prevent any kind of spoofing.	**		
R-21	The Split Architecture should monitor information required for management purposes.	**	**	(b)
R-22	The Split Architecture should generate traps when rules are violated.	**	**	(b)
R-23	The Split Architecture should extract accounting information.	**	**	(b), (h)
R-24	The Split Architecture should collect traffic statistics.	**	-	(b)
R-25	The Split Architecture should support OAM mechanisms according to the applied data plane technologies.	**	**	(e)
R-26	The Split Architecture should make use of OAM functions provided by the interface.	**	**	(e)
R-27	The Split Architecture shall support the monitoring of links between interfaces.	**	**	(b), (e), (g)
R-28	The data path element should provide logically separated access to its internal forwarding and processing logic in order to control both independently.	**	**	(c)
R-29	It should be possible to define chains of processing functions to implement complex processing.	**	**	
R-30	The Split Architecture shall support deployment of legacy and future protocol/service-aware processing function.	**	**	(c)
R-31	The introduction of a new protocol/service aware processing function should not necessitate the update of other functions.	**	**	(c)
R-32	The architecture of a data path element shall support loading of processing functions at run-time without service interruption.	**	**	(c)
R-33	A processing function instance should be controllable at run-time by the associated control entity in the control plane.	**	**	(c)
R-34	A processing function should expose module specific configuration parameters to an associated entity in the control plane.	**	**	(b)
R-35	The Split Architecture should allow the exchange of opaque control information between a processing function on the data path element and the associated control entity with a well-defined protocol.	**	**	(a), (b)
R-36	The level of detail exposed by a processing module is module and vendor specific. However, each processing module should support a common API for control purposes.	**	**	(b)
R-37	Urgent notifications sent by a data path element should be prioritized and not be delayed by data traffic to the controller.	**	**	(j)
R-38	A data path element classifier should be constructed in a protocol agnostic manner or should be at least flexible enough to load new classifier functionality as a firmware upgrade with identical performance.	**	**	
R-39	The Split Architecture should introduce a clean split between processing and forwarding functionality.	**	**	

R-40	The Split Architecture should provide means to control processing functions from a controlling entity on heterogeneous hardware platforms.	**	**	(a)
R-41	Providers should have a maximum degree of freedom in the choice of data centre technologies.	-	**	(d)
R-42	Data centre virtualization must ensure high availability.	*	**	(d), (f)
R-43	The Private Cloud provisioning and management system shall have the ability to dedicate a specific share of resource per VPN.	**	-	(d)
R-44	Each VPN may have the exclusive access to the specific share of resource.	-	-	(d)
R-45	Each VPN shall have the ability to hold the requested resources without sharing with any other parties	**	-	(d)
R-46	Each VPN may have the ability to limit the stored data mobility to a certain geographic region confinement (country/state).	-	**	
R-47	The restoration capability awareness should to be scalable.	-	-	(f)
R-48	The virtualization functions QoS requirement should be synchronized with VPN service.	-	-	(j)
R-49	The VPN extension should support the network condition to be used for the traffic balancing and congestion avoidance decision-making.	-	*	
R-50	The VPN resource requested by the server can be optimized by statistical multiplexing of the resource.	-	*	
R-51	The VPN Extension should support the automatic end-to-end network configuration.	-	*	(b), (g)
R-52	Quality of Experience management should to be supported.	-	*	(b)
R-53	The data path element should expose to the load balancer/network controller the information regarding their availability, connections to other elements and load situations.	**	-	(b)
R-54	The data path element should provide an API exposing mechanism that can be used to configure for switching/routing flows of packets.	**	-	(b)
R-55	The Server/VM manager should expose to the load balancer/network controller the information regarding the operation of VMs including availability, load situation and the association to the servers.	**	-	(b)
R-56	The Server/VM manager should provide an API exposing mechanisms that can be used to control the instantiation and migration of VMs across the server farm.	**	-	(b)
R-57	The load-balancing solution should support L2-L7 flow detection/classification.	**	*	
R-58	The load-balancing solution should provide session persistence.	**	*	
R-59	The data path element should provide an API exposing mechanisms for switching the data path element between sleep/normal operation modes.	**	*	(i)
R-60	The data path element should expose metrics that can be used by energy optimization algorithms.	**	**	(b), (i)
R-61	The network management and configuration must provide predictable and consistent capabilities.	**	-	(b)
R-62	The network management and configuration should provide a cost vs. benefit ratio better than	-	-	(b)

	today's approaches.			
R-63	The OF domain should be able to interact with other domains through EGP.	*	**	
R-64	Information of a lower layer has to be exposed to a higher layer appropriately.	**	**	(a)
R-65	A data path network element should enable control plane applications to poll detailed configuration attributes of circuit-switching capable interfaces.	**	**	(k)
R-66	A data path element should enable control plane application to set configuration attributes of circuit-switching capable interfaces.	**	**	(k)
R-67	The Split architecture may allow implementing additional OAM solution when the interface does not provide any.	*	**	(e)

Annex C   ONF, ATCA and OpenStack membership overview

C.1   ONF, ATCA (executive & associate) and OpenStack members

Company	Country	Number of employees 2011	Net sales 2011 in $
Cisco Systems	USA	71.825	$43.218.000.000
Intel	USA	100.100	$53.999.000.000
Alcatel-Lucent	France	76.002	$19.325.431.850
IBM	USA	433.362	$106,900,000,000
Extreme Networks	USA	732	$ 334,428,000
Mellanox	USA	778	$259.251.000

C.2   ONF and ATCA executive members

Company	Country	Number of employees 2011	Net sales 2011 in $
Ericsson	Sweden	104.525	$33.911.224.032
Freescale	n.a.	n.a.	n.a.
Fujitsu	Japan	173.000	$56.956.393
Metaswitch Networks	UK	n.a.	n.a.
NEC	Japan	142.358	$47.326.944.900
Nokia Siemens Networks	Finland	71.825	$17.703.946.539
Oracle Corporation	USA	108.000	$35.622.000.000
Texas Instruments	USA	34.759	$13.735.000.000
ZTE Corporation	China	89.786	$1.099.645

C.3   ONF and OpenStack members

Company	Country	Number of employees 2011	Net sales 2011 in $
Brocade Communications Systems	USA	4.546	$2.147.442.000
Huawei Technologies	China	140.000	$203.396.000.000
Dell	USA	103.300	$61.494.000.000
VMware	USA	11.000	$3.767.096.000
Hewlett-Packard	USA	349.600	$127.245.000.000
Big Switch Networks	USA	n.a.	n.a.
Broadcom Corporation	USA	9.590	$7.389.000.000
Citrix	USA	6.936	$2.206.392.000
F5 Networks, Inc.	USA	2.488	$1.151.834.000
Juniper Networks	USA	9.129	$4.448.700.000
LineRate Systems	USA	n.a.	n.a.
Midokura	Japan	n.a.	n.a.
NTT Communications	Japan	49.991	$13.174.653
Spirent Communications plc	UK	1.500	$528.200.000

C.4   ATCA associate and OpenStack members

Company	Country	Number of employees 2011	Net sales 2011 in $
NetApp	n.a.	n.a.	n.a.

Arista Networks	USA	n.a.	n.a.

C.5   ONF members

Company	Country	Number of employees 2011	Net sales 2011 in $
6WIND	France	n.a.	n.a.
A10 Networks	USA	n.a.	n.a.
ADVA Optical Networking	Germany	1.304	$392.006.052
Argela	Turkey	n.a.	n.a.
Aricent Inc.	USA	n.a.	$563.000.000
Ciena Corporation	USA	4.339	$1.741.970.000
Colt	UK	n.a.	$1.959.778.086
Comcast Corporation	USA	126.000	$55.842.000.000
CompTIA	USA	n.a.	n.a.
Cyan	USA	200	n.a.
Deutsche Telekom	Germany	240.000	$74.013.365.276
Elbrys Networks	USA	n.a.	n.a.
ETRI	South Korea	n.a.	n.a.
EZchip	Israel	164	$63.457.000
Facebook	USA	2.661	$3.825.000.000
Force10networks	USA	n.a.	n.a.
France Telecom Orange	France	n.a.	$57.088.639.516
Gigamon	USA	n.a.	n.a.
Google	USA	32.467	$37.905.000.000
Hitachi	Japan	361.745	$112.401.000.000
Infinera	USA	1.181	$404.877.000
Infoblox	USA	494	$133.000.000
IP Infusion	USA	n.a.	n.a.
Ixia	USA	1.300	$249.670.000
Korea Telecom (KT Corporation)	South Korea	31.215	$19.089.000.000
LSI Corporation	USA	n.a.	$2.043.958.000
Luxoft	Russia	n.a.	n.a.
Marvell Technology Group Ltd	USA	5.893	$3.611.893.000
Microsoft	USA	90.000	$69.943.000.000
NCL Communications K.K.	Japan	n.a.	n.a.
Netgear	USA	791	$1.181.018.000
Netronome	USA	n.a.	n.a.
Nicira Networks	USA	n.a.	n.a.
PICA8	USA	16	$1.100.000
Radware	Israel	733	$167.020.000
Riverbed Technology	USA	1.610	$726.476.000
Samsung	South Korea	190.464	$143.069.254.000
SK Telecom	South Korea	n.a.	$13.789.000
Telecom Italia	Italy	84.889	$29.957.000
Tencent Holdings Limited	China	17.446	$363.292
Verizon	USA	193.900	$110.875.000.000

C.6   ATCA executive members

Company	Country	Number of employees 2011	Net sales 2011 in $
ADLINK Technology Inc.	Taiwan	n.a.	$173.785.767
Advanced Micro Devices, Inc.	USA	11.100	$6.568.000.000
Advanet Inc.	Japan	n.a.	n.a.
Advantech Co., LTD	Taiwan	3.000	$886.095.468
Aeroflex Incorporated	USA	2.900	$729.400.000
Agilent Technologies Inc.	USA	18.700	$6.615.000.000
Applied Micro	USA	728	$230.887.000
Astek Corporation	USA	45	$3.000.000
ATP Electronics Inc.	USA	220	$45.800.000
BAE Systems	UK	93.500	$30.446.669.846
CBT Technology Inc.	USA	458	$45.100.000
congatec AG	Germany	124	$60.143.740
Cypress Point Research	USA	n.a.	n.a.
Dawn VME Products	USA	45	$7.900.000
Elma Bustronic Corporation	USA	n.a.	n.a.
Elma Electronic, Inc.	Switzerland	280	$70.100.000
Emerson	USA	133.200	$24.222.000.000
ERNI Electronics GmbH	Germany	650	$151.305.006
Eurotech S.p.A.	Italy	463	$118.282.688
Fci Usa Llc	USA	14.000	$1.100.000.000
Foxconn Electronics	USA	140	$22.500.000
GE Intelligent Platforms	USA	n.a.	n.a.
General Micro Systems Inc.	USA	62	$12.900.000
Harting Inc. Of North America	USA	100	$18.500.000
HEITEC AG	Germany	850	$107.174.379
JBlade LLC	USA	n.a.	n.a.
JumpGen Systems	USA	10	$750.000
Kontron AG	Germany	2.978	$743.411.928
LiPPERT Embedded Computers	Germany	n.a.	n.a.
MEN Mikro Elektronik GmbH	Germany	n.a.	n.a.
Mercury Computer Systems, Inc.	USA	602	$229.000.000
MSC Vertriebs GmbH	Germany	n.a.	n.a.
n.a.T. GmbH	Germany	n.a.	n.a.
Narinet, Inc.	South Korea	n.a.	n.a.
National Instruments	USA	6.235	$1.020.000.000
OKI Networks Co., Ltd.	Japan	n.a.	$5.457.830
Padtec S.A.	Brazil	n.a.	n.a.
Pentair Technical Products	USA	250	$42.500.000
PFU Systems, Inc.	USA	39	$3.700.000
Pigeon Point Systems, LLC.	USA	n.a.	n.a.
Portwell, Inc.	USA	90	$47.800.000
PT	USA	143	$36.200.000
Radisys Corporation	USA	1.024	$330.865.000
RTD Embedded Technologies, Inc.	USA	53	$10.000.000

Sanritz Automation Co., Ltd.	Japan	n.a.	n.a.
Simonson Technology Services	USA	n.a.	n.a.
SLAC National Accelerator Laboratory	USA	1.500	n.a.
Southco Inc.	USA	2.800	$206.000.000
Telco Systems	USA	85	$14.500.000
Thales Australia	Australia	n.a.	n.a.
Trenton Technology Inc.	USA	n.a.	n.a.
UBER Co., Ltd.	Japan	n.a.	n.a.
VadaTech Inc.	USA	2	$140.000
VTI Instruments Corporation	USA	n.a.	n.a.
Wavetherm Corporation	USA	n.a.	n.a.
Yamaichi Electronics	Japan	3.860	$349.211.000
ZNYX Networks	USA	95	$20.400.000

C.7   OpenStack members

Company	Membership status
AT&T	platinum
Ubuntu/Cannonical	platinum
Nebula	platinum
Rackspace	platinum
Red Hat	platinum
SUSE	platinum
CCAT	gold
Cloudscaling	gold
Mirantis	gold
Morphlabs	gold
NEC	gold
Piston Cloud	gold
Yahoo!	gold
Cloudwatt	corporate sponsors
Enovance	corporate sponsors
Gale Technologies	corporate sponsors
Gridcentric	corporate sponsors
Internap	corporate sponsors
Metacloud	corporate sponsors
Paypal	corporate sponsors
RiverMeadow Software	corporate sponsors
Smartscale Systems	corporate sponsors
Transcend Computing	corporate sponsors
Xemeti	corporate sponsors
ActiveState	more supporters
Akamai	more supporters
Alertlogic	more supporters
Alpha Engineering	more supporters
AMD	more supporters
AppDynamics	more supporters

Appfog	more supporters
apriorit	more supporters
Aptira	more supporters
Axelaris	more supporters
B1 systems	more supporters
Bit-isle	more supporters
Bull	more supporters
Calexda	more supporters
catalyst	more supporters
EFEngine	more supporters
Cirrascale	more supporters
ClearPath	more supporters
cloudcentral	more supporters
cloudcruiser	more supporters
Cloud9ers	more supporters
CloudBees	more supporters
Cloudian	more supporters
Cloudpassage	more supporters
Cloudscale	more supporters
ComputeNext	more supporters
Convirture	more supporters
CSS corp	more supporters
Ctera	more supporters
CumuLogic	more supporters
Cybera	more supporters
Datadog	more supporters
Docomo innovations	more supporters
Dome 9	more supporters
EnStratus	more supporters
Equinix	more supporters
Fathomdb	more supporters
FEELingK (FLK)	more supporters
ForLinux	more supporters
GigaSpaces	more supporters
Gladinet	more supporters
Grid Dynamics	more supporters
Hastexo	more supporters
HyperStratus	more supporters
HyperTection	more supporters
Intalio	more supporters
I-Soft	more supporters
It synergy	more supporters
JDN ICT services	more supporters
Juniper Networks	more supporters
Mach technology	more supporters
Maldivica	more supporters
Memset	more supporters

MPSTOR	more supporters
Blitz	more supporters
NASA	more supporters
New Relic	more supporters
Nodeable	more supporters
Nuage & co	more supporters
Nubefy	more supporters
Objectif libre	more supporters
Opscode	more supporters
Opsview	more supporters
Ow2	more supporters
Puppet labs	more supporters
Quanta Computer	more supporters
Quorum Labs	more supporters
Rec5	more supporters
RightScale	more supporters
ScaleXtreme	more supporters
Scalr	more supporters
ServiceMesh	more supporters
SME	more supporters
Solidfire	more supporters
Sonian	more supporters
Spiceworks	more supporters
StackOps	more supporters
SwiftStack	more supporters
Tail-f	more supporters
UShareSoft	more supporters
VEXXHOST Inc.	more supporters
Vyatta	more supporters
Xeround	more supporters
Zadara	more supporters
Zenoss	more supporters
ZeroNines	more supporters
Zeus	more supporters

References

[1]   SPARC D2.1, "Initial definition of use cases and carrier requirements," 2011.

[2]   SPARC D2.2, "Revised definition of use cases and carrier requirements".

[3]   SPARC D3.3, "Split Architecture for Large-Scale Wide-Area Networks".

[4]   www.3gpp.org.

[5]   www.alcatel-lucent.com, "The LTE Network Architecture. Strategic White Paper".

[6]   "3GPP TS 36.414 version 10.1.0 Release 10 "S1 data transport"".

[7]   "3GPP TS 29.281 version 10.3.0 Release 10 "Tunnelling Protocol User Plane (GTPv1-U)"".

[8]   "3GPP TS 23829 Release 10.0.1 - Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)".

[9]   "3GPP TS 36.424 version 10.1.0 Release 10 - X2 data transport".

[10]   "3GPP TS 23.402 v11.3.0. (2012-06)"Architecture enhancements for non-3GPP accesses"".

[11]   Information Technology Infrastructure Library (ITIL), available online
        http://www.itil-officialsite.com/home/home.asp

[12]   SPARC D3.1, "Initial Split Architecture and Open Flow Protocol study".

[13]   SPRAC D3.2, "Update on Split Architecture for Large Scale Wide-area Networks".

[14]   SPRAC D4.1, "Status Report on the Prototype of Integrated OpenFlow Reference Architecture".

[15]   SPARC D4.2, "Description of OpenFlow protocol suite extensions".

[16]   SPARC D4.3, "Description of the implemented architecture".

[17]   SPARC D5.1, "Description of emulation platform architecture and according implementation plans".

[18]   SPARC D5.2, "Report on validation and performance evaluation experiments".

[19]   SPARC D6.1, "First annual dissemination report".

[20]   SPARC D6.2, "Second annual dissemination report".

[21]   ICT ALIEN project, http://www.fp7-alien.eu/

[22]   Michael Kennedy, "A TCO Analysis of Ericsson's Virtual Network System Concept Applied to Mobile Backhaul", ACG Research Inc., available at http://www.acgresearch.net/UserFiles/File/Business%20Case%20Analysis%20Docs/Ericsson%20White%20Paper_Virtual%20Network_ACG%20Research_2012(1).pdf

[23]   S. Verbrugge, D. Colle, M. Pickavet, P. Demeester, S. Pasqualini, A. Iselt, A. Kirstädter, R. Hülsermann, F.-J. Westphal, and M. Jäger, "Methodology and Input Availability Parameters for Calculating OpEx and CapEx Costs for Realistic Network Scenarios," Journal of Optical Networking, Vol. 5, No. 6, pp. 509–520, June 2006